



Bu kitap, yazarın yazılı izni olmaksızın herhangi bir şekilde kopyalanamaz, çoğaltılamaz, dağıtılamaz veya herhangi bir medya ortamında yayınlanamaz. Yazarın adı ve eserin adı belirtilmeden alıntı yapılamaz. Kitabın bütünü veya herhangi bir kısmı, yazarın yazılı izni olmaksızın herhangi bir dilde basılamaz veya tercüme edilemez.

©Turkcell. 2023.

Siber Güvenlik El Kitabı



DR. ALİ TAHA KOÇ

ÖNSÖZ

Dijital teknolojilerin gelişimiyle birlikte yaşadığımız dönüşümün hızı, her zamankinden daha fazla ve etki alanı daha da genişlemiş durumda. Tıpkı fiziksel uzay gibi sürekli genişleyen siber uzay, yeni nesil siber tehditleri de beraberinde getiriyor. Korumamız gereken dijital varlıkların sayısı gün geçtikçe artıyor.

Siber tehditlerden korunması gereken en kritik varlıkların başında ise “insan” geliyor. Dijitalin Yüzyılı’nda siber tehditlerin yıkıcı etkilerinden uzak kalabilmenin yolu ise toplum genelinde siber güvenlik kültürünü yaygınlaştırmak ve nitelikli uzman yetiştirmekten geçiyor.

Siber güvenliğin yalnızca teknik bir disiplin olmadığı, bugüne kadar yaşanan tecrübelerle yakından anlaşıldı. Siber tehditlerin hem kaynağı hem de engelleyicisi konumundaki “insan” faktörü, siber güvenliği davranış bilimleri, psikoloji ve sosyolojinin de konusu haline getirmiş durumda. Bu alanda teknik becerilerle birlikte empati, yaratıcılık, esneklik, iyi iletişim, sorun çözme ve dikkat becerilerinin de güçlü olması niteliği artıran önemli unsurlar.

Bizler de Türkiye’nin Turkcell’i olarak, ülkemizin Türkiye Yüzyılı vizyonuna ortak oluyor, Türkiye’nin yüzyılının aynı zamanda Dijitalin Yüzyılı olabilmesi için çalışmalarımızı sürdürüyoruz.

Siber Güvenliğin Süper Kadınları programı ile ülkemizin siber güvenlik alanında ihtiyaç duyduğu nitelikli insan kaynağının gelişimine katkıda bulunurken, siber güvenlikte kadınlarımızı daha çok fırsat sunulmasının önünü açmaktan mutluluk duyuyoruz.

Bu programın önemli bir çıktısı olan **Siber Güvenlik El Kitabı** ise programa katılan kadınlarımızın güçlü kalemi ve derin bilgileri ile siber güvenliğe kadın elinin dokunduğu kıymetli bir başucu çalışması oldu. Bu değerli çalışma, odağına yalnızca bu alanlarda faaliyet gösterenleri değil, herkesi alarak 7’den 70’e hepimizin istifade edebileceği bir eser oldu. Bu sayede siber güvenliğe kapsamlı bir giriş yaparak, siber dünyada da kendimizi ve sevdiklerimizi koruyacak, siber dünyanın zararlı ve yıkıcı etkilerinin bizlere ve çevremize sirayet etmesini engelleyeceğiz.

Bu güzel çalışmanın ortaya çıkmasında emeği geçen tüm kadınlarımıza, mentorlarımıza ve Turkcell çalışanlarımıza şükranlarımı sunarım.

Keyifle okunması dileğiyle,

Dr. Ali Taha Koç
Genel Müdür

İçindekiler

SİBER GÜVENLİK	1
BİLGİ GÜVENLİĞİ	7
BİLGİ GÜVENLİĞİ FARKINDALIĞI	13
İNTERNETİN EVRİMİ	17
SİBER GÜVENLİK STANDARTLARI	25
SAĞLIK SEKTÖRÜ AÇISINDAN SİBER GÜVENLİK	29
GÜVENLİ İNTERNET	37
SİBER SİGORTA	45
SİBER GÜVENLİKTE MAKİNE ÖĞRENMESİ	51
ÇOK FAKTÖRLÜ DOĞRULAMA	55
İNTERNETTE GÜVENLİ ALIŞVERİŞ İÇİN İPUÇLARI	61
UZAKTAN ÇALIŞMANIN GETİRDİĞİ RİSKLER VE TEDBİRLER	67
SOSYAL MÜHENDİSLİK	75
FİDYE YAZILIMLARI	81
SIZMA TESTİ	89
GÜVENLİ KOD GELİŞTİRME	95
KİŞİLİKSİZ KİŞİLER	101
MEMORYDEN NASIL BİLGİLER ELDE EDİLİR?	105
ADLİ BİLİŞİM	109
VERİLER SİLİNDİ Mİ?	113
İOS CİHAZ GÜVENLİĞİ	119
E-POSTA GÜVENLİĞİ	127

ÇOCUKLARDA AKILLI SAAT GÜVENLİĞİ	133
FIREWALL İLE ANTİVİRÜS PROGRAMI ARASINDAKİ FARK	141
MOBİL CİHAZ GÜVENLİĞİ	145
USB CİHAZLAR GERÇEKTEN GÜVENLİ Mİ?	151
MODEMİM GÜVENLİ Mİ?	157
ŞARJ KABLOLARI GERÇEKTEN GÜVENLİ Mİ?	169
MOBİL GÜVENLİK	173
WINDOWS PHONE GÜVENLİĞİ	179
BLOCKCHAIN NEDİR VE NASIL ÇALIŞIR?	185
DİJİTAL HAYAT	191
KORUMAMIZ GEREKEN DİJİTAL VARLIKLAR	195
SİBER HİJYEN	199
İNTERNET NASIL ÇALIŞIR?	205
METAVEVERSE	209
DİJİTAL HAYATTAKİ ANAHTARLARIMIZ	213
HALKA AÇIK KABLOSUZ AĞLAR VE RİSKLER	219
SAHTE KABLOSUZ AĞLAR	225
SİBER İSTİHBARAT VE SİBER TEHDİT İSTİHBARATI	233
TEHDİT AKTÖRLERİ VE MOTİVASYON KAYNAKLARI	239
İNTERNETİN KARANLIK DÜNYASI	247
KRİTİK ALTYAPILARIN GÜVENLİĞİ	253
VERİLERİMİZİN DÜŞMANI: KUANTUM BİLGİSAYARLAR	257
SİBER GÜVENLİK TEKNOLOJİLERİ	261
DOS VE DDOS SALDIRILARI	267
ORTADAKİ ADAM SALDIRISI (MITM)	271
İNSANSIZ HAVA ARAÇLARININ SİBER GÜVENLİKTEKİ YERİ	277
KEŞİF	283
PHISHING NEDİR?	289

HONEYPOT NEDİR?	295
OWASP	301
SUNUCU GÜVENLİĞİ	307
SİBER SALDIRILAR VE YAPAY ZEKA	311
DÜNYA TARİHİNDE SES GETİREN HACKERLAR VE YAPTIKLARI SALDIRILAR.....	315
PAROLA SALDIRILARI	321
WEB SHELL	327
DÜNYADAKİ SİBER SALDIRILAR VE ÜLKELERİN ALDIĞI ÖNLEMLER	331
PAROLA GÜVENLİĞİ	341
GÜÇLÜ PAROLANIN ÖNEMİ	347
KRİPTOGRAFİK HASH FONKSİYONLARI	353
VPN NEDİR, GÜVENLİ MİDİR? VPN'E NEDEN İHTİYAÇ DUYARIZ?	361
KRİPTOLOJİ NEDİR?	365
GİZLİLİK VE DİJİTAL GİZLİLİK	371
SOSYAL MEDYA HESABIM ÇALINDIKTAN SONRA NE YAPABİLİRİM?	379
SOSYAL MEDYADAN TACİZ ALTINDAYIM NEREYE BAŞVURMALIYIM?	385
FACEBOOK GÜVENLİĞİ	391
TWITTER GÜVENLİĞİ	397
LINKEDIN HESAPLARIMIZ GÜVENDE Mİ?	405
SİBER GÜVENLİKTE KARIYER	411
SİBER GÜVENLİK KAVRAMLARI	415
AKILLI EV ALETLERİ VE GÜVENLİĞİ	423
BİLİŞİM SUÇLARI NELERDİR?	429
BLOCKCHAIN'İN SİBER GÜVENLİKTE ROLÜ	435
SIZMA TESTİ RAPORU	441

MENTORLARIMIZ



DUYGU
FİDANCIOĞLU

T.C. Cumhurbaşkanlığı
DDO Siber Güvenlik Birim Müdürü



ARZU TEKİN

Vaka Müdahale Uzmanı



AYLİN AYARÖZ
GÖKSU

Kimlik Erişim ve
Yönetimi Uzmanı



BETÜL
KOCAMAN

Siber Güvenlik Analisti



**DAMLA
BAŘıVANCı**
Kimlik Eriřim ve
Yönetimi Uzmanı



DUYGU AKÇA
Siber Güvenlik
Zafiyet Analisti



ELİF YILDIZ
Kimlik Eriřim ve
Yönetimi Uzmanı



**ESMA GÜNEYRİ
ÖZMEN**
Siber Güvenlik
Güvence Uzmanı



FERİDE ÜNLÜ
Siber Güvenlik
Planlama Uzmanı



SAFİYE GÜNEř
Siber Güvenlik Analisti



SEVİM POYRAZ
Siber Güvenlik Vaka
Müdahale Uzmanı



ÜLKÜ KAHVE
Bilgi Güvenlięi Uzmanı



ZEYNEP YILDIRIM
Ofansif Güvenlik Uzmanı





SİBER GÜVENLİK

Siber Nedir ?

Siber kelimesi İngilizce “cyber” kelimesinden uyarlanıp kullanılmaya başlayan “internet’e ait olan”, “sanal gerçeklik” anlamına gelen bir kelimedir. Siber, bilişim alt yapısında çalışan geniş bir alt yapıdır. En büyük tehditlerin tam olarak bu büyük alanda olduğunu söylemek de hiç yanlış olmaz.

Siber Güvenlik Nedir?

Günümüzde teknoloji ve ağ sistemleri oldukça gelişmiş durumdadır. Siber güvenlik, bireyi ve toplumu bu sanal ortamın zararlı etkilerinden korumayı amaçlayan bir güvenlik sistemidir. Bireyler, şirketler, devletler ve kamu kuruluşları gerçek hayatta yaşanabilecek olumsuzluklardan korunmaya çalıştığı gibi sanal hayatta da korunma gereksinimi duyar. Bu korunma durumu da siber güvenlik ile mümkündür.

Siber Güvenlik Neden Önemlidir ?

Siber güvenliğin birinci amacı, bireylerin ve kurumların internet mecralarında olan verilerini güvende tutmasını sağlamaktır. Örneğin kötü amaçlı bir kişi sizin bağlı olduğunuz ağ üzerinden bilgisayarınıza sızdı ve verilerinizi ele geçirdi. Bunu asla istemezsiniz değil mi? Bu ve benzeri kötü olayları yaşamamak adına siber güvenliği sağlamak çok önemlidir.

Zafiyet ve Tehdit Kavramları

Zafiyet / açıklık (Vulnerability); Herhangi bir saldırganın sisteme/yazılıma/varlığa/ bilgiye zarar vermek için yararlanabileceği ve ilgili sistemde bulunan açıklıklar/eksiklikler/zayıflıklardır. Zafiyet; sistemin yapısal tasarım hatalarından, sisteme yüklenen programlardan ya da sistemlerdeki yanlış yapılandırma ayarlarından kaynaklanabilir. Sonuç olarak da bu varlığa yetkisiz erişim gibi sonuçlar doğurabilir (Başanoğlu, 2015.)

Tehdit (Threat): İsteyerek (bilinçli olarak) ya da istemeden (yanlışlıkla), mevcut bir zafiyetin istismarı (elde edilmesi, değiştirilmesi, imha edilmesi, zarar verilmesi gibi) ile ilişkili olarak bir kurum veya kuruluşa zarar verme ihtimali olan tüm potansiyel tehlikelerdir. Tehdit, yeri geldiğinde iç ağıdan gelebilecek saldırılar olabileceği gibi, yeri geldiğinde internetten, usb bellek veya CD DVD gibi ortamlardan da gelebilir. Bilgi (varlıklar), tehditlere karşı korunmalıdır.

Risk Kavramı

Bir varlık için tehdit ile zafiyetin örtüştüğü noktada risk ortaya çıkar. Herhangi bir saldırganın bir zafiyetten yararlanıp tehdit oluşturmaya yani sisteme zarar verme ihtimalidir.

Etki ve Olasılık Kavramları

Etki, tespit edilmiş olan zafiyetler sonucunda bilgi sistemleri süreçleri ve iş süreçleri üzerinde oluşabilecek negatif etkilerin tespiti.

Olasılık ise tanımlanmış olan riskin gerçekleşme ihtimalinin değerlendirilmesi ve derecelendirilmesidir.

Risk Değerlendirmesi (Etki x Olasılık)

Amaç ve hedeflere ulaşılmasını etkileyecek beklenen veya beklenmeyen herhangi bir faktörün analiz edilerek etki ve olasılık açısından değerlendirilmesidir. Haya-tın her anında risk değerlendirmesi yaparız. Karşıdan karşıya geçerken bile...

Risk ve Fırsat Yönetimi

Olumlu ve olumsuz durum oluşturabilecek belirsizlik içeren etken demektir. Teh-dit varsa risk var demektir. Peki, bu risk benim iştahımın altında mı, üstünde mi? Bu riski kabul ediyor muyum? Bu sorulara cevap verip risk ve fırsat yönetimini iyi yapmalıyız.

Risk İştahı Nedir?

Risk, benim/şirketin sahip olduğu misyon ve vizyon doğrultusunda kabul edilebilir mi? Yani yönetimin herhangi bir önlem almanın gerekliliğine hüküm vermeden önce maruz kalmaya hazır olduğu risk miktarıdır. Yönetimin kabul edilebilir ol-duğunu düşündüğü risk seviyesidir. Yani yönetimin herhangi bir önlem almanın gerekliliğine hüküm vermeden önce maruz kalmaya hazır olduğu risk miktarıdır. Yönetimin kabul edilebilir olduğunu düşündüğü risk seviyesidir.

Doğal Risk Nedir?

Doğal risk, riski yönetmek adına herhangi bir adım atılmadan önceki risk seviyesi-dir. Yönetim tarafından herhangi bir önlem alınmaması durumunda gerçekleşme olasılığının ve etkisinin değiştirilemeyeceği riskleri ifade eder.

Artık (Kalıntı) Risk Nedir?

Yönetimin, olumsuz bir olayın etki ve ihtimalini azaltmak amacıyla, riski karşıla-maya yönelik kontrol faaliyetleri de dâhil, aldığı tedbirlerden sonra kalan risktir. Bütünleştirilmiş İç Kontrol Çerçeve Programı (COSO) 2013'te bunu hedefler kap-samında, "Yönetim müdahâleleri geliştirilip uygulandıktan sonra hedeflerin yerine getirilmesine yönelik olarak arda kalan risk." olarak tanımlamıştır.

Risklere Karşı Şirketler Neler Yapabilir?

- Riskten Kaçınma
- Risk Azaltma
- Risk Transferi
- Risk Kabulü

Şirketler yaptığı faaliyetlerde karşılaştığı veya karşılaşılabilecek risklerle aşağıdaki dört başlıkta belirtildiği gibi davranabilir:

Riskten Kaçınma

Şirketler, faaliyet göstermek istediği alanlarda var olan risklerden kaçınmak için ilgili faaliyete veya projeye girmeyebilir, yatırım yapmayabilirler. Böylece var olabilecek risklerden kaçınmış olurlar. Riskten kaçınmak için örneğin yeni bir ürün tanıtımı yapmayabilir, var olan ürünün üretimini sonlandırabilir veya yeni bir ülkede bir yatırım yapmayabilir.

Risk Azaltma

Risk yönetiminde en yaygın olarak izlenen yöntemdir. Bu yöntemde, her risk için belirlenmiş kontrol faaliyetlerinin uygulanması suretiyle risklerin kabul edilebilir seviyelerde tutulması amaçlanır ve risklerle mücadele olarak da değerlendirilebilir.

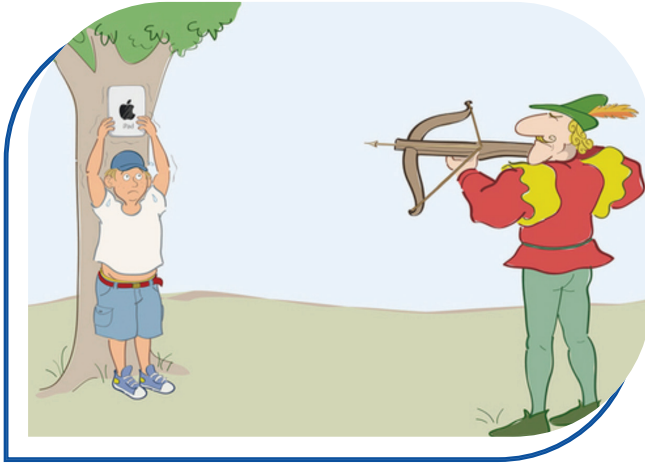
Risk Transferi

Bazı risklerin, tamamen veya kısmen üçüncü tarafa, başka kurumlara transfer edilmesidir. Kurum tesislerinin sigorta ettirilmesi veya güvenlik sisteminin özel şirketler aracılığıyla sağlanması gibi.

Risk Kabulü

Şirket tarafından riskle ilgili gerekli tüm yöntemler kullanıldıktan sonra belirli bir miktar risk kabul edilmek zorunda kalınabilir. Riskin belirlenemeyeceği, azaltılamayacağı veya transfer edilemeyeceği durumlarda risk kabul edilebilir. Risk meydana gelince ise kayıp ve zararlar kabul edileceği anlamına da gelir.

Tehdit zafiyet ve risk ilişkisine bir örnek:



Şekil 1 : Wilmarx'a ait bir resim

Resimde; sağdaki okçu adam, ağacın altındaki adamın elindeki hedefe nişan alıyor.

Okçunun, oku hedefe değil de hedefi tutan adamın herhangi bir yerine (bilinçli ya da bilmeyerek) atması bir tehdittir.

Soldaki adamın tehlikeye karşı vücudunu korumak için önlem almaması, örneğin darbeye karşı koruyan bir giysi giymemesi bir zafiyettir.

Kâğıdı tutan adamın vurulma ihtimali ise riski tanımlamaktır. Burada risk oranını okçunun yeteneği, oku attığı mesafe, oyunun oynandığı hava koşulları, hedef servisini sunan adamın almadığı önlemler gibi faktörler belirler.

Siber Suçlar

Siber güvenliğin karşı karşıya olduğu tehditlerin üç katmanı vardır:

1. Siber suç, finansal kazanç veya işlerin kesintiye uğraması için sistemleri hedefleyen tek aktörleri veya grupları içerir.
2. Siber saldırı, genellikle politik nedenli bilgi toplamayı içerir.
3. Siber terör, elektronik sistemleri panik veya korkuya neden olacak şekilde baltalamak için tasarlanır.

Peki, kötü amaçlı aktörler bilgisayar sistemlerinin kontrolünü nasıl kazanır?

Siber güvenliği tehdit etmek için kullanılan bazı yaygın yöntemler şunlardır:

- Kötü amaçlı yazılımlar (Virüs, Truva atları, casus yazılım, fidye yazılımı, reklam yazılımı, botnetler, SQL aşılama)
- Kimlik avı
- İşlemlere müdahâle etmeye yönelik saldırı
- Hizmeti engelleme saldırısı

Siber Saldırlara Karşı Kendinizi Koruyun

- Yazılımınızı ve işletim sisteminizi güncelleyin.
- Antivirüs yazılımı kullanın.
- Güçlü parolalar kullanın.
- Bilinmeyen göndericilerden gelen e-posta eklerini açmayın.
- Bilinmeyen göndericilerden gelen e-postalardaki veya tanınmayan web sitelerindeki bağlantılara tıklamayın.
- Halka açık yerlerde güvenli olmayan Wi-Fi ağlarını kullanmaktan kaçının.





BİLGİ GÜVENLİĞİ

Bilgi Nedir?

Birbiriyle henüz bağlantısı kurulmamış bilinenlere veri denir. Bilgi ise işlenmiş veriye denir. Bir konuya göre belirsizliği azaltan kaynaktır (Shannon).

Ölçme ile veriye ulaşılır, ispat ile veriden bilgiye ulaşılır. Veriler bir yaşam döngüsü içerisinde. Oluşturulur, işlenir, analiz edilir, saklanır ve en sonunda silinir.

Bilgi Varlığı (Information Asset)

Varlık, değerli olan ve korunması gereken unsurdur. Bilgi varlığı, kurum ve kuruluşlar için çok değerli olan tüm bilgilerdir. Bu bilgiler çok değerli olduklarından kişileri / firmayı istenmeyen bir durum karşısında olumsuz etkileyebilir.

Bilgi Varlığı Yönetimi

ISO 27001 bilgi güvenliği yönetim sistemi kapsamında varlıkların yönetimi çok önemlidir. Bilgi varlıkları; üretilen bilginin işlenmesi, saklanması, iletilmesi, korunması, sürekliliğinin sağlanması ve yok edilmesi için kullanılır.

Güvenlik

Tehdit; hayata, bilgiye her türlü faaliyete, çevreye ve/veya mülkiyete zarar verme potansiyeline sahip ve tehlike oluşturacağını işaret eden doğal veya insan yapımı olay, birey, tüzel varlık veya eylemdir.

Güvenlik ise gelebilecek tehditlere karşı önlem almaktır.

Bilgi Güvenliği

Bilgi kişi ve kurumlar için en önemli kaynaktır. Bu yüzden bu kaynağı koruma ihtiyacı duyulur. Bilginin taşıdığı değeri ölçmek de bilginin kendisi kadar önemlidir. Bilgiyi değerlendirirken bilginin kalitesini gösteren özelliklere bakılmalıdır. Bu özelliklere doğruluğu, güncelliği, konuyla olan ilgisi, bütünlüğü, gereksinimleri karşılayıp karşılamadığı vb. örnek olarak verebiliriz.

Bilgi güvenliğinin üç unsuru:

Bilgi güvenliği sadece bilginin başkasının eline geçmesinden yani gizliliğinden ibaret değildir. Bilginin karakteri şu üç unsurdan oluşur;

-Gizlilik (Confidentiality) - Bütünlük (Integrity) - Kullanılabilirlik (Availability)

-Gizlilik

Bilginin yetkisiz kişilerin eline geçmemesidir.

Örneğin evinizde çok yüklü miktarda paranız var. Böyle bir paranızın olduğunu bilmemesi gereken kişilerin bilmesi, paranın gizlilik güvenliğini tehlikeye sokar. Bu yüzden bilginin gizlilik güvenliğini sağlamaya özen göstermeliyiz.

-Bütünlük

Bilginin yetkisiz kişiler tarafından silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır.

Diyelim ki evinizdeki yüklü miktarda parayı bankaya koymak istediniz, bankacı işlemleri yaparken son rakamını değiştirdi. Bu durum bütünlüğünü bozmuş olur. Yani bütünlük güvenlik sorunları, bilginin orijinal hâlden farklılaşması ile olur diyebiliriz.

Kimlik doğrulama ve erişim kontrolü ile yetkisiz erişim tespit edilir ve engellenir. Bu süreçte kimlik tanımlama, kimlik doğrulama ve yetkilendirme yöntemleri (kullanıcı adı, şifre, parmak izi vb.) uygulanır.

-Kullanılabilirlik

Bilginin her ihtiyaç duyulduğunda ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Para örneğinden devam edelim. Paramızı bankamıza koyduk. Bir gün geldi araba almak istedik ve parayı çekmemiz gerekti. Parayı çekmek için gittiğimizde bankacı bize paranın tamamını veremeyeceğini söylerse bu bir kullanılabilirlik güvenlik sorunudur. Hepimiz herhangi bir durumda paraya hemen erişip kullanabilmek isteriz, değil mi?

Bu yüzden bu güvenliği sağlamak çok önemlidir.

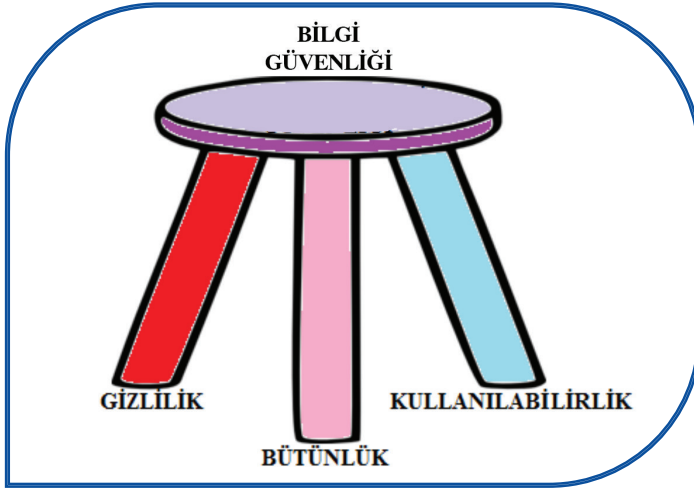
Veri depolama alanları bizler için önemlidir ve bu sistemlere hizmet veren cihazların altyapı yedekliliği ve yeterliliği olmalıdır.

Bu sayede büyük ölçüde kullanılabilir güvenliğini sağlamış oluruz.

Üç Bacaklı Tabure

Biz bu üç unsur ile bilgi varlıklarını koruruz. Bu üç unsur denge hâlinde olmalıdır.

Bu durumu, bilgi güvenliği unsurları için çok kullanılan “üç bacaklı tabure” örneği ile gözünüzde canlandırabilirsiniz.



Şekil 1: Üç Bacaklı Tabure

Bu taburedeki üç bacak aynı uzunlukta ve sağlamlıkta olduğu sürece dengede durmaya uygundur. Herhangi bir unsorda zayıflık olduğu anda taburenin o yöne doğru dengesini bozmuş oluruz.

Örneğin gizlilik unsurunu fazlasıyla desteklediniz ve uygulamaya girerken bir sürü güvenlik önlemi aldınız. Bu durumda uygulamaya erişiminiz zorlaşmış oldu yani dengeyi sağlayamamış oldunuz.

Aynı zamanda bilgi güvenliği için "en zayıf halka" kıyaslaması da kullanılır. Bilgilerimiz, bu üç unsurdan en güçsüzü kadar güvende demektir.

Bilgi Güvenliđini Tehdit Eden Unsurlar

- Yazılım ve / veya Donanım Hataları
- Projelendirme Hataları
- Veri Kayıpları
- Sistem Kaybı
- İnsan Hataları
- Hatalı Tasarlanmış Sistem Mimarileri
- Güvenlik Zafiyetleri
- Hatalı Modelleme

Bilgi Güvenliđi Standartları

ISO/IEC 27001 bilgi güvenliđi alanında dünya genelinde yaygın olarak kullanılan uluslararası standartlardan biridir. Söz konusu standart; kuruluşların, bilgi güvenliđinin en temel gereksinimleri olan 'gizlilik', 'bütünlük; 'kullanılabilirlik' ilkelerini sağlamasını amaçlamaktadır.

KAYNAKÇA

<tr.wikipedia.org/Wiki/Tehdit>
(BTK)





BİLGİ GÜVENLİĞİ FARKINDALIĞI

Bilgi güvenliği nedir?

Evden çıkarken kapımızı kilitlemek aslında sahip olduğumuz ve değer verdiğimiz her şeyi koruma altına alma içgüdüsünü gösterir. Peki internette bilgilerimizi de koruma içgüdüsüne sahip miyiz?

Hızla büyüyen ve gelişen teknoloji içinde bilgilerimiz dijital ortamda daha sık kullanılıyor. Bu bilgiler kişisel verilerimiz, ticari ve finansal bilgiler olabilir. Bu bizim için hem avantaj hem dezavantaj sağlar. Online alışverişlerde kart numarası ezberlemeye gerek kalmadan kaydettiğimiz kart bilgilerini kullanarak saniyeler içinde alışverişimizi tamamlayabiliyoruz.

Peki kartınızdan çekilen para ile siz alışveriş yapmadıysanız? Tam da burada bilgilerimizin yarattığı dezavantaj ile karşılaşabiliriz.

İnternet üzerinde kullandığımız verilerin güvenliğini sağlamak bizim elimizdedir. Bu güvenliği sağlamak için hepimizin *Bilgi Güvenliği Ve Farkındalığı* hakkında bilgi sahibi olması gerekir.

Bilgi güvenliği ve farkındalığı nedir?

Aslında kullandığımız internet sitelerinin güvenlik sistemleri vardır fakat bazen bilgilerimize ulaşmak isteyen yetkisiz kişiler bu güvenlik sistemlerini aşabilir ve bilgi sahibine saldırı düzenleyebilir. Bunun bir saldırı olduğunu bilgi güvenliği ve farkındalığı ile edindiğimiz bilgiler ile anlayabiliriz.

Örnek bir senaryo üzerinden ilerlersek...

Güvenlik donanımı iyi bir şirkette çalışıyorsunuz. Fakat yetkisiz kişiler bu güvenlik duvarlarını aşarak size bir e-posta gönderiyor. Bu e-mail içerisinde bir link var ve bu linke tıkladığınızda, yetkisiz kişiler gerek kişisel verilerinizi gerek şirketinizin verilerini ele geçirmiş olabilir. Fakat son kullanıcının farkındalığı sayesinde gelen e-mailin bir saldırı olduğu anlaşılacak gönderilen link açılmaz.

Her zaman internet üzerinden bir saldırı olması beklenmez. Bazen bir telefon araması ile arkadan gelen telsiz sesleri, sizi polis olduğuna inandırıp maddi birikimlerinize el koyabilir. Bu durumda emniyete giderek işlemleri kontrol etmeniz, bilgilerinizin güvenliği açısından farkındalığınızı gösterir. Bu sayede maddi ve manevi kayıp vermemiş olursunuz.

Bunun gibi olan ve olacak saldırılara karşı bilinçli son kullanıcılar olarak bilgilerimizi güvende tutmanın önemini anlayarak farkındalığımızı artırmalıyız.

Kullanıcının farkındalığı neyi değiştirir?

Bahsettiğimiz yaygın senaryoların nasıl sonuçlanacağı son kullanıcının elindedir. Eğer son kullanıcı bilgilerin hangi koşulda ve nasıl paylaşılacağını biliyorsa bütün güvenlik önlemleri aşılsa bile son kullanıcıyı aşmak mümkün değildir. (Güvenlik sistemlerini aşan yetkisiz kullanıcıların, son kullanıcının farkındalığını aşması mümkün değildir.)

Akıllı telefon giriş şifreleri, kurum içindeki masamızın temiz tutulması, mobil bankacılık şifrelerimiz, bilgisayarımızın veya telefonumuzun başından ayrıldığıımızda ekranımızın kendini kilitlemesi gibi önlemlerin yanı sıra güçlü parolalar seçmek, maillerimize gelen linkleri daha detaylı inceleyerek açmak; farkındalığımızın artmasını ve olası saldırılara karşı daha bilinçli son kullanıcılar olmamızı sağlar.

Farkındalığın artması için ne yapılabilir?

Konu hakkında güncel bilgileri okumak, bilgi güvenliği ve farkındalık eğitimlerine katılmak, kullanıcının farkındalığının artmasını destekleyecektir.

Kurumlarınızda düzenli işleyen bir siber güvenlik farkındalığı

Şirketinize yönelik olası saldırılara karşı daha bilinçli son kullanıcılar sayesinde herhangi bir veri ifşası olmadan şirketinizin itibarı korunur. Böylece bilgi sızıntısı önlenerek, zamandan ve paradan tasarruf edilmiş olunur.

Her bilgi aynı güvenlikte mi olmalıdır?

Her edindiğimiz bilgi güvenli ortamlar içinde bulunmalıdır ve bazı özel durumlarda edinilen bilgilerin güvenliği artırılmalıdır. Örneğin, önemli bir dosya transferi sağlanacaksa şifreli yöntemlere geçilmelidir.





İNTERNETİN EVİRİMİ

İnternet; telefonlarda, bilgisayarlarda, tabletlerde hatta televizyonlarda bile kullanılan ağıdır. Peki tam olarak nedir?

İnternet bütün dünyada kullanılan veri ve bilgiyi iletmeyi ve almayı sağlayan iletişim ağıdır. İnternet aracılığıyla istenilen web sitesine ve bilgiye erişim sağlanabilir.

1985 yılında kullanılmaya başlanan İngilizce internet kelimesi, “kendi aralarında bağlantılı ağlar” anlamına gelen Interconnected Networks teriminin kısaltmasıdır. Ön ek olan inter-, İngilizcede arasında ve karşılıklı anlamlarına, net kelimesi ise ağ anlamına gelir.

Zaman zaman internet kelimesi yerine kullanılan “WWW” ve internet ile eş anlamlı değildir.

İnternet kim tarafından ve nasıl icat edilmiştir?

Ağ teknolojisi ilk geliştirildiğinde, birçok bilim insanı ve mühendis ARPANET’i oluşturmak için araştırmalarını bir araya getirmiştir.

Bu isimlerden bazıları, uzun yıllar ARPANET’i öneren ve yöneten Lawrence Roberts ile World Wide Web’i icat eden Tim Berners-Lee’dir.

Bilgisayar bilimcileri, internetin ana yapı taşlarından biri hâline gelecek olan elektronik verileri etkin bir şekilde iletmek için bir yöntem olan “paket anahtarlama” kavramını geliştirdiler. Paket anahtarlama paket farklı yolları kullanarak hedef noktaya ulaşır. Paketler, düğümler üzerinde ayrı ayrı iletir ve iletildiği anda en uygun yoldan hedef düğüme gönderilir.

1975’te ARPANET, 60’tan fazla düğümü kapsayan bir ağ hâline geldi ve daha sonra diğer mucitlerin kreasyonları ile bugünkü bildiğimiz şekliyle web’in yolunu açtı.

ARPANET ve World Wide Web birbirinden farklıdır.

ARPANET, bilgisayarların birbirine bağlanmasına izin veren fiziksel bir sistemken World Wide Web bu bağlantılarda gezinmek için kullanılan bir dizi dil ve protokoldür. ARPANET’e donanım, World Wide Web’e ise bir yazılım diyebiliriz.

Sonuç olarak ARPANET (Gelişmiş Araştırma Projeleri Dairesi Ağı) dünyanın her yerindeki bilgisayarlarını birbirine bağladı.

İnternet Gelişim Dönemleri Nelerdir?

Dünya nüfusunun yaklaşık %60'ı bugün internet sayesinde iletişim kuruyor. İnternet üzerinden veri paylaşımı sağlayan ve her gün milyarlarca insanın etkileşim kurmasını mümkün kılan World Wide Web (www) ilk çıktığı zamanlardan bugüne kadar çok değişti ve değişmeye devam ediyor.

İnternetin ortaya çıktığı zamandan bugüne kadar geçirdiği aşamaları 4'e ayırabiliriz. Bunlar web 1.0, web 2.0, web 3.0 ve web 4.0'dır.

Web Teknolojisi	Geçerlilik Yılı	Odak Noktası
Web 1.0 (monolog)	1995 – 2000	Döküman Odaklı
Web 2.0 (interaktif web)	2000 – 2010	İnsan Odaklı
Web 3.0 (semantik web)	2010 – 2020	Bilgi Odaklı
Web 4.0 (intelligent web)	2020 – 2030	Sanal gerçeklik odaklı

1980'lerin sonunda Web 1.0 olarak bildiğimiz internet ağıyla tanıştık. Web 1.0 oldukça az katılımcıya sahipti. 20 yıldan uzun bir süredir ise hayatımızda, etkileşimli internet olarak bildiğimiz web 2.0 var. web 2.0 ise web 3.0 teknolojisine doğru bir gelişim gösterdi. Kaydedilen teknolojik gelişmelere bağlı olarak günümüze kadar web 1.0, web 2.0, web 3.0 ve web 4.0 olmak üzere farklı internet dönemleri ortaya çıktı.

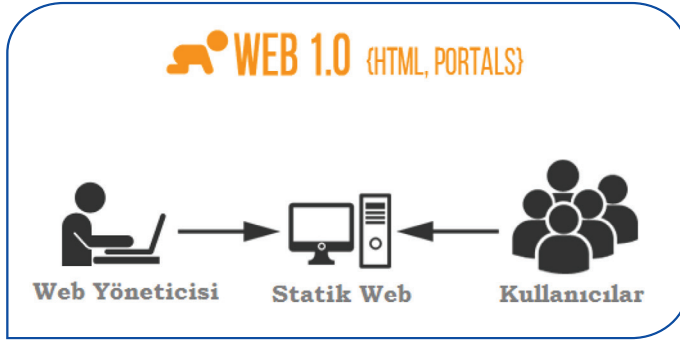
Gelin web'in bu kısa evrimine bir göz atalım;

Web 1.0 Nedir?

Web 1.0'a internetin en ilkel dönemi diyebiliriz.

Kullanıcılar bu dönemde interneti tek yönlü olarak sadece bilgi almak amaçlı kullanıyorlardı ve sadece okuyucu konumunda olabiliyorlardı. Kullanıcı, sunucuya bağlanıp web sayfasındaki bilgiyi alıp daha sonrasında sayfadan çıkabiliyordu.

Gün geçtikçe insanların internetteki bilgiye olan ihtiyacı arttı ve web 1.0'ın kullanıcılara sağladığı kısıtlı imkânlar insanların ihtiyacını yeterli seviyede karşılayamamaya başladı. Bu ihtiyaçları karşılamak adına web 2.0 teknolojisi geliştirilmeye başlandı.



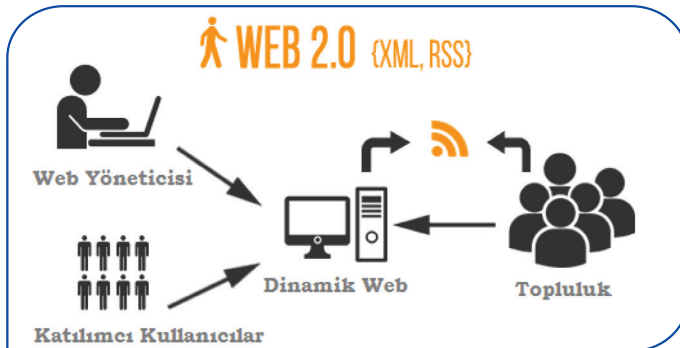
Web 2.0 Nedir?

Web 2.0'a internetin sosyal hâli diyebiliriz.

Kullanıcıların yalnızca bilgi almadığı; bilgi verdiği, bilgi ürettiği, paylaşımda bulunduğu, tartıştığı vb. özellikleri aktif kullandığı yapıya Web 2.0 denir. Kullanıcıların yalnızca bilgi almadığı; bilgi verdiği, bilgi ürettiği, paylaşımda bulunduğu, tartıştığı vb. özellikleri aktif kullandığı yapıya Web 2.0 denir. Yani günümüzde internet, sadece bilgi alınmak için kullanılmaz; bilgi paylaşımı ya da üretimi yapmak için de pek çok açıdan aktif katılım olanağı sağlar. Bu da insanların daha fazla üretmesine ve birbirine yardımcı olmasına olanak tanır. Tabii daha fazla bilgi alma olanağı da yine bu yapı doğrultusunda önemli bir potansiyel teşkil eder.

Kısacası Web 1.0 ile başlayan "İletim" dönemi sona erdi ve "İletişim" dönemi başladı. Blog sayfaları, web kütüphaneleri, e-posta, telefon uygulamaları gibi teknolojiler bu dönemde oluştu. Facebook, Twitter, Instagram gibi uygulamalar da bu dönemin uygulamaları arasındadır.

Web 2.0'da kullanıcılar bir gelir elde etmeden bu işi yaparken web 2.0'ın sunduğu uygulamalar vb. teknolojiler bundan kazanç sağlıyordu. Zamanla birçok yenilik ile Web 3.0 teknolojisi geliştirilmeye başlandı.



Web 3.0 Nedir?

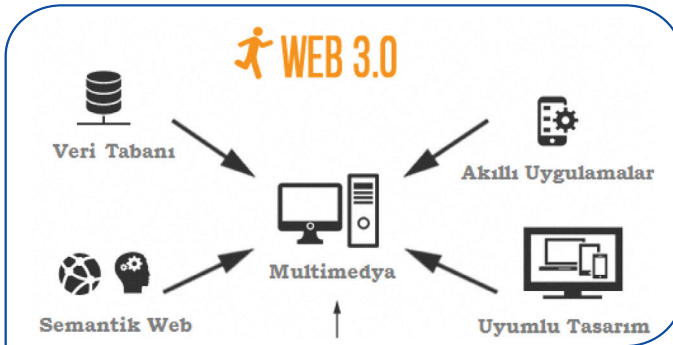
Günümüzdeki güncel hâliyle kabaca bir tanım yapmak istersek Web 3.0; temelinde veri odaklı olan internetin merkeziyetsiz, P2P, blok zincir destekli ve kişiselleşmiş olarak kullanılabilecek olmasıdır. Web siteleri ve uygulamalar için üçüncü nesil internet hizmetleri olacaktır. Nihai hedef; daha akıllı, nesnelerle ve etrafımızdaki her şey ile bağlantılı olan, tamamen açık web siteleri oluşturmaktır. Girdiğiniz veriyi doğru şekilde yorumlamakla birlikte metin, ses veya diğer medyalar aracılığıyla aktardığınız her şeyi çözümleyebilen yeni bir internet türüdür diyebiliriz.

Web 3.0, sunucuyu ortadan kaldırarak verilerin doğrudan bilgisayarlar tarafından okunup yapay zekâ ile yorumlanmasını sağlıyor. Kullanıcı veriyi kullanırken bilgisayar da bu veriyi analiz ederek yorumluyor. Yani daha önce bakmış olduğunuz bir ürünün reklamlarının sürekli karşınıza çıkması gibi düşünebilirsiniz.

Kısacası yapay zekâ ile sadece doküman içeriğini bulmakla yetinilmiyor, o içeriğin anlamları da yorumlanıyor.

NFT, blockchain, kripto paralar, metaverse, 3D görselleştirme ile etkileşimli görünüm, yapay zekâ, Apple'ın sunduğu sanal asistan Siri, Amazon'un sunduğu sanal asistan Alexa ve bağlantılı akıllı evler Web 3.0'ın kullanım alanları arasında yer alıyor.

Web 3.0'ı Öncekilerden Üstün Kılan Nedir?



Semantik web: Online ağlar üzerinde yer alan içeriklerin yalnızca insanlar tarafından değil; makineler tarafından da anlaşılabilir, yorumlanabilir ve kullanılabilir olmasını hedefleyen web projesini ifade eder.

Daha verimli tarama: Önceki teknolojilere göre bir arama motorunda en iyi sonucu bulmak mümkün hâle geldi.

Artan bilgi bağlantısı: Daha büyük veri kümeleri ile kullanıcılar ihtiyaçlarını daha doğru bilgilerle elde edebilir hâle geldi.

Merkezi kontrol noktasının yokluğu (merkeziyetsizlik): Araçlar denklemden çıkarıldı ve verilerin şifrelenemediği güvenilir bir platform hâline geldi.

Daha iyi müşteri desteği: Aynı anda birden fazla müşteri ile konuşulmasını sağlayan akıllı sohbet robotları kullanılarak kesintisiz hizmet sağlanır hâle geldi.

Peki ya Web 4.0 Nedir?

Web 4.0, kişisel dosyaların, verilerin ve içeriklerin depolanmasında internet tabanlı bilişim (bulut bilişim) uygulamalarının öne çıktığı, işletim sisteminden tüm uygulamalara kadar her şeyin fiziksel disklerden uzaklaşarak tamamıyla sanal networkler üzerinde kurulduğu, gerçek ve sanalın iç içe geçtiği bir web teknolojisidir. Web 4.0 teknolojisinde yapay zekâ ve artırılmış gerçeklik teknolojisi ön plana çıkmaktadır. Kişisel asistanlar olan bilgisayarlardan sanal gerçekliklere, hologramlara, tüm ev aletlerinin internete bağlanmasına (nesnelerin interneti) kadar makineler ve insanlar arasında son derece akıllı etkileşimler olacağı ve makinelerin internette yer alan içeriği yorumlayıp anlamlandırabilecek zekâ düzeyine ulaşarak en yüksek performansla en kaliteli sonuçlara ulaştıracağı bir internet formunu ifade etmektedir. Bu nedenle bu dönem “simbiyotik web” ya da “akıllı web” dönemi olarak da adlandırılmaktadır. İnsan gibi düşünebilen yapay zekâ algoritmaları sayesinde web ve kullanıcılar arasındaki ilişki daha kişiselleştirilmiş olarak karşımıza çıkar. Kullanıcılar Web 4.0 ile bilgisayarlara yüklenen programlara ihtiyaç duymadan web’de kurulu olan işletim sistemindeki programları, dünyanın herhangi bir yerinden bulut üzerinden bağlanarak hemen kullanabilir. Web 4.0 teknolojilerini verimli bir şekilde kullanmak için yüksek hızda internet bağlantısının olması gerekmektedir. Saniyede 100 gigabit bağlantı hızı ve bant aralığının olduğu web mimarisinin olması gerektiği öngörülmektedir.

Örneğin bir ev almak istediğinizde emlak ofisine veya şantiyeye gitmeye ihtiyacınız olmayacak. Sanal gerçeklik sayesinde bulunduğunuz yer emlak ofisi olacak ve nihayetinde satın almak istediğiniz daireye ait tüm detayları evin içinde geziyormuş gibi görebileceksiniz.

Google Docs & Spreadsheets, YouOS, DesktopTwo, EyeOS gibi uygulamalar bu dönemin uygulamaları arasındadır.



Notlar

Akronim: İki veya daha fazla sözcüğün baş harflerinden veya ilk birkaç harfinden oluşturulmuş kelime.

KAYNAKÇA

World Wide Web (Dünya Çapında Ağ) sözcüklerinin akronimidir

<https://tr.wikipedia.org/wiki/%C4%B0internet#:~:text=9%20D%C4%B1%C5%9F%20ba%C4%9Flant%C4%B1lar,-etimoloji,kelimesi%20ise%20a%C4%9F%20anlam%C4%B1na%20gelir.>

<https://www.zmescience.com/science/who-invented-the-internet-05264/>

<https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet>

<https://study.com/academy/lesson/what-is-the-history-of-the-internet-origins-timeline.html>

https://uzmancoin.com/web-3-0-nedir?gclid=Cj0KCQjwwfiaBhC7ARIsAGvcPe5nlhvcy3EQn2-ExlYi7Edlua4Z_kEFKAjSBmgo3q4u4JwwwVwK4XwaAgLFEALw_wcB

<https://mechtekho.com/web-gelisim-evreleri-ve-web-4-0-teknolojisi/>

<https://bilgibilimi.net/web-1-0-web-2-0-web-3-0-nedir/>

[https://www.elektrikde.com/web-3-0-nedir-ozellikleri-ve-faydalari-nelerdir/#:~:text=Web%203.0%C4%B1%20%C3%96ncekilerden%20%C3%9Cst%C3%BCn,\(DoS\)%20sald%C4%B1r%C4%B1lar%C4%B1n%C4%B1n%20etkinli%C4%9Fin%20azalt%C4%B1r.](https://www.elektrikde.com/web-3-0-nedir-ozellikleri-ve-faydalari-nelerdir/#:~:text=Web%203.0%C4%B1%20%C3%96ncekilerden%20%C3%9Cst%C3%BCn,(DoS)%20sald%C4%B1r%C4%B1lar%C4%B1n%C4%B1n%20etkinli%C4%9Fin%20azalt%C4%B1r.)

<https://cyberartspro.com/20220722-gunumuzun-web-teknolojisi-web-3-0/>

<https://www.timetoast.com/timelines/evolucion-de-la-web-1-0-a-la-web-4-0>

<https://nttdata-solutions.com/>

<https://netvent.com/>





SİBER GÜVENLİK STANDARTLARI

Siber güvenlik bir kural, bir cihaz ya da yönetim sistemi değil, bir gerekliliktir. Bireysel ve toplumsal durumlarda farklılıklar göstermesine rağmen ana fikri güvenliğin genel çerçevesini belirlemektir. Kontrol ihtiyaca göre yapılır, yani ne kadar hassas bilgi olduğu ve müşterinin istekleri göz önünde bulundurulur. Ayrıca ülke, banka, telekomünikasyon ve bireyler için farklı regülasyonlar bulunur ve ihtiyaca göre değişiklik gösterebilir.

Bilgi güvenliği, veri sızıntısı vakalarının önüne geçmek amacıyla kuruluşlar tarafından başvurulmuş bir yaklaşımdır. Temel olarak, hassas verilerin korunduğu Bilgi Teknolojileri (BT) sistemlerinin yetkisiz erişim, kullanım, iş akışında kesintiye sebep olabilecek değişiklikler ve imha gibi durumlarla karşılaşmaması için geliştirilen siber güvenlik politikalarını içerir. Bu politikalar aynı zamanda bilginin kullanılabilirliğini önemli ölçüde destekler.

Türkiye’de, “düzenleyici ve denetleyici kurumlar” tarafından bilgi güvenliği konusunda regülasyon düzenlemeleri yapılmaktadır. Bu düzenlemeler, bilgi teknolojileri, sağlık, enerji ve bankacılık gibi birçok sektörü kapsar, kanun ve yönetmelikler aracılığıyla gerçekleştirilir.

İyi pratikler, belirli bir alanda en etkili ve başarılı sonuçları elde etmek için benimsenen yöntemlerdir. Bunlar, bir sektör veya disiplin içinde kabul görmüş, denenmiş ve başarılı olduğu kanıtlanmış yaklaşımları içerir. İyi pratikler, bilgi birikimi ve deneyimlerin birleştirilerek ortaya çıkarılan en iyi yöntemleri temsil eder. Regülasyonlar ise devlet veya yetkilendirilmiş kuruluşlar tarafından belirlenen, belli bir sektör veya faaliyet alanını düzenlemek amacıyla oluşturulan yasal kurallar ve yönetmeliklerdir. Regülasyonlar kamu güvenliği, tüketici koruması, veri gizliliği gibi konuları düzenlemek ve belirli bir sektörde uyulması zorunlu standartları belirlemek için kullanılır.

Bilgi güvenliğinin uygulanmasında dünyaca kabul görmüş birçok iyi pratik standart ve çerçeve bulunmaktadır. Bu standartlar ve çerçeveler, kurumların bilgi güvenliği süreçlerini etkin bir şekilde yönetmelerine yardımcı olmak için bir araya getirilmiştir. İşte bu standartlardan bazıları:

ISO 27001: Bilgi Güvenliği Yönetim Sistemi, kuruluşların bilgi güvenliği risklerini yönetmelerini ve güvenli bir bilgi yönetim sistemi kurmalarını sağlar.

COBIT: Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri, kurumların bilgi ve teknoloji yönetiminde en iyi uygulamaları benimsemelerini sağlayarak bilgi varlıklarını kurumalarına ve riskleri etkin bir şekilde yönetmelerine yardımcı olur.

PCI-DSS: Ödeme Kartları Endüstrisi Veri Koruma Standartları, ödeme kartı işlemleriyle ilgilenen kuruluşlar için güvenli ödeme işlemlerinin gerçekleştirilmesi ve müşteri verilerinin korunması için gereken kontrolleri belirler.

NIST: 800-53 Güvenlik ve Mahremiyet Kontrolleri, bilgi sistemlerinin güvenlik ve mahremiyetini sağlamak için kullanılan kapsamlı bir kontrol kataloğunu içerir.

HIPAA: Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası, ABD'deki sağlık sektöründe kişisel sağlık bilgilerinin gizliliğini, güvenliğini ve bütünlüğünü korumayı amaçlayan yasal bir çerçevedir.

BTK-BDDK: Ülkemizde BTK ve BDDK tarafından düzenlenen 5651 sayılı kanun çerçevesindeki regülasyonlar, kuruluşlar tarafından isteğe bağlı olarak uygulanabilir.

CIS ve CSSM: Kuruluşlar tarafından isteğe bağlı olarak kullanılabilen güvenlik çerçeveleridir ve uygunluk analizi sağlarlar.

OWASP ve MITRE: Kuruluşlar tarafından seçimli olarak kullanılabilen teknik güvenlik kaynaklarıdır ve web uygulama güvenliği alanına odaklanırlar.

2016 yılında yürürlüğe giren ve net, keskin hatlara sahip olan “Kişisel Verilerin Korunması Kanunu (KVKK)” ile tüm sektörlerin “Veri Sınıflandırma ve Verinin Güvenli Paylaşımı” konusunda çalışma yapması zorunlu hâle getirilmiştir. 6698 sayılı kanun çerçevesinde, genel nitelikli veya hassas nitelikli olsun, tüm kişisel veriler ilgili yasa maddeleri tarafından koruma altına alınmıştır.

Regülasyonları sadece ISO 27001 ve KVKK ile sınırlamak yanlış olacaktır. EU-GDPR, PCI-DSS, HIPAA, PII gibi veri güvenliği odaklı tüm regülasyonlar, sınıflandırma faaliyetini sistemdeki temel bir unsur hâline getirmektedir. Unutulmamalıdır ki sınıflandırılmış verilerin kurumsal düzeyde yönetimi daha kolay ve güvenli olacaktır.

Yasal yönü düşünüldüğünde, regülasyonlar kapsamında (ISO 27001) verilerin sınıflandırılması, etiketlenmesi ve belirlenen standartlara göre kullanılması zorunlu hâle getirilmiştir. Bu gereklilik; bilişim, havacılık, haberleşme, uydu hizmetleri, altyapı hizmetleri, gümrük hizmetleri ve birçok diğer sektörde faaliyet gösteren kuruluşları da kapsamaktadır.

Bu standartlar ve çerçeveler, kişi ve kuruluşlara bilgi güvenliği alanında rehberlik sağlar ve en iyi uygulamaları takip etmelerine yardımcı olur.





SAĞLIK SEKTÖRÜNDE SİBER GÜVENLİK

Sağlık sektörü, siber güvenlik çözümlerinin kritik öneme sahip olduğu alanlar arasında yer almaktadır. Bünyesinde bulundurduğu hassas verilerin veri güvenliği hakkında sorun yaşanması hâli, kamuoyuna ait çok temel bilgilerin sızdırılması ile sonuçlanabilmektedir. Sağlık alanı içerisinde faaliyet gösteren kurum ve kuruluşların itibarlarını ve hastalarını koruyabilmek için siber saldırı tehditlerine karşı kapsamlı siber güvenlik önlemleri almaları gerekmektedir.

1-Sağlıkta Veri Güvenliği

Sağlık hizmetlerinde bilgi teknolojilerinin kullanılması hizmet kalitesini artırmaktadır. Teknoloji kullanılırken bilginin gizliliği yani veri korunması da önem kazanmaktadır. Sistemsel ve fiziksel önlemlerin yanı sıra sağlık kurumunda çalışanların bilgi güvenlik politikalarını bilmeleri gerekmektedir. Olabilecek riskleri en düşük seviyeye indirgeyebilmek için çalışanların donanım ve yazılım standartlarını bilmeleri önemsenmelidir.

Sağlıkta veri güvenliği için korunması gereken veriler:

- İsimler
- Doğum ve ölüm tarihleri, kabul ve taburcu tarihleri, tedavi tarihleri
- Telefon ve faks numaraları, diğer iletişim bilgileri
- Adresler
- Tıbbi kayıt numaraları
- Sosyal güvenlik numaraları
- Fotoğraflar ve karşılaştırılabilir görüntüler
- Parmak, retina ve ses kayıtları dâhil biyometrik tanımlayıcılar
- Kişiyi tanımlayacak diğer numaralar şeklinde listelenebilmektedir.

Sağlık kuruluşlarının yükümlülükleri arasında elektronik ortamda tutulan ve internet üzerinden gönderilen tüm kişisel verilerin saklanması yönelik gerekli önlemleri almak bulunmaktadır. Bir ihlal durumunda veri sorumlusuna yönelik cezai yaptırım uygulanmaktadır. Bu durum sağlık sektöründe siber güvenliği bir zorunluluk hâline getirmektedir.

2-Sağlık Sektöründe Siber Riskler ve Yaygın Tehditler

Sağlık sektöründe siber tehditler, insan hayatında ölümcül ya da telafi edilemez sonuçlara, küçük çaplı kliniklerde saldırı sonrası kapanmalara sebep olabilmektedir. Siber saldırılar sadece hastalar ve kurumlar için değil, aynı zamanda doktor, hemşire ve tüm sağlık çalışanları için de tehdit oluşturmaktadır.

Sağlık sektöründeki olası siber tehditler aşağıda listelenmiştir:

- Mali değeri için veri hırsızlığı: İsim, adres, sosyal güvenlik detayları, finansal bilgiler vb. kişisel verilerin çalınıp satılması,
- Fidyeye yazılımı: Bir ücret ödenmediği sürece kullanıcılarının verilerine ulaşımını veya sisteme erişimini engellemek ya da verileri silmek için kötü amaçlı yazılım kullanılması
- Veri bozulması: Siyasi veya kişisel kazanç için test sonuçlarını değiştirme gibi verilerin kasıtlı bozulması
- Hizmet reddi saldırıları: Şantaj, intikam veya eylem ile harekete geçerek gereksiz talepler ile bir ağ ya da sistemin işleyişini durdurmak
- İş e-posta uyumu: Finansal kazanç için sahte kişisel hesapların oluşturulması ve kullanılması
- Çalışanların kasıtsız eylemleri: Personelin kasıtsız eylemleri ve risk altındaki sistemler nedeniyle veri kaybı ya da sistemlerin ciddi şekilde bozulmasıdır.

Sağlık sektöründeki yaygın güvenlik açıkları aşağıda listelenmiştir:

- Güncelliğini yitirmiş teknolojik cihaz ve yazılımların kullanılması.
- Ağ güvenliği takibi yapılmayan bağlantı sistemleri.
- Güvenli olmayan herkese açık ağ bağlantılarının kullanılması.
Üzerinde etkin bir kontrol sağlanamayan dışarıdan sisteme bağlanan ağlar, sistemi saldırıya açık hâle getirebilmektedir.
- Eski donanımların tam olarak imha edilmeden elden çıkarılması.
Örneğin; hasta kayıtlarına ait verileri sadece silmek bilgilerin erişilmez olduğu anlamına gelmemektedir. Herhangi bir bilgisayar korsanının eline geçen eski bir donanım veya sabit disk, yeniden yapılandırılıp silinen bilgiler kurtarılırsa istenmeyen sonuçlar ortaya çıkabilmektedir.
- Herkesin kullanımına açık yetkilendirme ile kısıtlanmamış bilgisayar sistemleri risk oluşturmaktadır.
- Güvenli olmayan mobil cihazların kullanımı güvenlik açığına sebebiyet vermektedir. Mobil oturum ile sisteme giriş izni veren kurumlara dışarıdan bağlanan mobil cihazlar her zaman güvenlik standartlarını karşılamamaktadır.

Bilgisayar korsanları açık buldukları bir sistem üzerinden hassas bilgilere ulaşabilmekte ve bunları kendi menfaatleri için diledikleri gibi kullanabilmektedir.

3-Tıbbi Cihazlara Yönelik Siber Saldırıları

Hastalara doğrudan zarar vermeye veya hastaları tehdit ederek bir menfaat elde etmeye yönelik yapılan siber saldırılara “medjacking” adı verilmektedir. Medjacking, genellikle hastane ağlarında arka kapılar oluşturarak tıbbi cihazların ele geçirilmesini amaçlamaktadır.

Saldırganlar, eski teknolojilere dayalı medikal sistemlere yeni teknolojilere göre daha kolay yetkisiz erişim sağlamaktadır. Tanı ve tedavi ile yaşam destek için kullanılan araçların bir kısmı eski ve standart işletim sistemlerini kullanmaktadır. Bu durum saldırıların işini kolaylaştırmaktadır. Bir sağlık kurumunda farklı türde ve sayıca fazla tıbbi cihaz bulunur. Saldırganların sadece bir cihazı ele geçirmesi tüm sistemi tehdit altına sokabilmekte ve saldırı ağıdaki daha değerli veriye sahip diğer tüm kaynaklara da erişim olanağı elde edebilmektedir.

Teknolojinin gelişmesi ve tıbbi cihazların çeşitlenmesinin hızı ile bu cihazların hem kendi güvenlikleri ve diğer bilişim sistemleri güvenliği hem de veri kaynakları için risk oluşturma ve saldırıların ilgisini çekme hızı doğru orantılı olarak artmaktadır. Tıbbi bir cihazın tanımlanan işlevleri yerine getirebilmesi için bir bilgisayar ortamı ile ağ ortamında iletişim hâlinde olması gerekmektedir. Bilgisayar korsanının bir tıbbi cihazın kontrolünü ele geçirebilmek için ağıdaki bilgisayarı ele geçirmesi yeterli olmaktadır.

Zafiyet barındırdığı tespit edilmiş cihazlara insülin pompaları, görüntüleme cihazları, kalp pilleri ve defibrilatörler örnek verilebilir. Bu cihazların bazılarında saldırı gerçekleştirilmişken bazılarında sadece zafiyet bulunduğu tespit edilmiştir.

4-Siber Saldırganlar Neden Sağlık Sektörünü Hedefler?

Siber saldırılar türünden bağımsız olarak genellikle temel nedeni kritik veri erişimi olmaktadır. Sağlık sektörünü hedefleyen saldırıların:

- Hastaların tıbbi bilgileri, özlük bilgileri ve hastane fatura kayıtları gibi verilen internetin karanlık ortamlarında kolayca alıcı bulabilecek olması
- Teknolojik kaynağı arttırılan hastanelerde internet bağlantılı tıbbi cihazların uzaktan erişim yoluyla ele geçirilmeye uygun olması
- Fidyeye yazılım saldırılarının hasta bakımı kaynaklarını ve kurum idari yapısına ait sistemleri kilitlemesi sonucunda maddi kazanç elde edebiliyor olması
- Hassas verilerin çalınarak kamuoyuna açıklanabilmesi.
Örneğin ünlüler, siyasetçiler veya diğer yüksek profilili insanların tıbbi bilgilerinin yayınlanması.
- Devlet hedefli saldırılarda zarar boyutunu büyütme gibi motivasyonları bulunmaktadır.

5-Sağlık Sektörünü Hedef Almış Siber Saldırıları

2017 yılında 100'ü aşkın ülkeye saldırı yapan WannaCry fidye yazılım virüsü, Birleşik Krallık Sağlık Servisi'ni ciddi boyutlarda zarara uğratan bir saldırı gerçekleştirdi. 12 Mayıs'ta bilgisayar korsanları İngiltere Sağlık Servisi NHS'nin verilerini Microsoft işletim sistemlerindeki bir açıktan yararlanarak rehin aldı. NHS personellerinden biri kendisine gönderilen ve masum gözükten e-postayı açarak ortalama saldırısına düşürüldü, e-postanın açılmasıyla WannaCry virüsü sistemlerinde aktif hâle gelerek tüm verileri şifreledi ve hastanenin çalışamaz hâle gelmesini sağladı. Kısa süre içerisinde tüm sağlık personeli ekranda beliren fidye mesajıyla karşılaştı. Mesajda 3 gün içerisinde belirlenen para istenen hesaba yatırılmazsa fidyenin miktarının 2 katına çıkacağı, 7 gün içinde yatırılmazsa dosyalara bir daha asla erişemeyecekleri yazmaktaydı.

İngiltere'de birçok hastane, "WannaCry" virüsü kendi sistemlerine bulaşmadan önce sistemlerini elektronik olarak korumaya alabilmişti fakat bu, siber saldırının etkisinin trajik boyutlara ulaşmasını engelleyememişti. Sağlık alanında bulaştığı tüm bilgisayarlarda elektronik hasta kayıtlarına zarar verdiği için işlemler kâğıt-kalem usulüne döndü. Bu durum hastane rutininin daha da yavaşlamasına sebep oldu. Üstelik sistemler düzeltildiğinde tekrar kâğıt üstündeki verileri sisteme işlemek fazlaca mesai gerektirdi.

Kâğıtla işlem yapılamayan, sadece elektronik olarak gerçekleştirilen bazı muayenelere hasta kabul edilemedi ve doktorlar acil ihtiyaçları olan röntgen cihazlarını dahi kullanamadı. Londra'nın en büyük hastanelerinde kan ürünlerinin tutulduğu buzdolaplarının kontrol sistemlerinin bozulması cerrahi operasyonların aksamasına sebep oldu. Londra Hastanesi travma, felç ve kalp krizi merkezlerini kapatarak hastalarını uzaklara göndermek zorunda kaldı.

Bu saldırı, NHS bilişim sistemlerinin saldırılara karşı ne kadar savunmasız olduğunu ve kriz durumunun yönetilemediğini göstermesi açısından önemlidir. NHS bilgisayarlarında Windows XP sistemleri kullanılırken Microsoft'un 2017 Mart ayında yayınladığı güncellemenin zamanında yüklenmediği veya sistemlerin bu yamadan faydalanamayacak kadar eski olduğunu gösterdi. Saldırı, sağlık sektörü için büyük bir ders oldu. Zararın ne denli büyük olabileceği ile tüm dünya yüzleşti ve hastanelerin bilişim sistemlerinin geliştirilmesi gerektiği gözler önüne serilmiş oldu.

6-Sağlık Sektöründe Siber Güvenlik Nasıl Sağlanır?

Sağlık teknolojileri ve hasta bilgilerinin güvenliğini sağlamak için daha fazla maliyet ve çaba sarf edilmelidir. Sektörde kullanılan cihazlar için güvenlik, ürün tasarlarken baştan hesap edilmeli, sonradan düşünülmemelidir.

Siber güvenlik, hasta bakım kültürünün bir parçası hâline getirilmelidir. Sağlık sektöründe yeterli fiziki koşullar oluşturularak, yasal sorumluluklar çerçevesinde alanında uzman kişilere yetki verilip bilgi güvenliğinin oluşturulması sağlanmalıdır.

Bu bağlamda uzmanlarca yapılan öneriler şu şekilde sıralanabilir:

- Tüm personele düzenli aralıklarla bilgi güvenliği eğitimi verilmeli
- Bilgi güvenliği yönetim sisteminin etkili işlemesi amacıyla, yöneticiler ve çalışanlar iş birliği içinde olmalı
- Profesyonel yazılım firmalarıyla çalışılmalı
- Sağlık çalışanlarının ve hastaların bilgi güvenliği bağlamında haklarının ihlal edildiğini düşündükleri durumlarda hastanede başvurabilecekleri bir birim bulunmalı
- ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı kullanımının tüm hastanelerde yaygınlaştırılmasını sağlamak amaçlı gerekli şartlar oluşturulmalı
- Hasta ve hastaneye ait bilgilerin üçüncü kişilerce paylaşılmasının önüne geçmek için informal kanalların kullanımını ortadan kaldırmak ve personelin yaptırımlardan haberdar edilerek gerekirse cezai işlem uygulanmalı.

Gelecek siber saldırı risklerine karşı üzerinde durulması gereken öncelikli 10 konu başlığı şöyledir:

- Siber güvenlik farkındalığı
- E-posta güvenlik sistemleri
- Endpoint koruma sistemleri
- Erişim politikaları ve uygulamaları
- Verilerin korunması ve veri kayıplarının önlenmesi
- Varlık (envanter) yönetimi
- Network yönetimi
- Zafiyet yönetimi
- Olay müdahâlesi
- Medikal cihaz güvenliği
- Siber güvenlik politikaları

KAYNAKÇA

<https://dergipark.org.tr/tr/download/article-file/658839>
<https://jag.journalagent.com/jaren/pdfs/JAREN-27879-REVIEW-TOSUN.pdf>
Rachel Clarke, M.D., and Taryn Youngstein, M.D. Cyberattack on Britain's National Health Service – A Wake-up Call for Modern Medicine. NEJM June 7, 2017
<https://www.drozdogan.com/wanna-cry-virusu-ile-ingiltere-saglik-sistemine-siber-saldiri/>
<https://kron.com.tr/saglik-alaninda-siber-guvenlik>
<https://cdn.istanbul.edu.tr/file/JTA6CLJ8T5/D2114C8AB5284539BA6ADCB6CDDC2861>
Ayala, L., (2016), "Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention", Apress, Berkeley, CA
<https://revisionlegal.com/internet-law/data-breach/medjacking/>
<https://ccip.khas.edu.tr/post/22/saglik-sektorunde-yeni-tehlike-siber-riskler>
<https://beranet.com/blog/saglik-sektoru-acisindan-siber-guvenligin-onemi>

AYŞE
GÜL ASLAN

KONU
07





GÜVENLİ İNTERNET

Evlerimizi, sitelerimizi, gittiğimiz yolları kısacası yaşadığımız mekânları, anları nasıl güvenli kılmak için tedbirler alıyorsak artık hayatımızın bir parçası olan internet ve onun uzantılarını güvenli hâle getirmek için de bilinçli olmalıyız.

Güvenli İnternet Nedir?

İnternet dediğimiz olgunun güvenliği, ağ güvenliği, uygulama ve işletim sistemleri güvenliği ile bir bütündür. Yani arama yaptığımız internet tarayıcıları, kullandığımız modemler, alışveriş siteleri, telefonlarda kullandığımız uygulamalar, e-postalarımız, kaydolduğumuz üyelikler, kullandığımız sosyal ağlar, izlediğimiz videolar, tıkladığımız linkler, indirdiğimiz dosyalar ve daha fazlası bu bütünün içindedir. Günlük hayatımızda bilgiye ulaşmak, iletişim, eğlence, bankacılık, eğitim ve alışveriş için kullandığımız internet, gerekli tedbirler alınmadığı takdirde maalesef hiç güvenli değildir. Nasıl ki gerçek hayatta olası tehlikelere karşı kapımızı kilitleyip kameralar, alarmlar taktırıp kendimize güvenli alanlar sağlıyorsak aynı ehemmiyeti internet kullanımında da göstermek zorundayız. Gerekli tedbirleri alarak internetteki tehlikelere karşı her adımımızı güven içinde atabilir kendimizi ve ailemizi gelebilecek olan zararlardan koruyabiliriz.

Peki, nedir bu tehlikeler?

Kötü amaçlı veya zararlı yazılımlar, kişisel verilerin ele geçirilmesi, çocuk istismarı, dolandırıcılık, müstehcenlik, kumar, siber zorbalık vb.

Kötü amaçlı ve zararlı yazılımlar, kullanıcının yani bizlerin izin vermediği işlemlerin gerçekleştirilmesine sebep olan yazılımlardır.



Bilgisayar virüsleri

Cihazınızın çalışma şekline müdahale edebilen, yavaşlatabilen, silebilen ve dosyaların içinde saklanıp başka cihazlara yayılabilen programlardır.



Solucanlar

Çalışmak için bir programa ihtiyaç duymayan, ağdan veya bir dosyadan kolaylıkla bilgisayara bulaşabilen, hızla çoğalıp yayılabilen yazılımlardır.



Truva Atları

Faydalı veya zararsız bir program gibi görünür. Saldırgan bir programın içine zararlı kodlar yerleştirir. Kullanıcı programı açtığında Truva atları aktif hâle gelir. Bunlar sayesinde uzaktan erişim sağlanabilir. Her türlü kişisel bilginiz ele geçirilebilir.



Reklam Yazılımları

Pazarlama amaçlı verileri toplayan yazılımdır. Siteler ziyaret edildiğinde cihazlara yüklenip aktifleşir. Kullanıcı izni olmadan kullanılırsa kötü amaçlı hâle gelir.



Botnet

Robot ağının kısaltılmışı olan botnet ile bilgisayarınız zombiye dönüşür. Saldırgan bilgisayarımızı uzaktan kontrol edebilir ve başka ağlara bağlanıp yasal olmayan işlemler yapabilir.



Kişisel verilerin ele geçirilmesi

Yukarıda adı geçen ve adı geçmeyen birçok yöntemle kişisel verilerimiz ele geçirilebilir ve kötü amaçla kullanılabilir.



Çocuk istismarı

Çocuklar maalesef her alanda olduğu gibi bu alanda da zayıf halka. Denetimsiz internet kullanımı çocukların yaşlarına uygun olmayan içeriklere maruz kalmasına sebep olabilir. Kandırılabilir, dolandırılabilir, siber zorbalığa maruz kalıp korkutulabilir, taciz edilebilir, her türlü istismara uğrayabilir hatta kaçırılabilir.



Dolandırıcılık

Banka linkleri taklit edilerek, piyango veya bağış adı altında, yüksek kârlı iş teklifi sunularak, duygusal boşluklardan faydalanarak, millî ve manevi duygular sömürülerek gerçekleştirilen farklı dolandırıcılık türleriyle karşılaşılabiliriz.



Müstehcenlik

İnternet kullanımı sırasında maalesef isteğimiz dışında pornografik yazı ve görüntülere rastlamak mümkün.



Kumar

Çok yaygın bir şekilde reklamlarını gördüğümüz kumar ve bahis siteleri özendirici yayınlar yapmaktadır.



Siber zorbalık

Dijital ortamda hedef kişinin kasıtlı, düzenli ve devamlı olarak korkutulması, utandırılması, incitilmesi, tehdit edilmesi, kısaca her türlü rahatsız edici davranışa maruz bırakılması.



İnternetteki Tehlikelerden Nasıl Korunuruz?



Virüs koruma programları kullanmaya özen göstermeli ve onları sürekli güncel tutmalıyız. Bu programlar bizi zararlı ve kötü amaçlı yazılımlardan korur.



Kişisel bilgi güvenliğimizi sağlamalıyız. Kimlik bilgilerimizden adresimize, fotoğraflarımızdan pasaport numaramıza, sosyal kültürel psikolojik bilgilerimizden kan grubumuza kadar bize ait bütün bilgiler kişisel bilgidir.



İnternette ve sosyal ağlarda açık bir şekilde konum bilgisi, adres ve iletişim bilgisi paylaşılmamalıyız.



Çevrim içi satın almalarda güvenli ve bilinen siteleri kullanmalıyız. [http:](http://) yerine [https:](https://) (S harfi secure (güvenli) anlamına gelir), ile başlayan adresleri kullanmaya dikkat etmeliyiz. Adres çubuğunun başındaki kilit işareti de güvenli olduğunu gösterir. Bu sitelerde her türlü iletişim ve kredi kartı bilgilerimizi kullandığımız için bunlara maksimum düzeyde dikkat etmeliyiz. Sanal kredi kartı kullanmayı alışkanlık edinmeli, üyelik şifrelerimizi güvenli ve güçlü oluşturmamız.





E-postadan, başka bir internet sitesinden veya arama motorundan bulup tıklamak yerine girmek istediğimiz siteye adres satırına yazarak ulaşmalıyız.



Ortak kullanılan ağlarda (kafe, alışveriş merkezi, iş yeri gibi) kişisel işlemler yapmamaya ve kendi bilgisayarımızı kullanmaya özen göstermeliyiz.



Telefonlarımıza gereksiz uygulamaları yüklememeliyiz. Zira uygulamalar her türlü erişime izin hakkı isteyerek kurulum sağlıyor. Erişim kontrolünü mutlaka sınırlı tutmaya çalışmalıyız.



Çocuk istismarının önlenmesi için alınması gereken tedbirleri şöyle sıralayabiliriz:



Öncelikle çocuğumuzun bilgisayar, telefon veya tablet kullanımı yaşına göre sınırlı sürede olmalı.



Odasında tek başına bu cihazlarla bırakmamalıyız.



Çocuğumuzun ziyaret edeceği siteleri daha güvenli hâle getirmek için filtreler veya ebeveyn denetim programları kullanmalı, onun iyiliği ve güvenliği için olduğu onu uygun ve etkili bir dille anlatmalı hatta örnek olunmalıyız.



Uygun yaşa gelmeden sosyal ağlarda hesap açmasına izin vermemeliyiz. Hesap açılrsa bile asla denetimsiz kullandırmamalıyız.



Kişisel bilgilerin ne olduğu ve bu bilgilerin kendisine ve ailesine özel olduğu konusunda bilgilendirilmeliyiz.



İnternette kötü ve çirkin bir durumla karşılaştıklarında ne yapmaları gerektiği konusunda net bir şekilde anlatmalı ve bize güvenmelerini sağlamalıyız.



Dolandırıcılığa karşı yine kişisel verilerin güvenliği ile ilgili güvenlik önlemlerini almalıyız. Şüpheli e-posta veya sosyal ağ mesajlarına karşı uyanık olmalıyız. Para veya hediye kazandınız gibi açıklamalara teyit etmeden asla güvenmemeliyiz.



Müstehcenlik ve kumar için filtreler koymalı, kullanıma göre aile veya çocuk profilleri oluşturup bu tür çirkin ve kötü amaçlı içeriklerden kaçınmalıyız.



Siber zorbalığı önlemenin başında yine kişisel verilerimizin gizliliği ilk sıradadır. Çünkü kaba ve saldırgan kişiler profil bilgileri üzerinden yola çıkarak saldırılarını yapmaya başlar. Ne kadar çok veri paylaşırsak o kadar çok malzeme vermiş oluruz. Tanımadığımız kişilerle bağlantı kurmaktan kaçınmalıyız. Zorbalık içeren mesajları paylaşarak buna ortak olmamalı, kötü olanı yaymamalıyız.

İnternet, hayatımıza getirdiği kolaylıklar kadar risk ve tehlikelerini de beraberinde getirmiştir. Fakat insan olarak tercihlerimizle iyi olanı hayatımıza rehber edinebilecek iradeye sahibiz. Bu irademizi iyiden güzelden ve faydalı olan-
dan yana kullanarak dijital dünyanın tehlikelerini bertaraf edebiliriz. Bütün bunların yanında bizler ve çocuklarımız dijital okur-yazarlık seviyemizi artırıp sorumluluk sahibi bilinçli bireyler olarak artık kaçınılmaz olan bu dijital hayata güvenle adapte olabiliriz.







SİBER SİGORTA

Sigorta Nedir?

Günümüzde hepimiz beklenmeyen durumlar karşısında maddi ve manevi olarak değer verdiğimiz varlıklarımıza zarar gelmemesi adına sigorta yaptırmanın, lüksten ziyade bir ihtiyaç ve mecburiyet hâline geldiğinin farkındayız.

Sigorta; tatile çıktığımızda geride kalan evimizi, beklenmeyen bir anda yaşanabilecek doğal felaketler karşısında zarar görebilecek varlıklarımızı, uyurken iş yerimizi ve arabamızı güvenceye almamızı sağlıyor.

Peki ya pandemi dönemi sonrasında hem bireysel hem kurumsal hayatlarımızın içerisine iyice dâhil olan ve bizim hakkımızda bizden çok şey bilen sosyal medya şirketleri verilerimizi nasıl güvenceye alıyor? İşte bu kısımda da “Siber Sigorta” devreye giriyor.

Siber Sigorta Nedir?

Siber sigorta, gizliliği zorunlu olan ve korunma ihtiyacı duyulan verilerin hukuka aykırı yollarla ortaya çıkarılması ve paylaşılması ile oluşacak hasara karşı yapılan sigorta poliçesi olarak ifade edilir.

We Are Social Digital’in 2022 raporuna göre internet kullanıcı sayısı %4 oranında (+192 milyon), sosyal medya kullanıcıları %10,1 (424 milyon) artış gösterdi. Buna ek olarak sigorta şirketi Hiscox tarafından 2018 Ekim’inde yapılan bir araştırmaya göre küçük ölçekli işletmelerin %30’u bir önceki yıla kıyasla en az bir kere veri sızıntısıyla karşı karşıya kaldı. Bu artış karşısında veri ihlalleri, fidye yazılımlar ve e-dolandırıcılık vakaları da manşetlerden düşmüyor. İngiliz medyasında yer alan haberlere göre, Hive fidye yazılımı grubunun İngiltere’de yer alan iki okulun bilgi sistemine sızarak öğrencilerin ev adreslerini, banka verilerini ve tıbbi bilgilerini elde ettiği, verilerin sızdırılmaması karşılığında ailelerden yaklaşık 608.000 \$ talep ettiği iddia edildi.

Peki bu veriler ve haberler ardı sıra birbirini takip ederken biz kendimizi ve işletmemizi olası bir siber saldırı durumu için nasıl güvence altına alabiliriz?

Sorumuzun en güncel cevabı: Siber Sigorta.

Siber Sigortanın Kapsamı Nedir?

Verilerin herhangi bir şekilde kaybolması, ihlal edilmesi veya çalınması bizleri olumsuz etkiler. Eğer bir işveren konumundaysak veri ihlali durumu, müşterilerimizin bize olan güvenini kaybetmelerine sebebiyet verebileceği gibi saldırıdan kurtulmak yüklü finansal maliyetler yaratabilir.

Siber sigorta, normal sigorta anlayışına ek olarak riskleri azaltmayı da hedefler. Bu nedenle siber sigorta, ilgili güvenlik vakasının yaşanması durumlarında, personelin farkındalığını artırmak ve personel tarafından alınması gereken aksiyonları belirlemek için eğitimler vermeyi ve kurumlar tarafında alınması gereken siber güvenlik önlemlerinin belirlenmesini de kapsamında tutar.





Siber sigorta řu konularda bizlere yardımcı olur:

- İhlal edilen verilerin kurtarılması (fidye yazılımı saldırısı gibi bazı durumlar)
- Güvenlięi ihlal edilmiř bilgisayar sistemlerindeki herhangi bir hasarı onarmanın toplam maliyeti
- Hukuki cezalar
- Ödeme araçlarının hileli kullanımından oluşacak zararlar
- Sanal saygınlığa ilişkin hukuki destekler
- Ortalama gibi saldırılar sonucu oluşacak maddi kayıpların belirli miktarlarda giderimi
- Siber fidye ve řantajlar sebebiyle doğacak kayıplar
- Kredi ve banka kartı ile cep telefonu, e-posta ve benzeri araçlara yönelik řifre koruma hizmetleri



Türkiye’de Siber Sigorta

Siber sigortalar, dünyanın diğer yerlerinde olduğu gibi Türkiye’de de veri koruma ve siber koruma isimleriyle tüketicilere sunulmaya başlanmıştır. Türkiye’de ilk kez 2017 yılında Anadolu Sigorta tarafından piyasaya sürülmüştür ancak Amerika merkezli AIG Sigortanın ise Türkiye’de 2012 yılından beri bu alanda sigorta hizmeti verdiği görülmektedir.

Bugün ise Aksigorta (Siber Koruma Sigortası), Allianz Sigorta (Siber Sorumluluk Sigortası), Doğa Sigorta (Ticari Siber Güvenlik Sigortası) aralarında bulunduğu 11 sigorta şirketinin tek başına siber sigorta poliçesi sağlayabildiği bilinmektedir.

KAYNAKÇA:

https://www.trendmicro.com/tr_tr/what-is/cyber-insurance.html
https://www.researchgate.net/publication/357529498_NFT%27LER_OZELINDE_SIBER_SIGORTAYA_BIR_BAKIS
<https://siberbulten.com/siber-guvenlik/siber-sigorta-nedir-isletmenizi-nasil-korur/>
<https://therecord.media/ransomware-group-demands-500000-from-british-schools-citing-cyber-insurance-policy/>
<https://dijilopedi.com/2021-dunya-internet-sosyal-medya-ve-mobil-kullanim-istatistikleri/>
<https://www.financialexpress.com/money/insurance/cyber-risks-need-to-popularise-cyber-insurance/2177213/>
<https://periscope.com.tr/we-are-social-global-dijital-2022-raporu/#:~:text=D%C4%B0J%C4%B0TAL%20B%C3%9C%C3%9CME,58%2C4%C3%BCne%20e%C5%9Fit.>





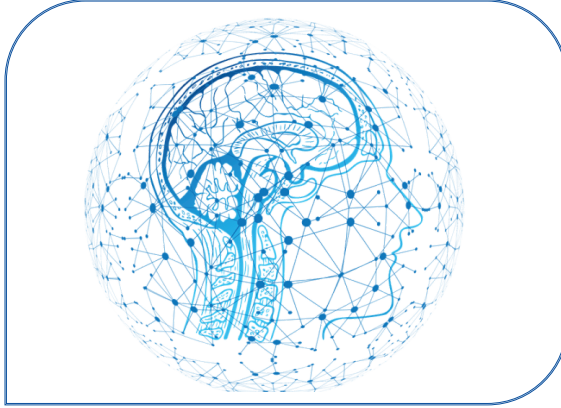
SİBER GÜVENLİKTE MAKİNE ÖĞRENMESİ

Makine Öğrenmesi Nedir?

Makine öğrenmesi, tıpkı insan zekâsında olduğu gibi bir yandan elindeki verileri işlerken diğer yandan insan zekâsının uzun süreler uğraştığı veri girdilerini bir bilgisayar sistemine çok kısa sürelerde aktarımını sağlayarak nasıl tahminler yapılacağını öğretme sürecinde kullanılan bir algoritmalar bütünüdür.

Kısaca, deneyimden öğrenmek de denilebilir.

Klasik bilgisayar yazılımlarından temel farkı; geliştiricinin, sisteme örneğin saz kelimesinin bir müzik terimini mi yoksa bir bitki adını mı temsil ettiğini belirten bir kod yazmamış olmasıdır. Bunun yerine, bir makine öğrenmesi modelini, büyük miktarda veri ile eğiterek bu gibi ayrımları yapması sağlanır.



Siber Güvenlikte Makine Öğrenmesi Neden Kullanılır?

Günümüzde makine öğrenimi siber güvenlik sektörü için önemli bir teknoloji hâline gelmiştir. Büyük ölçekli verileri değerlendirme sürecini kolaylaştırır.

Siber tehditleri belirlemede ve bu tehditlere karşı koruma yazılımları geliştirme gibi birçok uygulamada kullanılır.

Siber güvenliği en zorlayan kısımlardan biri olan büyük miktarda veri alıp göndermek gibi faaliyetlerde makine öğrenimi uzmanlara yardım eder.

Sisteme gelip giden aramaların yanında tüm şüpheli etkinlikleri de takip eder.

Virüs gibi zararlı yazılım tehditleri için anti-virüs yazılımları önerilmektedir. Geleneksel anti-virüs yazılımları, oluşturulan yeni virüsler için yükseltmelere ihtiyaç duyar. Tabii bu noktada işi kolaylaştırmak adına makine öğrenimi ile entegre olan anti-virüs yazılımlarının kullanımı son yıllarda dikkat çekmektedir. Bu entegrasyon, daha önce karşılaşılan tehditleri ve yeni oluşturulmuş virüslerden kaynaklanan tehditleri yönetebilir.

Bazı siber tehditler, sistem kullanıcılarından herhangi birinin oturum açma bilgilerine erişim ile gerçekleşebilir. Bu gibi tehditlerde tespit, kullanıcı bilgileri gerçek olduğundan dolayı zordur. Bu noktada devreye makine öğrenimi uygulamaları girer. Makine öğrenimi bu gibi olaylar için kullanıcı davranış modellemesi kullanılarak yardım sağlayabilir. Algoritma, kullanıcıların oturum açma-kapama gibi davranışlarını belirlemek için eğitilir. Olağan dışı bir olay gerçekleştiği takdirde sistem bunu anlayabilir ve buna yönelik uyarı ve tepkilerde bulunabilir.

Çalışanların şirket e-posta hesaplarının izlenmesi kimlik avı saldırıları açısından kritiktir. Bu saldırılar, çalışanlara sahte e-postalar göndererek birtakım önemli bilgileri elde etmektedir. Makine öğrenmesinde doğal dil işleme kullanılarak e-postaları taramak, saldırı kalıpları olup olmadığını ayırt etmek mümkündür. Bu çözüm yoluyla birlikte tehditler en az seviyeye indirilebilir.

Siber Güvenlikte Makine Öğrenmesi Neden Zorunlu Hâle Gelmektedir?

Makine öğrenimiyle birlikte siber saldırılara karşı yanıt vermek amacı ile kalıplar analiz edilebilir ve öğrenilebilir. Rutin görevlere harcanan süreler azaltılabilir ve kaynaklar daha verimli şekilde kullanılabilir.

Gelişen teknoloji ile birlikte, bilgisayar korsanları hâli hazırda yapay zekâ ve makine öğrenmesi sistemlerini siber saldırılar için kullandıklarından dolayı güvenlik için de bu sistemler zorunlu hâle gelmektedir.



KAYNAKÇA:

1. Nick Heath, "What is machine learning? Everything you need to know," 16 Aralık 2020.
2. Javaid Nabi, "Machine Learning – Fundamentals," 15 Ağustos 2018.
3. Vahit Buğra Yeşilkaynak, "Yapay zekâ, makine öğrenmesi ve derin öğrenme kavramları arasındaki farklar nedir?" 20 Haziran 2020.
4. Global Radiance Review, "Use of machine learning in cyber security."
5. Alex Polyakov, "Machine learning for cyber security 101," 4 Ekim 2018.
6. Geeks for Geeks, "Top 5 applications of machine learning in cyber security," 13 Eylül 2022.
7. Al Perlman, "The growing role of machine learning in cyber security."





ÇOK FAKTÖRLÜ DOĞRULAMA

Çok Faktörlü Doğrulama - SİZ SAHİDEN SİZ MİSİNİZ?

Çok Faktörlü Doğrulama [Multi-Factor Authentication (MFA)], kimlik ve erişim yönetiminin önemli bir bileşeni olarak günümüzde birçok alanda sıklıkla kullandığımız bir güvenlik yöntemidir. Adından da anlaşılacağı üzere bir kişi veya nesne, herhangi bir kaynaktan (ağ, cihaz, uygulama vb.) oturum açmak istediğinde kişiyi veya nesneyi birçok aşamadan geçirerek kişi veya nesnenin kaynak tarafından bilinen kimlik ve erişim bilgilerine sahip olup olmadığını test etmek üzerine tasarlanmıştır.

Bu güvenlik yöntemi herhangi bir kaynaktan oturum açmak isteyen kullanıcıyı "Siz sahiden siz misiniz?" anlayışı ile birçok güvenlik aşamasından geçirip, test ederek çalışır. Buradaki önemli detay bu aşamaların (güvenlik sorularının) birbirinden bağımsız olmasıdır. Birbirinden bağımsız güvenlik sorularının olması elbette ki güvenliğin sağlanması açısından faydalı bir faktördür.



Kullanıcı; Bilgi Faktörleri, Sahiplik Faktörleri ve Doğal Faktörler olmak üzere temel 3 ana güvenlik aşamasından geçirilir.

Örnek vermemiz gerekirse kullanıcıdan ilk olarak kaynak tarafından bilinen kimlik ve erişim bilgileri talep edilir ki bunlar genellikle kullanıcı adı ve paroladır. Daha sonraki aşamada sahiplik bilgisi içeren tek kullanımlık bir parola istenebilir ve en son aşamada ise kullanıcıdan kişiye özel ve doğal bir faktör olan parmak izi, yüz tanıma vb. gibi bir doğrulama isteyebilir. Burada 3 ana başlıktan birer tane doğrulama içerecek şekilde bir örnek verdik. Fakat bu aşamalar artırılabilir veya azaltılabilir.

Çok faktörlü doğrulamanın nasıl çalıştığından bahsettik. Bu güvenlik sistemini neden kullanmalıyız, biraz da bundan bahsedelim.

Çok faktörlü doğrulama kullanmamız tüm tehditleri ortadan kaldırmasa bile kötü niyetli bilgisayar korsanlarının birçoğunu caydırıcı nitelikte bir güvenlik yöntemidir. Günümüzde teknolojik gelişmelerin artması ile teknoloji hayatımızın her alanına girmeye başladı. Bankacılık işlemleri, alışverişler ve daha birçok gündelik iş, sanal dünyaya taşındı. Birçoğumuzun birden fazla platformda birden fazla sosyal medya hesabı var. İyi ama bunların güvenliği nasıl daha iyi bir şekilde sağlanır? Tek bir parola yeterli midir? Elbette değildir.

Düşünsenize, bankanızın mobil uygulamasındaki online bankacılık işlemlerinizi için bir parola belirliyorsunuz fakat parolanız kötü niyetli bir bilgisayar korsanının eline geçiyor. Bu çok büyük bir güvenlik açığıdır. Bu yüzden çok faktörlü doğrulama kullanmalıyız. Parolanızı eline geçiren kötü niyetli bir bilgisayar korsanı olsa dahi diğer doğrulama aşamalarını geçemeyecek veya uğraşmak istemeyecek ve hesabınızın güvenliği çok büyük bir oranda sağlanmış olacaktır.

Peki bu güvenlik sistemi şu anda hangi sektörlerde kullanılıyor?

Bankacılık ve finans sektöründeki erişim güvenliği ve kimlik doğrulaması konularının ekstra önem taşımasıyla birlikte çok faktörlü doğrulamanın en çok bu sektörde kullanılıyor olması tahmin edilebilir bir sonuç. Fakat bu güvenlik yöntemi başka alanlarda da kullanılmaktadır. Erişim güvenliği ve kimlik doğrulaması konularının önemi ve ihtiyacı, artan teknolojik gelişmelerin de etkisiyle her alanda kendisini hissettirmektedir.

Bu sebeple eğitim sektöründen sağlık sektörüne, online alışveriş sektöründen telekomünikasyon sektörüne kadar birçok sektörde kullanılıyor ve hatta kullanılması da ihtiyaç hâline geliyor.

Çok faktörlü doğrulama kullanmanın önemini artık biliyoruz fakat bunu kullanmak da her zaman yeterli olmaz. Elbette kaynağı daha güvenilir kılar fakat burada önemli olan kaynağa erişimin 2 veya çok faktörlü olması değildir, önemli olan doğrulama aşamalarında seçilen güvenlik sorularının kalitesidir. Doğrulama aşamaları birbirinden bağımsız ve olabildiğince kişiye özel erişimli sorulardan seçilmelidir.

Bütün bunların yanında hâlâ yüzde yüz bir güvenlikten söz edemeyiz. Son zamanlarda bu güvenlik yöntemini de atlatıp sistemlere sızan bilgisayar korsanları mevcut. Kimlik doğrulama ve erişim güvenliği konularına önem veren birçok şirket gibi, Cisco, Uber ve EA Games gibi büyük şirketler de çok faktörlü doğrulama kullanıyordu. Fakat bu üç şirketin de ne yazık ki çok faktörlü doğrulama aşamaları kötü niyetli bilgisayar korsanları tarafından atlatılıp sistemlerine sızıldı.

Peki Cisco nasıl hacklendi, haydi bakalım:

Yayımlanan blog yazısına göre tehdit aktörleri Cisco çalışanı bir kişinin şahsi Google hesabını ele geçirmiş ve orada kayıtlı olan kurumsal ağa Cisco uzantılı erişim parolasını kullanarak girişi denemiş.. Saldırgan grup, elde ettiği kişisel bilgiler ile MFA atlatma tekniklerini kullanarak kullanıcıya gelen doğrulama kodunu almayı/onaylatmayı başarmış. Bu yöntemle ağ üzerinde bulunan önemli hesaplara ulaşmış, bunları internette yayımlamışlardır.

Siber güvenlik uzmanları, saldırganın içeride çok daha farklı ve fazla sisteme erişmiş olabileceğini düşünüyor.

Über'in hacklenmesi:

Uber'in dünyaca tanınan bir yazılım şirketinin çok faktörlü doğrulama sistemini kullandığını bilen hacker, sosyal mühendislik ile bir Uber çalışanını takibe almış ve kendisi hakkında bilgiler edinmeye başlamış. Avı için planlarını hazırlayan hacker, sahte bir Uber giriş sayfası oluşturmuş. Daha sonra bu sayfa sayesinde kurbanın giriş bilgilerini elde eden hacker'ın atlatması gereken bir tek MFA kalmış. Uber çalışanına saatlerce arka arkaya giriş bildirimini gönderen hacker, daha sonra çalışana WhatsApp üzerinden ulaşarak sistemde bir arıza olduğunu ve bildirimlerden birini onaylaması gerektiğini söylemiş. Çalışan bildirim onaylamış ve bu sayede hacker sisteme sızmış.

Hacker, kendisiyle konuşanlara hangi belgeleri ya da ne tür bilgilerini aldığını açıklamasa da pek çok güvenlik uzmanı hackerın kullanıcıların özel bilgilerinden tutun da şirketin mali kayıtlarına kadar birçok veriyi ele geçirmiş olabileceğini düşünüyor.

EA Games ise daha farklı bir yöntemle hacklenmiş, bir de ona bakalım:

Ünlü oyun firmasının çalışanlarının cihazlarında tuttuğu çerezleri çalmayı başaran ve 780GB boyutundaki veriyi işleyen hacker grubu, EA Games'in kullandığı şirket içi özel hesaplara giriş yapmayı başarmış ve oyun motoru ile oyunlarda kullanılan kaynak kodlarına erişmiş. EA Games'i bu kodları internete ve rakiplerine vermekle tehdit eden hacker grubu, şantajları karşılığında büyük bir para istemiş.

Özetlemek gerekirse çok faktörlü doğrulama yöntemini kullanmak çoğu kötü niyetli hacker için caydırıcı niteliktedir. Fakat tamamen güvenlidir dememiz yanlış olur. Dünyaca ünlü yazılım şirketlerinden destek alan büyük şirketlerin bile bu tarz saldırılara maruz kaldığını duyuyoruz. Hâl böyleyken çok faktörlü doğrulama yöntemi ne yaptığını bilen bir hacker için atlatılmayacak bir yöntem değildir.

Büyük ve bilinen siber güvenlik şirketlerinden biri bu konu hakkında bir rapor yayımladı. Rapordaki bilgilere göre hackerlardan korunmak için yapılabilecek en iyi yöntemlerden biri düzenli olarak çerezleri temizlemek. Böylelikle sürekli olarak tutulan önemli bilgilerin dışarıya erişimi engellenebiliyor ve hesap güvenliğiniz sağlanabiliyor. Bütün bu anlatılanları ele aldığımızda diyebiliriz ki kişisel verilerinizin güvenliğine önem veriyorsanız çok faktörlü doğrulamayı imkânlar dâhilinde her yerde kullanmalısınız.

KAYNAKÇA

<https://www.pwfactor.com/makale/adan-zye-cok-faktorlu-kimlik-dogrulama/>

<https://securifyid.com/2021/03/05/cok-faktorlu-kimlik-dogrulama-mfa-nedir-2/>

https://www.tamindir.com/haber/hackerlar-cerezleri-kullaniyor_75595/

<https://www.siber.care/blog/10-soruda-cisco-nasil-hacklendi>

<https://siberbulten.com/siber-guvenlik/cisco-nasil-hacklendi-nasil-aksiyon-aldi/>

<https://www.webtekno.com/uber-hacklendi-iste-saldirinin-detaylari-h127970.html>

https://www.cenuta.com/blog/active-directory-nedir-ne-ise-yarar-ve-nasil-kullanilir-active-directory-kurulumu-ve-kullanimi/#Active_Directory_Nedir

İKRA MELİS AYGEN

KONU
11



İNTERNETTE GÜVENLİ ALİŞVERİŞ İÇİN İPUÇLARI

Birçok avantaja sahip olması nedeniyle günümüzde sıklıkla tercih edilen online alışverişler, veri güvenliği ve dolandırıcılık gibi sorunları ortaya çıkarmıştır.

Yapılan araştırmalara göre 2022'nin ilk yarısında Türkiye'de çeşitli kurumlara yapılan 388 bin 497 finansal saldırı tespit edildi. Saldırıya uğrayanlar arasında %57'lik oranla ödeme sistemleri en önde yer alırken bunu %24 ile e-ticaret siteleri ve %19 ile bankalar izledi.

Hem hızlı hem güvenli bir şekilde internetten alışveriş yapabilmek için siber saldırganlara karşı alabileceğiniz önlemleri sizin için derledik.



Öncelikle bilinen web sitelerinden alışveriş yapın. Alışveriş yaptığınız internet sitesinin adresinin muhakkak <https://> ile başlamasına ve SSL sertifikasına sahip olmasına dikkat edin. Bu sistem kartların başkaları tarafından kopyalanmasını engeller.



İnternette alışveriş yaparken dikkat edebileceğiniz bir husus da ürünleri çeşitli sitelerden araştırmaktır. Eğer ürün hakkında yapılan yorumların çoğu olumsuzsa ve şikâyetler fazlaysa alışveriş kararınızı tekrar gözden geçirmelisiniz. Ayrıca satıcının adres ve telefon bilgisini öğrenmek de oldukça önemlidir. İletişim kanallarını kontrol etmezseniz alışverişinizi sorunsuz yapmış olsanız bile alışveriş sonrasında çıkabilecek bir sorunda yetkili birine ulaşmanız mümkün olmayabilir.



Birçok kişinin ertelediği yazılım güncellemeleri de güvenliğinizi sağlamak için kullanabileceğiniz yöntemlerden biridir. Bu güncellemeler yazılımcılar tarafından mevcut hataları gidermek ve sürekli olarak geliştirilmekte olan saldırılara karşı önlem almak için yayımlanır. Bunları yüklemek sizi sanal ortamda daha güvenli hâle getirecektir.



Birden fazla bilgisayarınız varsa bir tanesini sadece online alışveriş ve internet bankacılığı için kullanabilirsiniz. Bu bilgisayar ile internette gezinme, dosya indirme, mailleri kontrol etme, sosyal medyada vakit geçirme gibi etkinlikleri yapılarak bir çeşit izolasyon sağlayabilirsiniz çeşitli saldırılardan uzaklaşmış olursunuz. Bunu yapamıyorsanız sadece bu tür işlemler için kullanacağınız bir e-mail adresi de faydalı olacaktır.



Herkesin kullanımına açık olan wifi ağlarını bankacılık işlemleri ve online alışveriş için kullanmamalısınız.

Çünkü kafe, alışveriş merkezi, toplu taşıma araçları gibi yerlerde ortak kullanılan internet ağları oldukça güvensizdir. Verilerinizi kullanarak girdiğiniz bütün siteler, başkaları tarafından kolaylıkla izlenebilir ve saldırganlar bu şekilde bilgilerinizi kolaylıkla ele geçirebilirler.



Güçlü şifreler kullanmak her zaman güvende kalmanızı sağlar. Basit şifreler kolaylıkla kırılabilir, özellikle sizinle bağlantılı isim-soy isim, doğum tarihi gibi bilgiler siber saldırganlar için bulunmaz nimettir. Bu nedenle her hesabınız için farklı bir parola kullanmaya ve şifrenizin küçük-büyük harf, rakam, mümkünse özel karakter içermesine dikkat edin.



Satın alma işleminizi tamamlarken satıcıların yasal olarak ne tür verilere ihtiyaç duydukları hakkında bilgi sahibi olmalısınız. Bir web sitesi sizden adınızı, iletişim bilgilerinizi ve fatura bilgilerinizi ister. Bazı kişiler pazarlama amacıyla ek bilgiler isteyebilir ancak bu zorunlu değildir. Hiçbir web sitesi size bir şey satmak için kimlik numaranızı istemez. Unutmayın ne kadar çok bilgi verirseniz saldırganlar için o kadar erişilebilir hâle gelirsiniz.

Ödeme Yöntemlerinde Dikkat Edilmesi Gerekenler

Kullanıcılar bir web sitesinden alışveriş yaparken ödeme ekranına geldiklerinde çoğu zaman kendilerine sunulan ödeme alternatiflerini dikkate almazlar. Hâlbuki internetten yaptığımız alışverişlerde ödediğimiz para satıcıya aktarılırken kullanabileceğimiz birçok farklı ödeme yöntemi mevcuttur. Güvenli ödeme yöntemi güvenli alışveriş yapmanın ilk kuralıdır.



İnternet alışverişlerinde kullanılan sanal POS uygulaması tüm güvenilir firmalar tarafından tercih edilir. Alışveriş yapılan internet sitesinde online ödeme özelliğinin varlığını kontrol etmelisiniz. Kapıda ödeme seçeneği genellikle bankalarla iş birliği bulunmayan şirketler tarafından kullanılır.

Sahte ve yanlış ürün gönderimi riski taşıyan bu yöntemi seçerken dikkatli olmalısınız.



Genellikle kredi/banka kartı bilgilerini girmek istemeyen kullanıcıların tercih ettiği havale-EFT yöntemi, en güvenli ödeme seçeneklerinden biridir. Çünkü tüm işlemlerin kullanıcı tarafından onaylanması gerekir, bu da alışveriş deneyimini çok daha uzun ve yavaş hâle getirir. Yine de bu yöntemi tercih ederseniz gerekli tutarı doğru ad-soyad ve hesap numarasına gönderdiğinizden emin olmalı ve işlem dekontunu saklamalısınız.



3D-Secure sistemini bulunduran siteleri kullanın.

Bu güvenlik sistemi kredi kartı ödemelerinde sıklıkla kullanılır. Bu yöntem sayesinde kartınızdan para çekilmeden önce telefonunuza bankanız tarafından bir onay şifresi gönderilir. Bu sayede telefonunuza gelen şifre girilmeden, sizin onayınız dışında yapılabilecek bir alışverişini önlemiş olursunuz.





İnternette alışveriş yaparken çok yüksek limiti olan bir kredi kartını kullanmak yerine sanal kart kullanın.

Bankanızın uygulamasına girerek limitini ve kullanım süresini belirleyebileceğiniz sanal kartları kolaylıkla oluşturabilirsiniz.

Bu yöntemde tıpkı kredi kartı gibi bir numaranız olur, alışveriş yapacağınız zaman sadece yeterli tutarı karta gönderirsiniz ve böylece kredi kartınızın kopyalanma riskini engellemiş olursunuz.

Bu yöntemleri uygulayarak kişisel bilgilerinizi koruyabilir, kötü amaçlı saldırıların önüne geçebilirsiniz. Güvenli ve keyifli alışverişler dileriz.

KAYNAKÇA

<https://berqnet.com/blog/internetten-guvenli-alisveris-nasil-yapilir>
<https://www.safewise.com/blog/10-cybersecurity-tips-for-online-shopping/>
<https://nordvpn-com.translate.goog/blog/how-to-shop-safely-online/>
<https://www.hepsiburada.com/hayatburada/internetten-guvenli-alisveris-nasil-yapilir/>
<https://www.cybermagonline.com/turkiye039deki-finansal-siber-tehditler-2022039nin-ikinci-ceyreginde-11-artti>
<https://www.iyzico.com/blog/internetten-alisveriste-odeme-yontemleri/>
<https://www.akarsuglobal.com/blog/%C4%B0nternetten-G%C3%BCvenli-Alisveris>

KEVSER KAHRAMAN

KONU
12





UZAKTAN ÇALIŞMANIN GETİRDİĞİ RİSKLER VE TEDBİRLER

Güvenli Olmayan Ağlar

Uzaktan çalışmanın getirdiği en büyük risk faktörlerinden biri çalışanların kullandığı wi-fi ağlarının yeterince güvenli olmamasıdır. Saldırganlar tarafından daha kolay bulunabilen ve daha basit bir şekilde erişim sağlanan kamusal alanlardaki ücretsiz wi-fi ağları, kötü niyetli kimselerin en çok bulunduğu alanlardandır. Ücretsiz wi-fi ağları ile saldırırganlar, ağ içinde aktarılan verileri izleyebilir hatta ele geçirebilir. Bu ağlarla saldırırganlar hem kullanıcıların hem de kuruluşların gizli bilgilerine erişebilir.

Bunun yanı sıra evlerde kullanılan wi-fi ağları da ne yazık ki şirket ağları kadar güçlü ve güvenlik duvarına sahip olmadığı için saldırılara daha açık bir konumdadır. Kullanılan diğer donanım parçaları gibi yönlendiricilerin de bakımı ve güncellemesi yapılmalıdır. Aksi hâlde saldırırganların faydalanabileceği ve zaman içinde kurumsal veri ihlallerine yol açabilecek güvenlik açıklarına sahip olacaktır.



KİMLİK AVI DOLANDIRICILIĞI

Uzaktan çalışanlara yönelik en büyük siber tehditlerden biri de kimlik avı dolandırıcılığıdır. Bir çalışan e-posta hesabına gelen güvenli gibi görünen kötü niyetli bir bağlantıya tıkladığında zararlı bir yazılımla siber saldırganların bilgilerine ulaşmasına sebep olur. Bu durumda saldırganlar şirketin bir çalışanı gibi önemli ve hassas bilgilere erişebilir.

GÜVENSİZ PAROLALAR

12345678

PxH1#n!8

Siber saldırganlar için gelişmiş bir güvenlik duvarını aşmaktansa zayıf parolalara erişmek daha tercih edilir. Bu nedenle hassas şirket bilgilerine erişmek için hesap parolalarını kırmaya çalışırlar. Siber suçlular şifreleri kırmak için çeşitli yöntemler kullanır. Bunlardan bir tanesi yaygın kullanılan parola listelerini denemektir. Bu parolalarla kolayca hesaba erişim sağlayabilirler. Bu nedenle hesaplara erişimlerin iki kademeli kimlik doğrulaması yoluyla korunması gerekmektedir. Çalışanların parolalarıyla giriş yaptıktan sonra SMS, arama gibi yöntemler ile iletilecek olan tek kullanımlık şifreyle giriş yapması parolanın güvenliğini sağlamak için önemli bir yoldur. Bunun yanında bir parolanın birden fazla platform için kullanılması şifrenin kırılması hâlinde birden fazla hesaba erişim olanağı sağlayacağı için tercih edilmemelidir. Çalışanların parolalarını akıllı telefonlardaki dijital notlar gibi güvenli olmayan yerlerde saklaması, parolalarda kişisel bilgilerini kullanması şirketin tüm kurumsal ağını riske atmaktadır.

BİLGİSAYAR PAYLAŞIMI

Bilgisayar paylaşımı bazı durumlarda siber saldırılara neden olabilir.

Eğer bilgisayar paylaşımı yapılıyorsa kullanan her kullanıcının erişimi için farklı şifreleme yapılmalıdır. Riskleri en aza indirmek için güncel anti-virüs yazılımları ile cihazların korunmasına dikkat edilmelidir.

Bu önlemler sağlanmadığı takdirde kötü amaçlı yazılımların şirket ağlarına taşınma riski vardır.

GÜVENLİ OLMAYAN CİHAZLAR

Uzaktan çalışanlar çalışırken şirket ağına erişmek için genellikle kişisel cihazlarını kullanırlar. Kişisel cihazlar genelde kurumsal cihazlar kadar güvenli değildir. Çalışanlar e-posta filtreleme, güvenlik duvarları ve şifreleme gibi güvenlik özelliklerini kullanmadığı takdirde kurumsal güvenlik ekiplerinin neler olup bittiğine dair denetimi olmayacaktır. Bu ekstra güvenlik önlemleri olmadan kurumsal ağlar, kişisel cihazları giriş alanı olarak kullanabilecek siber suçlulara karşı risk altında olacaktır.

Kişisel bilgisayarınızdan giriş yaptığınız herhangi bir web sitede saniyeler içerisinde açılıp kapanan belki de dikkatinizi çekmeyecek pop-up ekranlarının açılması, arka planda bilgisayarınıza zararlı yazılım yükleyebilir. Cep telefonunuzdan sosyal medya araçlarını kullanarak giriş yapmanız da bilgi güvenliği yönünden risk taşımaktadır. Buna ek olarak, kişisel bir cep telefonunda çalışma yapıldığında (telefon görüşmeleri ve iş hesaplarında oturum açma gibi) telefon şifrelenmediği sürece saldırganlar tarafından bu verilere erişilebilme riski vardır.

Siber suçlular arasında popüler olan bir diğer cihaz da yazıcılardır. Günümüzdeki wi-fi yazıcıları, yazdırmayı kolaylaştıran ve saldırganların faydalanabileceği ciddi güvenlik sorunlarına açık birçok özelliğe sahiptir.

Uzaktan çalışanlar kişisel yazıcılardan iş belgelerini yazdırdıklarında genelde şirkette yaptıkları gibi güvenli parçalama hizmetlerine erişimleri olmaz. Herhangi bir belgeyi yazdırmak, kurumsal bilgileri daha fazla riske sokar.



NETWORK GÜVENLİĞİNİN SAĞLANMASI

Öncelikle şirketlerin network altyapılarının iyi tasarlanmış olması gerekmektedir.

Güvenlik duvarlarında gerekli kurallar oluşturularak sisteme zarar verilmesinin etkisi azaltılabilir. Özellikle güvenlik duvarlarında "rate limiting" (hız sınırlaması) özelliğın kullanılması ve belirli bir IP adresinden gelecek olan maksimum paket sayısının (sınır) belirlenerek sınırı aşan IP adreslerinin engellenmesi sağlanabilir. Donanımlı ve tecrübeli BT uzmanları tarafından internet trafiğinin 7/24 izlenmesi gerekmektedir.



ŞİFRE BELİRLEME KRİTERLERİ

Çalışanların hesaplarında güçlü şifreler kullanması olası bir insan faktöründen kaynaklı siber saldırıların önüne geçebilmektedir. Bu yüzden çalışanların güçlü şifre tercih etmesi önerilir. Tahmin edilmesi ve deneme yanılma metodu ile ele geçirilmesi oldukça zor olan şifreler güçlü şifre olarak adlandırılır.

Oluşturulan bir şifrenin kırılmasının güç olabilmesi için en azından küçük, büyük harf ve rakam gibi 3 farklı tipte karakterden oluşturulması gerekir. Mümkünse özel karakter de içeren şifreler kullanılması şifrenizin kırılmasını güçleştirir. Güvenliğiniz için şifrelerinizi belirli aralıklarla değiştirmelisiniz. Şifreleriniz ne kadar uzun ve karmaşıksa bu o kadar güvendesiniz demektir.



GÜÇLÜ BİR ŞİFRE OLUŞTURURKEN

- **Uzun bir şifre belirleyin:** Sistemin izin verdiği ölçüde maksimum uzunlukta bir şifre oluşturun.
- Şifrenizde özel karakterlere yer verin: Sadece sayı ve harf kullanmak yerine %, ?, \$, & gibi farklı karakterler kullanmayı tercih edin.
- **Şifrenizi sadece rakam veya harflerden oluşturmayın:** Etkili bir şifre oluştururken sadece rakamları kullanmayın. Örneğin ‘0123456789’ şifresi kolayca tahmin edilebilir duruyor. Tıpkı rakamlar gibi “asdfghjk” gibi bir şifre de kolayca kırılabilir. Harf ve rakamları birlikte kullanmanız şifrenizi daha etkili ve tahmin edilemez hâle getirir. Bu adımda şifrenizi daha güvenli yapmak için ayrıca büyük ve küçük harfleri kullanmayı tercih edebilirsiniz.
- Kişiyi özgü tanımlayıcı terimler kullanmayın: Adınız, soyadınız, doğum tarihiniz gibi kişisel bilgilerinizi kullanmaktan kaçının.
- **Yaygın kelime ve söz öbeklerinden sakının:** ‘şifre’, ‘123456’ gibi yaygın ifadeleri tercih etmeyin.
- Şifrenizi asla paylaşmayın veya kaydetmeyin: Herkesin kullandığı bilgisayarlarda şifrenizi asla kaydetmeyin veya “beni hatırla” kutucuğunu işaretlemeyin. Kişisel cihazınızı kullanmıyorsanız kişisel hesaplarınıza giriş yapmaktan kaçının.
- **Şifrenizi düzenli olarak değiştirin:** Şifreler kalitelerini zamanla kaybeder, çünkü şifrenizi ne kadar uzun süre kullanırsanız hackerların kırmaya çalışması için o kadar zamanı olur. Şifrenizi düzenli olarak değiştirmek, siber suçluların hep bir adım önünde olmanızı sağlar.



VPN GİZLİLİĞİNİN KORUNMASI

VPN ile bir internet bağlantısı oluşturduğunuzda verileriniz şifrelenir ve ulaşmak isteyen kötü niyetli kişilerden de doğal olarak sizin bilgilerinize erişimi olan internet sağlayıcınızdan da gizlenir. Kullandığımız arama motorları başta olmak üzere gün içerisinde ziyaret ettiğimiz birçok site, çerezler aracılığı ile erişim bilgilerimizi, IP adresimizi, lokasyonumuzu ve internetteki davranışlarımızı kaydeder ve depolar. Facebook, Google, Microsoft gibi firmaların platformları ise zaten bizim tüketici davranışlarımızı, arama alışkanlıklarımızı ve kişisel bilgilerimizi kaydederek, saklayarak ve analiz ederek varlığını sürdürmektedir. VPN kullanarak verileri gizleme imkanına erişebilirsiniz.

Şirketler, çalışanların kurumsal kaynaklara uzaktan bağlanmaları durumunda güvenli bir kanal kurmak ve kurumsal verileri dışarıdan istenmeyen erişime karşı korumak için güvenilir bir VPN kurmalı ve aynı zamanda VPN olmadan harici ağlardan kurumsal kaynaklara olan bağlantıları yasaklamalıdır.



ANTI-VİRÜS YAZILIMLARININ ÖNEMİ

Bilgi güvenliğinin büyük önem taşıdığı bu dönemde firmalar ve kurumlar da güvenlik alanında büyük yatırımlar yapmaya başladı. Bu durumla paralel olarak zararlı yazılımlar ve bilgi korsanlığının önüne geçmek adına, anti-virüs firmaları da büyük bir ivme ile yükselişe geçti. Hiç beklenmeyen olası bir siber saldırının veya bilgi hırsızlığının önüne geçmek için anti-virüs programları büyük önem arz ediyor.

KAYNAKÇA

<https://www.redcentricplc.com/network-security/top-5-security-concerns-of-remote-working/>
<https://denetik.com/uzaktan-calismada-siber-guvenlik-acisindan-ilk-5-risk-nedir/>
<https://www.softwareone.com/tr-tr/blog/articles/2020/10/26/uzaktan-calismanin-getirilmesi-guvenlik-risklerini-nasil-azaltabiliriz>
<https://andysto.com/what-are-the-most-common-remote-work-security-risks/#:~:text=The%20risk%20of%20physical%20theft,can%20be%20accessed%20by%20cybercriminals.>
<https://gaissecurity.com/blog/uzaktan-calisma-modellerinde-siber-guvenlik-riskleri/>
<https://blog.lexpera.com.tr/uzaktan-calisma-modeli-riskleri-ve-dikkat-edilmesi-gereken-hususlar-hakkinda/>
<https://it.bilgi.edu.tr/tr/guvenlik/sifre/>
<https://tr.godaddy.com/blog/guclu-sifre-olusturmak-icin-10-yontem/>
<https://webmasto.com/vpn-kullanmanin-faydalari-5-onemli-sebep>
<https://www.karel.com.tr/blog/kurumsal-bilgi-guvenligi-icin-anti-viruslerin-onemi>





SOSYAL MÜHENDİSLİK

Siber saldırganlarla ilgili en yaygın yanılgı, insanların bilgisayarlarını veya hesaplarını ele geçirmek için son derece gelişmiş araçlar ve teknikler kullandıklarıdır. Tabii ki son derece gelişmiş araçlar ve teknolojiler kullanarak da büyük zararlar verebilirler fakat siber saldırganlar için bilgilerinizi çalmanın, hesaplarınızı ele geçirmenin veya sistemlerinize kötü niyetli yazılımlar bulaştırmanın en kolay yolunun, sosyal mühendislik yöntemlerini kullanmak olduğunu söyleyebiliriz.

Sosyal mühendislik nedir ve siber saldırılardan nasıl korunabiliriz?

Bilgi güvenliği bağlamında sosyal mühendislik, eylemleri gerçekleştirmek veya gizli bilgileri ifşa etmek için insanları psikolojik olarak manipüle etmektir. İnsan, her zaman güvenlik zincirinin en zayıf halkası olarak bilinir çünkü çoğu zaman duygularıyla hareket ederler.

En basit tanımıyla sosyal mühendislik; bilgilerinize ulaşmak, hesaplarınızı ele geçirmek veya sistemlerinize zararlı yazılımlar bulaştırmak isteyen kişilerin sizi çeşitli yöntemlerle kandırarak ve güveninizi kazanarak bunları elde etmesidir. Bu alanda uzman olan Kevin Mitnick'in deyişiyle bir aldatma sanatıdır. Sosyal mühendislik, bir insanın aklını veya mantığını perdeleyerek kalbine hitap etmektir. Bir insanın hislerine hitap edebilirsiniz ona istediğiniz her şeyi yaptırabilirsiniz. Bu yöntemin kötü amaçlar için kullanılmasına ise sosyal mühendislik denir. Genelde insanların zayıflıklarından, korkularından, sevgilerinden kısacası duygularından faydalanırlar. Kullanıcıları hassas bilgileri ifşa etmeleri için kandırmak, siber güvenlik dünyasında yeni bir şey değildir. Değişen tek şey ise saldırı yöntemidir. Bilgi edinmek için kullanılan hikâyeler ve oltalama gibi diğer tehditleri içeren organize gruplardan gelen karmaşık saldırılar yeni saldırı yöntemlerindendir.

Sosyal mühendislik terimi ilk kez 1894'te Hollandalı sanayici JC Van Marken tarafından kullanılmış ancak 1990'lardan beri bir siber saldırı yöntemi olmuştur.

Sosyal mühendisliği günlük yaşantımızdan bir örnekle açıklamak istiyorum. Çocuklar genelde ıspanak yemeyi sevmezler. Anneleri yemeleri için bir tabak ıspanak koyduğunda ve yemelerini söylediğinde muhtemelen yemeyeceklerdir. Ancak anneleri tabaktaki yemeğin babalarının en sevdiği yemek olduğunu, birazdan gelip yiyeceğini ve onu yememesi gerektiğini söylerse çocuk ıspanağın çok lezzetli bir yemek olduğunu düşünecek ve muhtemelen yemek isteyecektir. Sosyal mühendislik de aslında tam olarak bu mantığı temel almaktadır.

İki tip sosyal mühendislik saldırısı vardır: Bireysel ve şirket bazlı. Bireysel olanlarda kişiye yönelik bilgi edinme, kandırma, sosyal medya hesabını ele geçirme, kredi kartı numarasını öğrenme gibi olaylar hâkimken şirket bazlı olanda şirket personellerini çeşitli yöntemlerle kandırarak şirketteki bilgilerin ele geçirilmesi hedeflenir.

Sosyal mühendislik saldırılarında önce bir kurban seçilir. Daha sonra kurban hakkında detaylı bilgi toplanır. Zaafları ve karakteristik özellikleri öğrenilerek belli bir saldırı profili oluşturulur.

Sosyal mühendislikte en yaygın kullanılan saldırı yöntemlerinden biri oltama yani phishing saldırıdır. Phishing saldırılarında e-posta kullanılarak bilgisayarlara, telefonlara virüs gibi zararlı yazılımlar bulaştırılmaya çalışılır. İnandırıcı olması adına genellikle kullanıcının bankasından veya bilinen web sitelerinden gönderilmiş gibi e-posta yollar. Genellikle kullanıcının e-postada yer alan sahte bağlantılara tıklaması hedeflenerek kredi kartı, şifre gibi bilgilerine ulaşılmaya çalışılır. E-postayla virüs içeren bir dosya gönderilerek de kullanıcıların sistemlerine zararlı yazılımlar bulaştırmak amaçlanır.

Kısa mesaj ya da son dönemlerde yaşandığı gibi sosyal medya uygulamalarındaki direkt mesajlar kullanılarak yapılan sosyal mühendislik saldırıları ise mesaj oltalama saldırıları (smishing) olarak adlandırılır. Size kendi yaşadığım bir mesaj oltalama saldırısını anlatmak istiyorum. Bir gün yakın bir arkadaşım bir sosyal medya uygulamasından direkt mesaj attı. Buraya kadar her şey normaldi, nasıl olduğumu soran bir mesajdı ve cevap verdim. Biraz konuşmaya devam ettikten sonra benden telefon numaramı istedi. Ben de yakın arkadaş olduğumuz için şaşırarak benim telefon numaramın onda zaten olduğunu söyledim. Yeni bir hat aldığını ve bütün numaraların silindiğini söyledi. Bu cümleden sonra inanıp inanmamak sizin elinizde. Ben inanmadım ve o arkadaşıma telefon numarası üzerinden mesaj attım. Hesabının çalındığını ve mesaj atan kişinin o olmadığını öğrendim. Daha sonra ise ortak bir arkadaşımız beni aradı ve dolandırıldığını anlattı. Siber saldırganın telefon numarasını mesaj atmış ve daha sonra söylediği gibi gelen mesajı onaylamış. Ne yazık ki hesabından bir miktar para çekilmiş ve mesajı onaylayan kendisi olduğu için dolandırıldığını ispat ederek parayı geri alması da mümkün olamadı.

Teknoloji ilerledikçe siber saldırılar da artıyor. Sosyal mühendislik saldırıları da diğer saldırılara göre daha kolay olduğu için siber saldırganlar tarafından sıklıkla tercih ediliyor. Uyanık olarak, kanıt isteyerek ve telefon numarası, kredi kartı numarası vs. istendiğinde şüphelenip atmayarak sosyal mühendislik saldırılarından korunabilirsiniz.

Sosyal mühendislikte yeni bir devri başlatan çok gerçekçi yapay seslerin oluşturulabildiği platformlar var. Kendi sesinizi o platformlardan birine tanımlayıp sonra birine telefondan dinlettiğinizi düşünün. Siz aslında başka bir yerde başka şeyler konuşurken aradığınız kişi sizin onunla konuştuğunuzu zannedecektir. Kulağa ne kadar da korkunç geliyor değil mi? Sizden mesajla kredi kartı numaranızı isteyen

bir arkadaşınızı teyit için aradığınızı ve telefonda da aynı cümleyi söylediğini hayal edin. Hiçbiriniz bunun oluşturulmuş yapay bir ses olduğunu düşünmeyecek ve o arkadaşınıza inanarak kredi kartı numaranızı göndereceksiniz. Sonucunda ise kartınızdan çekilen paralar ve dolandırıldığınız gerçeğiyle yüzleşmek zorunda kalacaksınız. Çok ürkütücü değil mi?

Bu tür dolandırıcılıklar için kullanılan “vishing” terimi “ses dolandırıcılığı” anlamına gelen “voice phishing” kelimelerinden oluşuyor.

Daha önce yaşanmış ve şirketi büyük bir zarara uğratmış bir vishing saldırısından bahsetmek istiyorum. Dolandırıcılar, piyasada satılan ve ses üreten bir yapay zekâ yazılımını kullanarak Alman şirket patronunun sesini taklit ettiler. Zanlılar, para transferi masraflarının hemen karşılanacağı sözünü vererek Alman şirketin sahip olduğu Birleşik Krallık merkezli bir enerji firmasının baş yöneticisini, parayı bir saat içinde acilen Macar tedarikçiye göndermesi için kandırdılar. Patronunun her zamanki hafif Alman aksanını duyan firma yöneticisinin hiçbir şeyden şüphelenmediği ifade edildi. Dolandırıcılar, para transfer masraflarını karşılamadıkları gibi Alman patronun sesini yeniden kullanarak İngiliz firma yöneticisinden ikinci kez acil para transferi yapmasını istediler. İngiliz firma yöneticisi bu sefer ödemeyi yapmayı reddetti. Diğer bir taraftan firma yöneticisinin Macaristan’a gönderdiği para Meksika’ya ve dünyanın başka yerlerine aktarıldı. Yetkili makamlar bu bilişim suçunu işleyenleri henüz saptayabilmiş değil.

Bu aralar haberlerde en çok duyduğumuz sosyal mühendislik çeşitlerinden biri de siber saldırganların telefonla arayıp polis taklidi yaparak seçtikleri kurbanın kredi kartı bilgilerini elde etmeye çalışmalarıdır. Hırsızlar banka hesabınızdan bir miktar para çalmış gibi türlü bahanelerle insanları kandırmaya çalışıyorlar. Ne yazık ki bilinçsiz kullanıcılar siber saldırganların polis olduğuna inanıyor ve istedikleri bilgileri onlara veriyorlar. Bazı filmlerde de yer aldığı gibi bunu daha ileriye taşıyan siber saldırganlar da var. Bir adres vererek istedikleri kadar parayı banka hesaplarından çekmelerini ve o adrese götürmelerini istiyorlar. Tabii ki bundan kimsenin haberi olmasın diye de tehdit ediyorlar. Onlar da biliyor ki kurban bunu birilerine anlattığında siber farkındalığı olan biri çıkacak ve arayanların dolandırıcı olduğunu söyleyecektir. Bu gibi sosyal mühendislik saldırılarından korunabilmek için telefonda kendini polis memuru vb. gibi tanıtan kimseye itibar etmemelisiniz.

Sosyal Mühendislik Saldırılarından Nasıl Korunabiliriz?

Sosyal mühendisliğin ne olduğundan, çeşitlerinden ve yaşanmış gerçek örneklerinden bahsettim. Son olarak bu saldırılardan korunmak ve kurban olmamak için yapabileceklerinize bakalım.

Hiçbir zaman kimseye tam güvenmeyin. Bir şeyin doğruluğundan şüphe ederse-
niz araştırmadan harekete geçmeyin. E-postanıza gelen maillerdeki linklere emin
olmadan tıklamayın ve istenen bilgi alanlarını doldurmayın. Yine mail yoluyla ge-
len dosyalara tıklamadan önce dikkatli olun. Arkadaşınız, yakınınız, akrabanız gibi
davranıp sizden kişisel bilgilerinizi isteyen kişilere kanıt olmadan inanmayın ve iste-
dikleri bilgileri göndermeyin. Telefonda polis savcı gibi davranıp sizden para veya
kredi kartı bilgilerinizi isteyen kişilere bunları vermeyin.

Paranoyak olmanıza gerek yok fakat her şeye ve herkese de hemen kanmamalı
ve şüpheli yaklaşmasını da bilmelisiniz. Unutmayın, sağduyu çoğunlukla en iyi
savunmanızdır.

KAYNAKÇA

<https://www.sans.org/newsletters/ouch/social-engineering-attacks/>

<https://www.proofpoint.com/uk/threat-reference/social-engineering>

<https://teyit.org/ses-dolandiriciligi-243-bin-dolara-mal-oldu>

<https://www.silicon.co.uk/workspace/how-to-explain-social-engineering-to-a-five-year-old-172740>



MİHRİMAH GÖKNAR & MERVE ACAR

**KONU
14**

FİDYE YAZILIMLARI

Fidye Yazılım Nedir?

Pek çoğumuz Yeşilçam filmlerinde ve günümüzde de pek çok filme konu olan; el konulan önemli bir şey için mağdur taraftan para istenmesi olarak bilinen fidye olayına en az bir kere denk gelmişizdir. Peki bu olay bilgisayar dünyasında ne anlama gelmektedir?

Fidye yazılım, bir bilgisayar ya da bilgisayar ağına zarar vermek için tasarlanmış kötü amaçlı yazılımların alt kategorilerinden biridir. Siber güvenlik alanında “ransomware” adıyla anılmaktadır. Kişi veya kurumların cihazlarındaki dosyalara erişimi kısıtlamak bu dosyalara bağlı sistemleri kullanılamaz hâle getirmek için oluşturulmuş, sürekli kendini geliştirmekte olan kötü amaçlı bir yazılım biçimidir. Saldırganlar kullanıcıların sistemlerine tekrar ulaşabilmeleri için ödeme talep etmektedir. Eğer ödeme gerçekleşmezse sızdırılmış verileri veya kimlik doğrulama bilgilerini farklı kişi veya kurumlara satmakla ya da sızdırmakla tehdit etmektedirler.

Günlük hayatımızdan örnek vermek gerekirse telefonumuza kötü niyetli kişiler tarafından gönderilen linklere tıkladığımızda kişisel bilgilerimize erişimin kapısını açmış oluruz ve bu şekilde bilgilerimizi paylaşma konusunda tehditlere maruz kalabiliriz.

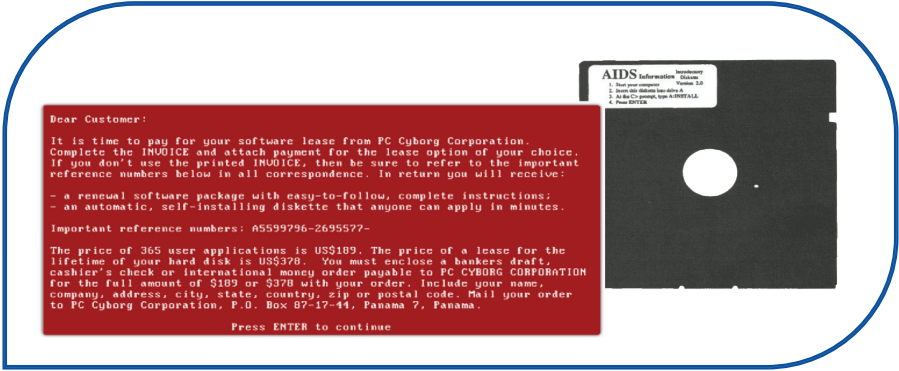


Fidye Yazılıma Genel Bakış

Fidye yazılım son zamanlarda gündeme gelmiş olsa da temeli 1980'li yıllara dayanmaktadır.

1989: İlk Fidye Yazılımı (AIDS Bilgi Diski Truva Atı)

İlk fidye yazılımı 1989 yılında bir biyolog olan Dr. Joseph Popp tarafından geliştirildi. Yazılım ilk olarak bir disket yardımıyla manuel olarak dağıtıldı. Bu disketi kullanan kullanıcıların verileri de kötü amaçlı yazılımla birlikte kaydedildi ve her kullanıcı bir kurban hâline geldi. Kullanıcılar yeni bilgisayarlara da bu disketi taktığında yazılım birçok makineye sızdı ve bulaşma hızı giderek arttı. Belirli sayıda sistem önyüklemesinden sonra artık yazılım etkinleşti. Dosyaları şifreleyerek sistemi kullanılamaz hâle getirdi. Ve sistemi düzeltmek için Panama'daki bir hesaba para gönderilmesi talep edildi.



2022: Günümüzde Siber Zorbalık

Artan ölçek ve veri sızıntıları sebebiyle fidye yazılımdan elde edilen gelirler gittikçe devasa rakamlara dönüşmektedir. Birçok kötü amaçlı yazılımın hızla gelişmesi sistemleri korumayı oldukça zorlaştırmaktadır. Geçmiş yıllarda üçlü gaspın öncülerinden biri olarak bilinen, günümüzde gelişmiş hâliyle saldırıları destekleyen SunCrypt varyantının yeni yetenekleri arasında işlem sonlandırma, hizmetleri durdurma ve fidye yazılımı yürütmek için makineyi temizleme yer alıyor. Bu gelişmeler sebebiyle artık kişi ve kurumların kendilerini koruması için ayrı bir finansal yatırım yapması gerekiyor.

Fidye Yazılım Türleri

Kitleyiciler (Locker) Fidye Yazılımları: Kitleyici sistemin asıl amacı kullanıcıyı korkutarak ödeme yapmasını sağlamaktır. Kullanıcının sistemine bulaşarak çeşitli fonksiyonları geçici veya kalıcı olarak kullanıma kapatabilmektedir. Örneğin bulaşan yazılımın amacına göre bazı fare fonksiyonlarını kısıtlayabilmekte veya klavye kullanımını tamamen sonlandırabilmektedir.



Şifreleyici (Crypto) Fidye Yazılımları: Şifreleyiciler eriştikleri sistemlerdeki dosya veya verileri farklı şifreleme sistemleri kullanarak şifreler, ardından kurbanlara dosyalarının şifrelendiğini bildirir ve işlevselliği tekrar kazanabilmeleri için fidye talep ederler.

Fidye Yazılımı Nasıl Bulaşır?

Kimlik Avı E-Postaları

Saldırganlar kişinin ilgi alanlarını tespit edebilmek için sosyal mühendislik yönteminden yararlanırlar. Bu yöntem sayesinde kişinin, ilgi alanına hitap eden, içerisinde kötü amaçlı bir dosya veya dosya ekini içeren bağlantıya tıklamasını sağlayarak kimlik avını gerçekleştirirler.

Uzak Masaüstü Protokolü (Rdp)

Saldırlardan korunmak için BT yöneticileri tarafından oluşturulmuş kullanıcının makinesini yapılandırma ve erişimi düzenleme gibi özellikleri kötü amaçları için kullanarak fidye yazılımı şifre işlemi başlatabilir veya makinenin tam kontrolünü ele geçirerek işlevselliği geri kazanabilmemiz için fidye ödenmesini talep ederler.

Güvenli Olmayan Sitelerden Yapılan İndirmeler

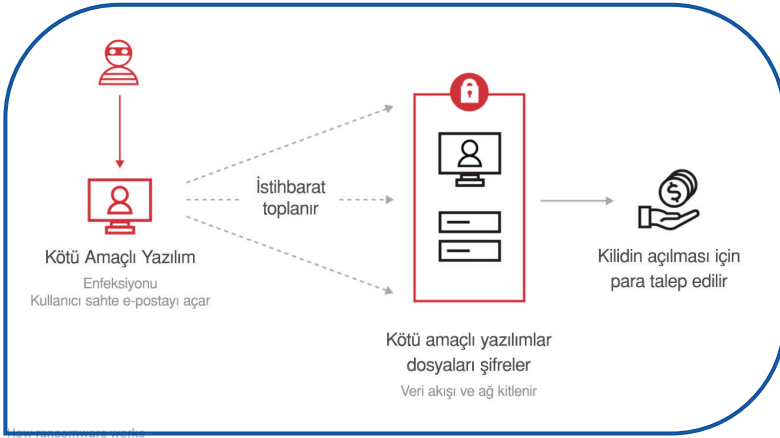
Bu tip siteleri ziyaret eden kişilerin indirdiği dosyaların içerisine yüklenmiş bulunan kötü amaçlı yazılımlar sayesinde bilgisayarda bulunan dosya ve veriler kullanıcıya tehdit unsuru oluşturur.

Usb Sürücüler

Fidye yazılımların sistemlere sızmak için kullandığı yollardan biridir. USB sürücüler, promosyon amaçlı uygulamalar gibi görünerek kullanıcının şüphelenmesini engeller. Kullanıcı anlayamadan bilgisayarına yerleştirilmiş fidye yazılımların açılmasına sebep olabilir.

Fidye Yazılım Sistemi Nasıl Çalışır?

Fidye yazılımının temel işlevi iki yönlüdür: Verileri şifrelemek ve fidye mesajını iletmek.



Yayıma Stratejileri

Fidye yazılımlarının yayımları genellikle ortalama saldırıları ile başlar. Bu tür saldırılarda kullanıcı; e-mail veya mesaj yoluyla gelen, ödül veya para vadeden, kaynağı bilinmeyen linklere tıklayarak fidye yazılımına maruz kalır.

Türüne göre bu yazılım: hemen veya sistemde belirsiz bir süre (kullanıcı fark etmeden) saklanıp istediği zaman çıkarak dosyaları şifreleyebilir, cihaz fonksiyonlarını engelleyip en basit işleri bile yapmanıza engel olabilir.

Ek olarak fidye yazılımları, Malware (kötü amaçlı yazılım), güvenilir olmayan kaynaklardan dosya indirilmesi ve hatta güvenliği ihmal edilmiş Wi-Fi ağıyla da bulaşabilir. Ayrıca saldırganlar bir sistemi fidye yazılımı ile ihlal etmek için kullanıcının haberi olmadan uzak masaüstü bağlantısı (Remote Desktop Protocol) kurarak, zararlı yazılım yükleyebilir.

Önleme Yöntemleri

Fidye yazılımlarına maruz kalmamak için:

- E-posta adresinizi herkesin erişebileceği web sitelerine vermekten kaçının.
- E-posta içeriğini kontrol edin, bilinmeyen kaynaktan gelen ekleri indirmeyin ve linklerin uzantısını kontrol etmeden tıklamayın.
- Güvenlik ikonu olan ve https bağlantılı  <https://> siteleri kullanın.
- Dosya ve sisteminizi düzenli bir şekilde yedekleyin. Bulut depolama üzerine yedeklemek kolay olsa da sabit disk gibi fiziksel bir depolama üzerine yedekleme yapmak her zaman tavsiye edilir.
- Sisteminizi, uygulamalarınızı en güncel güvenlik yamaları ile güncel tutmanız her zaman yararınıza olur ve güvenilir anti-virüs programları kullanmanız kesinlikle tavsiye edilir.

Fidye Yazılımlarından Nasıl Korunabiliriz?

- İlginizi çekse bile şüpheli görünen herhangi bir bağlantıya tıklamayın.
- Şüpheli olun ve kişisel bilgileriniz gerektiğinden fazla bir şekilde talep ediliyorsa asla paylaşmayın.
- Bilgisayar gibi verilerinizin bulunduğu teknolojik sistemlerinizde lisanslı ve güvenilir anti-virüs yazılımları kullanın.
- Verilerinizi güvenilir sistemlere belirli aralıklarla yedeklemeye özen gösterin.
- Tehlikeli web sitelerinin zararlarından korunmak için DNS filtrelemeleri kullanın.
- Sosyal mühendislik durumlarına karşı dikkatli olun.
- Bilgisayarlarınızda kullandığınız işletim sistemlerinin lisanslı ve güncel olduğundan emin olun.
- İşletme veya kurumosunuzdaki çalışanları bilinçlendirmek için belirli aralıklarla eğitimler düzenleyin.

KAYNAKÇA

Görsel1: <https://www.techinside.com/guncelleme-kiligindaki-fidye-yazilimi-fantom/>

Görsel2: https://cibertura.com/?p=720&et_blog

Görsel3: <https://jooinn.com/web-security-concept-with-digital-padlock.html>

<https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ransomware.pdf>

https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-insightidr-ransomware-playbook.pdf

<https://5harad.com/papers/ransomware.pdf>

<https://www.kaspersky.com.tr/blog/history-of-ransomware/9509/>

<https://tr.safetynetdetectives.com/blog/ransomware-statistics-tr/>

<https://floodlar.com/suncrypt-fidye-yazilimi-hala-hayatta-ve-2022de-tekmeliyor/>

<https://www.cozumpark.com/fidye-yazilimleri-nedir-nasil-korunulur/>

<https://berqnet.com/blog/fidye-yazilimi>

<http://w3.bilecik.edu.tr/bilgiislem/2016/02/08/kotu-amacli-fidye-yazilimleri-hakkinda/>

<https://www.618media.com/blog/fidye-yazilimi-nedir/>

Calder, A. (2021). The Ransomware Threat Landscape : Prepare For, Recognise and Survive Ransomware Attacks. ITgp.

Ransomware Nedir, Nasıl Çalışır? Ransomware Virüsünün Mail Yoluyla Bulaşmasını Engelleme » Uzman Posta. (2022, April 19). Uzman Posta. <https://uzmanposta.com/blog/ransomware/>

Bertia, S. B. Xavier, G. J. W. Kathrine and G. M. Palmer, "A Study about Detecting Ransomware by Using Different Algorithms," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 1293-1300, doi: 10.1109/ICAAIC53929.2022.9792587.





SIZMA TESTİ

Sızma Testi

Sızma testi, sistemin (Taşınabilir bilgisayarlar, masaüstü bilgisayarlar ve sunucu bilgisayarlar gibi) güvenliğini değerlendirmek üzere bir bilgisayar sistemi üzerinde gerçekleştirilen yetkilendirilmiş bir siber saldırıdır. Bir kuruluşun güvenlik açıklarını belirlemek için sistematik olarak gerçekleştirilen bir çalışmadır.

Başka bir deyişle bir saldırganın yararlanabileceği yerel ağ, internet ya da web uygulaması gibi olası saldırı yüzeylerinde bulunabilecek güvenlik açıklarını veya bir yazılım uygulamasındaki zayıflıkları (zafiyet) ve riskleri ortaya çıkaracak bir testtir. Bu testin genel amacı test edilen sistemin güvenlik açıklarını bulmaktır.

ÜÇ TÜR SIZMA TESTİ VARDIR

Blackbox ve whitebox sızma testleri, bilgisayar sistemlerinin ve yazılımlarının güvenlik açıklarını tespit etmek ve bu açıkları kapatmak için kullanılan önemli güvenlik testleridir. Her ikisi de siber güvenlik alanında oldukça önemlidir ancak farklı yaklaşımlar kullanırlar. Aşağıdaki gibi açıklayabiliriz:

Siyah Kutu Sızma Testleri (Blackbox):

Tanım: Blackbox sızma testleri, siber saldırganların gözünden bir sistem veya uygulamanın güvenlik açıklarını değerlendirmek için yapılan bir test türüdür. Sızma testi uzmanları, sistemin iç işleyişine dair önceden bilgiye sahip değildirler.

Yaklaşım: Blackbox testlerde sızma testi uzmanları, hedef sistemle dışarıdan etkileşimde bulunurlar. Web uygulamaları, ağlar, sunucular ve diğer hedefler üzerinde yapılan sızma testlerinde, sızma testi uzmanları sistemi tarar, güvenlik açıkları arar ve siber saldırılar gerçekleştirirler.

Avantajlar: Bu yaklaşım, gerçek dünya saldırganları gibi hareket etme eğilimindedir. Bu nedenle sistemin gerçek dünya koşullarında ne kadar güvenli olduğunu değerlendirmek için kullanışlıdır.

Sınırlamalar: Blackbox sızma testleri, içsel işleyişi anlamamakla birlikte, zaman ve kaynak yoğun olabilir ve tespit edilen güvenlik açıklarının tam olarak nerede olduğunu belirlemek de daha zor olabilir.



Beyaz Kutu Sızma Testleri (Whitebox):

Tanım: Whitebox sızma testleri, test edilen sistemin veya uygulamanın iç işleyişi hakkında detaylı bilgiye sahip olan sızma testi uzmanları tarafından gerçekleştirilir. Bu yaklaşım, kod inceleme, yapısal analiz ve diğer içsel bilgilere dayanır.



Yaklaşım: Whitebox testlerde, sızma testi uzmanları hedef sistemin kodunu, yapısal tasarımını ve iç işleyişini inceleyebilirler. Bu, potansiyel güvenlik açıklarını daha hassas bir şekilde tespit etmelerine yardımcı olur.

Avantajlar: Bu yaklaşım, sistem veya uygulamanın iç işleyişini daha derinlemesine anlamalarını sağlar, böylece daha spesifik güvenlik açıkları tespit edilebilir. Kodun ve iç yapının daha iyi anlaşılması, daha etkili güvenlik önlemleri almayı sağlar.

Sınırlamalar: Whitebox sızma testleri için daha fazla bilgiye ihtiyaç vardır, bu nedenle sızma testi uzmanlarının bilgiye ulaşabilmesi gerekebilir. Ayrıca gerçek dünya saldırganlarının bakış açısını tam olarak yansıtmayabilir.

Sızma testleri, genel olarak bir organizasyonun siber güvenlik önlemlerini geliştirmesine yardımcı olur. Tipik olarak hem blackbox hem de whitebox sızma testleri birleştirilir ve organizasyonun genel güvenlik durumunu daha iyi değerlendirmek için birbirini tamamlayıcı bir şekilde kullanılır.

Gri Kutu Sızma Testi (Grey Box):

Siyah kutu ve beyaz kutu arası bir testtir. Bilgi sistemine, kuruluş ve sistemi hakkında sınırlı miktarda bilgi ile girmeye çalışmaktır. Bu durum, kuruluş içindeki kullanıcı hesabı ile sistemin bazı hatalarına içeriden erişebilecek bir şirketin ortak çalışanı olarak veya bir siteye erişmeyi başarabilecek biri içinde bilgisayar korsanlığının başlangıç noktası olarak konumlandırarak sistemin hatalarını kontrol etmeyi mümkün kılar. Siyah kutu testinden bir sonraki adım Gri kutu testidir. Siyah kutu sızma testi ekibi, sistemi dışarıdan bir bakış açısıyla inceliyorsa Gri kutu sızma testi ekibi, bir sistemde yükseltilmiş ayrıcalıklara sahip bir kullanıcının erişim ve bilgi seviyesine sahiptir. Gri kutu testindeki amaç, ağın güvenliğinin Siyah kutu değerlendirmesinden daha odaklı ve verimli bir şekilde değerlendirilmesini sağlamaktır.



Neden Sızma Testi Yaptırmalıyız?

Sızma testi güvenlik için yaptırılmalıdır. Genellikle işinizi tehdit edebilecek çeşitli saldırıları simüle eder. Örneğin evinizden kapıyı kapatıp kilitlemeden çıkarsanız girmek isteyen biri kolaylıkla girebilir. Ama evden çıkmadan önce kapıyı kilitlerseniz bir güvenlik önlemi almış olursunuz. Kapıyı kilitleyip alarm ve kamera sistemi de kurarsanız güvenlik önlemini arttırmış olursunuz. Benzer şekilde, sızma testleri de oluşabilecek saldırılara karşı alınabilecek önlemlerden biridir. Sızma testi sertifikası, ekosistemde çalışabilecek test uzmanlarını yetiştirmek amacıyla tasarlanır. Sertifikayı almak isteyen her aday, ilgili kursları başarıyla tamamlamalı ve bir sınavı geçmelidir. Bu sınav, adayın temel bilgi güvenliği prensipleri ve güncel sızma testi teknikleri hakkındaki bilgi seviyesini değerlendirir. Ülkemizde Türk Standardları Enstitüsü (TSE), sızma testi yapmak isteyen personel ve firmaları TS 13638 standardına göre sertifikalandırmaktadır.



Ne Sıklıkla Sızma Testi Yaptırmalıyız?

Ağ güvenliği yönetimini sağlamak için sızma testi düzenli olarak yapılmalıdır. Yeni keşfedilen tehditlerin veya ortaya çıkan güvenlik açıklarının saldırganlar tarafından potansiyel olarak nasıl saldırıya uğrayabileceğini görebilmek için planlama yapmanız gerekmektedir. Her şirketin sızma testi yapma sıklığı farklı olabilir. Çünkü her şirket aynı derecede güvenliğe ihtiyaç duymaz.

Bir şirketin sızma testi yaptırmaya sıklığı çeşitli faktörlere bağlıdır. Bu faktörlere şirket büyüklüğü, bütçe, yönetmelikler ve altyapı örnek olarak verilebilir.



Sızma Testinin Faydaları Nelerdir?

Sızma testi yapılan sistemler, test sonrası yaptığı düzeltmeler sayesinde olası saldırılara karşı önlemini önceden almış olmaktadır. Bu sayede herhangi bir veri sızdırılmasının önüne geçtiği gibi sistemlerinin de zarar görmesini engellemektedir. Ayrıca tespit edilmesi zor olan zafiyetlerin, test sırasında kullanılan yazılımlar ile tespiti daha kolay olmaktadır. Teknik personel için küçük görünen ve ertelenen bazı hataların veya zafiyetlerin, test sonucunda daha büyük zararlara yol açabileceği tespit edilebilmektedir ve gerekli önlemlerin alınabilmesi sağlanmaktadır. Sızma testlerinin sağladığı yararlar ve ne kadar kritik bir rol aldığı düşünüldüğünde sistemler için bir ekstra değil, zorunluluktur. Sızma testleri aşağıdaki güvenlik etkinliklerini destekler:

- Sistemdeki zayıflıkları bulma
- Kontrollerin sağlamlığının belirlenmesi
- Veri gizliliği ve güvenlik düzenlemeleriyle uyumluluğu destekleme

KAYNAKÇA:

https://tr.wikipedia.org/wiki/S%C4%B1zma_testi
<https://www.btyon.com.tr/sizma-testi-nedir.php>
<http://ozdenercin.com/2018/07/29/iot-sizma-testi-metodolojisi/>
<https://www.syberidea.com/pentest-sizma-testi-nedir-neden-onemlidir/>
<https://secromix.com/blog/sizma-testi-nedir-ve-yararlari-nelerdir/>
<https://www.beamteknoloji.com/akreditasyon-ve-sertifikalar/>
<https://optimumsiber.online/gray-box-grı-kutu-sizma-testi/>
https://www.beyaz.net/tr/guvenlik/makaleler/black_box_ve_white_box_testi.html





GÜVENLİ KOD GELİŞTİRME

Güvenli Kod Geliştirme Nedir?

Teknolojinin her alanda gelişmesiyle birlikte bilgiye ulaşmamız ve bilgiyi kullanmamız çok daha kolay bir hâle gelmiştir. Tabii ki bu durum siber güvenlik dünyasını etkilemiş ve siber saldırganlar için bir avantaja dönüşmüştür. Teknoloji gelişmeye devam ettikçe siber saldırılar için yeni yöntemler ve teknikler geliştirilmiş, kötü niyetli kişiler verileri zorla elde ederek kendi çıkarları için kullanmıştır.

Yazılımların görevlerini yerine getirirken tehdit veya saldırılardan başarılı bir şekilde korunmasına ve siber tehditlere karşı önleyici tedbirler alınmasına yazılım güvenliği denir. Yazılım güvenliğinin amacı, tüm saldırılara karşı daha dayanıklı bir yapı geliştirmektir.

Yazılım geliştiricilerin yazılım oluştururken aldığı kodlama uygulamaları, teknikler ve kararlar için güvenli kodlama standartları geçerlidir. Geliştiriciler güvenlik açıklarını en aza indiren kod geliştirmeyi amaçlarlar. Bazı çözümler diğerlerinden daha güvenlidir ve güvenli kodlama standartları, geliştiricileri ve yazılım mühendislerini en hızlı çözüm olmasa bile en güvenli yaklaşımı benimsemeye teşvik eder.

Güvenli programlama olarak da bilinen güvenli kodlama, olası güvenlik açıklarını (verileri açığa çıkarabilecek veya hedeflenen bir sistemde zarara neden olabilecek) önlemek amacıyla sıkı ilkeleri izleyen yüksek seviyeli bir dilde kod yazmayı içerir. Güvenli kodlama, kod yazmaktan, derlemekten ve uygulamalara kod yayımlamaktan çok daha fazlasıdır.

Yazılımlarımızı Güvenli Geliştirmezsek Ne Gibi Sorunlarla Karşılaşırız?

Eğer yazılımlarımızı güvenli bir şekilde geliştirmezsek saldırıya uğradığımızda aşağıdaki sorunlarla karşı karşıya kalabiliriz:

Yazılım tamamen etkisiz hâle getirilip kullanılması engellenebilir.

Yazılıma zararlı bir kod eklenerek işlevi bozulabilir ya da kötü amaçlar için kullanılabilir.

Yazılımdaki zafiyetler tespit edilerek bulunduğu sistemdeki diğer yazılımlara sızarak tüm veri merkezlerine erişim sağlanabilir.

Güvenli Yazılım Geliştirme İpuçları Nelerdir?

1.Yetkileri Sınırlandırmak

Yazılımı geliştirirken gerektiği kadar yetki verilerek uygulamanın sistem üzerinde yapabileceği değişiklikler kısıtlanır. Böylece uygulamadaki zayıflık kullanılarak sistemin kalanına sızılmaz.

2.Tüm Erişimleri Denetlemek

Bir alana yapılan her erişimde yetki kontrolü yapılarak erişim denetimi sağlanmalıdır. Tüm erişimler denetlenirken aynı zamanda normal durumların dışında da başlatma, kapatma, geri kazanım ve bakım aşamalarında erişimin denetlenmesi gerekmektedir. Gelen bir erişim isteğinin yanıtı verilirken de yetki kontrolü yapılmalıdır.

Bazı erişim kontrolü teknikleri aşağıda verilmiştir:

Yalnızca yetkili kullanıcıların korumalı URL'lere, hizmetlere, uygulama verilerine, kullanıcı verilerine vb. erişmesi gerekir.

Hesap denetimi uygulanmalı ve kullanılmayan hesaplar silinmelidir.

İşlem sayısı belirli bir süre boyunca tek bir kullanıcı veya cihaz için sınırlı olmalıdır.

3.Erişimleri Ayrı Tutmak

Yazılımda bulunan yüksek güvenli bir alana erişilmeye çalışıldığında tek bir koşula bağlı olarak izin verilmemeli, birden fazla koşul doğrulanarak erişim denetimi artırılmalıdır. İki faktörlü doğrulama buna örnek olarak verilebilir (2fa). Kullanıcı, yazılımda bulunan önemli bir alana erişmeden önce sunucuda daha sonra erişmek istediği alan oturum açmalıdır. Her iki koşul sağlandığında erişime izin verilmeli, sağlanmadığında erişim reddedilmelidir.

4.Saldırı Yapılabilecek Arayüz Alanlarını En Aza İndirmek

Saldırı yüzey alanı, yetkisi olmayan bir kullanıcının yazılım ortamından veri girebileceği, veri alabileceği veya yetkisiz işlem yapabileceği alandır. Bu sebeple uygulamaya gereksiz özellikler eklenmemelidir. İletişim yapılacak noktalar sınırlanmalıdır. Saldırının yapılabileceği yüzey alanı tasarım sırasında belirlenmeli ve sürekli olarak kontrol edilmelidir.

5.Verileri Şifreleme (Kriptografi)

Yazılımdaki verileri korumanın en iyi yollarından biri de verilerin şifrlenmesidir. Yazılımın içerisindeki hassas bilgilerin şifreleme yöntemleri ile saklanması gerekmektedir. Şifreleme yöntemleri bilinen ve test edilmiş şifreleme yöntemleri olmalıdır. Günümüzde algoritmalar çok kısa sürede çözülebildiği için şifreleme yöntemleri sık sık kontrol edilmeli ve güncel tutulmalıdır.

6.Kullanıcı Girdilerinin Kontrolü

Girdi Kontrolü, uygulama tarafından sağlanan girişte uygulanan bir kontroldür. Kötü niyetli bir kullanıcı tarayıcıdan yazılama bir kod veya komutun enjekte ederek saldırılara neden olabilir. Bu tür saldırılardan korunmak için yazılıma dâhil edilen her girdinin giriş doğrulamasından geçerek denetlenmesi gerekmektedir.

Giriş doğrulamasını gerçekleştirmek için kullanılabilecek bazı teknikler şunlardır:

- Yazılıma dâhil edilen girdi içerisine eklenen zararlı kodu çalıştırmak amacıyla kötüye kullanılabilecek etiketlerin veya kod parçacıklarının filtrelenmesi.
- URL'ler, HTTP başlıkları, gömülü kod vb. dâhil olmak üzere veriler işlenmeden önce kullanıcı tarafından sağlanan tüm verilerin doğrulaması.

7.Parola Yönetimi

Parola yönetimi, önemli verilerin gizliliğini ve kullanılabilirliğini korumak amacıyla parola saklarken kullanıcıların uyması gereken kurallarıdır.

Bunları aşağıdaki gibi sıralayabiliriz:

- Parolaların yeniden kullanılması engellenmelidir.
- Parola sıfırlama işlemi gerçekleştirildiğinde kullanıcılar bilgilendirilmelidir.
- Başarılı oturum açma işleminde kullanıcıya daha önceki oturum açma hata sayısı bildirilmelidir.
- Parolaların, parola karmaşıklık ilkesine göre belirlenmesi sağlanmalıdır.



8.Oturum Yönetimi

Farklı kullanıcıların bir web uygulaması hizmetinden gelen birden çok isteği güvenli bir şekilde işleme süreci oturum yönetimi olarak bilinir.

Oturum yönetiminde dikkat edilmesi gereken hususlar şunlardır:

- Oturum kapatıldıktan sonra oturumlar ve bağlantılar tamamen sonlandırılmalıdır.
- Aynı kullanıcıya birden fazla oturum açma izni verilmemelidir.
- Risklere ve iş hedeflerine bağlı olarak, oturum hareketsizliği zaman aşımı aralığı mümkün olduğunca düşük olmalıdır.





KİŞİLİKSİZ KİŞİLER

Birçoğumuz Tesla'nın CEO'su Elon Musk'ın, yatırımcıları kripto para borsasında yatırım yapmaya teşvik ettiği bir videoya rastlamışızdır. Ya da Jordan Peel'in yüz hareketlerinin Obama'nın yüzüne aktarıldığı sahte videosundan haberdarsınızdır. Ancak ne Elon Musk ne de Barack Obama böyle bir videoda yer aldı. Peki ya Facebook'un kurucusu Mark Zuckerberg'in deepfake videosunu duydunuz mu?

Örnekleri artırmak istersek bizi uzun bir liste karşılayacaktır. Hayatımıza bu kadar yerleşmiş olan deepfake nedir? Deep learning (derin öğrenme) ve fake (sahte) kelimelerinin birleştirilmesiyle yeni bir anlama kavuşan Deepfake kişilerin yüz, ses, mimik ve hareketlerini yapay zekâ teknolojileri yardımıyla taklit ederek oldukça gerçekçi görüntüler ve video montajları üretmeyi sağlıyor. Gerçekçilik, modelleri eğitmek için kullanılan fotoğraf ve videoların sayısı ile doğru orantılı olarak değişiyor. Özetle diyebiliriz ki elimizde videosunu oluşturmak istediğimiz kişiye ait örnek veriler bulunması gerekiyor.

Ne kadar çok veriye sahip olursak videonun gerçekçiliği o kadar artacaktır. Bu veriler derin öğrenme teknolojisi ile eğitilerek dublör dediğimiz kişinin yüzüne yapıştırılıyor ve böylelikle dublörümüzün söylediği ya da yaptığı şeyleri, görüntülerini kullandığımız kişi yapıyormuş gibi videolar üretebiliyoruz. Bu nedenle kullanılan dublörün asıl kişiye benzer fiziksel özellikler sergilemesi de videonun gerçekçiliği açısından önemli.

Deepfake ile oluşturulan içerikler, dijital bilgilerin doğruluğu için bir tehdit unsuru hâline gelebilir ve kötü amaçlar için kullanılabilir. Deepfake özellikle sahte pornografik içerikli videolarda kullanıldığından tepki almaktadır. Kişilerin yüzlerinin bilgileri dışında bu tarz içerikli videolarda kullanımıyla karşılaşılmaktadır ve bu durum ciddi bir tehdit hâline gelmektedir. Deepfake ile oluşturulan sahte verilerle mücadelede yine yapay zekâ teknolojisiyle üretilen çözümler kullanılacağı aşikârdır. Bu konuda birçok ünlü marka deepfake tespitleri için çözüm araştırmaları yapmaktadır. Sadece görüntü değil ses verisi de dijital dünya için bir tehdit unsuru olarak görülebilir. Kişilerin birkaç dakikadan oluşan ses kayıtları kullanılarak o kişinin sesine ait yeni ses verileri üretilmektedir.

Teknolojinin ilerlemesiyle artan sosyal medya kullanımı kişilerin sosyal medya ortamlarına resim ve video paylaşımını bir ihtiyaç hâline getirmiştir. Verilerin artmasıyla bu alanda ticari bir rekabet ortamı da oluşmuştur. Görüntüler kullanılarak oluşturulan sahte içerikler, kullanılan kişiler için problem oluşturmaktadır. Deepfake teknolojisi hepimiz için bir tehdit unsuru barındırır da en çok toplumda belli prestije sahip kişileri, aktörleri, iş adamlarını ve siyasileri hedef almaktadır. Siyasi propaganda, dolandırıcılık, hukuki bir süreçte adaleti yanıltmak için sahte veri üretimi ya da tamamen intikam, kıskançlık, şantaj amaçlı kullanımı olasıdır.

Sıradan insanlar için deepfake bir tehdit midir? Ben kendi hâlinde yaşayan bir vatandaşım, deepfake ile ne işim olur gibi bir düşünceye kapılmak doğru mudur? Bu konuda şahsi görüşüm görüntülerimizi sosyal medya platformlarında paylaşırken daha hassas davranmamız gerektiğidir. Herkese açık hesaplarda şahsi bilgilerimizi paylaşmamalıyız. Farkında olmadığımız bir düşmanımız olabilir ya da görüntülerimiz dolandırıcılık amaçlı kullanılabilir. Bu konuyu hafife almamalıyız çünkü deepfake teknolojisi şu anda herhangi bir akıllı telefon uygulamasında bile kullanılabilecek kadar gelişmiş durumdadır.

Dolandırıcılık ile alakalı bir örnek vermek istersek bir yakınımız görüntülü olarak bizi arayıp borç para ya da daha farklı isteklerde bulunabilir ve biz ona inandığımız için isteğini hemen yerine getirebiliriz.

Hindistan'da ise eski bir bakana şantajı yapılarak 50.000 Hindistan Rupisi dolandırılması olayı dünya gündeminde ilk sıralarda yer almıştı. Bu olayda bakan sosyal medya üzerinden sahte bir avatar ile sohbet etmeye başladıktan bir süre sonra soyunmasını istemiş ve bakanın izlediği görüntüler şantajcılar tarafından kaydedilerek dolandırıcılık gerçekleşmiştir.

Pandemiyle beraber evden çalışma da artmış, deep-fake de iş dünyasını daha fazla etkilemiştir. Dolandırıcılar, uzaktan çalışma pozisyonunda paylaşılan iş ilanlarına deepfake kullanarak başvurularda bulunmakta ve firmaların kritik pozisyonlarına yerleşebilmektedir. Böylelikle veri sızdırma, şirket hesaplarını hackleme ya da verilerin fidye amaçlı kullanımı gibi suçlar gerçekleştirilebilmektedirler.

Bu kısma kadar deepfake'in hep olumsuz yanlarından bahsettik, bu teknolojinin hiç olumlu bir getirisi yok mu? Bu soruya güncel ve bizden bir örnek vermek istersek Ziraat Bankasının hazırladığı Kemal Sunal'ın görüntü ve sesinin derin öğrenme teknolojileri kullanılarak oluşturulan "Sen Hep Gülümse" isimli reklam filmi biçilmiş kaftan. İçimizi ısıtan film ile aslında bu teknolojinin her zaman kötü amaçlarla kullanılmadığını görüyoruz. Bu reklam filmiyle anlıyoruz ki çok ünlü Yeşilçam yıldızları ya da dünyaca ünlü aktörler yaşamlarından sonra da bizler için unutulmaz eserlerini sergilemeye devam edebilecekler. Ayrıca bizler de çeşitli uygulamalar aracılığıyla kaybettiğimiz yakınlarımızın ya da belki hiç canlı olarak görmediğimiz büyüklerimizin günümüze uyarlanmış videolarını ve görüntülerini elde edebileceğiz. Ya da olayı yaşayan tarihi şahsiyetlerden dinleyebilme imkânı olması sizce de kulağa çok hoş gelmiyor mu?

Deep-fake ister iyi bir amaçla isterse bir suç unsuru olarak kullanılsın unutmamamız gereken şey karşımızdaki kişi gördüğümüz kişi olmayabilir. Dijital dünya da gördüğümüz her veriyi inanmamalı ve sorgulamalıyız.

KAYNAKÇA

<https://www.dijifi.org/2019/09/deepfake.html>

<https://sputniknews.com.tr/20220216/oluleri-canlandirmaktan-santaj-videolarina-deepfake-nedir-vehangi-tehlikeleri-iceriyor-1053901032.html>





MEMORYDEN NASIL BİLGİLER ELDE EDİLİR?

Hafıza (Memory) Nedir?

Hafıza (Memory); bilgisayar, akıllı telefon gibi elektronik cihazda programlar çalıştıran, geçici ve kalıcı bilgilerin depolanmasından ve onların tekrar kullanılmasından sorumlu olan, teknolojik aletlerin en önemli parçalarından biridir. USB bellekler, CD, DVD, kamera veya telefonlarda bulunan SD kartlar kişisel verilerin bulunduğu hafıza parçalarından bazılarıdır. Bu parçalarda eğer ele geçilirse kişisel güvenliğimizi tehlikeye atacak birçok bilgi yer alır.

Hafızadaki bilgiler neden önemlidir?

Adli bilişim incelemesinde kullanılan bir yöntem olan hafızanın imajının alınması yöntemiyle size ait olan sosyal medya şifreleri, kullanıcı adları, web sitelerine giriş bilgileri ve benzeri kişisel veriler açığa çıkarılır. Bu yöntemde sizin web sitelerine kullanıcı bilgilerinizi girmeniz veya sosyal medyalara kullanıcı adı ve şifrelerinizi girmeniz beklenir. Siz giriş yaptıktan sonra kişisel bilgileriniz hafızada depolanır ve bir açık hâline gelir.

Güvenliğimizi sağlamak için neler yapabiliriz?

Burada karşımıza birçok yol çıkıyor. Bunları avantaj ve dezavantajları ile inceleyeceğiz.

Fiziksel Silmek

Ulaşılabilir olmasını engellemek için medyanın fiziksel olarak yok edilmesi anlamına gelir. Bir kez zarar verilmesi durumunda medyanın geri dönüşü özel ekipmanlar kullanılmadığı sürece mümkün değildir. Cihazı kullanmaya devam etmek için medyayı kaldırıp yok etmeniz gereklidir. Bu metot CD, DVD ve USB gibi taşınabilir hafıza bellekleri için daha uygundur. Bu avantajları yanı sıra cihazı tekrar kullanmak için imha edilen depolama aracı yerine yeni bir araç eklemeniz, cihazların toksik madde içermesi gibi dezavantajları bulunmaktadır.

Güvenilir Silme Yazılımları

Verilerin silinmesi için yazılımlardan faydalanmayı içerir. Bu yöntem ucuz ve basittir. Ayrıca cihaz ve hafıza parçaları, silme işleminden sonra tekrar kullanılabilir. Fakat sürücülerin büyüklüğüne göre işlem süresi değişiklik gösterebilir ve hafıza kısımların ayrılması teknik yardım gerektirebilir.

Fabrika Ayarlarını Geri Yükleme

Birçok cihazda olan bu seçenek cihazı, aldığınız koşullarına geri döndürür. Taşınabilir depolama cihazları olan USB, DVD, CD için uygun bir yöntemdir. Bu yöntemde cihazın üreticisine sıfırlama işlemi konusunda güvenmek zorundasınızdır. Bu sebeple üretici ile fikir alışverişinde bulunmak tavsiye edilir.

Uzmanla Göndermek

Güvenli silme işlerinizi sizin yerinize yapan birçok şirket bulunmaktadır. Silme işlemi etkin bir şekilde tamamlandıktan sonra cihaz yeniden kullanılmaya hazır bir şekilde size iade edilir. Fabrika ayarlarını geri yüklemek yönetiminde olduğu gibi güvenlik konusunda araştırma yapmanız gereklidir.

Format Atmak

Format atmak ortamı biçimlendirip veri yapıları ve dosya sisteminin yeniden oluşturulmasını sağlar. Bu yöntemde veriler kurtulamayacağı için tam format rahatlıkla yapılabilir. Bununla beraber ücretsiz yazılımlar ile bilgilerin tekrar kurtulabilir olması da dikkatle değerlendirilmelidir.

KAYNAKÇA:

<http://hâliiozturkci.com/adli-bilisim-hafiza-imaji-uzerinden-facebook-sifresini-elde-etme/>

<https://ico.org.uk/your-data-matters/online/deleting-your-data-from-computers-laptops-and-other-devices/>





ADLİ BİLİŞİM

Nerede o eski günler... Sebze, meyve alabilmek için ya manava gitmemiz gerekirdi ya da pazarın kurulduğu günleri beklememiz... Şimdi öyle mi?

Hayatımızın her alanında günden güne dijitalleşmeyi daha çok hissediyoruz ve hızlı bir şekilde uyum sağlıyoruz.

Yağmurlu bir kış gününü hayal edelim. Alışveriş için pazara giderken çamurlaşmış toprağa her bastığımızda ayak izimiz kalır. Ama biz artık alışveriş için pazara, çarşıya gitmek zorunda değiliz. E-ticaret yoluyla azımsanmayacak kadar çok alışveriş yapıyoruz.

Peki biz bu yolla ayak izimizi kaybettirebilir miyiz?

Dijitalleşen hayatımızda ayak izi bırakmak için yağmurun yağmasına gerek yok. Hepimizin kolayca benimsediği bu yeni hayat tarzıyla beraber dijital ortamda bırakılan ayak izleri sayesinde birçok adli vakanın hızlı bir şekilde çözülmesi sağlanmıştır ve sağlanmaya devam etmektedir.

Adli bilişim dalındaki kavramlardan biri olan dijital delil, günlük hayatımızda kullandığımız iletişim kurmamıza yarayan uygulamalarda, e-posta kutularında, çevrimiçi depolama alanlarında, elektronik cihazda (kalp pili de dâhil) var olan her türlü bilgidir. Dijital delil kullanılarak çözülmüş vakalardan biri Ross Comptom davasıdır.

Dayton Daily News'in haberine göre kundakçılık ve sigorta dolandırıcılığıyla suçlanan Ross Compton, 2017 yılında kalp pilinden alınan verilere dayanarak tutuklanmıştır. Compton 2016'da yaşanan kundaklama olayına istinaden yangın başladığı sırada uyuduğunu belirtmiş, daha sonra uyanıp polisi aradığı ve eşyalarını bavula koyup evden çıktığı yönünde ifade vermiştir. Soruşturmayı yürüten ekip şüphelinin kalp pili verilerini incelemeyi talep etmiştir. İnceleme sonucunda verilen ifadeyle kalp pili verileri arasında tutarsızlık tespit edilmiş ve suçlu işlediği kesinleşmiştir.

Arama geçmişi dijital delil tespit edilebilecek verileri içeren bir depolama çeşidi olarak sayılabilir. Arama geçmişlerinin takibi sayesinde büyük felaketlerin önüne geçilmiştir.

2009 yılında Krenar Lusha'nın arama geçmişinde güçlü patlayıcılar hakkında yaptığı araştırma, bilgisayarında ise patlayıcılar hakkında kılavuz bulunmuştur. Bu deliller doğrultusunda soruşturma açılmış, evinde yapılan aramalar sonucunda bu yönde fiziksel kanıtların da bulunmasıyla Birleşik Krallık'ta tutuklanmıştır. Yine arama geçmişindeki veriler sayesinde 2006 yılında ABD'nin Teksas eyaletinde işlenen bir suç 2010 yılında çözüme kavuşmuştur. Kari Baker 2006 yılında hayatını kaybetmiştir. Eşi, ölümünü yüksek doz uyku hâpi kullandığını ve Kari Baker tarafından kaleme alındığını iddia ettiği mektubu göstererek açıklamıştır. Fakat soruşturmayı yürüten ekip tarafından araştırmalar devam etmiş ve Kari Baker'in eşinin internet arama geçmişinde fazla doz uyku hâpi kullanımı üzerine aramalar bulunmuştur. Ve elbette fiziksel kanıtlarla beraber şüphelinin suçu kesinleşmiştir.

Dijital ortamlarda paylaşılan her şey, yeni teknolojiler sayesinde üzerinden yıllar geçse bile erişilebilir hâle gelmiştir. İyi bir analiz sürecinin akabinde birçok vaka aydınlatılabilirken can kaybına sebep olacak felaketler de önlenbilir olmuştur.

KAYNAKÇA:

<https://www.precisedigital.com/4-cases-solved-with-digital-evidence/>

<https://www.daytondailynews.com/news/crime-law/prosecutor-man-awaiting-arson-trial-middle-town-pacemaker-case-dies/PORi20NIKa8ONyVZis7RvN/>

<https://www.iigpi.com/5-cases-cracked-with-digital-forensics/46/2821/>





VERİLER SİLİNDİ Mİ?

Veriler bilgisayarda nasıl saklanır?

Kullandığımız telefon, tablet ve bilgisayarlarda bizler hakkında birçok kişisel veri bulunur. Bu veriler özel fotoğraf ve videolarımız, ses dosyalarımız, metin belgelerimiz, çalıştığımız kuruma ait veriler, kredi kartı bilgileri, doğum tarihi gibi hassas verilerdir ve bize özeldir. Başkaları tarafından görülmesi sorun oluşturabilir. Bu sebeple daha bilinçli kullanıcılar olmak için arka planda neler olduğunu bilmemiz faydalı olacaktır.

Cihazlarımızda tuttuğumuz veriler yanlışlıkla silinebilir ya da artık o dosyaya ihtiyaç kalmadığı için geri dönüşüm kutusuna gönderilir. Silindikten sonra ortadan kaybolan verilere aslında ne olur?

Bu soruya yanıt vermeden önce cihazlarımızda verilerin nasıl tutulduğuna cevap vermek daha doğru olacaktır.

Bilgisayar sistemlerinde her şey 0 ve 1 olarak ifade edilir. Bu sebeple bilgisayarımda bulunan her türlü dosya 0 ve 1'lerin anlamlı olarak bir araya gelmesiyle oluşan değerler şeklinde disklerde saklanır.

Veriler disk üzerinde bölümlere ayrılmış olarak depolanır. Ayrıca hangi verinin hangi bölümde tutulduğu bilgisi de dosya sistemi tarafından bilinmektedir. Dosya sistemi depolama cihazı üzerinde bulunan verilerin tutulduğu bölümleri organize ederek verilere kolayca ulaşmamızı sağlar. Bir dosyaya ulaşmak istediğimizde işletim sistemi bu dosyanın nerede olduğu bilgisini dosya sisteminin öğrenir ve disk üzerinde ilgili bölüme giderek bizim için dosyayı hazır hâle getirir.

Silme işlemi yaptığımızda arka planda neler olur?

Bir dosyayı silmek istediğimizde sil tuşuna basarak dosyayı geri dönüşüm kutusuna göndeririz. Yapılan bu işlem, dosyayı bulunduğu klasörden alıp geri dönüşüm kutusuna taşımaktır. Belirli bir süre geçtikten sonra geri dönüşüm kutusundan da otomatik olarak silinir. Artık dosyayı hiçbir klasörün içerisinde göremeyiz ancak bu diskten silindiği anlamına gelmez. Dosya sisteminde verinin bulunduğu bölüm bilgisi silinir. Diskin bölümlerinde veri tutulan kısımlar dosya sistemi tarafından “veri yazılamaz” olarak kabul edilir. Silme işlemi yapıldığında dosya sistemi verilerin tutulduğu bölümü “veri yazılabilir” olarak kabul

etmeye başlar. Yani silinen dosya disk üzerinde tutulmaya devam eder ancak dosya sistemi verinin tutulduğu bölümü boş olarak değerlendirmeye başlar ve üzerine yeni veriler yazılmasına olanak tanır.

Verileri sildiğimizde neden kalıcı olarak silinmez?

Bir dosyayı sil tuşuna basarak sildiğimizde dosya sisteminden o dosyanın hangi bölümde tutulduğu bilgisi silinir. Bu işlem oldukça kısa sürer.

Eğer her seferinde veriler kalıcı olarak silinirse hem veri üzerine yeni değerler(?) yazılacağı için daha fazla işlem gerekir hem de dosya boyutuna bağlı olarak silme işlemi daha fazla vakit alır. Bu da cihazın performansını olumsuz etkiler. Bu sebeple cihazlarda varsayılan silme işleminde veri fiziksel olarak değil mantıksal olarak silinir.

Kalıcı olarak verileri silmek mümkün mü?

Bir dosyayı sildiğimizde dosyanın diskten silinmediğini öğrendik. Ancak çeşitli sebeplerden ötürü verileri kalıcı olarak silmek isteyebiliriz. Verilerin diskte 0 ve 1 şeklinde tutulduğundan bahsetmiştik. Bir veriyi kalıcı olarak silmek için verinin üzerine 0, 1 veya random olarak 0 ve 1'ler yazdırarak verilerin silinmesini sağlayabiliriz. Ancak bu işlemi bir kez yapmak yeterli olmayacaktır. Bu işlemi defalarca tekrar etmek her seferinde verinin geri getirilme olasılığını azaltır.

Silinen veriler geri getirilebilir mi?

Günümüzde kullanılan cihazlarda farklı teknolojiler kullanılmaktadır. Çoğunlukla masaüstü bilgisayarlarda kullanılan kısaca hdd olarak adlandırılan sabit disk sürücülerini veriyi disk üzerine manyetik olarak işler. Bu sebeple uzun süre diskte tutulan veri silindikten sonra disk üzerinde izleri kalabilir.

Bunu kâğıt üzerine belirgin yazılan yazıların silgi ile silindikten sonra izi kalması gibi düşünebiliriz.

Üzerine defalarca veri yazılmış olsa bile verileri geri getirmek için veri kurtarma işlemi yapan ticari kuruluşlar verilerinizi kurtarmaya yardımcı olabilir. Bu kuruluşlarda çalışan uzman kişiler gelişmiş cihazlar kullanarak verinin disk üzerinde bıraktığı izleri takip eder ve verileri geri getirmeye çalışır. Verilerin kayıpsız şekilde geri getirilebileceğinin garantisi yoktur. Ancak depolama cihazı fiziksel ağır hasar almadığı sürece geri getirilme ihtimali her zaman vardır.

Silinen verileri geri getirmek için her zaman uzman kişilere başvurmamıza gerek kalmayabilir. Verileri geri getirmek için ücretsiz birçok yazılım geliştirilmiştir.

Yanlışlıkla silinen verileri geri getirmek için bu yazılımlar kullanılabilir. Ancak dikkat edilmesi gereken bir nokta var. Dosya silindikten sonra verinin bulunduğu bölüm boş olarak değerlendirildiği için bilgisayarınızı kullanmaya devam ederek o bölüme veri yazılmasına sebep olabilirsiniz. Üzerine veri yazıldıkça da istediğiniz verileri kayıpsız geri getirme olasılığınız azalır. Bu yazılımlar silinen veriler üzerine yeni veriler yazılmadıysa verileri geri getirebilir. Bu sebeple bir dosyayı yanlışlıkla sildiyseniz hızlı ve dikkatli davranmanız oldukça önemlidir.

Daha hızlı ve maliyetli olan ve özellikle dizüstü bilgisayarlarda yaygın olarak kullanılmaya başlayan ssd yani katı hâl sürücüleri veri depolama işleminde daha farklı bir yöntem kullanır. Veri yazma işleminde dijital olarak yazma işlemi gerçekleştirdiği için silinen verileri geri getirmek oldukça zordur. Verileri geri getirmek için uzman kişiler tarafından diskin detaylı analiz edilmesi gerekir. Ssd disklerde kullanılan teknoloji sayesinde verinin bulunduğu bölümden veri tamamen silindiği için verileri geri getirmekte daha farklı yöntemler uzmanlar tarafından uygulanmalıdır.

Yazılımlar verileri nasıl geri getirir?

40 dairelik bir apartman düşünün. Ev sahibi 18. dairede oturan kiracıya evden çıkmasını söyledi. Cama kiralık ilanı asıldı ve zilden adı silindi. Artık orada kimsenin oturmadığı düşünülüyor ancak eski kiracılar yeni kiracı gelene kadar evde yaşamaya devam etmekte. Orada hâlâ kiracı olduğunu anlamak için bütün daireleri gezip kontrol etmemiz gerekir. İşte verileri geri getirmek için kullanılan yazılımlar da tam olarak bunu yapar. Dosya sisteminde boş olarak işaretlenmiş bölümlere tek tek bakarak verileri bulup getirmeye çalışır.

Format atıldığında veriler kalıcı olarak silinir mi?

Format atıldığı zaman verilerin geri getirilemeyeceği düşünülür. Birçok insan tarafından böyle düşünülse de bu doğru değildir. Format atıldıktan sonra veriler diskte durmaya devam eder. Ancak bu verilerin adresleri artık hafızada tutulmaz. Kısacası format atıldığı zaman veriler üzerinde değil dosya sisteminde işlem yapılır. Dosya sistemi artık hangi verinin nerede tutulduğu bilgisine sahip değildir. Bu sebeple verileri görmek istediğimizde dosya sistemi verileri bize getiremez.

Kısa bir süre de olsa kullandığınız bilgisayar, telefon veya diskinizi satmak ya da bir başkasına vermek isteyebilirsiniz. Bunu yapmadan önce verilerin kötü niyetli kişiler tarafından geri getirilebileceğini unutmayın. Çeşitli yöntemlerle geri getirilen verileriniz kötü niyetli kişiler tarafından tehdit ve şantaj için aleyhinize kullanılabilir. Bu sebeple her zaman dikkatli olmakta fayda var.

Özetle silmekle verileri gerçekten silmiş olmayız. Sadece o verilere ulaşmak artık eskisi kadar kolay değildir.

**DİLAN
ÇELİK**
KONU
21





IOS CİHAZ GÜVENLİĞİ

- IOS (iPhone Operating System), ilk kez 29 Haziran 2007 yılında Apple şirketi tarafından tanıtıldı. iOS nedir, diye sorarsak tamamen kapalı kaynak koda sahip Linux tabanlı bir işletim sistemidir. Burada biraz açık ve kapalı kaynak kodlardan bahsetmek istiyorum.
- Açık kaynak kodlara herkes tarafından erişim sağlandığı için programlar bu kodlarla kolayca çalışabilir. Bu sayede basit ve hızlı gelişebilir. Kapalı kaynak kodlarına göre teknik destek ve donanım yönünden daha yetersiz ve kapsamlı testlerden geçmediğinden her an bir güvenlik açığı oluşma riski vardır. Açık kaynak kodlu Android işletim sistemi ücretsiz olduğu için her cihazda kullanılabilir ancak iOS işletim sistemi sadece Apple cihazlarında kullanılabilir.
- iOS cihazlar, güçlü yazılımı sayesinde daha az güçlü donanım kullanabilir. Güvenlik açısından karşılaştırsak iOS platformunun daha güvenli olduğu sonucuna varabiliriz. Ancak tabii ki iOS cihazlarının güvenliği için yapmamız gereken bazı şeyler vardır.

Bunları maddelersek:



Parolalarınızı güçlü ve benzersiz olacak şekilde ayarlayın.

Apple kimlik ve parolaları çözülmesi zor, güçlü ve benzersiz şifreler olmalıdır. Parolaların biyografik bilgilerle (doğum tarihi, ad, soyad ...) ilgili olmamasına özen göstermelisiniz. Mesela "1A2vXb78t" şifresini tahmin etmek veya denemeler yaparak kırmak '123456789'a göre aylar sürecektir. Bu sebeple şifrelerinizde maksimum uzunluğu hedefleyip özel karakterlere yer vermeye çalışın.



iPhone'umu Bul uygulamasını kullanın.

Cihazda bulunan güvenlik uygulaması olan iPhone'umu Bul uygulamasını hırsızlık vb. durumlar için kullanın. Bu uygulama ile cihaz bulunmasa bile veriler uzaktan silinebilir. **iPhone'umu Bul özelliğini aktif etmek için** Ayarlar > iPhone'umu Bul'a tıklayıp açık konuma getirin.



İki faktörlü doğrulama özelliğini aktifleştirin.

Apple Kimliğiniz için ek bir güvenlik katmanı olan iki faktörlü kimlik doğrulama, başka biri parolanızı bilse bile hesabınıza sizin dışınızda kimsenin erişmemesini sağlamak için tasarlanmıştır. İki faktörlü kimlik doğrulamayla, hesabınıza güvenilir bir aygıttan veya web'den yalnızca siz erişebilirsiniz. İki faktörlü kimlik doğrulamayı açmak için Ayarlar> [adınız]> Parola ve Güvenlik'e gidin. İki Faktörlü Kimlik Doğrulamayı Aç'a dokunun. Sürdür'e dokunun. Giriş yaparken doğrulama kodunun gönderilmesini istediğiniz telefon numarasını girin. Kodları kısa mesaj veya otomatik telefon aramasıyla almayı tercih edebilirsiniz.

İleri'ye dokunun. Telefon numaranızı doğrulamak ve iki faktörlü kimlik doğrulamayı açmak için doğrulama kodunu girin.



Cihazınızı jailbreak yapmayın.

Jailbreak, Apple'ın mobil cihazlarındaki işletim sistemlerinde bulunan kısıtlamaların kaldırılması amacı ile yapılan erişim işlemidir.

Apple'ın yazılımı için benimsediği "duvarlarla çevrili bahçe" yaklaşımı, Android işletim sisteminin özelleştirmeye yönelik sunduğu çok çeşitli seçeneklere her zaman ters düşmüştür. Cihazına jailbreak uygulayan kullanıcıların başlıca sebeplerinden biri, iOS'u Android'e benzetmektir.

Jailbreak hem geçmişte hem de günümüzde, Apple'ın onaylamadığı uygulamaları yüklemenin ve arayüzü özelleştirmenin bir yolu olmuştur. Jailbreak yapma cihazda güvenlik açıklarının oluşmasına sebebiyet vermektedir.



Uygulamalarınızı bilin ve kişiselleştirin.

Uygulama izinlerini okuyun ve bunlara aşına olun. Uygulamalar çerezler yardımıyla kullanıcıdan veri toplar ve bu veriler çeşitli amaçlar için kullanılır. Uygulamaları kişiselleştirerek bu çerezleri ve toplanan verilerinizi yönetebilirsiniz.



Cihazınızı güncel tutun.

Otomatik iOS güncellemelerini açık tutun. Telefonunuzun her daim güncel olduğundan emin olun. Telefon güncellemesi yapılmayan telefonlar kötü ve virüslü dosyalara karşı dirençsiz kalır. Apple cihazınızı güncelleştirmek için

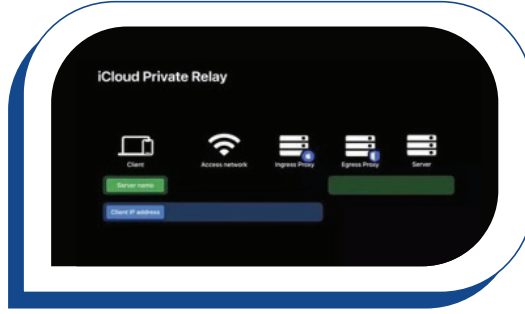


Ayarlar> Genel> Yazılım Güncelleme> Otomatik Güncellemeler bölümüne gidin. iOS Güncellemelerini İndir'i ve iOS Güncellemelerini Yükle'yi açın.

07

Touch ID veya Face ID kullanın.

Face ID ve Touch ID kullanarak birçok işlemi çok daha güvenli bir şekilde yapabilirsiniz. Bu özellikleri kullanarak telefon kilidini açabilir, telefonu başlatabilir, ödeme yapabilir, bazı yazılım ve programlara giriş yapabilirsiniz.

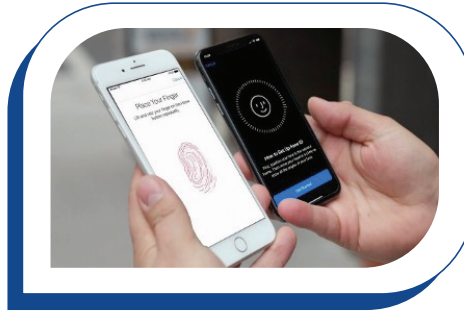


Touch ID özelliğini aktifleştirmek için

Ayarlar> Touch ID ve Parola'ya dokunup parolanızı girin.
Parmak İzi Ekle'ye dokununuz. Ve parmak izinizi tanıtır.

Face ID özelliğini aktifleştirmek için

Ayarlar> Face ID ve Parola> Face ID'yi Ayarla bölümüne gidin,
sonra ekrandaki yönergeleri izleyin.



08

Apple ile giriş yap özelliğini kullanın

Apple ile Giriş Yap özelliği, tümüyle gizliliğinize saygı duyacak ve kişisel bilgilerinizin kontrolünü elinizde tutmanızı sağlayacak şekilde tasarlanmıştır ve iki faktörlü kimlik doğrulama özelliği ile entegre çalışmaktadır.

Bu da gizliliğin korunmasında büyük avantaj sağlamaktadır.

09

Akıllı takip önleme özelliğini aktif edin

Akıllı Takip Önleme, siteler arası izlemeyle mücadele etmek için en son yapay öğrenme teknolojisini ve aygıt içi akıllı teknolojileri kullanır.

Bu özellik, IP adresinizi takip edicilerden gizler. Dolayısıyla internette nelere baktığınız reklam verenleri değil yalnızca sizi ilgilendirir. Bu da Safari de daha rahat gezmenize olanak sağlar.

10

iCloud Özel Geçiş özelliği

iCloud Özel Geçiş (beta), sanal olarak herhangi bir ağa bağlanmanıza ve daha güvenli ve özel bir şekilde Safari ile dolaşmanıza izin veren bir internet gizlilik servisi. Aygıtınızdan ayrılan trafiğin şifrelenmesini sağlar ve kimsenin hakkınızda ayrıntılı bir profil yaratmak amacıyla IP adresinizi, konumunuzu ve dolaşma etkinliğinizi kullanamaması için iki ayrı internet geçişi kullanır. iCloud Özel Geçiş'i ayarlamak için Ayarlar > [adınız] > iCloud'a gidin. Özel Geçiş'e dokunup ardından da Özel Geçiş'i açın.

11

Ekran kilitlenme süresini minimal tutun

Cihaz ekranınızın hızlı bir şekilde kapandığından emin olun.

iPhone cihazınızda otomatik kilit sürenizi ayarlamak için Ayarlar>Ekran ve Parlaklık> Otomatik Kilit'e gidin. Burada kilit süresini değiştirebilirsiniz.



12

E-Postamı Gizle özelliğini kullanın

Kişisel e-posta adresinizi gizli tutmak için E-Postamı Gizle'yi kullanabilirsiniz. E-Postamı Gizle ile, kişisel e-posta hesabınıza yönlendirilen benzersiz, rasgele e-posta adresleri oluşturabilirsiniz, böylece web'de form doldururken veya bültenlere kaydolarken ya da e-posta gönderirken gerçek e-posta adresinizi paylaşmanız gerekmez.

Özelliği kullanmak için Ayarlar> [adınız]> iCloud> E-Postamı Gizle'ye gittikten sonra yeni adres yaratıp yönergeleri izleyebilirsiniz.



ŞÜKRAN
ÜN

KONU
22



E-POSTA GÜVENLİĞİ



Gün geçtikçe çoğumuzun yaşamı dijital cihaz ve mecralarla entegre hâle gelmeye başladı, hayatlarımız siberleşti diyebiliriz. Günümüzde e-posta, siber yaşamımızın önemli bir parçasını içinde barındırıyor ve siber yaşamımıza dair önemli bir kapının anahtarı niteliği ile karşımıza çıkıyor. Bu sebeplerle dijital kimliğimizin bir parçası olan e-postalarımızı güvende tutmak, sosyal ilişkilerimizi ve kişisel verilerimizi de güvende tutmak anlamına geliyor. Bu yazıda e-posta güvenliğini sağlamak için neler yapabileceğimizin, hangi tehditlerle karşı karşıya olduğumuzun ve e-posta güvenliğinin neden önemli olduğunun üzerinde duracağız.

E-posta Güvenliği Nedir?

“Peki e-posta güvenliği deyince ne anlıyoruz? Öncelikle e-postanın adresine ulaşıncaya kadar geçtiği güzergâhta yetkisiz kişilerce okunup okunmadığı önemlidir. İkinci ve bazı durumlarda ilkinden daha önemli olan nokta ise gönderenin gerçekten gönderen olduğunu iddia ettiği kişi olup olmadığıdır, yani e-postanın başlık (header) kısmında ismi ve e-posta adresi yazan kişi, gerçekten söz konusu e-postayı gönderen kişi midir? Yoksa ortada bir tür kimlik hırsızlığı mı vardır?” (Levi, 2003)

Levi'nin de açıkladığı gibi siber yaşam kavramı bazı güvenlik açıklarını beraberinde getirdi. Verilerimizin etrafına çit örmemiz mümkün değil maalesef. Ancak e-postalarımızı korumak için önlemler alarak siber yaşam kalitemizi artırmak mümkün.

E-posta güvenliği kişilerin ya da kurumların, kötü niyetli yazılım ya da kişilerin yetkisiz erişimlerine karşı alınan önlemlerini, politikalarını, geliştirilmiş yazılımlarını ve tekniklerini kapsar diyebiliriz.



E-postalarda Ne Tür Güvenlik Tehditleri Bulunur?

E-posta servisleri çok büyük bir habitatı kapsadığından erişimi kolay ve yaygınlaşmış platformlardır. Öyle ki geçerli bir e-posta adresiniz olmadığı takdirde birçok mecraya sınırlı olarak erişebilirsiniz.

Bununla birlikte bir e-posta adresi siber yaşamınızda kullandığınız araçların çoğunun tek anahtarı hâline gelebilir. İşte bu sebeplerle ne tür risklerle yüz yüze olduğumuzun farkında olmamız gerekir.

Teknik olarak her şeye kararında, bir miktar da şüpheci yaklaşmalı ve gerekli önlemleri almalıyız. E-postalar gönderen bilgisi, alıcı veya alıcılar bilgisi, başlık, gövde metni, ekler ve URL'ler gibi unsurlar içerir.

Bu unsurlardan doğan güvenlik zafiyetlerini inceleyelim.

Sahte e-postalar ve URL'ler

Tanıdığımız birinden e-posta aldığımızı düşünmek oldukça kolay ancak alışkanlıklarımız bizi köreltebilir. Hatalı yapılandırılmış e-postalar ciddi riskler barındırır. Örneğin patronunuzdan aldığınızı düşündüğünüz bir e-posta taklit edilmiş bir e-posta adresi olabilir.

Bu konuda yeterince dikkatli miyiz?

İnsanlık olarak duygusal manipülasyona açık varlıklarız. Tam olarak bu noktada cezbedici, merak uyandırıcı ya da tehdit içerikli e-postalara karşı dikkatli olmamız gerekiyor. Bu e-postalardan en yaygın olanları “Hediye kazandınız”, “Tebrikler! Çekiliş sonucunuzu öğrenin”, “Tatil Kampanyası” gibi başlıklara ya da bunlara benzer başlıklara sahip olanlardır. Heyecan ve merak duygusuyla açılan bu e-postalar kişisel bilgilerinizden bazılarını talep etme yoluyla ciddi güvenlik sorunlarına sebep olabilmektedir. Yanı sıra zararlı yazılım içerikli URL'lerin gövde metinlerinin içine gömülmesi ve tek tıkla bağlantılarının verilerini yetkisiz olarak kullanması, söz konusu tehditlerden biridir.

Fidye Virüsleri

Art niyetli amaçlarla dağıtılan kod bloklarını fidye virüsleri olarak nitelendirebiliriz. Dosya ekleri ve URL'ler fidye virüslerini konumlandırmak için biçilmiş kaftanlardır. Link tıklamaları, ek dosya indirmeleri gibi eylemler sonucu fidye virüsleri bilgisayarınızı, sosyal ya da kurumsal ağınıza çökertebileceği gibi kişi listelerinize erişerek hızla yayılım gösterme eğilimindedir.

Sistemselsel zafiyetlerinden doğan suistimalleri de göz ardı edemeyiz. Şimdi o suistimalleri inceleyelim:

İnternet Tarayıcısı Faktörü

Sadece e-posta kullanırken dikkatli olmamız yeterli olmuyor maalesef, siber dünyada yer alan her şeyin zafiyeti bulunabiliyor. Bu zafiyetlerin doğurduğu güvenlik açıkları ilişkili araçlarda da zafiyetlere sebebiyet veriyor. İnternet tarayıcıları da risk faktörü en yüksek araçlardan biri olarak karşımıza çıkıyor. Veri sızıntılarını önleyebilmek için dijital okur-yazarlık kavramını iyi sindirmiş olmamız gerekiyor.

Spam e-postalar

Spam e-postalardan almayanımız, maruz kalmayanımız yoktur. Peki ya e-posta kutunuzun kapasitesini dolduracak kadar spamı aynı anda aldığınızı düşünebiliyor musunuz? Bu durumda iletişim ve iş süreçlerinizin ne kadar aksayacağını, siber yaşamın günlük yaşamınıza ne kadar güçlü bir şekilde etki edebileceğini anlamak oldukça kolaylaşıyor.



- Dijital okuryazarlık bilinci geliştirebiliriz.
- Güçlü parolalar kullanabiliriz.
- Düzenli olarak parolalarınızı değiştirebilirsiniz.
- Parola güvenlik sorularının cevaplarının gerçekten “güvenli” olduğundan emin olabiliriz.
- Hesaplarımızdan çıkış yapabiliriz.
- Farklı işlevler için farklı e-posta adresleri edinebiliriz.
- Ortak ağ kullanırken dikkatli olabiliriz.
- Spam filtresi kullanabiliriz.
- Şüpheli e-postaları spam olarak işaretleyebiliriz.
- Zaman dilimi bazında gelen-giden e-posta sayılarına sınırlandırma getirebiliriz.
- Çift aşamalı doğrulamayı aktifleştirebiliriz.
- Anti-virüs yazılımları ile şüpheli e-postaları tarayabiliriz.
- Güvenlik duvarı kurabiliriz.
- Semantik güvenlik uygulamaları kullanabiliriz.

KAYNAKÇA

Levi, A. (2003). Nasıl bir E-posta güvenliği? Bilişim Güvenlik, 38-40.





ÇOCUKLARDA AKILLI SAAT GÜVENLİĞİ

Akıllı Saat Nedir?

Akıllı saat, saat şeklinde takılabilen bir bilgisayardır. Modern akıllı saatler günlük kullanım için yerel bir dokunmatik ekran arayüzü sağlarken ilişkili bir akıllı telefon uygulaması uzun süreli biyoizleme gibi yönetim ve telemetri sağlar. İlk modeller; hesaplamalar, dijital zaman anlatımı, çeviriler ve oyun oynama gibi temel görevleri yerine getirebilse de 2015'ten bu yana piyasaya sürülen akıllı saatler, mobil uygulamalar, mobil işletim sistemi ve Wi-Fi / Bluetooth bağlantısı dâhil olmak üzere akıllı telefonlara daha yakın daha genel işlevlere sahiptir. Bazı akıllı saatler, FM radyo ve Bluetooth kulaklık aracılığıyla dijital ses ve video dosyalarının oynatılması ile taşınabilir medya oynatıcılar olarak işlev görür. Saatli telefonlar (veya telefon saatleri) olarak adlandırılan bazı modeller, telefon görüşmeleri yapma gibi mobil hücrel işlevlere sahiptir.

Yazılım Güvenliği

Güvenlik yazılımı; sunucuları, dizüstü bilgisayarları, mobil cihazları ve ağları yetkisiz erişimlerden, izinsiz girişlerden, virüslerden ve diğer tehditlerden korumak ve güvence altına almak için tasarlanmıştır. Güvenlik yazılımı; verileri, kullanıcıları, sistemleri ve şirketleri çok çeşitli risklerden korumaya yardımcı olabilir.

Yazılım Güvenliği Niye Önemlidir?

Güvenlik yazılımı hem iş hem de bilgi güvenliğini artırabilir. Güvenlik yazılımı olmadan veya eski çözümler kullanarak çalışmak, kuruluşları ve kullanıcıları bilgisayar korsanları, casus yazılımlar, virüsler ve kötü amaçlı yazılımlar dâhil olmak üzere çok çeşitli tehditlere maruz bırakır. Siber tehditlerin artan karmaşıklığı ve çeşitliliği ve mobilite, uzaktan çalışma ve Nesnelerin İnterneti'ndeki artış nedeniyle korunması gereken uç noktaların sayısının artması birçok işletmenin daha gelişmiş güvenlik yazılımı çözümleri kullanmasını gerektirmektedir.

Akıllı Saatler Hacklenebilir mi?

Bu cihazlar için bazı saldırı girişimleri zaten kaydedilmiştir. Akıllı saatlerle ilgili henüz çok büyük ihlaller yaşanmamış olsa da beyaz şapkalı bilgisayar korsanları (işletmelerin ürünlerindeki / programlarındaki / yazılımlarındaki zayıflıkları belirlemelerine yardımcı olan "iyi" bilgisayar korsanları olarak da bilinir.) bazı güvenlik açıklarını ortaya çıkarmaya yardımcı olmuştur.

Kimlik Avı

Kimlik avı, sahte bir uygulama indirip içine herhangi bir kişisel bilgi girerseniz oluşabilir. Bu uygulamalar resmi olmayan uygulama mağazalarında daha yaygındır ancak Google ve Apple uygulama mağazalarında yoktur. Bu sahte uygulamalar, Google hesabınıza giriş yapmanızı isteyerek çalışır ve ardından doldurtulan sahte bir formla kimlik bilgilerinizi ele geçirerek hesabınızı tehlikeye atmanıza sebep olur.

Bluetooth Düşük Enerji

Bluetooth Düşük Enerji, akıllı saatinizi telefonunuzla, kulaklıklarınızla ve diğer cihazlarla eşleştirir. Ancak karmaşık protokolleri sayesinde Bluetooth veri şifrelemesinde güvenlik açıkları vardır. Verilerin zayıf şifrelenmesi ile, bir suçlu minimum çaba harcayarak bağlantınıza ulaşabilir (Bluetooth, akıllı saatler gibi kablosuz öncelikli cihazlarda önemli bir bağlantı özelliğidir.)

İvmeölçer

İvmeölçer verileri, akıllı saatinizin atılan adımlar gibi sağlık ve fitness özellikleri için hareketi izlemesine yardımcı olur.

İvmeölçer verileri, şifreleri ve kredi kartı numaralarını ortaya çıkarmak için de analiz edilebilir. Yinelenen hareket verileri eğilimleri, kimlik bilgilerinizi yeniden üreten bilgisayar klavyesi yazma hareketlerini bulmak için kullanılabilir. Kuşkusuz, bu çok fazla çalışma gerektirir, bunun için bilgisayar korsanlarının tercih edeceği bir yöntem değildir ancak yine de kullanılması mümkündür. Geliri yeterince iyiye siber suçlular bu yöntemle daha yüksek değerli hedefleri seçebilir.

Fabrika Varsayılan Parolaları

Varsayılan fabrika parolaları, IoT cihazlarına erişmek için kullanılan bir arka uç teknik aracıdır. Cihazları eve götürdükten sonra bunlar değişmeden gittiğinden bir bilgisayar korsanı şifrenizi çevrimiçi olarak kolayca bulabilir veya varsayılan şifreleri dark web'de satın alabilir.

Bu kolay erişimi önlemek için tüketicilerin öncelikle neyin var olduğunun farkında olmaları gerekir.

Genellikle üreticiler şifre değiştirme talimatlarını bir kullanıcının asla okumadığı teknik kılavuzlara gömer. Bazen şifrenizi doğru bir şekilde güncellemek için doğrudan şirketle iletişime geçmeniz gerekir. Ancak daha ucuz akıllı saatler satın alan bazı sahipler, orijinal üreticiyle iletişim kurmanın bir yolunu bile bulamaz. Ucuz çevrimiçi ürünler genellikle toplu olarak satın alınır ve tonlarca

ikincil distribütör tarafından yeniden markalanır. Birçok çocuk saati bu şekilde satılır ve onlar büyük bir güvenlik tehdidiyle karşı karşıya bırakılır. Bu nedenle akıllı saatleri yalnızca Apple, Fitbit veya Garmin gibi güvenilir, tanınmış markalardan satın almanız en iyisidir.

Kısa Mesajı Yeniden Yapılandırma

Bazı çocukların akıllı saatlerinin sadece bir metin göndererek hacklenebilir olduğu keşfedilmiştir. Özel olarak yazılmış metin mesajları kullanılarak bazı saatler bilgisayar korsanına fayda sağlamak için yeniden programlanabilir. Bu yöntem, saati suçlunun telefonuna tamir ederek cihaza daha fazla kontrol ve erişim sağlayabilir. Daha sonra saati GPS üzerinden izleyebilir ve hatta kullanıcıyı arayabilirler.

Düşük kaliteli çocuk modellerinde keşfedilmesine rağmen diğer birçok ucuz akıllı saat benzer güvenlik açıklarına sahip olabilir. Bunun nedeni, daha ucuz üreticilerin genellikle giriş seviyesi bir ürünü bir araya getirirken kullanıcı dostu olmaktan ziyade güvenliğe fazla önem vermemeleridir. Apple gibi saygın üst düzey markalar daha fazla hesap verebilirlikle tutulurken yine de güvenlik tartışmasına karşı bu kolaylık ile karşılaşılıyor.

Bu güvenlik endişeleri, üreticileri şifrelemeye ve uygulama mağazasını da kötü amaçlı yazılımlarına karşı korumaya daha fazla önem vererek yükseltme yapmaya yönlendirdi. Bununla birlikte endüstri standartlarının eksikliği, herhangi bir ürünün uygun şekilde korunacağını garanti etmeyi imkânsız kılmaktadır.

Akıllı Telefonunuzu Koruyun

Bu bir yazım hatası değil, akıllı saat güvenliği akıllı telefonunuzda başlar. Güvenlik açığının en büyük noktalarından biri, akıllı saatiniz ve akıllı telefonunuz arasındaki iletişim bağlantısıdır. Daha da korkutucu olanı, bilgisayar korsanlarının verileri koklamak için her ikisine de sızması gerekmez, yalnızca birine erişimleri yeterlidir.

Başka birinin akıllı telefonunuza girmesinin en kolay yolu sahte uygulamalardır. Bu, Android çalıştıran telefonlarda en yaygın olanıdır ancak iOS çalıştıran telefonlar tamamen bağışık değildir. İyi bir kural, Google Play Store veya iOS App Store'dan indirilen uygulamalara bağlı kalmaktır. İndirmeden önce uygulamaların güvenilirliğini araştırın. Ve eğer bir iOS kullanıyorsanız telefonunuzu özgürleştirirken jailbreak yapmak sizi bazı güvenlik baş ağrılarına açabilir.

Akıllı saat yazılımınızı düzenli olarak güncelleyin

Geliştiriciler bir nedenden dolayı güncellemeler yayımladılar. Güncellemeler genellikle belirli bir işletim sisteminin veya uygulamanın performansını artırmakla kalmaz, aynı zamanda tehlikeli güvenlik açıklarını da düzeltir.

Akıllı saatiniz veya favori uygulamanız yeniden başlatılırken 30 saniye beklemek can sıkıcı olsa da vicdansız bilgisayar korsanlarıyla uğraşmak için saatler harcamak zorunda kalmanızı önleyebilir.

Fitness verilerinize dikkat edin

Verilerinize zarar verebilecek tek kişi bilgisayar korsanları değildir, reklamverenler ve sigorta şirketleri de zarar verebilir. Şirketler genellikle pazarlama ve fiyatlandırmalarını bilgilendirmek için tüketiciler hakkında veri satın alır.

Bu, sağlık ve fitness verileri söz konusu olduğunda özellikle endişe vericidir. Akıllı saatler sizin hakkınızda birçok arzu edilen bilgiyi taşıyabilir. Örneğin bir sigorta şirketi kalp rahatsızlığınız olduğunu veya yüksek miktarda doymuş yağ yediğinizi görürse sizi istenmeyen primlerle vurmaya çalışabilir veya daha da sizi sigortalamayı reddedebilir.

Herhangi bir fitness uygulamasını kullanmadan önce gizlilik ayarlarını kontrol edin. Nelerin herkese açık olarak paylaşılacağını seçin. Ayrıca kullanıcı adı olarak bir takma ad kullanmayı düşünün, böylece günlük sodyum tüketiminiz size geri bağlanamaz.

Hırsızlığı Caydıran Ayarları Etkinleştirin

Karşılaşılabileceğiniz dijital tehlikelerin ötesinde, her zaman akılda tutulması gereken şey: Birisi akıllı saatinizi çalabilir ve verilerinizi alabilir.

Akıllı saat üreticileri bu olasılığın farkındadır. Bu yüzden birçoğu hırsızlığı caydırmak için güvenlik ayarları oluşturmuştur. Apple'ın Etkinleştirme Kilidi'ni ele alalım: Hırsızların Apple Watch'unuzu onaylanmamış bir aygıtla eşleştirmesini önler. Diğer akıllı saatlerin bu konuda kendi görüşleri vardır, bu nedenle özelliğin adı ne olursa olsun etkinleştirildiğinden emin olun!

Akıllı Saatiniz Şifrelerinizin İzlenmesi ve Çalınması Sebebiyle Saldırıya Uğrayabilir

Beltramelli, “Akıllı saatler ve fitness izleyicileri gibi bileklik ve kol bandı cihazları, tüketici elektroniği pazarında zaten önemli bir yer tuttu ve her yerde yaygınlaşıyor.” diye açıklıyor. “Bununla birlikte, giyilebilir olma doğaları gereği bu cihazlar, diğerlerinin yanı sıra kullanıcıların gizliliğini tehdit eden yeni bir yaygın saldırı yüzeyi sağlıyor.” Tezine eşlik eden bir videoda Beltramelli, güvenliği ihlal edilmiş bir akıllı saatin, sadece elinin hareket etme şeklini algılayarak hangi düğmelere bastığını nasıl anlamlandırabileceğini gösteriyor. İstismarın arkasındaki temel ilke, akıllı tuş vuruşu izleme programlarının, yazma alışkanlıklarından oluşturulan davranışsal biyometrik profillere dayanarak bireysel insanları tanıyabildiklerinin gösterilmesine benzer.

Bir elin uzaydaki hareketi, kişiden kişiye biraz farklı olsa da teoride, kişisel kimlik bilgileri için çıkarılabilir ve birinin girişlerini tehlikeye atmak için daha akıllı girişimlerde bulunmak için kullanılabilir.

Bu sorun, çoğu klavyenin ve pin pedin boyutunun, insanların bunları kullanırken kendilerini daha rahat hissetmelerini sağlamak için standartlaştırılmış olması nedeniyle daha da kötüleşmiştir. Gizmodo’nun işaret ettiği gibi Beltramelli’nin araştırması alarm için acil bir neden olmamalıdır. İstismar yalnızca araştırmanın güvenliği ihlal edilmiş bir akıllı saatin iç kısımlarına tam ve derin erişimi olduğu için gerçekleştirilebilir. Kutudan yeni çıkmış bir Apple veya Android saat kullanan herkes iyi olmalıdır.

Yine de dikkatli olun. Bu yüzden Google ve Apple, üçüncü taraf uygulama mağazalarındaki kabataslak uygulamaları süslü yeni oyuncaklarınızdan çok uzakta tutmanız konusunda ısrar ediyor.

Çocuklarda Akıllı Saat ve Veri Güvenliği

Akıllı saat güvenliği konusunu düşünürken ilk olarak aklınıza her zaman şu gelsin: “Herhangi bir siber korsan çocuğumun akıllı saatini ele geçirirse onunla iletişime geçebilir mi? Ona zarar verebilir mi?” Bu bağlamda bu içeriğimize bu sorular üzerinden gideceğiz. Yetişkinler için de önerilerimiz tabii ki olacak.

Akıllı saat güvenliği, cihazımızı siber korsanlardan ve siber dolandırıcılardan korumak için aldığımız önlemlerin genel adıdır.

Cihazınıza sızan herhangi bir siber korsan, kullanıcıya farklı konularda saldırabilir. Örneğin akıllı saatlerin topladığı veriler ifşa edilebilir veya farklı kişilere satılabilir. “Akıllı saatler veri mi topluyor?” diye soru sorabilirsiniz. Evet, topluyor.

Akıllı saatler birçok kişisel bilgiyi bluetooth ve internet gibi bağlantılardan geçirdikten sonra toplar. Akıllı saatlerde her ne kadar çok büyük, endişe verici veri ihlalleri yaşanmamış olsa da bu yaşanmayacağı anlamına gelmiyor. Bu yüzden her zaman bilgimiz olması gereken konulardan biri de bu. Düşük güvenlik gücüne sahip akıllı saatlerde basit bir SMS ile akıllı saatlerin ele geçirildiği bilinen bir gerçek. Bu tür güvenlik açıklarının oluşmasının temel nedeni ise üretici firmaların güvenliğe önem vermek yerine sadece görünüş ve kullanım kolaylığına önem vermesi. Ancak sektörde herhangi bir güvenlik standardı olmadığı için bu tür açıklarla karşılaşmamız mümkün. Bu yüzden mümkün olduğu kadar araştırma yapın ve ona göre cihaz alın.

Almak istediğiniz cihazın güvenilir olduğundan emin olmak için kullanıcı yorumları oldukça yardımcı olacaktır. Bu konudaki araştırmalarınızı sadece Türkçe olarak değil, aynı zamanda İngilizce olarak da yapmanızı tavsiye ediyoruz. Örneğin X bir cihaz hakkında arama mı yapmak istiyorsunuz? Kullandığınız arama motoruna giriş yapın ve X güvenlik açığı, X güvenliği veya X güvenliği hakkında gibi aramalar yapın.

Aradığınız ürünün güvenlik açığı olduğunu mu gördünüz? O zaman ikinci bir aramaya geçmeniz gerekiyor. Bu güvenlik açığı ile ilgili nasıl bir çözüm üretildiğini araştırın. Herhangi bir veri sızıntısı olup olmadığını kontrol edin.

KAYNAKÇA:

Smartwatch - Wikipedia

Smartwatch Security - Safety & Risks (kaspersky.com)

Your Smartwatch Can Be Hacked To Monitor And Steal Your Passwords | HuffPost The WorldPost

What Is Security Software? - Cisco

Akıllı Saat Güvenliği: Akıllı Saat Seçerken Bunlara Dikkat Edin! (lorentlabs.com)





FIREWALL İLE ANTİVİRÜS PROGRAMI ARASINDAKİ FARK

Firewall Nedir?

Firewall, bir diğer adı güvenlik duvarı olan bu cihaz, gelen ve giden veri paketlerini kontrol eden, kontrol ederken de zafiyet tespit ederse sisteme bulaşmasını engelleyen bir çeşit koruma kalkanıdır.

Firewall üzerinde önceden belirlenmiş kurallar kullanılır fakat ek olarak kullanıcı kuralları yazabilir veya istediği kuralları kaldırabilir. Bu kuralların yazılma amacı, sisteme virüslerin geçişini engellemek ve performansını negatif yönde etkileyecek faktörlerden sistemi uzak tutmaktır.

Örneğin güvenlik duvarı yazılmış olan kurallara uymayan bir ağ trafiği tespit ederse ağınıza erişmesini engeller. “Black-Hat Hacker” gibi amaçları sisteme zarar vermek olan saldırganlardan bazıları dış ağdan iç ağa sızmaya çalışırlar. Bu nedenle Firewall üzerinde yazılmış olan bu kurallar güvenlik için önemli bir yere sahiptir.

Günlük yaşantımızla Firewall’u özdeşleştirecek olursak rezervasyon ile çalışan bir restoran düşünelim. Girişte duran görevlinin elinde rezervasyon yaptırmış olan müşterilerin adlarının bir listesi olsun ve x kişisi rezervasyonsuz gelirse restorana giriş yapamaz gibi bir kural bulunsun. Eğer restoran sahibi, girişteki görevliye x kişisi gelirse restorana alabilirsiniz derse o zaman x kişisi restorana giriş yapabilir. Buradaki restoran sahibini Firewall üzerine ek kurallar yazan kişi, girişteki görevliyi Firewall, girişteki görevlide bulunan adların yazdığı listeyi Firewall üzerindeki kurallar ve restorana girmeye çalışan kişiyi ağ trafiği olarak düşünebiliriz.

Anti-virüs Nedir?

Bilgisayarınızı zararlı yazılımlardan korumak ve kurtarmak amacıyla üretilmiş olan yazılımlara anti-virüs programı denir. Bilgisayarların, saldırganlar yoluyla gelebilecek zararlı yazılımlar tarafından her zaman korunması gerekmektedir. Bu zararlı yazılımlar bilgisayarınıza harici bir disk yoluyla, mail yoluyla veya herhangi bir riskli siteye tıklanması yoluyla çok kolay bir şekilde bulaşabilir.

Bilgisayarlarımızda kişisel verilerimiz gibi önemli bilgiler barınmasından dolayı ve- yahut kötü amaçlı yazılımlar bizim adımıza bir işlem yapıyormuş gibi davranışlarda bulunabileceğinden sisteme virüs bulaşması kötü sonuçlara yol açabilir. Bu yüzden cihazlarımızın güvenliğini sağlamak çok önemlidir.

Anti-virüsler ise burada devreye girmektedir. Düzenli olarak bilgisayarlarındaki aktiviteleri takip eder ve zararlı yazılımların bulaşması engeller. Anti-virüs programları zararlı yazılımı bulmak, silmek veya karantina altına almak gibi çeşitli yöntemler izler.

İyi bir anti-virüs'te bulunması gereken özellikler şunlardır:

Yeni oluşturulmuş zararlı yazılımlar için anti-virüs veri tabanının düzenli olarak güncelleniyor olması.

Eski oluşturulmuş, uzun zamandır bilinen zararlı yazılımların yanı sıra güncel oluşturulmuş kötü yazılımlardan da koruyabilmesi.

Kurulmuş olan cihazı yormaması, performansını negatif etkilememesi.

Modern ve gelişmiş özelliklere sahip olması.

Anti-virüsün önemi şöyle bir örnekle açıklanabilir:

100 kişinin çalıştığı bir şirketimiz var. Çalışanlardan birisinin flash diskinde virüs barınıyor olsun. Bu flash diski şirketteki bilgisayarlara taktıkça virüs, flash diski taktığı her bilgisayara bulaşır ve eğer bilgisayarlarda iyi bir anti-virüs yoksa virüs tespit edilemeyebilir. Direkt kendini belli eden değil de bilgisayarda barınan fakat sistemi yavaş yavaş çökerten bir virüs olabilir veya anında bilgisayarın sistemini çökerten bir virüs ile karşılaşılabilir. Eğer bu virüsler yayılmaya devam ederse şirketin bilgileri saldırgan tarafından ele geçirilebilir. Daha sonrasında şirket için çok daha maliyetli bir çözüm olur ve bilgisayarların sistemlerini kurtarabiliyor olsak da şirketin verileri çalındığı için kötü bir sonuçla karşılaşılabilir. Bundan dolayı her bilgisayarda iyi bir anti-virüs olması gerekir.

Firewall İle Anti-Virüs Programı Arasındaki Fark Nedir?

Az önce de dediğimiz gibi firewall, dışarıdan içeri gelen veya içeriden dışarı giden veri paketlerini inceler. Anti-virüs yazısındaki vermiş olduğumuz örnekte saldırgan virüsü yaymaya iç ağdan başlar, bu tür zararlı yazılımları firewall tespit edemez çünkü bu virüsün dışarı ile bir bağlantısı yoktur. Sadece iç ağda dolanır ve iç ağda yayılır.

Anti-virüs ise dışarıdan gelen veya içeriden giden ağ trafiğini kontrol etmez, zararlı yazılımlara ve bu yazılımların detaylarına odaklanır.

Kısaca firewall ve anti-virüs için farklı konular üzerine çalışıyor fakat ikisi de koruma kalkanı görevi görüyor diyebiliriz. Bundan dolayı tek başına firewall yeterli olamaz, anti-virüsün de endpoint dediğimiz son kullanıcıları yani bilgisayarları denetliyor olması gerekir. Bu şekilde bilgisayarımızı ve verilerimizi güvende tutabiliriz.

**DİLARA
ŞENTÜRK**

**KONU
25**





MOBİL CİHAZ GÜVENLİĞİ

Mobil cihazların hayatımızdaki yeri gün geçtikçe daha da artmaktadır. Alışverişten banka işlerine, film izlemekten sosyal medya kullanımına kadar neredeyse her şeyi bu cihazlar üzerinden yapabilmekteyiz.

Mobil cihazlar ile birlikte birçok alandaki iş yapış şekillerimiz de değişmektedir. Bu kadar erişilebilir durumdayken ve birçok işimizi de mobil cihazlar üzerinden yapıyorken güvenlik eskisinden çok daha önemli ve kritik bir konu olarak karşımıza çıkmaktadır.

Kullanıcıların verilerini korumak için dikkat etmesi gereken başlıca güvenlik risklerini şu şekilde sıralayabiliriz:



Şifre Kullanımı

Mobil cihaza şifre koymak, cihazın çalınması durumunda veya uzaktan erişilmesi sırasında bazı saldırıları engelleyecektir.

Hesaplarınızın ele geçirilmesini önlemek için tamamen özgün ve karmaşık bir şifre belirleyin ve şifrenizi kimseyle paylaşmayın. Ayrıca diğer sitelerde ve cihazlarda kullandığınız bir şifreyi de tekrar kullanmayın. Ek olarak mümkünse SMS, Google Authenticator gibi çok adımlı kimlik doğrulama yöntemlerini kullanmaya çalışın.



Uygulamalar

Bir uygulama indirmeden önce uygulama hakkında araştırma yapın ve marketlerde bulunan uygulamaları tercih edin. Ayrıca uygulama izinleri penceresini onaylamadan önce mutlaka okuyun, sıkıcı gibi gözükse de sisteminizi güvende tutmanızı sağlayacak en iyi önlemdir.



Yazılım Güncelleme

Yazılım güncellemeleri, güvenlik ve gizlilik açıklarını giderir. Yazılımınızı güncelleniz en güncel çözümlerden yararlanacağınız anlamına gelir. Siber tehditlere ve her türlü saldırılara karşı korunmuş olmak için güncellemeleri etkinleştirerek işletim sisteminizi güncel tutmalısınız.



Kablosuz Ağ Bağlantıları

Halka açık kablosuz ağlar, siber suçlular tarafından çoğunlukla hedef alınır.

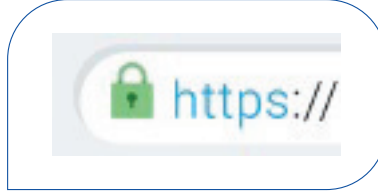
Özellikle kişisel verilerinize erişim sağlarken saldırıya uğrama riskini azaltmak için halka açık ağ bağlantınızı kısıtlamalısınız.



Şüpheli linklere tıklamayın

Siber suçlular, yaygın olarak kullanılan bir internet sitesinin adres uzantısına benzer bir bağlantı üretebilir (www.xyzwbank.com yerine www.xyzvvbank.com gibi) ve bu bağlantılar ilk bakışta gerçeğinden ayırt edilemeyebilir.

Bu tarz linklere tıkladığınızda kişisel bilgileriniz çalınabilir veya cihazınıza kötü amaçlı yazılım yüklenebilir. Bundan dolayı kişisel verilerinizi gireceğiniz sitelerin bağlantısının güvenli olduğundan emin olun.



Şekil 1: Site Bağlantısı Güvenli



Cihazınız Çalınırsa/Kaybolursa

Alınabilecek önlemlerin başında verilerin telefonda şifreli tutulması, yardımcı programlar ile verilerin uzaktan silinmesi ya da transfer edilmesi gelmektedir.



Sosyal Mühendislik Dolandırıcılığı

Bu dolandırıcılar insanların parolaları, bankacılık bilgileri gibi kişisel bilgilerini elde etmek için çalışır. Sosyal mühendislik dolandırıcılıkları e-posta, mesajlar ve telefon görüşmeleri şeklinde görünür. Eğer durumun şüpheli olduğunu düşünüyorsanız kesinlikle bu isteklere yanıt vermeyin.

KAYNAKÇA

<https://www.incehesap.com/blog/mobil-cihazlar-icin-guvenlik-tavsiyeleri/>
<https://sibermetin.com/mobil-cihaz-guvenligi>
<https://gelecegiyazanlar.turkcell.com.tr/blog/akilli-telefonlarda-guvenlik-riskleri>
<http://www.protekbilisim.com/cozumler/mobil-cihaz-guvenligi-ve-yonetimi>
<https://www.verizon.com/articles/mobile-device-security/>





USB CİHAZLAR GERÇEKTEN GÜVENLİ Mİ?

USB CİHAZLAR GERÇEKTEN GÜVENLİ Mİ?

USB, Universal Serial Bus (Evrensel Seri Veri Yolu), 1990'lı yılların ortasında geliştirilerek bir aygıtı şarj etmeye yarayan, iki aygıt arasında veri aktarmayı kolaylaştıran yaygın bir bağlayıcı hâline gelmiştir. Veri akışının daha hızlı yapılabilmesini, ana makine ile yan donanım arasındaki bilgi ve elektrik akımının seri bir şekilde aktarılmasını sağlar. Bu bağlamda USB temel olarak çok çeşitli bağlantı tipleri sayesinde dijital kamera, akıllı telefon, güç ünitesi, fare, mikrofon ve harici bellek gibi pek çok donanımın ana yönetici makine ile bağlantı kurmasını sağlar. (En bilindik şekliyle bilgisayar, yazıcı, akıllı televizyon, dijital fotoğraf baskı makinesi ana makine olarak ele alınabilir.)

Bilgisayarınızın üzerinde USB bağlantı uçlarının kolaylıkla monte edilebileceği USB girişleri bulunur. Peki bilgisayarlar ve diğer elektronik cihazlar arasında bağlantı, iletişim ve güç paylaşımına olanak sağlayan bu USB girişleri ile bağladığımız USB cihazlar güvenli mi?



Her şeyden önce siber güvenlik için farkında olmak ve çevremizde farkındalık yaratmak oldukça önemlidir. Sizin siber güvenliğiniz online olarak bağlantılı olduğunuz herkesin güvenliğini kapsar. Zararsız gibi görünse de bir USB bellek veya bir şarj kablosu dahi tüm kişisel verilerinizi ele geçirebilir ve kötü amaçlı yazılımların size ulaşmasını a sebep olabilir. Örneğin USB bellek, bilgisayar korsanlarının fidye yazılımı ve diğer kötü amaçlı yazılım türlerini yüklemesinin yaygın bir yoludur. Bir USB bellek, birden fazla kişi tarafından kullanıldığında veri kaybına sebep olabilmekte, kullanıldığı elektronik cihazlardan verileri toplayabilmekte ve bu veriler kötü niyetli kişilerce kullanılabilir. Özel olarak tasarlanmış bellekler gizlenmiş virüsleri taşıyor olabilir ve bu da zaman içerisinde verilerinize zarar verebilir.

Herkesin kullandığı bir bilgisayara ya da tanımadığınız bir kişinin bilgisayarına USB belleğinizi takarsanız bu, verilerinizi riske atmak demektir. Çünkü herkesin kullandığı bir bilgisayara kim nasıl erişim sağladı veya herhangi bir zararlı yazılım yükledi mi bunu bilemezsiniz. Bir USB belleğin nereden geldiğini bilmiyorsanız elektronik cihazınıza takmadan önce iki kez düşünmenizde fayda var. Bir ağ üzerindeyseniz kötü amaçlı yazılım diğer bilgisayarlara yayılabilir ve hatta tüm ağı kapatabilir. Ayrıca USB bellekte yer alan dosyalardan şüphe duyuyorsanız herhangi bir şey yapmadan önce üzerlerinde virüs taraması yapmayı da ihmal etmeyin. Çünkü dosya sizi bir kimlik avı sitesine götürüp giriş bilgilerinizi girmeniz için kandırabilir.

Dikkatli olmanın yanı sıra korunmak için yapmanız gereken şeyler ise bilgisayarınızın işletim sistemini güncel tutmak, etkili güvenlik araçlarının yüklü olduğundan emin olmak ve bu programları düzenli olarak güncellemektir. İşletme bilgisayarlarına ve özellikle sunuculara kaynağı belirsiz USB bellek takılmamalı, kullandığınız cihazın yetkilerini, aynı zamanda bilgisayarlarınızın yetkilerini gözden geçirmelisiniz. Kötü niyetli kişiler cihazınıza erişebilir ve verilerinizi hem çalabilir hem de yok edebilir. Bu oldukça riskli bir durumdur.

Hem bilgisayarınızın hem de USB belleklerin verilerini şifreleyin. Belleğin cihaza her takılışında istenen şifre sayesinde yetkisiz kullanıcıların bellekteki dosyalara erişme tehlikesi neredeyse ortadan kalktığı için veri kaybı yaşama ihtimalinden uzaklaşmış olur. Veri transferi gerçekleştirirken çevrimiçi olmayın. İnternete bağlı cihazlarda USB belleklerin virüs gibi sebeplerle zarar görme ihtimali çok yüksek olmasa da özellikle kritik dosyaların USB belleğe aktarılması sırasında internet bağlantısının kapatılması, verilerinize yönelik riskleri azaltır. Otomatik Çalıştır'ı devre dışı bırakarak virüslü bir USB sürücüdeki kötü amaçlı kodun otomatik olarak açılmasını önleyebilirsiniz. (Otomatik Çalıştırma özelliği, USB sürücüler ve CD'ler gibi çıkarılabilir ortam aygıtlarının takıldığında otomatik olarak açılmasını sağlar.) Hatta mümkünse USB bellek girişinin kullanılabilir hâlde bırakılmaması bizleri daha güvende tutmaya yardımcı olacaktır.



USB cihazları kadar dikkat etmemiz gereken bir diğ er  rnek ise standart řarj kablolarıdır. Bu kablolar aygıtları řarj etmek ve gerektiğinde dosya aktarımı gibi řeyleri yapabilmeniz i in tasarlanmıřtır. Ancak bunlarla g r nt  itibarıyla  ok benzer olan ve  zel olarak tasarlanmıř kablolar, bu iřlemlerden  ok daha fazlasını yapabilir.

Bir řarj kablosu, g r nt  olarak birebir aynı olması ve telefonunuzu řarj etmenin yanı sıra i erisinde bulunan bir hotspot ile k t  niyetli kiřilerin kolayca eriřebilmesine olanak saėlar. Bu kabloyu bilgisayarınıza baėladığınız ve onay verdiğiniz anda bir hacker, t m verilerinize eriřmiř demektir. Bu noktada yapmanız gereken en  nemli řey ise orijinal řarj kablolarını kullanmak olacaktır.

USB bellek  rneğinde olduėu gibi etrafta g rd ğ n z herhangi bir kabloyu direkt olarak bilgisayarınıza baėlamamanız da bu soruna karřı etkili bir   z m olabilir.

KAYNAK A:

<https://www.nyu.edu/life/information-technology/about-nyu-it/nyu-it-news/the-download/the-download-features/cybersecurity-free-usb-ransomware.html>

<https://www.griffith.edu.au/about-griffith/cybersecurity/cyber-safety-with-usb-drives>

<https://www.freepik.com>

Kitap: USB Explained - Steven McDowell, Martin D. Seyer

FATMA CEYDA ORUÇ

KONU
27





MODEMİM GÜVENLİ Mİ?

Modem ve Cihaz Güvenliği Nedir, Ne Kadar Önemlidir?

21. yüzyıl dünyasında internet kullanımı olmadan bir hayat düşünmemiz mümkün müdür? Özellikle internet kullanımı her çeşidi ve her şekli ile yalnızca eğlence amaçlı değil; iş, eğitim, sanat, iletişim gibi günlük hayatın temel dinamiklerini yönlendirecek boyuta gelmişken? Bir günün içerisinde zamanımızın önemli bir bölümünü bir çevrimiçi ders, dizüstü bilgisayarda şirketle önemli bir toplantı, sosyal mecralarda paylaşımda bulunma, bazen herhangi bir rezervasyon veya küçük işlemler için de olsa internet bağlantısı bulunan cihazlarda harcarız. Peki bu kullanımın dozajının hayatımıza etkisi nedir? Bir kafede, misafir olarak bulunduğumuz evde, okulda, kurumsal alanda, öğrenci yurdunda hatta metro istasyonlarında dahi kolayca bağlanıp hemen kullanmaya başladığımız internet aslında nedir taşıdığı riskler ve güvenlik sorunlarının çapı ne olabilir hiç düşündünüz mü? Gelin birlikte inceleyelim.

Ev gibi küçük dijital ekosistemlerde dahi mobil veri kullanılmadığı takdirde bir modem cihazı üzerinden internet bağlantısını kullanan birçok alt kullanıcı bulunur. Bahsedilen internet kullanımının boyutu ve önemi göz önüne alındığında tüm kullanıcıları ve cihazları birbirine ve kendine bağlayan modem cihazı elbette bu ekosistemin en önemli üyelerinden biridir.



Özellikle fiber optik kabloların ve güçlü altyapıların hayatımıza daha da dâhil olmaya başladığı son dönemlerde modemlerin etki alanı ve yayılımı artmış olup ağdaki fonksiyonu da güçlenmiş ve önemi reddedilemez bir konuma gelmiştir. Kullanıcılara yüksek miktarlarda veri kullanımı ve konforu sağlaması gibi özellikleri ise kişisel mobil veri kullanımına kıyasla genelde topluluklara hitap eden modem cihazı kullanımının popülaritesini artırmıştır. Bu durum göz önüne alındığında internet kullanımı ve ağ paylaşımının sağladığı kolaylık ve basitliğin yanı sıra yol açabileceği riskli durumlara da dikkat edip tüm ekosistemini güvenli tutmak veya en azından güvenli tutmaya çalışmak bilinçli bir kullanıcının öncelikli görevidir.

Zira halka açık bir erişim noktasından kablosuz cihazla internete bağlanmak gibi basit görünebilen bir olay bağlantı kurulduğu anda sizi uzaktaki bir saldırganın muhtemel ihlallerine açık hâle getirebilir. Hatta birçok kullanıcı kablosuz ağ ayarlarını dahi olduğu gibi bırakarak farkında olmadan kendini açık hedef haline getirebilir. İşte tam da bu yüzden her kullanıcı güvenli bir internet kullanımı için modem ve cihaz güvenliğini sağlamayı öğrenmek ve uygulamak sorumluluğundadır diyebiliriz.

Kablosuz ağ güvenliği kavramı; kullanıcının tasarrufunda bulunan modem, yönlendirici gibi kablosuz cihazların ve bu ortamdaki veri transferi, ağ paylaşımı ve bağlantıların tamamının güvenliğini kapsamakta olduğu için kablosuz ağ ilişkili tüm kavramlar bu etki alanında bulunmaktadır, bütüncül bir bakışla dikkat gerektirir. Bu bilinci kazandıktan sonra herhangi bir kablosuz ağdaki internet kullanıcısı veri güvenliği söz konusu olduğunda artık çok daha dikkatli davranabilecektir. Evine giren ve çıkan tüm verilerin -banka kartı bilgileri, tüm hesaplarının şifreleri, e-postaları, kişisel verileri gibi kablosuz yönlendirici üzerinden aktığını fark edip güvenlik önlemleri alacağını, dışarıdan gelecek saldırılara kimliğini gizleyerek, bant genişliğini çalmaya çalışarak ve yazılım kusurlarından faydalanarak kablosuz ağ sisteminin güvenliğine zarar vermeye çalışan saldırganlara karşı karmaşık olmayan bilinçli hamlelerle güvenliğini sağlayabileceğini rahatlıkla söyleriz.

Bir Remote Hijack Saldırısı Örneği

Belirli güvenlik önlemlerini almadığımızda ne kadar etkilenebiliriz ve yıkımları neler olur, bir saldırı örneği üzerinden inceleyelim.



CVE-2019-19494 olarak izlenen ve Cable Haunt ismiyle bilinen bir modem saldırısının yarattığı güvenlik açığının yakın zamana kadar Avrupa'daki neredeyse tüm kablolu modemleri etkilediği ve birçoğunun hâlâ risk altında olduğu düşünülmektedir.

Siber dünyanın dikkatini çekmeyi başarmış bu saldırının Danimarka merkezli güvenlik danışmanlığı yapan Lyrebirds tarafından araştırılıp ve raporlanması sonucu hemen harekete geçildi. Ancak yalnızca Avrupa'da tahminen 200 milyon kablolu modem olduğu ve Firmware güncellemesi olmadan güvenli olarak test edilen neredeyse hiçbir kablolu modem olmadığı için savunmasız modemler tahminen saptandı. Sorundan haberdar edilin kim, sorunu çözmek için kime ürün yazılımı gönderiliyor? Her iki durumda da dünya çapında hâlâ savunmasız modemlerin bulunduğundan şüphelenilmeye devam ediliyor.

Peki 200 milyon civarı modemın güvenliğini tehdit eden saldırıya zemin hazırlayan hata nerede bulundu? Cevap ise biraz şaşırtıcı: Yarı iletken şirketi Broadcom tarafından yapılan çipler üzerinde spektrum analiz aracını çalıştıran referans yazılımında. Yani olayı basit bir dile indirirsek birkaç parça kod metni milyonlarca insanın güvenliğini tehlikeye attı. Ayrıca çipin kullanımının bu kadar yoğun olması saldırının etki alanını daha da genişletti, çünkü spektrum çözümleyici yerel ağa maruz kalsa da saldırganlara dünyanın herhangi bir yerinden uzaktan erişim için Cable Haunt'lı kötüye kullanabilme imkânı verdi.

Saldırı süreci, kurbanların kötü niyetli JavaScript kodu sunan bubi tuzağına sahip (booby-trapped) bir web sitesine çekilmesiyle başlatılıp bir WebSocket bağlantısı aracılığıyla uzaktan kod yürütülmesine karşı savunmasız olduğunun keşfedilmesiyle devam etti. Ardından gelen arabellek taşması saldırısı, tehdit aktörlerinin modeme erişmesini sağlarken bilgisayarda bulunan tarayıcı güvenlik mekanizmaları ise bir DNS yeniden bağlama saldırısı ile başarıyla atlatılıp tamamlandı.

Genel olarak bu saldırı, websocket istemcisinin uygun şekilde yetkilendirilmemesi, varsayılan kimlik bilgileri ve spektrum analizöründeki bir programlama hatası nedeniyle mümkün kılındı denilebilir. Bu güvenlik açıkları, bir saldırganın tüm birim ve üzerinden akan trafiği uzaktan kontrol imkânı sağladı ve hem kullanıcı hem de ISS için görünmez olabilme, uzaktan sistem güncellemelerini görmezden gelebilme gibi büyük hatalara yol açtı.

Teknik görünen saldırı, kullanıcı güvenliğini nasıl tehdit eder?

Cevap çok basit: DNS ayarlarında değişiklik yaparak, modem belleğini değiştirerek, cihazları bir botnet'e bağlamak veya özel bilgileri ele geçirmek için uzaktan Ortadaki Adam (MitM) saldırıları gerçekleştirerek...



Bu riski şöyle ele alalım; Ortadaki Adam olarak tanımlanan saldırılarda istismarcı, kurban ve gerçek sunucu arasına yerleşir ve kullanıcıyı aslında hep kullandığı siteleri gezindiğine ikna ederek gönderdiği tüm bilgileri kendinde tutar; bunlar e-devlet şifresi, kart ve kimlik bilgileri, herhangi bir sitede kullanılan herhangi bir bilgi olabilir.

Korkunç değil mi?

Neyse ki güvenlik araştırma ekibi, hızlıca savunmaya geçti ve bir kavram kanıtı (POC) açığı oluşturdu, bunu çeşitli kablo modemlerdeki birden çok aygıt yazılımı sürümüne karşı başarıyla test etti ve güvenlik açığı olduğu onaylanan modemlerin ve donanım yazılımı sürümlerinin listesini “cablehaunt.com” web sitesinde raporladı.



Ayrıca kullanıcıların belirli kablo modemlerinin tehlide duyarlı olup olmadığını kendilerinin kontrol etmelerini sağlayan POC kodunu da kullanıma açtı. Araştırmacılar mümkün olduğu kadar çok sayıda en büyük İSS'yi ve üreticiyi bilgilendirdiklerini de söylediler. Kullanıcılar ise güncellemeleri takip etmeye yönlendirildi. Bu arada BankInfoSecurity, Broadcom'un şirketin referans kodunda ilgili düzeltmeyi yaptığını ve bu düzeltmenin Mayıs 2019'da müşterilere sunulduğunu söylediğini de aktardı. Sonuç olarak araştırmacılar, kullanıcıların ve üreticilerin aslında Cable Haunt'ı kötüye kullanan gerçek vahşi saldırıların farkında olmadıklarına dikkat çekti. Bu gösteriyor ki tüm bu saldırı süreci aslında biraz bilgisizliğin sonucuydu ve gerisi çorap söküğü gibi devam etti.

Ve çıkarabileceğimiz ders de şu olmalı: Güvenlik açığı oluşması tamamen kullanıcı sorumluluğunda olmasa da kullanıcının tutumu oldukça etkilidir.

```
docker run -it --rm cable-haunt-vulnerability-test sh  
vi test.py  
pipenv run python test.py
```

Saldırı mağdurlarının kullanması için geliştirilen Python kod parçası

Neler Yapılmalı?

Modem ve cihaz güvenliğini, dolayısıyla bütün olarak kablosuz ağ güvenliğini sağlamak için bir kullanıcı ne gibi önlemler alabilir?

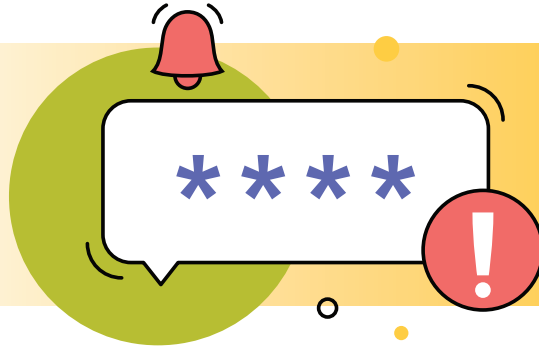
İlk olarak temel düzeyde cihaz şifresinin basit ve tahmin edilebilir olmaması ve cihaz kullanılmadığı takdirde kablosuz ağ



(Wi-Fi) özelliğinin kapalı tutulmasından başlanabilir, bunlara dikkat etmek kullanıcıyı habersiz bir durumda saldırıya uğramaktan büyük ölçüde korur. Daha sonra çok bilinen bir önlem olarak yönlendiricideki iki önemli parolayı da değiştirmekte fayda vardır, ilki aygıtın ayarlarını yönetmenize izin veren parola ve ikincisi diğer aygıtları kablosuz ağa bağlamanıza olanak veren paroladır. Bunların dışında tabii olarak hassas bilgilerin özellikle şifrelenmesi de gerekir. Genellikle yönlendiriciler aygıtı kurmak için varsayılan parolalarla birlikte gönderilir hatta parolalar yönlendiricinin üzerindeki bir etikete bile yazdırılır. Üstelik kolaylık sağlamak için birçok yönlendiricinin varsayılan parolaları da çevrimiçi olarak görünür ve herkesin bu kadar kolay ulaşması güvenlik açısından kullanıcıyı çıkmaza sokabilir.

Örneğin kullanıcı; komşusunun küçük bir çevrimiçi dedektifiği sonucu ağına erişmesinin ve potansiyel olarak yönlendiriciyi kontrol etmek için varsayılan basit parolayı kullanmasının sonucunda parolaları değiştirilmiş, çevrimiçi eylemleri gözetlenmiş veya ağa bağlı bir sabit sürücüdeki dosyalarına erişilmiş bir kurban konumuna düşebilir. Bunu önlemek için ayarlar ve bağlantı şifreleri, yönlendiricinin mobil uygulaması veya ayarlar sayfası (diğer adıyla 192.168.1.1) aracılığıyla değiştirilebilir. Dikkat edilmesi gereken kısım, oluşturulan parolanın güçlü ve benzersiz, yani birbirinden ve kullanılan diğer parolalardan farklı olduğundan emin olmaktır.

Uygun, güçlü ve güvenli bir şifrenin karmaşık olması gerekir; en az sekiz karakter uzunluğunda, büyük ve küçük harflerin (A, B, C, D, 1,2,3,-,*!,e, f, G, H, J, K, L ve M) karışımını içeren bir şifre kullanmak oldukça önemlidir. Ayrıca Wi-Fi kullanıcı adı ve şifresi değiştirilse de modem arayüzündeki varsayılan kullanıcı adı ve şifreyi değiştirmeye de dikkat edilmesi gerekir. Bunlar dışında en azından cihazla gelen karmaşık şifreyi doğum tarihinizle değiştirmemek de temel seviyede bir önlemdir.



Parola ve fiziksel önlemlerin dışında neler yapılır?

Yine nispeten basit bir hamle olarak cihaz sürücülerinin güncel tutulması da büyük önem taşır. Eğer yönlendirici otomatik güncellemeler sağlamıyorsa kullanıcı yeni bellenimi(firmware) üreticinin web sitesinden düzenli olarak indirip yüklemelidir. Çünkü en güncel tehlikelerden ancak en güncel savunma araçlarıyla korunulur, bu da siber güvenlikte önceliği güncellemeye vermektir.

Loading



Güncelleme sıklığı değışmekle birlikte tüketici raporlarında elektronik test denetçisi Richard Fisco, güvende olmak için en az üç ayda bir yeni güncellemeleri kontrol etmek gerektiğini söylemektedir. Ancak doğaldır ki tüm şirketler eninde sonunda eski modeller için yeni yazılım yayımlamayı bırakır. Fisco bu durumlar için yönlendiricinin artık güncelleme almadığı fark edilirse kullanmaya devam etmenin çok riskli olduğunu belirtmiştir ve durumu üretici ile doğrulayıp ömrünün sonuna gelmiş yönlendiriciyi yenisiyle değiştirmeyi önermektedir. Bu tarz önlemlere virüs yazılımı ve güvenlik duvarının aktif tutulması da eklenebilir.

Ayrıca büyük bir kitleye açık şifresiz ağlara bağlanmaktan -örneğin özel şifrelenmemiş kurumsal ağlar- ve bu ağlar üzerinden bilgi göndermekten kaçınmak, bağlanılsa bile hemen listeden silmek ve SSL sertifikalı siteleri tercih etmek de önemli adımlardır. Ücretsiz ve kolaylıkla bağlanılabilen kablosuz ağlar iyi niyetli görünse de kuruluş amacının insanların modem ağına katılmasını sağlayarak cihazlarına sızma olabileceği de göz önünde bulundurulmalıdır.

Moderni gizlemek başlığı altında toplanabilecek bir dizi önlem yukarıda bahsedilenlere kıyasla biraz daha üst düzey güvenlik önlemleridir.

İlk olarak şifresiz misafir ağını iptal ederek başlanıp kablosuz özelliği sağlayan donanımın kaynak paylaşım özelliği ve kablosuz Ad-Hoc özelliği kapatılarak tehlike riski azaltılır. Daha gelişmiş bir önlem olarak modem arayüzünden MAC adresi filtrelemesi yapılması çok etkili bir savunmadır.

MAC adres kontrolü, yabancı kullanıcıların şifreyi kırsa bile MAC adreslerinin modemde kayıtlı olmaması nedeniyle erişimini engellemeyi sağlar.

Bu şekilde kullanıcı sadece kendisine ve güvenilir kişilere ait cihazlara erişim izni vermiş olur ve diğer riskleri direkt olarak ortadan kaldırır, bu yüzden alınabilecek en etkili önlemlerden biri MAC adres listesi oluşturmaktır.

Moderni gizlemek adına kritik bir işlemten daha bahsedilebilir:

SSID adının değiştirilmesi ve gizlenmesi. Varsayılan SSID adı yönlendiricinin marka ve modelini ortaya çıkarır ve varsayılan şifrenin de tahminini kolaylaştırarak potansiyel saldırı riski taşır.

Ama burada esas olan en iyi önlem SSID adının gizlenmesidir, çünkü kablosuz ağ arayan hiç kimse ilk kez bağlanmak amacıyla moderni ve bağlantı adını görüntüleyemez, böylece MAC adresi filtresinden daha kesin bir çözüm sunar.

Yeni bir cihaz aracılığıyla kablosuz ağa bağlanmak manuel giriş gerektirse de üst düzey bir güvenlik için göze alınması mantıklıdır.

Ek olarak aynı ağa bağlı cihazların birbirine de bağlanmasını sağlayan UPnP özelliği de çoğu modemde varsayılan ayar olarak kuruludur fakat kapatılmasında fayda vardır. Sağladığı kolaylığın taşıdığı güvenlik riskine değmediği düşünülmekte ve herhangi bir zararlı yazılımın ağa yayılmasını kolaylaştırdığı için kullanımı tavsiye edilmemektedir.

Bir diğ er tavsiye edilmeyen  zellik de hem kablosuz hem kablolu ađ bađlantısını aynı anda (bridge mode) kullanmaktır.

Bu gibi  zelliklerin kolaylık sađladığı d   n lse de y ksek risk ta şmaları i lem g venilirliğini azaltmaktadır.

Son olarak yukarıda bir  rneđi de incelenen uzaktan y netimle saldırı ihtimalinin ortadan kaldırılması i in modem ve/veya y nlendiricilerin uzaktan y netim -WAN'dan web eri imini olarak da bilinir  zelliđinin  ok gerekli deđilse modem aray z nden kapatılması g venlik amacıyla uzmanlar tarafından  nerilmektedir, b ylece ađın dı ından y nlendiricinin kontrol paneline eri im engellenir.

G venlik protokol  olarak g n m zde WPA3 kullanımı  nerilir    nk  bilgisayar korsanlığı ara larının kullanımını zorla tırarak g ncel standartlara uygun bir koruma sađlamaktadır. Bunun haricinde WPA2-AES de kullanılabilir g r lmekte fakat WPA2 desteklemeyen cihazların kullanılması tavsiye edilmemektedir.

Peki t m bunlara dikkat eden bir kullanıcı yine de bir zafiyet sonucu saldırıya uđradığını d   n rse ne yapmalıdır?  ncelikle cihazı fabrika ayarlarına getirmek i in resetleyip  nlemleri ba tan itibaren adım adım izleyerek cihazını tekrar g venli h le getirilebilir ve bilin li bir ađ kullanıcısı olarak siber tehlikelerden kolaylıkla korunabilir.



KAYNAKÇA

<https://www.guvenliweb.org.tr/dokuman-detay/kablosuz-ag-modem-guvenligi>

<https://www.tp-link.com/tr/press/news/17973/>

<https://www.consumerreports.org/digital-security/ways-to-boost-router-security-a3824459325/>

<https://cablehaunt.com/>

<https://www.welivesecurity.com/2020/01/14/millions-modems-vulnerable-remote-hijacking/>

<https://github.com/Lyrebirds/cable-haunt-vulnerability-test>





ŞARJ KABLOLARI GERÇEKTEN GÜVENLİ Mİ?

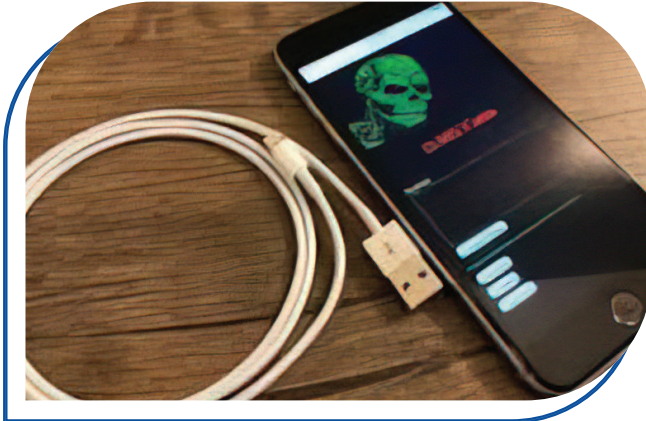
ŞARJ KABLOLARI GERÇEKTEN GÜVENLİ Mİ?

Hayatımızda internetin ve cep telefonlarımızın olmadığını hiç düşündünüz mü? Bu sorunun cevabına herkesin “Düşünemiyorum” diye verdiğini tahmin ediyorum. Çünkü artık telefonlarımız ve internet olmadan yaşayamaz olduk. Her saniye her ihtiyacımız olduğunda elimiz daima telefonumuza ve dolayısıyla internete gider. Kimi zaman bir bilgiyi öğrenmek kimi zaman ise sosyal medyaya girmek için... Kendimizi o kadar çok kaptırırız ki bir bakarız telefonumuzun şarjı biter.

Genelde telefonlarımızı şarj etmek için telefonu aldığımızda verilen orijinal şarj kablolarını kullanırız. Fakat zamanla bu şarj kablolarımız kullanım durumumuza bağlı olarak yıpranır, aşınır, kopar ya da kaybolur. Yeni kabloya ihtiyaç duyduğumuzda orijinal kabloların pahalı olması nedeniyle alternatif kablo arayışına gireriz. Nasıl olsa hepsinin kullanım amacı aynı, ne fark eder deriz.

Ancak asıl hikaye burada başlar. Aldığımız o sahte kablolar ile hack'lenebileceğinizi hiç düşündünüz mü? Fotoğraflarımız, maillerimiz, mesajlarımız, banka bilgilerimize kadar tüm verilerimizin korsanların eline geçtiğini düşünmek bile istemeyiz. Çünkü artık tüm hayatımız ve gizliliğimizi telefonlarımızda tutuyoruz.

Güvenlik araştırmacısı Mike Grover, modifiye ettiği kablo tasarımları ile kullanıcıların basit bir şekilde hack'lenebileceğini ortaya çıkarttı. Yapmış olduğu tasarımına OMG ismini vererek kabloların üretilmesini ve satılmasını sağladı. Bu kablolar normal hatta orijinal bir kablo gibi görünür ve kullanıcılar farkı anlayamaz. Kabloların içerisinde küçük bir çip ve hacker'ın bağlanabileceği Wi-Fi noktaları da mevcuttur.



Kullanıcılar şarj kablolarını taktıklarında hack'erler wi-fi noktaları üzerinden bağlantı sağlar, kötü niyetli yazılımları ilgili cihaza indirip cihazın tüm kontrollerini ve verileri ele geçirmiş olurlar ki bu verilere cihazların giriş şifreleri de dâhildir.

Örneğin Vice.com'da yer alan bir haberde orijinal Apple USB kablosu gibi görünen bir şarjkablosu ile hackerların bilgisayarları nasıl ele geçirebildikleri anlatıldı. Joseph Cox, kaleme aldığı yazıda konuyu şu ifadelerle dile getiriyor: "Apple'ın kablosunu iPod'uma taktım ve her zaman yaptığım gibi onu da Mac'ime bağladım. iPod'um şarj olmaya başlarken iTunes cihazı algıladı ve iPod'um bu bilgisayar güvenilir mi sorusunu sordu. Buraya kadar her şey gayet normaldi"

Fakat Cox'a göre söz konusu kablo bir sırrı gizlemektedir. Şöyle devam ediyor Cox: "Kısa bir süre sonra bir hacker uzaktan Mac ekranımda bir terminal açtı ve bilgisayarımda komutları çalıştırmalarını sağladı. Zira bu güvenilir bir kablo değildi. Aksine bir implant entegre edilmiş şekilde modifiye edilmiş kablonun içine yerleştirilen ekstra bileşenle korsanların bilgisayara uzaktan bağlanmasını sağlıyordu."

KAYNAKÇA

www.siberbulten.com - <https://siberbulten.com/dijital-guvenlik/sarj-kablosu-deyip-gecmeyin-bilgisayariniz-hackerlarin-eline-gecmis-olabilir/>
www.Vice.com
-<https://www.vice.com/en/article/3kx5nk/fake-apple-lightning-cable-hacks-your-computer-omg-cable-mass-produced-sold>
www.siberbasin.net - <https://siberbasin.net/sarj-kablolari-artik-cihazinizi-hacklemek-icin-kullanilabilir/>





MOBİL GÜVENLİK

Mobil güvenlik, akıllı telefonlar ve tabletler gibi mobil cihazlarda veri güvenliğini sağlama çabasıdır. Genellikle mobil güvenlik, cihazlarda kişisel bilgilerin korunması, güvenlik açıklarının kapatılması ve veri sızıntılarının engellenmesi üzerine odaklanır. Gelişen dünyayla birlikte teknolojik cihazların kullanımı artıkça cihazların güvenliğinin sağlanması giderek daha önemli bir konu hâline gelmiştir. Mobil güvenlik kavramını size Birleşik Krallık Siber Güvenlik Merkezi'nin paylaştığı 12 maddelik "Son Kullanıcı Cihazları Güvenlik Kılavuzu" kapsamında anlatmak isterim.

1.Yetkilendirme ve Doğrulama (Authentication): Kullanıcıların mobil cihazlara, hizmetlere ve cihazlardan hizmetlere erişimi sağlamak için üç farklı erişim türü vardır:

- 1. Kullanıcının Cihaza Erişimi:** Kullanıcılar, mobil cihazlarına erişmeden önce gerekli güvenlik protokollerini tamamlamalıdır.
- 2. Kullanıcının Servise Erişimi:** Kurumsal bir hizmete erişim için kullanıcılar cihazlarıyla servisin talep ettiği protokolleri tamamlamalıdır.
- 3. Cihazdan Servise Erişim:** Sadece erişim izni olan ve gereken protokolleri tamamlamış olan cihazlar, kurumsal hizmete erişebilir.

Tüm bu kimlik doğrulama adımları, kurumların istedikleri protokollere göre kullanıcılar tarafından uygulanabilir. Bu, kimlik doğrulama süreçlerinin birbirine entegre veya bağımsız olarak kullanılabilmesi anlamına gelir; güvenlik ve yetkilendirme gereksinimlerine uygun bir şekilde yapılandırılmalıdır.

2. Güvenli İşletim Sistemine Ulaşım (Secure Boot): Yetkisi olmayan herhangi bir donanım veya yazılımın cihazınızın işletim sistemine erişmeye çalışması engellenmelidir. Herhangi bir erişim girişimi tespit edilmelidir.

3. Platform Bütünlüğü ve Application Sandbox: Cihazınız, bir uygulamanın cihaz içinde potansiyel bir tehdit oluşturması durumunda güvenli bir şekilde

çalışmaya devam etmelidir. Ayrıca cihazınızdaki uygulamaların yeteneklerini sınırlayabilmelisiniz.

4. Güvenli ve Yetkilendirilmiş Uygulamalar (Application Whitelisting):

Cihazınızda hangi uygulamaların çalışabileceği ile ilgili bir beyaz liste oluşturmalsınız ve sadece bu uygulamalara izin vermelisiniz.

5. Zorunlu Güvenlik Politikaları: Kurumlar tarafından belirlenmiş olan güvenlik politikaları, cihazlara etkin bir şekilde iletmeli ve uygulanmalıdır. Bu politikaları değiştirmemelisiniz. Güvenlik politikaları, kurumlar tarafından dikkatle hazırlanmış olup sizin güvenliğiniz için tasarlanmıştır.

6. Hareket Hâlindeki Verinin Korunması (Data in Transit): Cihazınızdan kuruma giden veya kurumdan cihazınıza gelen verinin bu süreçlerde korunması, verilerinizin güvenliği için büyük bir öneme sahiptir.

7. Cihazdaki Verinin Korunması (Data at Rest): Cihazınızda bulunan verilerin şifrelenmiş olarak korunması son derece önemlidir. Bu sayede verileriniz güvende olur.

8. Zararlı Yazılım Tespiti ve Engellenmesi: Mobil cihazınız herhangi bir zararlı yazılımı algılamalı, izole etmeli ve erişimini engellemelidir. Bu amaçla gerekli politikaları ve önlemleri cihazınıza etkin bir şekilde uygulamalısınız.

9. Cihaz İşletim Sistemi Güncelleme: Cihazınızı güncel tutmalı ve yeni güvenlik yamalarını yüklemelisiniz. Bu sayede cihazınız, yeni tehditlere karşı daha güvenli bir şekilde korunmuş olur.

10. Veri Analizi ve Durum Raporu: Kurum içinde bulunan cihazlarımız, güvenlikle ilgili tüm önemli durumları raporlamalı ve bu raporlar, ilgili kurum birimleri tarafından düzenli olarak incelenmelidir. Böylece cihazlarda meydana gelebilecek sorunlar kurum tarafından çözülür.

11. Harici Arabirim Koruma/Engelleme: Cihazınız, güvenilmeyen ağlara veya cihazlara karşı koruma sağlamalı ve potansiyel güvenlik tehditlerini önlemelidir. Bu tür yazılımların neden olduğu riskler çok ciddi olabilir.

12. Sorun Giderme & Hazır Olma: Cihazınızda herhangi bir güvenlik ihlali durumunda ortaya çıkabilecek sorunları ve bu sorunların çözümünü önceden belirlemeniz gerekmektedir.

MOBİL CİHAZ GÜVENLİĞİ (MDM, MOBILE DEVICE MANAGEMENT) NEDİR?

Mobil cihaz güvenliği farklı işletim sistemleri ile çalışan akıllı telefonlar, tablet ile dizüstü bilgisayarlar gibi mobil cihazların genel olarak cihaz, içerik, uygulama ve güvenlik açısından uzaktan izlenmesi, güvenliğinin sağlanması, yönetilmesi ve desteklenmesini sağlayan yazılımsal bir mobil cihaz güvenliği sistemidir. Bir MDM sistemi genellikle aşağıdaki bileşenlerden oluşur:

1. Mobil Cihaz Güvenliği (Mobile Device Management, MDM): Cihazın güvenliği ve yönetimi, kullanıcı güvenliği.

2. Mobil Uygulama Yönetimi (Mobile Application Management, MAM): Mobil cihazlardaki uygulamaların yönetimi ve güvenliği.

3. Mobil İçerik Güvenliği (Mobile Content Management, MCM): Mobil belge, veri ve içerik güvenliği ile güvenli web tarayıcı uygulaması.

4. Mobil E-Posta Yönetimi (Mobile E-Mail Management, MEM): Kurumsal e-postaların güvenliği ve güvenli e-posta uygulaması.

5. Kişisel Cihaz Yönetimi (Bring Your Own Device, BYOD): Çalışanların kendi mobil cihazlarıyla kurumsal kaynaklara ve uygulamalara güvenli erişimini sağlama.

MOBİL CİHAZ GÜVENLİĞİ SİZE NEYİ SAĞLAR VE İHTİYAÇ NASIL BELİRLENİR?

Mobil cihaz güvenliği, farklı işletim sistemleri (örneğin iOS, Android, Windows Mobile, BlackBerry) ile çalışan akıllı telefonlar, tabletler ve dizüstü bilgisayarlar gibi mobil cihazların yönetimi ve güvenliğini sağlayan bir yazılım sistemidir. Bu sistem, mobil cihazların güvenlik kapasitelerini artırmak ve kullanımını kolaylaştırmak için cihazlar arasında belirli protokollerle iletişim kurabilir.

Mobil cihaz güvenliğinde, aynı işletim sistemine sahip farklı üreticiler arasında bile güvenlik kapasiteleri açısından ciddi farklılıklar olabilir. Bu nedenle bir mobil cihaz güvenlik sistemi seçerken, hangi platformda ve hangi cihaz türünde kullanacağınızı belirlemeli ve güvenlik amaçlarınızı net bir şekilde tanımlamalısınız.

KAYNAKÇA:

<https://tr.theastrologypage.com/mobile-security>

<https://www.linkedin.com/pulse/mobil-cihaz-g%C3%BCvenli%C4%9Fi-klavuzu-12-temel-prensip-abdullah-diltemiz/?originalSubdomain=tr>

<http://www.sibergah.com/uc-nokta-guvenligi/mobil-guvenlik/kurumlarda-mobil-cihaz-guvenligi-mdm/>

https://en.wikipedia.org/wiki/Mobile_device_management

<https://www.gartner.com/doc/2757817/magic-quadrant-enterprise-mobility-management>





WINDOWS PHONE GÜVENLİĞİ

Windows Phone Güvenliđi

Windows Phone, Microsoft tarafından geliştirilen ve Windows Mobil işletim sistemine son verildikten sonra sisteme geçen mobil işletim sistemidir. 2008'de, Microsoft Windows Mobile ekibini bir araya getirmiş ve Windows Mobile dışında yeni bir işletim sistemi geliştirilmesi için çalışmalara başlamıştır.

Yeni işletim sistemi olan Windows Phone, 2009 yılında duyurulmak istenmiştir ama geliştirme sürecindeki gecikmelerden kaynaklı olarak Microsoft, ara sürüm olarak kabul edilen Windows Mobile 6.5'i geliştirmiş ve duyurmuştur. Windows Phone, 15 Şubat 2010 tarihinde Barcelona'da düzenlenen Mobil Dünya Kongresi'nde resmi olarak tanıtılmıştır. Windows Phone çok hızlı geliştirilince eski Windows Mobile uygulamalarıyla uyumlu çalışmamıştır. 16 Eylül 2010 tarihinde final yazılım kiti yayımlanmıştır. Sonrasında Windows Phone işletim sistemine sahip cihaz üretmek yerine WebOS işletim sistemiyle devam etmişlerdir. Windows Phone işletim sistemi kullanıldığı sürece 6 sürüm kullanılmıştır.

Bunlar sırasıyla şöyledir:

Windows Phone 7 sürümü - 21 Ekim 2010

Windows Phone 7.5 sürümü - 27 Eylül 2011

Windows Phone 7.8 sürümü - 1 Şubat 2013

Windows Phone 8 sürümü - 29 Ekim 2012

Windows Phone 8.1 sürümü - 15 Temmuz 2014

Windows Phone 10 sürümü - 20 Kasım 2015

1. Windows Phone Cihazları

Windows Phone 7.0 Cihazları

2010 yılında tasarımsal değişiklikler yapılarak birinci nesil cihazlar Windows Phone 7 ile gelmiştir. Windows Phone 7'de Metro UI arayüzü kullanılmıştır. Windows Phone 7'de uygulama geliştirme yöntemleri kullanılamamaktadır; gerekli olan geliştiriciler HTML 5 ve Native desteđi bu işletim sistemine uyumlu değildir.

Windows Phone 7.5 Cihazları

Windows Phone 7.5 Mango sürümü 2011 yılında piyasaya sürülmüştür.



Windows Phone 7.8 Cihazları

2013 yılında Microsoft, Tango güncelleştirmesiyle Windows Phone 7.8'i açıklamıştır.

Windows Phone 8.0 Cihazları

2012 yılında, Windows Phone işletim sisteminin ikinci nesli olan Windows Phone 8 açıklanmıştır. Microsoft, Windows Phone 7'de olan Modern UI 'ye benzer olan Windows 8 Core yapısını yerleştirmiştir. Windows Phone 8 ile Windows 8 kullanım açısından benzerdir.



Şekil 1: Windows 8 ve Windows Phone 8

Dev Center, Windows Phone uygulamaları için oluşturulan mağazayken Windows Store, sadece Windows Phone 8 uygulamalarına ait bir mağazadır. Bu ayrılığın olmasının nedeni uygulamaların hepsi Windows Phone 8'de aynı şekilde çalışmamaktadır. Ayrıca Windows 7'de uygulama geliştirme yöntemleri kullanılamadığından bahsetmiştik ama Windows Phone 8, HTML 5 VE Native desteği sunularak uygulama geliştirme yönetimlerini kullanabilecek hâle gelmiştir.

Windows Phone 8.1 Cihazları

Windows Phone 8.1 Windows Phone işletim sisteminin üçüncü neslidir. 2014 yılında Microsoft'un bir kongresinde tanıtılmıştır. Windows Phone 8 sürümünü çalıştırabilen tüm telefonlar Windows Phone 8.1'e de yükseltilebilmiştir.

Windows Phone 10 Cihazları

Windows Phone 10, Microsoft tarafından şimdiye kadarki en kapsamlı platform olarak 2015 yılında açıklandı. Ayrıca Windows Phone 10 uygulamaları Windows Store'da yayımlanmıştır.

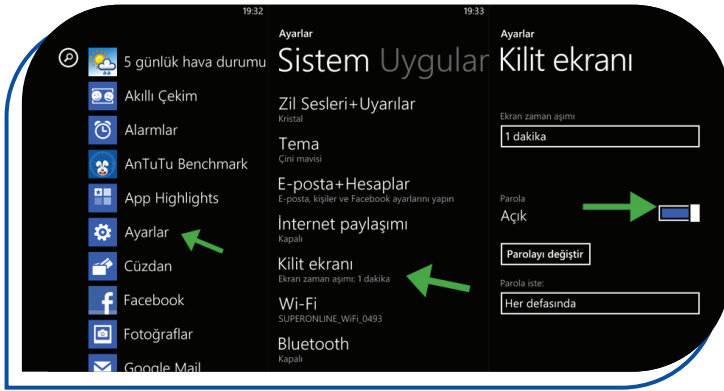
Windows Phone Güvenliđi

Mobil telefonların güvenliđi, akıllı telefonların kullanımının her geen gn artmasıyla daha da nemli hle gelmektedir. Akıllı telefonlar kiřisel kullanımlar dıřında hassas veri ieren banka iřlemlerinde, iř yeri iin olan verileri depolamak gibi pek ok alanda kullanılmaktadır.

Son zamanlarda mobil cihazlarda tehditler, sanal saldırılar ok yaygınlařmıřtır. Akıllı telefonlarının bu řekilde kullanılmasıyla, mobil güvenliđin de sađlanması zorunlu hle gelmiřtir. Bu güvenliđi sađlamak iin de mobil cihazın sahip olduđu iřletim sisteminin bazı kısıtlamalar koymas, kt amalı uygulamaları ve veri dosyaları tespit etmek gibi bazı nlemler alması gerekmektedir.

Telefonda řifre/PIN ayarlaması yapılmalı.

Telefonun kaybolması ya da izinsiz kullanılması durumuna karřı řifre/PIN ayarlaması yapılmalıdır. Bu ayarlama sırasıyla řu řekilde yapılmaktadır:



ncelikle ayarlar kısmından sistem uygulamasına gidilmeli ve oradan kilit ekranı seilerek bir řifre ayarlanmalıdır. Burada seilen řifre herkesin kolayca bulacađı ya da tahmin edebileceđi bir řifre olmamalıdır.

Telefonun kaybolması durumunda sorun yařamamak iin gerekli uygulama indirilmeli.

Windows Phone iřletim sistemine ait olan "Telefonumu bul" uygulaması indirilmelidir. Bu uygulama Windows Phone 8 ve st srmlerde kullanılabilir. Bu uygulamayla telefonun alınmıř veya kaybolmuř telefona uzaktan eriřimle verileri uzaktan kilitleme ve silme, hatta cihaz bulma zelliđi ile korur. <http://www.windowsphone.com/tr-tr> 'den indirilebilir.

Telefonun güvenlik ayarları değiştirilmemeli.

Telefonun fabrika ayarlarının ya da işletim sistemi ayarlarının değiştirilmesi telefonu saldırılara karşı daha açık hâle getirir. Ayrıca telefon tarafından sunulan güvenlik özellikleri zayıflatılmış olur.

Telefondaki veriler yedeklenmeli.

Telefonda bulunan bütün verilerin yedeklenmesi tavsiye edilmektedir. Bu verileri kişisel bilgisayarlarda, harici depolama aygıtlarında saklanabilir. Böylece oluşabilecek herhangi çalınma, kayıp durumunda verilerin güvenliğini sağlamış olur.

Yedekleme işlemi ise şu şekilde yapılır:

Ayarlarda sistem seçilir ve yedekleme ayarları kısmından yedekleme işlemi ayarlanabilir.

Uygulamaların yükleneceği kaynağa dikkat edilmeli.

Bir uygulamayı indirmeden önce, yasal ve güvenilir olup olmadığına bakılmalı. İndirilen uygulamalar, işletim sisteminin resmi olan Windows Store ya da Dev Center uygulama alanından indirilmelidir. Dev Center'dan indirilen uygulamaların da dikkatli bir şekilde incelenmesi gerekir. Ek olarak uygulamaları indirdikten sonra verilen izinlere karşı dikkatli olunmalı ve yüklenmeden önce uygulamalar için gizlilik ayarları kontrol edilmelidir.

Yazılım güncellemeleri özenle takip edilmeli.

Telefonun işletim sistemi güncel tutulmalıdır. İşletim sistemini güncel tutarak siber tehditlere karşı önlem alınmış olunur.

Gelebilecek zararlı bir içerik gelmesi durumunda buna karşı önlem alınmalı.

Cihazdaki uygulamalar ve ziyaret edilen yerlerden gelebilecek zararlı içeriklere karşı antivirüs yüklenmelidir. Güvenlik duvarı (firewall) yüklenmelidir.

KAYNAKÇA

https://tr.wikipedia.org/wiki/Windows_Phone
https://www.trendmicro.com/tr_tr/business/products/user-protection/sps/mobile.html
https://tr.wikipedia.org/wiki/Mobil_g%C3%BCvenlik
https://tr.wikipedia.org/wiki/Windows_10_Mobile
https://tr.wikipedia.org/wiki/Windows_Phone_8
<https://tuketici.btk.gov.tr/tuketici-icin-akilli-telefon-guvenlik-ipuclari-guncellendi>
<https://www.enkisa.com/windows-phone-8-kilit-ekranina-sifre-koyma-21606.html>
<https://www.gigasoft.com.tr/mobil-cihaz-guvenligi-ve-yonetimi/>





BLOCKCHAIN NEDİR VE NASIL ÇALIŞIR?

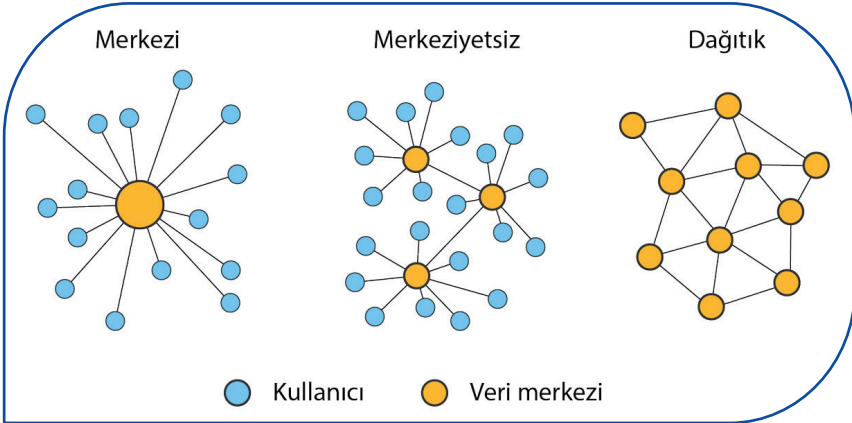
“Blockchain: Teknoloji Uzayında Yeni Bir Yıldız, Ama Ne Kadar Güvende?”

Kripto paraların altın çağı tüm hızıyla devam ediyor. Herkes Bitcoin, Ethereum ve benzerlerini konuşuyor. Ancak bu dijital para birimlerinin arka planında yer alan ve tüm bu büyümlü dünyayı yöneten asıl kahraman blockchain teknolojisi. Tamamen şeffaf, merkezi olmayan ve genellikle hacklenemez olarak tanımlanan bu teknoloji, modern finansın geleceği olabilir mi? Öte yandan, bu yeni teknoloji güvenlik konusunda gerçekten sarsılmaz bir kale mi? Gelin birlikte bakalım.

Blockchain: Dijital Çağın Açık Defteri

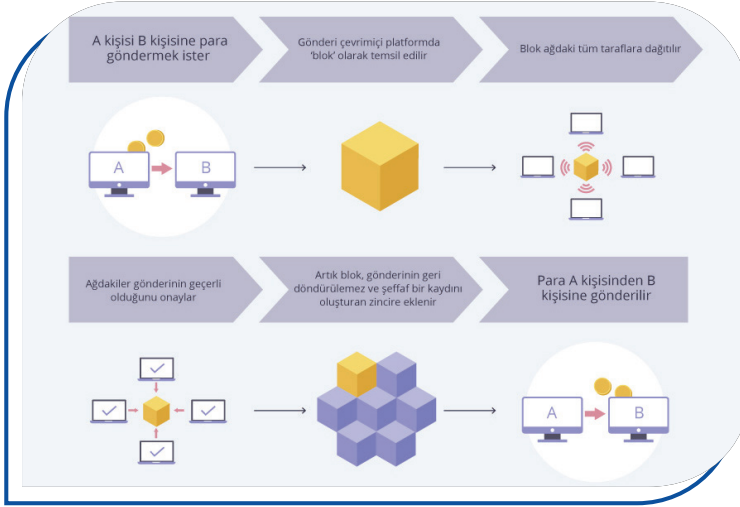
Blockchain, esasen bir tür merkeziyetsiz, dağıtık ve aynı zamanda genel incelemeye açık olan özel bir veri tabanıdır. Birbirini takip eden bloklarla oluşturulan bir veri zinciri ve bu zincirin her bir halkası, önceki halkaya atıfta bulunur. Blockchain’de yapılan her işlem, bu büyüleyici veri zincirinin bir parçası olur.

Merkezi, merkeziyetsiz ve dağıtık terimleri bizim için önemli, bu nedenle görselle daha iyi anlaşılabilceğini düşündüm.



Blockchain Nasıl Çalışır?

Blockchain’de işlemler, bloklar hâlinde saklanır ve her yeni oluşturulan blok, kendisinden önceki bloka atıfta bulunan bir kimlik numarası, yani “hash” ile



işaretlenir. Bu bloklar bir zincir oluşturur ve bu yapıya “blok zinciri” adı verilir. Bu zincir sürekli olarak büyür ve uzar.

Güven unsurunu sağlamak için Bitcoin gibi blok zincirlerinde işlemler, ağıdaki özel bir bilgisayar türü olan madenci tarafından doğrulanmadan bloka eklenmez. Bu şekilde topluluk, hileli bir işlemin blok zincirine kaydedilmesini engeller. Blockchain sistemi, adaptasyon sağlayabilen cihazlar tarafından oluşturulur. İşlemler, bu anonim cihazlar aracılığıyla gerçekleştirilir ve dış müdahâlelere tamamen kapalıdır. Blockchain, diğer internet sistemlerinde olduğu gibi verilerin tek bir merkezde toplanması yerine birden fazla cihaza veya bilgisayara dağıtılarak çalışır.

Bu sayede, dışarıdan yapılabilecek tüm müdahâleler engellenir. Blockchain veri tabanı, yalnızca kullanıcılarına değil herkese açıktır. Bu da kontrolün şeffaf bir şekilde gerçekleştirilmesini sağlar. Bir blok içinde kaydedilen işlemler, cüzdan adresleri, işlem kimlikleri (transaction ID) ve miktarlar, herkes tarafından kontrol edilebilir.

Dijital Kalesi mi, Açık Hedefi mi?

Siber saldırılar arttıkça, blockchain teknolojisi hakkındaki endişeler de doğal olarak artıyor. Her ne kadar bu teknoloji, genellikle hacklenemez olarak tanımlansa da aslında bir dizi saldırı türüne karşı hassas olabilir. Ancak endişelenmeyin, blockchain teknolojisinin arkasında birçok güvenlik önlemi bulunuyor ve bu önlemler, çoğu saldırıyı etkisiz hâle getirebiliyor.

Saldırı Türleri: Bilgiyi Güç Yapmak

Blockchain üzerinde gerçekleştirilebilecek saldırılar nelerdir? Hackerlar ve siber suçlular, blockchain teknolojisinin güvenlik zafiyetlerini manipüle ederek hasar verebilirler. İşte hackerların dört ana yöntemi:

Yönlendirme saldırısı, %51 saldırısı, Sybil saldırısı ve kimlik avı saldırısı. Bu saldırıları anlamak, blockchain teknolojisinin güvenlik zafiyetlerini daha iyi anlamanıza ve buna göre önlem almanıza yardımcı olabilir.

1. Yönlendirme Saldırısı: Blok zincirleri, gerçek zamanlı olarak gerçekleştirilen büyük veri transferlerine bağlıdır. Becerikli hackerlar, ISP'lere (İnternet Servis Sağlayıcıları) giderken verileri yakalayabilir.
2. %51 Saldırısı: Eğer bir grup etik dışı madenci, bir blok zinciri ağının madencilik gücünün %50'sinden fazlasını elde ederse defter üzerindeki kontrolü ele geçirebilir.
3. Sybil Saldırısı: Sybil saldırıları, hedef ağı çok sayıda sahte kimlikle doldurarak sistemi çökertir.
4. Kimlik Avı Saldırısı: Bu klasik hacker taktiği, blockchain ile de çalışır. Kimlik avı, siber suçluların cüzdan sahiplerine kimlik bilgilerini soran yanlış ancak ikna edici görünen e-postalar gönderdikleri bir aldatmacadır.

Blockchain Güvenlik Duvarı: Yardımcı Araçlar

SWC, MythX, Echidna, Manticore, Oyente gibi birçok test aracı, blockchain teknolojisinin güvenliğini sağlamak için kullanılıyor. Bu araçlar, verilerin güvenliğini korumak için hayati öneme sahip ve siber suçlulara karşı güçlü bir direniş sağlıyor.

Sonuç olarak blockchain teknolojisi, çağımızın en büyüleyici ve en çok tartışılan teknolojik yeniliklerinden biri.

Her ne kadar bazı güvenlik zorlukları olsa da, doğru araçlar ve bilgi ile bu teknoloji, dijital dünyamızda daha güvenli ve şeffaf bir geleceğin anahtarı olabilir.

KAYNAKÇA:

(<https://www.bitpanda.com/academy/tr/dersler/blockchain-nedir>)

(<https://tedmem.org/mem-notlari/degerlendirme/egitimde-blokszincir-teknolojisi>)





DİJİTAL HAYAT

Dijital Hayat

Teknoloji gelişmesini ilk çağdan bu yana devam ettirmektedir. Gittikçe hızlanan ve genişleyen bu gelişme süreci, hayatımızın da her alanına girmiştir. İnsan hayatına doğrudan dâhil olan dijitalleşme gün geçtikçe normalleşmektedir. Artık hemen hemen herkesin dünyaya açılan kapısı olan akıllı telefonlar, hayatın dijitalleşmesinin en önemli yardımcılarındandır.

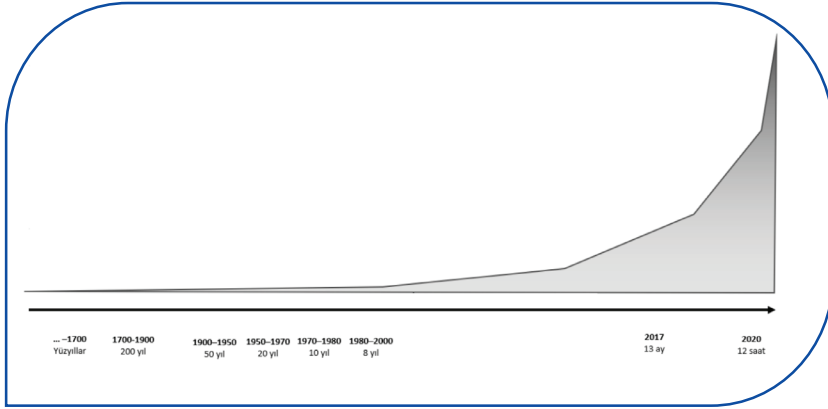
Toplumsal hayatın neredeyse tüm alanlarında yaşanan dijitalleşme dönüşümüne hep birlikte tanıklık ediyoruz. Bu dönüşümle birlikte hayatımıza; sosyal platformlar, dijital bankacılık, sanal cüzdanlar, çevrimiçi alışveriş gibi birçok yeni kavram girmiştir. Her gün yeni kavramlar ve alanlar türeyerek dijital hayata dâhil olmaktadır.

Ekim 2022 itibarıyla 7,99 milyar dünya nüfusunun %68,6'sı mobil telefon kullanıcısı, %63,5'i internet kullanıcısı ve %59,3'ü sosyal medya kullanıcısıdır. Dünya genelinde her gün 1 milyondan fazla yeni sosyal medya kullanıcısı sisteme dâhil olmaktadır (We Are Social, 2022).

Dijital ortamda artan kullanıcı sayısı, erişilebilir bilginin katlanarak artışı beraberinde getirmiştir. İnternete bağlı hemen her cihazdan bilgiye ulaşılabilir olması, yeni bilgilerin kolay bir şekilde yayılmasına ve çoğalmasına yardımcı olmaktadır. Bu durum bilginin sürekli bir döngüde bulunmasını, sürekli olarak yeni kişilere ulaşmasını sağlar. Buckminster Fuller'in "Bilgi katlanma eğrisi" (Şekil-1) grafiği bilginin zamanla kümülatif artışı net bir şekilde göstermektedir.

İnsanoğlu yapısı gereği etrafındakiler ile iletişime geçme ve sosyalleşme gereksinimi duyar. 30 yıl önce albümlerde sakladığımız fotoğraflar, yakın çevremizle paylaştığımız kişisel verilerimiz, günümüzde sosyal platformlar, dijital uygulamalar ile internet ortamında depolanmış ve kolay ulaşılabilir durumdadır. Zamanımızın büyük kısmını geçirdiğimiz ya da günlük işlerimizi hallettiğimiz uygulamalar hayatımızı kolaylaştırmasının yanında bazı yükümlülükleri de beraberinde getirmektedir.

Teknolojinin hayatımıza dâhil olmasıyla vatandaşlık numaralarımızdan kredi kartı bilgilerimize, telefon numaramızdan, parmak izimize, ev adreslerimizden konumlarımıza kadar birçok veriyi biz istemesek de birçok kişi ya da uygulamayla anlık olarak paylaşmaktayız. Paylaşılan verilerin bizim için yararlı olacak şekilde kullanılmasının dışında, kötü amaçlı kişilerin eline geçmesi durumunda maddi, manevi sorunlar ortaya çıkarabilir.



(Şekil-1. Bilgi Katlanma Eğrisi)

Online alışveriş sitelerinde paylaştığımız telefon numarası, adres, kredi kartı bilgilerinin; akıllı ev aletleri ile paylaştığımız sabit internet şifrelerinin ya da herhangi bir uygulamayla paylaştığımız kişisel verilerin korunması ve güvenliği konusunda tedbirli olunmalıdır. Kişinin alacağı tedbirlerin yanında bilgi paylaştığı ortam ve uygulamaların verilerin korunması için aldığı ya da alacağı güvenlik önlemleri de en az kullanıcının gösterdiği bireysel çaba kadar önemlidir. Kullanıcılar, platformların mevcut güvenlik önlemlerini incelemeyen önemli bilgileri paylaşmamaya özen göstermelidir.

Dijitalleşen insan, hayatı hızlı ve pratik yaşıyor olsa da bu yararın arkasında bulunan büyük tehditler göz ardı etmemeli ufak açıkların dahi büyük sonuçlara neden olabileceğini unutmamalıdır.





KORUMAMIZ GEREKEN DİJİTAL VARLIKLAR

Korumamız Gereken Dijital Varlıklar

Dijital olarak yani elektronik ortamda var olan her şey dijital varlıktır. Fotoğraflar, videolar, dosyalar, e-postalar vb. unsurlar dijital varlıklara örnektir. Dijital varlıkları doğru bir şekilde muhafaza etmek önemlidir.

Günümüzde dijital varlıklar genel olarak ikiye ayrılır: kurumsal dijital varlıklar ve bireysel dijital varlıklar.

Kurumsal dijital varlıklar denilince akla birçok örnek gelir. Önemli bilgilerin saklandığı dosyalar, müşterilerin telefon numaraları, adresleri, fotoğraflar, videolar, çeşitli yazılım ve programlar da kurumsal dijital varlıklara örnektir. Bu varlıkların güvenli bir şekilde saklanması oldukça önemlidir.

Yüksek önem taşıyan bir diğer dijital varlık da müşterilerin telefon numaraları, adresleri gibi bilgilerinin saklandığı veri tabanlarıdır. Tabii yine fotoğraflar, videolar, çeşitli yazılım ve programlar da kurumsal dijital varlıklara örnektir. Bu varlıkların güvenli bir şekilde saklanması oldukça önemlidir ve varlıkları daha değerli kılar. Kurumsal dijital varlıkların ele geçirilmesi durumunda şirketler önemli maddi/manevi zararlara uğrayabilir. Verilerin korunması için yüksek maliyetli yazılımlar satın almak şirketlerin aldıkları önlemlerden biridir.

Bireysel dijital varlıklar için de kurumsal dijital varlıkların birçoğunu örnek gösterebiliriz. Fotoğraflarımız, videolarımız, belgelerimiz, işyerinde gerekli olan sunum dosyalarımız, e-postalarımız, alışveriş sitelerinde kullandığımız kredi kartı bilgilerimiz gibi unsurlar bireysel dijital varlıklardan bazılarıdır. Bireysel dijital varlıkların ele geçirilmesi genelde kurumsal dijital varlıkların ele geçirilmesi kadar büyük hasarlara yol açmasa da korunması için önlemler almak gereklidir.

Genel olarak dijital varlıklar kişiler ve kurumlar için oldukça önemlidir ve siber dünyada saldırılara açıktır. Kötü niyetli kişilerin eline geçen dijital varlıklar şirketler ve kişiler için büyük ve geri dönülemez zararlara sebep olabilir. Dijital varlıkları korumak; dijital varlıklarımızı güvenli bir şekilde saklamak, kötü amaçlı kişilerin ulaşımını engellemek, kişisel / kurumsal zararları önlemek vb. durumlar için önlem alınmalıdır. Tamamen güvenli bir yöntem olmasa da çeşitli yöntemlerle dijital varlıkları koruyup güvenliğini artırmak mümkündür.

Dijital varlıkları korumayı şu şekillerde gerçekleştirebiliriz:

- Önemli dosyaları/belgeleri yedekleyerek dijital ortamlardaki güncelleme ya da arızalanma durumlarında kaybetmenin önüne geçilebilir.
- Gizli olması gereken belgeleri/verileri şifrelemeyle erişimi kısıtlayıp güvende tutmak mümkündür.
- Logolar gibi özel varlıklar için telif haklarını alarak korumak uygun bir yöntemdir.
- Kurumlarda kurum içi güvenliğin sağlanması, dışarıya veri/bilgi sızmaması açısından işe alınan kişilere çeşitli konularda gizlilik sözleşmesi imzalanması önemlidir.
- Dijital ortamdaki hesaplarımıza giriş için birkaç adımlı giriş yöntemleri kullanarak yine bu hesaplardaki bilgilerin güvenliği artırılır.
- Bankaların çevrimiçi sitelerinde ya da uygulamalarında yapılan işlemlerden sonra güvenli çıkış yapılması hesabın güvenliğini artırır.
- Özellikle kurumlarda dijital varlıkları korumak için profesyonel yardım alınabilir. Dijital varlıkların yönetilmesine önem verilmelidir.
- Dijital varlıkları siber saldırılardan korumak için tıklanılan linklere, bağlanılan sunuculara, internet sağlayıcılarına dikkat edilmeli, güvenli olmayan bağlantılar kurulmamasına özen gösterilmelidir.

Dijital varlıkların sayısı oldukça fazladır ve gün geçtikçe artmaktadır. Bahsedilen yolların izlenmesi dijital varlıkların ele geçirilmeleri, kötü amaçlı kullanılmaları, kaybedilmeleri sebebiyle oluşabilecek hasarları önlemek için büyük ölçüde etkili olacaktır.

**SEDA
DURAN**

**KONU
34**





SİBER HİJYEN

Hijyen, sağlığa zararlı her türlü ortamlardan korunmak için yapılan, alışkanlık hâline getirilen kurallar bütünü anlamına gelmektedir.

Siber hijyen de sistemlerin, ağların, verilerin ve kullanıcıların zararlı yazılımlardan, saldırılardan korunmak ve bunun sürekliliğinin sağlanması için yapılması gereken rutinlerdir.

İnternetin hayatımızın her alanında yer alması hayatımızı zaman, maliyet, fiziksel güç gibi yönleriyle kolaylaştırırken birçok güvenlik riski ile siber saldırıların da hedef alanlarını artırmaktadır.

Siber Hijyenin Önemi

Bireylerin ve kurumların dijital ortamda mahremiyetlerinin ve kişisel bilgilerinin korunması, maddi ve manevi kayıpların önlenmesi için siber hijyen önemli bir yere sahiptir. Öncelikle şirket yöneticileri, bilgi teknoloji departmanı birim/birimleri ile tüm departmanlar ve kullanıcılar “Siber saldırganlar bize ulaşamaz veya bizimle uğraşmaz, daha önce test yaptırıldık bir açığımız yok vb” yaklaşımlardan kaçınılmalıdır, siber tehdit ve saldırı olma ihtimali göz ardı edilmemelidir.

Birtakım kurallar ile bu risklerin en aza indirilmesi ve engellenmesi mümkündür.

Siber Hijyen Kuralları Nedir?



1 Özellikle kullandığımız sosyal ağ gibi platformlarda hesap bilgilerimizi ve bazı kişisel bilgilerimizi korumak amacı ile profillerimizi gizli (private) olarak kullanmak ve tanımadığımız profilleri uzak tutmak. Hesabın gizlilik ayarlarını güvenliği en üst düzeyde tutacak şekilde ayarlamak. Telefon numarası, ev veya iş adresi gibi kişisel bilgileri, özel fotoğrafları sosyal ağ platformlarında paylaşmamak.

2 Kullanıcısı olduğumuz dijital platformlarda parolalarımızı aynı seçmemek, bu sayede herhangi birinin bulunması/çalınması ihtimaline karşı diğer hesaplarımıza ulaşılabilirliği engellemek.

3 Kullanıcısı olduğumuz dijital platformlarda hesaplarımızın ele geçirilmesi ihtimallerine karşı kurtarma e-postası/telefon numarası belirlemek.

4 Güçlü parolalar belirlemek. Güçlü şifrelerin içermesi gereken unsurlar; en az 12 karakter, büyük ve küçük harf, rakam, özel karakterdir. İçermesi gerekenlerin yanında içermemesi gereken unsurlar olarak; özellikle kendi isim/soyisminiz, doğum tarihiniz, doğum yeriniz, tuttuğunuz spor takımı isimleri/kuruluş yılları, ardışık rakamlar veya alfabede/klavyede ardışık harfler vb. sayılabilir.

5 Güçlü parolanızı belirledikten sonra minimum altı ayda bir şifrenizi değiştirmek.

6 Parolanız size özeldir. Parolanızı akrabalarınız, yakınlarınız, arkadaşlarınız, hizmet aldığınız kurum personelleri de dâhil olmak üzere **Hiç Kimse** ile paylaşmamak, herhangi bir yere not etmemek.

7

Kullanıcısı olduğunuz dijital platformda parolanızın yanı sıra e-posta veya sms olarak gönderilen kodla girişi sağlayabileceğiniz İki Faktörlü Kimlik Doğrulamasını kullanmak.

8

Tarayıcılarınızın parolanızı hatırlamasına izin vermemek.

9

Kullandığınız hesaplara en son erişimin nerede ve hangi saatte olduğunu düzenli olarak kontrol etmek ve emin olmadığınız erişim durumları için parolanızı değiştirmek.

10

Kablosuz ağlara bağlanarak kullanılabilir cihazlar için varsayılan ismi ve parolayı değiştirmek.

11

Bilgisayarınızdan yapacağınız günlük işler için tüm yetkilere sahip kullanıcı (Administrator) yerine yetkileri kısıtlı bir kullanıcı ile yürütmek. Varsa kullanılmayan kullanıcıları silmek...

12

Bilgisayar, telefon gibi cihazlarda parola ile açılan ekran kilidini etkinleştirmek. Belirlediğiniz süre içinde herhangi bir işlem yapılmadığında bu kilidi aktifleştirecek şekilde ayarlamak.

13

İnternet üzerinden yapacağınız işlemler için bulunduğunuz web sitesinin SSL Sertifikası'nın (Adres çubuğunda kapalı bir kilit olarak gözüktür.) olmasına dikkat etmek ve varsa kalitesinin kontrol edilmesi.

14

Tarayıcınızda işlemlerinizi bitirdikten sonra çerezleri ve önbelleği temizlemek.

15

E-posta, SMS gibi iletişim kanalları ile gönderilen bilinmeyen/beklenmeyen linklere tıklamamak.

16

Bilinmeyen/tanınmayan wi-fi, bluetooth cihazlarına bağlanmamak; bilinmeyen/tanınmayan USB cihazlarını kendi cihazınıza bağlamamak, bağlamak gerekiyorsa virüs taraması yapmak.

17

Cihazlarınızda güvenlik duvarını etkinleştirmek/devre dışı bırakmamak, anti-virüs yazılımı kullanmak.

- 18 Tarayıcılarda AdBlock gibi reklam engelleme eklentileri kullanmak.
- 19 Çoğu yazılım güncellemesinin güvenlik amaçlı olması nedeniyle cihazlarınızın, kullandığınız yazılımların, işletim sistemlerinin güncellemelerini takip ederek veya otomatik yazılım güncelleme özelliğini aktifleştirerek güncel tutmak.
- 20 Önemli dosyaları şifreleyerek, sabit bir diskte veya bulut tabanlı bir sunucuda yedeklemek.
- 21 Kullanılan uygulamalarda konum bilgisinin kullanılması gerekiyorsa sadece uygulamayı kullanırken erişimine izin vermek.
- 22 Kullanacağınız yazılım/uygulamanın üreticisini araştırmak, güvenilemeyen/bilinmeyen kaynaklardan uygulama veya yazılımları indirmemek/kullanmamak.
- 23 Herkese açık kablosuz ağlara bağlanmamak. Bağlanmak gerekiyorsa VPN kullanmak.
- 24 Kullanılan uygulamalar ve programlarda kurulum aşamasında veya sonrasında istenen erişimleri iyice okuyarak verilecek izinleri belirlemek.
- 25 Sahip olunan wi-fi'nin varsayılan ismini ve parolasını değiştirmek, kablosuz ağınıza bağlanacak cihazları belirlemek için ağ cihazınızın yönetim konsolunu kullanmak.
- 26 Sahip olunan cihazları kullanması için başka birine verirken veya satarken verilerinizi başka bir cihaza yedekledikten sonra, cihazı sıfırlamak/fabrika ayarlarına döndürmek.
- 27 Sahip olunan wi-fi'de misafir ağı oluşturarak, sizin ve diğer kullanıcıların bağlandığı ağı ayrı tutmak.
- 28 Sahip olunan ağ kablolu ise boşta olan kabloları ortada bırakmamak, ağ cihazı gözden uzak bir yerde barındırmak.

29

Yeni teknolojileri takip ederek tehdit oluşturabilecek unsurları arařtırmak.

30

E-ticaret platformlarının arařtırılarak güvenilmeyen platformlara kiřisel bilgileri ve finansal bilgileri girmek.

31

Kripto para iřlemleri yapıyorsanız yukarıda belirtilen web tabanlı yazılımlar ve uygulamalar için belirtilen siber hijyen kurallarının yanında güvenli/yasal kripto para borsalarını kullanmak, cüzdan yedeđinizi almak, sođuk cüzdan kullanmak, iřlemlerinizi tek bir cihazdan gerekleřtirmek ve yeni bařladıysanız kk kripto para miktarları ile denemeler yapmak.

32

Ađ güvenliđinin sađlanması için kullanılabilecek cihazları arařtırmak, temin etmek, eđer bu cihaza/cihazlara sahipseniz yapılandırmasını dođru yapmak, dzenli kontrol etmek.

33

Kurum ve řirketlerin, bnyesindeki tm departmanlara siber gvenlik konusunda eđitimler vermesi ve her geen gn deđiřen geliřen teknolojilerle birlikte siber saldırıların da deđiřebileceđi gz nnde bulundurularak eđitimleri gncellemek ve srdrmek. Son kullanıcıları da bu alanda srekli olarak arařtırma yapmak ve eđitimlere katılmak ynnde desteklemek.

Her konuda olduđu gibi "siber gvenlik" ve "siber gvenlik" konusunda da en nemli husus farkındalıktır. Kiřisel hijyen için yapılanlar sađlıđımız için ne kadar nemliyse siber hijyen de diđital ortamlarımızın sađlıđı ve güvenliđi için o kadar nemlidir.

Siber hijyen farkındalıđı ve oluřan bilincin transferi ile güvenliđimizi st seviyelere tařımak mmkndr.





İNTERNET NASIL ÇALIŞIR?

Arpanet

İnternet, her ne kadar günümüzde eğlence amaçlı kullanımıyla ön planda olsa da ortaya çıkışında daha çok insanların elde ettikleri bilgileri saklama isteği ve saklanan bu bilgilerin aktarılmasına duyulan ihtiyaç rol oynamıştır.

1960'larda soğuk savaş devam ederken henüz bilgisayarlar yerlerinden oynatılamayacak boyutlara sahip olduğu için aralarında bilgi aktarımı maalesef posta yoluyla sağlanmak zorundaydı. Ayrıca bilgilerin tek bir merkezde tutulması, olası bir saldırı durumunda bu bilgilerin tamamen kaybolabileceği anlamına geldiği için bu bilgisayarlar büyük bir güvenlik tehdidiyle de karşı karşıyaydı. Amerika Birleşik Devletleri bu sorununa çözüm olması amacıyla aynı yıllarda ülkenin araştırma alanında faaliyet gösteren ve ARPA olarak kısaltılan Advanced Research Projects Agency (Gelişmiş Araştırma Projeleri Dairesi) ile birlikte bir proje geliştirmeye başladı. Öncelikli olarak amaç güvenilir kaynaklar arasında bilgi aktarımını sağlamaktı ve böylelikle olası bir saldırı durumunda bir kaynak erişilemez olsa bile diğer kaynaklardan bilgiye ulaşım mümkün olacaktı. Böyle bir ağın yaratılması için akademik araştırmaların merkezi olan üniversitelerden oluşan dört adet düğüm noktası seçildi: Kaliforniya Üniversitesi (Santa Barbara ve Los Angeles kampüsleri), Stanford Araştırma Enstitüsü, Utah Üniversitesi (Şekil 1).

Bu dört bilgisayar arasında oluşturulan ve Arpanet ismi verilen bu ağ, günümüzdeki internetin ilk hâli olarak bilinmektedir.



Şekil 1: ARPANET düğüm noktaları

Zamanla bu başlangıçtaki dört düğüm noktasına başka üniversiteler ve araştırma merkezleri de eklendi ve Arpanet 1970'lerin ortasında neredeyse 60 düğüm noktasına sahipti. Günümüzde dünyanın hemen hemen her noktasına bağlanabiliyor olduğumuz düşünülünce bu sayı küçük gelse de o dönem için daha önce başarılmamış bir gelişmeydi. Fakat bu büyüme yeni ihtiyaçları da beraberinde getirdi. Artık sabit hatlar üzerinden erişim yeterli gelmiyordu ve daha fazla noktaya ulaşmak için kablosuz bir iletişim modeline geçilmesi

lazımdı. Bunun için de Arpanet gibi çeşitli yerel ağların uydular aracılığıyla birbirine bağlanması ve bu esnada da ortak bir dili konuşmaları gerekliydi. Bu aşamada da internet protokolleri önemli bir rol oynuyordu.

TCP/IP Modeli

İnternet üzerinden veri aktarımında bir standart oluşmasının gerekliliğiyle birlikte TCP/IP modeli denilen ve birtakım protokollerin birbiriyle ortak çalışmasından meydana gelen bir sistem geliştirildi. Karmaşık gibi görünse de aslında basit bir anlayışla çalışmakta olan bu sistemde bir veri, bilgisayarlar arasındaki yolculuğunu dört farklı katmana uğratarak gerçekleştirilmektedir:

Uygulama katmanı: Gönderilecek verinin dosya türüne uygun uygulama türü ve protokoller seçilir.

Taşıma katmanı: Verinin nasıl taşınacağına karar verilir. İhtiyaca göre iki farklı taşıma protokolü arasından bir tercih yapılır: TCP (yavaş fakat güvenli) veya UDP (hızlı fakat güvensiz).

İnternet katmanı: İnternete erişimi olan her bilgisayarın, internet üzerinde bulunabilmesi için kendisine atanan bir adresi vardır. Bu adrese IP (İnternet Protokol) adresi adı verilir. Hedef ve kaynak bilgisayarların IP adresleri de verinin üzerine bu aşamada işlenir.

Ağ ara yüz katmanı: Son olarak veri, bilgisayarların birbiri arasında iletişim kurabileceği bir biçim olan ikilik sayı sistemine çevrilir ve internet kablolarındaki fiziksel yolculuğuna başlar.

Bu taşıma aşamalarında veri, aktarılabilmek için küçük parçalara ayrılır ve her bir parça teker teker hedef bilgisayara gönderilip orada birleştirilerek tekrar bir bütün hâline gelir.

İnternet

TCP/IP sisteminin 1970'lerde standart bir şekilde kullanılmasıyla birlikte internet veri gönderiminde istikrarlı olabildiğini göstermişti. Fakat gerçek anlamda kullanıcı dostu bir internetin ortaya çıkmasına biraz zaman daha vardı.

1985'te National Science Foundation (NSF), yani Ulusal Bilim Vakfı, NSFnet adı verilen ilk yüksek hızlı internet ağının sahibi oldu. Bu ağ sayesinde internet yalnızca araştırmalar için değil, aynı zamanda kişisel kullanım için de kullanılabilir hâle geldi. 1990'larda kablosuz internetin keşfi ve Windows 98 gibi kullanıcı dostu bir bilgisayar işletim sisteminin ortaya çıkışı ile birlikte kişisel bilgisayarlar ve internetin kullanımı yaygınlaştı, nihayet günümüzdeki anlamıyla internet ortaya çıkmış oldu.

Her ne kadar başlangıçta bilgilerin yok olmaması adına geliştirilmiş olsa da internet gelişim sürecindeyken birbirini tanıyan ve denetim altındaki bilgisayarlar arasında veri aktarımını sağlamak amacı taşıdığı için ağ içerisindeki bilgisayarlardan gelebilecek saldırılar ve saldırıların önlenmesi, tasarımının öne çıkan parçalarından değildi. Daha çok iletilmek istenen bilginin doğru ve hızlı bir şekilde iletilip iletilmediğinin kontrol edilmesiyle ilgilenildiğinden internet ilk ortaya çıktığı zamanlarda güvenli olmak üzerine tasarlanmamıştı.

Bu sebeple de internetin tamamen güvenilir bir şekilde çalışması mümkün değildir. Bizim elimizden geldiği ölçüde internetteki tehditlerin farkında olup kendimizi bu tehditlerden nasıl koruyacağımızı öğrenmemiz gerekir.





METaverse

İnsan-İnternet Etkileşiminin Zirvesi:

Metaverse ve Beraberinde Getirdiği Güvenlik Sorunları

Fiziksel dünyada en temel gereksinimlerimizden biri güven duygusudur. Kendimizi güvende hissetmediğimiz herhangi bir yerde bulunmak istemez, güvenmediğimiz insanlarla iletişimimizi sürdürmeyiz.

İnternet dünyasında ise gerçek hayatta tanımadığımız birçok insanla iletişim kurarken ortaya çıkabilecek güvenlik zafiyetlerini göz ardı edebiliriz.

İnternet teknolojisi ortaya çıktığı zamandan bu yana çok hızlı bir şekilde hayatımızın büyük bir parçası hâline geldi. Başlarda tek taraflı bir iletişim kanalı olarak düşünebileceğimiz internet zaman içinde kullanıcıların kendi içeriklerini üretip paylaşabildiği, birbirleriyle bilgi alışverişinde bulunabildiği çok yönlü bir iletişim-etkileşim aracına dönüştü. Öyle ki nesnelerin interneti dediğimiz bir teknoloji ile artık sadece insanlar değil çeşitli cihazlar, ev aletleri, makineler, otomobiller vs. birbiriyle haberleşebilir duruma geldi. Tüm bunlar internet ortamında var olan bilginin katlanarak artmasını sağladı. Bilginin katlanarak artması ise onun korunmasını zorlaştırdı ve bu durum birçok güvenlik sorununu beraberinde getirdi.

Her gün milyarlarca bilgi girişinin yapıldığı internet dünyası ile artık yeni bir etkileşim biçimi geliştiriliyor. Adını son günlerde çok fazla duyduğumuz bir kavram var: Metaverse.

Kimi araştırmacılar tarafından metaverse kelimesi Türkçeye kurgusal evren olarak çevrilmiş ve fiziksel hayatın internet ortamındaki bir simülasyonu olarak ifade edilmiştir. Başlangıçta internet karşısında pasif tüketici olarak var olan kullanıcı, zaman içinde onunla etkileşime girip onu üreten kullanıcıya dönüşmüştü. Şimdi ise kullanıcıdan metaverse ile internetin içinde bir dünya kurması ve gerçek dünyadaki yaşantısını kısmen de olsa buraya taşıması bekleniyor. Metaverse henüz yolun çok başında bir teknoloji. Şu an hayal edildiği gibi gerçekleşebilmesi için birçok teknik sorunun aşılması gerekiyor. Eğer bu sorunlar aşıp istenildiği gibi bir sanal evren inşa edilebilirse insan yaşamını çok derinden etkileyen bir teknoloji olabilir.

Günümüz internet teknolojisinde paylaşımlarımız, takip ettiğimiz içerikler, yorum yaptığımız ya da beğendiğimiz gönderiler, satın aldığımız ürün ve hizmetler; bizim yaşam biçimimiz, siyasi görüşümüz, tüketim alışkanlıklarımız, istemediğimiz kişi ve gruplara fikir verebilir. Bununla birlikte kullandığımız uygulamalar, e-postamıza düşen bir mail, kaynağını bilmediğimiz bir bağlantı, bilgisayarımıza indirdiğimiz bir dosya; ad, soyad, iletişim bilgilerimiz, adres bilgilerimiz, banka hesap bilgilerimiz gibi kişisel verilerimizin çalınmasına sebebiyet verebilir.

Hâlihazırda siber güvenlik alanında bu tür güvenlik sorunlarının önüne geçebilmek için gerekli çalışmalar yapılıyor. Metaverse teknolojisine bakacak olursak kullanıcılar burada kendilerine ait bir avatarla sanal şehirlerde dolaşabilecek, kripto paralarını yönettikleri sanal bir cüzdana sahip olabilecek, sanal mağazalardan alışveriş yapabilecek, sanal arsalar satın alabilecek, kendi sosyal statülerini daha iyi ifade edebilmek için çok değerli bir NFT'ye çok yüksek miktarda ödeme yapabilecek, dünyaca ünlü sanatçıların konserlerine katılabilecek, belki hayranı olduğu sanatçıyla bir kafede oturabilecek, daha önce bilgisayarında oynadığı oyunun içinde yer alabilecek ve daha birçok farklı şeyi deneyimleyebilecek.

Bazı şirketlerin metaverse arsaları satın almaya başladığını, dünyaca ünlü markaların burada mağazalar açtıklarını, ünlü sanatçıların burada parti vermeye başladığını görüyoruz. Tüm bunların zaman içinde ne gibi sonuçlar doğuracağını, insan yaşamını nasıl değiştireceğini, zamanımızı nasıl şekillendirebileceğini şimdiden kestirebilmek çok zor. Ancak şu an için bile neredeyse gerçek yaşamdaki gibi tüm varlığımızla yer almaya çalıştığımız bir dünyada hiç istemediğimiz bir şekilde çok daha değerli bilgilerimiz kötü niyetli kişilerin eline geçebilir ve işlenen bir suça alet edilebilir.

Öyle ki metaverse dünyasına fiziksel olarak entegre olabilmemizi sağlayan araçlar, sanal gerçeklik gözlükleri, oyun konsolları, sanal dünyadaki hareketleri hissedebilmemizi ve aynı zamanda gerçek dünyadaki hareketlerimizi de sanal dünyaya aktarabilmemizi sağlayan duyuşsal kıyafetler; biyolojik özelliklerimize dair birçok veriyi henüz ne şekilde kontrol edileceği belli olmayan bir sisteme işleyecek. Ses biyometrimiz, yüz hatlarımız, kalp atış hızımız, gözlerimizin hareketleri, çeşitli sağlık problemlerimiz hakkındaki bilgiler ve daha bilmediğimiz birçok başka şey bir veri olarak burada yer alabilecek. Bu verilerimizin kötü niyetli kişi ve grupların eline geçmesi bizi daha manipüle edilebilir hâle getirebildiği gibi, sesimizin ve yüzümüzün taklit edilmesiyle bizi bir suçun ortağı durumuna da düşürebilir. Son zamanlarda yapılan deepfake uygulamaları bunun küçük bir örneği olarak gösterilebilir. Bunlar metaverse ile ortaya çıkabilecek güvenlik sorunlarından birkaçı.

Dijital cüzdanımızın güvenliği, yapılacak ticari işlemler, dijital sanat eserlerinin korunması gibi konuları da göz önünde bulundurduğumuzda buradaki güvenlik zafiyetlerinin çok büyük zararlar doğuracağı ortada. Tüm bu gelişmeler bizlere internetin hayatımızda yer alma katsayısı arttıkça güvenlik problemlerinin de arttığını ve buna paralel olarak yapılacak siber güvenlik çalışmalarının ne kadar önemli olduğunu ifade etmekte. Bunun için tüm kullanıcıların bu konuda bilinçlendirilmesi gerektiği gibi siber güvenlik alanında yeni yaklaşım ve araçlara, nitelikli insan gücüne ihtiyaç duyulabilir.





DİJİTAL HAYATTAKİ ANAHTARLARIMIZ

DİJİTAL HAYATIMIZIN ANAHTARLARI

Teknolojideki gelişimle birlikte insanların kişisel bilgileri de dijital ortamda muhafaza edilmeye başlandı. Telefon numaralarımız, elektronik posta adreslerimiz, kredi kartı numaralarımız veya en basit yoluyla adımız, soyadımız ve doğum tarihimiz gibi kendimizle ilgili birçok bilgiyi dijital ortamda paylaşıyoruz. Eğer yeterli korumayı sağlamazsak bilgilerimiz, başkaları tarafından ele geçirilebilir hâle geliyor. Önlem alma noktasında ise dijital hayatımızın anahtarları devreye giriyor.

Parola Nedir?

Parola, çevrimiçi hesaplarda oturum açmak ve başka kullanıcıların erişimini engellemek için kullanılan gizli anahtarlara denir. Parolalar kullanıcılar tarafından belirlenebiliyor olmakla birlikte kullandığınız tarayıcının önerdiği parolayı da seçebilirsiniz. Peki, kendiniz nasıl güçlü bir parola oluşturabilirsiniz?

Güçlü Parola Oluşturma

Oluşturulan bir parolanın “güçlü” kabul edilebilmesi için aşağıdaki özelliklere sahip olmalıdır.

En az 8 karakterden oluşur.

Harflerin yanı sıra, rakam ve “?, @, !, #, %, +, -, *” gibi özel karakterler içerir.

Büyük ve küçük harfler bir arada kullanılır.

Bu kurallara uygun parola oluştururken yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir:

Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin doğum tarihiniz, çocuğunuzun adı, soyadınız, vb.)

Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.

“1234” veya “abcd” gibi devam eden dizinler kullanılmamalıdır.

Neler Yapılabilir?

Şarkı sözlerinden, deyimlerden veya atasözlerinden esinlenip cümlelerin baş harflerini birleştirebilirsiniz.

Örn: 10 yılda 15 milyon genç, yarattık her yaştan. → 10y15mg,yhy.

Klişe ve kolay tahmin edilen, basit bir ifade olmamak şartı ile cümleleri olduğu gibi parola yapabilirsiniz.

Örn: Dikkat!Yolda3KişiVar.

Benzer rakam ve harfleri birbiri yerine kullanabilirsiniz. Bu yöntem saldırganlar tarafından da bilindiği için diğer yöntemlerle birlikte kullanmak daha uygun olacaktır.

Örn: 'S' yerine 5, 'G' yerine 6, 'ı, i, l, L' yerine 1 vb.

Bir cümledeki sadece sesli ve sessiz harfleri kullanabilirsiniz.

Örn: Örnek bir parola veriyorum. → rnk!prlvryrm

PIN (Personal Identification Number)

Kişisel tanıtim numarasıdır. 4 ya da 6 rakamlı numaralardan oluşur. PIN kodu, cep telefonlarının SIM kartlarında, ağ sistemlerinde, bilgisayar ağlarında kullanılabilir. Kaba kuvvet saldırısı (brute force) ve bir kelime listesi ile kırılabilir gibi dursa da PIN kodları, belirli bir denemeden sonra kendini iptal etmek üzere kodlanmıştır. Örneğin birçok cep telefonunda PIN'i 5 kere yanlış girmeniz hâlinde cihaz 10 dakika boyunca kendini beklemeye alır. Ya da bir SIM kartı, PIN kodu 3 kere yanlış girilmesi hâlinde PIN kodu girme menüsünü iptal eder ve 'kurtarma parolası' denilen PUK kodu devreye girer.

TAN (Transaction Authentication Number)

Banka işlemlerindeki onaylama numaralarıdır. İnternet bankacılığında banka işlemlerini yapmak için tek seferlik kullanılan kodlardır. TAN'lar geleneksel tek katmanlı kimlik korumalarının çok daha ötesinde, ikinci bir güvenlik katmanıdır. Oturum açma verileri alınsa dahi geçerli bir TAN olmadan hiçbir işlem gerçekleştirilemez.

Klasik TAN: Banka, kullanıcı için bir dizi benzersiz TAN oluşturur. Tipik olarak, bir listede normal bir kullanıcı için yarım yıl yetecek kadar 50 TAN baslıdır; her TAN altı veya sekiz karakter uzunluğundadır.

Dizine Alınmış TAN (iTAN): Dizine alınmış TAN'lar kimlik avı riskini azaltır. Bir işleme yetki vermek için kullanıcıdan; listeden rastgele bir TAN kullanması değil, bir sıra numarası (dizin) ile tanımlanan belirli bir TAN girmesi istenir. Endeks banka tarafından rastgele seçildiğinden bir saldırgan tarafından edinilen keyfi bir TAN genellikle değersizdir.

CAPTCHA ile Dizinlenmiş TAN (iTANplus): iTAN'a girmeden önce kullanıcıya arka planda, işlem verilerini ve kullanıcının doğum tarihi gibi saldırganın bilmediği düşünülen verileri içeren bir CAPTCHA sunulur. Bu, saldırganın CAPTCHA'yı taklit etmesini zorlaştırmayı amaçlar ve ortadaki adam (Man-in-the-middle) saldırısının riskini azaltır.

Mobil TAN (mTAN): Kullanıcı bir işlem başlattığında banka tarafından bir TAN oluşturularak kullanıcının cep telefonuna SMS ile gönderilir. Ayrıca SMS, kullanıcının işlemin bankaya iletilirken değiştirilmediğini doğrulamasını sağlayan işlem verilerini de içerebilir.

pushTAN: pushTAN, Alman Sparkassen bankacılık grubu tarafından mTAN planının bazı eksikliklerini azaltan uygulama tabanlı bir TAN planıdır. SMS mesajlarının maliyetini ortadan kaldırır. Mesajlar özel bir metin mesajı uygulaması aracılığıyla şifreli bir internet bağlantısı kullanılarak, kullanıcının akıllı telefonuna gönderildiği için SIM kartı dolandırıcılığına açık değildir. Bilgisayar ve akıllı telefona paralel kötü amaçlı yazılım bulaşması riskini azaltmak için mobil cihazda yetki yükseltilmiş veya IOS cihazlar için zincir kırma işlemi (jailbreak) yapılmışsa pushTAN uygulaması çalışmayı durdurur.

4)E-imza

Elektronik imza ya da sayısal imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan, kimlik doğrulama amacıyla kullanılan, elektronik veridir. Elektronik ortamlarda imza yerine kullanılabilen yasal kimlik doğrulama sistemidir. Bu, kişinin imzasının taranmış hâli olabilemle birlikte kişiye ait ses, göz retinası veya sayısallaştırılmış bir imza da olabilir. E-imza'nın en kullanışlı özelliği ise kişiye, kimliğini ispatlama şansı vermesidir. Gönderim sırasında ne bilgiyi imzalayan gönderici mesajı gönderdiğini inkâr edebilir ne de alıcı, mesajı almadığını iddia edebilir. E-imza, bir algoritma veya bir matematik formülü ve bir anahtarla birlikte şifrelenir.

E-imza Nasıl Onaylanır?

Bir elektronik imza yaratmak için imzalayan, mesajın kısaltılmış bir sürümü olan bir özet değeri ve bu özet değerini şifrelemek için kendi özel/gizli anahtarını kullanır. Şifrelenmiş özet değeri elektronik imzadır. Eğer mesaj herhangi bir nedenden dolayı değişikliğe uğrarsa değişmiş olan mesajın özet değeri de

orijinal özet değerinden farklı olacaktır. Elektronik imza, mesaj için de onu yaratan özel anahtar için de tek olduğundan değiştirilmesi mümkün değildir. Daha sonra elektronik imza, mesaja eklenir ve ikisi birden alıcıya gönderilir. Alıcı, gelen mesajdan özet değerini tekrar yaratır ve gönderenin açık anahtarını gelen mesajdaki özet değerinin şifresini çözmede kullanır. Eğer alıcının hesaplamış olduğu özet değeri ile mesajın içerisinde yer alan özet değerleri aynı ise şu iki şey doğrulanmış olur:

Elektronik imza gönderenin özel/gizli anahtarı kullanılarak yaratılmıştır.

Bu gönderenin yetkinliğini tanırlar ve gönderen mesajı imzalamadığını iddia edemez. Kimse gönderenin adını kullanmaya çalışmamıştır.

Mesaj değiştirilmemiştir. Bu mesajın doğruluğu onaylanmıştır.

KAYNAKÇA:

<https://bidb.beun.edu.tr/bilgilendirme/guclu-parola-olusturma.html>

https://tr.wikipedia.org/wiki/Elektronik_imza

https://en.wikipedia.org/wiki/Transaction_authentication_number





HALKA AÇIK KABLOSUZ AĞLAR VE RİSKLER

HALKA AÇIK KABLOSUZ AĞLAR ve RİSKLER

HALKA AÇIK KABLOSUZ AĞLAR

Dünyanın vazgeçilmez teknolojilerin öncülerinden biri kablosuz ağlardır. Birçok yerde bulunan herkesin ücretsiz ve şifreye ihtiyaç duymadan kullanılabildiği kablosuz ağlar, halka açık ağlardır.

Hastaneler, havaalanları, restoranlar, kafeler gibi birçok alanda bu çeşit ağlara erişebilmek mümkündür.

Kullanıcılar bir dakikadan fazla zaman geçirecekleri her yerde, hemen kablosuz ağ aramaya başlar. Kısa süre önce yapılan bir ankette, tablet kullanıcılarının %70'i ve akıllı telefon/cep telefonu kullanıcılarının %53'ü halka açık wi-fi erişim noktalarını kullandıklarını belirtmiştir.

Ev dışındayken ücretsiz bir şekilde interneti kullanabiliyor olmak oldukça faydalıdır. Seyahat hâlinde ya da tatildeyken mobil veriyi tüketmek yerine etrafta kolaylıkla bulunulabilecek, ortak kullanıma açık, parolasız kablosuz ağlara bağlanmanın işleri kolaylaştıracağı düşünülür. Birçok anlamda kullanışlı ve rahat olan bu ağlar, gerekli zamanlarda işe yarar.

Önceden hakkında bilgi sahibi olunmayan ve daha önce görülmemiş bir yere seyahat ediliyorsa ücretsiz kablosuz ağlara bağlanarak çevrimiçi haritalara bakılabilir, navigasyon takibi yapılabilir. Herkese açık ağlar aracılığıyla fotoğraflar sosyal medyada paylaşılabilir, iş postalarına bakılabilir ya da para transfer etmek için bankacılık uygulamaları kullanılabilir.

HALKA AÇIK KABLOSUZ AĞLARDA RİSKLER

Kablosuz ağların büyük bir güvenlik riski oluşturduğu unutulmamalıdır. Bu çeşit ağlar güvensiz kablosuz ağlar sınıfına girmektedir. Halka açık kablosuz ağlar üzerinden gönderilen veriler siber saldırganlar tarafından kolaylıkla ele geçirilebilir. Bu durum birçok akıllı telefon, tablet ve laptop kullanıcısının kişisel bilgileri, dijital kimlikleri ve paralarının güvenliği açısından risk oluşturmaktadır. Ayrıca kullanılan cihazda etkili bir güvenlik olmaması ve koruma ürünüyle korunmaması riskleri daha da artırır.

Ağ bağlantısı kurmak için doğrulama gerekmemesi kullanıcılara olduğu kadar siber saldırganlara da cazip gelmektedir. Aynı ağ üzerinde bulunan güvenli cihazlara erişilebilmesi açısından siber saldırganlara bir fırsat niteliği taşımaktadır. Siber saldırganlar bu ağlara sızarak, ağ üzerinde gerçekleşen iletişimi dinleyebilir, kurbanları sahte sitelere yönlendirebilir veya kredi kartı, kimlik, parola gibi kritik bilgileri kolaylıkla ele geçirebilirler. Güvensiz bir ağa iş cihazıyla bağlanması durumunda şirkete ait bilgiler siber saldırganların eline geçebilir. Ayrıca siber saldırganlar halka açık alanlardaki bu güvenli olmayan ağları kötü amaçlı yazılımları dağıtmak için de kullanabilmektedirler.

AĞ TRAFİĞİNİN DİNLENMESİ

Bir cihazın ağ üzerinden başka ağ elemanları ve başka bilgisayarlarla arasında gerçekleşen veri trafiğinde yer alan paketleri ele geçirebilmek için veri dinleme işlemidir. Bu işlemde ek veri paketleri göndermeksizin yalnızca başka cihazlar tarafından gönderilen paketler izlenir.

ORTADAKİ ADAM SALDIRISI (MITM)

Ortakdaki adam saldırısı kötü niyetli bir kişinin iki bağlantı arasındaki iletişimi dinlemesi, değişiklikler yapması, kullanıcılara ait verileri alması anlamına gelmektedir.

Pek çok ortakdaki adam saldırı çeşidi mevcuttur. Ortadaki adam saldırısı, kullanıcının ağ trafiğini dinlemek, kullanıcıyı sahte bir web sitesine yönlendirmek veya kullanıcıya kötü amaçlı yazılım göndermek gibi çeşitli şekillerde gerçekleşebilir. Bir kullanıcının online bankacılık sayfasına gönderdiği erişim talebinin engellenmesi ve bu talebe uygun gibi görünen sahte bir online bankacılık sayfasıyla geri dönülmesi ortakdaki adam saldırısına bir örnektir.

Bu örnekler dosya paylaşımından e-posta sağlayıcılarına kadar birçok farklı yerde meydana gelebilmektedir.

Örneğin, bir kafenin açık internetine bağlanmış bir müşteri e-postalarına bakmak istediğinde onun ağını izleyen bir siber saldırgan, sayfaya gönderilen istek başarılıysa, müşteriye kendi oluşturduğu sahte bir web sitesine yönlendirebilir. Bu durumda saldırganın ele geçirdiği kullanıcı adı, şifre gibi bilgiler kötü amaçlar için kullanılmak üzere kaydedilebilir. Saldırgan bu bilgilerle kendi kötü yazılımlarını müşterinin e-posta adresindeki kişilere yollayabileceği gibi müşteriye ait bilgileri müşteriye karşı kullanabilir.

ALINABİLECEK GÜVENLİK ÖNLEMLERİ

- Halka açık alanlardaki kablosuz ağlar yapısı gereği güvensiz olduğundan dikkatli olunmalıdır.
- Kişisel verilerin iletildiği ya da bankacılık işlemlerinin yapıldığı URL adresinde SSL bağlantısı olmalıdır. HTTPS protokolünü kullanan web siteleri kullanılmalıdır.
- VPN ya da Proxy gibi bağlantıyı şifreleyen yazılımlar kullanılmalıdır.
- Halka açık alanlardaki kablosuz ağlara bağlı cihazlarda anti-virüs yazılımları kullanılmalıdır.
- İşletim sistemi güncel tutulmalıdır.
- Gerekemediği müddetçe kredi kartı ile alışveriş yapılmamalıdır.
- Cihazlarda açık olan paylaşımların tümü kapalı olmalıdır.
- Kullanılan cihazda mutlaka aktif halde bir güvenlik duvarı olmalıdır.



- İhtiyaç olmadığı durumlarda kablosuz ağ bağlantısı kapatılmalıdır.
- Halka açık alanlardaki ağlara bağlanırken “otomatik bağlan” seçeneği asla işaretlenmemelidir.
- Kablosuz ağların etkin nokta isimleri kontrol edilmelidir. Çünkü örneğin bir kafeye ait ağ ismi KahveDukkani iken KahveDukkani1 gibi benzer isme sahip ancak sahte olan bir ağa bağlanma riski bulunmaktadır.
- Kimlik doğrulama gerektiren hizmetler halka açık ağlardan birine bağlıyken kullanılmamalıdır.
- Gerçekten ihtiyaç duyulmadığı takdirde halka açık alanlardaki kablosuz ağlara bağlanmaktan kaçınılmalıdır.

KAYNAKÇA:

<https://www.kaspersky.com.tr>

İLAYDA DURLANIK

KONU
39

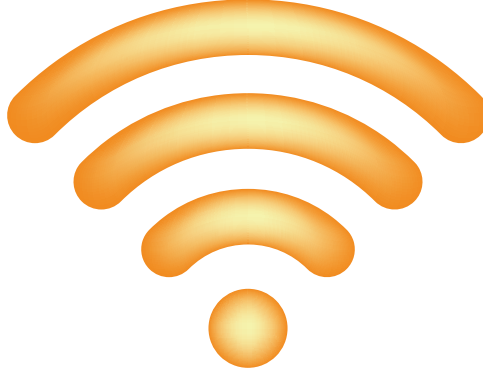




SAHTE KABLOSUZ AĞLAR

Kablosuz ağlar hayatımızın her anında karşımıza çıkmakta. Kablolu ağların aksine, sahip olduğu düşük maliyet ile yüksek erişilebilirlik durumundan dolayı kablolu ağları geride bırakarak çok hızlı bir gelişim gösterdi. Bunun sonucunda kablosuz ağlar, günün her anında rahatça internete bağlanmamızı sağlayarak mobil dünyanın vazgeçilmez bir parçası haline geldi.

Kablosuz ağ teknolojileri 20 yılı aşkın süredir hayatımızın bir parçası olmasının yanı sıra geleceğimizin de vazgeçilmezi olma yolunda ilerlemekte ve her geçen gün daha iyi bir bağlantı ve erişim sağlamak için gelişen ve çeşitlenen bir araç haline gelmektedir. Oldukça güçlü ve etkili bu araç, hayatımızı da iç içe geçmiş bir ağ şeklinde örmüştür. Bunun sonucunda hayatımızdan büyük ve önemli parçaları da artık içinde bulunduran bu gizemli ve tehlikeli ağı kullanabilmek için ona güvenmemiz gerekir.



Kablosuz ağların kullanımı arttıkça kablosuz güvenlik konusu daha da önem kazandı. Kablosuz ağların bu kadar erişilebilir olması saldırıların uygulanabilmesi için saldırganlara büyük bir fırsat sağlamaktadır. Saldırganlar standartlaşmış kablosuz güvenliği üzerinde açıklar aramakta ve çeşitli amaçlar doğrultusunda bazı yöntemler kullanarak saldırılar yapmaktadır.

Bu saldırılar bazen küçük etkiler yaratsa da ticari kuruluş ve önemli iletişim devamlılığı gerektiren sistemler için büyük zararlar verebildiği görülmüştür. Bu saldırıların temel amaçları gizli anahtarları ele geçirmek, kablosuz ağın iletişimini keserek diğer legal kullanıcıların iletişimini sabote etmektir.



Sahte Eriřim Noktası nedir?

Kullanıcının bulunduđu yerde sağlanan yasal bir erişim noktası gibi görünen, ama aslında kablosuz iletişimlari izlemek üzere bir korsan tarafından oluşturulmuş bir Wi-Fi erişim noktasına sahte erişim noktası denir.

Sahte AP (eriřim noktası) yayını, kurum isimleriyle veya insanların ilgisini çekebilecek bir SSID'yle (kablosuz bağlantı noktası adı) bir kablosuz ađ yayını yapmayı ifade eder. Bir nevi sosyal mühendislik saldırısı olan bu atakta kullanıcılar ađa bağlanır ve internete çıkarlar (eriřirler). Bütün trafikleri sahte AP üzerinden geçtiđi için arp zehirlenme*, DNS zehirlenme* gibi MITM (ortadaki adam) saldırıları veya oturum çalmak için sidejacking* ataklar yapmak mümkündür. Bu ataklardan en bilineni evil twin saldırısıdır.



ARP zehirlenmesi

Ađda MAC adresine göre iletilen paketin, aynı MAC adresini taklit ederek paketin ele geçirip, yönlendiriciye gitmesi gerekirken saldırganın eline geçmesini sağlayan saldırı türü.



DNS zehirlenme

DNS sunucularındaki açıklıklardan faydalanarak herhangi bir alan adının orijinalinden farklı bir IP adresine yönlendirilmesini sağlayan bir siber saldırı çeşididir.



Sidejacking

Oturum ele geçirme, bir bilgisayar sistemindeki bilgilere veya hizmetlere yetkisiz erişim elde etmek için geçerli bir bilgisayar oturumunun kullanılmasıdır.



Evil Twin (Kötü İkiz) Saldırısı Nedir?

Bir Evil Twin saldırısında saldırgan, internete bağlanan bir cihaz ve o interneti yayan router (yönlendirici) veya erişim noktası arasına girip hedeflemiş olduğu kişiye kendini interneti yayan yönlendirici gibi gösterir ve gerçek yönlendiriciye deauth saldırısı (Kullanıcının ağ bağlantısını kesme saldırısı) uygular. Gerçek yönlendirici, deauth saldırısından dolayı internet hizmetini yayamayacak durumda olacağından saldırgan bu arada devreye girer.

Saldırganlar, bir Evil Twin saldırısı gerçekleştirmek için öncelikle sabırsız kullanıcıları hedefler. Ne yazık ki birçok insan bu tür kullanım alışkanlığına sahiptir. Genellikle kafeterya veya halka açık bir alanda bulunduğumuz kuruluşun ücretsiz sunmuş olduğu wi-fi ağına girmek isteriz. Ancak bu isteğimizin bir bedeli olabilir. Saldırganlar güvenli görünen bir wi-fi ağının bağlantısını kendi internetini yayan bir yönlendirici gibi gösterebilir ve bu ağa bağlandığınızda kullanıcı olarak çevrimiçi yapılan her şeyi görebilir veya çalabilir.

Evil Twin saldırılar neden bu kadar tehlikeli?

Saldırganlar başarılı olduklarında cihazınıza erişilmesine izin verirler. Bu, oturum açma kimlik bilgilerini ve finansal veriler de dahil olmak üzere diğer özel bilgileri potansiyel olarak çalabilecekleri anlamına gelir (Kullanıcı Evil Twin wi-fi'ye bağlandığında finansal işlem gerçekleştirirse). Ayrıca bilgisayar korsanları cihazınıza kötü amaçlı yazılım da ekleyebilir.

Evil Twin wi-fi saldırıları çoğu zaman gerçek doğalarını ortaya çıkarabilecek açıklayıcı işaretler bırakmaz. İnternete erişim sağlama birincil görevlerini yerine getirirler ve birçok kurban bunu sorgulamaz. Kullanıcılar, kötü bir ikiz saldırısının kurbanı olduklarını ancak daha sonra kendi adlarına yetkisiz eylemler yapıldığını fark ederler.



Kötü İkiz Saldırı Örneği

Bir kullanıcının yerel bir kafede halka açık bir wi-fi ağına bağlanmaya karar verdiğini varsayalım. Oradaki erişim noktasına daha önce bağlandıysa, bu yüzden ağın güvenli ve güvenilir olduğunu varsayması durumu daha da kötüleştirir. Bir bilgisayar korsanı, aynı SSID adına ve meşru erişim noktasından daha güçlü bir sinyale sahip kötü bir ikiz ağ kurabilir. Kullanıcı, "Güvenli Değil" olarak listelenmesine rağmen ağa bağlanabilir.

Ağa bağlarken kullanıcı bakiyesini kontrol etmek için banka hesabına giriş yapar ve daha sonra işlerini takip etmek için şirketlerinin portalına* erişir. Kullanıcı verilerini şifrelemek için bir sanal özel ağ (VPN) kurmadığından, Evil Twin ağ, bilgisayar korsanının bankacılık bilgilerine ve şirket web sitesine erişmesine izin verir.



Kendinizi Kötü Bir İkiz Saldırıdan Nasıl Korursunuz?

Evil Twin saldırıları tespit etmek zor olabilir ancak halka açık wi-fi ağlarına bağlanırken kendinizi korumak için atabileceğiniz birçok adım vardır.

Kendi Erişim Noktanızı Kullanın

Kendinizi kötü niyetli bir ikiz saldırıdan korumanın en kolay yolu, mümkün olduğunca halka açık wi-fi yerine kişisel bir erişim noktası kullanmaktır. Bu, bilgisayar korsanlarının verilerinize erişmesini önler. Erişim noktanızı gizli tutmak için bir şifre belirlemeyi de unutmayın.

Güvenli Olmayan Wi-Fi Bağlantı Noktalarından Kaçının

Genel bir ağa bağlanmanız gerekiyorsa "Güvenli Değil" olarak işaretlenmiş erişim noktalarından kaçınmaya çalışın.

Güvenli olmayan ağlar, meşru güvenlik özelliklerinden yoksundur ve Evil Twin ağlar neredeyse her zaman bu atamaya sahiptir.

Bilgisayar korsanları genellikle bunu savuşturan ve riskleri bilmeden ağlara bağlanan insanlara güvenir.

Otomatik Bağlantıyı Devre Dışı Bırak

Cihazınızda otomatik bağlantı etkinse, kapsama alanına girdiğinizde daha önce kullandığınız tüm ağlara otomatik olarak bağlanır. Bu, özellikle geçmişte kötü bir ikiz ağa bilmeden bağlandıysanız halka açık yerlerde tehlikeli olabilir. Her zaman istediğiniz ağa bağlandığınızdan emin olmak için evinizden veya ofisinizden her ayrıldığınızda otomatik bağlantıyı devre dışı bırakın.

Genel Wi-Fi'de Asla Özel Hesaplara Giriş Yapmayın

Herkese açık wi-fi kullanırken mümkün olduğunca özel hesaplara giriş yapmaktan kaçınmalısınız. Bilgisayar korsanları, yalnızca şeytani ikiz ağlarına bağlıyken kullanırsanız oturum açma bilgilerinize erişebilir, bu nedenle oturumun kapalı kalması özel bilgilerinizin korunmasına yardımcı olabilir.

Trafiği Şifrelemek için VPN Kullanın

VPN, saldırganı görmeden önce verilerinizi şifreleyerek sizi Evil Twin saldırısından korumaya yardımcı olabilir. Cihazınıza güvenilir bir VPN uygulaması indirdiğinizde çevrimiçi etkinliğinizi ağa göndermeden önce şifreler veya karıştırır, bu da saldırganın okumasını ve anlamasını imkansız hale getirir.

Https Web Sitelerine Bağlı Kalın

Herkese açık bir ağ kullanırken yalnızca HTTPS web sitelerini ziyaret ettiğinizden emin olun. Bu siteler uçtan uca şifreleme sunarak saldırganların siz onları kullanırken etkinliğinizi izlemesini engeller.

İki Faktörlü Kimlik Doğrulamayı Kullan

Özel hesaplarınıza iki faktörlü kimlik doğrulama eklemek, saldırganların bunlara erişmesini önlemenin harika bir yoludur. Saldırganlar oturum açma bilgilerinize erişse bile, iki faktörlü kimlik doğrulama, onların hesabınıza başarıyla erişmesini engeller

Bir Saldırıya Kurban Olursanız Ne Yapmalısınız?

Saldırganın Evil Twin saldırı yoluyla verilerinizi ihlal ettiğini keşfederseniz Tüketici Şikayet Merkezine şikayette bulunabilirsiniz. Saldırganlar saldırı sırasında para çaldıysa veya bankacılık bilgilerinize erişim sağladıysa yerel polis departmanınızla ve bankanız veya kredi kartı şirketinizle de iletişime geçmelisiniz.

Evil Twin saldırıları, saldırganların çevrimiçi olarak hassas bilgilere erişmek için kullandıkları yöntemlerden yalnızca biridir. Kendinizi siber saldırılardan daha fazla korumak için saygın bir virüsten koruma yazılımı indirmeyi düşünün ve siber güvenlik haberlerini okuyun.

KAYNAKÇA

<https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks>
<https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/>
<https://ahmetemindilben.com.tr/evil-twin-saldirisi-nedir-nasil-yapilir/>
<https://www.siberportal.org/red-team/wireless-penetration-tests/rogue-access-point-attack-by-using-easy-creds-on-kali/>
<https://www.web-gelistirme-sc.com/tr/network/kotu-bir-ikiz-ve-haydut-bir-erisim-noktasi-arasindaki-fark-nedir/1968375292/>
<https://www.ozztech.net/siber-guvenlik/evil-twin-attack-seytani-ikiz-saldirisi-nedir/>
<https://www.bgasecurity.com/2015/03/szma-testlerinde-kablosuz-aglar-ve-atak-2/#:~:text=Sahte%20AP%20yay%C4%B1nC4%B1%2C%20kurum%20isimleriyle,a%C4%9Fa%20ba%C4%9Flan%C4%B1r%20ve%20internet%20%C3%A7%C4%B1karlar.>
https://docs.trendmicro.com/all/smb/wfbs-s/v9.0/tr-tr/wfbs_9.0_olhsrv/fake_access_pt.html
<https://www.netser.com.tr/tr/blog/kablosuz-ag-guvenligi-nedir>





SİBER İSTİHBARAT VE SİBER TEHDİT İSTİHBARATI

Siber İstihbarat ve Siber Tehdit İstihbaratı

Teknolojinin gelişmesiyle ve yaygınlaşmasıyla internet yaşantımızın vazgeçilmez bir unsuru hâline geldi. Gündelik hayatımızda bile hemen hemen her işimizi genel ağ ile bağlantıda ilerletmeye başladık. Yapacaklarımızı hızlı ve kolayca gerçekleştikçe de daha çok bağımlısı olduk. Artık internet, her sıkıntıda imdadımıza koşan bir dost oldu.

Ama işler bazen hiç de gözüktüğü gibi gerçekleşmiyor ve güvendiğiniz dostunuz sizin için en büyük tehdit hâline gelebiliyor. Bu nedenle var olan tehditlerden korunmak için saldırganların bir sonraki adımlarını bilmeliyiz ve önlem almalıyız. İşte bu noktada kurtarıcı niteliğinde olan siber istihbarat kavramıyla karşılaşıyoruz.

İstihbarat, toplanan verilerin işlenmesi sonucu anlaşılabilir hâle gelme sürecidir. Askerî, siyasi, sosyal, coğrafi, ekonomik vb. alanlarda istihbarat faaliyetlerini görebiliriz. Dijitalleşen dünya ile siber istihbarat da bu alanlar içerisine eklenmiştir. Siber istihbarat ile şirketler, verilerinin kimin tarafından ve hangi yöntemle tehdit edildiği bilgisine farklı yöntemlerle ulaşabilmektedir.

İstihbarat Toplama Yöntemleri

HUMINT: Kaynağının insan olduğu istihbarat yöntemidir. Hedef olarak belirlenmiş kişilerin casuslar ya da gizli ajanlar tarafından sorgulanması ya da takip edilmesiyle toplanan verilerdir.

OSINT: Gizlilik gerektirmeyen ve halka açık kaynaklardan (gazete, televizyon, sosyal medya vb.) bilgi elde etme yöntemidir. Çalışanlar hakkında bilgileri, sosyal ağ içeriklerini, kişisel blogları, paylaşım sitelerindeki fotoğrafları bu alanın tekniklerine örnek verebiliriz. Bu yöntem tamamıyla yasaldır.

SIGINT: Elektronik sinyallerden toplanan istihbarattır. COMINT (İletişim istihbaratı) ve ELINT (Elektronik istihbarat) olarak iki alt başlığa ayrılabilir. COMINT iletişim tabanlı olup ses ve veri içeren radyo dalgalarını kullanır. ELINT ise elektronik cihazlardan yayılan dalgaları kullanılır. Her ikisinden de ülkelere özel ve gizli bilgiler elde edilir.

GEOINT: Coğrafi konum istihbaratı da denir. Belirli alanlar, gözetleme uçakları, uydular gibi araçlarla yukarıdan görüntülenerek o bölgedeki insan faaliyetleri hakkında veriler toplanır.

Siber Tehdit İstihbaratı ve Siber Tehdit

Gerçek dünyada fiziksel ya da sözlü saldırılara uğrayabileceğimiz gibi güvenilir limanımız hâline gelmiş ve özel verilerin depolandığı sanal dünyada da tehditlere ve saldırılara maruz kalabiliriz. Hatta bu daha önceden tanımadığımız, dünyanın diğer ucunda olan bir birey tarafından gerçekleştirilebilir. Bu yüzden sanal ortamda depoladığımız verileri korumak için saldırıların kullandığı yöntemler ve bunlara karşı alınacak önlemler hakkında bilgi sahibi olmalıyız. İlk önce yöntem yani siber tehdit türlerinden bahsedelim.

Siber Tehdit

Bir kişi ya da topluluk tarafından cihazlarınıza ve içindeki verilere izinsiz erişim sonucu zarar verme faaliyetlerine siber tehdit denir. Maddi kazanç, verilerin değiştirilmesi veya silinmesi, kaotik bir ortam oluşturma, kişiyi kontrol etme gibi hedefleri olabilir. Günümüzdeki siber tehdit türlerine şunları örnek verebiliriz:

- Phishing (Oltalama)
- Malware (Kötü amaçlı yazılım)
- DDoS saldırıları
- Unauthorized Network Access (Doğrulanmamış ağ erişimi)
- Fidye yazılımı
- Kripto hırsızlığı
- Parola saldırıları
- 0-day Vulnerability (Sıfıncı gün zafiyetleri) vb.

Bu tehditler ile beraber dijital dünyada da istihbaratın önemi ortaya çıkmış, siber tehdit istihbaratı adını almıştır. Siber tehdit istihbaratı şirketlere, saldırı öncesi harekete geçebilmesi için verileri analiz ederek işlenmiş bilgiler sunar. İşlenme süreci 4 aşamalı ve sürekli tekrarlanan bir yaşam döngüsüdür.

Siber Tehdit İstihbaratın Yaşam Döngüsü:

1. İstihbarat İhtiyaçlarının Tespiti ve Yönlendirilmesi: Sürecin birinci aşamasında planlama yapıp hangi alanda istihbarat toplanacağına karar verilir yani ihtiyaçlar belirlenir. Böylece gereksiz bilgi ve zaman kaybının önüne geçilir. Saldırı hakkında olan ne, nerede, nasıl ve kim tarafından gibi soruların cevabının arandığı aşamadır.

2. Haberlerin Toplanması: Belirlenen ihtiyaçlar için harekete geçilen adımdır. Verilerin toplanması insani bir kaynaktan yapılabileceği gibi açık kaynaklardan (internet siteleri, televizyon, gazete vb.) da yapılabilir.

3. Haberlerin İşlenmesi: Farklı alt disiplinlerin beraber çalıştığı ve analizin gerçekleştirildiği aşamadır. Toplanan veriler bu aşamaya gelmeden ham veri şeklindedir. Veriler kategorilere ayrılır ve yorumlanarak bilgi hâlini alır. Diğer bir deyişle verilerin kişiler tarafından anlayabilecekleri forma dönüştüğü aşamadır.

4. İstihbaratın Yayımlı ve Kullanılması: Son aşamaya gelindiğinde toplanan veri artık bilgi hâlini almıştır ve müşteriye teslim için hazırdır. Son aşama bilgilerin ilgili kişilere ulaştırılmasını kapsar.

Siber Tehdit İstihbaratını 3 gruba ayırabiliriz:

1. Stratejik İstihbarat: Zarar verme potansiyeli olan kurum ya da kişilerin takibi sonucu elde edilen istihbarattır. Saldırganın amacı, yöntemleri, geçmişte yaptığı ya da yapabilme olasılığı olan saldırıları hakkında bilgiler içerir. Tehdit eden kişinin tanınmasını sağlar. Bu gruptaki bilgiler siber güvenlik alanında uzman olmayan kişiler için hazırlanmıştır.

2. Taktiksel İstihbarat: En kolay istihbarat türüdür ve yakın zaman odaklı olduğu için kısa süreli bir ömrü olabilir. Ağ üzerinde kötü amaçlı hareketleri belirleyen verileri içerir. Bu veriler şüpheli hareketlerdir. Olağan dışı bir ağ trafiği ya da artan indirme talepleri örnek verilebilir.

3. Operasyonel İstihbarat: Geçmiş verileri analiz ederek saldırı ve saldırıyı yapan kişi ya da kişiler hakkındaki soruları cevaplar. Taktikselden daha uzun ömürlüdür çünkü saldırıların saldırı yöntemlerini değiştirmeleri kolay değildir.

Siber Tehdit İstihbaratının Faydaları Nelerdir?

Veriler analiz edilerek olası saldırılara önlem alınır bilgilerin saldırıların eline geçmesi ve veri kaybı önlenir.

Saldırının gerçekleştirdikten sonra nasıl, nereden ve kimin tarafından gerçekleştirildiğinin önemi yoktur. Siber istihbarat anlık bir ihlalin farkına varılmasını sağlar.

Önceki yapılan saldırıların analizleriyle yenilerinin önüne geçilir.

Verilerin analiziyle sistem açıklarının belirlenmesini sağlar.

Toplanan istihbarat kurumlar arası paylaşılarak kitlesel bir mücadeleye olanak verir.

Siber Tehdit İstihbarat ve Siber İstihbarat Arasındaki Fark Nedir?

Siber istihbarat kurumları tehdit edebilecek unsurları belirlemek için gerçekleştirilen bilgi toplama sürecidir. Siber tehdit istihbaratı ise bütün bilişim teknolojilerini hedef alarak toplanan verileri anlamlı hâle getirmek için bir yaşam döngüsü içine sokar. Aslında farktan çok aralarında düzenli ve sürekli işleyen bir döngü vardır.

Güvenliğin ve veri ihlalinin önemine bu yıl gerçekleşen bir saldırıyı örnek vererek dikkat çekmek istiyorum. 15 Eylül tarihinde Uber'e genç bir hacker tarafından bir saldırı düzenlendi. Saldırı sosyal mühendislik yöntemini kullanarak yapıldı.

Sosyal mühendislik yöntemlerinden kısaca bahsetmem gerekirse:

Örneğin bir şirket çalışanısınız ve sizin bilgilerinizle sistem girişi yapıyor. Sahte kimliğe sahip saldırgan tarafından gelen mail ya da mesajla kandırılıyorsunuz ve sizin aracılığıyla şirket verilerinin ihlali gerçekleşiyor. Uber saldırısı da şirket çalışanına gönderilen kısa mesaj yardımıyla yapıldı. Olay, hackerin Slack üzerinden itirafta bulunması sonucu öğrenildi. Bu saldırıda veri ihlalinin gerçekleştiğini görüyoruz. Saldırı gerçekleştikten sonra kimin tarafından ve nasıl gerçekleştiği bilgilerini öğrenmemiz bize bir fayda sağlamadı. Çünkü veri ihlali çoktan gerçekleşmiş ve paylaşılmıştı. Sonuç, itibar kaybı ve kullanıcıların şirkete karşı güven eksikliği oldu. Bu saldırı örneğinde bir maddi kayıp yaşanmadı ama yaşanabilirdi de.

Yazımızın da konusu olan siber istihbaratın önemi de burada ortaya çıkıyor. Eğer kurum tarafından bu konuya saldırı öncesi önem verilseydi hacker daha açığı bulmadan kapatılıp önlem alınabilirdi.

Sosyal ağdayken yalnız olmadığımızı unutmamalıyız. Bize karşı mevcut ya da olası tehditlerin karşısında bilinçli olmalıyız. Şimdiye kadar bir saldırı yaşamamanız bunun gerçekleşmeyeceği anlamına gelmez. Hatta bu cümleleri okurken bile verilerinizin çalınmadığını bilemezsiniz. Bilinçli ve tedbirli olmanız dileğiyle...

KAYNAKÇA:

Slack, bulut tabanlı bir ekip iş birliği uygulamasıdır.

<https://www.bgasecurity.com/2019/07/siber-istihbarat-nedir/>

<https://www.bgasecurity.com/2019/06/siber-tehdit-istihbarati-veri-toplama-ve-isleme/>

<https://seccops.com/hizmetler/siber-istihbarat-hizmeti/>

<https://www.bgasecurity.com/2018/01/siber-tehdit-istihbarati/>

<https://gaissecurity.com/blog/siber-istihbarat-ve-siber-tehdit-istihbarati/>

<https://berqnet.com/blog/siber-istihbarat>

<https://www.kaspersky.com.tr/resource-center/definitions/threat-intelligence>

https://en.wikipedia.org/wiki/Geospatial_intelligence

<http://ozdenercin.com/2019/03/29/osint-open-source-intelligence-acik-kaynak-istihbarati/>

https://tr.wikipedia.org/wiki/Elektronik_istihbarat

<https://tr.wikipedia.org/wiki/COMINT>





TEHDİT AKTÖRLERİ VE MOTİVASYON KAYNAKLARI

TEHDİT AKTÖRLERİ ve MOTİVASYON KAYNAKLARI

Siber Tehdit Nedir?

Siber tehdit, bir bilgi teknolojisi varlığına, bilgisayar ağına, fikri mülkiyete veya herhangi bir hassas veriye yetkisiz erişim sağlamayı, zarar vermeyi, bozmayı veya çalmayı amaçlayan başarılı bir siber saldırı olasılığını ifade etmektedir. Siber tehditler güvenilir kullanıcılar tarafından bir kurum ya da kuruluş içerisinde ya da bilinmeyen konumlardan gelebilmektedir.

Siber Tehdit Kategorileri Nelerdir?

Ağ Saldırıları

Ağ yapısına zarar verme, çalışma performansını etkileme amacı taşıyan saldırganlar sistemin çalışmasına zarar verecek zafiyet ve açıklıklardan yararlanarak saldırı gerçekleştirilmektedir. Bu saldırılardan korunmak için sistem ve yazılımların güncel kalmasını sağlamak gerekmektedir.

Saldırganlar ağa çok sayıda istek ve IP paketi göndererek CPU ve RAM gibi sistem için hayati öneme sahip kaynakları hedef alabilmektedir. Bu tür saldırılar tipik botnet ve zombi saldırılarını kapsamaktadır, iletişim altyapıları sayesinde uzaktan kontrol edilebildikleri gibi farklı türde saldırılar başlatabilecek komutlar da içerebilmektedir. Çözüm odaklı ürünler kullanarak bu saldırılara karşı bilinçlenmek ve koruma sağlanmalıdır.

Mobil Uygulama Saldırıları

Günümüzde teknolojinin gelişmesiyle akıllı telefon, tablet gibi mobil cihazların kullanımı yaygınlaşmıştır. Hızla büyümeye devam eden mobil dünyada pek çok işletme iş süreçlerini mobil uygulamalar üzerinden yürütmektedir. Bu durum saldırganlar için geniş bir atak yüzeyi oluşturmaktadır. Mobil uygulama saldırılarında saldırgan tarafından erişim yükseltilmesi, kişisel verilerin sızdırılması, bilgilerin dışarıya aktarılması, kötü amaçlı yazılımların çalıştırılması gibi güvenlik sorunlarına yol açabilecek güvenlik açıkları ve yanlış yapılandırmalar kullanılmaktadır.

Mobil uygulama güvenliğindeki temel problem, mobil cihaz kullanıcılarının indirdikleri ve kullandıkları uygulamaların gerçekte ne yaptığını bilmemesinden kaynaklanmaktadır. Bir mobil uygulama, kötü niyetli saldırılar için en kolay giriş noktaları arasında yer almaktadır. Mobil uygulamalarda yaygın olan güvenlik tehditleri hakkında bilgi edinerek, hassas verileri güvende tutmak için kapsamlı bir mobil güvenlik stratejisi uygulanması gerekmektedir.

Web Uygulama Saldırıları

Web uygulama güvenliği, üzerinde bulundurduğu verilere gizlilik, bütünlük ve erişilebilirliğin sağlanabilmesi amacıyla alınan tedbirlerin tümünü ifade etmektedir. Web uygulamalarındaki kod kaynaklı zafiyetler veya sunucu-istemci kaynaklı zafiyetlerin kullanılması ile yapılan saldırılar web uygulama saldırıları olarak adlandırılmaktadır. Açıklıkların istismar edilmesi, kişi ve kurumlar için maddi ve manevi zararlara neden olabilmektedir. Bankacılık ve e-ticaret gibi kullanıcıların hassas bilgilerini işleyen web uygulamalarının güvenlik testlerinin yapılması şirketlerin iç ve dış kaynaklarının korunması için önem arz etmektedir. Web uygulamalarına yönelik yapılan saldırıları önleme amacıyla geliştirilen akademik ve ticari birçok güvenlik çözümü bulunmaktadır, saldırılardan korunmak için bu çözümler tercih edilebilmektedir.

Host Tehditleri

İşletim sistemleri, veri tabanı sunucuları, güvenlik duvarları, posta sunucuları vb. teknolojilere yapılan saldırılar host tehditlerine girmektedir. Ana bilgisayarların işletim sisteminin ve uygulamalarının uygun şekilde sıkılaştırılarak daha güvenli hâle getirilmesi tehditlere karşı en iyi korunmayı sağlamaktadır.

İnsan/Kullanıcı/Çalışan Hedefli Saldırıları

İnsan davranışlarındaki yanlışları veya zaafları kötüye kullanarak bir sistemin ele geçirilmesi mümkün olmaktadır. Örneğin saldırganlar kurum çalışanları arasındaki zayıf halkayı hedefleyip bu kişilerin zafiyetleri ve hatalarını sosyal mühendislik adı verilen teknikler ile kötüye kullanarak sistemlere izinsiz erişim elde edebilmektedirler. Bu tip saldırılarda zarar verilmek istenen hedef her zaman firma değil insan yani kurbanın kendisi de olabilmektedir. Bu noktada siber güvenlik farkındalığına sahip olmak kişinin kendisini ve bağlantılı olduğu kişileri/kurumları koruması için önemli hâle gelmektedir.

Siber Tehdit Aktörlerinin Profilleri

Tehdit Aktörü: Tehdit aktörü bir kurumun/kişinin güvenliğini etkileyen olaylardan veya potansiyel olaylardan sorumlu kişi/kişiler veya kurum/kurumlardır. Kötü niyetli aktörler olarak da tanımlanabilmektedir.

Hacker: Genel anlamıyla “hack” kelimesi bir sisteme izinsiz erişim elde etmek anlamına gelmektedir. Bu eylemi gerçekleştiren kişiler ise “hacker” olarak adlandırılmaktadır. Bu terim popüler kültürde “bilgisayar korsanı” ile ilişkilendirilmiştir, teknik bilgisi ile bilgisayar sistemlerine girmek için hata veya istismar kullanan kişilerdir.

Saldırgan: Siber saldırılar, bilgisayar sistemlerine yetkisiz erişim sağlama ve verileri çalma, değiştirme veya yok etme girişimleridir. Saldırgan, kullanılan yöntemden bağımsız olarak bu kötü niyetli faaliyetleri gerçekleştiren kişi veya kuruluştur.

Bir tehdit aktörü, bir bilgisayar korsanı veya saldırganla karşılaştığında herhangi bir teknik beceriye sahip olmayabilir. Kötü niyetli şekilde bir kişi/kuruluşun güvenliği-ni veya verilerini tehlikeye atma misyonu güderken fiziksel imhadan hassas bilgileri kopyalamaya kadar her yöntemi kullanabilmektedir.

Bilgisayar korsanları (hacker), faaliyetlerini yürütmek için güvenlik açıklarını ve zafiyetleri kullanmaktadır. Saldırganlar ise tahribat yaratmak için herhangi bir yolu kullanabilmektedirler. Örneğin bir saldırgan, hedeflerine ulaşmak için hassas dosyaları silen veya işi herhangi bir şekilde kesintiye uğratan, firma içerisinde barınan mut-suz bir çalışan olabilmektedir. Saldırgan basitçe bir sistemin anahtarını kapatarak hedeflediği zarara ulaşabilirken bir bilgisayar korsanı aynı zararı teknik birikimiyle güvenlik açıklarını, yanlış yapılandırmaları ve zafiyetleri kullanarak vermektedir.

Tehdit Aktörü Türleri

Hackivistler: Genelde politik amaçları olan saldırganlardır. Propagandalarına yardımcı olan yüksek etkili saldırılar oluşturmayı veya karşı oldukları kuruluşlara zarar vermeyi hedeflemektedirler. Niyetlerinin temeli kendilerine fayda sağlamak ve problem olarak gördükleri bir konuya dikkat çekebilmektir.

Organize Suç Ekipleri: Bu saldırı grupları en fazla kârı getirecek eylemleri gerçekleştirmeyi hedeflemektedir. Müşterilerin ve çalışanların sağlık kayıtları, so-syal güvenlik numaraları, kredi kartları ve bankacılık bilgileri gibi hassas kişisel verileri ele geçirip bunlar üzerinden fidye talebinde bulunmaktadır.

Devlet Destekli Tehdit Aktörleri: Devlet tarafından iyi finanse edilerek karmaşık hedefli saldırılar gerçekleştirmektedirler. Casusluk amacı gütmektedirler ve genellikle moti-vasyonları politik, ekonomik, teknik veya askerî sebeplerden oluşmaktadır.

Siber Teröristler: Belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanan kişi veya gruplardan oluşmaktadırlar. İnternet terör eylemi olarak kabul edilen eylemleri gerçekleştirmektedirler.

Fırsatçı Kişi/Kişiler: Bu saldırganlar genellikle şöhret arzusıyla hareket eden amatör suçlulardan oluşmaktadır. Her zaman zarar verme amacıyla hareket et-

mezler bazen kuruluşların güvenlik açıklarını bulmasına ve kapatmasına yardımcı olarak isim duyurmaya da çalışabilirler.

Mutsuz Çalışanlar: Kurumlara karşı kötü niyetli faaliyet gösteren kişiler, intikam almak veya bir tür mali kazanç elde etmek isteyen hoşnutsuz çalışanlar ya da eski çalışanlar olabilmektedir. Bazen kurum içerisindeki kişiler, organize suç veya devlet destekli bilgisayar korsanları gibi diğer tehdit aktörleriyle, sadakat duygusu, para veya prestij karşılığında iş birliği yapabilmektedirler.

Gelişmiş Kalıcı Tehditler (APT)

APT Nedir?

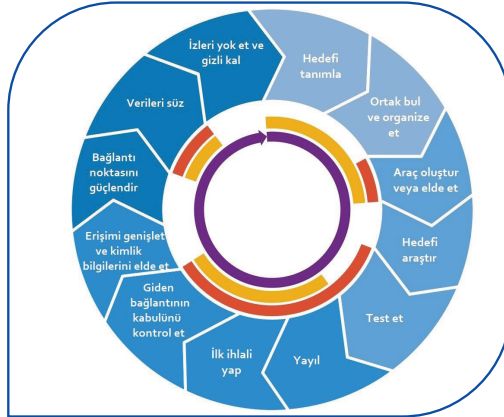
Gelişmiş Kalıcı Tehdit (Advanced Persistent Threat) bir kişi veya grubun bir ağa yetkisiz erişim sağladığı ve uzun bir süre algılanamayan bilgisayar ağı saldırısıdır. APT grupları, sofistike siber saldırılar gerçekleştirebilecek bilgisayar korsanlarından (hacker) oluşmaktadır. Bu gruplar, daha önceden kullanılmış saldırı tekniklerini kullanabilmekte veya bir “zero day” zafiyeti keşfederek daha önceden gerçekleştirilmemiş siber saldırılar ortaya çıkarabilmektedir. APT saldırılarını klasik saldırı yöntemlerinden ayıran temel neden saldırganların davranış biçimleridir. Çoğunlukla otomasyona dayanmayan manuel saldırılar olarak bilinen APT saldırılarında vur-kaç mantığı kullanılmaz. Amaçları sisteme zarar vermekten çok, ağa erişip sistemi alarma geçirmeden verileri çıkarmak için yeterince içeride kalabilmektir.

Bilgisayar korsanı grubu veya APT, saldırıyı sabotajdan ticari casusluğa; fikri mülkiyet unsurlarını çalmaktan kişisel finans bilgilerini toplamaya kadar değişebilen belirli bir amaçla tasarlanmaktadır. Ulus devlet destekli saldırılar ile doğrudan bağlantılı olabildikleri gibi bunlardan bağımsız şekilde de geniş çaplı hedeflere izinsiz erişim sağlayabilmektedirler. Mevcut güvenlik önlemlerini aşmak ve olabildiğince çok zarara fark edilmeden yol açmayı hedeflemektedirler. Kararlı ve deneyimli bir suçlu grubu istediğini almak için pek çok giriş noktasından faydalanabilir ve aylarca, yıllarca tespit edilmeyebilir. APT saldırılarındaki en büyük tehlike, keşfedilseler ve mevcut tehdit ortadan kalkmış gibi görünse bile korsanlar, diledikleri zaman geri dönmek için birden fazla kapıyı açık bırakmış olabilmektedirler. Ayrıca anti virüs ve güvenlik duvarları gibi birçok geleneksel siber savunma yöntemleri çoğu zaman bu tür saldırılara karşı koruma sağlamamaktadır.

APT Yaşam Döngüsü

Gelişmiş sürekli tehditlerin arkasındaki aktörler, bir süreç ya da öldürme zincirini izleyerek hedef kuruluşlar için artan ve değişen bir risk oluşturur:

- 1- Tekil hedef için belirli kuruluşları hedefleme
- 2- Çevrede yer edinme girişi
- 3- Tehdit altındaki sistemleri hedef ağı erişim olarak kullanma
- 4- Saldırı hedefini gerçekleştirmeye yardımcı olan ek araçlar kullanma
- 5- Gelecekteki inisiyatiflere erişimi korumak için izleri örtme



Şekil 1: APT yaşam döngüsünü ayrıntılı gösteren şema

Not: Şekildeki yaşam döngüsü görseli ilgili linkten alınmış yukarıda SmartArt hâlinde eklenmiştir.

Link: <https://www.bgasecurity.com/2019/05/siber-guvenlik-saldirilarinin-motivasyon-ve-amaclari-bolum-5/>

Siber Saldırıların Motivasyon ve Amaçları

Siber saldırılara karşı etkin bir şekilde mücadele edebilmek için saldırıların arkasındaki amaçları ve motivasyonu anlamak gerekmektedir. Siber saldırıların yöntemleri ve amaçları çeşitlilik gösterse de ana motivasyonlar aşağıdaki başlıklar altında incelenebilir:

Siyasi veya Sosyal Açından Tarafı Bir Nuktada Bulunmak: Bilgisayar korsanları, hükümetlerden, politikacıardan, toplumdan, büyük marka şirketlerden ve güncel olaylardan herhangi birine yönelik eleştirilerini ifade etmek için saldırılabilmektedir. Örneğin kendileriyle aynı fikirde olmadıklarında hedefin web sitelerini çökertmek gibi saldırılar yapabilmektedirler.

Mali motivasyonlar: Bir kuruluşun saldırıya uğramasının en olası nedeni mali motivasyonlardır. Siber saldırıların yaklaşık dörtte üçü esas olarak doğrudan finansal hesaplardan para çalmak, kredi kartı bilgilerini ele geçirmek, veri ihlallerine neden olmak, fidye talep etmek gibi finansal kazançları hedeflemektedir.

İdeolojik Motivasyonlar: Müşterilere karşı olan itibarın kaybedilmesini, hizmet verme kalitesinin düşmesini amaçlayan düşmanlar bulunabilmektedir. Örneğin rekabette olan iki firmadan biri diğerinin hizmet kesintisine sebebiyet vererek kurbanın müşterilerini almaya çalışabilmektedir. İdeolojik motivasyon içeren saldırılar her zaman dışarıdan gelen tehditler olmamaktadır. Kurum içerisindeki mutsuz bir çalışan veya kurumla sıkıntı yaşamış eski bir çalışan da aynı motivasyonu paylaşabilmektedir.

Siyasi Motivasyonlar: Devlet destekli saldırıların arkasında siyasi motivasyonların bulunması oldukça yüksek bir ihtimaldir. Saldırı çapı büyük ve geniş kaynaklara sahip olan saldırıların çoğunluğu bu motivasyonu paylaşmaktadır.

KAYNAKÇA

<https://www.upguard.com/blog/cyber-threat>
<https://www.beyondtrust.com/blog/entry/difference-between-a-threat-actor-hacker-attacker>
<https://www.csoonline.com/article/3203804/know-your-enemy-understanding-threat-actors.html#/>
<https://www.kaspersky.com.tr/resource-center/definitions/advanced-persistent-threats>
<https://www.lifars.com/2020/03/motivations-behind-cyber-attacks/>
<https://www.bgasecurity.com/2019/05/siber-guvenlik-saldirilarinin-motivasyon-ve-amaclari-bolum-5/>
<https://www.innova.com.tr/tr/blog/guvenlik-blog/mobil-uygulamaların-guvenligini-nasil-saglayabilirsiniz>
<https://www.bgasecurity.com/2019/05/siber-guvenlik-tehdit-kategorileri-bolum-4/>
<https://dergipark.org.tr/tr/download/article-file/209001>
<https://cahitcengizhan.com/siber-tehdit-aktorleri-2/>
<https://dergipark.org.tr/tr/download/article-file/401125#:~:text=Web%20uygulama%20g%C3%BCvenli%C4%9Fi%2C%20%C3%BCzerinde%20bulundurdu%C4%9Fu,ve%20manevi%20zararlara%20neden%20olabilmektedir.>





İNTERNETİN KARANLIK DÜNYASI

İnternetin Karanlık Dünyası

İnternet sonsuz bir bilgi kaynağı... Her zaman bu bilgi kaynağına ihtiyaç duyuyoruz. Fakat sanılanın aksine sadece sınırlı bir kısmına ulaşabiliyoruz. Peki ulaşamadığımız kısımda gizli neler olabilir? Hiç bu kısmı merak ettiniz mi? İşte internetin diğer yüzü Dark Web.

Herkesin rahatlıkla giremediği, girmek için özel tarayıcılar gerektiren, genellikle yasal olmayan gizli bilgilerin ve içeriklerin bulunduğu ağıdır. Gizli olması herkes için merak uyandırdığı kadar korku da uyandırır. Uyuşturucular, yasadışı silahlar ve çeşitli dolandırıcılıklar Dark Web'de karşılaşılabileceğiniz yasal olmayan öğelerden sadece bazılarıdır. Çoğunlukla yasal olmayan öğeler barındırırken yasal olanları da barındırır. Veri tabanları, şirketlerin kendi yapısında oluşturduğu ağlar, aynı şekilde hükûmetlerin özel ağlarını da bu yasal bilgilere örnek verebiliriz.

Dark Web nasıl ortaya çıktı? Neden ortaya çıktı ve çıkmasını tetikleyen unsurlar nelerdir?

Dark Web günümüzde popüler olsa da internet kadar eski bir kavramdır. Aslında her şey ARPANET ile başlamış gibi gözüküyor. ARPANET Birleşik Devletler Savunma Bakanlığı bünyesine bağlı ARPA tarafından geliştirilen dünyanın ilk paket dağıtım ağı ve evrensel internetin öncüsüdür. Tabii o zamanlar kişisel bilgisayarlar herkeste yoktu. Zamanla her evde bir bilgisayar olmaya başladı ve internete ulaşım kolaylaştı. Bu şekilde dünya küreselleşiyordu fakat verinin gizliliği ne durumdaydı? Veriler nerede saklanmalıydı? Farklı yollar deneseler de güvenlik önlemlerini alamadılar. Bu yüzden erişim gizliliği olan Dark Web ortaya çıktı.

Dark Web'e nasıl giriş yapılır?

Dark Web'e Chrome, Firefox gibi normal tarayıcılar ile erişim sağlayamayız. Dark Web'e özel tarayıcılar sayesinde girilir. Bunlara örnek Tor gibi tarayıcılarıdır. Tor başlangıçta ABD istihbaratının çevrimiçi iletişimini korumaya yardımcı olmak için geliştirilmiştir. Şu anda ise karanlık web'deki sitelere ulaşmanın birkaç yolundan biridir. Bu tarz tarayıcıları kullanarak erişim sağlandığınızda anonim olursunuz. Sanal Özel Ağlar yani VPN de Dark Web'e erişim için özel izin veren sunucuları sunar.

Tor ile giriş yaparsak güvende olur muyuz?

Tor, gizli sekmelerin tüm bilgileri unutmaz özelliklerini sağlarken gezinme alışkanlıklarınızı ve kullandığınız aygıt hakkındaki bilgileri de gizleyerek, uçtan uca tamamen gizli ve gerçek anlamda kişisel bir tarama sunar. Sizin bilgilerinizi gizleyerek anonim yapar. Bu yüzden güvenlidir diyebiliriz.

Dark Web'e girmek ne kadar güvenli?

Dark Web'e girmek tehlikeli olabilir. Çünkü kolay erişim sağlanamaz ve nasıl giriş yapılacağı bilinmiyorsa tehlikede olabilirsiniz. Eğer güvenli bir şekilde girmek istiyorsanız Tor gibi araçları kullanarak güvenli giriş yapabilirsiniz.

Güvenli erişimi sadece Tor ile yapabilir miyiz? Nasıl daha güvenli olabiliriz?

Kullandığınız posta adresini, parolalarınızı ve kişisel bilgilerinizi normal hayatınızda kullandıklarınızdan farklı seçmelisiniz. Aksi takdirde sizin bilgilerinize kolayca ulaşabileceklerdir.

Dark Web üzerinden paylaşılan dosyaları indirmemelisiniz. Giriş yaptığınız tarayıcının erişim izinleri olabildiğince kısıtlamalısınız.

Dark Web'e girmek yasak değildir. Ancak Dark Web'in içinde yasal olmayan adreslere yönlendirilebilirsiniz. Eğer ki yanlış adresi girerseniz ya da size internet üzerinden bir davetiye gönderilirse ve bu adreslerde herhangi bir aktivitede bulunursanız suçlu duruma düşebilirsiniz. Aynı şekilde yasal olmayan alışveriş (örneğin uyuşturucu, kaçak silah alımı) gerçekleştirirseniz suçlu olursunuz ve ceza alırsınız.

Yukarıda bahsettiğimiz suç durumu olaylarına örnek bir haber:

Avrupa Birliği Polis Teşkilatı (Europol) öncülüğünde eş zamanlı olarak dokuz ülkede gerçekleştirilen operasyonda, internetteki "Karanlık Web" üzerinden yasa dışı ticaret yaptıkları belirlenen 150 kişi gözaltına alındı.

"Dark Hunter" (Karanlık Avcı) adı verilen operasyonda 26.7 milyon euro tutarında nakit ve sanal paranın yanı sıra 234 kilo uyuşturucu ve 45 ateşli silah ele

geçirildi. Europol ve Eurojust tarafından yönlendirilen operasyona Avustralya, Bulgaristan, Fransa, Almanya, İtalya, Hollanda, İsviçre, İngiltere ve ABD güvenlik birimleri katıldı.

Dark Hunter Operasyonu, dünyanın en büyük yasa dışı pazarı olan “Dark Market”in kapatılarak sunucularına el konmasının ardından elde edilen bilgiler ışığında gerçekleştirildi.

Almanya polisinin, karanlık ağdaki pazarın işletmecisi olduğu iddiasıyla tutukladığı kişiden önemli kanıtlar elde ettiği açıklandı.

<https://www.bbc.com/turkce/haberler-dunya-59055369>

Dark Web’de ulaşabileceğimiz veri türleri; veri sızıntısı sonucu ele geçirilen kimlik numaraları, ücretli platformlara ait kullanıcı adı ve parola bilgileri, yasa dışı maddelerin satışı, rahatsız edici hizmetler, sahte teknolojik ürün satışı, kiralık katiller ve benzeri illegal dünyadır.

Bir haberle örnek verecek olursak:

Gerçekleşen bir veri ihlali sonrası elde edilen bilgiler internetin karanlık yüzü olarak bilinen Dark Web’de satışa çıkarılıyor. Hackerlerin kendi aralarında gerçekleştirdikleri pazar ortamında sızdırılan kullanıcı bilgileri 2 dolara alıcılarını buluyor. En son ünlü yayın platformu Disney+ gerçekleşen veri sızıntısında milyonlarca kullanıcının bilgilerinin satışa çıkarıldığını da hatırlatan Gürsel Tursun, platformlara ya da şirketlere gerçekleşen saldırıların başka boyutlarda tekrardan tehlike yaratabildiğini ve bunun neticesinde hem şirket hem de kullanıcıların da çeşitli zararlar görebildiğini aktarıyor.

<https://www.hurriyet.com.tr/teknoloji/kullanici-larin-ozel-bilgileri-dark-web-uzerinden-2-dolara-satiliyor-41548141>

Dark Web diğer yüzeysel ağlara nazaran çok daha fazla tehdit ve olumsuzluk içerir. Bunun bilincinde olarak erişim sağlamak gerekmektedir.

Karşılaşabileceğimiz tehdit türleri:

Keylogger, fidye ve bot gibi kötü amaçlı yazılımlar cihazlarımıza sızabilir.

Dolandırıcılar burada aktif olarak bulundukları için güvenli erişim yapmazsanız ve hizmet almak isterseniz dolandırma riskiyle karşı karşıya kalabilirsiniz.

Bu tehditlerden kaçınmak için almanız gereken birkaç kolay önlem vardır.

Dark Web tehditleri günümüzde yaygındır ve bunun önüne geçilmesi gerekmektedir.

Antivirus yazılımları kullanmak, kötü amaçlı yazılımlardan büyük ölçüde kaçınmanızı sağlar.

Ayrıca kimlik koruması yapan çeşitli uygulamaları da kullanmanız sizi Dark Web tehditlerinden koruyacaktır.

Bir haberle örneklendirsek:

Hackerler 1 Milyondan Fazla Kredi Kartını Dark Web'e Sızdırdı

BidenCash adlı bir karanlık web pazarı, 1.2 milyondan fazla kredi kartının ayrıntılarını çevrimiçi olarak yayımladı. Bleeping Computer tarafından yayımlanan bir rapora göre sızıntıda kart numaraları, son kullanma tarihleri, CVV numaraları, kart sahibi isimleri, banka isimleri, kart türleri, fiziksel adresler, e-posta adresleri, Sosyal Güvenlik numaraları ve telefon numaraları gibi bilgiler yer alıyor. Bu bilgiler siber suçluların finansal dolandırıcılık ve kimlik hırsızlığı yapmaları için yeterli. Kartların çoğunluğu ABD'den gelirken diğerleri Hindistan, Brezilya, Birleşik Krallık, Meksika, Avustralya, İspanya ve Çin'den geliyordu. Bazı kartların süresi 2023'ten önce dolmazken diğerleri 2026'ya kadar geçerliliğini koruyacak.

<https://hwp.com.tr/hackerlar-1-milyondan-fazla-kredi-kartini-dark-we-be-sizdirdi-218797>

Peki araştırdık, güvenliğimizi sağladık ve giriş yaptık. Bundan sonraki ve en önemli aşama ne? Korunmak! Yukarıda belirttiğimiz gibi kendinizi güvene alırsanız, erişim yaparken kısıtlandırırsanız, kendinize ait bilgileriniz ile erişim yapmazsanız, Dark Web'de herhangi bir şeyi indirmezsensiz ve bunun gibi güvenli önlemler alırsanız biraz daha tehlikeyi azaltabilirsiniz.





KRİTİK ALTYAPILARIN GÜVENLİĞİ

Kritik Altyapıların Güvenliđi

Kritik altyapı sistemleri; her türlü faaliyetin yürüyeabilmesi, gündelik yaşamın aksamadan sağlanmasında kullanılan büyük önem arz eden sistemlerin, internet aracılığı ile kontrol edildiđi sistemlerdir. Kritik altyapılar ülkelerin ekonomik-sosyal işleyişlerini sürdürebilmeleri ve devamlılıklarının sağlanmasında önemli yere sahip olan sistemlerdir. Sadece ülkelerin kendi bünyelerinde deđil global olarak tüm dünyanın iletişiminde uluslararası öneme sahiptir. Kritik altyapılar internetin yaygınlaşması ve siber güvenlik kavramının güvenli bir internet ortamı oluşturması sonucunda oluşmuştur. Bu altyapıların kontrol edilebilmesi ve devamlılıklarının sürdürebilmesi için internet gerekmektedir.

1997 yılında Amerika Birleşik Devletleri tarafından hazırlanan “Amerika Birleşik Devletleri Başkanlık Komisyonu’nun Kritik Altyapıların Korunması Hakkında” yazdıkları raporda ilk defa kritik altyapı terimi kullanılmıştır. Devlet düzeninin ve toplum işleyişinin sağlanması, en sağlıklı şekilde işlemesi için gerekli ve birbiriyle bağlantılı sistemleri anlatmak için kullanılmıştır. Kritik altyapı sistemi ülkemizde siber güvenliğin sağlanması hakkında 2012 yılında oluşturulan Siber Güvenlik Kurulu’nun ilk toplantısında “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planıyla” kabul edilmiştir.

Ükelere, devletlere ait özel bilgiler barındıran,, barındırdığı bilgilerin nitelikleri ve herhangi bir siber saldırı sonucunda üçüncü kişilerin ulaşabilmesi tehlikesinde kişi ve kişilerin can ve mal kaybına, telafi edilemez hasarlara, ulusal hatta uluslararası güvenliğin bozulmasına sebep olabilecek sistemleri içeren karmaşık ve büyük sistemlerdir. Bu sistemlerin kapsayabileceđi altyapılara birkaç örnek olarak bilgi ve iletişim teknolojileri, sağlık hizmetleri, ulaşım araç ve ađları, gıda ve üretim sistemleri verilebilir. Kritik altyapı kavramının birçok ürün ve hizmeti bünyesinde barındırdığı görölmektedir.

Teknolojinin gelişmesi hayatımızı her ne kadar kolaylaştırmış ve fayda sağlamış olsa da bir o kadar risk ve tehdide açıktır. Kritik öneme sahip bu iletişim teknolojisinde oluşabilecek tehditler, siber boyutta savaşlara sebep olabilir. Savaşlar cephelerden internet ortamına taşınmıştır.

Kritik altyapıyı tehlikeye atabilecek pek çok tehdit unsuru bulunmaktadır. İnsanlardan bağımsız olarak oluşabilecek doğal olayların yanı sıra insan hataları ya da terörizm ve savaşlar, büyük hasarlara neden olabilecek durumlardır.

Tam bu noktada siber dünyayı kontrol altına almak ve bu tehditlere engel olabilmek için savunulmaya ihtiyaç vardır. İnternet ortamında bilgilerin yayılma hızı saniyeler içerisinde çok büyük kitlelere ulaşabilecek kadar ciddi bir durumdadır. Siber güvenliğin ulusal ve uluslararası güvenlik açısından önemi çok fazladır.

Şekil-1

Doğal Olaylar	Teknik/İnsan Hataları	Terörizm, Suçlar ve Savaş
Meteorolojik afetler	Sistemsal hatalar (örn: yetersiz planlama)	Terörizm
Jeolojik afetler	İhmal ve dikkatsizlik	Sabotaj
Salgın hastalıklar	Kazalar ve acil durumlar	Diğer suçlar
Kozmik olaylar (örn: meteor yağmuru)	Organizasyondan kaynaklanan hatalar (örn: koordinasyon eksikliği)	Savaşlar

Kaynak: Claudia Bach, Anil K. Gupta, Sreeja S. Nair and Jörn Birkmann, 'Critical Infrastructures and Disaster Risk Reduction', ss.17

Kritik altyapıların güvenliğinin tam anlamıyla sağlanması mümkün olmasa da üzerinde her ülke, kurum ve kuruluşun farklı yaklaşımları olan ve korunması son derece önemli olan bir yapıdır. Türkiye'de bu kurumlardan birine AFAD'ı örnek gösterebiliriz. Her ne kadar AFAD'ın çalışmaları, genel olarak doğal afetler sonucu oluşabilecek durumlara önlem almak ve oluşan problemleri çözmeye çalışmak olarak gözüküyor olsa da siber güvenlik alanında tehditlere karşı hazırlıklı olmak gibi önlemleri ve bu konuda çalışmaları da vardır.

Sonuç olarak kritik altyapıya dâhil olan ya da gelecek yaşantımızda bu bünyeye dâhil olabilecek bütün sistemlerle şahısların, toplum ve toplulukların, devletlerin, uluslararası ilişkilerin güvenliği için tüm kurum ve kuruluşların kendi kritik bilgilerini koruması için saldırılara hazır bir durumda bulunması gerekir.





VERİLERİMİZİN DÜŞMANI KUANTUM BİLGİSAYARLAR

VERİLERİMİZİN DÜŞMANI: KUANTUM BİLGİSAYARLAR

Son otuz yıldır küresel iletişimin dijital altyapısının bir bileşeni olan açık anahtarlı krypto sistemler, gün geçtikçe daha da önem kazanmaktadır. Mobil iletişim, ekonomi, iş dünyası, sosyal ağlar, devlet işleri, bankacılık gibi birçok alanda güvenli veri aktarımı ve veri saklama gibi uygulamalarda büyük rol oynamaktadır. Günümüzde kullanılan en önemli şifreleme algoritmaları simetrik şifreleme ve açık anahtarlı şifrelemedir.

Simetrik şifreleme algoritmalarında hem şifreleme hem de deşifreleme işlemi için aynı anahtar kullanılır. Asimetrik algoritmalarda ise birbirine matematiksel olarak bağlı olan gizli ve açık anahtar çifti kullanılır. Mesajı gönderen kişi göndermeden önce alıcının açık anahtarını kullanarak mesajını şifreler. Mesaj alıcıya ulaştığında, alıcı şifrelenmiş mesajı kendi gizli anahtarını kullanarak deşifre eder. Asimetrik şifreleme algoritmaları çözülmesi uzun zaman alan matematiksel problemlere dayanılarak tasarlanmıştır. Buna örnek olarak çarpanlara ayırma problemi verilebilir. Küçük sayılar için iki sayının çarpımını hesaplamak ve verilen bir sayıyı çarpanlarına ayırmak kolaydır. Büyük iki sayının verildiğini varsayalım ve yine bu iki sayının çarpımını hesaplamak hesap makinesi ya da bilgisayarımız sayesinde kolay olabilir. Ancak çok büyük bir sayıyı çarpanlarına ayırmak bilgisayar kullanılsa bile çok uzun zaman alabilir. Bu probleminden yola çıkarak geliştirilen asimetrik şifreleme algoritmaları şifrelenmiş bir bilginin çözülmesi için geçen süreyi oldukça uzatır ve klasik bilgisayarlar kullanılsa bile çözülemez duruma getirir. Böylece bilginin güvenliği sağlanmış olur.

Klasik bilgisayarlardan farklı olarak kuantum bilgisayarlar, veriler üzerinde işlem yapabilmek adına *süperpozisyon* prensibi ve kuantum dolaşıklığı gibi kuantum mekaniği konseptlerini kullanır.

Çalışma mantığını klasik bilgisayarlar ile kıyaslayarak şu şekilde anlatabiliriz:

Klasik bilgisayarlar işlemleri ikili sayı sistemi denilen 0 ve 1 değerlerini temel alan bitler yardımı ile yapar. Bilgisayarlarda yapılan tüm işlemler 0 ve 1'lere dönüştürülerek gerçekleştirilir. Kuantum bilgisayarlarda ise bit yerine kübit kullanılmaktadır. Klasik bilgisayarlarda bir bit sadece 0 ya da 1 değerini alabiliyorken kuantum bilgisayarlarda ise bir kübit 0 ve 1'lerin aynı anda olası kombinasyonlarından oluşabilir. Bu duruma *süperpozisyon* denir.

Peter Shor'un 1994'te yayımladığı *"Algorithms for quantum computation: discrete logarithms and factoring"* isimli makaleye dayanarak güçlü kuantum bilgisayarlar ile çarpanlara ayırma, ayrık logaritma problemi gibi problemlerin polinomsal sürede çözülebileceği ve bu problemlerin temel oluşturduğu kriptografik algoritmaların da kullanılabilirliğini ve güvenilirliğini yitireceği sonucuna varılabilir. Kuantum bilgisayarların en iyi ve yaygın olarak herkes tarafından kullanılan şifreleme algoritmalarını bile çok hızlı bir şekilde etkisiz kılması, ister istemez bilgisayar korsanlarının da bu konulara karşı ilgisini artırmaktadır. Dolayısıyla bu gücün siber güvenliği de tehdit etmesinden endişe duyulmaktadır.

Kuantum bilgisayarların, farklı şifreleme teknikleri ve siber güvenlik çözümlerinin temel olarak kullanıldığı finans sektörü ve devlet kurumları gibi kişisel ve gizli verilerin yetkisiz erişimden korunması gereken alanlar başta olmak üzere siber güvenliği de tehdit etmesinden endişe duyulmaktadır.

Kuantum bilgisayarlar, şu anda gündelik hayatımızdaki klasik bilgisayarlar gibi yaygın olarak kullanılsa bile o zaman geldiğinde hazırlıklı olmak ve en azından kritik öneme sahip sistemleri ve sektörleri güvenli tutmak için hazırlık yapmakta fayda olacaktır. Bu nedenle Başta NIST (Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü) olmak üzere bu sürecin ciddiyetinin farkında olan birçok kurum, kuantum sonrası kriptografi üzerine akademik araştırmalar başlatmış ve eski algoritmaların yerini alabilecek yeni algoritmalar tasarlamak üzerine çalışmalarını hızlandırmıştır.

2016 yılının Aralık ayında NIST tarafından başlatılan kuantum sonrası kriptografi standartlaşma sürecinde geçtiğimiz temmuz ayında üçüncü aşama tamamlandı ve standartlaşması planlanan şifreleme ve imzalama algoritmaları duyuruldu.

Son olarak her ne kadar bu algoritmalar kuantum ataklara karşı dayanıklı olsa da henüz yeni algoritmalar olduğu için duyurulan bu algoritmalara karşı ortaya çıkan yeni ataklar incelenmeli ve gerekli önlemler alınmalıdır.

KAYNAKÇA

P. W. Shor, «Algorithms for quantum computation: discrete logarithms and factoring.» %1 içinde *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994.





SİBER GÜVENLİK TEKNOLOJİLERİ

SİBER GÜVENLİK TEKNOLOJİLERİ

Siber güvenlik, saldırganların ve savunucuların sürekli rekabet ettiği bir alandır.

Her kuruluşta saldırganların erişim elde etmeye çalıştığı ve çeşitli zararlara neden olabileceği güvenlik açıkları bulunmaktadır. Siber saldırganlar bu güvenlik açıklarını tespit etmeye ve bunlardan yararlanmaya çalışırken siber güvenlik uzmanlarının görevi bu açıkları kapatmaya çalışmaktır.

Siber savunmanın saldırıdan daha zor olduğu su götürmez bir gerçektir. Bir siber saldırgan kuruluş içerisindeki güvenlik açıklarını belirlemeye ve bunlardan yararlanmaya ihtiyaç duyarken siber güvenlik uzmanları bir kurumun içerisinde bulunan tüm güvenlik açıklarını bulup kapatmaya çalışır.

İki role baktığımızda beceri ve yetkinlik anlamında benzerdir. Hem saldırı tarafından hem de savunma tarafından bakıldığında kurum içerisindeki potansiyel güvenlik açıklarının belirlenmesi gerekir. Siber güvenlik uzmanının saldırgandan ayrılan tarafı bulunan güvenlik açığını kapatmak için bir adım daha ileriye düşünmesidir.

Siber savunma neden yapılır?

Bir kurumun siber savunma stratejisinin olmaması o kurumun verilerinin savunmasız kalmasına neden olur. Veriler yanlış kişilere geçtiğinde çok tehlikeli olabilir ve kuruma çok ciddi zararlar verebilir. Örneğin siber savunma olmazsa saldırganlar müşterilerin kişisel bilgilerine erişebilir; bu da müşterilerin azalmasına, markaya olan güvenin zedelenmesine ve yasal problemlere yol açar. Siber savunma, devlet kurumları, telekom ve internet servis sağlayıcıları, sağlık hizmetleri, finans ve bankacılık kurumları, otomotiv endüstrisi dâhil olmak üzere tüm sektörler için önemlidir.

Günümüzde saldırılar daha sık ve karmaşık hâle geldikçe kurumlar siber güvenliği daha fazla ele almaktadır. Her kurum kendi içerisinde gelebilecek tehditlere karşı bir strateji hazırlar. Şimdi bu stratejilere ve siber savunmanın nasıl yapılması gerektiğine bakalım.

1. Aşama: Tehdit

Siber güvenlik savunma aşamalarının en temelinde oluşabilecek tehditlerin belirlenmesi yatar. Uygun savunmalar yalnızca karşılaşılan tehditleri anlayarak ve siber savunmanın en çok nerede risk altında olduğu anlaşılabilir. Genelde tehditlerin ortaya çıkmasında iki temel neden vardır: teknik ve insan güvenlik açıkları. Teknik güvenlik açıkları düzenli bir güvenlik açığı taraması ile tespit edilebilir. Buna karşılık, insandan kaynaklı güvenlik zayıflıkları, çok daha fazla zarar verici olabilir, bu nedenle siber suçlular kimlik avını bu kadar çok tercih etmektedir. Kurum içi kimlik avı bilgilendirme eğitimleri siber tehditleri azaltmak için çok önemlidir. Çalışanların kimlik avı e-postalarını nasıl ta-

niyacıklarını ve e-postayı açtıklarında veya kötü amaçlı bir bağlantıya tıkladıklarında ne yapacaklarını bilmesi kurumu güvende tutmak için oldukça önemlidir.

2. Aşama: Koruma

Bir kurum tehditleri algılamak için çok iyi hazırlanmış olsa bile bazı saldırılar ilk savunma katmanlarını geçebilir. Kurumlar güçlü siber güvenlik kontrolleri uygulamalı ve çalışanların siber güvenlik savunmalarını ve ihlallerini nasıl yöneteceklerini bilmelerini sağlamalıdır. Eğitim ve profesyonel sertifika, güvenlik önlemlerinizi uygulamak ve sürdürmek için ihtiyaç duyduğunuz kalifiye personele sahip olmanızı sağlamaya yardımcı olur.

3. Aşama: Yönetim

Bu aşama, kuruluşların siber güvenlik risklerini daha geniş operasyonlarının bir parçası olarak yönetme biçimleriyle tanımlanır. Risk bazlı güvenlik kontrollerini kurumsal süreçlere yerleştirmek, tedarik zincirlerinin güvenliğini yönetmek ve güvenlik kontrollerinin güncel kalmasını sağlamak için düzenli denetimler yapmak gibi önlemleri içerir. Kuruluşlar bu görevleri ISO 27001'in yardımıyla gerçekleştirebilir.

4. Aşama: Yanıt

Uyguladığınız güvenlik önlemleri, başarılı bir saldırı olasılığını ve etkisini en aza indirmelidir ancak bir veri ihlalinin gerçekleşmesi için yalnızca bir hata yeterlidir. Bu nedenle kuruluşlar, yıkıcı bir olay durumunda ne olacağını ele alan bir güvenlik katmanı benimsemelidir.

5. Aşama: İyileşme

Son güvenlik katmanı, bir veri ihlalinin sonrasını ele alır. Bazen, kuruluşların her zamanki gibi işlerine tamamen dönmesi genellikle aylar aldığından kurtarma süreci planladığınızdan daha yıkıcı olabilir. Yerinde bir siber sigortaya sahip olmak, kuruluşlara gönül rahatlığı verebilir, en çok ihtiyaç duydukları anda koruma sağlar ve kuruluşun mümkün olan en kısa sürede normal işine dönmesine yardımcı olur. Her şey başarısız olsa bile bir şeylerin yeniden inşa edilmesinin maliyetini karşılayabilir.

Günümüzde sızdırılan bilgiler ile sağlık, endüstri, teknoloji gibi alanlarda yaşamın devamlılığını tehlikeye sokan faaliyetler gerçekleştirilmektedir. Özel hayatın gizliliği ihlal edilerek insanların hayatları tehlikeye altına girmektedir. Bilişim hayatımızın her alanında yer aldığından yaşanan bu tehditler devam edecektir. Tehditler devam ettiği müddetçe siber güvenlik kavramının önemi hayatımızda daha da büyük bir yer kaplayacaktır.

Tüm dünyada teknolojinin gelişmesi ve siber güvenlik kavramının ortaya çıkmasıyla şirketlerde yer alan siber güvenlik uzmanlarına duyulan ihtiyaç her geçen gün artıyor. Kurumların içerisinde yer alan SOC (Security Operation Center), siber güvenlik olaylarının analiz, tespit ve müdahâlesinde aktif rol oynayan bir güvenlik merkezidir.

Şirketlerde çalışan etik siber güvenlik uzmanları kurumlarını korumak ve şirketin devam-

İliğini gözetmek için farklı araçlara ve teknolojilere ihtiyaç duyar. Bu yazıda siber güvenlik teknolojilerinden birkaçını ele alıp onların siber güvenlik uzmanlarının hayatlarında nasıl bir yer kapladığına yakından bakmaya çalışacağız.

İlk olarak SIEM’i ele alarak başlayalım.

SIEM’in açılımı Security Information and Event Management’dir. Türkçeye Güvenlik Bilgileri ve Olay Yönetimi olarak çevirebiliriz. SIEM, günlük verilerin birden fazla kaynaktan toplanıp analiz edildiği ve şüpheli durumun belirlenip gerekli bulguların siber güvenlik uzmanlarına bildirildiği bir teknolojidir. SIEM için cihazların kayıtlarına ihtiyaç vardır. SIEM günlük olarak cihazlardan gelen kayıtları toplar, bunları raporlar ve alarmları tetikler. SIEM, logları topladıktan sonra bu logları anlamlı hâle getirip gerektiğinde alarm üretmeyi başarır. SIEM anlık olarak ağda bulunan tüm cihazlar üzerindeki hareketlerin izlenmesinde yardımcı olur. SIEM’in topladığı bu kayıtlar oluşabilecek herhangi bir saldırıda saldırının nereden, kimden ve hangi yollarla geldiğinin anlaşılabilmesinde yardımcı olmaktadır.

Peki SIEM nasıl çalışır?

Öncelikle ağ üzerindeki cihazlardan toplanan kayıtlar belirli bir formata dönüştürülür. Oluşan olaylar saldırı tiplerine göre kategorilendirilir. Bağımsız gibi görünen olaylar birbiri ile ilişkilendirilir. İlgili kişilerin bildirilmesi amacıyla toplanan bu verilerden bir alarm oluşturulur. En son aşamada ise bu verilerden oluşan kapsamlı bir analiz raporu hazırlanır.

Şimdi SOC’de kullanılan bir diğer siber güvenlik teknolojisi olan SOAR’ı inceleyelim.

SOAR, Security Orchestration Automation and Response kelimelerinin baş harflerinin kısaltmasıdır. Türkçeye “Güvenlik Düzenleme, Otomasyon ve Yanıt” olarak çevrilebilir. Adından da anlaşılacağı üzere kurum içerisinde yer alan verilerin toplanması ve analiz edilmesine yardımcı olan bir araçtır. SOAR’ı biraz daha anlayabilmek için kısaltmasında da geçen orkestrasyon (düzenleme), otomasyon ve yanıt başlıklarını daha yakından ele alalım.

Düzenleme, farklı pek çok kaynaktan bilgilerin toplanması ve birleştirilmesinin ortak bir yerden yönetimidir. Örnek verecek olursak şüpheli bir kod için öncelikle kodun kaynağının ve kötü amaçlı yazılım içerip içermediğinin bulunması gerekmektedir. Normalde manuel olarak çok uzun sürecek olan bu işlem SOAR ürünü ile kısa sürelerde çözülebilir. SOAR, arka planda şüpheli kodu inceler ve bize bilgiyi sunar.

Otomasyon, insana gerek duyulmayacak biçimde güvenlik yazılımlarının tekrarlanması sağlayan özelliklerdir. Otomasyona bir örnek olarak belirli bir dakika içinde gelen belirlenmiş sayıdan fazla erişim denemesini algılayan ve ilgili kaynağın IP adresini karantınaya alan bir SOAR kuralı verilebilir.

Tepki veya olaya müdahâle, SOAR’ın tekrar eden süreçlere yönelik olan sürecidir. İnsan gücünden çok daha çabuk sürelerde olaylara müdahâle edilmesine yarar.

Peki SOAR ile neler yapılabilir?

- 1) Tehdit istihbaratları SOAR ile entegre edilerek güvenlik açıklıkları giderilebilir.
- 2) SOAR ile belirli kural setleri oluşturularak hızlı aksiyonlar alınması sağlanabilir.
- 3) SOAR ile iş süreçlerini yönetmek oldukça kolaylaşabilir.
- 4) SOAR ürünü raporlama konusunda çeşitli görseller ile destekleme sağlar.

SOAR ile SIEM arasındaki temel farklar nelerdir?

SIEM, temelde kayıtların toplanması ve analiz için olan bir araçken SOAR ilgili uyarılara müdahâlede de bulunur. SOAR, SIEM'den gelen verileri yönetmek ve müdahâlede bulunulması için tasarlanmıştır. SOAR farklı sistemlerden gelen verilerle birlikte SIEM'den gelen alarmlara müdahâle eder.

Farklardan bir diğeri insan müdahâlesi konusunda ortaya çıkar. SIEM aracında oluşturulan kurallar sürekli gözden geçirilmelidir. SOAR ise ana amacı olan otomasyon sayesinde insan etkinliğini en aza indirmeyi hedefler.

Kuruluşumuzda hem SIEM hem de SOAR'ı birlikte kullanabilir miyiz?

Bu sorunun yanıtı “Evet, kullanabiliriz.” olacaktır.

Bunu bir örnekle açıklayalım: Bir kuruluşta olduğunuzu düşünün. Kuruluş içerisinde siber güvenlik analisti olarak görev yapıyorsunuz. SIEM cihazından gelen alarmlardan hangilerinin gerçek olup olmadığını uyarıları değerlendirerek karar verdiniz. Fakat olaya müdahâle kısmı saatler sürebilir.

Bunun yerine SIEM'in SOAR ürünü ile entegre çalıştığı bir senaryoda gelen alarmin otomatik bir şekilde gerçek olup olmadığı, hangi kaynaklardan geldiği anlaşılmış olacaktır, böylece müdahâle süresi ciddi anlamda kısılacaktır. Bu bir bakıma çalışan siber güvenlik uzmanlarının özel becerilerini farklı alanlarda gerçekleştirme özgürlüğünü de kazandıracaktır.

KAYNAKÇA:

- <https://cahitcengizhan.com/bilisim-guvenligi-turlerinin-tarihsel-gelisimi/>
- https://www.beyaz.net/tr/guvenlik/makaleler/siem_ve_soar_olmadan_soc_olur_mu.html
- <https://www.netsmart.com.tr/2020/09/02/siem-vs-soar/>
- <https://www.mshowto.org/acik-kaynak-soar-cozumleri-bolum-1.html#close>
- <https://cybersecurityguide.org/resources/cyber-defense/>
- <https://www.fornetix.com/articles/pivoting-from-cyber-security-to-cyber-defense/>
- <https://www.itgovernance.eu/blog/en/the-5-stages-of-an-effective-cyber-defence-strategy>
- <https://fatihmertugtegitim.medium.com/>



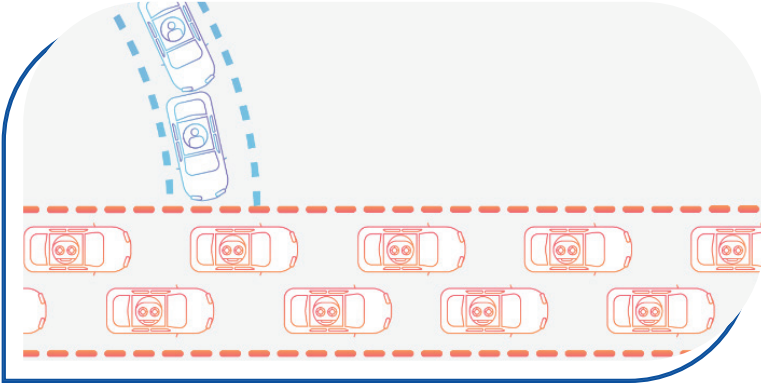


DOS VE DDOS SALDIRILARI

Hizmet Reddi Saldırısı (DoS saldırısı) ve Dağıtık Hizmet Reddi Saldırısı (DDoS saldırısı)

Hedef bir sistemi kullanıcılar tarafından kullanılamaz hâle getirmeyi amaçlayan bir saldırı çeşididir. DoS ve DDoS saldırıları genellikle, sistemleri aşırı yüklemek ve isteklerin yerine getirilmesini önlemek amacıyla hedeflenen makineyi veya kaynağı gereksiz isteklerle doldurarak gerçekleştirilir.

Yüksek bir seviyeden bir DDoS saldırısı, otoyolu tıkayan ve düzenli trafiğin hedefine ulaşmasını engelleyen beklenmedik bir trafik sıkışıklığı gibidir. İşine gitmek isteyen biri normalde 5 dakikada gideceği yolu 2 saatte gidiyorsa gideceği yere geç ulaşır, bu beklenmedik bir durum olur. O yolu tıkayan trafik veya kaza vb. durumlar kişinin gideceği yere uzun sürede erişmesine sebep olur, DoS-DDoS saldırıları da böyledir.



DoS saldırılarında tek bir kaynak kullanılırken DDoS saldırısı tek bir kaynak ile gerçekleştirilmez birden çok kaynak kullanılır. Genellikle BotNet kullanılır ve siber saldırganın kimliği belirsizdir. BotNet sözcüğü “robot” ve “network” (ağ) sözcüklerinin birleşiminden türetilmiştir. Siber suçlular, Zombie hâline getirdikleri cihazlardan oluşan Botnetleri istedikleri zaman uzaktan kontrol ederek DDoS saldırısı yapabilirler. BotNet, siber saldırganlar tarafından ücret karşılığında hizmet olarak da sunulmaktadır.

Saldırı Neden Yapılır?

DDoS saldırılarının arkasında birçok motivasyon faktörünün olması mümkündür. Bunlardan birkaç tanesine değinmeye çalışırsak:

Para: Sonucu para kazanma veya para kaybettirmeye yönelik gerçekleştirilen ataklara tekabül eden motivasyondur. Rakip firmalara karşı avantaj sağlama çabası, şantaj yoluyla para alma, hisse değeri kaybettirme vb. sebeplerden dolayı olabilir.

İdeolojik: Siyasi, politik vb. nedenlerden ötürü gerçekleştirilir.

Dikkat Dağıtma: Hedef organizasyonun personel ve cihazlarını oyalayarak asıl niyet olan veri sızdırma vb. faaliyetlerin tespitini engellemeye yönelik olarak gerçekleştirilir. Bunlar genel olarak bahsi geçen motivasyonlar olup ek olarak farklı motivasyonların da olması söz konusudur.

DDoS Saldırı Çeşitleri

Saldırganlar genel olarak üç tip DDoS saldırı yöntemi kullanmaktadır. Bu saldırı tipleri aşağıdaki başlıklarda tanımlanmıştır.

Volümetrik (Hacimsel) Saldırıları (Ağ): Saldırganlar tarafından en sık kullanılan atak çeşidi olup hedef bilgisayarın kullanmakta olduğu internet bant genişliğini tüketmeyi hedeflemektedir.

Bant genişliği tüketmek... İnternette bir siteye erişmek istediğimizi varsayalım. Bizim bu siteye erişmemizi engelleyen saldırganlar siteye gönderdiğimiz bağlantı isteği dışında gereksiz birçok bağlantı göndererek sistemin yanıt vermesini engellemiş olur.

Amplifikasyon (Ağ Zaman Protokolü) Saldırıları: İnternette genel hizmet veren sunuculara (ana bilgisayar olarak düşünebilirsiniz) küçük paketler göndererek internet kullanıcılarına büyük paketler göndermesi sağlanır. Beklentiye cevap veremeyen kullanıcı sistemi işlevsiz kalır.

Protokol Saldırıları: Genellikle bağlantı oturum bilgisi (session) kullanan Güvenlik Duvarı, Yük Dengeleme Cihazları, Yönlendiriciler vb. sistemler hedef alınır. Çok sayıda oturum açma isteğinde bulunup oturum tamamlanmadan yeni istekler gönderilir. Bu şekilde ağ ve güvenlik cihazlarının oturum tablolarını doldurup işlevsiz hâle gelmesi sağlanır.

Uygulama Saldırıları: Web uygulama servislerine yapılan ataklardır. Hedef uygulamalara kapasitelerinin çok üzerinde istek gönderilerek, kaynaklarının tüketilmesi yöntemi ile sistemin işlevsiz hâle getirilmesi asıl amaçtır.

KAYNAKÇA

<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

<https://berqnet.com/blog/dos-ddos-saldirisi-nedir>

https://en.wikipedia.org/wiki/Denial-of-service_attack

<https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks>

<https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks>

<https://www.barikat.com.tr/images/blog/loddos-ddos-saldirilari-degerlendirme-raporu.pdf>





ORTADAKİ ADAM SALDIRISI (MITM)

Ortadaki Adam Saldırısı Nedir?

Ortadaki Adam Saldırısı (Man In The Middle), saldırıyı yapan saldırgan makinesinin bir kullanıcı ile bir uygulama arasındaki konuşmayı dinlemesi veya taraflardan birinin kimliğine bürünerek, normal bir bilgi alışverişi gibi görünmesini sağlamak için kendisini uygulama ile kullanıcı arasına konumlandırmasıyla oluşur.

MITM saldırısının amacı, oturum açma kimlik bilgileri, hesap ayrıntıları ve kredi kartı numaraları gibi kişisel bilgileri çalmaktır. Saldırının hedefleri genellikle finansal uygulamalar, e-ticaret siteleri ve oturum açmanın gerekli olduğu diğer web sitelerinin kullanıcılarıdır. Bu saldırı, gelişmiş kalıcı tehdit (APT) saldırısının sızma aşaması sırasında güvenli bir dayanak elde etmek için de kullanılabilir. Saldırı, saldırganın araya girip tüm konuşmayı kontrol ettiği gizli bir dinleme türüdür.

Ortadaki Adam Saldırısı Nasıl Çalışır?

Ortadaki Adam Saldırısı ağ içerisindeki iki cihazın etkileşimi sırasında dışarıdan üçüncü bir kişinin araya girerek gelen giden verileri alabilmesine olanak sağlayan bir saldırı çeşididir. Saldırı sırasında siber suçlular kendilerini veri işlemlerinin veya çevrimiçi iletişimin ortasına sokar. Saldırı tipi veri ele geçirme ve şifre çözme olarak bilinen iki aşamalı süreçten geçer. Veri ele geçirme, saldırganın istemci ile sunucu arasındaki veri aktarımını engellemesini gerektirir. Saldırgan, istemci ve sunucuyu birbiriyle bilgi alışverişinde bulunduklarına inandırırken kendini istemci makine yerine konumlandırarak üzerinden veri trafiğinin geçmesini sağlar.

Ortadaki adam saldırısını saldırganlar sıklıkla halka açık bir alanda parola gerektirmeyen sahte bir wi-fi etkin noktası oluşturarak yaparlar. Bir kurban etkin noktaya bağlanırsa, saldırgan gerçekleştirdiği tüm çevrimiçi veri alışverişlerine erişim kazanır.

Müdahâle için daha aktif bir yaklaşım benimsemek isteyen saldırganlar, aşağıdaki saldırılardan birini başlatabilir:

IP Sahtekârlığı: Saldırgan IP adresindeki paket başlıklarını değiştirerek kendisini bir uygulama olarak gösterir. Bu işlem sonucunda, uygulamaya bağlı bir URL'ye erişmeye çalışan kullanıcılar, saldırganın web sitesine yönlendirilir.

ARP Sahtekârlığı: Saldırganın yerel alan ağı (LAN) üzerinden sahte adres çözümleme protokolü (ARP) istekleri göndermesidir. Çoğu zaman cihazlar internete bağlanmalarını sağlayan yönlendirici veya ağ geçidi ile iletişim kurmak için adres çözümleme protokolünü kullanır. ARP istek paketinin içinde, medya erişim kontrol adresi (MAC) adresini öğrenmek istediği cihazın IP adresi bulunur. ARP isteğini ağdaki tüm cihazlar alır. İnternet Protokol'un (IP'nin) kendisine ait olmadığını anlayan cihazlar ARP istek paketlerini siler. Saldırganın amacı ağ geçidi gibi bir uç sistemin IP adresiyle kendi MAC adresini eşleştirerek kendi makinesi üzerinden veri trafiğini yönlendirmektir.

DNS Sahtekârlığı: Bu saldırıda, hedef web sitesine erişmeye çalışan kullanıcılar, değiştirilen DNS kaydı tarafından saldırırganın sitesine gönderilir. DNS sahtekârlığı, bir kullanıcının trafiği yönlendirmek veya kullanıcıların kimlik bilgilerini çalmak amacıyla gerçek gibi görünen gizlenmiş sahte bir web sitesine gitmeye zorlandığı bir saldırı türüdür.

Ortadaki Adam Saldırısı, veri ele geçirilince bitmez. Kurbanın şifrelenmiş verilerine eriştikten sonra, saldırırganın okuyabilmesi ve verileri kullanabilmesi için şifresinin çözülmesi gerekir. Kullanıcıya veya uygulamaya fark ettirmeden kurbanın verilerinin şifresini çözmek için farklı yöntemler kullanılabilir:

HTTPS Sahtekârlığı: HTTPS (Güvenli Hyper Text Transfer) protokolü, güçlü TLS şifrelemesi kullanır. Bu protokol HTTPS'ye göre yüksek derecede güvenli, modern web iletişim protokolüdür. Siber suçlular yüksek güvenli HTTPS protokolünü de atlatmanın yolunu bulmuştur. HTTPS sahtekârlığı, bir saldırırganın hedef web sitesininkine çok benzeyen bir domain kullanmasından oluşur. "Homograf saldırısı" olarak da bilinen bu taktik ile hedef domainde karakterler, görünüş olarak çok benzeyen ASCII olmayan diğer karakterlerle değiştirilir. Kullanıcının, gitmek istediği web sitesindeki domainle neredeyse aynı görünmesi dolayısıyla farkı fark etmesi pek olası değildir. Saldırgan, tarayıcının güvenli bağlantı göstergesinden emin olacak şekilde ayarlamıştır.

SSL Sahtekârlığı: SSL sahtekârlığı, saldırırganın bir kullanıcı ile bir web sitesi arasındaki bağlantıyı kesmesini içerir. Kullanıcının güvenli HTTPS bağlantılı web sitesinin güvenli olmayan bir HTTP sürümüne indirgerek yapılır. Bu durum, kullanıcıyı güvenli olmayan siteye bağlarken, saldırırgan güvenli siteyle bağlantısını sürdürür ve kullanıcının etkinliğini saldırırgan tarafından şifrelenmemiş bir biçimde görünür hâle getirir.

SSL Beast: TLS 1.0 ve daha eski SSL protokollerindeki ağ güvenlik açıklarını hedefleyen bir saldırdır. Bu saldırıda, kurbanın bilgisayarına bir web uygulaması tarafından gönderilen şifreli tanımlama bilgilerini engelleyen kötü amaçlı JavaScript bulaşır. Ardından, çerezlerin ve kimlik doğrulama belirteçlerinin şifresini çözmek için uygulamanın şifreli blok zincirleme (CBC) güvenliği ihlal edilir.

SSL Kaçırma: Oturum ele geçirme saldırısıdır. Session hijacking olarak da bilinir. Saldırgan oturum anahtarına/kimlik bilgilerine yetkisiz erişim sağlar ve geçerli bir oturumu istismar eder.

Ortadaki Adam Saldırıların Sonuçları

Siber suçlular, ortadaki adam saldırıları kullanarak kullanıcı adları, parolalar, kredi kartı numaraları ve banka hesabı ayrıntıları gibi hassas bilgileri ele geçirebilir. Bir suçlu bu bilgilere sahip olduğunda, hesap bilgilerini manipüle edebilir, para çalabilir veya yetkisiz satın alma işlemleri yapabilir. Ortadaki adam saldırganları genellikle bankacılığı, çevrimiçi perakendecileri ve hizmet olarak yazılım (SaaS) platformu müşterilerini hedefler.

Kuruluşlar açısından bakıldığında ortadaki adam saldırıları kuruluşlardaki uzun vadeli gelişmiş kalıcı tehdit (APT) kampanyaları için bir ilk ağ geçidi olarak kullanılır. Siber suçlular, belirli uygulamalar için bir kullanıcının kimlik bilgilerini alarak şirket verilerini ele geçirebilir, üretim ortamlarını bozabilir veya BT altyapısını ele geçirmek için tüm ağa girebilir.

Ortadaki Adam Saldırısı Önleme

Ortadaki adam saldırılarını engellemek, kullanıcılar için birkaç pratik adımın yanı sıra uygulamalar için şifreleme ve doğrulama yöntemlerinin bir kombinasyonunu gerektirir. Kendinizi güvene alabileceğiniz yollar:

- Parola koruması olmayan Wi-Fi ağlarına bağlanmak saldırıya uğrama riskini artırır. Halka açık Wi-Fi bağlantıları siber suçluların saldırı ve müdahâlesine açıktır. Mümkün olduğunca bu tür güvensiz bağlantılara bağlanılmamalıdır.
- Bir web sitesinin güvenli olmadığını bildiren tarayıcı bildirimlerine dikkat edilmelidir. Kullanıcılar, URL'sinde "HTTP" yerine "HTTPS" gösteren web sitelerini ziyaret etmelidir. URL'den önce web sitesinin güvenli olduğunu belirten kilit işaretinin varlığına dikkat edilmelidir.

• Siber suçlular, kullanıcıları kandırmak için kimlik avı e-postaları oluşturur. Kullanıcılar, doğrulanmamış veya bilinmeyen kaynaklardan gelen e-postaları açmamalıdır. Kimlik avı e-postaları genellikle insanların ilgisini çekecek şekilde hazırlanır. Bankadan veya finans kurumu vb. yasal kaynaktan geliyormuş gibi görünür. Kullanıcıların bir bağlantıya tıklaması amaçlanarak sahte web sitesine bağlantı veren linkler yüklenebilir. Kullanıcılar, hesabına gelen e-postanın güvenliğinden emin olmadan bu linklere tıklamamalı parola vb. özel bilgilerini hiçbir zaman girmemelidir.

Web sitesi operatörleri için TLS ve HTTPS güvenli iletişim protokolleri, iletilen verileri güçlü bir şekilde şifreleyerek ve kimliklerini doğrulayarak kimlik sahtekârlığı saldırılarını azaltmaya yardımcı olur. Bunu yapmak site trafiğine müdahâle edilmesini önler ve kimlik doğrulama belirteçleri gibi hassas verilerin şifresinin çözülmesini engeller.

KAYNAKLAR :

https://csrc.nist.gov/glossary/term/man_in_the_middle_attack

<https://heimdalsecurity.com/blog/man-in-the-middle-mitm-attack/>

<https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM>

<https://doubleoctopus.com/security-wiki/threats-and-tools/https-spoofing/>

<https://cybersecgirll.blogspot.com/2021/07/arp-spoof-nedir-nasl-kullanlr-ilk-basta.html>

https://en.wikipedia.org/wiki/Man-in-the-middle_attack





İNSANSIZ HAVA ARAÇLARININ SİBER GÜVENLİKTEKİ YERİ

Bu yazımızda insansız hava araçlarının tanımına, kullanım alanlarına ve siber güvenlikteki yerlerine değineceğiz. Savunma teknolojileri alanındaki gelişmelerle beraber, insansız hava aracı kullanımı birçok alanda ciddi ölçüde arttı. Maliyet açısından avantaj sağlayan bu araçlar acaba sanıldığı kadar güvenli mi?

İnsansız Hava Aracı Nedir?

Kısaltılmış hâliyle İHA'ları üç farklı kategoride inceleyebiliriz.

Döner Kanatlılar (Drone)

Sabit Kanatlılar (Uçak)

VTOL'ler (Dikey Kalkışlı Uçak)

Örnek vermek gerekirse drone'lar teknoloji çağının hem hobi olarak kullanılan hem de askerî alanlarda önemli rol oynayan araçlarındandır. İnsansız hava araçları genel olarak kullanımı yönünden iki farklı grupta incelenir. Bunlardan birincisi bir kullanıcı (operatör) yardımı ile uzaktan kumanda ile yönlendirilenler, ikincisi ise makinenin beynine (uçuş kontrol birimi) rota bilgisi önceden kodlanmış olanlardır.

İnsansız hava araçlarının büyük çoğunluğu radyo frekansı ile kontrol edilmektedir ve uçuş sırasında uydu sinyalleri kullanmaktadır.

Buradan da anlayabileceğimiz gibi bu mekanizmadaki teknolojilere uzaktan saldırı yapmak mümkündür.

İnsansız Hava Araçları ve Güvenlik Açıkları

Günümüzde kullanılan İHA'larda ciddi güvenlik açıkları bulunmaktadır. İddiam o yöndedir ki dolandırıcılar ve siber saldırganlar insansız uçağın sistemini ve komutasını bir mil öteden ele geçirebilirler. Örneğin bazı modellerde Wi-Fi bağlantı şifrelemesi o kadar zayıftır ki dakikalar içerisinde kırılabilir. Daha da kötüsü, saldırganlar Wi-Fi bağlantısına seri saldırılar yaparak kullanıcıyı ağdan atıp, kontrolü ele geçirebilirler.

Bir başka örnekle uçaktan 1 kilometre uzakta bulunan bir hacker, ağ üzerinde, uçağa yeniden yönlendirici komutlar gönderebilir. Hatta ve hatta kontrolü ele geçirip uçağı rotasından çıkarabilir ve bir binaya çarpması için yönlendirebilir.

İnsansız Hava Araçlarına Yapılabilecek Saldırıları

1-) Sinyal Bozma Saldırıları

İHA'ları hedef alan bir saldırgan uzaktan İHA sistemine radyo sinyalleri göndererek İHA'nın kumanda ile olan bağıını kesebilmektedir.

2-) Veri Trafikini Dinleme

Yazılım sistemlerinde zayıf şifreleme teknikleri kullanıyorsa veya uzaktan saldırılara karşı hiçbir güvenliği yoksa İHA'lara saldırı yapacak kişi kolaylıkla veri trafiğini ele geçirebilir ve İHA'da bulunan bütün bilgilere erişebilir.

3-) Sahte Uydu Sinyalleri

Önceden tanımlanmış konum bilgileri sahte uydu sinyalleri gönderilerek İHA'ların GPS'ten uçuş kontrol kartına aktardığı rota bilgisi değiştirilebilir.

4-) Tersine Mühendislik

İHA'ların kullandığı yazılım ve donanım yönleri keşfedilir ve tersine mühendislik uygulanarak İHA geliştirilebilir veya yeni türevleri üretilebilir.

Geçmişten Bir Örnek

2011 yılında kayıtlara "RQ-170 incident" olarak geçen İran'ın Amerika Birleşik Devletleri'ne ait bir İHA'yı kontrollü bir şekilde kendi topraklarına indirmesi ve sonrasında tersine mühendislik uygulayarak İHA'nın aynısını üretebilmesi çarpıcı bir olaydır.

5-) Aşırı Sinyal Yükleme

İHA'lara saldıran kişi İHA uçuş kontrol birimine çok fazla sayıda bağlanma isteği oluşturacak paket yüklemesi yapar ve İHA'nın beyni bu çok sayıda oluşan komutları kaldıramaz doğal olarak servis dışı kalır.

6-) Özel Veri Paketi Göndermek

İHA'ya kendi yazılımının yönetemeyeceği veri paketi gönderilir, yazılımın çalışması durdurulur veya saldırı yapacak kişi yazılım zafiyetlerinden yararlanır ve açıklıklardan faydalanarak İHA kontrolörüne sızar ve kontrolü ele geçirir.

7-)Algılayıcıları Yanıltma

Algılayıcılar İHA'ların yönünü belirlemek için kullandığı görüntü işleme yazılımlarıdır bu durum ise kolaylıkla bozulabilir yani İHA'ların kameralarının algıladığı görüntüye müdahâle edilir ve İHA manipüle edilir.

İnsansız Hava Araçları ve Siber Kılavuz

İHA'lar kolay ve hızlı kurulumu sahip araçlardır. Bununla birlikte iletişimde şifresiz kanalları tercih etmeleri ve birden fazla açık porta sahip olmaları kolay ele geçirilmelerine sebep olmaktadır. İHA ele geçirme saldırıları **DroneJacking** olarak adlandırılır ve yakın gelecekte siber suçlar arasında popülerlik sıralamasında üst seviyelerde gösterilecektir.

İHA'ların hacklenmesi mantığı esasında günümüzde de duyulan ve bilinen bir saldırı yöntemi olan DDOS saldırılarına çok benzer. Uçuş hâlindeki İHA'lara kontrol istekleri gönderilebilir hatta basit bir program sayesinde isteklerin sayısı binlere kadar çıkarılabilir. Bu istekler İHA'ların işlemcisini kilitlemesine ve aracın kendisini kapatmasına neden olmaktadır.

MALDRONE: Diğer adıyla drone'lar için malware, İHA'ları hedefleyen bir tür kötü amaçlı yazılım türüdür.

İHA'lar aslında uçan bilgisayarlar olarak da bilinmektedir. Kısaca bir bilgisayar veya telefonla aynı türden saldırılara karşı duyarlı olduklarını düşünmemizde fayda vardır.

SKYJACK AKA: Diğer adıyla ise zombi drone yazılımı, havada sizin drone'unuzdan farklı drone'ların hacklenmesini sağlayan saldırı çeşididir. Drone'a eklenen Raspberry Pi bilgisayarı sayesinde aracınız etrafta dolaşan ve diğer araçları arayan bir tür cihaza dönüşmüştür. Yani bu yazılımı kullanan bir drone havada başka bir drone bulunca onun kablosuz ağına saldırır ve operatörüyle drone arasındaki bağlantıyı keser.

İnsansız Hava Araçlarının Güvenliği İçin Almanız Gereken Önlemler

1-) İHA Yazılımını Düzenli Olarak Güncellemek

İHA'ları düzenli olarak güncellemek gelecek saldırılara karşı açıkların kapatılmasında ve siber saldırıların karşı aracı güvende tutmanıza yardımcı olacaktır.

2-) Baz İstasyonunda Güçlü Bir Şifre Kullanmak

Bu durum, günlük hayatta karşılaştığımız sosyal medya hesaplarının zayıf parolalardan dolayı ele geçirilmesi gibi düşünülebilir. Az tekrar eden sayılar veya karakterler, büyük küçük harflerin özenle seçilmesi gibi. Unutmayalım ki sadece İHA konusunda değil teknolojinin her alanında güçlü şifreler en büyük savunma mekanizmasıdır.

3-) Kumanda Seçimi

Eğer telefon veya bilgisayar kullanıyorsanız cihazınızı güvende tutup zararlı yazılım bulaşmasına izin vermeyin. Kumanda olarak telefon veya bilgisayar kullanmak siber saldırıya daha çok zemin hazırlamanız anlamına gelmektedir. Çünkü siber saldırgan İHA'ya saldırıda başarısız olursa bilgisayar veya telefonunuza da saldırı atarak İHA'yı bir şekilde ele geçirebilir.

4-) VPN Kullanmak

VPN bilindiği üzere bağlantı şifreleme görevi görür, şifrelenen bağlantılara erişmek oldukça zordur.

5-) Bağlanabilecek Cihaz Sayısı Sınırı

Kendinizin veya yakın çevrenin kimliklerinden oluşan bağlantılar tutun ve sayıya göre sınırlandırın. Bu durum siber saldırı yapacak kişinin İHA'lara erişmesini engelleyecektir.

6-) İHA'da Eve Dönüş Modu (RTL) Olması

RTL modu başlangıç noktası verilen İHA için aslında bir bitiş noktasıdır. Yani eğer İHA uzaktan bir saldırıya karşı servis dışı kalıp sinyali kaybederse o noktaya geri dönmesini sağlayan moddur.

Görüldüğü üzere hayatımızın birçok noktasında yer alan; yeri geldiğinde çekimler yaptığımız, yeri geldiğinde hobi amaçlı uçurduğumuz, yeri geldiğinde de savunma sanayisinde kullandığımız insansız hava araçları siber suçların ve saldırıların odağı hâline gelebilir. Ülkemizde ve dünyada insansız hava araçlarının siber güvenliği konusunda özel eğitimler verilmekte ve üretici firmalar da bu alanda departmanlar bulundurmaktadır.

Bizler ne olursa olsun her konuda önlemimizi alalım, siber saldırılara uğramayalım.





KEŞİF

Siber saldırıların en önemli kısmı keşif yapma ve bilgi toplama adımıdır. Keşif adımıyla toplanan bilgilere göre saldırı yöntemi daha sağlam bir şekilde oluşturulabilir.

Atlanmayan bir keşif adımı ve düzgünce toplanmış bilgilerle başarılı bir siber saldırı gerçekleştirilebilir. Sektöre yeni girmiş çoğu siber güvenlikle uğraşan insanın önemsemediği ve atladığı bir adım olan keşif adımı aslında en can alıcı adımdır. Doğru ve özenli yapılmış bir keşif adımı ile istenen sistem açıklarına, bilgilere ve elde edilmek istenen verilere kolayca ulaşılabilir ve nasıl saldıracağınızı verimli bir şekilde planlayabilirsiniz. Saldırı tespiti ya da önlemesi yapan sistemlere yakalanmamak, entegre edilmiş alarm sistemlerinin devre dışı kalmasını sağlamak, sağlanan erişimin korunması ve bunların sonucunda başarılı bir siber saldırı detaylıca yapılmış bir keşif adımıyla mümkündür.

Keşif adımıyla; kullanılan teknoloji türü, sunucular, işletim sistemi, e-posta adresleri, kullanıcı adları ve parolalar gibi bilgilere ulaşılma-ya çalışılır. Toplanan bilgilerden yola çıkılarak saldırı yöntemi ve izlenecek adımlar belirlenir. Keşif, aktif ve pasif olmak üzere iki farklı şekilde yapılabilir.

Aktif Keşif

Saldırılması hedeflenen sistemle iletişim kurularak yapılan keşiftir. Sisteme girmek için çeşitli araçlar ve casus yazılımlar kullanılmaktadır. Sistemle kurulan iletişim doğrudan ya da dolaylı olabilir. İletişim sürecinde yapılan işlemler saldırılması hedeflenen sistemin ağ trafiğinde görüntülenebilmektedir. Bu görüntülenme hedef sistemin log'ları incelenirse ve fark edilirse sağlanır. Örneğin IP adresine port taraması yapılırsa firewall log'larına düşmüş olacaktır. Aktif keşfe en güzel günlük örneklerden biri, biri hakkın-da merak ettiğimiz bir şeyi kişinin kendisine soru sorarak öğrenmektir.

Aktif keşifte, hedef cihazdaki aktif servisleri belirlemek önemli bir adımdır. Aktif servislerin taranması işlemi port taraması yapılarak NMAP ile gerçekleştirilebilir. NMAP ile yaptığımız taramada hedef sistemdeki kapalı ya da açık portların görülmesi, sistemin çalışan servislerin durumlarının görüntülenmesi, sistemin firewall'unun olup olmadığının anlaşılması, taranan ağın haritasının çıkarılması veya versiyon kontrolü yapılabilir.

Pasif Keşif

Saldırılması hedeflenen sistemle iletişim kurmadan bilgiler toplanılır. Herkese açık olarak paylaştığınız bilgilerin toplanması, arama motorlarından adınızı aratarak elde edilebilen bilgilerin alınması pasif keşfe örnektir. Pasif keşfe en güzel günlük örneklerden biri, birisi hakkına merak ettiğiniz şeyi kişinin kendisine değil de onu tanıyan insanlara sorarak öğrenmenizdir.

Şimdi pasif keşif yapabileceğimiz bazı yöntemlere göz atalım. İlk olarak arama motoruna ad soyad yazılarak arama yapılabilir. Bu sayede herkese açık olarak paylaşılmış bilgilere, fotoğraflara, kişinin yaşına, e-posta adreslerine ve okuduğu okullar gibi bilgilere ulaşılabilir.

Çıkan sosyal medya hesapları analiz edilerek kişi hakkında birçok bilgi elde edilebilir. Hedef sisteme ait IP hakkında bilgilere ipsorgu.com gibi siteler veya nslookup gibi araçlar sayesinde ulaşılabilir.

IP adresine CloudFlare Bypass yapılarak da ulaşılabilir. Hedef sistemin subdomainleri ve içerikleri gibi bilgilere arama motoru üzerinden ulaşılabilir. Yine e-posta adresleri, subdomainler, virtual hostlar ve açık olan portlar gibi bilgilere theHarvester aracılığı ile ulaşılabilir. WHOIS kullanarak domainler hakkında bazı bilgilere ulaşılabilir.

Archive.org kullanarak bir sitenin geçmişteki hâline bakabilir ve burada unutulmuş bilgiler ya da sistem açıkları sayesinde bugünkü sistemin kullandığı araçlar hakkında bilgilere ulaşılabilir. Archive.org ücretsiz bir site olup detay analizi yapılabilir. Oldukça kullanışlı bir sitedir. Shodan arama motoru kullanılarak internete bağlı cihazların tespiti yapılabilir. Zoomeye arama motoruyla da Shodan ile yapılan işlem gibi internete bağlı cihaz tespiti ve bu cihazların filtrelenebilir. Pasif keşif yaparak elde ettiğimiz e-posta adresinin daha önce siber saldırıdan etkilenip etkilenmediğini haveibeenpwned.com yardımıyla görüntüleyebiliriz. Google Advanced Search yardımıyla birçok gerekli bilgiye ulaşılabilir.

Pasif keşifte önemli olan araçların nasıl kullanılacağı ve buradan yola çıkarak nasıl iz sürülebileceğidir.

Sosyal Mühendislik

Bilgi güvenliği bağlamında sosyal mühendislik, eylemleri gerçekleştirmeye veya gizli bilgileri ifşa etmeye yönelik olarak insanların psikolojik manipülasyonudur. Bu, gizli bilgilerin ifşa edilmesiyle ilgili olmayan sosyal bilimlerdeki toplum mühendisliğinden farklıdır. Tüm sosyal mühendislik teknikleri karar verme sürecinin belirli özelliklerine dayanır. Sosyal mühendislikteki saldırılar, çalışanların gizli bilgilerini çalmak için kullanılabilir. En yaygın telefon görüşmesi sırasında çeşitli bilgilerin alınmasıyla yapılır. Bazen de şirket çalışanları bilgileri çalarlar ve fark edilmezler. Bu da başka bir örnektir.

Sosyal mühendislik, Robert Cialdini'nin oluşturduğu altı ilkeye dayanır: karşılıklık, bağlılık ve tutarlılık, sosyal kanıt, otorite, sempati ve kıtlık.

Sosyal mühendisliğe karşı şirketlerin alabileceği bazı tedbirler şunlardır:

- Çalışanları güvenlik protokolleri konusunda bilinçlendirmek
- Çalışan/personel düzeyinde standart bir çerçeve oluşturup kuralları belirlemek
- Güvenlik politikaları, prosedürleri ve protokolleri oluşturmak
- Güvenlik çerçevesi için habersiz periyodik testler düzenlemek
- Sosyal mühendislik hilelerine maruz bırakarak direnç aşılama
- Kilitli çöp kutuları ve bunların anahtarlarının sadece belli personelde bulunduğu bir atık yönetim sistemi kullanmak

Unutmamamız gerekir ki hiçbir çözüm bilgi güvenliği için mükemmel olmayacaktır ve şimdiye kadarki hiçbir sistem yüzde yüz güvenlik sağlamaz.





Senelerdir Eskimeyen Yöntem: Phishing

En eski ve en etkili saldırılardan biri olan phishing, bir diğer adıyla oltalama saldırısına bir göz atalım. Seçilen kişilerin e-postalarına; indirim haberleri, hediye kazandıklarını söyleyen mesajlar ve bunlara benzer cezbedici iletiler göndererek kişilerin kimlik bilgileri, banka hesap bilgileri, şifreleri ve bunlara benzer önemli bilgilerinin ele geçirilmesi hedeflenir.

Hedefin cezbedici linke tıklanması sağlanarak açılan sayfayla birlikte zararlı yazılımların sisteme girişi sağlanır. Böylece sistem zararlı yazılımı gönderen kişilerce ele geçirilmiş olur. Cezbedici iletiler; ücretsiz tatil, para ödülü, çekiliş, sosyal yardım, maaş ikramiyesi gibi ilgi çekici konular olabilir. Bu iletiler resmî kurumlarca gönderilmişçesine düzenlenerek şüphe çekmemek amaçlanır.

Kaç yıldır kullanılsa da yeterince bilinçli olunmadığı için bu yöntemle günümüzde bile dolandırılan çok fazla insan vardır.

Bilinçlendirme çalışmaları için güvenlik teşkilatlarınca taraflarımıza mesajlar gönderiliyor. Bu mesaj içerikleri “Para, ödül, hediye kazandınız gibi mesajlara itibar etmeyiniz!” ya da “Sizi arayıp bilgilerinizi isteyen kişilerle kişisel bilgilerinizi paylaşmayınız.” şeklindedir.

**ESRA
BAŞKURT**
KONU
50



PHISHING NEDİR?



Phishing (oltalama), kötü niyetli kişilerin, bireyleri, kişisel bilgileri, bankacılık bilgileri, kredi kartı numaraları ve şifreler gibi hassas verilere ulaşmaya ikna etmeye çalıştığı bir siber suç türüdür. Bu tür dolandırıcılık, aldatıcı e-postalar, telefon aramaları veya kısa mesajlar yoluyla gerçekleştirilir. Kişilerin bu bilgilerini ele geçirirse, saldırganlar daha sonra önemli hesaplara erişim sağlamak için bu verileri kullanabilirler. Bu tür bir saldırı sonucunda kimlik hırsızlığı ve maddi kayıplar meydana gelebilir.



Phishing E-postalarının Ortak Özellikleri

1 Olağanüstü İyilik

İnsanları tuzağa düşürmek için tasarlanan ilgi çekici açıklamalar veya teklifler bu sınıfa girer. E-posta adresinize gönderilen bedava tatil bileti buna örnek gösterilebilir. Saldırganlar sosyal mühendislikle veya ağ trafiği dinlemesi ile tatile gitmek istediğinizi öğrenmiş olabilir. Bu zafiyeti kullanmak için e-posta adresinize cazip bir teklif gönderebilir. Bu tür şüpheli mesajları açmamak gerekir. Unutmayın ki bedava peynir sadece fare kapanında olur.

2 Aciliyet Duygusu

Siber suçlular arasında yaygın bir taktik, süper fırsatların yalnızca sınırlı bir süre için geçerli olduğunu belirterek sizi hızlı hareket etmeye zorlamaktır. Bazıları size yanıt vermek için yalnızca birkaç dakikanızın olduğunu bile söyleyebilir. Bu tür e-postalarla karşılaştığınızda, en iyisi onları görmezden gelmektir. Bazen, kişisel bilgilerinizi hemen güncellemezseniz hesabınızın askıya alınacağını iddia edebilirler. Güvenilir kuruluşlar genellikle bir hesabı feshetmeden önce kullanıcılara yeterli zaman tanır ve kişisel bilgilerini İnternet üzerinden güncellemelerini talep etmez. Şüphe duyduğunuzda, bir e-postadaki bir bağlantıya tıklamak yerine doğrudan kaynağı ziyaret etmek daha güvenli bir yaklaşımdır.

3

Bağlantılar

Herhangi bir bağlantının görünen metni ile üzerine gelindiğinde gösterdiği bağlantı farklı olabilir. Bağlantı metni üzerinde fare ile gezinildiğinde ekranınızda görünen URL, yönlendirilecek olan URL'yi temsil eder. Bu URL, beklenen alan adından oldukça farklı bir alan adı içerebilir veya popüler bir web sitesinin benzer karakterler kullanılarak oluşturulmuş yanıltıcı bir alan adını işaret ediyor olabilir.

Örneğin, "www.abc.com" şeklinde bir sitemiz olduğunu düşünelim. URL içindeki "com" kısaltması yerine "r" ve "n" harfleri kullanılarak hedef kullanıcıyı farklı bir bağlantıya yönlendirilmeye çalışılmıştır.

E-posta adreslerine güvenilir kaynaklardan gelen mesajlar da farklı bir adrese yönlendiren bağlantılar içerebilir. Güvenilir kaynaktan gelen mesajlarda genellikle yönlendirme bağlantısını kontrol etme ihtiyacı hissedilmez; bu nedenle bu tür mesajlarla karşılaşan insanlar phishing saldırısına uğrayabilir.

4

Eklenen Belgeler

Bir e-postada beklemediğiniz veya anlamsız bir ek görürseniz, açmayın! Genellikle fidye yazılımı veya diğer virüsler gibi zararlı yazılımlar içerirler. Tıklanması her zaman güvenli olan tek dosya türü bir .txt dosyasıdır.

5

Beklenmeyen Gönderici

Tanıdığınız veya tanımadığınız birinden gelen şüpheli mesajlar phishing saldırısı içeriyor olabilir.



Phishing Saldırılarını Önleme Yolları

Günümüzde var olan ve günden güne gelişen teknoloji ile siber suçluların kullandıkları saldırı yöntemleri değişiklik göstermektedir. Bu saldırılardan basit güvenlik önlemleri olarak kaçınılabilir.

1

Phishing Teknikleri Hakkında Bilginiz Olsun

Güncel phishing saldırılarını takip ederek kişisel bilgilerinize ulaşmak isteyen kişilerin saldırılarını fark edebilirsiniz.

2

Tıklamadan Önce Düşünün!

Sayfa kaynağı güvenilir sitelerde bağlantıları açmak bir zafiyet oluşturmaz. Ancak rastgele e-postalarda ve anlık mesajlarda görünen bağlantılara tıklamak o kadar akıllıca bir hareket değildir. Tıklamadan önce emin olmadığınız bağlantıların üzerine gelin. Yönlendirilecek bağlantının beklenen alan adını içerip içermediğinden emin olun.

Bir phishing e-postası, yasal bir şirketten geldiğini iddia edebilir ve tıkladığınızda web sitesinin bağlantısı, tam olarak gerçek web sitesi gibi görünebilir. E-posta, sizden bilgileri doldurmanızı isteyebilir ancak e-posta adınızı içermeyebilir. Çoğu phishing e-postası genellikle "Sayın Müşteri" ifadesiyle başlar, bu yüzden bu tür e-postalarla karşılaştığınızda dikkatli olmalısınız. Şüpheli durumlarda, potansiyel olarak tehlikeli bir bağlantıya tıklamak yerine doğrudan kaynağa gidin.

3

Bir Phishing Önleme Aracı Edinin

İnternet kullanıcılarının %97'sinin karmaşık phishing e-postalarını tanımlamadığını, bu kişilerin %30'unun bu e-postaları açtığını ve %12'sinin bu e-postalardan zarar gördüğünü biliyor musunuz? Ayrıca phishing saldırıları önceki yıla göre %65 arttı. Bu saldırılardan korunmak için phishing önleme aracı (anti-phishing toolbar) edinebilirsiniz. Kullanılan araca göre farklı özellikler olsa da genel olarak kullanıcının güvenilir sayfalarda gezinmesini sağlar. Şüpheli görülen sayfalarda kullanıcıya uyarı verir, sayfanın erişimini engeller. Netcraft anti-phishing yazılımı bu araçlara örnek verilebilir. Yazılım phishing saldırısı yapılabilecek sitelere erişimi engellemesinin yanı sıra banka bilgisinin kötüye kullanımını engelleme ve kötü amaçlı yazılımların cihazınızda çalışmasını engelleme gibi özellikleri vardır.

4

Sitenin Güvenliğini Doğrulayın

Hassas finansal bilgiler ile işlem yaparken biraz temkinli olmak doğaldır. Ancak güvenli bir web sitesinde olduğunuz sürece herhangi bir sorunla karşılaşmazsınız. Herhangi bir bilgi göndermeden önce sitenin URL'sinin "https" ile başladığından ve adres çubuğunun yanında kapalı bir kilit simgesinin bulunduğundan emin olun. Sitenin güvenlik sertifikasını da kontrol edin. Belirli bir web sitesinin kötü amaçlı dosyalar içerebileceğini belirten bir mesaj alırsanız, web sitesini açmayın. Şüpheli e-postalardan veya web sitelerinden asla dosya indirmeyin. Arama motorları bile kullanıcıları düşük maliyetli ürünler sunan bir phishing web sayfasına yönlendirebilecek belirli bağlantılar gösterebilir. Kullanıcı böyle bir web sitesinde alışveriş yaparsa, siber suçlular kredi kartı bilgilerine erişecektir.

5

Çevrimiçi Hesaplarınızı Düzenli Olarak Kontrol Edin

Olası bir hesap çalınma durumunu fark edebilmek adına düzenli olarak çevrimiçi hesapların kontrol edilmesi önemlidir. Teknik olarak ihtiyacınız olmasa bile çevrimiçi hesaplarınızın her birini düzenli olarak kontrol edin. Şifrelerinizi de düzenli olarak değiştirme alışkanlığı edinin. Banka kimlik avı ve kredi kartı kimlik avı dolandırıcılıklarını önlemek için ekstrelerinizi düzenli olarak kişisel olarak kontrol etmelisiniz. Mali hesaplarınız için aylık hesap özetleri alın ve bilginiz dışında herhangi bir dolandırıcılık işlemi yapılmadığından emin olmak için her girişi dikkatlice kontrol edin.

6

Tarayıcınızın Sürümünü Güncelleyin

Yaygın kullanılan tarayıcılarda güvenlik açıklarının bulunması nedeniyle sık sık güvenlik yamaları yayımlanır. Eğer kullanıcı tarayıcısını yeni yamalarla güncellemezse var olan sürümde bulunan zafiyetler siber suçlular tarafından sömürülebilir. Bu nedenle tarayıcının güncel olması önemlidir.

7

Güvenlik Duvarı Kullanın

Güvenlik duvarı, bilgisayarınızı dışarıdan gelebilecek tehditlere karşı korur. Mevcut antivirüs yazılımına ait veya işletim sistemi tarafından varsayılan olarak sunulan güvenlik duvarını her zaman etkin tutmaya özen gösterin.

8

Pop-Uplara (Açılır Pencere) Karşı Dikkatli Olun

Açılır pencereler genellikle bir web sitesinin doğal bileşenleri gibi görünür. Çoğunlukla ortalama amaçlı olabilmektedir. Birçok popüler tarayıcı açılır pencereleri yönetmenize imkân sağlar. Gerekli görülen durumlarda açılır pencerelere izin verebilirsiniz. Bazı açılır pencerelerde kullanıcıyı kandırmaya yönelik, “iptal”, “kapat” gibi butonlar görülebilir. Bu butonlar açılır pencereyi kapatmak yerine ortalama ya da zararlı içeriği olan sayfalara yönlendirebilir. Bunun yerine pencerenin üst köşesindeki küçük “x” işaretine tıklayın.

9

Kişisel Bilgilerinizi Asla Paylaşmayın

Kişisel veya mali açıdan hassas bilgileri asla internet üzerinden paylaşmamalısınız. Şüphe duyduğunuzda, söz konusu şirketin resmî web sitesinde bulunan iletişim bilgileri üzerinden iletişime geçmelisiniz. Phishing e-postalarının çoğu sizi finansal veya kişisel bilgi girişlerinin gerektiği sahte sayfalara yönlendirmeye çalışır. Yetkili kimseler de dâhil olmak üzere kimseye hassas bilgiler içeren bir e-posta göndermeyin. Web sitesinin adresini kontrol etmeyi alışkanlık hâline getirin.

Antivirüs yazılımı kullanmanın birçok nedeni vardır. Virüsten koruma yazılımının içerdiği özel imzalar, bilinen tehditlere ve güvenlik açıklarına karşı koruma sağlar. Bu nedenle yazılımınızı güncel tutmanız önemlidir, çünkü sürekli yeni güvenlik açıkları keşfedilmektedir. Antivirüs yazılımları internet üzerinden gelen her dosyayı tarar ve sisteminizin zarar görmesini önlemeye yardımcı olur. Bununla birlikte, phishing saldırılarını önlemek için casus yazılım engelleme ve güvenlik duvarı ayarları da kullanılmalı, ayrıca kullanıcılar programları düzenli olarak güncellemelidir.



Phishing e-postasına cevap verilirse ne yapılmalıdır?

Farkında olmadan bir phishing e-postasına kimlik bilgilerinizi ya da banka bilgilerinizi göndermiş olabilirsiniz. Bu dakikadan sonra dolandırılma ihtimaliniz çok yüksek olsa da hızlı hareket ederseniz zararı en aza indirebilirsiniz.

Şifrelerinizi değiştirin. Banka şifreleriniz, kredi kartı ve diğer hesaplarınız için kullandığınız şifreleri mutlaka değiştirin. Bu şifrelerin kırılmasını daha zor hâle getirmek için parolanızda sayıların, harflerin ve sembollerin bir kombinasyonunu kullanın. Varsa çok faktörlü kimlik doğrulamayı etkinleştirin. Çok faktörlü kimlik doğrulama bir hesaba erişmek için akıllı telefonunuza gönderilen bir kod gibi ikinci bir bilgi parçasının girilmesini gerektirir.

Bankanızla iletişime geçin. Kredi kartı bilgilerinizi verdiyseniz hemen kredi kartı sağlayıcınızı arayın. Yetkisiz satın alma işlemlerini önlemek için kredi kartınızı dondurun ve yenisini isteyin.

Siber suçlular phishing saldırılarını ve diğer tekniklerini geliştirmeye devam ederken güvenlik yazılımları kullanılabilir.

KAYNAKÇA

<https://www.phishing.org/>

<https://wethegeek.com/6-free-anti-phishing-toolbars-to-prevent-unwanted-online-activities/>

<https://uzmanposta.com/blog/phishing-nedir/>





HONEYPOT NEDİR?

Bal K p  (Honeypot) Nedir?

Bal K p , bilgisayar sistemlerinin siber saldırılara kar ı benzersiz  ekillerde savunma yapmasına yardımcı olabilecek bir g venlik aracıdır. Bal k pleri bilgisayar ađına bađlıdır. Bu ađa bađlı sistem, siber saldırganları ger ek hedeflerinden uzakla tırmak i in bir tuzak gibi hareket ederek saldırıları erkenden tespit etmeye ve uygun bir yanıt verilmesine olanak sađlar.

Bal k pleri, internette potansiyel bir hedef olarak hareket eder ve bilgi sistemine yapılan herhangi bir yetkisiz giri im hakkında koruma sistemlerini bilgilendirir.  ođunlukla siber g venlikle uđra an b y k  irketler ve kurulu lar tarafından kullanılır. Siber g venlik ara tırmacılarının saldırganlar tarafından kullanılan farklı saldırı t rleri hakkında bilgi edinmesine yardımcı olur.



Bal K p  T rleri

 stenilen saldırı senaryolarını ve ortamlarını sađlamak i in farklı t rde Bal k pleri mevcuttur. Bunun i in belirlenmi  bir standart olmasa da bal k pleri kullanım amacına ve  r n sistemleriyle etkile imlerine g re sınıflandırılabilir.

Bal k pleri etkile im seviyelerine g re   e ayrılır:

Saf Bal k pleri: Bir Bal K p n n ađ bađlantısını izleyen tam te ekk ll   retim sistemleridir. En karma ık ve bakımı en zor olanlardır, ancak aynı zamanda sahte gizli dosyalar ve kullanıcı bilgileriyle birlikte saldırganlar i in en ger ek i g r n me sahiptirler.

D   k Etkile imli Bal k pleri: Su luların dikkatini  eken hizmetleri ve sistemleri taklit eder. Botnet'ler ve solucanlar k t  ama lı yazılımları gibi k r saldırılardan veri toplamak i in bir y ntem sunarlar.

Y ksek Etkile imli Bal k pleri: T m hizmetleri ve uygulamaları sim le etmek ve saldırgana zaman kaybettirmek  zere tasarlanmı tır.

Bal k pleri kullanım ama larına g re ikiye ayrılır:

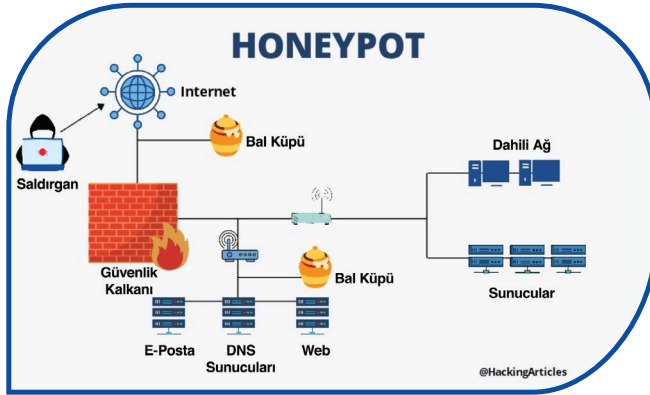
 retim Bal k pleri: Genellikle izinsiz giri  tespit sisteminin (IDS) bir par ası olarak,  alı an ađlar ve sunucular i inde sahte sistemler olarak hizmet verir. G venlik a ıklarını azaltmaya yardımcı olmak i in k t  niyetli etkinlikleri analiz ederken su luların dikkatini ger ek sistemden saptırırlar.

Araştırma Bal küpleri: Eğitim ve güvenlik geliştirme amaçlı kullanılır. Saldırıyı analiz etmek için çalışıldığında izleyebileceğiniz veriler içerirler.

Bal küplerinin Çalışma Mantığı

Saldırgan, saldırmak istediğinde karşısında yapılandırılan bir sistemi görür. Gördüğü sisteme sanki gerçek bir sistemmiş gibi saldırmayı dener ve Bal Küpü devreye girer. Saldırganın hareketlerini, saldırı tekniğini loglamaya başlar. Böylelikle saldırırganın nereden ve hangi teknikle saldırmış olduğunu öğrenerek sistemde gerekli güvenlik önlemleri almaya çalışılır.

Bir Bal Küpünün temel amacı saldırıları tespit etmek, öğrenmek ve güvenliğini arttırmak için bilgiyi kullanmaktır.



Şekil 1: Bal Küpü Sisteminin Çalışma Mantığının Gösterimi

Bal küplerinin Avantajları

Honeypot kullanımının başlıca yararları aşağıdaki gibi sıralanabilir:

- Güvenliği artırır.
- Anlaşılması basit, kullanımı ve bakımı kolaydır.
- Saldırgan herhangi bir şifreleme yöntemi kullansa bile, Bal Küpü tarafından kötü amaçlı aktivite kaydedilir.
- Saldırıyı yapan kişilerin davranışlarının, nasıl bir yol izlediklerinin incelenmesini sağlar.
- Güvenlik uzmanlarının bilinen ve bilinmeyen saldırılar hakkında daha fazla bilgi edinmesine yardımcı olabilir.
- Sızma testi işlemleri için kullanılabilir.
- Bal Küpü tekniği herhangi bir üst düzey ekipman gerektirmez. Sistemin tek

amacı, yüksek performans gerektirmeyen hacker ile etkileşim kurmaktır. Bu nedenle kurulumu uygun maliyetlidir.

- False-Positive uyarıların daha az gelmesini sağlar.
- Olay müdahâle süreçlerini test etmeye yardımcı olur.
- Dikkat dağıtıcı bir yapıya sahiptir.

Bal küplerinin Dezavantajları

Honeypot kullanımının başlıca zararları aşağıdaki gibi sıralanabilir:

- Uygun yere konumlandırılmazsa sisteme girişi kolaylaştırabilir.
- Yakalanan kötü amaçlı trafik, yalnızca Bal Küpü ağını hedef aldığında toplanabilir. Bu nedenle saldırganlar ilgili ağın bir Bal Küpü ağı olduğundan şüphelenirlerse bundan kaçınabilirler.
- Saldırgan sistemde Bal Küpü olduğunu tespit ederse, Bal Küpüne dokunmadan diğer sistemlere saldırmaya devam edebilir.
- Bal Küpünde “parmak izi” olduğundan saldırgan, üretim sistemlerine hedeflenen gerçek bir istismarın gözden kaçırılması için sahte saldırılar oluşturabilir.
- İyi tasarlanmamış bir Bal Küpü kritik sistem bilgilerini içerebilir ve tüm sistemi tehlikeye atabilir.
- Her zaman bir saldırganı tanımlayamaz.
- Bir Bal Küpü saldırıya uğradığında diğer sistemlere saldırmak için kullanılabilir.



Bal K p  Tespit Y ntemleri

- Siber saldırılar ve izinsiz giriřler s z konusu olduėunda, zaman  nemlidir.
- Bal k pleri gibi  eřitli teknikler, siber g venlik ekibini  ok hızlı bir řekilde ayaėa kaldırabilir.
- Bal k plerini tespit etmek i in bazı yazılımlar vardır. Bunlardan  ne  ıkanı Send-Safe Honeypot Hunter'dır. Bunun gibi yazılımlar portları, portlarda  alıřan servisleri analiz ederek sistemin ger ek veya tuzak bir sistem olduėunu anlamaya yarar. Diėer bir yazılım ise Nessus'tur. Bu da uzak sistemde Bal K p  olup olmadıėını tespit etmek i in sistemi analiz eden bir yazılımdır.

Diėer bazı yazılımlar ise řunlardır:

- Dionaea
- Conpot
- Amun
- Kojoney HonSSH
- Glastopf
- Kippo

KAYNAK A

[1] <https://muhammedyusufolgun.blogspot.com/p/bal-kupu-honeypot-nedir.html>

[2] <https://oxylabs.io/blog/what-is-a-honeypot>





OWASP

HEY OWASP NESİN SEN?

OWASP (Open Web Application Security Project) yani Açık Web Uygulaması Güvenlik Projesi, Web uygulamalarını güvenli bir şekilde korunmasını sağlamasıyla, güvenlik açıklarının kapatılmasıyla ilgili çalışmalar yapan bağımsız topluluktur. OWASP Top 10 bilinen tüm web açıklıklarını puanlama sistemi yaparak sıralar ve en popüler liste olarak yayımlar. Bu listeyle kullanıcıların; tehditlerin, risklerin sonuçlarının ve önlemlerin farkında olması amaçlanmıştır.

OWASP Top 10 - 2017	BNIT	OWASP Top 10 -2021
A1 Injection		A1 Broken Access Control
A2 Broken Authentication		A2 Cryptographic Failures
A3 Sensitive Data Exposure		A3 Injection
A4 XML External Entities (XXE)		A4 Insecure Design
A5 Broken Access Control		A5 Security Misconfiguration
A6 Security Misconfiguration		A6 Vulnerable and Outdated Components
A7 Cross-Site Scripting (XSS)		A7 Identification and Authentication Failures
A8 Insecure Deserialization		A8 Software and Data Integrity Failures
A9 Using Components with Known Vulnerabilities		A9 Security Logging and Monitoring Failures
A10 Insufficient Logging & Monitoring		A10 Server-Side Request Forgery

Peki Güvenlik Açığı ne demek?

Donanımsal ya da yazılımsal eksiklikler/hatalar güvenlik açığı anlamına gelmektedir. Donanımsal açıklık, donanım tasarımı hatalarıdır, cihaz modellerine özgüdür.

Yazılımsal güvenlik açığı ise uygulama kodlarından ya da işletim sistemindeki hatalardan kaynaklanmaktadır. Kullandığımız mobil uygulamalar, web tarayıcıları üretici firma tarafından güncellenerek güvenlik açıklarını kapatmayı, riskleri en aza indirmeyi hedefler.

Güvenlik Açıkları için nasıl önlemler alabiliriz?

Eski yazılımlar kullanmak saldırganların güvenlik açığı tespit etmesine neden olabilir. Yani kullandığımız uygulamaları güncellemeliyiz.

Web sitelerine giriş şifrelerini, mobil uygulama şifreleri için tahmin edilmesi zor, güçlü şifreler olacak şekilde oluşturmalıyız. Farklı uygulamalar için farklı şifreler oluşturmalıyız böylece bir uygulamadaki bilgilerimiz ele geçirilse bile saldırganlar diğer uygulamalardaki şifremize erişip zarar veremeyecektir.

Firewall (güvenlik duvarı) araçlarını bireysel ve iş yerlerinde kullanmamız siber saldırıların önüne geçmeye yardımcı olur. Bu sayede kötü niyetli saldırganlar kişisel verilerimize ulaşamayacaklardır.

1) BROKEN ACCESS CONTROL (Eriřim Kontrolü İhlali)

Yetkilendirme açığı olarak tanımlayabiliriz. Kimliği doğrulanmış kullanıcıların sistemde yapabileceğı olaylar ve yapamayacağı olayların doğru şekilde ayarlanmamasından oluşur bu zafiyet. Saldırganlar, kullanıcıların hesaplarına erişebilir, verilerini değiřtirebilir, erişim kısıtlamalarında bulunabilir. Bu zafiyete önlem olarak izin kontrol sistemi doğru şekilde yapılmalı, yanlış erişimlerin kayıtları tutulmalı ve bu log kayıtları sistem yöneticisine raporlanmalıdır.

2) CRYPTOGRAPHIC FAILURES (Şifreleme Hataları)

Verilerin şifrlenmemesi veya şifrelenen verilerin önceden bilinen şifreleme algoritmaları ile kullanılmasıyla ortaya çıkar. Kredi kartı bilgileri, parolalar gibi işlemlerinin istemci tarafından şifrlenmesi gerekir. Saldırganlar, SQL Injection yöntemiyle veri tabanına kolaylıkla sızıp bu verilere apaçık şekilde erişebilir. Eğer bu veriler şifrelenmiş olursa saldırgan şifreli verileri anlamlandıramaz ve istediğine ulaşamaz. Sadece sistem tarafından veriler değil kullanıcı tarafından girilen verilerde sistem tarafından şifrelenerek kaydedilmeli. İstemciden sunucuya aktarırken de şifreleme algoritmaları kullanılmalıdır. Aksi durumda saldırganlar istemci-sunucu,sunucu-istemci arasındaki veri aktarımını izleyerek de bilgileri ele geçirebilirler.

Örneğın, <https://gelecegiyazanlar.turkcell.com.tr/> sitesine kaydolurken kullanıcı adına Merve_61, şifre kısmına da 123456 şekilde kaydolduğumu varsayalım (Bu şifre çok kolay tahmin edilebilir, zayıf şifreye örnek olması için verdim.), site şifremini kaydederken güncel ve güçlü şifreleme algoritmasını kullanmadıysa saldırgan kayıt olarak girdiğim bu bilgileri olduğı gibi görecektir. Bu zafiyetten etkilenmek için yedekleme işlemi, veri transferi işlemi yapılırken eski, default şifreleme algoritmaları yerine güncel ve güçlü şifreleme algoritmaları kullanılmalıdır. http, ftp, smtp gibi güvensiz protokoller yerine şifreli transfer yapan https, ftps, smtps protokolleri tercih edilmelidir. (Farkları sondaki 's' harfi yani security ifadesiyle yapılan işlemlerdir.)

3) INJECTION (Enjeksiyonlar)

Kullanıcıdan alınan ve kontrol edilmeyen verilerden kaynaklıdır. Saldırgan, uygulamanın programlanmadığı bir şeyi yapmaya zorlamak amacıyla web sitesine geçersiz veriler enjekte eder.

->SQL Injection saldırıları, kullanıcıdan gelen verileri doğrudan SQL sorgularına dâhil ederek web sitesine sızma işlemidir. Saldırganlar, tablolardaki verileri görebilir, değiřtirebilir, silebilir, yönetici hesabını ele geçirebilir. Bu tür saldırıları önlemek için verilerin komutlardan ve sorgulardan ayrı tutulması gerekir.

4) INSECURE DESIGN

(Güvensiz Tasarım)

Tasarım ve mimarideki eksikliklerle ilgili risklere odaklanır. Tehdit modellemesi, güvenli tasarım kalıplarına duyulan ihtiyaca odaklanır. Güvensiz tasarımdaki kusurlar, uygulama ile düzeltilemez.

5) SECURITY MISCONFIGURATION

(Yanlış Güvenlik Yapılandırmaları)

Servis ayarlarının yanlış ya da eksik yapılandırmasından dolayı oluşur. Saldırganlar sistemler hakkında yetkisiz erişim, yetki yükseltme işlemleri için sistemlerdeki düzeltilmemiş açıklıklardan yararlanıyorlar. Bu açıklıklardan sızarak sistemin içine, korumasız dosyalara erişmeye çalışırlar. Bu zafiyetten korunmak için gereksiz bileşenler, kullanılmayan özellikler kaldırılabilir. Yeni güncellemelerle gelen notlar inceleyip yeni yapılandırmalar yapılabilir. Sistem her zaman güncel tutulmalıdır.

6) VULNERABLE AND OUTDATED COMPONENTS

(Savunmasız ve Eski Bileşenler)

Kullanılan servisler, kütüphaneler, uygulamalar ve çeşitli eklentilerin eski veya exploitleri olduğu bilinen sürümlerin kullanılmasıyla oluşur. (Exploit: Sistem açıklarını kullanan, kod hatalarından faydalanan, planlanmamış ve istenmeyen hatalar oluşturmak için hazırlanan kodlar ve programlara denir.) Bu zafiyeti önlemek için kullanılmayan gereksiz özellikleri, bileşenleri ve dosyaları kaldırmak gerekir. İstemci ve sunucu tarafındaki bileşenlerin sürümlerinin devamlı güncel olup olmadığı kontrol edilmelidir. Düzenli olarak Zero Day denilen yeni çıkan zafiyetleri kontrol edip sistemi güncel tutmak gerekir.

7) IDENTIFICATION AND AUTHENTICATION FAILURES

(Tanımlama ve Kimlik Doğrulama Hataları)

Kimlik doğrulama, oturum yönetimi gibi fonksiyonların yanlış kullanılıp uygulanması sonucu ortaya çıkar. Kötü niyetli saldırganlar genellikle Brute Force (kaba kuvvet saldırısı) yaparak sistemdeki kayıtlı kullanıcıların kullanıcı adı, parolalarını çalabilir. Bazı kullanıcılar kullanıcı adı ve parolalarını ilk oluşturdukları şekilde default parolaları yani sistemin otomatik olarak verdiği şifreyi değiştirmeden kullanır. Saldırganlar bu şekilde olan kullanıcıların bilgilerine daha kolay erişebilir. Bu saldırıdan korunmak için tahmin edilmesi zor, güçlü parolalar kullanılmalıdır, çok faktörlü kimlik doğrulaması işlemleri uygulanmalıdır.

8) SOFTWARE AND DATA INTEGRITY FAILURES (Yazılım ve Veri Bütünlüğü Hataları)

Bütünlük doğrulaması yapılmadan yazılım güncellemelerinin otomatik olarak yapıldığı CI(Continuous Integration-Sürekli Entegrasyon) ve CD(Continuous Delivery-Sürekli Teslimat) süreçlerine odaklanır.

9) SECURITY LOGGING AND MONITORING FAILURES (Güvenlik Günlüğü ve İzleme Hataları)

Yeterli loglama yapılmadığı için eksik veya etkisiz yapılandırmalar yüzünden, saldırganların sisteme daha fazla saldırmasına, sistemdeki kalma süresini artırarak, sistemdeki verileri kurcalayıp istediği gibi değiştirmesine ya da yok etmesine imkân verir. Bu tür bir zafiyeti önlemek için tüm oturum açma işlemlerinin ve sistemden alınan tüm hataların düzenli olarak log kaydı tutulabilir.

10) SERVER-SIDE REQUEST FORGERY (SSRF – Sunucu Tarafı İstek Sahteciliği)

Bir saldırganın güvenlik açığı bulunan uygulamanın arka uç sunucusundan hazırlanmış istekler göndermesine olanak sağlar. Saldırganlar genellikle güvenlik duvarlarının arkasındaki ve harici ağdan erişilemeyen dâhili sistemleri hedeflemek için SSRF saldırılarını kullanır.

KAYNAKÇA

<https://owasp.org/www-project-top-ten/>

https://www.beyaz.net/tr/guvenlik/makaleler/owasp_nedir.html

<https://www.siberkavram.com/2022/04/owasp-top-10.html>

<https://berqnet.com/blog/guvenlik-acigi>

[https://www.bntpro.com/owasp-top-10-2021-listesi-ve-f5-awaf-korumalari/#:~:text=OWASP%20Top%2010%20\(Open%20Web,yaz%C4%B1l%C4%B1m%20geli%C5%9Firme%20k%C3%BCl%C3%BCr%C3%BCn%C3%BC%20de%C4%9Fi%C5%9Firmeyi%20ama%C3%A7lamaktad%C4%B1r.](https://www.bntpro.com/owasp-top-10-2021-listesi-ve-f5-awaf-korumalari/#:~:text=OWASP%20Top%2010%20(Open%20Web,yaz%C4%B1l%C4%B1m%20geli%C5%9Firme%20k%C3%BCl%C3%BCr%C3%BCn%C3%BC%20de%C4%9Fi%C5%9Firmeyi%20ama%C3%A7lamaktad%C4%B1r.)





SUNUCU GÜVENLİĞİ

Sunucu nedir?

Sunucular kullanıcılara veri sunmak amacıyla yüksek teknolojiye sahip güçlü bilgisayarlardır. Standart kullanıcı bilgisayarlarından temel farkı kullanıcı bilgisayarları kişiye özel iken sunucular yüzlerce kullanıcıya aynı anda servis sağlar, bundan dolayı sunucular kişisel bilgisayarlardan daha yüksek teknolojiye sahiptir. Yüksek sayıda kullanıcılara aynı anda 7/24 geri dönüş sağladığı için kullanıcı bilgisayarlarından farklı olarak yüksek kapasiteli RAM, depolama alanı, CPU gibi donanımlara sahiptir. Yüksek teknolojisi ve sürekli çalışması nedeniyle daha çok elektrik tükettiği için ısınma problemi ile karşılaşılabilir. Isınmalara karşı hava sirkülasyonunu sağlayacak soğutma sistemleri bulunmaktadır. Bu bilgisayarların bulunduğu yerler sunucu odaları olarak adlandırılır. Yüksek teknolojiye sahip özel cihazlar oldukları için sunucular 7/24 internet, güç (elektrik) ve güvenlik sağlayacak bu odalarda yer alır. Sunduğu verilere göre sınıflandırılabilirler. Örneğin e-posta servisini çalıştırıyorsa e-posta sunucusu (e-mail server), web sitesi çalıştırıyorsa web sunucusu (web server), dosya çalıştırıyorsa dosya sunucusu (file server) olarak sınıflandırılabilir. Sunucular bulundurdıkları yüzlerce kullanıcıya sağladığı veri nedeniyle siber saldırılara maruz kalmaktadır. Bundan dolayı güvenliklerinin sağlanması gerekmektedir.

Sunucu güvenliği nedir?

Sunucu güvenliği, sunucularda tutulan hassas veri ve kaynakları korumak için kullanılan tüm süreç ve araçlardır. Sunucular bulundurdıkları hassas veriler nedeniyle siber saldırılara hedef olurlar. Finansal kazanç ve diğer nedenlerle sunucularda güvenlik açıklarından yararlanmak için siber suçlular sürekli tetikte olurlar.

Zayıf şifre, yeni yazılım güncellenmemesi gibi çok küçük sorunlar, sunucularda büyük sonuçlara yol açabilir.

Bu sebeple, güvenliği artırmak için ağımdaki potansiyel saldırılara karşı sorunları belirleyip sistemin güvenliğini sağlamalıyız. Güvenliğin sağlanması için birçok strateji bulunmaktadır. Bazıları aşağıdaki gibidir.

1. Güvenlik duvarı (firewall):

Güvenlik duvarı bir ağa yetkisiz erişimi önleyen, ağlar arası iletişimde ağ trafiğini izleyen ve denetleyen bir yazılım veya donanım aygıtıdır. Güvenlik altyapınız için bir güvenlik duvarından yararlanarak gelen ve giden trafiği önceden tanımlanmış bir dizi güvenlik ilkelerinden denetlenir.

2. Yazılım güncellemeleri:

Siber tehditlerinden korunması için düzenli güncellemeler yapılması gerekir. Eğer başarısız bir güncellenme olursa siber suçluların yeni ataklarına karşı koruma sağlanamaz ise büyük sonuçlara yol açabilir.

3. SSH (Güvenli kabuk):

SSH (Secure Shell, Güvenli Kabuk), Linux sunucularına güvenli bir şekilde erişmek için kullanılan şifreli bir protokoldür. SSH sunucusunun varsayılan yapılandırmasında TCP (iletim kontrol protokolü) 22'den gelen bağlantı noktası olduğu iyi bilindiği için kötü amaçlı saldırganlar tarafından hedeftir. Çalışan bir SSH varsa ve dış dünyaya açıldıysa, güçlü parola ve kullanıcı adı gereklidir. Çünkü siber suçlular parolayı veya kullanıcı adını tahmin ederlerse sisteme sızarak sunucu ve tüm kullanıcıların verilerini tehlike altına sokabilirler. Güvenli bağlantı kurulmasını şifreleme tekniği ile sağlar. Farklı bir bağlantı noktası kullanılması saldırılara karşı alınacak yöntemlerden bir tanesidir.

4. Root(kök dizini) girişi engellenmesi:

Root (cihaza en üst düzey erişim izni olan) girişi en yaygın ve en tehlikeli güvenlik ihlallerinden biridir. SSH aracılığıyla kök dizininde doğrudan oturum açmaya izin verir. Bununla birlikte kök parolanızı kaba kuvvet saldırısı (birden fazla parola veya kullanıcı adı deneme) ile ele geçirerek sisteme erişir. Bu saldırı altında ağır hasar alır. Bu gibi durumların oluşmaması için kök girişinin engellenmesi gerekir.

5. Açık portlar kontrolü:

Portlar ile sunuculara bağlanan geçişlerdir. Sunucuya giriş için aktif portların görüntülenmesi ve kullanılmayanların kapatılmasının yanı sıra saldırı amaçlı kullanıcıların geçiş yapabilecekleri portlar da kapatılarak daha güvenli ağ sağlanır.

6. Boş parola:

Sistemde parola kullanmayan kullanıcıların bağlantı kurmaması için sunuculara erişmesini engellemek gerekir. Bunun gibi kullanıcıları engellemek için **sshd_config** dosyasındaki **PermitEmptyPasswords** satırın yanına **no** yazarak ayarlanabilir.

7. Sınırlı oturum açma/kapama:

Sunucularda istediğimiz kadar parola denemesi yaparak erişim sağlayabiliriz fakat saldırganlar sunucuya kaba kuvvet saldırısını uygulamak için bu güvenlik açığını kullanabilir. Sınırlı sayıda denemeden sonra SSH bağlantısını otomatik olarak sonlandırabilirsiniz.

8. SSH Version 2:

İlk sürümdeki birçok güvenlik açığı nedeniyle SSH 2 sürümü yayımlandı.

KAYNAKÇA

<https://www.cenuta.com/sunucu-vps-vds-nedir-video>
<https://www.hosting.com.tr/bilgi-bankasi/server-nedir-turleri-nelerdir/>
<https://www.arge24.com.tr/sunucu-guvenlik-servisleri-sunucularinizi-nasil-korur/>
<https://maryateknoloji.com.tr/sunucu-guvenligi/>
<https://www.limonhost.net/makaleler/genel/ssh-nedir-ssh-ne-ise-yarar/>
https://www.hostinger.web.tr/rehberler/ssh-nedir#SSH_nedir
<https://www.goldverikurtarma.com/sunucu-guvenligi-nedir>
<https://www.dmbilisim.com/cozumlerimiz/server-security.html>





SİBER SALDIRILAR VE YAPAY ZEKÂ

Siber Saldırılar ve Yapay Zekâ (AI)

Siber güvenlik dünyası çok disiplinli ve birçok alanla derinden ilişkili bir başlıktır.

Yapay zekâ (Artificial Intelligence) uygulamalarının siber güvenlik alanında kullanılması birçok endüstrinin geleceğini güvenceye almasını sağlar.

Günümüzde yapay zekâ çalışmaları daha hızlı cevaplar, daha iyi sonuçlar ve gelişmiş verimliliği sağlar.

AI(Artificial Intelligence) ve ML(Machine Learning) nedir?

Yapay zekâ (AI, Artificial intelligence): Görevleri yerine getirmek için insan zekâsını taklit eden ve topladıkları bilgilere göre yinelemeli olarak kendilerini iyileştirebilen sistemler veya makineler anlamına gelir.

Makine öğrenimi (ML, Machine learning): Mevcut davranış şablonlarını kullanarak önceki veri ve sonuçlara göre karar alma yapıları oluşturur. Yine de bazı değişiklikler için insan müdahâlesi gerektirir. Makine öğrenimi, bugüne kadarki en uygun AI siber güvenlik disiplindir.

Yapay Zekânın Siber Saldırılar Dünyasındaki Rolü Nedir?

Yapay zekânın siber güvenlikteki rolü, kuruluşların güvenliğındeki riski azaltmak ve genel güvenlik duruşlarını iyileştirmelerine yardımcı olmaktır.

AI, kalıpları (patterns) ve eğilimleri (trends) belirlemek için geçmiş verilerden öğrenerek siber güvenlik dünyasındaki sorunları çözmeye çalışır. Bu bilgiler daha sonra gelecekteki saldırılar hakkında tahminlerde bulunmak için kullanılır.

Yapay zekâ destekli sistemler, tehditlere otomatik olarak yanıt verecek ve daha hızlı zaman ölçeklerinde siber tehditlerle mücadele edecek şekilde de yapılandırılabilir.

Kurumsal saldırı yüzeyi gelişmeye devam ederken, siber tehditleri ve siber saldırıları analiz etmek ve geliştirmek çok zor olmaya başladı.

Yapay zekâ araçları ve yöntemleri, hassas bilgileri korumada, ihlal riskini azaltmada ve daha etkili ve verimli tehdit algılama ve tehdit kaldırma özellikleriyle güvenlik önlemlerini iyileştirmede yardımcı olmak için gelişti.

Ek olarak, tehdit algılama, kullanıcı davranışlarını analiz edip sınıflandırarak iyi ve kötü hareketliliği birbirinden ayırabilme, birbiriyle alakasız gibi görünen saldırı özelliklerini yorumlayıp kurallara göre alarm üretme gibi çeşitli kritik işlevlere sahip olan siber güvenlik odaklı yapay zekâ uygulamaları siber savunma ekiplerinin işini kolaylaştırıyor.

Otonom güvenlik sistemleri yeni nesil savunma teknolojisi olarak görülmektedir. Bunun sebebi riskleri algılayıp alarm üretmek ve tehditleri saptamaktan daha fazlasını yapabiliyor olmasıdır. Mesela tehditleri saptadıktan sonra müdahâleye gerek duymadan kendi kontrol altına alabilmektedir.

Güvenlik ve Suç Önleme

Yapay Zekâ Güvenlik ve Suç Önleme alanında büyük kolaylık sağlıyor. Örneğin: Bilgisayar İstatistikleri (CompStat) AI sistemi, 1995'ten beri New York polis departmanı tarafından kullanılmaktadır. CompStat, organizasyon yönetimi ve felsefesini içeren, ancak farklı yazılım araçlarına dayanan bir yapay zekâ biçimidir. Sistem, "tahmini polislik" için kullanılan ilk araçtı ve ABD'deki birçok polis karakolu, o zamandan beri suçları araştırmak için CompStat'ı kullanıyor. Kaliforniya merkezli Armorway gibi yapay zekâ tabanlı suç analizi araçları, terörist tehditleri tahmin etmek için yapay zekâ ve oyun teorisini kullanıyor. Sahil Güvenlik ayrıca Los Angeles, Boston ve New York'ta liman güvenliği için Armorway'i kullanıyor.

KAYNAKÇA:

<https://www.semanticscholar.org/paper/Model-Aided-Deep-Learning-Method-for-Path-Loss-in-Throne-Zibar/3a7777aeebc8caa7a5298ad0dee5871aba23c1d6>

<https://cihanozhan.medium.com/yapay-zekâ-g%C3%BCvenli%C4%9Fi-giri%C5%9F-599e4b691068>

<https://thecyphere.com/blog/ai-in-cyber-security/#:~:text=AI%20works%20in%20cyber%20security,cyber%20threats%20in%20quicker%20timescales.>

<https://www.kaspersky.com.tr/resource-center/definitions/ai-cybersecurity>

<https://www.yapayzekâtr.com/2021/08/04/siber-guvenlikte-yapay-zekâ-uygulamaları/>

<https://bilginc.com/tr/blog/siber-guvenlikte-yapay-zekâ-ai-uygulamaları-273/>





DÜNYA TARİHİNDE SES GETİREN HACKERLAR VE YAPTIKLARI SALDIRILAR



Martin Gottesfeld

FBI'nin Anonymous denen hacker topluluğunun en önemli hacker'ı olarak nitelendirdiği Gottesfeld 2014 yılında Boston Çocuk Hastanesinin hack'lenmesiyle ilgili olarak suçlandı. Gottesfeld hastaneyi hedef aldığını kabul etti, ancak bunu masum, öğrenme güçlüğü çeken, 15 yaşındaki bir kızı savunmak için yaptığını söyledi.

Yapmış olduğu bu saldırı dava kapsamında savcılar; hastaneye yönelik DDoS saldırısının yedi gün sürdüğünü ve kurumun günlük operasyonlarını ve hastanede yapılan

araştırmaları aksattığını iddia ediyor. Yaklaşık 40 bin kötü amaçlı yazılım bulaşmış yönlendiricinin kullanıldığı saldırıda sadece Boston Çocuk Hastanesi değil diğer hastanelerin de zarar gördüğü iddialar arasındadır.

Bu iddialar neticesinde FBI tarafından yakalanan hacker ABD Bölge Yargıcı Nathaniel Gorton tarafından 10 yıl hapse mahkum edildi. Hapis cezasının dışında verdiği zararlardan dolayı 443 bin dolar tazminat ödemesine hükmedildi.

Yargıç Gorton, dava sırasında "Kusura bakmayın, suçunuz aşağılık, alçakça ve iğrençti," dedi.

Hacker bu dava sonrasında açlık grevine girdi. Savunmasının arkasında duran Gottesfeld açlık grevine iki talep karşılanana kadar devam edeceğini söyledi. Başkan adaylarından, çocukların Pelletier'in iddia ettiği şekilde kötü muamele görmeyeceklerine dair söz ve Massachusetts'in ABD'li avukatı Carmen Ortiz tarafından yürütülen "siyasi" kovuşturma tarzına son verilmesi taleplerinde bulundu.



Gary McKinnon (UFO-Hackerı)

McKinnon, 2002 yılında ABD tarafından "askerî bilgisayarlara yapılan en büyük saldırı" kapsamında suçlanmıştır. Yaptığı internet saldırıları kendisinin UFO'lara olan ilgisinden kaynaklanır.

McKinnon, New Jersey ve Kuzey Virginia'da, sivil ve ABD deniz veri tabanları da dâhil olmak üzere 14 eyalette 97 bilgisayara yasadışı yollardan girerek 700.000 dolarlık hasara neden olmak ve askerî tedarik hatlarını bozmakla suçlanmıştır.

McKinnon, kendisini serbest enerji teorisini kanıtlamak amacıyla savunmuştur. 2000-2002 yılları arasında NASA'nın ve ABD Silahlı Kuvvetleri'nin bilgisayar ağla-

rında bu konu hakkında kanıt aramıştır. Bu sebeple medyada “UFO-Hackeri” olarak tanımlanmaktadır. UFO’lar hakkında bilgi aradığını ve zarar vermek istemediğini belirtip “Niyetim asla güvenliği bozmak değildi. Oturum açmış olmam ve şifre olmaması, güvenliğin olmadığı anlamına geliyor.” diyerek savunmada bulundu. Hatta yaptığı eylemin hack’lediği bilgisayar sistemleriyle ilgili sorunları ortaya çıkardığı için kendisine teşekkür edilmesi gerektiğini söyledi.

McKinnon’a son yıllarda bir otizm türü olan Asperger sendromu teşhisi kondu ve destekçileri, durumunun suç davranışını kısmen açıkladığını savundu.

İngiltere İçişleri Bakanı Theresa May, ABD’nin iade talebini, McKinnon’un Asperger hastalığı ve depresyonunun ABD hapisanesine gönderilmesi hâlinde kendisi için bir risk oluşturacağını söyleyerek insan hakları gerekçesiyle iptal etti. “İlgili tüm materyalleri dikkatlice inceledikten sonra, Bay McKinnon’un iade edilmesinin, yaşamını sona erdirmesi konusunda yüksek bir riske yol açacağı ve iade kararının Bay McKinnon’un insan haklarıyla bağdaşmayacağı sonucuna vardım.” dedi.



Robert Tappan Morris

Bilgisayar dünyasının ilk solucan virüsü olarak bilinen ‘Morris solucanı’nın yaratıcısı olan Morris, bu virüsü “internet dünyasının ne kadar büyük olduğunu test etmek için” yazdığını iddia etmiş olsa da 1988 yılında yani daha net ifadeyle 50.000 bilgisayarın internet erişimi bulunan dönemde yarattığı virüsü 6000 bilgisayara yaymayı başarmıştı.

Bu iddiası onu aklamaya yeterli gelmeyerek o zamanlar yeni olan Bilgisayar Sahtekârlığı ve Kötüye Kullanımı Yasası (CFAA) kapsamında ilk ceza alan hacker olmuştur. Yarattığı bu virüs ona 3 yıl hapis, 400 saat sosyal hizmet görevi ve 10.500\$’a mal olmuştur.



Matthew Bevan & Richard Price

İngiliz asıllı iki hacker Amerikan ordusunun Griffiss Hava Kuvvetleri Üssü’ne ait araştırma laboratuvarına saldırarak bilgisayarlarına sızmayı başarmıştır. Bu saldırılar sonucunda bazı savaş simülasyonlarını ele geçirmişlerdir. Tabii bu kadarla sınırlı kalmayarak bazı ABD ajanları arasındaki mesajları da ele geçirerek bunları Kuzey Kore’ye satmışlardır. Bu olay tarihte

iki devleti karşı karşıya getiren ve savaşın eşiğinden döndüren olay olarak nitelendirilmektedir.



Jonathan James

James dünyada yargılanan ve hüküm giyen ilk 18 yaş altı hacker olma özelliğine sahiptir. James, ABD Savunma Bakanlığındaki bilgisayarlardan birine bir arka kapı (backdoor) programı yerleştirerek, NASA bilgisayarlarından 1.7 milyon dolarlık yazılımı çalmıştır. James Uluslararası Uzay İstasyonu'nun nem ve sıcaklık değerlerini değiştirmesiyle kendisini ele vermiştir. 18 yaşının altında olduğu için 6 ay ev hapsi cezası alan James, ev hapsi kurallarına uymadığı için Alabama'ya askerî hizmete gönderilmiş ve burada 6 ay hizmette bulunmuştur.

2007 yılında TJX mağazasının hack'lenmesi olayında şüpheliler arasında olan James bu suçla ilgisi olmadığını şöyle ifade etmiştir; “Benim gerçekten TJX olayı ile ilgili hiçbir ilgim yok. ABD adalet sistemine tüm inancımı kaybettim, belki şu anki hareketim ve mektubum halka kuvvetli bir mesaj olacaktır. Her hâlukarda ben bu durum üzerindeki kontrolümü kaybettim ve bu benim tekrar kontrolü kazanmamın tek yolu.” Bu sözlerinin ardından intihar ederek yaşamına son vermiştir.



Adrian Lamo (Evsiz hacker)

Lamo, internet kafeleri, kütüphaneleri ve kafeleri kullanarak hack girişimlerini bu mekanlarda yapmasıyla camia-da “Evsiz hacker” olarak adını duyurmuştur.

Lamo'nun en bilinen hack işlemi New York Times ve Microsoft'un sistemlerine girmeyi başarmış olmasıdır. Aynı zamanda Yahoo!, Bank of America, Citigroup ve Cingular sistemlerine de girmiş olduğu ihtimallerini üzerinde durulmuştur. Lamo, 2010 yılında Amerika askerî yetkililerine Amerikan askerî Bradley Manning'in Wikileaks'e bilgi sızdığını ihbar etmiştir. Bu suçlar sonucunda altı ay ev hapsi, 2 yıl bilgisayardan uzak durma ve 65.000\$ para cezası verilmiştir.



Barnaby Jack

Jack 2018 yılında 2 ATM satın almış, bunların yazılımlarını inceleyerek zayıf noktalarını tespit etmiş, bu zayıflıkları nasıl manipüle edebileceği üzerinde çalışmalar yapmıştır. İnsanların banka hesap numaralarına ulaşarak şifrelerini çalmak gibi birçok konu üzerinde çalışmıştır.

2010 yılında Las Vegas'ta düzenlenen Jeff Moss'un girişimiyle başlatılan Black Hat Briefings adlı bilgi güvenliğiyle ilgilenenlerin bir araya geldiği konferansa katılmıştır. Konferansta sahneye çıkarak sadece bir telefon modemi

aracılığıyla ATM'ye bağlanarak şifre dahi kullanmadan bütün parayı çekmiştir. Ardından "Buradaki amacım insanlara bir modem vasıtasıyla ATM'lere sızıp nasıl para çalacaklarını göstermek değil. Amacım, ATM sistemlerinde bulunan açıkların nelere yol açabileceğini göstermek ve bu açıklıkların kapatılması için gereken önlemlerin alınmasını sağlamak." diyerek bu işlemin aslında ne kadar tehlikeli bir hâl alabileceğini herkese göstermiştir. Ses getiren bu gösterisi bilgisayar teknolojisine "Jackpotting" olarak geçmiştir.



Onel de Guzman

2000 yılında Filipinler'deki çevirmeli bağlantının dakika başı ücretlendiriliyor olması Guzman'ın bütçesine yetmiyordu. Bu yüzden internet erişim parolalarını çalmaya yönelik kod yazan Guzman kullanıcılara konu satırında "ILOVEYOU" yazan bir eposta gönderiyordu. İçerisinde "LOVE-LETTER-FOR-YOU.txt.vbs" dosyasıyla gelen e-posta bu dosyayı açanların şifrelerini alıyor ve tüm dosyalarının üzerine yazılıyordu. Ardından kendisini kurbanın adres defterindeki kişilere gönderiyordu. Bu virüs kısa sürede dünya çapında yayılarak birçok insanın şifresinin deşifre olmasına neden oldu.

**MERYEM
ARPACI**

**KONU
56**





PAROLA SALDIRILARI

Teknolojinin hızlı gelişimiyle sanal ortamdaki gizliliğimiz en az gerçek hayattaki gizliliğimiz kadar önem kazanmıştır. Sanal ortamdaki gizliliğimizi sağlayabilmek için bir anahtar görevini üstlenen parola kavramı ortaya çıkmıştır.

Parolalar, bir sisteme giriş yapabilmek için belirlediğimiz gizli anahtarlardır. Parolalı sistemlere sadece anahtarı bilen kişiler erişim sağlayabilir, bu nedenle gizliliğimizi korur. Parola kavramı sık sık şifre ile karıştırılan bir kavramdır.



Şifre bir verinin üçüncü şahıslar tarafından okunabilmesinin önüne geçmek için o veriyi karmaşıklığa kavuşturmayı denir. Şifreleme (encryption) ile verilerimiz veri tabanında gizli bir biçimde tutulur. Bu sayede o veri tabanına erişen bir internet korsanının bu şifrelemeyi çözmeden verileri okuyabilmesi imkânsız hâle gelir.

Gerçek hayatta hırsız diye nitelendirdiğimiz kişilerin sanal dünyadaki karşılığı internet korsanıdır. Bu kötü niyetli kişiler çoğu zaman farkında olmasak da bize sanal dünyada saldırmaktadır. Burada saldırı kavramı gerçek hayattaki anlamına yakın kullanılsa da sanal saldırılar biraz farklıdır. Bir kişi veya kurumun bazı sistem zafiyetleri veya zararlı yazılımlar vasıtasıyla kişisel verilerinin çalınmasına siber saldırı denir.

Siber saldırıların birçok çeşidi vardır. Bunlardan biri de parola saldırılarıdır. Parola saldırıları, internet korsanlarının çeşitli verilerin parolasını ele geçirebilmek için yaptığı saldırılara denir. Bu saldırıların amacı sosyal medya hesaplarını ele geçirebilmek, kişisel veya kurumsal bazı verilere erişebilmek, banka hesabı parolaları gibi bazı önemli parolaları ele geçirebilmek olabilir. Bu nedenle oldukça önemli ve dikkat edilmesi gereken bir konudur.

Parola Saldırıları Çeşitleri

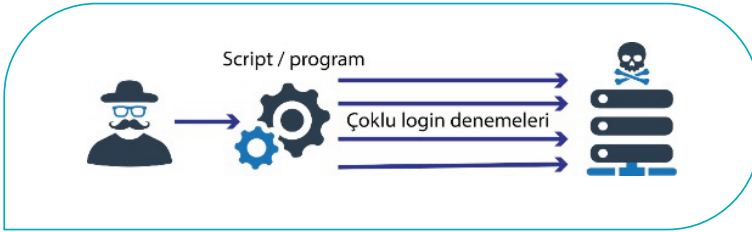
1 - Oltalama (Phishing)

Kurban olarak belirlenen kişilere, kişisel verileri çalmayı hedef alan e-posta gönderilmesine oltalama (phishing) saldırıları denir. İsminden de anlaşılacağı üzere hazırlanan e-posta ne kadar çok kişiye gönderilirse, kurbanların bu ağa yakalanma ihtimali de artar. İnternette gezerken karşımıza çıkan “Dikkat, telefonunuzda virüs var! Hemen bu programı indirip telefonunuzu virüslerden koruyun!” gibi kapatılmamakta ısrar eden reklamlar, kendini resmi bir kurum gibi tanıtır sizden bazı veri taleplerinde bulunan siteler sık sık karşılaştığımız oltalama (phishing) saldırılarıdır. Örnek olarak saldırgan, size yönelttiği linkte kurumsal bir link izlenimi oluşturabilmek için ilk bakışta göze çarpmayan değişiklikler yapıp (instagram.hellpcentre, help.twitterr gibi) hesabınızın çalınmış olabileceğini, yönlendirdiği link ile hesabınızı güvene alabileceğinizi söyler ve sizi parolanızı talep eden bir form veya özel hazırlanmış bir siteye yönlendirir. Parolanızı girmeniz durumunda saldırgan hesabınıza erişim sağlar. Parolanızı değiştirip kendi e-postasını hesabınıza ekleyerek sizin hesabınıza erişebilmenizi engeller. Bu durumun yaşanmaması için muhakkak iki faktörlü kimlik doğrulamasını aktif etmeli, size gönderilen her linke tıklamamalısınız.

2 - Kaba Kuvvet (Brute Force)

Parolanın deneme yanılma yöntemiyle bir wordlist (metin belgesi) ve saldırı aracı kullanılarak kırılmasıdır. Wordlist içerisine olası parolalar yazılır. Genellikle kişiye özel wordlist hazırlanır. Bu aşamada kurban hakkında toplanan bilgilerden yararlanılır. (Kurbanın doğum tarihi, ilgi alanları, varsa evcil hayvanının adı, tuttuğu takım). Ek olarak wordlist içerisine sık kullanılan şifreler de eklenir (12345, abcde, sanane, qwerty, Galatasaray). Şifreleriniz eğer bunlardan biriye acil olarak değiştirmeniz gerekmektedir.

Bir diğer önemli husus ise parolanızın karmaşıklığı. Brute force saldırıları ile parolanın kırılabilme süresi, parolanın karmaşıklığına göre değişir. Örneğin parolanız 12345, 19055091 gibi şifreler ise kırılması anlık; mE@y#M&ş!eRw?n13 gibi bir şifre ise kırılması 29 trilyon yıl sürer. Bu nedenle parolanızın içerisinde büyük-küçük harf, rakam ve özel karakterlerin bulunması parolanızın kırılabilme olasılığını minimuma düşürür.



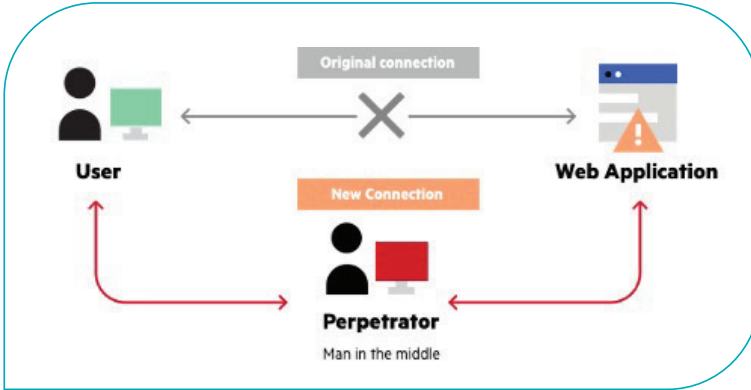
3 - Keylogger (Tuş Kaydedici)

Keylogger, bir çeşit zararlı yazılımdır. Cihazınıza bulaştığı andan itibaren bütün klavye hareketlerinizi kaydedip saldırgana iletir.

Herhangi bir platforma parolanızı kullanarak giriş yapmanız halinde saldırgan parolanızı öğrenmiş olur. Bu tarz zararlı yazılımlar birçok yerden bulaşabilir. Cihaza güvenilir olmayan yerlerden dosya yüklemek (pdf, mp3, jpg-jpeg, apk, mp4, zip ...), halka açık yerlerdeki parola korumasız wi-fi ağlarına bağlanmak, özel hazırlanmış bazı linklere tıklamak cihazınıza keylogger bulaşmasına sebep olabilir.

4 - Man in the Middle

Bu saldırı tipi Türkçe çevirisinden de anlaşılabilceği üzere (ortadaki adam) saldırganın kurbanın bağlantı isteği attığı sunucu ile kurbanın arasına girerek bağlantıyı üzerinden yönlelmesidir. Bu sayede aradaki iletişimi dinleyerek parolalarınızı ele geçirebilir. Bu saldırıdan korunmanın bazı yolları vardır. Bunlardan biri VPN (sanal özel ağ) kullanmaktır. VPN, web trafiğini şifreleyerek saldırganın ağı okumasını zorlaştırır. Bir diğer yol 2FA (two factor authentication) yani iki faktörlü kimlik doğrulaması kullanmaktır. 2FA parola korumanıza ek bir koruma daha sağladığından iyi bir korunma yöntemidir.



5 - Sosyal Mühendislik

İnsanların manipölasyon yoluyla bilgilerinin çalınmasına sosyal mühendislik denir. Sosyal mühendislik, bir nevi insan kandırma sanatıdır (bir diğer adıyla insan korsanlığı). Saldırgan, kurbanın kendini güvende hissetmesini sağlayarak istediği şeyleri yapmaya ikna eder. Bu noktada kurbanın nasıl düşündüğünün ve nelerden hoşlandığının bilinmesi önemlidir. Bu sebeple saldırgan kurbanı analiz ederek kurban hakkında genel bir profil oluşturur ve ona yönelik saldırılar yapar.

Mesela sosyal medya hesaplarında bir spor kulübüne ait çok sayıda hesapla etkileşimde bulunan fanatik birine karşı saldırgan, o spor kulübüyle yakından ilişkiliymiş gibi kurbanın ilgisini çekebilecek davranışlar sergilerse saldırının başarı oranı çok daha yüksek olur. Günümüzdeki siber saldırıların neredeyse tümünde sosyal mühendislikten yararlanılır. Bu terimi ortaya çıkaran ve bilgisayar tarihinin en eski korsanı olarak bilinen Kevin Mitnick, giriş yaptığı sistemlerin %80'ine sosyal mühendislik yoluyla girdiğini belirtmiştir. Bu nedenle bu tarz manipölasyonlara karşı dikkatli olmamız gerekmektedir.

KAYNAKÇA

<https://www.passwordmonster.com/>
<https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>
<https://www.altosec.com/blog-parolasaldirilari.html>
<https://berqnet.com/blog/sosyal-muhendislik-saldirilari>





WEB SHELL

Shell

Shell (kabuk), bilgisayar dünyasında işletim sistemi ile kullanıcı arasındaki arayüzdür. İşletim sisteminin bir parçası olmayan ancak işletim sisteminin gerekli aksiyonları (program çalıştırma, dosya açma vb.) alması için kullanılan bu katman komut yorumlayıcısı olarak da adlandırılabilir.

Siber dünyada shell dosyaları da kötü amaçlı kişilerin kurban sistemlere uzaktan erişimine izin veren zararlı bir komut dosyasıdır. Saldırganlar sistemleri ele geçirip buralarda kalıcılığı sağlamak için shelleri sık olarak tercih etmektedir. Yazımızda sık tercih edilen türü olan webshellere değineceğiz.

Web Shell Nedir, Türleri Nelerdir?

Web shell, siber saldırılarda web sunucusuna uzaktan bağlanabilen ve erişimi olan herhangi programlama dili ile yazılmış kötü amaçlı kod bloklarıdır.

Bind Shell

Saldırgan hedef cihaza zararlı kod göndererek bir iletişim kanalı (port, dinleyici) oluşturur. Oluşturulan bu port veya dinleyici ile saldırı hedefe bağlanıp hedef üzerinde komutları çalıştırabilir. Bu shell (kabuk) açıklıklarından biri port'un dinlediğini gören herkesin bind shell'e bağlanıp bu işlemi yapabilmesidir, en basit çözümü ise şifre koruması eklemektir.

Bind shell kullanılan saldırılar hedef bilgisayarda işlem yapmak üzerine olduğundan dosya ekleme, silme, bozma gibi işlemler yapılabilir. Örneğin bind shell saldırısı ile bir personel dosyası eklenip sosyal mühendislik de kullanılarak firmaya yönelik büyük bir saldırı yapılabilir ya da önemli dosyalar silinerek firmanın verileri, projeleri ve tasarımları yok edilerek uzun dönemli çalışmalarına zarar verilebilir.

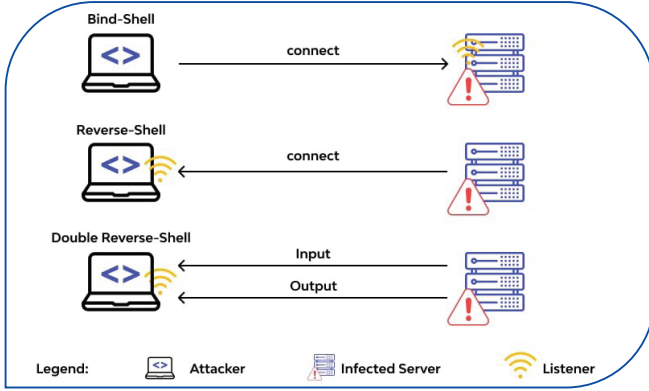
Reverse Shell

Bu shell türünde, normalden farklı olarak kurban makine saldırı makinesinin dinlediği bir porta yayın yaparak saldırı ile iletişim kurar. Saldırgan sunucular çoğunlukla belirli portlardan iletişim isteğini kabul eder ancak sunucu istediği porta istek gönderebilir. Reverse shell bu gibi durumlarda saldırı ve hedef arasında iletişim kurmak için kullanılır.

Bu shell türünde bind shell'in aksine saldırı dinleyici olduğundan diğer saldırıların hedef makineyi dinleyici olarak kullanması önlenir. Hedefin bağlanabileceği yaygın portların kullanımı ile bağlantıda güvenlik duvarı engeli ortadan kaldırılıyor. Reverse shell kullanılarak yapılan saldırılar genel anlamda bilgi almak için yapılır. Örneğin, bir bankanın sunucusuna reverse shell ile bir saldırı yapıldığında kullanıcıların bilgileri, yaptıkları işlemlerin bilgileri saldırıların eline geçer.

Double Reverse Shell

Reverse shell'e benzer şekilde ancak hedef cihazdan saldırgan cihaza "input" ve "output" olarak iki port ile bağlanarak çalışır.



Web Shell'lerin Tespiti ve Korunma Yolları

Web shell saldırılarından korunmak için hedef cihazlardaki dinleyicilerin düzenli kontrolü yapıp sadece gerekli ve güvenli portlar dinleyici olarak kullanılıp diğer portlar güvenlik duvarı tarafından korunabilir. Kontroller ile sunucuda olmaması gereken dosyalar bulunabilir, güvenlik uygulamaları ile web kabukları tespit edilebilir, İnternet Bilgi Servisleri (ISS) tarafından yaratılan işlemlere bakılarak alarm verilen şüpheli senaryolar incelenerek web kabuğu saldırıları tespit edilebilir.

Web shell saldırılarından korunmak için düzenli güvenlik yamaları yapıp güvenlik duvarları kullanılarak saldırganların ulaşması zorlaştırılabilir. Ağ sistemleri ayrıştırılarak saldırıya uğrama durumunda saldırının tüm sisteme ulaşması engellenebilir. Sisteme erişim için her zaman kimlik doğrulama istenilerek bağlantı kurulması sağlanabilir. Bu şekilde şüpheli kişilerin sisteme bağlanıp web shell atılmasının önüne geçilmiş oluruz. Şüpheli bir bağlantı keşfedildiği zaman sistem resetlenerek bağlantı kesilerek saldırı anlık olarak durdurulabilir.

KAYNAKÇA

<https://www.youtube.com/watch?v=bU4mOpmuH8Q>

<https://securityboulevard.com/2019/08/what-is-a-reverse-shell/>

<https://www.geeksforgeeks.org/what-are-webshells/>

<https://www.invecti.com/blog/web-security/how-web-shells-work/>

https://medium.com/@PenTest_duck/bind-vs-reverse-vs-encrypted-shells-what-should-you-use-6e-ad1d947aa9

<https://www.wallarm.com/what/what-is-a-web-shell-attack-how-to-detect-and-prevent-it>

<https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/instructions-how-detect-webshells#:~:text=The%20simplest%20way%20to%20detect,that%20should%20not%20be%20there,>

<https://www.ssl2buy.com/cybersecurity/web-shell-attacks>





DÜNYADAKİ SİBER SALDIRILAR VE ÜLKELERİN ALDIĞI ÖNLEMLER

DÜNYADAKİ SİBER SALDIRILAR VE ÜLKELERİN ALDIĞI ÖNLEMLER

Geçmişte uygulanan güvenlik tedbirleri teknolojinin gelişmesiyle, yerini modern güvenlik uygulamalarına bırakmıştır. Dış dünyaya açık olan teknolojik cihazların ve kullanılan ağların korunması siber güvenlik alanını oluşturmaktadır. Siber güvenlik, teknolojinin gelişmesiyle daha da önem kazanmıştır.

Siber güvenlik, siber uzayı oluşturan bilgi teknolojileri sistemlerinin tehditlerden korunmasını, buradaki bilginin gizlilik, bütünlük ve erişilebilirliğinin güvenli bir şekilde sağlanmasını, saldırı ve siber durumların belirlenmesini, bu belirlemelere yönelik önlemlerin alınmasını ve sonrasında ise sistemlerde karşılaşılan sorunların saldırı öncesine geri getirilmesi olarak ifade edilmektedir.

Siber uzay, (orijinal anlamını karşılamasa da yaygın olan bir başka kullanımıyla sanal alem, cyberspace) terimi bilgisayarların ve onu kullanan insanların internet ve benzeri ağlar içinde kurduğu iletişimden doğan sanal gerçeklik ortamını anlatan metaforik bir soyutlamadır. Siber uzay kavramı Türkçede zaman zaman “siber ortam” olarak da kullanılmaktadır. Siber saldırılar, bir iş veya kişisel bilgisayar ağı içindeki önemli belgelere ve sistemlere zarar vermeyi veya bunların kontrolünü ele geçirmeyi ya da bunlara erişim sağlamayı amaçlar.

Bu saldırıların başlangıcı olarak bilinen 1988 yılında saldırının gerçekleştirilme nedeni merak ve eğlenceyken, günümüze gelindiğinde ise saldırıların motivasyonunda ciddi değişimler olduğu görülmektedir. Siber saldırılar önceleri kendini ispat etme, heyecan yaratma, karşı tarafı cezalandırma, zarar verme, vb daha masum gerekçeler ile yapılırken, daha sonra veri hırsızlığı, ticari kazanç sağlama, menfaat temin etme, ülkeleri cezalandırma gibi daha profesyonel ve kötü-cül amaçlarla yapılmaya başlanmıştır.

Mali Motivasyonlar: Tehdit aktörleri doğrudan ve dolaylı olarak maddi kazanç sağlamak isteyebilirler. Sektörel rakipler kurumunuza zarar vermek isteyebilir ve bunu yapmak için maddi zarar vermek isteyebilir.

İdeolojik Motivasyonlar: Müşterilerinize karşı olan itibarınızı kaybetmenizi, hizmet verme kalitesinin düşmesini isteyen düşmanlarınız bulunabilir. Bunlar dışarıdan gelen tehditler olmak zorunda değildir. Kurum içerisinde mutsuz bir çalışan ve kurumla sıkıntı yaşamış eski bir çalışan da aynı motivasyonu paylaşabilir.

Siyasi Motivasyonlar: Devlet destekli saldırıların arkasında siyasi motivasyonların bulunması ihtimali çok yüksektir. Büyük çapta yapılan ve geniş bir kaynak kapasitesine sahip olan saldırıların çoğunluğu bu motivasyonu paylaşır.

Prestij ve Merak Motivasyonu: Kendilerini kanıtlama güdüsü hisseden tehdit aktörleri prestij kazanmak ve isimlerini duyurmak için saldırı eylemleri gerçekleştirebilir. Bu motivasyonu paylaşan kişilerin amaçları kötü yönde eğilim göstermek zorunda değildir. Örneğin kurumların sistemlerinde açık bulup bunları bildiren, olası büyük kayıpların önüne geçmek için bu işi yapan ve karşılığında ödül alan aktörler vardır.

Uluslararası İlişkiler Açısından Siber Güvenlik

Günümüzde siber saldırı gibi tüm entegre sistemlere zarar verebilecek tehditler büyük bir sorun hâline gelmiştir. Dolayısıyla daha kapsamlı bir kurumsal boyutun yanı sıra toplumsal, ulusal ve uluslararası boyutlara ulaşmıştır. Ciddi bir artış gösteren siber tehdit ve saldırılar, birçok ülkenin bu alanda güvenlik stratejileri geliştirmesini sağlamıştır. Özel kurumlar siber güvenlik hakkında görüşlerini aldıkları özel BT uzmanlarını bünyelerine katma ve yetiştirme ihtiyacı duymaktadırlar. Resmî ve özel firmalarca, siber saldırılara karşı büyük yatırımlar yapılmaktadır.

Siber güvenliğin devletlerarası ilişkiler açısından önemli rol oynadığına dair birçok veri mevcuttur. Siber güvenlik sorunlarının uluslararası ilişkiler boyutunda ciddi oranda artması sonucu devletler "siber politikalar" adıyla çalışmalar yapmaktadır. Değişen dünya açısından çıkar mücadelesinin ön planda olduğu, siber güvenlik ve temelindeki araçlarla siber saldırılara karşı, devletler siber saldırının nereden geldiği ile ilgili tespitler yapabilmekte ve bu durum uluslararası sistemi olumsuz etkilemektedir. Siber tehditlerin varlığı ve olası siber saldırılar devletleri sıcak çatışmalara sürükleyecek hâle gelmiştir.

Siber güvenliğin sağlanması ve siber savaşla mücadele, yalnızca devletlerin çabalarıyla mümkün değildir. Devlet ve devlet dışı birçok kurum, kuruluşların küreselleşen dünyada topyekûn hareket ettiği görülmektedir. Avrupa Konseyi tarafından imzalanan ve 2004'te yürürlüğe giren Budapeşte Konvansiyonu ilk sözleşme ve bu sözleşmeyi ifade eden Şubat 2005'teki AB'nin 2005/222 / JHA hükmü buna örnektir.. Hüküm daha sonra 14 Ağustos 2013 tarihinde Bilgi Sistemlerine Saldırı Yönergesi olarak değiştirmiştir. İmzalanan bu anlaşma aynı zamanda AB için siber sahada yapılan ilk anlaşmadır.

Yakın Süreçteki Siber Saldırıları

Siber saldırıya uğrayan FBI'n e-posta sistemi hacklendi

ABD Federal Soruşturma Bürosu'nun (FBI) e-posta sistemine sızan bilgisayar korsanları, on binlerce kişiye 'olası siber saldırılara karşı uyarı' mesajı gönderdi.

Sisteme sızıldığı, FBI ve diğer güvenlik uzmanları tarafından doğrulandı.

Federal Soruşturma Bürosu'ndan yapılan açıklamada, sahte maillerin @ic.fbi.gov ile biten gerçek bir FBI e-posta adresinden gönderildiği belirtildi.

Siber saldırıdan etkilenen donanımın 'sorunun anlaşılmasından hemen sonra ivedilikle çevrim dışı moda alınmasına rağmen bunun devam eden bir durum' olduğu ve daha fazla detay verilemeyeceği bilgisi paylaşıldı.

E-posta spam göndericilerini ve spam ile ilgili etkinlikleri izleyen Cenevre merkezli sanal tehdit takip kuruluşu Spamhaus Project'in Twitter hesabından yapılan açıklamada, bilgisayar korsanlarının "olası bir siber saldırıya karşı on binlerce e-posta gönderdiği" belirtildi.



Gizli bilgiler, telefon konuşmaları: Belaruslu hackerlar Lukaşenko yönetiminin kayıtlarını yayınladı

Belarus'ta Devlet Başkanı Aleksander Lukaşenko'nun sürdürdüğü baskı rejimine karşı mücadele eden ve kendini siber aktiviste olarak tanıtan bir grup hacker, hükûmetin ve istihbaratın en hassas verilerini ele geçirmeyi başardı. "Belarus Siber Partizanları" olarak tanınan hacker grubu, amacının "Belaruslu yetkililer tarafından işlenen suçların kanıtlarını yayınlamak" olarak tanımlanarak 1994'ten beri ülkenin başındaki Lukaşenko rejimini zayıflatmak olduğunu söylüyor. Euronews'e konuşan grup, temmuz ayında hükûmetin bilgisayarlarına sızarak beş terabayttan fazla veri elde ettiğini ve şimdiye kadar çalınan verilerin yüzde 0,01'ini bile yayınlamadığını söyledi. Zaman içinde hackerler, Lukaşenko'nun ülkedeki muhalefeti ezmesine yardım eden her bir kişi hakkındaki bilgileri paylaşmayı planladıklarını belirtti.



Paylaşılan dosyalarda neler var?

Hackerlar, ülkenin en gizli bilgilerinin bazı bölümlerini yayınladılar. Söz konusu belgelerde, polis muhbirlerinin listeleri, üst düzey hükümet yetkilileri ve casuslar hakkında kişisel bilgiler bulunuyor.

Son 10 yıl içinde yakın çevremizdeki ülkelerden Estonya, Ukrayna, İran'a da ülkelerarası saldırılar yapılmış ve bu ülkelerdeki farklı sistemlere ve ekonomilerine ciddi zararlar verilmiştir. 2008 yılında Rusya ile Gürcistan arasında yaşanan savaşta Rusya'ya ait siber alandan Gürcistan'a yapılan siber saldırı da bu duruma örnek gösterilebilir. Rusya, Gürcistan'a yönelik siber saldırılarda herhangi bir katkısı olmadığını iddia etse de, bu saldırıların Rusya'nın bilgisi dâhilinde devlet destekli olarak mı, yoksa bu ülkede bulunan terör örgütleri tarafından mı gerçekleştirildiği kesinlik kazanmamıştır.

Siber saldırıların güncel örneklerinden biri de 2007 yılında Estonya'ya düzenlenen yüksek yoğunluklu saldırılardır. Estonya'ya düzenlenen bu yoğun siber saldırıların başlangıç noktasını ülkede yaşayan Rus kökenli azınlıklarla Estonyalılar arasındaki sorun meydana getirmiştir. Geçmişten gelen anlaşmazlığa 2007 yılının Nisan ayında ortaya çıkan sorunlar da eklenince, ülke yoğun bir siber saldırı tehdidi altına girmiştir. Bu süreçte Estonya hükûmetine ve ulusal medyaya ait sitelere yoğun DDoS saldırıları yapılmış ve bazı siteler kullanılamaz hâle getirilmiştir.

Siber Güvenlik ile İlgili Ülke Bazında Alınabilecek Önlemler

Sistem Mimarilerinin Rehabilite Edilmesi

Siber Güvenlik Eğitimindeki Boşlukların Giderilmesi

Millî Yazılım ve Donanımların Geliştirilmesi

Şebekelerimizde Kullanılan Yabancı Ürünlerin Yol Açabileceği Tehditlerin Giderilmesi

Milli Savunma Kalkanının Tesis Edilmesi

Gizlilik Artırıcı Teknolojilerin Etkin Kullanımı

Casus Yazılım Tespiti ve Sistemlerden Silme

Açıklık Tarayıcılar

Saldırı veya Misilleme Tedbirlerinin Alınması

Ülkelerin Siber Güvenlik Stratejileri

ABD

ABD, siber güvenlik, siber uzay konularında diğer ülkelere önder konumdadır. Özellikle Avrupa ve Asya'daki ülkelere siber sorunlarla mücadele konusunda rol model durumuna gelmiştir. 11 Eylül 2001'deki ABD'deki saldırıların ardından siber güvenlik ve kritik bilgi altyapılarının korunması alanlarında çeşitli değişiklikler yapılmıştır. Siber güvenliğin sağlanması için DHS bünyesinde Altyapı Koruması (OIP) ve Siber Güvenlik ve İletişim Departmanı (CS&C) kurulmuştur. OIP, mevcut altyapıların korunması konusundaki çalışmalarını koordine etmekten, mevcut altyapı sektörlerindeki güvenlik açığı değerlendirmesine yönelik çalışmaları desteklemekten ve uluslararası güvenlik kültürünün oluşturulmasını teşvik eden uluslararası programlar ilişkiler kurmak ve sürdürmekten ve ayrıca kritik altyapıların korunmasından sorumludur. Öte yandan CS&C, siber tehditler, risk yönetimi, acil durumlarda iletişim ve müdahâle merkezlerinin kurulması gibi konularda özel sektör ile işbirliği kurmaya yetkilidir.

ALMANYA

Almanya siber güvenlik yarışına ABD'den daha sonra başlamıştır. 2011 yılında ilk ulusal siber güvenlik stratejisini oluşturmuş, o yıldan sonra büyük ve hızlı bir gelişme göstermiştir. Almanya 2015 yılında siber güvenlikle ilgili stratejisini günün şartlarına göre revize etmiştir. Bu hedefle Almanya, kritik bilgi sistemi altyapılarının korunmasına önem verir hale gelmiştir. Ek olarak, internet kullanımının her geçen gün artması ve yayılmasıyla, sadece her ülkenin kendi sistemlerinde değil diğer ülkelerin sistemlerindeki saldırılardan da etkilenebilecek duruma gelinmiştir. Bu nedenle de siber güvenlik ve siber savunma mekanizmalarının uluslararası düzeyde önemi ve iş birliğinin gerekliliği Almanya'nın ilgili stratejilerinde vurgulanmaktadır. Ayrıca stratejide Birleşmiş Milletler, Avrupa Birliği, NATO, G8 ve diğer uluslararası kuruluşların birlikte çalışması gerektiğini vurgulamaktadır. Almanya'daki kritik altyapıların siber tehditlerden korunmasından ve bu konudaki çalışmaların koordinasyonundan sorumlu olan Federal Bilgi Güvenliği Ofisi'nin (BSI), 2011 yılında hazırlanan ve daha sonradan güncellenen stratejik planın ardından yetkileri artırılmıştır. Ancak Almanya günümüzde siber güvenlik konusunda ABD tarafından geliştirilen askerî yazılımlarına kısmen bağlı kalmaya devam etmektedir.

BİRLEŞİK KRALLIK

Ekim 2010'da İngiltere hükûmeti Ulusal Güvenlik Strateji Raporunu İngiliz parlamentosuna sunmuş ve bu rapor kabul edilerek yayımlanmıştır. Bu rapor, Birleşik Krallık'ın karşılaşılabileceği riskleri gruplara ayırmış ve siber saldırıları en yüksek risk grubu olarak kabul etmiştir. Raporda ayrıca siber saldırı alanındaki diğer ülkelerin siber saldırıları ve terörist grupların ve örgütlü ağların yönlendirdiği siber saldırılar da konu edilmiştir. Ulusal Güvenlik Strateji Raporu, birçok ülkenin Birleşik Krallık'a siber saldırılar gerçekleştirdiğini açıkça göstermektedir ve siber güvenliğin, rapor yılı boyunca ve takip eden beş yıl boyunca en yüksek dereceli ulusal güvenlik risklerinden biri olarak görülmesi gerektiğini vurgulamaktadır.

KANADA

Kanada'da siber güvenliğin sağlanması ve siber olaylarla mücadelede ulusal ve uluslararası mevzularda liderlik görevi üstlenen Kanada Siber Olaylara Müdahâle Merkezidir (CCIRC). CCIRC, gerçek zamanlı olarak herhangi bir siber tehlike olup olmadığını incelemekte ve anında müdahâle etmektedir. Merkez, kritik altyapı sektörlerine olaylara müdahâle, koordinasyon ve destek sağlama, izleme ve siber güvenlik tehditleri analiz etme; bilgi teknolojileri alanlarında danışmanlık sağlama ve farkındalığın artırılması ile ilgili eğitim faaliyetleri yürütmektedir.

TÜRKİYE

Türkiye'nin siber güvenlik stratejisi çalışma tarihi oldukça yakındır. Siber güvenlik açısından öne çıkan en önemli çalışmalardan biri, bu alanı düzenleyen bazı yasaların onaylanmasıdır. 2004 yılında kabul edilen 5070 sayılı Elektronik İmza Kanunu ile 2008 yılında iletişim sektörünü düzenlemek üzere kabul edilen Elektronik İletişim Güvenliği Yönetmeliği bu düzenlemelerden ilk olanlardır. Yüksek Planlama Kurulu kararında yer alan Bilgi Toplumu 2006/38, 2006 yılında 28242 sayılı Resmî Gazete'de yayımlanmıştır. Ayrıca konu ile ilgili bir Strateji ve Ek Eylem Planı geliştirilmiştir. Bu plan içerisine öncelikle bilgi güvenliği için yasal düzenlemeler yapılması ve bilgisayar etkinlikleri ve kamu kurumlarının bilgi güvenliğini sağlamaya yönelik faaliyetler için acil bir müdahâle merkezi kurulması yer almıştır.

Bu kapsamda, Bilgisayar Olayları Müdahâle Ekibi (TRBOME), TÜBİTAK Bilgi ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi (BİLGEM) kurulmuştur. Siber güvenlik konusunda en somut adım, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetimi ve Koordinasyonu ile ilgili 2012/3842 Bakanlar Kurulu Kararıdır.

Siber güvenlikle ilgili kararları belirlemek, 155 Siber Suç ve Türkiye'nin Siber Güvenlik Politikası planlarını, programlarını, raporlarını hazırlamak, ilkeleri ve standartları onaylamak ve uygulamalarını ve koordinasyonlarını sağlamak için "Siber Güvenlik Konseyi" kurulmuştur. Konsey içerisinde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Dışişleri Bakanlığı Müsteşarlığı, İçişleri, Millî Savunma, Ulaştırma, Denizcilik ve Haberleşme Müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarlığı, Ulusal İstih-

barat Teşkilatı Müsteşarlığı, Genelkurmay Başkanlığı, Haberleşme Elektronik ve Bilişim Sistemleri Müdürlüğü, Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Başkanlığı, Mali Suçları Araştırma Kurulu Başkanlığı, Telekomünikasyon İletişim Başkanlığı ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığından üyelerin bulunması kararlaştırılmıştır. Ulusal siber güvenliğin sağlanması amacıyla politika ve strateji geliştirme ve eylem planları hazırlama görevi Ulaştırma Bakanlığına verilmiştir. Ulaştırma Bakanlığı da ilgili kurum ve kuruluşların görüşlerini alarak bir siber güvenlik eylem planı hazırlamıştır.

Ülkelerin Siber Güvenlik Gücü Sıralamaları

Harvard Üniversitesine bağlı Belfer Center, kamuya açık verilerden elde ettiği bilgilere göre 30 devletin siber alanlardaki zayıf ve güçlü yönlerini ölçerek hazırladığı listeyi yayımlamıştır. 30 ülkenin 7 farklı alandaki siber güçlerinin ölçüldüğü bu testin içerisinde Türkiye de bulunmaktadır.

Amerika Birleşik Devletleri: 50,24

Çin: 41,47

Birleşik Krallık: 33,57

Rusya: 28,38

Hollanda: 24,18

Fransa: 23,43

Almanya: 22,42

Kanada: 21,50

Japonya: 21,03

Avustralya: 20,04

İsrail: 20,01

İspanya: 18,50

İsveç: 18

Estonya: 17

Yeni Zelanda: 16,50

Kore Cumhuriyeti: 16

İsviçre: 16

Singapur: 14

Malezya: 12

Vietnam: 10

Hindistan: 9

Türkiye: 8

İran: 8

Brezilya: 7

Ukrayna: 6,5

Belfer Center National Cyber Power Index 2020 "Top 10"			Specific Rankings	
#	Country	Overall score	Capability	Intent
1	 United States	50.24	1	2
2	 China	41.47	2	1
3	 United Kingdom	35.57	3	3
4	 Russia	28.38	10	4
5	 Netherlands	24.18	9	5
6	 France	23.43	5	11
7	 Germany	22.42	4	12
8	 Canada	21.50	11	9
9	 Japan	21.03	8	14
10	 Australia	20.04	16	8

Suudi Arabistan: 6

Litvanya: 5

İtalya: 4

Mısır: 3

Harvard Üniversitesi araştırmacıları, siber güvenlik testlerinde tek bir verinin yeterli olmayacağını, gücün tutarlı bir şekilde ölçülmesi için 7 farklı faktörün göz önünde bulundurulması gerektiğini söylüyor. Bu faktörler:

- Yerel grupların çevrimiçi incelenmesi ve gözlemlenmesi
- Ulusal siber savunmaların geliştirilmesi ve güçlendirilmesi
- Bilgi ortamının kontrol edilip yönetilmesi
- Ulusal güvenlik için yabancı istihbarat toplanması
- Siber alan üzerinden milli gelir elde edilmesi
- Düşmanın altyapılarının ve sistemlerinin yok edilip devre dışı bırakılması
- Siber normların ve teknik standartların uluslararası olarak tanımlanması

KAYNAKÇA

- Ulusal Siber Güvenlik Stratejisi 2016 - 2019, <http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf>, 2018.
https://tr.wikipedia.org/wiki/Siber_uzay
M.G. Todd, "Armed Attack In Cyberspace:Detering Asymmetric Warfare With Anasymmetric Definition", Air Force Law Review, (2009), P.68.
T. Kimberly, et al. "The evolution of android Malware and android analysis techniques." ACM Computing Surveys (CSUR) 49.4, 2017, P. 76.
<https://www.bgasecurity.com>
Güntay, 2018, s. 80-81
<https://tr.euronews.com/>
M.S. Schmidt & D. E. Sanger, China Army Face U.S. Charges of Cyberattacks, <http://www.nytimes.com/2014/05/20/us/us-tocharge-chinese-workers>.
Turhan, 2010, s. 103
Sanalp ve Denker, 2016, s. 28,30
İstanbul Bilgi Üniversite Bilgi Teknolojisi ve Teknolojisi Hukuk Enstitüsü, 2012, s. 30
Turhan, 2010, s. 114-115
Hekim & Başbüyük, 2013, s. 154-155
<https://www.webtekno.com/>





PAROLA GÜVENLİĞİ

Parola nedir ve neden kullanılır?

Parola, yetkili bir kullanıcıyı veya işlemi (erişime izin vermek amacıyla) yetkisiz bir kullanıcıdan, işleminden ayırt etmeyi amaçlayan bir kelime, kelime birleşmesi veya karakter ve kelime birleşmesidir.

Parola bir kişinin kimliğini kanıtlamak veya erişim yetkisi alabilmesi için bir parolanın kullanılması, var olması demektir.

Bir parolanın güvenli olabilmesi için kimse ile paylaşılmaması tavsiye edilir. Parola, kimlik doğrulama sağlamak için genellikle bir kullanıcı adı veya başka bir mekanizma ile örneği kullanıcı ID ile eşleştirilir. Parolalar, yetkili erişim sağladığı ve hesaplara ve sistemlere yetkisiz erişimi engellediği için siber güvenlik açısından kritik öneme sahiptir. Parola güvenliğinin önemi, daha güçlü parolaların siber saldırılara karşı daha iyi koruma sağlamasıdır. Güçlü parolaların tahmin edilmesi zordur ve yalnızca bir sistemde veya hesapta kullanılır.

Parola tehlikeleri

Parola, kişilerin kişisel bilgilerini yetkisiz kullanıcılar tarafından görüntülenmekten korumalarına yardımcı olur. Bu nedenle parolaların güvenliğini sağlamak önemlidir. Parolanın güvenliğini temin edebilmek için ona ait tehlikeleri anlamak çok önemlidir.

Parolalarla İlgili Olası Güvenlik Tehlikeleri:

- Parolalar başka kişilerle paylaşılabilir ve kötüye kullanılabilir.
- Parolalar unutulabilir.
- Çalınan parola, kişisel bilgilerinizi toplayabilen yetkisiz bir kullanıcı tarafından kullanılabilir.
- İsim, doğum tarihi, cep telefonu numarası gibi kolay parolalar herkes tarafından tahmin edilebilir ve kötüye kullanılabilir.
- Tüm hesaplar için aynı parola kullanılırsa bilgisayar korsanlarının tüm hesapları ele geçirme ihtimali olacaktır.
- Yönlendirmek için parolalar asla kâğıda (veya) başka bir yere yazılmamalıdır.

Parola Güvenliđi

Parola ayarlarken her konuya ait farklı parola seçmeniz güvenliđinizin açısından çok önemlidir. Hesapları ayarlayabileceđiniz çeşitli parolalar vardır.

Aşağıdakiler bunlara dair bazı örneklerdir:

Güçlü bir parolanın en önemli yönü, hatırlamanın kolay olmasıdır. Hatırlanması zor olan parolalar, gerektiđinden daha sık sıfırlanma eğilimindedir. Ve insanların parolalarını hatırlaması zorsa parolalarını bir yere yazmaları veya bir cihazda kayıtlı tutmalarını gerektirir. Bu da parolaların çalınmasına sebep olabilir. Bu eğilimlerin her ikisi de en güçlü parolaları bile zayıflatır.

Bunu önlemek için parolalarınızı tahmin edilmesi zor, hatırlaması kolay ve yalnızca bir kaynađa erişmek için kullanılır hâle getirmek gerekir.

Güçlü bir parola örneđi: En-Güz3el-Gün. Bu, tahmin edilmesi zor olan uzun bir paroladır. Özel karakterleri ve sayıları vardır. Kolay hatırlanacak şekilde biçimlendirilmiştir. Ve hiçbir kişisel bilgi içermez.

Ancak fark etmiş olabileceđiniz gibi bu güçlü parola örneđi yalnızca rastgele bir karakter dizisi değildir. Ve olması da gerekmez. Aslında, parolanızın rastgele bir karakter dizisi olmaması en iyisidir.

Bunlar temel parola güvenliđi ipuçlarıdır: Daha karmaşık bir parola yerine daha uzun bir parolayı tercih edin, hatırlaması kolay uzun parolalar kullanın ve her hesap için farklı bir parolanız olsun.

Sadece bu yazmış olduđum basit parola güvenlik ipuçlarını takip etmek parola güvenliđinizi önemli ölçüde artıracaktır. Güvenlik ipuçlarını ne kadar eksiksiz uygularsanız parolalarınız o kadar güçlü olur.

Aşağıdaki ipuçları size parola güvenliği konusunda yardımcı olacaktır:

- Kişisel bilgilerden kaçının. Kişisel bilgilerin hatırlanması son derece kolaydır. Lakin kişisel bilgileri parolalarınıza dâhil etmenin sorunu, kişisel bilgilerinizin çoğunun sosyal medya profillerinizde ve diğer çevrimiçi veri tabanlarında herkese açık olmasıdır.
- Her hesabınız için farklı parolalar kullandığınızdan emin olun. Aksi takdirde bir parolanız ele geçerse, diğer hesaplarınız da tehlikede olur.
- Parolanızı girerken kimsenin izlemediğinden emin olun ve bilgisayarınızdan uzaklaşırsanız, etrafta biri varsa bilgisayarı kapalı tutun.
- Kapsamlı güvenlik yazılımı kullanın. Tuş kaydedicileri ve diğer kötü amaçlı yazılımları önlemek için güncel tutun.
- Sizin olmayan bilgisayarlarda parola girmekten kaçının; parolalarınızı çalan kötü amaçlı yazılımlara sahip olabilirler.
- Güvenli olmayan Wi-Fi bağlantıları -havaalanı veya kafe gibi- kullanırken parola girmekten kaçının; bilgisayar korsanları bu güvenli olmayan bağlantı üzerinden parolalarınızı ve verilerinizi ele geçirip kullanabilirler.
- Korunan bilgilerin hassasiyetine bağlı olarak, parolalarınızı periyodik olarak değiştirmeli ve en az bir yıl boyunca tekrar parola kullanmaktan kaçınmalısınız.
- Parolanızda en az 9 karakter küçük ve büyük harf, sayı ve sembol kullanın.
- Parolanızı hatırlamanız için size ipucu verecek, ancak aslında parolanızı içermeyen bir "İpucu sayfası" da yazabilirsiniz. Örneğin: "İpucu sayfanızda" "Olmak mı, olmamak mı?" yazabilir.
- Parolanızın gücünü kontrol edin. Kaydolduğunuz web sitesi, bir şifre gücü analizörü sunuyorsa, buna dikkat edin ve tavsiyelerine kulak verin. Son olarak, parolanızı kimseyle hatta yakınlarınızla bile paylaşmayın.



2022 yılında en çok kullanılan parolalar

Parolaların önemi ve korunmasının zorunluluğundan her zaman bahsedilse de maalesef çoğu zaman parola ayarlanırken yanlış kararlar alınıyor. Aşağıdaki liste 2022 yılında en çok kullanılan parolaları içeriyor.

123456

123456789

qwerty

password

1234567

12345678

12345

iloveyou

111111

123123

KAYNAKÇA:

Common Passwords 2022 - Is Yours on the List? | CyberNews

<https://www.mcafee.com/blogs/consumer/family-safety/15-tips-to-better-password-security/Most|mcafee>

<https://techcult.com/most-common-passwords> | Techult

<https://infosecawareness.in/concept/password-threats> | Infosecawareness

**BUKET
BAYIK**

**KONU
60**





GÜÇLÜ PAROLANIN ÖNEMİ

Güçlü parolalar bilgileri koruyabilir mi? Güçlü bir parola nasıl oluşturulur?

- Güçlü bir parola, kimlik hırsızlığına karşı temel koruma sağlar. Şifre tahmini, bilgisayar korsanlarının bilgisayarlara erişmesinin en popüler yollarından biridir. Basit ve yaygın olarak kullanılan parolalar, bilgisayar korsanlarının bir bilgi işlem aygıtına erişmesini ve ele geçirmesini kolaylaştırır.

Öte yandan, tahmin edilmesi zor bir parola, sıradan bilgisayar korsanlarının bir makineye girmesini çok zorlaştırır ve onları başka bir hedef aramaya yöneltir. Parolanın karmaşıklığı arttıkça, birinin bilgisayarına yetkisiz sızma olasılığı azalır.

Bilgisayar korsanları, Haziran 2021'de şimdiye kadar edindikleri en büyük çalıntı şifre koleksiyonunu yayımladılar. RockYou2021 şifre sızıntısı sonucunda 8,4 milyardan fazla şifre açığa çıktı ve milyonlarca insan hesap ele geçirme, finansal dolandırıcılık ve kimlik hırsızlığı riskine maruz kaldı.

Dolandırıcılar kimlik bilgilerinizi ele geçirmeyi başarırca, banka ve e-posta hesaplarınız saldırıya uğrayabilir ve kimliğiniz çalınabilir. Ancak çok az insan, artan tehdide rağmen şifrelerini korumak için yeterli önlem alıyor.

Peki bilgisayar korsanları ilk etapta şifreleri nasıl alır?



1 Ortalama (Phishing) Saldırıları

Bilgisayar korsanları bankanız veya e-ticaret mağazaları gibi güvenilir kuruluşlardan geldiği iddia edilen resmî görünümlü e-postalar gönderir. Ortalama e-postaları sahte bir web sitesini ziyaret etmeniz için sizi kandıran bağlantılar içerir. Bağlantıya tıklamak, bilgisayar korsanının bilgisayarınıza erişmesini sağlayan kötü amaçlı yazılım indirmesini tetikleyebilir. Bu noktada hırsız şifrelerinizi çalabilir.



2 Sahte “Şifre Sıfırlama” E-postalar

Bilgisayar korsanları, çevrimiçi hesaplarınızdan birinden geldiği iddia edilen sahte e-postalar göndererek hesabınızı doğrulamanızı veya şifrenizi sıfırlamanızı ister. E-posta, sizi sahte bir web sitesine yönlendiren bir bağlantı içerecektir. Bağlantıya tıklarsanız, bilgisayar korsanı web sitesinde paylaştığınız tüm ayrıntıları görecektir.



3 Cihazlarınıza Kötü Amaçlı Yazılım Bulaştırma

Bilgisayar korsanları, spam e-postalarla veya sahte web siteleriyle, tıkladığınızda kötü amaçlı yazılım indirmesini tetikleyecek bağlantılar gönderir.

Keylogger programları, yazdığınız her şeyi yakaladığı için bilgisayar korsanlarının sizi gözetlemesine olanak tanır.

İçeri girdikten sonra, kötü amaçlı yazılım bilgisayarınızı keşfedebilir ve şifreleri çalmak için tuş vuruşlarını kaydedebilir.

Yeterince bilgi aldıklarında, bilgisayar korsanları e-postanız, sosyal medyanız ve çevrimiçi bankacılığınız dahil olmak üzere hesaplarınıza erişebilir.



4 Kaba Kuvvet (Brute-Force) Saldırıları

Saldırganlar, farklı parolaları hızla denemek için otomatik bir bilgisayar algoritması kullanır. Bazı kaba kuvvet saldırıları saniyede bir milyar şifreyi deneyebilir.

Kaba kuvvet programları harfler, sayılar ve semboller arasında yinelenir. Başarılı bir kombinasyon bulana kadar her seferinde bir karakter değiştirir.



5 Sözlük (Dictionary) Saldırıları

Bilgisayar korsanları, bilgisayar korsanlığı için bir sözlük görevi gören tanımlanmış bir ortak parola listesi kullanır. Saldırgan, sözlükteki her şifreyi farklı kullanıcı adlarıyla birleştirerek bir hesabı kırmaya çalışır. Erişim sağladığında, hesaplarınızı kilitleyebilir, kişisel verilerinizi çalabilir ve bilgileri çeşitli kimlik hırsızlığı türleri için kullanabilirler.



6 Kimlik Bilgileri Doldurma

Bilgisayar korsanları, bir veri ihlalinin ardından kullanıcı adlarının ve parolaların bir listesini alır. Saldırganlar, aynı oturum açma kimlik bilgilerini yeniden kullanan diğer çevrimiçi hesapları bulmaya çalışır. Bilgisayar korsanları, birden fazla kombinasyon denemek yerine, her kullanıcı adı için yalnızca bir parola dener.



7 Ortadaki Adam (Man-in-the-Middle) Saldırıları

Bilgisayar korsanları kendilerini bir kullanıcı ile kullanıcının erişmek istediği gerçek site arasına sokmak için sahte bir web sitesi veya sunucu kullandığında gerçekleşir. Saldırganlar daha sonra bir kullanıcının oturum açma oturumunu ele geçirebilir.

Parola korsanlığının neden olduğu zararı en aza indirmek istiyorsanız, güvenliğini ihlal edilmiş bir parolanın açıklayıcı göstergelerini tespit etme yeteneğini geliştirmelisiniz.

İşte bazı uyarı işaretleri:

1 Şifren çalışmıyor

Bilgisayar korsanları bir hesaba eriştiğinde, genellikle şifreyi değiştirir ve sizi kilitler. Genelde kullandığınız şifreler işe yaramazsa, saldırıya uğramış olabilirsiniz.

2 Yavaş bilgisayar performansı

Zamanla, hepimiz bilgisayarlarımızın yavaşladığını deneyimlemiştir, ancak ani bir gecikme, makinenize parolaları çalan kötü amaçlı yazılımların yüklendiğini gösterebilir.

3 Fidye yazılımı mesajları

Kötü amaçlı yazılımlar, programlarınızı ve dosyalarınızı şifrelemek için bilgisayar korsanları tarafından kullanılabilir ve siz onları geri almak için ödeme yapana kadar sizi kilitleyebilir.

4 Arkadaşlarınız ve aile üyeleriniz sizden çevrimiçi olarak tuhaf mesajlar alır.

Bilgisayar korsanları hesaplarınıza erişirse, genellikle arkadaşlarınızı ve ailenizi dolandırmaya çalışırlar. Birisi size "sizin" hesabınızdan garip mesajlar aldığını söylerse dikkatli olun.

Bilgisayar Korsanlarının Ele Geçiremeyeceği Güçlü Parolalar Nasıl Oluşturulur?

Güçlü bir parola oluşturmak sandığınız kadar zor değil. Ayrıca, her hesap için karmaşık, benzersiz parolalar belirlemek, bilgisayar korsanlarını uzak tutmanın en iyi yollarından biridir.

Güçlü bir parola için;

1 Sıralı sayılar ve harfler kullanmayın.

Örneğin, 1234, qwerty, jklm, 6789 vb. kullanmayın.

2 Doğum yılınızı veya doğum ayınızı/gününüzü şifrenize eklemeyin.

Siber suçluların sosyal medya hesaplarınızı gözetleyerek bu bilgileri kolayca bulabileceğini unutmayın.



En az sekiz harf, sayı ve sembolden oluşan bir kombinasyon kullanın.

Parolanız ne kadar uzun ve karakter çeşitliliği ne kadar fazlaysa, tahmin edilmesi o kadar zor olur.

Örneğin, K5o#eb7Qa! büyük ve küçük harflerin, sayıların ve simgelerin benzersiz bir kombinasyonunu kullanır.



Farklı alakasız kelimeleri şifrenizde veya parolanızda birleştirin.

Bu, siber suçluların şifrenizi tahmin etmesini zorlaştırır. Popüler şarkılardan, filmlerden veya televizyon programlarından cümleler kullanmayın.

Parolanızı oluşturmak için üç veya dört uzun kelime kullanın.



Sözlükte bulunan adları veya kelimeleri kullanmayın.

İnsanların karmaşık parolalar oluşturma konusunda sıklıkla sahip oldukları endişelerden biri, özellikle hatırlanması gereken birkaç parola olduğunda, onları unutmaya korkusudur. Doğal olarak, kişi ezberlemesi kolay bir şey düşünmeye çalışmalıdır. Bunu yapmanın bir yolu, bir cümleyi başkaları tarafından kolayca tanınmayan bir şeye dönüştürmektir.

Bunu yapmak için, belirli kelimeleri sayı veya sembollerle değiştirerek cümledeki her kelimenin ilk harfini kullanın. Örneğin, "için" kelimesi 4 rakamı ile veya "sayı" kelimesi # sembolü ile değiştirilebilir. Bu yöntemle, "Sayıyı bir sonraki sefer için kaydedin" gibi bir parola #bSs4K şeklinde yazılabilir.



Şifrelerinizi tekrar kullanmayın.

Her cihaz, uygulama, web sitesi ve yazılım parçası benzersiz ve güçlü bir parola veya PIN gerektirir. Unutmayın, bir siber suçlu parolalarınızdan birini tahmin ederse, bunu tüm kişisel ve profesyonel hesaplarınızı ele geçirmeye

Şifrelerinizi asla kimseyle paylaşmayın.

Buna iş arkadaşlarınız, BT/destek ekibi, müşteri hizmetleri/yardım masası personeli, aile üyeleri ve arkadaşlar da dâhildir.

KAYNAKÇA

Aura. (2022). "How Do Hackers Get Passwords? (And How To Stop Them)". <https://www.aura.com/learn/how-do-hackers-get-passwords>

Secure Data Recovery. "The Importance of Strong, Secure Passwords". <https://www.securedatarecovery.com/resources/the-importance-of-strong-secure-passwords>

Terranova Security. (2022). "How to Create a Strong Password in 7 Easy Steps". <https://terranoasecurity.com/how-to-create-a-strong-password-in-7-easy-steps/>





KRİPTOGRAFİK HASH FONKSİYONLARI

Kriptografik Hash Fonksiyonları

Kriptografi, Yunanca *kryptós* 'gizli' ve *gráphein* 'yazma' kelimelerinin birleşiminden oluşan, bilgilerin farklı yöntemler kullanılarak şifrelendiği bir bilim dalıdır.

Kriptografi uzun seneler askerî alanlarda kullanım bulmuştur. 1970'li yıllardan itibaren internet ve bilgisayar kullanımının yaygınlaşması ile birlikte kriptografi sivil alanda da kullanılmaya başlanmıştır. İnternet bankacılığı aracılığı ile yaptığımız ödemelerin sahte bir bankaya iletilmemesi, bir transferin değişmemesi, internet üzerinden yaptığımız alışverişlerde güvenli bir şekilde kredi kartımızı kullanabilmemiz, web hizmetleri sırasında verilen bilgilerin ya da arkadaşlarımızla mesajlaşmalarımızın üçüncü şahıslar tarafından görünmemesi kriptografinin günümüzdeki kullanımlarına örnek olarak verilebilir.

Günümüzde kullanılan kriptografi yöntemleri çoğunlukla matematiksel bir temele sahiptir ve standartlaştırılmıştır. Bu yöntemlerin güvenliği kriptografiler tarafından incelenir ve herhangi bir açık veya zayıflık bulunursa bu kamuoyu ile paylaşılır.

Hash fonksiyonları ise değişken uzunlukta bir girdi kümesini sabit uzunlukta bir çıktı kümesine eşleyen matematiksel fonksiyonlardır. Hash kelimesi kökenini Fransızcadan almaktadır ve İngilizcede kıyma ile patatesten yapılan bir tava yemeğinin adı ve aynı zamanda doğramak, et kıymak fiilleri yerine kullanılmaktadır. Bu anlamda bakıldığında hash fonksiyonlarının işlevi kıyma makinesi ile kıyaslanabilir. Bir et parçası kıyma makinesine verildiğinde küçük parçalara ayrılıyorsa, hash fonksiyonu da girdi değerini daha küçük boyuttaki bir çıktıya dönüştürür. Girdi kümesi farklı uzunlukta olurken, çıktı kümesinin sabit bir uzunluğu olması hash fonksiyonlarının farklı girdiler için aynı çıktı değerlerini vermesine neden olabilir. Buna karşılık kriptografik hash fonksiyonları pratikte çarpışmaya dayanıklı tek yönlü fonksiyonlardır. Çarpışmaya dayanıklıdan kasıt farklı girdi değerleri için aynı çıktı değerinin hesaplanmasının maliyetli olduğundan pratikte imkânsız olmasıdır.

Kıyma makinesi benzetmesine dönersek; makineden geçen kıymayı tek bir et parçası hâline geri getirmek ne kadar imkânsızsa, kriptografik hash fonksiyonunun verdiği çıktıdan da girdiye ulaşmak o kadar imkânsızdır. Bu özellik literatürde tek yönlülük olarak adlandırılır.



Şekil 1: Hash Fonksiyonlarının Çalışma Prensibi

Aynı zamanda girdi değerindeki küçük bir değişiklik bile hesaplanan hash değerinin değişmesine neden olur. Bu özelliği sayesinde veriler üzerinde yapılan herhangi bir değişiklik saptanabilir (veri bütünlüğü).

Aşağıdaki tabloda sha-256 algoritması ile özetlenen iki örnek metin verilmiştir. Verilen iki metindeki tek fark 'g' ve 'G' harflerinin boyutu olmasına rağmen, birbirleriyle bağlantısı olmayan iki farklı değer hesaplanmıştır.

Metin	SHA-256 Hash Değeri
Siber Güvenlik	b9a7b303d963ea542311e34da2eab3fef50cac30e175765ae43b3d905125dd54
Siber Güvenlik	d49f97f929ab51a7359461fbf107568d44df3a8ae15d0c1047f825f58253bd22

Tablo 1: Örnek SHA-256 Örnekleri

Günümüze kadar geliştirilmiş birçok kriptografik hash fonksiyonu olmasına rağmen çoğunluğu güvenlik açıklıkları nedeniyle kullanılmamaktadır. Aşağıdaki tabloda bazı hash fonksiyonlarının çıktı (özet/karma) değerlerinin boyutlarına ve güvenlik durumlarıyla ilgili bilgiye ulaşabilirsiniz. Çakışma Direnci Açıklığı, şu ana kadar fonksiyon için herhangi bir çakışma bulunup bulunmadığını belirtmektedir.

Hash Fonksiyonu	Özet Boyutu (bit)	Çakışma Direnci Açıklığı
MD4	128	Var
MD5	128	Var
SHA-1	160	Var
RIPEMD	128	Var
RIPEMD-160	160	Yok
SHA-256	256	Yok
SHA-512	512	Yok

Tablo 2: Hash Fonksiyonları Güvenlik Düzeyleri

Kriptografik Hash Fonksiyonlarının Özellikleri

Kriptografik hash fonksiyonları temelde aşağıda açıklayacağımız üç ana güvenlik gereksinimini karşılamalıdır.

Tek Yönlü Fonksiyon/ Ters Görüntüye Dayanıklılık (one-way function / pre-image resistance): Hesaplanan hash değeri üzerinden girdi değerinin pratik olarak hesaplanmasının mümkün olmaması ters görüntüye dayanıklılık olarak adlandırılır.

İkinci Ters Görüntüye Dayanıklılık (second pre-image resistance): Belirli bir hash fonksiyonu ve girdi değeri verildiğinde aynı hash değerini veren ikinci bir girdi değerinin bulunması hesaplama açısından zor ise, fonksiyon ikinci ters görüntüye dayanıklıdır.

Çakışmaya Dayanıklılık (collision resistant): Belirli bir hash fonksiyonu altında aynı hash değerine sahip birbirinden farklı iki girdi değerinin hesaplanması mümkün değil ise, fonksiyon çakışmaya dayanıklıdır.

Hash Fonksiyonlarının Kullanım Alanları:

Şifrelerin saklanması: Uygulama ve/veya web sitelerinde kullandığımız parolalar genellikle veri tabanında orijinal hâliyle değil de şifrelenmiş bir formda tutulur. Parola girişi sırasında, girilen parola şifrelenir ve veri tabanında şifre-

lenmiş şekilde tutulan girdilerle karşılaştırılır. Eğer şifrelenmiş formlar birbiri ile örtüşürse giriş yapılabilir, aksi halde girilen parola yanlış uyarısı alınır. Burada önemli olan nokta parolanın şifrelenmiş formunun geri orijinal formuna döndürülmesinin oldukça zor hatta imkânsız olmasıdır. Hash fonksiyonları tek yönlü fonksiyonlar olduğu için bu özelliği sağlamaktadır. Örneğin 2021 yılında ünlü bir çevrimiçi yemek siparişi sitesi kullanıcı bilgilerinin ele geçirildiğini açıklarken, kullanıcı güvenliği gereği giriş şifrelerinin veri tabanında SHA-256 kriptografik algoritması ile sakladığını belirtmiştir. Bu sayede korsanların şifrelere doğrudan erişimi engellenmiştir. Fakat kullanılan bazı saldırı yöntemlerine karşı tek başına tam bir güvenlik sağlayamamaktadır. Buna ek olarak kullanıcıların güçlü parola oluşturmaya özen göstermeleri gerekmektedir.

Veri/Dosya Bütünlüğü: Hash fonksiyonları, bir belge/program veya dosyanın aktarımı sırasında değişikliklere karşı korunmasını destekler. Aktarılan dosyanın ilk hash değeri ile aktarımdan sonraki hash değerinin birbiri ile uyuşması gerekir. Örneğin; adli bilişimde inceleme, kaynağın alınan kopyası (imajı) üzerinde yapılır, eğer kopya üzerinde herhangi bir değişiklik yapılırsa orijinalden farklı bir hash değeri hesaplanacağı için kopya üzerinde yapılan küçük bir değişiklik bile kolayca fark edilebilir. Bu sayede delil bütünlüğü sağlanmış olur.

Arama: Kriptografik kullanımları dışında hash fonksiyonları veri tabanı içerisindeki aramalarda da önemli bir rol oynar. Veri tabanındaki her bir nesne için hash değeri hesaplanarak bir hash tablosunda saklanır. Arama sırasında sorgunun hash değeri tablodaki hash değerleri ile karşılaştırılır. Hash tabloları kullanılarak arama alanı azaltılır ve bu sayede arama işlemi hız kazanır.

Dijital İmza: Uzun bir m mesajını doğrudan imzalamak çok maliyetli olabileceği için, bunun yerine mesajın hash değeri h (m) dijital olarak imzalanır. Bu yaklaşımda farklı bir m* mesajının aynı hash değerini verme ihtimalinin pratikte imkânsız olduğu kabul edilir (ikinci ters görüntüye dayanıklılık özelliği). Aksi bir durum m mesajının dijital imzasının, m* mesajına da uygulanmasına ve farklı bir mesajın örneğin daha yüksek meblağlı bir sözleşmenin onaylanmasına neden olur.

Hash Fonksiyonlarına Karşı Siber Saldırı Örnekleri

Siber güvenlik alanında özellikle veri bütünlüğü sağlamak ve denetlemek amacıyla kullanılan hash fonksiyonlarının korsanlar tarafından kırılması kolay değildir. Buna rağmen hash fonksiyonlarının doğrudan veya dolaylı yoldan kırılmasına olanak veren saldırı türleri mevcuttur. Aşağıda bunlara örnek olarak kaba kuvvet saldırısı, sözlük saldırısı ve doğum günü paradoksu (saldırısı) açıklanmaktadır.

Kaba Kuvvet Saldırısı (Brute Force Attack)

Eski ve korsanlar arasında oldukça popüler bir saldırı türü olan kaba kuvvet saldırısı, orijinal metni bulmak için deneme yanılma yöntemini kullanır. Korsanlar doğru tahminde bulunmayı umarak tüm olası kombinasyonları tek tek dener.

Sözlük Saldırısı (Dictionary Attack)

Sözlük saldırısı, kaba kuvvet saldırısının bir alt türü sayılabilir. Kaba kuvvet saldırısında tüm olasılıklar denenirken, sözlük saldırısında örneğin en olası parolaların bir listesi çıkarılır ve onun üzerinde tarama yapılır.

Sözlük	Veri Tabanı
Olası Parola	SHA-256 Hash Değeri
123456	499244eb17c6b2dcc65f95a36376ca6a660b486dad44bebc1f8ef3db77c7fcb1
abc123	6ca13d52ca70c883e0f0bb101e425a89e8624de51db2d2392593af6a84118090
11111	d17f25ecfbc7857f7bebea469308be0b2580943e96d13a3ad98a13675c4bfc2
Password	e7cf3ef4f17c3999a94f2c6f612e8a888e5b1026878e4e19398b23bd38ec221a
123456789	15e2b0d3c33891ebb0f1ef609ec419420c20e320ce94c65fbc8c3312448eb225

Tablo 3: Sık Kullanılan Parolaların SHA-256 Değerleri

Yukarıdaki tabloda en çok kullanılan parolalar ve sha-256 algoritması ile özetlenmiş değerleri gösterilmektedir. Korsanların ele geçirdiği karma değerleri ise veri tabanı sütunu altında listelenmiş olarak düşünelim. Eğer sözlükteki hash değerleri ile veri tabanında bulunan hash değerleri arasında eşleşme bulunursa, korsan parolanın orijinalini ele geçirmiş olur. Bu saldırının başarılı olmasının en temel nedeni özelleştirilmeyen zayıf parola kullanımıdır.

Doğum Günü Saldırısı

Doğum günü paradoksu bu saldırı çeşidinin ana düşünce yapısını oluşturur. En az iki kişinin aynı doğum gününe sahip olabilmesi için bir odada en az kaç kişinin olması gerektiği problemine cevap aranır. Bu yaklaşım hash fonksiyonlarının çakışma direnci özelliğine uygulanır. Saldırıda bellek ve zaman izin verdiği ölçüde çok fazla hash değeri hesaplanır ve depolanır. Hash değerleri doğum günlerine karşılık gelir. Sonrasında ise depolanan hash değerleri sıralanır ve bir çakışma aranır. Doğum günü saldırısını önlemek için seçili n bit değeri hash değerinin hesaplanabilmesi ve depolanmasını imkânsız kılacak kadar büyük seçilmelidir.

KAYNAKÇA:

<https://emn178.github.io/online-tools/sha256.html>

Buchmann, J., 2016. Einführung in die Kryptographie. 6. Hrsg. Darmstadt: Springer Verlag Berlin Heidelberg

Josef Pieprzyk, 2003, Fundamentals of Computer Security, Springer-Verlag Berlin Heidelberg

Stephan Spitz, 2011, Kryptographie und IT-Sicherheit, Springer Fachmedien Wiesbaden GmbH

https://www.beyaz.net/tr/guvenlik/makaleler/hash_fonksiyonu_ozetleme_fonksiyonu_ve_birthday_attack.html

[https://www.semanticscholar.org/paper/Analysis-of-Secure-Hash-Algorithm-\(SHA\)-512-for-on-Sumagita-Riadi/c8a362ba959effb9ee8e9c51fa09ccab5c25a957/figure/3](https://www.semanticscholar.org/paper/Analysis-of-Secure-Hash-Algorithm-(SHA)-512-for-on-Sumagita-Riadi/c8a362ba959effb9ee8e9c51fa09ccab5c25a957/figure/3)

<https://electriccoin.co/blog/lessons-from-the-history-of-attacks-on-secure-hash-functions/>





VPN NEDİR, GÜVENLİ MİDİR? VPN'E NEDEN İHTİYAÇ DUYARIZ?

VPN Nedir, Güvenli Midir? VPN'e Neden İhtiyaç Duyarız?

Virtual Private Network, halk arasında bilinen adıyla kısaca VPN, Türkçemize “Sanal Özel Ağ” şeklinde çevrilen bir bilgisayar ağları terimidir. Pek çok kişi için girilmesi sakıncalı olan internet sitelerine bağlanabilmek amacını taşıyor olduğundan akıllarda karanlık bir anlam yer etmiş olsa da aslında VPN, vakti zamanında farklı konumlardaki bilgisayarların uçtan uca güvenli iletişim sağlaması amacıyla geliştirilmiştir. Güvenli iletişimin öneminden ve dijital haberleşme esnasında karşılaşılabilecek güvenlik sorunlarından bahsetmemek olmaz...

Örneğin, güvenliği kritik seviyede tutması gereken ve farklı konumlarda şubeleri olan bir şirket, müşterilerinin kişisel bilgilerini ve kredi kartı, parola gibi hassas verilerini saklıyor ve işliyor olabilir. Muhasebe, AR-GE gibi çok kritik bilgilerin tutulduğu herhangi bir departmanda şubeler arası iletişim kurulmak istendiğinde şayet bu iletişim açık bir ağ veya internet üzerinden yapılacak olursa bu durum çok büyük bir güvenlik açığı teşkil ediyor olacaktır.

Çünkü açık ağlar üzerinden aktarılan verilerin her zaman birileri tarafından dinlenme ve/veya değiştirilme riski vardır. Benzer durumlarda iletişimin güvenli sağlanabilmesi için eskiden şubeler arası özel fiziksel bir ağ hattı kiralanır ve “intranet” olarak adlandırılan bu kapalı ağın üzerinden yalnızca hattaki bilgisayarlar iletişim kurabilirdi, dolayısıyla kötü niyetli kişilerin, aktarılan bilgileri ele geçirme ve müdahale etme riskine kapalı, müstakil bir hat oluşturulurdu. Ancak dünya üzerinde birbiriyle iletişim kurması gereken bilgisayarların sayısı arttıkça ve hassas verilerin taşınmasını gerektiren dijital teknolojiler yaygınlaşmaya devam ettikçe özel fiziksel hat kiralamanın sürdürülebilir ve ölçeklenebilir olmadığı anlaşıldı. Bu durum yeni bir ihtiyacın önünü açtı ve böylece fiziksel özel ağların yerini tutabilecek bir teknoloji olan Sanal Özel Ağ (VPN) doğdu.

VPN'in işleyiş prensibi, günümüzde pek çok bilgisayar kullanıcısı için kapalı bir kutu ve aslında internet kullanan hemen hemen herkesin merak ettiği bir konudur. Sistemi kabaca açıklamak gerekirse VPN sunucuları, dünya üzerinde farklı konumlarda bulunan bilgisayarlardan oluşur. VPN kullanmak istediğinizde ve elinizdeki bilgisayara bir VPN programını yüklediğinizde ilgili yazılım, VPN sunucularından biriyle bilgisayarınız arasında şifreli bir tünel açar. Böylece bilgisayarınız, internet üzerinden bağlanmak istediği noktalara artık bu VPN sunucusu üzerinden bağlanır; internette IP'nizi sorguladığınızda yerel ağınızdaki bilgisayarınızın IP adresi yerine VPN sunucusunun IP adresini görmeyiz sebebi budur.

Ancak bu noktada VPN'i Proxy Server (Vekil Sunucu) ile karıştırmamak gerekir. Vekil sunucular yalnızca sizin adınıza bir internet sitesine bağlanıp ilgili içeriği önünüze getirirken VPN, sanki siz bağlanmak istediğiniz makineyle aynı lokasyondaymışsınız ve onunla aynı ağa bağlıymışsınız gibi davranılmasını sağlar. VPN bir nevi sizi alıp bağlanmak istediğiniz yere taşır. Ve bu işlemi, aktarılan verileri “tünelleyerek” yapar.

Yani akıştaki veriler şifreleme kalitesine göre dışarıdan ya hiç okunamaz ya da uzun sürede ve çok zor okunur, genellikle hiç okunmaz.

Şifreleme ve Tünelleme süreçlerinin nasıl işlediğinden bahsedecek olsak yazı teknik ayrıntılarla dolu ve muhtemelen gayet sıkıcı bir hâl alır, bu sebeple ayrıntıya girmeyeceğiz ancak tünellemenin en azından hangi aşamada gerçekleştiğine kısaca değinebiliriz.

İletişim esnasında gönderici bilgisayarlar, iletecekleri verilerin önlerine çeşitli bilgiler (başlıklar) ekleyip karşı tarafa tüm iletiyi bu şekilde yollar, alıcı taraflar ise iletilen bilginin içindeki başlıkları tek tek açarak okur ve esas veriye böylelikle ulaşır. İşte tünelleme tam bu noktada, bahsetmiş olduğumuz başlıklara yapılan birtakım müdahâleler sonucunda gerçekleşir.

Merak edilen bir diğer husus ise VPN'in günlük hayatta hangi durumlarda ihtiyaç duyulabileceği... VPN gerektirebilecek veya kullanmanın işe yarayabileceği birkaç durumu aşağıdaki gibi sıralayabiliriz:

1. Bir şirketin farklı şubeleri arasında güvenli iletişim kurmak istiyorsak veya bir çalışan olarak çalıştığımız kurumun ağına, izin dâhilinde uzaktan güvenli şekilde bağlanmak istiyorsak...

(Son zamanlarda, çalışanların işlerine uzaktan devam edebilmiş olması nı VPN teknolojisine borçluyuz. VPN olmasaydı pandemi döneminde neredeyse hiçbir şirket uzaktan çalışamazdı ve dünya çapında pek çok kurumun işleri tamamen durmuş olurdu).

2. Belirli içeriklere erişmek için bağlanmak istediğimiz bir ağ varsa ancak bu yerel ağa fiziksel olarak uzaktaysak ve konumumuz gereği bağlanamıyorsak...

(Pek çok uygulama, farklı ülkelerdeki müşterilerinin erişimine farklı kaynakları açıyor. Örneğin bir film portalı, yalnızca belirli bir ülkedeki müşterilerine fazladan birkaç film sunuyor olabilir ve siz VPN sayesinde tıpkı o ülkede yaşayan bir vatandaş gibi o ağa bağlanıp önceden konumunuz gereği erişemediğiniz içeriklere ulaşabilirsiniz).

3. Bir ağa bağlanıp kritik bir işlem yapacaksak ancak bağlanacağımız ağa güvenmiyorsak ve şifreli iletişim kurmak istiyorsak...

(Kritik bilgilerinizi sunarak bir işlem gerçekleştirecekseniz ve umumi bir kabloşuz ağa bağlanmanız gerekiyorsa... Örneğin bir oteldeyseniz muhtemelen mevcut kabloşuz ağa güvenmiyorsunuzdur veya en azından güvenmemeniz gerekir. Bağlantınız ve verileriniz şifreleneceğinden böyle bir durumda yine VPN kullanabilirsiniz).

4. Bulduğumuz yerdeki yasaklanmış bir içeriğe erişmek istiyorsak... (VPN'in, kullanıcıyı konumundan bağımsızlaştırdığını söylemiştik. Benzer şekilde bulunduğunuz bölgede erişiminizin yasaklandığı içeriklere ulaşabilirsiniz).

Son olarak belirtmek isterim ki siber güvenlik herhangi bir anlamda şakası olmayan bir konudur. Bulduğunuz ortamlarda her daim attığınız adımların bilincinde olmanız dileğiyle...





KRİPTOLOJİ NEDİR?

Kriptoloji nedir?

Kriptoloji, şifre bilimidir. İletilerin mesajın belli bir metoda göre şifrelenmesi, bu iletilerin güvenli bir ortamda alıcıya iletilmesi ve iletilmiş olan mesajın deşifre edilmesidir.

Kriptoloji türleri nelerdir?

Kriptoloji bilimi kendi içerisinde iki farklı branşa ayrılır. Bunlar Kriptografi; şifreli yazı yazma ve Kriptanaliz; şifreleri çözme ya da analiz etmedir.

Kriptoloji = Kriptografi + Kriptanaliz

Kriptografi; bir matematiksel yöntemler bütünüdür ve önemli bilgilerin veya mesajların güvenliği için gerekli gizlilik, aslıyla aynılık, kimlik denetimi ve asılsız reddi önleme gibi şartları sağlamak amacı taşır. Bu yöntemler, bir bilginin iletimi esnasında ve saklanma süresinde karşılaşılabilecek aktif saldırı ya da pasif algılamalardan bilgiyi koruma amacı güder.

Kriptanaliz; şifreli veriler verildiğinde orijinal yani düz veriler hakkında mümkün olduğunca fazla bilgi edinmektir. Bunu başarmak için iki yönünü göz önüne almak faydalıdır. Birincisi, sistemi kırmak yani şifreleme sürecinin nasıl çalıştığını keşfetmektir. İkincisi ise belirli bir şifreli mesaj veya mesaj grubu için benzersiz olan anahtarı çözmektir.

Şifrelemenin temel amaçları:

Gizlilik (privacy/confidentiality): Bilgiyi görme yetkisi olanlar dışındaki herkesten gizli tutmak.

Kimlik denetimi (authentication/identification): İletimi gerçekleştirilen bir mesajın göndericisinin gerçekten gönderen kişi olduğu garantisidir.

Bütünlük ya da aslıyla ayrılık (integrity): Bir bağlantının tamamı ya da tek bir veri parçası için mesajın gönderildiği gibi olduğu; üzerinde hiçbir değişiklik, ekleme, yeniden düzenleme yapılmadığı garantisidir.

Reddedilmezlik (non-repudiation): Göndericinin ondan gelen mesajı inkar edememesi (Böylece bir mesaj gönderildiğinde alıcı göndericinin mesajı gönderdiğini ispatlayabilir.)

Erişim kontrolü (access control): İzinsiz kişi ya da uygulamaların erişmemeleri gereken kaynaklara erişemeyecekleri garantisi (Ağ güvenliği bağlamında, erişim kontrolü, ana bilgisayar sistemlerine erişimleri kontrol etme ve limitlendirme yetisidir. Bu kontrolü başarmak için, erişimi kazanmaya çalışan her varlık ilk olarak tanımlanmalı veya doğrulanmalıdır. Erişim kontrolü servisleri kimlik denetimi yapılmış varlıkların kaynaklara ancak kendilerine izin verilen şekilde erişebilecekleri garantisini vermekle yükümlüdür.)

Kriptoloji hangi alanlarda kullanılır?

Kriptoloji kişiler arası iletişimden özel ya da devlet kurumları arası iletişimlere; sistemlerin oluşumundan ve işleyişindeki güvenlik boşluklarına kadar her türlü dallara alakalıdır.

İletişim kurmak isteyen iki kişinin birbirlerine e-posta aracılığı ile mesaj göndermesini örnek verebiliriz. Bu mesajlar birçok bilgisayardan geçmektedir. A kullanıcısından B kullanıcısına gittiğinde daha önce açılıp okunmadığını veya açılıp üstünde değişiklik yapılmadığını bilemeyiz. Bu yüzden devreye kriptolama girmektedir. Kripto teknikleri genelde bu yazıyı daha önce hazırlanmış bir algoritma ile şifreli bir metin hâline getirir.

Kriptolama nasıl yapılır?

Kriptoloji algoritmaları tamamen matematiksel fonksiyonlardan oluşur. Örneğin Sezar şifrelemesi yöntemi oldukça basittir. Ana mesajda bulunan her bir harfi mesajda belirtilen anahtar sayı yani 3 harf kayma kadar ileri götürerek şifreli mesaj oluşturulabilir. Şifreli mesajı okumak için ise mesajda bulunan her harfi anahtar sayısı kadar geriye götürmek gerekir.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

KEY:3

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

SIBER GUVENLIGIN SUPER KADINLARI = VLEHU JXYHQOLJLQ VXSHU NDGLQO-DUL

Şifreleme

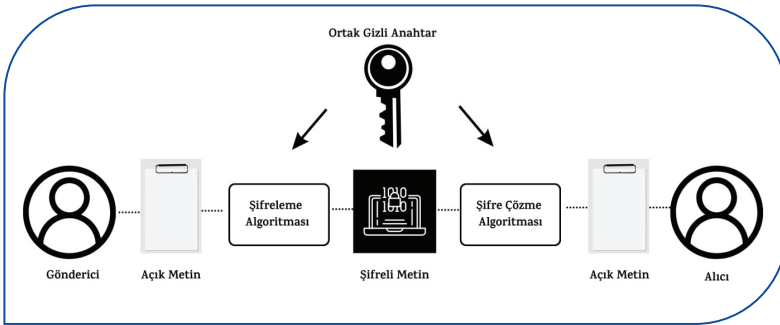
Şifreleme, var olan bir metni veya içeriğin anlaşılmasını ve çözülmesini olabildiği kadar karmaşıklaştırmaktır. Amacı, mesajı doğru kişiye veya kişilere araya herhangi bir dış etken girmeden, mesajın niteliği bozulmadan ulaştırmaktır. Gönderilmek istenen bu iletinin içeriğine düz metin yani “plaintext” denir. İletin içeriğini gizlemek için yapılan işleme “encryption” denir. Düz metin şifrelendikten sonra oluşan metne ise şifreli metin yani “cipher-text” denir.

Şifreleme algoritmaları anahtar kullanma yöntemlerine göre iki kategoriye ayrılmaktadır:

- Gizli anahtarlı (Simetrik) şifreleme algoritmaları
- Açık anahtarlı (Asimetrik) şifreleme algoritmaları

Simetrik Şifreleme

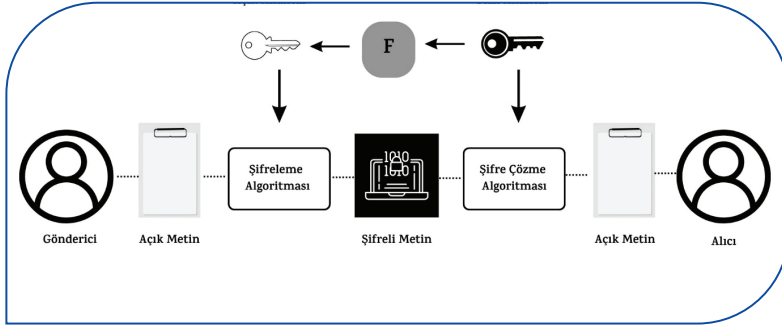
Simetrik şifreleme, şifrelenecek bilginin veya mesajın aynı gizli anahtar ile şifrenmesi ve çözülmesini sağlayan şifreleme yöntemidir. Asimetrik şifrelemeye göre oldukça hızlıdır. Simetrik şifreleme tek bir gizli anahtarın şifreleme ve okumada kullanılmasından dolayı güvenlik konusunda bazı sorunlara neden olabilmektedir. Örnek olarak Triple DES, AES, Blowfish, RC4 ve RC5 verilebilir.



Asimetrik Şifreleme

Asimetrik şifreleme, genel ve özel anahtar kullanımına dayanan simetrik şifrelemeye göre daha güvenli ve yavaş bir şifreleme sistemidir. Asimetrik şifrelemede genel anahtar herkese dağıtılabilirken, özel anahtar sadece şifreleyen tarafından bilinmelidir ve korunmalıdır. Yani kimseyle paylaşılmamalıdır. Asimetrik şifrelemede etkili bir güvenliğin sağlanması buna bağlıdır.

Örnek olarak RSA, DH, DSA, ECDSA ve Eliptik eğri tabanlılar verilebilir.



Simetrik Şifreleme ve Asimetrik Şifreleme Farkları

Simetrik Şifreleme	Asimetrik Şifreleme
Güvenli bir anahtar değişimine ihtiyaç duyulur.	Böyle bir durum yoktur.
Tek bir anahtar kullanılır.	Farklı iki anahtar kullanılır.
Şifreleme işlemi hızlı bir şekilde çalışır.	Şifreleme işlemi çok yavaş bir şekilde çalışır.
Gizlilik sağlar.	Gizlilik ve özgünlük sağlar.
Aktarmak için büyük miktarda veri olduğunda kullanılır.	Aktarmak için küçük miktarda veri olduğunda kullanılır.
Şifreleme sonucunda, şifreli metnin boyutu, orijinal düz metinle aynı veya daha küçük.	Şifreleme sonucunda, şifreli metnin boyutu, orijinal düz metinle aynı veya daha büyük.
Kaynak kullanımı düşüktür.	Kaynak kullanımı yüksektir.

KAYNAKÇA:

<https://tr.wikipedia.org/wiki/Kriptografi>

<https://tr.wikipedia.org/wiki/Kriptanaliz>

<https://tr.wikipedia.org/wiki/Kriptoloji>





GİZLİLİK VE DİJİTAL GİZLİLİK

Gizlilik Nedir?

Gizlilik bir işlem sırasında, bu işlemi gerçekleştiren taraflara ait bilgilerin, işlem verilerinin, dokümanların vb. verilerin başka kişilerden veya kurumlardan saklı tutulması olayıdır. E-ticaret siteleri de dâhil olmak üzere, birçok sitede de olduğu gibi, gizlilik sözleşmesi söz konusudur.

Gizlilik Neden Önemlidir?

Gizlilik hepimizin hayatında büyük anlam taşıyan bir kavramdır. Kişisel bilgilerin gizlenmesi durumu bizi bazı tehlikelerden korur aksi hâlde başımızı belaya sokabilir.

Örneğin T.C. kimlik numarası, banka bilgileri, telefon numarası, özel dosyalar (fotoğraf, video, işle ilgili belgeler) vb. bilgilerin başkalarıyla paylaşılması dolandırıcılık, kimlik hırsızlığı ve işle ilgili belgelerde patent veya fikir bilgilerinin çalınması gibi sonuçlarla bizi karşı karşıya getirebilir. Bunlar hiç kimsenin başına gelmesini istemediği ve istemeyeceği durumlar. Bu yüzden kişisel bilgilerimizin korunması konusunda dikkatli davranmalıyız.

Dijital Dünyada Gizlilik

Gittikçe büyüyen dünyamızda işleri kolaylaştırmak için gün geçtikçe dijitalleşiyoruz. Üstelik dijital dünyada pandemiden dolayı daha da hızlı bir şekilde ilerliyoruz. Yani yaptığımız işlemleri daha çok elektronik ortamdan yapmaya başladık.

Alışveriş, banka işlemleri ve eğitimlerimiz de elektronik ortamda gerçekleşmeye başladı. Bu tür işlemlerimizi gerçekleştirirken gereken bilgileri çoğu zaman şüphe duymadan giriyoruz. Ama girdiğimiz bu bilgilerin aslında ne kadar önemli olduğunu bilsek bile çoğu zaman sosyal medya veya iletişim kurabilme güdüsüyle önemsemeyebiliriz.

Mesela gencinden yaşlısına herkesin akıllı telefonunda bulunan Whatsapp uygulamasının gizlilik sözleşmesi 2021 Mayıs'ta güncellenmişti. Güncellenen yeni sözleşmeyle beraber gizliliğin ihlal edildiğini düşünen bazı kullanıcılar Whatsapp hesabını silerken bazıları da kullanmaya devam etti. Hatta o dönemler diğer mesajlaşma uygulamaları da popülerleşmeye başladı. Whatsapp'ın bu sözleşme değişikliğinden sonra en çok indirilme Telegram adlı uygulamadan yana olurken Bip ve Signal adlı uygulamalara da geçiş yaşandı.

Dijital Gizlilik Nedir?

Dijital gizlilik, kullanıcıların çevrimiçi ortam üzerinden gerçekleştirdiği bankacılık işlemleri, ticari işlemler, alışveriş, vatandaşlık hizmetleri ve sosyal ağ etkileşimi gibi faaliyetler sırasında kişisel bilgilerinin toplanması, işlenmesi ve dağıtımının korunmasını ifade eder.

Dijital Gizlilik Neden Önemlidir?

Dijital gizliliğin önemli olmasının sebebi neredeyse bütün hareket ve işlemlerimizi kaydediyor olmasıdır. Örneğin alışveriş için ziyaret ettiğiniz bir siteden sipariş vereceksiniz. Sizin adınızı, soyadınızı, telefon numaranızı, kapıda ödeme olmazsa kart bilgilerinizi, evinizin adresini girmenizi istiyor. Hatta bazı sitelerde T.C. kimlik numaranızı girmeniz zorunlu olabiliyor. Bu paylaştığımız bilgiler üyelik bilgilerinin koyulduğu bir ortamda saklanıyor ve tekrar alışveriş yaptığımızda yazmamıza gerek kalmıyor. Aslında iyi bir şey gibi gözükse de bütün bilgilerimizi kayıt altına alıyor. Bu bilgilerin saklandığı yere kötü niyetli birinin sızması ve o kişinin bilgilerimizi çalma olasılığı oldukça fazla. Yani bilgilerimizin ne kadar önemli olduğuna ve nereye kaydedilmesine izin verdiğimizize önem vermeliyiz.

Sosyal Medyanın Dijital Gizliliğe Etkisi

Sosyal medya aslında dijital gizlilik açısından çok büyük önem taşıyan bir medya çünkü neredeyse bütün hayatımızı sosyal medyada paylaşıyoruz. En başta kendimizi; denediğimiz ve beğendiğimiz tatları, sevdiklerimizle beraber olduğumuz anları, gezip gördüğümüz ülkeleri, mekanları, tabiatı, küçük sevimli dostlarımızı, giydiklerimizi ve hissettiklerimizi...

Sosyal medya aslında bizim bir nevi dijital günlüğümüz. Günlük olarak kullanan insanlar da mevcut zaten. İnsanlar burada mutluluklarını ve acılarını paylaşabiliyor veya kendi durumlarını sosyal medyadan paylaşarak destek arayabiliyor. Örneğin SMA'lı çocukların aileleri ilaçların fiyatları dolayısıyla yardım kampanyaları başlatabiliyor veya bazı insanlar hasta hayvanların veteriner masrafları için destek arayabiliyor. Böyle konularda sosyal medyanın desteği oldukça fazla...

Ancak bu tür iyi niyetli davranışlar bazen suistimal edilebiliyor ve dolandırıcılar da bundan faydalanıyor. Örneğin jandarma, polis veya savcı isimleri kullanılarak yapılan dolandırma vakaları olabiliyor. Yanı sıra hediye, çekiliş ve hatta iş ilanlarınızı telefonunuza mesaj göndererek kişisel bilgilerinizi öğrenmeye çalışıyorlar.

“Ben böyle şeylere inanmam.” ve “Kimse beni kandıramaz.” deseniz bile bu insanlar kolaylıkla yalan söyleyebildiği için söylerken duydukları rahatlık ve kendilerine olan güvenleri sizi buna inandırabilir.

Güvenlik güçleri sizden altın, para veya kart bilgilerinizi talep etmez. Bunu her zaman aklınızda bulundurun lütfen. “Peki bu insanlar benim numaramı nereden buldu?” diye düşünüyor olabilirsiniz. Büyük ihtimalle numaranızı girdiğiniz bir sitenin telefon numaralarının saklandığı kısma erişebilen art niyetli biri buldu ve bundan faydalanmak istedi. Bu yüzden böyle durumlarla karşılaştığınızda gerçekten kiminle konuştuğunuzu bilmenizde fayda var. Örneğin eğer bir banka işlemi yapacaksanız yapacağınız işlemleri bankanın mobil uygulamasından veya şubeye giderek birebir gerçekleştirmeniz çok daha güvenli olacaktır.

Dijital Dünyada Gizli Kalmanın Zorlukları

Dijital dünyayla iç içe olan sosyal medya gizli kalmamızı zorlaştırıyor aslında. Paylaşma iç güdümüzden dolayı. Sevdiğimiz birinin fotoğrafını gördüğümüzde “Çok güzel çıkmışsın!” tarzı yorumlar yapmak içimizden gelen bir şey veya aslında sevmediğimiz, kullanmaktan memnun olmadığımız bir ürüne yaptığımız “Herkes iyi olduğunu söylemiş ama aslında ... yanları da var.” gibisinden birilerine yardım etme, bilgilendirme iç güdüsüyle yaptığımız yorumlar bile bizim hakkımızda bilgi toplanmasını sağlıyor.

Sizin bu ürünü kullandığınız ve bundan memnun olup olmadığınız gibi bilgiler alınarak müşteri memnuniyeti adına saklanıyor. Mesela herhangi bir şey alacaksınız ve araştırma yapıyorsunuz. Araştırmanızı yaptıktan sonra diğer ziyaret ettiğiniz sitelerde bile araştırma yaptığınız şey hakkında çıkan reklamlara şahit olmuşsunuzdur. Bunun sebebi araştırma yaparken girdiğiniz sitelerin nelerle ilgili olduğunu kaydeden bir mekanizma olması. Hangi içerikteki videoları izlediğiniz, sitede ne kadar süre vakit geçirdiğiniz ve bir videoyu kaç saniye boyunca izlediğiniz bilgilerini tutup sizin neleri sevip sevmediğinizi ve neleri almak için potansiyel müşteri olduğunuzu hesaplıyor. Buna dayanarak sitenin aldığı işbirliği reklamlarını ilginizi doğrudan doğruya önümüze çıkartıyor. Yani dijital dünyada gizli kalmak sandığımızdan daha zor...

Dijital Gizliliği Korumamanın Dezavantajları

Dijital gizliliğimizi korumadığımızda aslında neler olabileceğini tahmin edebiliyoruz. En basiti dolandırıcılık vakaları hepimizin bildiği gibi... Bunun için isminiz, soy isminiz ve fotoğrafınız bile yeterli olabilir. Sizmişsiniz gibi bir hesap açıp sizin isminizi ve fotoğrafınızı kullanıp yakınlarınızdan para isteyebilirler.

Kimlik hırsızlığı ile sizin yapmadığınız eylemleri sanki siz yapmışsınız gibi gösterebilirler. Örneğin araba kiralama sizin isminiz ve kimlik numaranızı kullanarak yapıldıysa ve arabayı alan kişi geri götürmediyse suç sizin üstünüze kalacaktır. Hem de siz yapmadığınız halde. Hiç adil değil öyle değil mi?

Telif hakları ile ilgili olan işlerde ise mesela bir şarkı kaydettiniz ve yakında yayınlayacaksınız. Yayınlamadan önce son hâlini birkaç tanıdığınıza attınız. Attığınız şarkıya ulaşan biri sizin şarkınızı indirdi ve siz yayınlamadan önce şarkınızı sızdırdı. Bu durumda şarkınız daha önceden dinlenildiği için siz yayınladığınızda alacağınız dinlenme şarkınız sızdırıldığı için beklenilenden daha az olacak ve sizi büyük bir zarara uğratacak.

Bunlar aslında olağanüstü olaylar değiller. Şu ana kadar başımıza gelmediği için “Bizim bilgilerimizi kim ne yapsın.” şeklinde düşünüyor olabilirsiniz. Ama başınıza geldiğinde keşke her şeyimi bu kadar açık bir şekilde paylaşmasaydım diyebilirsiniz. O yüzden bu tür şeyler başınıza gelmeden önce dijital gizliliğinize dikkat edin.

Dijital Gizliliği Korumanın Yolları

Günlük hayatımızda dijital gizlilik dolayısıyla sorun yaşamamak için neleri paylaşacağımız konusunda dikkatli olmalıyız.

Sosyal medyada paylaştığınız fotoğraf, video veya yazı gibi içeriklerin ne kadar önemli olabileceğini düşünün. Her anınızı sosyal medya aracılığıyla paylaşmayın. Sizi takip eden insanlar için açık bir yol demektir bu.

Kredi / banka kartı şifrelerinizi sık sık değiştirmeye özen gösterin ve hesap hareketlerinizi kontrol edin.

Kullandığınız hesaplara güçlü şifreler verin. Fiziksel ortamda telefon ve bilgisayarınızdan bilgilerinizi çalmaya çalışan birilerini caydırmak amaçlı telefon ve bilgisayar giriş ekranlarınıza da şifreler ekleyin. Kendinizin ve çocuğunuzun adı, doğum tarihleri gibi anlamlı şifreler veya asd123, qwerty123, 123456789 gibi kolay tahmin edilebilecek şifreler koymayın. Şifrelerinizde büyük harf, küçük harf, rakam ve soru işareti, nokta, yıldız gibi özel işaretler kullanmaya özen gösterin.

Kişisel bilgilerinizi, parolalarınızı saklamak için herkese açık platformları kullanmayın eğer kağıda yazıyorsanız da yazdığınız kâğıtları insanların kolaylıkla erişebilecekleri yerlere saklamayın.

Telefon veya bilgisayarlarınızın güncellemelerini yapın. Çünkü güvenlikle ilgili bir geliştirmeye gidilmiş olabilir.

Bazı telefonlarda uygulamaları indirdikten sonra “Takip etmeye izin ver.” diye bir özellik var. Bunu reddederek uygulamanın sizin hareketlerinizi izlemesini reddedebilirsiniz. Ayrıca indirdiğiniz uygulamaların ayarlarına giderek konum ayarını da kapatırsanız uygulamanın sizin konumuzu kontrol etmesini de engelleyebilirsiniz.

Kayıt olduğunuz sosyal medya sitelerinde e-posta adresinizi ve telefon numaranızı herkese açık bir şekilde paylaşmayın.

Arama ve mesajlaşma için kullandığınız uygulamaların mesajlarınızı şifreleme ile sakladığından emin olun aksi takdirde herkes mesajlarınızı açıkça görüp anlayabilir.

Elimizden geldiğinde bu önlemleri alarak kendi dijital gizliliğimizi sağlamaya çalışalım.

Dijital Gizliliğin İhlal Edilmesi Durumunda Yapılabilecekler

Ne kadar dikkat etsek de dijital gizliliğimiz ihlal edilebilir. Örneğin bankada para çekmek isterken bile kartı koyduğumuz alanda bir kart kopyalama mekanizması olabilir. Kart bilgilerinizi kopyalayarak sizin adınızla işlem yapabilirler.

Telefon numaranızı istemediğiniz yerlerde görebilirsiniz. Yani birisi sizin numaranızı izninizi dışında paylaşmış olabilir veya herkesin görmesini istemediğiniz bilgilerinizi, fotoğraflarınızı, videolarınızı bir sosyal medya ortamında görebilirsiniz. Bunlar kanunlarımızca aslında birer suçtur. Sırasıyla kişisel verileri ele geçirme, kişisel bilgileri başkasına verme ve kişisel verileri yayma suçunu oluşturur.

Kişisel verileri hukuka aykırı olarak birine verme veya ele geçirme suçu şikâyetâbi suçlar arasında yer almaz. Bu yüzden sizin şikâyetçi olmanız gerekmez. Suçun işlendiği öğrenildiğinde savcılık tarafından soruşturma başlatılmalıdır.

Suçun dava zamanaşımı süresi 8 yıl olduğu için soruşturma yapılabilmesi için suçun işlendiği tarihten itibaren 8 yıl geçmeden önce suç bildirilmelidir. Aksi takdirde suçla ilgili soruşturma yapılamaz.

KAYNAKÇA

Gizlilik tanımı:

<https://destek.kmk.net.tr/gizlilik-privacy-nedir>

Dijital Gizlilik tanımı: <https://tr.wikipedia.org/wiki/Gizlilik#:~:text=Dijital%20gizlilik%2C%20kullan%C4%B1c%C4%B1lar%C4%B1n%20C3%A7evrimi%C3%A7i%20ortam,ve%20da%C4%9F%C4%B1t%C4%B1n%C4%B1n%C4%B1n%20korunmas%C4%B1n%C4%B1%20ifade%20eder>

Dijital Gizliliğin İhlali:

<https://barandogan.av.tr/blog/ceza-hukuku/kisisel-verilerin-ele-gecirilmesi-yayilmasi-baskasina-verilmesi-sucu.html>





SOSYAL MEDYA HESABIM ÇALINDIKTAN SONRA NE YAPABİLİRİM?

Sosyal medya hesabım çalınırsa ne yapabilirim, karşılaşabileceğim tehditler neler? Hesabımın daha güvenli olabilmesi için alabileceğim önlemler nelerdir?

Sosyal medya günümüzde herkes tarafından kullanılmaktadır ve “herkes tarafından kullanılabilir olma” özelliği sosyal medyayı yararlı olduğu kadar güvenlik ihtiyacının arttığı bir ortam hâline de getirmiştir. Çünkü dünyamızda kabul etsek de etmesek de kötü niyetli insanlar vardır.

Sosyal medyayı hayatımızın her yerinde kullanabiliyoruz; para kazanabilmek, geniş kitlelere kısa zamanda hitap edebilmek, sosyalleşmek, ilgi duyduğumuz herhangi bir konudan bilgi alabileceğimiz kişilere ulaşabilmek artık bu platformlar sayesinde çok daha kolay.

Şüphesiz olan şu ki sosyal medyanın insan hayatına katkıları gözle görülür düzeyde, peki ama bu platformların taşıdığı riskler ya da kendi içinde barındırdığı tehlikeler yok mudur?

Tabii ki vardır, örnek vermek gerekirse; kişisel bilgilerimizi herkese açık bir şekilde paylaşmanın çok da önemli olmadığını düşünebilirsiniz... Kim, benim kişisel bilgilerimi neden elde etmeye çalışsın ya da nasıl elde edebilir ki diye de düşünebilirsiniz. Fakat emin olun, sosyal medyada konumunuzu ya da telefon numaranızı paylaşmanızın veya bir kafeye gittiğinizde orada olduğunuzu belli eden aksiyonlar sergilemenizin, gerçek hayatta sırtınıza ev adresinizin yazılı olduğu bir kâğıdı asarak gezmenizden pek de bir farkı yoktur. Bunlar kötü niyetli insanlara yardımcı olmaya ve onlara aralık bir kapı bırakmaya sebep olur.

Peki ne yapalım sosyal medya hesaplarımızı mı kapatalım, sosyal hayattan kendimizi mi soyutlayalım, insanlarla iletişim mi kurmayalım diye soruyor olabilirsiniz... Cevap tabii ki hayır, her zaman olduğu gibi önlemimizi alıp, gelecekte, iletişimden, bize böylesine fayda sağlayan platformlardan mahrum kalmadan hayatımızı devam ettirebilmek mümkün.

Öncelikle karşılaşabileceğimiz tehditler nelerdir bunlardan bahsedelim...

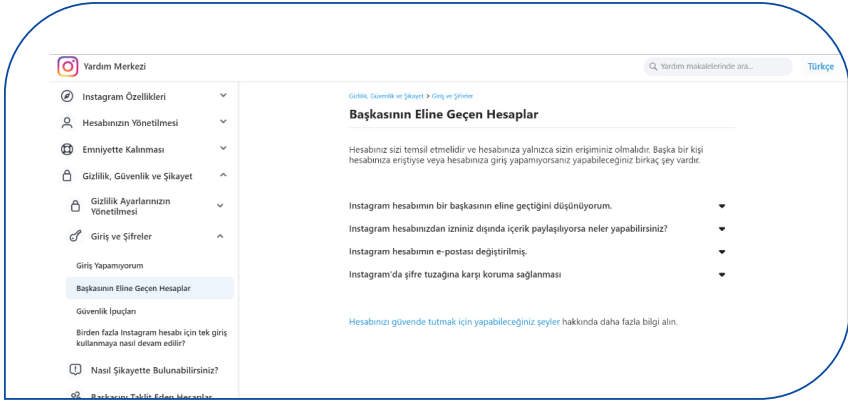
İlk olarak bahsetmem gereken şudur ki sizin isminizi ve fotoğraflarınızı içeren bir sosyal medya hesabı ele geçirildiği takdirde, aksini beyan etmediğiniz sürece, o hesap tarafından yayımlanan mesajlar, paylaşılan gönderiler gibi yapılan hamlelerden siz sorumlu sayılıyorsunuz, tabii ki gerekli mercilerde “aksini beyan etmediğiniz sürece”.

Peki, varsayalım ki sosyal medya hesabınız ele geçirildi ve sizin adınıza yalan yanlış paylaşımlar yapılıyor, ilk olarak yapmanız gereken şey ne?

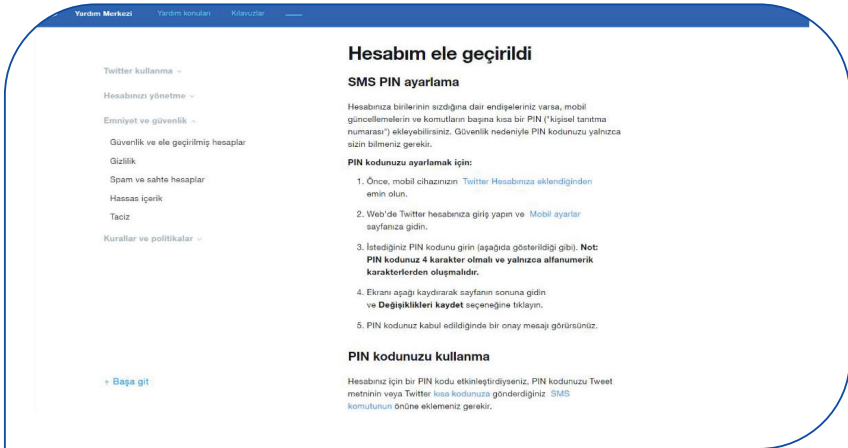
İlk olarak yapmanız gereken, çevrenizdeki insanları olası dolandırıcılık hamlelerine ya da yanlış bilgilere itibar etmemeleri konusunda uyarmak.

İkinci olarak ise, sosyal medya platformlarının kendi bünyelerinde var olan “gizlilik” veya “yardım” seçeneklerine başvurup, hesabınızın başkası tarafından ele geçirildiğini bu platformlara bildirip, bu konuda onlardan bilgilendirip, yardımcı olmalarını istemek.

Yol göstermesi açısından birkaç görsel paylaşacağım:



Görsel 1. Instagram Şikâyet Sayfası



Görsel 2. Twitter Şikâyet Sayfası

Peki diyelim ki, platformların yardım seçeneğinde bildirimizi de yaptık fakat geri dönüş alamıyoruz ya da bu durumun tehlikeli bir durum olmadığına karar verip hiçbir şey yapmadılar. O zaman ne yapmalıyız? İşin peşini bırakacak değiliz tabii.

Yapılacak hamle basittir, savcılığa gidip çalınan hesap için suç duyurusunda bulunmak. Suç duyurunuzu yaptıktan sonra, en azından çalınan hesap üstünden yapılan usulsüz işler için kendinizi sağlama almış olacaksınız bu da sizi bir nebze de olsa rahatlatacaktır.

Sosyal medya hesabımız çalındı dedik, dolandırıcılık yapıldı dedik içimizi kararttık. Ama sosyal medya hesabımız var diye bunları kesin yaşayacağız diye bir şart yok elbette. Başta bahsettiğimiz gibi önlemlerimizi alıp, böyle tehlikelerin önüne geçmemiz gayet mümkün.

Biraz da alabileceğimiz önlemlerden bahsedelim...

İlk olarak güçlü ve karmaşık parolalar belirleyin. Bu şekilde siber korsanların parolaları ele geçirmek için kullandığı, internette hâli hazırda var olan ve sizin de küçük bir aramayla erişebileceğiniz parola listelerinden sıyrılmış oluyorsunuz.

Eğer kullandığınız uygulamada “iki faktörlü kimlik doğrulama” özelliği varsa bunu kesinlikle aktif hâle getirin ve siber korsanların motivasyonunu kırın. Bu şekilde hırsızların atlayıp tırmanacağı duvara keskin teller inşa ediyormuş gibi düşünebilirsiniz.

İnternette gördüğünüz her şeye tıklamayın. Özellikle “kolay yolla para kazanma”, “yeni insanlarla tanışma fırsatı”, “bedava oyun indir”, “evde otururken para kazanmak”, “tatil kazanma fırsatları” gibi insanları manipüle eden, çekici gelen başlıklara hiç tıklamayın.

Hesabınızın herkese açık olma özelliğini kesinlikle kapatın. Yaptığınız basit bir paylaşım, insanlar sizin hangi saatte nerede olduğunuzu bilebilir. Özellikle tatile gittiğinizde, herkese açık bir tatil paylaşımı yaptığınızda sizi izleyen, adresinize erişebilecek insanlara “Bakin ben evde değilim, gidin rahat rahat evimi soyun” mesajını veriyorsunuz. Buna çok dikkat edin.

Şifresiz Wi-Fi ağlarına bağlanmayın. Bağlandığınız ağ üzerinden sizin verilerinize rahatlıkla erişebilirler, diyelim ki bağlanmak zorunda kaldınız o zaman sonrasında mutlaka telefon ya da bilgisayarınızdan, hangisinden bağlandıysanız,





Görsel 3. Adımlarını takip edip “bu ağı unut” seçeneğine tıklayın.

Tanımadığınız insanların takip veya arkadaşlık isteklerini kabul etmeyin.

Tanımadığınız insanlar size bir bağlantı gönderebilir ve siz de boş bulunup o bağlantıya tıklayabilirsiniz sonra bir bakmışsınız hesabınıza tekrar giriş yapamıyorsunuz.

Güvenilir antivirüs yazılımı kullanın. Bu yazılım, tıklayabileceğiniz güvenilir olmayan bağlantılar konusunda sizi uyacaktır.

Riski hiçbir zaman sıfırlayamayız ama o riski dikkate alınmayacak seviyelere düşürebiliriz, yapmamız gereken tek şey gerçek hayatta ne kadar temkinli ve dikkatliyse sanal dünyada da aynı şekilde temkinli, bilinçli, dikkatli olmak ve gerekli önlemleri almak...





SOSYAL MEDYADAN TACİZ ALTINDAYIM NEREYE BAŞVURMALIYIM?

Siber taciz, dijital araçlar ve teknolojiler kullanılarak gerçekleştirilen zorbalıktır. Sosyal ağların arkadaşlık, tanıtım, eğitim, ticaret gibi neredeyse her alanda kullanıldığı günümüz dünyasında bu tür zorbalıklarla sosyal medya mecralarında maalesef çok karşılaşabiliriz. Hedef olarak seçilebiliriz. Bizi üzmeye, utandırmaya, kızdırmaya, yıldırmaya ve hatta bazen istemediğimiz şeyleri yaptırmaya yönelik olarak tekrarlanan, kasıtlı davranışlara maruz kalabiliriz.

Sosyal medya üzerinden siber taciz eylemleri şu şekilde olabilir:

- Sosyal medyada bir kişi hakkında uydurma haberler yayımlayıp, bunları yaymak ya da utandırıcı fotoğraflar yayımlamak
- Sosyal medya platformları ve bunların mesajlaşma eklentileri üzerinden hakarete varan veya tehdit içerikli mesajlar yollamak
- Sosyal medya üzerinden kimlik ve bilgi hırsızlığı yapıp başka birinin kimliğiyle başkalarına kötü mesajlar göndermek
- Sosyal medyada bir başkasına ait rahatsızlık verici görüntüleri yayımlamak
- Bir başkasına ait özel ya da mahrem bilgileri sızdırmak
- Gerçek bir kişiye ait olmayan hesaplardan taciz etmek, rahatsızlık vermek
- Bir başkasının hesaplarını ele geçirmek, bu hesaplardan uygunsuz yayınlar yapmak
- Bir kimseyi rahatsız edici söylemlerde bulunarak, ısrarla takip etmek
- Bir kimsenin paylaşımlarına kasıtlı olarak sürekli olumsuz yorumlar yapmak

Sosyal medya üzerinden yapılan siber tacizler arkasında dijital izler bırakır. Bu durum aslında taciz ve zorbalığın durdurulmasını sağlayacak yararlı ipuçları temin edebilir. Sosyal medya üzerinden gerçekleşen tacizler , fiziksel taciz ve zorbalıklarda olduğu gibi yaş, meslek, cinsiyet ayırt etmeksizin herkes için ruhsal, psikolojik ve duygusal sorunlara neden olabilecek bir durumdur. İnsanları ağır travmalara sürükleyebilir.

Siber taciz çok önem verilmesi gereken ciddi bir sorun ve aynı zamanda suç teşkil etmektedir.

Peki öyleyse sosyal medyada siber taciz ve zorbalıklarla karşılaşıldığında ne yapılması gerekir?

- Öncelikle sizi taciz eden kişiyle iletişimi kesin.
- Sosyal medya hesaplarınızı herkesin erişimine açmayın. Mecbur olunmadığı durumlarda sosyal medya hesaplarınızı korunaklı hâle getirin.
- Tacizci ısrarla eylemlerine devam ediyorsa güvendiğiniz kişilere durumu anlatın.
- Tacize maruz kaldığınız sosyal medya platformlarına bu hesapları iletin ve şikâyetle bulunun.
- Gerekli ise sosyal medya hesaplarınızı silin ya da bir süreliğine dondurun.
- Güvenliğinizle ilgili endişe hissediyorsanız resmî makamlara gerekli şikâyetlerde bulunun.
- Siber zorbalık ve siber tacizin sosyal medyada herkesin başına gelebilecek bir sorun olduğunu unutmayın. Bu durumun üstünü örtmeyin ve önlemleri alın, uygulanabilecek tedbirleri öğrenin.
- Eğer ebeveynseniz çocuklarınıza güvenli internet kullanımını anlatın, onları takip edin ve gerekirse erişimlerini kontrollü hâle getirin.
- Haklarınızı iyi öğrenin, devletin ve sosyal medya mecralarının zorbalıkla mücadele politikalarını inceleyin. Şikâyetlerinizi resmî makamlara nasıl ileteceğinizi öğrenin.

RESMÎ MAKAMLARA ŞİKÂyetİMİZİN İLETİLME SÜREÇLERİ

Sosyal medyaya ait bilişim suçlarının tamamı şikâyetle bağılı değildir. Bazı suçlar şikâyetten bağımsız olarak, ihbar edilmesi üzerine savcılık tarafından kendiliğinden soruşturulur. Sosyal medyada siber tacize maruz kaldığımız zaman resmi makamlara bu durumu iletmek için ilgili kurumlara ihbarda bulunulabilir, suç duyurusu yapılabiliriz. Hatta bu ihbar sözlü şekilde de yapılabilir. Yetkili Cumhuriyet Başsavcılığı suçun işlendiği yerdeki Cumhuriyet Başsavcılığıdır. Bulunduğunuz yerdeki Cumhuriyet Başsavcılığına şikâyet dilekçenizi ibraz etmeniz üzerine dilekçeniz zaten yetkili Cumhuriyet Başsavcılığına gönderecektir.

Sosyal medyada tacize uğradığımızda şikayetlerimizi şu kurumlara iletiriz;

- Cumhuriyet savcılıkları
- Emniyet veya jandarma karakolları
- Siber Suçlar Şube Müdürlüğü
- Cimer

Siber Suçlarla Mücadele Daire Başkanlığının iletişim bilgileri:

Adres: İncek Mah. Boztepe Sk. No:125 Gölbaşı – ANKARA

Mail: siber@egm.gov.tr

Telefon: 0 312 462 55 00

Fax: 0 312 286 92 06

Sosyal medyada taciz veya zorbalığa uğradığımızda bu şikayetler mail üzerinden yapılamaz. Cimer üzerinden başvuru yapılabilir. Ancak Cimer sadece idari başvuru olarak değerlendirip konuyla ilgili birime yönlendirecektir.

Sosyal medya üzerinden uğradığımız tacizi şikayet dilekçesi ile bildirmek istersek bu dilekçe için dikkat edilmesi gereken noktalar şunlardır:

- Öncelikle dilekçeyi hangi Cumhuriyet Başsavcılığına vereceksek başlık olarak ilgili başsavcılık mutlaka yazılmalı.
- Soruşturmanın gidişatı hakkında ilgili tebligatların bize ulaşabilmesi için adımızı, soyadımızı, T.C. kimlik numaramızı ve adresimizi dilekçemizde açık ve anlaşılır şekilde yazmalıyız.
- Sosyal mecralar üzerinden taciz fiilini işleyen kişinin kimliği biliniyorsa adı soyadı belirtilmelidir. Ancak bu kişinin doğru tanımlanması genellikle zordur. Çünkü bazen bu kişiler sahte hesaplar üzerinden tacizi gerçekleştirmektedir. O nedenle savcılık kişinin kimlik tespitini digital veriler üzerinden yapar.
- Şikayet dilekçemizde uğradığımız zorbalığı açıkça ve detaylı olarak belirtmeliyiz.
- Siber tacizin gerçekleştiği tarihin belirtilmesi savcılığın yapacağı soruşturmayı ve sürecin işleyişini kolaylaştırma noktasında çok önemlidir.

- Sosyal mecraada uğradığımız tacize ait ekran görüntüsü, bilgi ve belgeler kuvvetli hukuki delillerdir. Bunlarda dilekçemizle beraber savcılığa sunulmalıdır.
- Dilekçemizin sonuç bölümünde şikayetin kabulü, suçu işleyen failin kimlik tespiti, soruşturmanın başlatılması ve kamu davası açılmasına hükmedilmesi istemlerinde bulunularak dilekçe bitirilmelidir.
- Şikayet dilekçemizde başvuru tarihi ve imzamızın mutlaka bulunması gerekmektedir. Bu süreçte hukuk büroları ve avukatlardan da destek alabiliriz.

Bilişim suçlarıyla ilgili hukuki çalışmalar çok eskiye dayanmamaktadır. Ancak bugün bu konuda çok etkili, hızlı, profesyonel çalışmalar yapılmakta ve önemli adımlar atılmaktadır. 13.10.2022 tarihinde "Dezenformasyonla Mücadele Düzenlemesi" olarak bilinen 7418 numaralı "Basın kanunu ile bazı kanunlarda değişiklik yapılmasına dair kanun Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Kamuoyunda "Sosyal Medya Yasası" olarak da tanınan ilgili kanunla idari para cezaları ve hapis cezalarıyla siber suçlara karşı mücadele güçlendirilmiştir.

**HATİCE
AKKOYUN**

**KONU
67**





FACEBOOK GÜVENLİĞİ

Facebook, kullanıcıların arkadaşlarıyla, aileleriyle iletişim kurmalarını ve fotoğraf, video, bağlantı paylaşımlarını sağlayan popüler bir sosyal ağıdır.

Facebook bütün bu olanakları bize sağlarken güvenliğimizi de tehlike altına atmaktadır. Kullanıcıların Facebook'ta paylaşımda bulunduğu her bilgi saldırganların işini kolaylaştırmaktadır.

Facebook, üye olurken kullandığımız ve paylaştığımız her türlü veriyi toplar. Bu verileri hesap oluşturmamızdan, paylaştığımız gönderilerden, mesajlarımızdan, konumumuzdan toplamaktadır. Ayrıca Facebook giriş yaptığımız cihazı, tarayıcıyı, kullandığımız operatörü de kaydetmektedir. Facebook, topladığı verileri reklam amaçlı da kullanmaktadır. Kullanıcının ilgisini çekecek reklamlar gösterir ve bunlara erişimini ölçer.

Hassas kişisel bilgilerin de paylaşıldığı Facebook'ta, kullanıcılar yeterli bilince sahip olmadığı sürece siber saldırıların da kurbanı olacaktır.

Peki Facebook Hesabımızın Güvenliğini Nasıl Sağlarız?

Öncelikle Facebook Gizlilik Politikası hakkında bilgi sahibi olmak ve Facebook'ta gördüğümüz her içeriğe inanmamak güvenliğimiz için en önemli adımlardır.

E-Posta Güvenliği



Facebook'ta üyelik oluştururken e-posta adresimizi doğru-
lamamızı ister ve Facebook bizimle e-posta adresimizden
iletişim kurar. Hesabımızda şüpheli bir hareket gözlemlendi-
ğinde e-posta adresimiz ile bize bildirilir. Kötü niyetli kişiler
e-posta adresimize erişirlerse Facebook hesabımıza da
erişmesi zor olmayacaktır.

Bu nedenle öncelikle e-posta güvenliğini sağlamalıyız.

Parola Güvenliği



Facebook şifrenizi sadece siz bilmelisiniz
ve aynı şifreyi internette başka yerde kullanmamalısınız.
Facebook şifreniz Instagram şifreniz ile aynı ise Instagram
hesabınız çalındığı zaman Facebook hesabınız da tehlike
altındadır demektir.

Şifreniz tahmin edilmesi zor, kişisel bilgi içermeyen, rakam,
sembol ve harflerden oluşan karmaşık bir yapıya sahip
olmalıdır. Şifreniz e-posta, telefon numarası, doğum günü-
nüz olmamalıdır.

Örneğin; **“Güçlüparola.”**

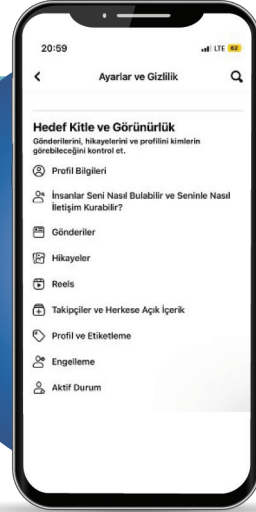
Parolasının yerine **“gUcLuP4r0I4.”** kullanılabilir.

Linklere Tıklama

Saldırganlar ele geçirdikleri herhangi bir tanıdığınızın hesabından size mesaj gönderebilir. Öncelikle “Ödül Kazandınız”, “Hesabınız Kapanacak” mesajları veya para talebinde bulunan bir mesaj aldığınızda mesaj aldığınız kişi ile iletişime geçip durumu bildirmelisiniz. Bu linkler otomatik gönderildiği için tanıdığınız bu durumun farkında bile olmayacaktır. Saldırgan tarafından gönderilen bağlantılara tıklamamalısınız. Eğer saldırı size yönlendirmelerde bulunuyorsa bu yönlendirmeleri dikkate almamalısınız. Tanımadığınız kişilerden gelen mesajları açmamalısınız. Sadece mesaj kutunuza gelen mesajlardaki bağlantılara değil, haber kaynağında da şüpheli bağlantılara tıklamamanız güvenliğinizi açısından önemlidir.

Gizlilik Ayarları

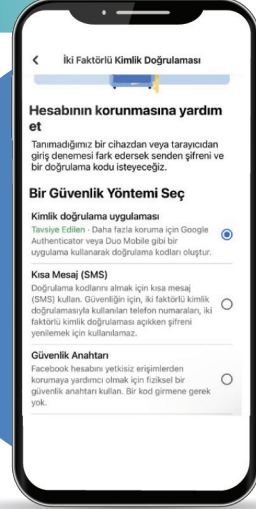
Facebook'un gizlilik ayarları, paylaştığımız gönderileri kimlerin görebileceğini ve diğer insanlarla nasıl bağlantı kuracağımızı kontrol etmemize yardımcı olur.



Hesabınızla ilgili bütün gizlilik ayarlarını tercihlerinize göre yapabilirsiniz. Ayarlarınızı istediğiniz zaman gözden geçirebilir ve değiştirebilirsiniz. Düzenli bir şekilde kontrol etmenizde fayda vardır.

İki Faktörlü Kimlik Doğrulaması

İki faktörlü kimlik doğrulaması, şifre kullanımına ek olarak hesap güvenliği için önemli bir faktördür. Saldırganlar hesabınızı ele geçirmek istediklerinde önce parolanıza erişmek isteyeceklerdir. Eğer hesabınızda iki faktörlü kimlik doğrulamasını aktif ederseniz, saldırgan parolanızı ele geçirmiş olsa bile hesabınıza ulaşamayacaktır.



Giriş Onaylarını Aktif Etme

Bu özellik, normalde giriş yapılan cihazın dışında başka bir cihaz tarafından giriş yapıldığında kullanıcıyı bilgilendirmek amacıyla sunulmuştur.



Genel olarak; Facebook'ta riskleri en aza indirmek için;

1

Arkadaş listenizde sadece güvendiğiniz kişileri bulundurmalısınız.

2

Önemli bilgiler hiçbir zaman paylaşılmamalıdır. Kimlik bilgileri, kredi kartı bilgileri, çalışılan kurum ve maaş bilgileri, konum bilgileri...

3

Hiç kimseye güvenilmemeli ve şüpheli bağlantıları tıklamaktan kaçınmalı.

4

Kötü amaçlı yazılımlar kaldırılmalı. Tarayıcınız her zaman güncel olmalıdır.

**HATİCE
AKKOYUN**

**KONU
68**





TWİTTER GÜVENLİĞİ

Twitter, yaygın olarak kullandığımız Facebook, Instagram gibi bir sosyal medya platformudur. Amacı, güncel olayları ve haberleri öğrenmek, düşüncelerimizi geniş bir kitleye sunmak, bir olay veya kişiyi takip etmek, başka kişiler ile iletişim kurmaktır.

Twitter sağladığı faydaların yanı sıra, kullanıcılarının davranışlarının analiz edilmesi, saldırganlara fırsat sunma, kişisel bilgilerimizi ele geçirerek güvenliğimizi tehdit etme gibi riskleri de beraberinde getirmektedir. Çok sayıda kullanıcının kişisel bilgilerini barındırdığı için saldırganlar tarafından hedef tutulmaktadır.

Kullanıcılar saldırganlara fırsat vermemek için bilgi güvenliklerini sağlamalı ve güvenlik önlemlerini almalıdır.



Siber Saldırı Örnekleri

Kimlik hırsızlığı; saldırının, kullanıcının hassas bilgilerine ulaşması ve bu bilgileri kötü amaçlı kullanmasıdır. Kimlik hırsızlığında genellikle kullanıcının şifresi ve banka hesap bilgileri hedeflenmektedir.

Saldırganlar, kullanıcı bilgilerini elde etmek için yasal bir siteden posta gönderiyormuş gibi yaparlar. Kullanıcı linki tıkladığında bilgilerinin çalınacağı sayfaya yönlendirilir. Böylece saldırı hedefine ulaşmış olur.

Kullanıcının paylaşmış olduğu telefon numarasını arayarak önemli bilgileri tuşlamasını ister ve kullanıcı bu komutları yerine getirirse saldırı hedefine ulaşmış olur.

Saldırgan, kullanıcının profil resmini ve kişisel bilgilerini kullanarak profilini klonlar. Klonlanan profil ile kullanıcının çevresine ulaşarak dolandırıcılık yapabilir.

Saldırgan, herhangi bir sahte profil oluşturarak arkadaşlık isteği gönderebilir. İstek kabul edilirse saldırıya bilgilere ulaşma imkanı verilmiş olur. Saldırgan bilgileri kötü amaçlı kullanabilir.

GÜVENLİĞİMİ NASIL SAĞLARIM?

Twitter ve diğer sosyal ağlara üye olmadan önce mutlaka gizlilik politikası, kullanım şartları ve özel şartlar okunmalı ve ona göre üye olunmalıdır.

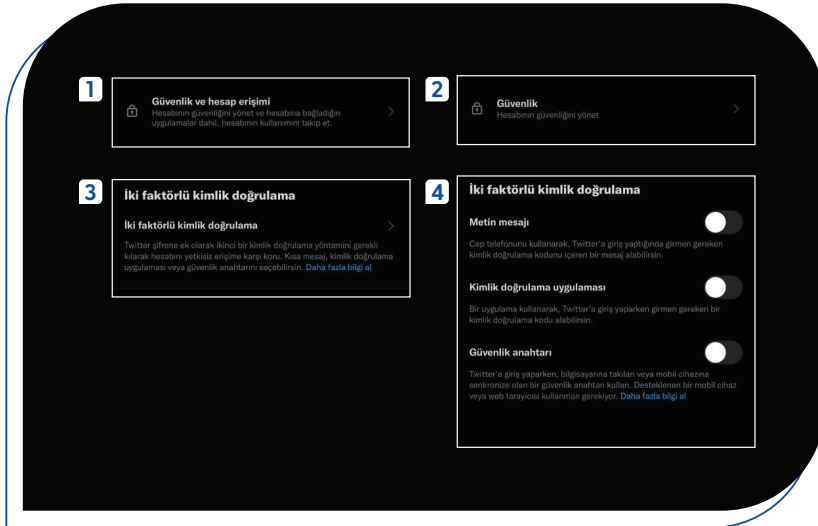
Çocuk kullanıcılar mümkün olduğunca uzak tutulmalıdır.

Bu konuda en büyük görev ailelere düşmektedir. Çocukların hassas bilgileri bu ortamda paylaşmadıklarından emin olunmalı ve çocuklar bu konuda bilgilendirilmelidir.

1

İki Faktörlü Doğrulamayı Aktif Etme

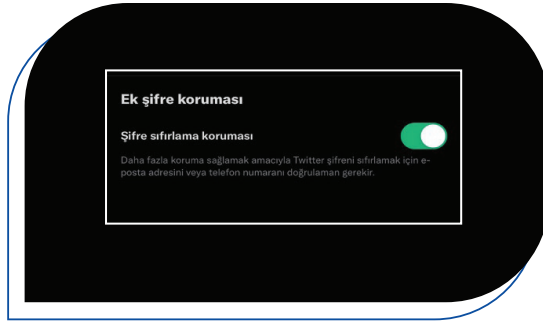
İki faktörlü doğrulama, şifrenizin çalınma ihtimaline karşı salgınların önünde bir engeldir. İki faktörlü kimlik doğrulamanın etkinleştirildiği hesaplarda önce şifre girilmesi istenecektir, daha sonra telefonunuza doğrulama kodu gönderilecektir. Yani, saldırganlar şifrenize erişim sağlamış olsa bile, cihazınızı ele geçiremedikleri sürece hesabınıza da erişim sağlayamayacaklardır. Aşağıdaki görsellerde İki Faktörlü Doğrulamayı Aktif Etme aşamaları gösterilmiştir.



2

Ek Şifre Koruması

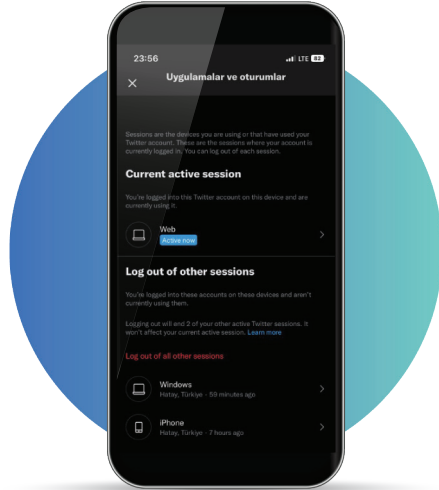
Saldırganlar şifre sıfırlama bölümünü kullanarak kayıtlı mail adresinizi tespit edebilirler. Bunu önlemek için ek şifre korumasını aktif edebilirsiniz. Artık böyle bir talep karşısında sistem e-posta veya telefon numarası isteyecektir.



3

Etkin Oturumları Kontrol Etme

Oturumlar,
Twitter hesabınıza
giriş yaptığınız cihazlardır.
Belli aralıklarla kontrol
ettiğinizde şüpheli bir durum
olup olmadığını buradan
görebilir ve yönetebilirsiniz.

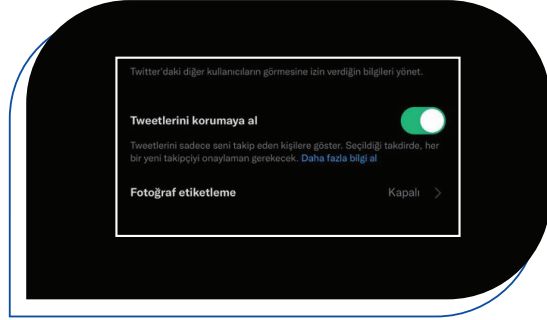


4

Gizlilik Ayarları

Tweetlerinizin başkaları tarafından görülmesi, fotoğraf etiketlemesine izin verilmesi, saldırganların sizin hakkınızda bilgi toplamasına imkan tanır.

Tweetlerinizi korumaya alarak güvenliğinizi riske atmamış olursunuz. Paylaşılan tweetlere GPS koordinat bilgisi eklenebilir. Bu da güvenliğimizi tehdit eden unsurlardan biridir. Konum bilgisini kaldırarak kötü niyetli saldırganların önüne geçmiş olursunuz.



Twitter'da arama kutucuğuna e-posta veya telefon numarası yazıldığında hesabınız görüntülenebilir. Bulunabilirlik ayarlarınızı yöneterek olası risklere karşı koruma sağlayabilirsiniz.

Twitter üzerinde özel mesajlar sadece takip ettiğiniz kişilerden gelmez. Herhangi bir kişi de size özel mesaj gönderebilir. Fakat takip etmediğiniz kişilerden özel mesaj gelmesini engelleyebilirsiniz. Bu da güvenliğiniz için bir avantajdır.

5

Güçlü Parola Kullanımı

Parola belirlenirken hatırlaması kolay, tahmin edilebilirliği yüksek parolalardan kaçınılmalıdır. En az 10 karakter uzunluğunda, büyük harf, küçük harf, sayı ve sembollerden oluşmalıdır. Doğum günü, telefon numarası, e-posta bilgilerini içermemelidir. Diğer sitelerde kullandığınız şifrelerden farklı olmalıdır.

6

Mail Güvenliđi

Twitter'a giriř yaparken kullandığınız mail güncel olmalı ve siz de mailinize ulaşabiliyor olmalısınız. Mail adresinizin řifresi güçlü olmalıdır. Unutmayın ki mail adresiniz tehlike altındaysa bütün hesaplarınız tehlike altındadır.

7

Linklere Tıklama

Siber saldırganlar, kullanıcılara binlerce mesaj gönderirler. Gönderilen bağlantıya tıklamak, eki açmak ya da formu doldurmak gibi yönlendirmelerde bulunurlar.

Bunu önlemek için tanımadığınız kişilerden gelen veya řüpheli gördüğünüz; ödül kazandınız, hesabınız kapanmak üzere gibi aldatmacalarla link gönderen hesapları dikkate almamalı ve size ulaşmasını engellemelisiniz.

Bu basit önlemlerin tümü siber saldırılardan korunmamıza yardımcı olacaktır.



*“Sırlarınızı
rüzgara ifşa ederseniz,
onları ağaçlara ifşa ettiği için
rüzgarı suçlamamalısınız.”*

(Gibran, Khalil)

**HATİCE
BAYDEMİR**

**KONU
69**



Linkedin HESAPLARIMIZ GÜVENDE Mİ?



Neredeyse hepimizin LinkedIn hesabı var.

Peki, bu kadar kişisel verinin bulunduğu LinkedIn hesabımız ne kadar güvenli?

LinkedIn nedir?

LinkedIn, Facebook ve Twitter gibi sosyal medya platformlarından biridir. Diğer sosyal medya platformlarından farklı olarak LinkedIn iş dünyası için kullanılır. İş bulmak, iş vermek veya iş hayatındaki önemli gelişmeleri takip etmek için kullanılabileceğiniz LinkedIn aynı zamanda meslektaşlarınızla bağlantı kurabilme imkanı sunar. Profilinizde CV'nizde bulunması gereken bilgiler bulunur. Ayrıca hesabınızı pdf olarak bilgisayarınıza kaydedebilir veya başkalarına gönderebilirsiniz. LinkedIn, dünyanın en geniş profesyonel iş ağıdır.

eBizMBA Nisan 2013 verilerine göre en sık kullanılan sosyal ağ sitelerine ve aylık ziyaret sayılarına bakıldığında Facebook'un 750 milyon aylık tekil kullanıcı sayısı ile birinci sırada olduğu, Twitter'in 250 milyon ile ikinci, LinkedIn'in 110 milyon aylık tekil kullanıcı sayısı ile üçüncü sırada olduğu görülmektedir.

Tablo1: eBizMBA Nisan 2013 Popüler Sosyal Paylaşım Siteleri

Sıra	Sosyal Paylaşım Sitesi Adı	Aylık Tekil Kullanıcı Sayısı
1	Facebook	750,000,000
2	Twitter	250,000,000
3	LinkedIn	110,000,000
4	Pinterest	85,500,000
5	MySpace	70,500,000
6	Google Plus+	65,000,000

Bu kadar popüler olan bir platform siber saldırıları da beraberinde getiriyor.

Siber saldırı nedir?

Siber saldırılar, bir iş veya kişisel bilgisayar ağı içindeki önemli belgelere ve sistemlere zarar vermeyi veya bunların kontrolünü ele geçirmeyi ya da bunlara erişim sağlamayı amaçlar.

Siber saldırılar, siyasi, kriminal veya kişisel amaçlarla, gizli bilgileri yok etmek veya bunlara erişim sağlamak için bireyler veya kurumlar tarafından gerçekleştirilir.

Bazı siber saldırı örnekleri:



Linkedin saldırıları giderek artıyor

LinkedIn, son çeyrekte kimlik avı saldırılarında en çok istismar edilen marka oldu. Check Point Research, LinkedIn hesabı kimlik bilgilerini çalmayı amaçlayan kimlik avı saldırılarının 2022'nin ilk çeyreğinde arttığını söylüyor. 2022'nin ilk çeyreği için LinkedIn, dünya genelinde Check Point tarafından analiz edilen tüm kimlik avı girişimlerinin %52'sini oluşturuyor.

Sıralamanın en üstündeki konumu, LinkedIn'in beşinci sırada olduğu ve tüm kimlik avı girişimlerinin yalnızca %8'ini oluşturduğu önceki çeyreğe göre büyük bir artış olduğunu ortaya koydu. LinkedIn tüm girişimlerin %14'ünde görünerek ikinci sıraya düşen DHL'den en üst sırayı aldı. 2021 yılında 700 milyon LinkedIn verisinin çalındığına dair haberler çıkmıştı.

Birçok kişisel verimizin bulunduğu LinkedIn hesabımızın güvenliğini artırmak için neler yapabiliriz, bakalım.

Linkedin hesabımızı daha güvenli hâle getirmek için yapmamız gerekenler:



Linkedin hesabınızın güvenli olmasının ilk adımı güçlü ve benzersiz bir parola oluşturmaktır. Bunun için parolanızda büyük küçük harf, sayı aynı zamanda noktalama işareti kullanmalısınız. Böyle bir parola oluşturmakta zorlanıyorsanız parola oluşturma sitelerini kullanabilirsiniz. Çoğu kişinin tercih ettiği basit parolalardan uzak durmalısınız. Adınız, soyadınız doğum tarihiniz gibi bilgilerinizi parola olarak kullanmamalısınız. Kullanıcıların düzenli aralıklarla parolalarını değiştirmeleri de güvenliği daha da artıracaktır.



Bu özelliği etkinleştirmek güvenliğimiz açısından en önemli adımlardan biridir. LinkedIn hesabınızı güvende tutmak için fazladan bir güvenlik katmanı eklemenizi sağlar. İki adımlı doğrulama özelliğini ayarlar bölümünden etkinleştirebilirsiniz.



Hesabınızı ve gizlilik ayarlarınızı gözden geçirin. LinkedIn hesabınız üzerinde birçok şey yapabilirsiniz. Gizlilik ayarlarınızı düzenleyerek hesabınızı daha güvenli hale getirebilirsiniz. Bu sizi saldırılara karşı olabildiğince güvenli duruma getirecektir.



Birçok LinkedIn kullanıcısı profiline e-posta adresi, cep telefonu veya ev adresini eklemektedir. Bu tür özel bilgilerin herkese açık bir şekilde paylaşılması gerekmektedir.



LinkedIn üzerinden bazı cihazlara erişim hakkı veririz. Hesabımıza erişimi olan cihazları ayarlar bölümünden görebiliriz. Bilgimiz dışında erişim varsa hemen bağlantısı kesilip hesabın parolası değiştirilmelidir.



Normalde LinkedIn profiliniz 'herkese açık' olarak ayarlanır. Yani LinkedIn platformundaki her kullanıcı sizin bilgilerinizi görüntüleyebilir. Hesap güvenliğinizi artırmak için ayarlara gidip gizlilik bölümünden görünürlük ayarlarını değiştirebilirsiniz.



Ama bu uygulamaları hesabınıza bağlarken, onların erişebileceği verilerin ne olduğuna dair yeterli bilgi aldığınızdan emin olun. Üçüncü taraf uygulamaları kişisel verilerinizi kullanabilir. Bu yüzden, verilerinizi tehlikeye atabilecek uygulamaları bağlamayın.



LinkedIn isteğe bağlı olarak kullanıcılara bazı reklamlar sunar. Bu reklamları ayarlar bölümünden yönetebiliriz. Reklam kişiselleştirmeyi açmak ya da kapatmak için ayarlara girip gizlilik bölümüne gitmeliyiz. Orada karşımıza reklam verileri çıkıyor. Profilinizde kişiselleştirilmiş reklamlar isterseniz evet seçeneğini seçebilirsiniz.



LinkedIn hesabınızı daha güvenli hâle getirebilmek için her kullanım sonrası oturumunuzu kapatın. Böylece cihaz üzerinden izinsiz olarak hesaba giriş yapılamayacaktır.

LinkedIn hesabım olmasa bile güvende değil miyim?

LinkedIn hesabınız olmasa bile bazı problemlerle karşılaşabilirsiniz. Mesela birisi sizin adınıza veya firmanızın adına hesap açabilir. Sizin bilgilerinizi kullanarak insanları dolandırıp suç işleyebilir. Bu sizi veya markanızı kötü bir duruma sürükleyecektir. Bu sebepten dolayı kendi adımızı veya markamızı sürekli olarak kontrol etmeliyiz.

KAYNAKÇA

1. elmadoktoru.com/ LinkedIn-hesap-guvenligi
2. negatif.net/ 5-adimda-LinkedIn-hesabi-nasil-guvenli-hale-getirilir
3. [1]KurumsalHaberler, Sosyal Medya Nedir, <http://www.kurumsalhaberler.com/pr/sosyal-medyanedir.aspx>
4. [2]eBizMBA, Top 15 Most Popular Social Networking Sites <http://www.ebizmba.com/articles/social-networkingwebsites>
5. [3] <https://www.microsoft.com/tr-tr/security/business/security-101/what-is-a-cyberattack>
6. [4] <https://www.techrepublic.com/article/LinkedIn-most-exploited-brand-phishing/>
7. Tablo1 Kaynak: https://www.asafvarol.com/makaleler/7_8.pdf





SİBER GÜVENLİKTE KARİYER

Neden Siber Güvenlik?

Siber güvenliğin önemini her geçen gün daha iyi anladığımız dijitalleşme çağı, bu alanda araştırma ve uzmanlaşma gerekliliğini de beraberinde getiriyor. Artan talep ile gittikçe popülerleşen bir kariyer yolu hâline gelen siber güvenlik oldukça geniş bir alanda çalışma imkânı sunuyor. Siber güvenlik teknolojinin dokunduğu her alanda bir ihtiyaç olduğundan adaylar aynı zamanda çalışmak istedikleri sektörü seçerken oldukça esnek davranabiliyor.

Siber güvenliğin çok geniş bir alanı kapsaması, farklı pozisyonlarda farklı sorumluluklar ile çeşitlenmekte olsa da genel olarak siber güvenlik uzmanını ciddi sorumluluklar beklemektedir.

Çeşitli sistemlerde siber saldırıların takibi
Başarılı siber saldırılara cevap verme
Sistemleri güvenlik açıklarına karşı değerlendirme
Güvenlik açıklarının takibi, doğrulanması ve raporlanması
Geliştiriciler ile çalışarak güvenli yazılım geliştirme
Güvenlik önlemlerinin tasarlanması ve uygulanması
Yönetim ile siber güvenlik bütçesinin hazırlanması
Çeşitli güvenlik sistemlerinin takibi ve bakımı

Siber güvenlik alanında kariyer yapmak isteyenlerin düşünebileceği pozisyonlardan bazıları:

Bilgi Güvenliği Uzmanı
Siber Güvenlik Mühendisi
CISO (Chief Information Security Officer)
Sızma Testi Uzmanı
Siber Güvenlik Analisti
Zararlı Yazılım Uzmanı

Nasıl Başlanır?

Siber güvenlik alanını tercih edecek öğrenciler için Bilgisayar Mühendisliği, Bilgi Teknolojileri ve Bilişim Mühendisliği gibi bölümler tercih etmeleri önerilse de eğitimin lisans ile sınırlı olmadığını biliyoruz. Lisans eğitimi dışında alınan online kurslar, bootcamp, workshop vb. kişisel gelişim aktiviteleri ile siber güvenlik kariyerinize adım atabilir ve uzmanlaşabilirsiniz. Diğer bilişim teknolojileri alanlarında da olduğu gibi siber güvenlik hakkında da internette kaynak bulmak oldukça kolaydır. Sınırsız kişisel gelişim fırsatı sunan siber güvenlik alanını tercih edeceklerin yaş, eğitim ve konum gibi kaygıları düşünmesine de gerek yoktur.





SİBER GÜVENLİK KAVRAMLARI

SİBER GÜVENLİK KAVRAMLARI

Bilgi (Knowledge): Genellikle geçerliliği veya doğruluğu varsayılacak şekilde mümkün olan en yüksek kesinlik derecesi ile karakterize edilen, kişiler veya gruplar için mevcut olan bir dizi gerçektir.

Veri (Data): Bilginin hammaddesidir ve ham gerçekleri ifade eder. Ölçüm, deney, gözlem, sayım veya araştırma yolu ile elde edilir.

Varlık (Asset): Bilişim sistemlerinde bulunan ve veri ile ilişkisi olan tüm bilgi, kaynak ve kişiyi ilgilendirecek şekilde değer içeren her şeydir.

Zafiyet (Vulnerability): Bir yazılımsal sistem ya da sistem parçalarının içerisinde yer alan sistem hataları, eksiklikler ve zayıflıklardır.

Risk: Açıklıklara yönelik tehditlerin ortaya çıkma ihtimalidir. Seçilen eylemin kayıpla sonuçlanma potansiyelidir.

Sömürmek (Exploit): Bilgisayar, yazılım, program veya herhangi bir dijital sistem üzerinde saldırı gerçekleştirmek amacıyla bulunan açıklık veya hataların oluşturduğu imkânların kullanımıdır.

Saldırı (Attack): Kişinin yetkili erişim veya izin olmaksızın bilgileri elde etme, değiştirme, yok etme, kaldırma veya açığa çıkarma girişimini içeren bir bilgi güvenliği tehdididir. Hem bireylere hem de kurumlara olabilir.

Siber Güvenlik (Cyber Security): Bilgisayarları, mobil cihazları, elektronik sistemleri, sunucuları ve ağları dijital saldırılardan koruma uygulamasıdır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir.

Sosyal Mühendislik: Kişileri kandırarak verilerini ifşa etmeye yönelik bir siber saldırı türüdür. Kötü amaçlı yazılımlar ile kişilerin bilgisayarlarına virüs bulaştırmak veya virüslü sitelerin bağlantılarını açmak için tasarlanan bir tekniktir.

Kandırmak (Spoofing): Bir siber suçlunun, bilinmeyen bir kaynaktan gelen bir iletişimi bilinen ve güvenilir bir kaynaktan geliyormuş gibi gizleme eylemidir. E-postalar, telefon görüşmeleri ve web siteleri için geçerli olabilir.

Oltalama Saldırısı (Phishing): Yasa dışı yollarla bir kişinin bilgilerini, parolasını veya kredi kartı gibi bilgilerini kaynağı bilinmeyen ve kişileri manipüle ederek öğrenme işlemidir.

Sıfırıncı Gün Saldırısı (ZeroDay): Yakın zaman içerisinde öğrenilen ve çok az sayıda kişiye bilindiği, bilgisayar korsanlarının saldırılabileceği açıklıklar barındıran yazılım ve donanım kusurlarıdır.

Kaba Kuvvet Saldırısı (Brute Force): Hedefe yönelik bilgi olmaması veya birden fazla opsiyon bulunan durumlarda istenen olasılıkların deneme yanılma yöntemi kullanılarak test edilmesi işlemidir.

BİLGİ GÜVENLİĞİ TEMELLERİ

CIA (C (Gizlilik) – I (Bütünlük) – A (Erişebilirlik)): Siber güvenliğin bilgi temellerini oluşturan Gizlilik, Bütünlük ve Erişebilirlik kavramlarını temsil etmek için kullanılır.

1. Gizlilik (Confidentiality): Bilgiye yalnızca yetkili kişilerin erişebilmesini ve erişim hakkına sahip olmayanlara karşı güvenliği sağlamayı amaçlamaktır.

2. Bütünlük (Integrity): Bilgiye yetki sahibi olmayan kişilerin izinsiz bir şekilde ekleme, değiştirme ve silme işlemi yapmadığından emin olmaktır.

3. Erişilebilirlik (Availability): Bilginin yetkili kimseler tarafından belirlenen, hedeflenen ve ihtiyaç duyulan süre boyunca ulaşılabilir ve kullanılabilir olmasını amaçlayan prensiptir.

Hack'lemek (Hacking): Kişisel veya kurumsal verilere yetkisiz erişim elde etmek için bir bilgisayar sistemi veya internet ağındaki zayıflıkları belirleme ve daha sonra bu zayıflıklardan yararlanma eylemidir.

Hacker: Sistem, network ve yazılım gibi birçok alanda bilgi sahibi olan ve teknik becerilerini problemleri çözmek için kullanan bilgisayar uzmanıdır. Elektronik sistemlere veya internet üzerindeki hesapların açıklarını kullanarak sistemlere erişim elde eden kişidir. Hacker, zararlı kişi anlamındaki **bilgisayar korsanı** ile ilişkilendirilmiştir.

Hacker Türleri

1. Siyah Şapkalı Hacker (Black Hat): Bilgisayar sistemlerine izinsiz giren kişilerdir. Gelişmiş teknik bilgileri ile gizli verileri çalarlar. Finansal kazanç ve kötü amaçlar için güvenlik açıkları ile sistemleri kullanılamaz hâle getirirler.

2. Beyaz Şapkalı Hacker (White Hat): Sistemlerdeki güvenlik açıklarını bulan siber güvenlik uzmanlarıdır. Güvenlik açıklarını bilgisayar korsanlarından önce tespit ederek bu sistemleri saldırılardan koruma yetkisine sahiptirler.

3. Gri Şapkalı Hacker (Grey Hat): Bilgisayar ağlarına ve sistemlerine girmenin yollarını bulan, yasallık sınırında saldırı yapan kişilerdir. Hem beyaz hem de siyah şapkalı hacker'ların özelliklerini gösterebilirler.

4. Yeşil Şapkalı Hacker (Green Hat): Bilgisayar korsanlığı dünyasında yeni olan ancak siber saldırı becerilerini arttırmaya odaklanmış kişilerdir. Amaçları, bir bilgisayar korsanına dönüşmektir.

5. Mavi Şapkalı Hacker (Blue Hat): Yeni bir yazılım veya sistem ağı piyasaya sürülmeden önce hata testi yapan kişilerdir. Görevleri, yeni yazılımdaki boşlukları veya güvenlik açıklarını bulmak ve bunları düzeltmektir.

6. Kırmızı Şapkalı Hacker (Red Hat): Siyah şapkalı hacker'ları etkisiz hâle getirmeye odaklanan ve sistemlerdeki güvenlik açıklarını tespit etmek için devlet kurumları tarafından işe alınan kişilerdir.

7. Amatör Hacker (Script Kiddie): İnternette kolayca bulunabilen hazır programları ve araçları kullanırlar. Genellikle sistemlere saldıran, kişilerin e-posta hesaplarını veya sosyal medya şifrelerini çalan kişilerdir.

8. Politik Motivasyonlu Hacker (Hacktivist): Kendilerine göre yanlış olan toplumsal veya politik sorunları dile getirmek amacıyla belirli sitelere ve bilgisayar ağlarına saldırılar düzenleyerek mesajlarını ileten gruplardır.

9. Yazılım Korsanı (Cracker): Lisanslı ve telif hakkına sahip ücretli yazılımları herhangi bir ücret ödemeden kullanan kişilerdir. Bilgisayar programları ve oyunları; izinsiz kopyalayarak, dağıtarak ve satarak para kazanırlar.

10. Kripto Korsanı (Cryptojacker): Kötü amaçlı yazılımlar ile birlikte kişilerin elektronik cihazlarını kullanırlar. Amaçları kişilerin verilerini çalmak değil, sistemlerini kripto para madenciliği için bir araç olarak kullanmaktır.

Mavi Takım (Blue Team): Güvenliği sağlamak, eksiklikleri belirlemek, her bir güvenlik önleminin etkinliğini doğrulamak ve tüm önlemlerin uygulamadan sonra da etkili olması için sistemlerin analizini yapan bir grup bireydir.

Kırmızı Takım (Red Team): Güvenlik geri bildirimini sağlamak için saldırgan veya rakip gibi düşünen bir gruptur. Simülasyon uygulamaları ve test yaklaşımları ile organizasyonların güvenlik için savunma hatlarını güçlendirirler.

Sızma (Penetrasyon) Testi: Bir siber güvenlik uzmanının bilgisayar sistemindeki güvenlik açıklarını bulmaya ve bunlardan yararlanmaya çalıştığı bir güvenlik alıştırmasıdır. Simüle edilmiş bu saldırının amacı, bir sistemin savunmasında saldırganların yararlanabileceği zayıf noktaları belirlemektir. Uygulayıcılarına, **pentester** denir.

Siber Ölüm Zinciri (Cyber Kill Chain): Bir siber saldırının analiz edilmesi ve gerekli önlemlerin alınabilmesi için saldırı yöntemlerinin geliştirilmesi ve strateji belirlenmesi gibi metotların kullanıldığı bir çerçevedir.

Yedi aşamadan oluşur: **Keşif, Silahlanma, İletme, Sömürme, Yükleme, Komuta Kontrol ve Eylemler.**

Zararlı Yazılım (Malware): Sistemlere erişim sağlamak, elektronik cihazların işlevlerini bozmak ve kritik bilgileri toplamak gibi farklı kötü amaçlar için kullanılan yazılımdır. Kötü amaçlı yazılım olarak da adlandırılır.

Zararlı Yazılım Türleri

1. Virüs: Kişilerin bilgisi ve izni olmadan bilgisayarın çalışma şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan bir bilgisayar programıdır. Kendisini diğer programlara kopyalayarak ve farklı sistemlerin içerisine girerek sistemlere zarar verir. Farklı çeşitleri vardır ve kullanıcı etkileşimi ile çalışırlar.

2. Truva Atı (Trojan): Kişileri kandırmak ve zarar vermek için güvenli gibi duran ancak kötü amaçlı bir programdır. Diğer zararlı yazılımlardan farklı olarak, farklı dosyalara veya bilgisayarlara bulaşarak kendilerini çoğaltmazlar.

3. Solucan (Worm): Kullanıcı etkileşimine ihtiyaç duymadan kendisini bütün ağ boyunca yayan programdır. Genellikle e-posta yoluyla bilgisayarlara bulaşarak kendini çoğaltır ve bilgisayardan bilgisayara yayılırlar.

4. Casus Yazılımı (Spyware): Bilgisayar, tablet, akıllı telefon gibi cihazlara kullanıcıların izni olmadan sızan, kullanıcıların verilerini toplayan ve bu verileri üçüncü taraflara ileten kötü amaçlı bir programdır.

5. Fidyeye Yazılımı (Ransomware): Bulaştığı bilişim sistemleri üzerindeki dosyalara erişim şifrelenir ve engellenir. Talep edilen fidye ücreti ödendikten sonra gönderdikleri şifreleme anahtarı ile bilgisayarın kilidini açarlar.

6. Reklam Yazılımı (Adware): Kişilerin izni olmadan bilgisayar ve mobil cihazların arka planında çalışan kötü amaçlı programlar olarak tanımlanır. Temel amaçları; reklam görüntülemek, internet arama verilerini reklam sitelerine yönlendirmek ve özelleştirilmiş reklamların görüntülenmesi için veriler analiz eden etmektir.

7. Kripto Hırsızlığı: Kişilerin cihazlarının (bilgisayar, telefon, tablet, sunucu vb.) siber suçlular tarafından kripto para madenciliği için gizli ve izinsiz bir şekilde kullanıldığı zararlı yazılımdır. Gizli bir şekilde arka planda çalışır.

8. Korkutma Yazılımı (Scareware): Kişilerin kötü amaçlı yazılım indirmeleri ve satın almaları için tasarlanan sahte senaryolardır. Genellikle uyarı şeklinde ortaya çıkar ve bilgisayarı korumak için ürün satın almayı önerir.

Kabuk Programlama (Shell): Linux ve Unix işletim sistemlerinde kullanıcının yazdığı komutları anlayan ve çalıştıran bir bilgisayar programı türüdür. Bazı sistemlerde **komut yorumlayıcısı** adı verilir.

Arka Kapı (Backdoor): Yetkili ve yetkisiz kullanıcıların bir bilgisayar sisteminde, ağ veya yazılım uygulamasındaki güvenlik önlemlerini aşarak üst düzey kullanıcı erişimi elde ettiği herhangi bir yöntemi ifade eder.

Klavye Dinleme Sistemi (Keylogger): Kişilerin akıllı bir cihaz ile etkileşime girerken etkinliğini kaydedebilen ve raporlayabilen bir araçtır. Klavyeden girilen bilgileri ve internet aktivitelerini toplayan casus yazılım türüdür.

Botnet: Siber suçluların kontrolü altında olan ve virüslü makineleri uzaktan yönetildiği bilgisayarlardan oluşan bir ağıdır. İstenmeyen e-postalar ve virüsler kendi kendine gönderilir.

Zombi Sunucu: Hack'lenmiş sunucuların farkında olmadan aracı olarak başka sunucuları hack'lemek için kullanılmasıdır. Uzaktan yönetilebilen sunuculardır ve köle sunucu olarak da tanımlanırlar.

Hacklenen sunucuların farkında olmadan aracı olarak başka sunucuları hacklemesi için kullanılmasıdır.

Tehdit (Threat): Bilgi varlıklarına zarar verme potansiyeline sahip olan olaylara neden olabilecek her türlü olasılıktır.

Tehdit Türleri

1. DoS Saldırısı (Denial of Service): İnternete bağlı bir bilişim sisteminin veya sunucunun hizmetlerini geçici veya süresiz olarak engelleyerek, kaynakların asıl kullanıcılar tarafından ulaşılmamasını hedefleyen bir siber saldırıdır.

2. DDoS Saldırısı (Distributed Denial of Service): DoS saldırısının farklı yerlerden ve birden çok bilgisayar üzerinden hedef sistem veya sistemlere yapılmasıyla ortaya çıkan saldırı türüdür.

3. Ortadaki Adam Saldırısı (Man in the Middle): Bilgisayar korsanlarının oturum açma, kişisel bilgileri çalma veya kişileri gözetlemek için iki taraf arasındaki iletişimi gizlice ilettiği veya değiştirdiği saldırı türüdür.

4. Parola Saldırısı (Password Attack): Sistemlerde saklanan şifreli verilerin, bilgisayar korsanları tarafından şifrelerin kırılması işlemidir. Deneme yanılma yöntemi veya parola listesi kullanılarak gerçekleştirilen bir saldırı türüdür.

5. SQL Enjeksiyonu (SQL Injection): SQL kullanan bir sunuya saldırmak için kullanılan ve kötü amaçlı kod eklenmesinden kaynaklanan bir atak tekniğidir. Bilgisayar korsanları, SQL dili özelliklerinden faydalanır.

Yazılım (Software): Değişik ve çeşitli görevler yapma amaçlı tasarlanmış elektronik aygıtların birbirleriyle haberleşebilmesini ve uyumunu sağlayarak kullanılabilirliklerini geliştirmeye yarayan makine komutlarıdır.

Bulut (Cloud): Doğal ölçekteki bir işletim sisteminin, çok basit görevlerini yapma imkânını kullanıcıya veren, web tabanlı uygulamalara erişim sağlayarak sadece bir ağ tarayıcısını çalıştıran basitleştirilmiş bir işletim sistemidir.

Alan Adı (Domain): İnternet üzerinde yetki ve kontrol alanını tanımlayan metin dizisidir. Kullanıcıların belirli bir web sitesine ulaşmak için bir tarayıcı penceresine yazdığı web sitesinin alan adı veya konumudur.

Giriş (Port): Bilgisayarlar arası iletişim sağlayan yazılım tabanlı bir teknolojidir. Ağ bağlantılarının başlangıç ve bitiş noktası olarak düşünülebilir. Birçok port numarası bulunur ve her port farklı hizmet ve iletişim ile ilişkilendirilir.

Protokol (Protocol): Ağ oluşturmada, verileri düzenlemek ve işlemek için iki ya da daha fazla bilgisayar arasındaki iletişimi sağlayan bir dizi kural kümeleridir.

Paket Çözümleyicisi (Sniffing): Belirli ağ paketleri üzerinden geçen tüm verileri yakalayarak ve kendi araçlarını kullanarak elde edilen verilerin içeriğini okuma, izleme ve değiştirme işlemidir.

Zehirleme (Poisoning): Genellikle ağ tabanlı saldırılarda daha çok karşımıza çıkan bir durumdur. Kişilerin akıllı cihazlar üzerinde kafa karışıklığı oluşturmalarına ve yanlış kararlar vermelerine sebep olan zararlı yanıtları içerir.

KAYNAKÇA

<https://tr.wikipedia.org/wiki/Bilgi>
<https://tr.wikipedia.org/wiki/Hacker>
<https://tr.wikipedia.org/wiki/Malware>
<https://berqnet.com/blog/zararli-yazilim>
<https://www.malwarebytes.com/backdoor>
<https://www.forcepoint.com/tr/cyber-edu/spoofing>
<https://tr.wikipedia.org/wiki/Yaz%C4%B1%C4%B1m>
<https://www.techopedia.com/definition/6060/attack>
https://en.wikipedia.org/wiki/Red_team#Cybersecurity
[https://en.wikipedia.org/wiki/Blue_team_\(computer_security\)#cite_note-ref1-1](https://en.wikipedia.org/wiki/Blue_team_(computer_security)#cite_note-ref1-1)
<https://www.kaspersky.com.tr/resource-center/definitions/what-is-cryptojacking>
<https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing>
https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas
<https://www.pandasecurity.com/en/mediacenter/security/14-types-of-hackers-to-watch-out-for>
CyberPath - Practical Penetration Testing





AKILLI EV ALETLERİ VE GÜVENLİĞİ

1945 yılında üretilen ilk dijital bilgisayar ve hemen onun ardından 1969 yılında icat edilen internet... İkisinin ortaya çıkışından sonra yaşadığımız dünya çok hızlı bir değişimden geçti. Eskiden telefonların ceplerde taşınabilmesi kadar küçük olması, birbiriyle kablosuz bağlantıyla haberleşen cihazlar birer hayal ürünüyken, şu anda telefonlarımızla evimizden kilometrelerce uzaktan kontrol edebildiğimiz ve evi kendi kendine temizleyen robot süpürgelerimiz var.

Dünyada sayısı 7 milyarı geçen bu cihazlar ve bu cihazların getirdiği hızlı gelişmeler biz insanların hayatlarını oldukça kolaylaştırırken aynı zamanda da şaşırtıp korkutuyor.. Dizilerde ve filmlerde bizden habersiz bizi izleyen, görüntümüzü ve sesimizi kaydeden, paylaşan; zaman zaman bizi gittiğimiz her yerde takip eden ev aletleri ortaya çıkmaya başladı.

Peki bu korkulardan hangileri ne kadar gerçek? Bu soruyu cevaplayabilmek için öncelikle nesnelerin interneti kavramından başlamalıyız.

Nedir Bu Nesnelerin İnterneti?

Nesnelerin interneti, yaşamımızda kullandığımız her türlü nesnenin internete erişmesi ve diğer cihazlarla bağlantı kurabilmesidir. Bu kavramın ilk örneği 1991 yılında Cambridge Üniversitesindeki profesörlerinin kahve makinesinin yanına gitmeden makinenin dolu olup olmadığını öğrenmek zaman kaybını önlemek istemeleriyle birlikte ortaya çıkmıştır. Bir kahve makinesi ve profesörlerle başlayan bu yolculuk internetin de günlük hayatımızın ayrılmaz bir parçası olmasıyla birlikte epey bir yol aldı. İlk olarak kahve makinesi, buzdolabı, televizyon gibi daha genel araçlarımız; telefon, tablet ya da bilgisayar gibi araçlar üzerinden bizim komutlarımız doğrultusunda uzaktan çalışabilir hâle geldi. Bugünlerde ise ev ve araba kilitlerimiz, ev termostatlarımız ve aklımıza gelebilecek her şey uzaktan kontrol edilebilir. Bu da akıllı ev ve akıllı şehir gibi yeni kavramların hayatımıza katılmasını sağladı.

Günlük hayatımızda, her şeyimizi cep telefonlarımızdaki uygulamalar üzerinden daha hızlı ve pratik yapabilir olmamız her ne kadar çekici gelse de azımsanmayacak ölçüde olumsuz yanları da var.

Peki Risklerimiz Neler?

Günlük hayatımızı kolaylaştıran bu cihazlar doğru bir şekilde çalışmak için bazı verilere ihtiyaç duyar veya çalışma esnasında üreticiye geri bildirim sağlamak için veri toplar. Örnek olarak robot süpürmeniz evinizin bir krokisini, bebek kameraları odanın görüntüsünü, akıllı yatağınız sizin uyku düzeninizi, akıllı saatler ise kalp atışınızdan çağrılarınıza ve konumlarınıza kadar neredeyse her şeyinizi kayıt altında tutar.

Akıllı ev aletlerinin topladığı bu bilgilerin depolanması ve şirketlerle paylaşılması dünyanın en büyük şirketlerinin bile zaman zaman hacklendiği bir dünyada, çok ciddi gizlilik ihlallerine sebebiyet verebilir. Dahası akıllı ev cihazlarınıza bir şekilde erişim sağlamış olan kötü niyetli insanların bu bilgileri kullanarak sizi, sevdiklerinizi tehdit edebilmesi veya adınıza haberiniz olmadan işlem yapabilmesine olanak tanır.

Ek olarak cihaza erişim sağladıktan sonra kameralardan evi izleyebilir ve kaydedebilirler; ses kaydedebilen cihazlar aracılığı ile söylediklerinizi dinleyip kayıt altına alabilir. Bu sayede kredi kartı şifreleriniz, telefon şifreleriniz ve daha birçok özel bilgiye ulaşabilirler ya da ele geçirilen cihazla aynı ağda olan diğer cihazlara (telefon, tablet, bilgisayar gibi kişisel eşyalar) erişim sağlayarak onları da ele geçirebilirler.. Evinizin sıcaklık ayarlarıyla oynayabilir; siz evde yokken boş fırın, ocak, mikrodalga gibi aletleri çalıştırabilir, aletlerin bozulmasına veya daha ciddi sonuçlara sebebiyet verebilir; güvenliğiniz için kullandığınız önemli cihazları devre dışı bırakabilirler.

Hangi Önlemleri Alabiliriz?

Akıllı ev aletlerimizin sahip olduğu riskler epey ciddi ve korkutucu olsa da bunların gerçekleşmesini minimuma indirmek için alabileceğimiz bazı önlemler mevcut.

Bu önlemleri almadan önce ve aldıktan sonra olarak ikiye ayırabiliriz.

Daha almadan önce önlem amaçlı yapabileceğimiz şeyler çok basit gözükse de aslında büyük öneme sahipler. İlk olarak gerçekten ihtiyacınız olup olmadığınıza emin olun. Her ne kadar basit bir şey gibi görünse de alacağınız en basit akıllı ev aleti bile çok ciddi güvenlik riski oluşturur hatta en basit görünen ev aletlerinde güvenlik açığı olma olasılığı daha fazladır. Eğer satın almaya kararlaysanız alacağınız ürünün özelliklerine ve donanımına dikkat edin. Ses komutlarıyla kullanmayacağınız bir cihazda ses algılama özelliğine sahip bir donanıma ihtiyacınız yok ya da televizyonunuzda sadece film ve dizi izleyecekseniz bir kamerası olması çok da gerekli değil. Adını duyurmuş ve güvenliğiyle öne çıkan markalardan almanız ve ürününüzün güncel modellerden biri olması da güvenlik açığı ihtimallerini düşürecektir.

Akıllı ev cihazınızı aldıktan sonra alabileceğiniz önlemlerin sayısı, almadan öncekine göre daha fazla ve biraz daha karmaşıktır. Wi-fi ağınızın güvenliğini sağlamak ve ağ üzerinden diğer cihazlara erişimi zorlaştırmak için wi-fi ağınıza güçlü bir parola koyun ve varsayılan ağ adını değiştirin. Kişisel cihazlarınız ve akıllı ev aletlerini aynı ağa bağlamak tehlikeli olacağı için ayrı bir parolası ve ismi olan bir misafir ağı oluşturun. Eski modellerde kapatılmamış güvenlik açıkları olması ihtimaline karşı wi-fi modemlerinizin güncel bir model olduğundan emin olun. Evdeki bütün akıllı aletlerinizi güçlü parolalarla



koruyun ve bu parolaları belirli aralıklarla yenileyin. Bir cihazda kullandığınız parola diğeriyle aynı olmasın. Anti-virüs programları kullanın ve bu programları güncel tutun gerekli güncellemeleri düzenli olarak yapın. Mümkün olan tüm cihaz ve hesaplarda çift faktörlü doğrulamayı etkinleştirin. Bu sayede izinsiz erişim sağlamaya çalışan insanların erişim sağlaması daha zor olacaktır. Gerekli olmayan veya kullanmadığınız ve veri toplayan özellikleri kapatın. Örnek olarak eğer o an kullanmıyorsanız cihazınızın ve uygulamanın kamera veya ses kaydetme gibi özelliklerini devre dışı bırakın. Mümkünse kullanmadığınız zamanlarda akıllı ev cihazlarınızın internetle olan bağlantısını kesin. Cihazınızın özelliklerini ve davranışlarını iyi tanıyın. Normal dışı olan hareketlerine dikkat edin (örneğin açılıp kapanmasına). Her türlü önleme rağmen herhangi bir ele geçirme durumunda kameralar üzerinden sizi gözetlemelerini engellemek amacıyla kameralarınız üzerine bant yapıştırmak da iyi bir çözüm yolu olabilir.

Tüm bu önlemleri alarak akıllı ev aletlerimizin keyfini çıkarabilir bize sunduğu imkânları kullanarak hayatımızı kolaylaştırabiliriz.

KAYNAKÇA

<https://www.computer.org/publications/tech-news/trends/7-actionable-tips-to-secure-your-smart-home-and-iot-devices>

<https://blog.avast.com/how-to-secure-your-smart-home>

<https://us.norton.com/blog/iot/smart-home-security-core#>

<https://siberbulten.com/makale-analiz-akilli-guvenlik-sistemleri-ve-barindirdigi-riskler/>

<https://blog.avast.com/iot-security-business-risk>

<https://www.kaspersky.com/resource-center/threats/internet-of-things-security-risks>





BİLİŞİM SUÇLARI NELERDİR?

SİZ ÇEVİRİMİÇİ OLDUĞUNUZA GÖRE KÖTÜ ADAMLAR DA ÖYLE!

Bilişim suçları, cep telefonu, bilgisayar, pos makinesi gibi türlü teknolojiler ve ağlar aracılığıyla, dijital ortamda kişi ve ya kurumlara maddi ve ya manevi zarar vermeyi amaçlayan gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen davranışları ifade eder.

Bu saldırılar, hakaret veya nefret içerikli kişisel bir mesajdan, bir ulusun güvenlik ve ekonomik bütünlüğüne yönelik bir tehdide kadar pek çok farklı şekilde karşımıza çıkabilir.

Bilişim suçları farklı kaynaklarda farklı sınıflandırmalara tabi tutulmuştur.

Örneğin, Türk Ceza Kanunu (TCK) temel alınarak aşağıdaki şekilde sınıflandırılabilir:

1. Bilgisayar sistem ve servislerine yetkisiz erişim: Bir kişiye ait e-posta, WhatsApp, sosyal medya hesaplarına yetkisiz girmek bu gruptaki bilişim suçlarına örnek olarak gösterilebilir. Özellikle başkasına ait sosyal medya hesaplarına yetkisiz erişim, eğlenceli bir durum olarak algılansa da, aslında ciddi bir suçtur.

2. Bilişim sistemlerini engelleme, bozma, verileri yok etme veya değiştirme: Sunucuya yapılan bir saldırı ile sistemi yetkisiz kılmak, başkasına ait bir bilgisayara illegal bir dosya göndermek veya yazılım yüklemek, klavye izleme (keylogger) yazılımları ile kişinin hareketlerini takip etmek ve kişisel verilerini çalmak gibi fiiller bu kapsamda suç olarak tanımlanmaktadır.

3. Kanunla Korunmuş Bir Eserin İzinsiz Kullanılması: Telif hakkı ihlalleri en çok işlenen sanal suçlar arasındadır ve çoğu zaman farkında bile olmadan gerçekleştirdiğimiz ciddi bir suçtur. Lisanssız yazılımlar, çevrimiçi yazılım korsanlarına davetiye olarak düşünülebilir ve kullanıcıyı risklere açık hale getirir. NullMixer gibi zararlı yazılımlar için farkında bile olmadan arka kapıyı açabilirsiniz ve kişisel verilerinizin çalınmasına sebep olabilirsiniz. Anlık olarak bu hizmetlerden ücretsiz faydalandığımızı hatta bunun cazip olduğunu düşünsek de bedeli çok ağır olabilir.

4. Yasadışı Yayınlar: Yasadışı yayınlar, vatanın birliğini tehdit eden, terör öğeleri içeren web sayfaları, genel ahlak kurallarını ihlal eden pornografik görüntüler ile kişi ve kurumlara karşı hakaret ve küçük düşürücü öğeleri barındıran yayınları kapsamaktadır (Digisophia, 2014). Dijital platformlarda sunulan ürünlerde içerik üreticileri, sunucu hizmeti veren yer sağlayıcıları ve bağlantıdan sorumlu erişim

sağlayıcıları sürecin hukuka uygun şekilde yönetilmesinde sorumluluk sahibidir. İçerik üretici hukuka uygun içerikler sağlamalı, ev sahibi olan yer sağlayıcıları misafirin hukuka uygunluğunu kontrol etmeli ve erişim sağlayıcıları hukuka aykırı içeriklere ait alternatif erişim bağlantısı, trafik akışı gibi dijital delilleri yasal süre boyunca saklamalıdır.

5. Müstehcenlik-Çocuk İstismarı: Her ne kadar müstehcenlik kavramı devletler ve uluslara göre farklılık gösterse de, ifade özgürlüğünün aşıldığı durumlarda, birçok yargılama mevzuatı bulunmaktadır ve en keskin cezalar çocuk istismarına yöneliktir.

6. Bilişim Yoluyla Dolandırıcılık: Banka veya kredi kartlarının kötüye kullanılması, ülkemizde ve dünyada da en yaygın bilişim suçları arasındadır. Ucuza telefon almaya çalışırken kargodan çıkan salatalıklar, 1 günde 10 kilo verdiren mucizelerin reklamlarını incelerken gelen şişman faturalar, x markasından 100 liralık hediyeye çeki almaya çalışırken hesaptan çekilen paralar hepimize tanıdık konular.

En çok kullanılan yöntemlerden bir tanesi de yemleme ya da diğer adıyla olta-lama (pishing) tekniğidir. Genellikle e-mail ya da WhatsApp aracılığıyla finansal kuruluşlardan ya da bankalardan acil ve çok önemli gibi görünen bir bilgilendirme mesajı gelir ve sisteme giriş yapmak için mesajda belirtilen linke tıkladığımızda virüs, solucan gibi zararlılara hoş geldin demiş oluruz. Linke tıkladığınızda açılan sitenin sahte olduğunu fark etmeyip hesap bilgilerinizi girdiğinizde ise zaten artık çok geçtir.

7. Bilişim Yoluyla Hakaret, Sövme ve Şantaj: Sosyal platformlarda kişiler ya da kurumlar hakkında aşağılayıcı ifadeler kullanmak, karalama çalışmaları, asılsız suçlamalar gibi hareketler bu kapsamdaki suçlardır.

Anlatılan bilişim suçları pek çok farklı şekilde işlenebilir.

Örneğin, çöpe dalma (scavenging) tekniğiyle çıktı birimlerinde üretilen ve daha sonra çöpe atılan kâğıt, mürekkep şeridi gibi malzemeler üzerinde kalan bilgiler depolanarak, bazı veriler geri getirilebilir.

Gizlice dinleme (eavesdropping) tekniğiyle veri taşımada kullanılan ağlara girilebilir veya bilişim sistemlerinin yaydığı elektromanyetik dalgalar kullanılarak verilere ulaşılabilir.

Salam tekniğiyle (salami techniques), çok fazla sayıda banka hesabından dikkat çekmeyecek kadar küçük miktarlarda para suçlunun hesabına aktarılır. Her bir mağdurdan, küsurat gibi oldukça küçük paralar alınması değersiz gibi gözükse de failin topladığı para adeta servet oluşturmaktadır.

En sık rastlanan zararlı yazılımlardan birisi ise Truva atıdır (Trojan horse). Genellikle ücretsiz yazılımlar veya e-mail yoluyla kullanıcılara ulaştırılır ve yararlı olduğu düşünülen yazılımlar vasıtasıyla cihazda bir arka kapı açılmasına ve cihaz kontrolünün kaybedilmesine sebep olur.

Bunların dışında, tarama (scanning), süper darbe (super zapping), gizli kapılar (trap doors), mantık bombaları (logic bombs), virüsler, ağ solucanları gibi pek çok saldırı tekniği bulunmaktadır.

Bilişim suçları doğrudan bilgisayar ağı ve aygıtlarını hedef alan suçlar ve bilgisayar ağı ve aygıtlarının araç olarak kullanıldığı suçlar olarak iki ana grupta da değerlendirilebilir. Bilgisayara yönelik suçlardan en sık karşılaşılanlar virüsler, kötü amaçlı yazılımlar (fidye yazılım, casus yazılım, Truva atı gibi) ve hizmet dışı bırakma (dos) saldırılarıdır. Belirtilen saldırıların amacı geleneksel olarak bir sistemi çökertmek ya da maddi kazanç sağlamak olarak kabul edilse de, otonom araçların kontrollerinin ele geçirilmesi, hastanelere ve elektrik şebekelerine sabotajlar düzenlenmesi gibi girişimler ve hatta ölümle sonuçlanan saldırılar da mevcuttur.

1998'de Amerika'da yoğun bakımdaki babasının mirasına el koymak isteyen ve bir hacker ile anlaşarak babasının ilacını değiştiren bir kişi babasının ölümüne sebep olmuştur ve bu olay tarihteki ilk siber cinayet olarak bilinmektedir.

2020 yılında Almanya'da Düsseldorf Üniversitesi Kliniği'nin sunucularına düzenlenen fidye yazılımı saldırısı hastane faaliyetlerinin durmasına sebep olmuştur. Acil müdahaleye ihtiyacı olan, fakat 30 kilometre uzaklıktaki Wuppertal hastanesine sevk edilmek zorunda kalan 32 yaşındaki bir hasta, gerekli tıbbi müdahaleye zamanında ulaşamadığı için kurtarılamamıştır.

İran'ın Buşehr ve Natanz'daki nükleer tesislerini hedef alan Stuxnet virüsünün uranyum gaz sızıntısına ve buna bağlı ölümlere sebep olduğu iddia edilmektedir. 2021 senesinde ABD'nin Florida eyaletine bağlı Oldsmar kentinde bir siber saldırgan içme suyu hattına bir saldırı düzenlemiş ve sudaki sodyum hidroksit miktarını 100 kat artırarak halkı zehirlemeye çalışmıştır.

Yine 2021 yılında, DarkSide korsan grubu, ABD'nin en büyük boru hattı olan Colonial Pipeline'a bir fidye yazılımı saldırısı düzenlemiştir ve 13 eyalet ve 260 teslimat noktasının hizmet dışı kalmasına sebep olmuştur. Saldırı sırasında 100 gb veri çalınmıştır ve bilgilerin geri alınabilmesi için 4,4 milyon dolar fidye ödenmiştir.

2024'e kadar sadece otomotiv sektöründe siber saldırılar sebebiyle 505 milyar dolarlık zarar oluşması beklenmektedir.

Farklı sektörlerde bunun gibi örnekleri çoğaltmak mümkündür.

Bilgisayar ağı ve aygıtları aracılığıyla yapılan saldırılarda ise en çok karşılaşılanlar, dolandırıcılık ve kimlik hırsızlığı, kişisel verilerin (kullanıcı adı, parola, kredi kartı verileri) çalınması ve siber izlemedir.

Yüzyılın hack'i olarak bilinen ve en büyük bilişim suçlarından biri olan Epsilon olayında çoğu e-posta bilgilerinden oluşan veriler ele geçirilmiştir. Best Buy, JP Morgan Chase gibi işletmelerle çalışan ve alanında lider şirketlerden olan Epsilon'un bu saldırıda 4 milyar dolar civarı bir hasar aldığı düşünülmektedir.

Ülkemizde de yakın zamanda Yonca Sağlık Hizmetleri Ltd. Şti.'ne düzenlenen siber saldırıda hasta ve çalışanların kimlik, özlük, finans, genetik bilgileri gibi kişisel veriler ele geçirilmiştir. Son dönemlerdeki en büyük veri ihlallerinden biri olarak değerlendirilen bu saldırıdan yaklaşık 500 bin kişi ve 2.5 milyon kayıt etkilenmiştir.

Benzer şekilde 2021 yılında Yemek Sepeti firmasına düzenlenen siber saldırıda 20 milyonun üzerinde kullanıcıya ait isim, soy isim, telefon numarası, adres ve kredi kartı bilgileri ele geçirilmiş ve bilgilerin ifşa edilmemesi karşılığında işletmeden yaklaşık 3 milyon TL değerinde fidye istenmiştir. Ayrıca işletmeye Kişisel Verileri Koruma Kurumu (KVKK) tarafından veri güvenliğine ilişkin yükümlülükler aykırı faaliyet sebebiyle 2 milyon TL, Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından ise güvenlik sorumluluklarını yerine getirmeme gerekçesiyle de 1 milyon TL'lik ceza verilmiştir.

Son dönemlerin en büyük bilişim suçları arasında bulunan "RockYou2021" saldırısı ile yaklaşık 8 buçuk milyar şifre internet ortamında paylaşılmıştır.

En ilginç bilişim saldırılardan bir tanesi de Ashley Madison çöpçatanlık uygulamasına gerçekleştirilmiştir. Site etik olmadığı gerekçesiyle saldırıya uğradıktan sonra, kullanıcılardan kişisel bilgileri ve sohbetlerini ifşa etmemek için şantaj yoluyla para talep edilmiş ve pek çok ilişkinin bitmesiyle sonuçlanmıştır.

Kısacası, akıllı evler, sürücüsüz otomobiller, artırılmış gerçeklik, sanal gerçeklik veya şu an aklımıza dahi gelmeyen ama birkaç yıl içinde günlük hayatımızın vazgeçilmezi olabilecek yeni buluşlarla teknoloji hayatımıza her geçen gün daha fazla dâhil olacak ve buna paralel olarak bilişim suçları da artış gösterecektir.

Maalesef, bilişim suçları genellikle orta üzeri ya da ileri seviye zekâya ve bilgi birikime sahipken, suç mağdurları genellikle bilinçsiz kullanıcılardan oluşmaktadır. Haliyle suçlular yanıltıcı, engelleyici, delil karartıcı türlü yöntemler kullanmakta ve teknolojinin oluşturduğu her fırsatla yöntemlerini sürekli geliştirmektedir.

Çevrimiçi olduğumuz her dakika bilişim suçlarının da kurban avında olduğumuzun bilincinde olmalı ve güvenlik önlemlerini ihmal etmemeliyiz. Her ne kadar internet ortamında %100 güvenlik sağlamak mümkün olmasa da, bilişim saldırıları insani zayıflıkları kullanılarak gerçekleştirilmektedir. Bu açıdan en büyük silahımız farkındalıktır.



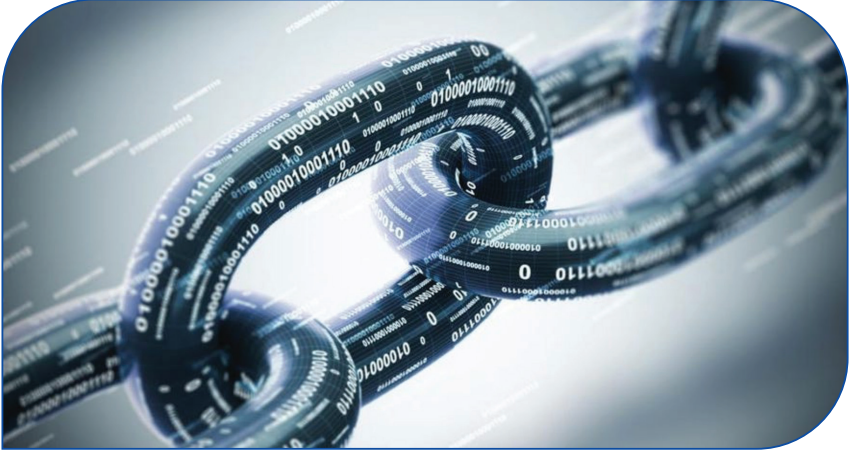


BLOCKCHAIN'İN SİBER GÜVENLİKTE ROLÜ

Blockchain (blok zinciri) teknolojisi, siber güvenliğin geleceğini büyük oranda değiştirebilir mi? Yapılan araştırmalara göre dünya genelinde her 35 saniyede bir siber saldırı gerçekleşiyor. Bu da mevcut siber güvenlik önlemlerinin hızla gelişen teknolojiye ayak uydurmakta zorlandığını açıklamaya yeterlidir.

Peki Blockchain siber güvenlik endüstrisini güçlendirmeye nasıl yardımcı olabilir ?

Blockchain, kişisel verilerimizi çalarak bize karşı kullanmak için çabalayan siyah şapkalı hackerlardan verilerimizi korumaya yönelik en temel adımlardan biridir. Ağdaki her bir işlemi şifreleyerek veri tabanına kaydeden dağıtık defter teknolojisidir.



Siber güvenlik endüstrisinde güçlü ve güvenilir bir altyapı oluşturmak için Blockchain'in dikkate değer özellikleri mevcuttur. Bunlardan kısaca bahsederek eğer;

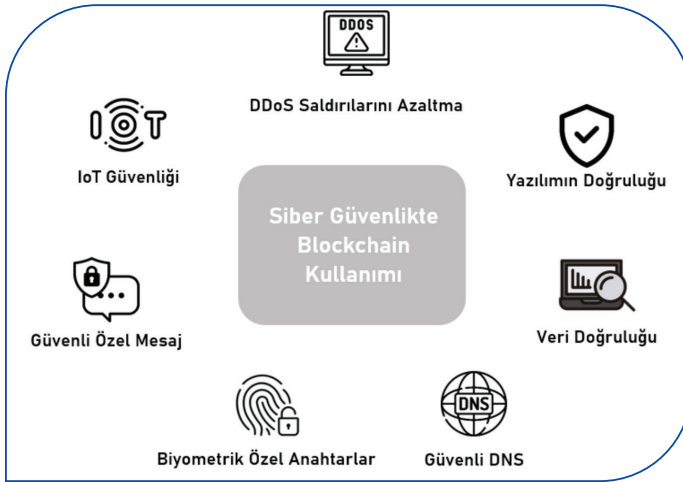
Zincirleme özelliği ile her işlem blok halinde birbirine bağlı olarak şifrelenip dizilir. Bu işlem, son bloğun değişmez olmasını sağlayarak veri güvenliğini sağlar.

Dağıtılmış ağ özelliği ile esneklik sağlarken veriyi bulut sunucusunda depolamak yerine tüm bilgisayar ağlarına dağıtır. Böylece merkezi bir kontrol noktası olmadan ağda birbirine bağlı bloklarda veri depolanır. Bu, Blockchain'i güvenli kılan en önemli özellikten biridir. Çünkü bu ağı hackleyebilmek için kullanıcıların %51'ini hacklemek gerekir. Bu saldırı teorik olarak mümkün olsa da pratikte mümkün değildir. Bitcoin, Ethereum gibi Blockchain kapasiteleri ve işlem güçleri hesaplandığında, saldırıların başarılı olma ihtimali oldukça zayıf kalır.

Diğer bir yandan, siber güvenlik tehditlerine karşı katmanlı koruma sağlayan birden fazla şifreleme biçimi uygulanır. Şifreler kriptografik hash fonksiyonları ve asimetrik anahtar algoritmaları içerir ve bloklar dijital imza kullanılarak şifrenir. Hash fonksiyonları, istenilen veri üzerine koruyucu katman örer. Böylece bu verilere bir müdahale ya da değişiklik yapıldığında fark etmek oldukça kolay hale gelir.

Siber Güvenlikte Blockchain Kullanımı

Teknoloji hayatımıza dahil olurken yanında bazı tehditleri de getirmektedir. IoT, akıllı şehirler gibi teknolojik gelişmelerle hayatımız kolaylaşırken, veri güvenliği konularında da tehditler artmaktadır. Blockchain'in şeffaf ve merkeziyetsiz yapısı ile siber tehditler için çeşitli güvenlik servisleri sağlayacak çözümler yapmak mümkündür. Blockchain'in, kriptografik algoritmalar, hash fonksiyonları ve dijital imzalar gibi güvenlik yöntemlerini kullandığından bahsedilmişti. Bu yöntemler bankacılık, sağlık, finans, elektronik oylama, akıllı ev teknolojileri gibi güvenlik ve mahremiyetin önemli olduğu sektörlerde rahatlıkla kullanılabilir.



Mesajlaşma şirketleri, uçtan uca şifreleme ile veri güvenliğini artırmak amacıyla siber güvenlik tehditlerine karşı kalkan görevi gören Blockchain'e hızla geçmeye başlamıştır. Sosyal medya platformları başta olmak üzere kullanıcı bilgilerinin yanlış ellere geçmesiyle veri ihlallerine neden olan birçok saldırı gerçekleşmiştir. Bunları engellemek için Blockchain teknolojisi gelecek vadetmektedir. Bilgi güvenliğinin 3 temel ilkesinden biri olan gizlilik, verilere yalnızca ilgili ve yetkili kişilerin erişimini sağlar. Burada gizlilik ilkesine destek sağlamaktadır.

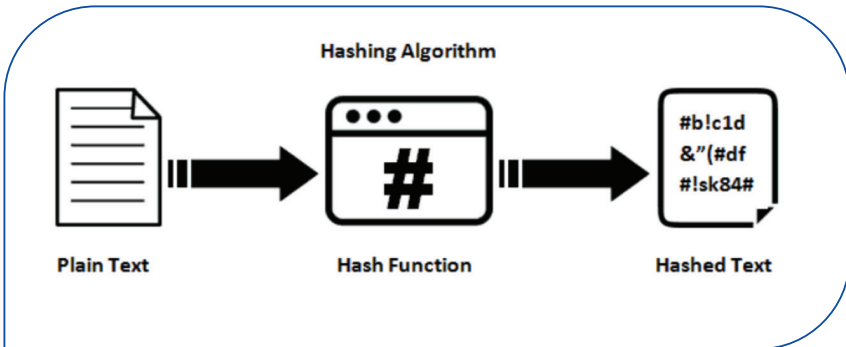
IoT (Nesnelerin İnterneti) kısmına baktığımızda akıllı anahtar, robot süpürge gibi savunmasız cihazlarla genel ev otomasyonuna erişim sağlamak artık bilgisayar korsanları için pek de zorlayıcı bir durum değil.

ABD'de bulunan Maryland Üniversitesi'nde yapılan bir araştırmada, robot süpür-gelerin evdeki sesleri dinleyerek kayıt altına alabileceği ortaya çıktı. Ev içinde ko-nuşulan her şey robot süpürge tarafından kaydedilebilirken, kişisel verilerin sızdırıl-ma tehlikesi söz konusu oldu.

Blockchain, yönetimlerini merkezi olmayan hale getirerek bu tür savunmasız sis-temleri ve cihazları korur. Yapay zeka ve IoT teknolojisi ile birleştirilen Blockchain, cihazların güvenlik kararlarını kendi başlarına vermelerini sağlar.

DNS, alan adlarının IP'ye dönüştürülmesi maksadıyla kullanılan ve 256 karaktere kadar da büyüyeabilen bir sistemdir. DNS girişlerinde yapılan yanlış bir yapılandır-ma, saldırganların IP adresi ile bir web sitesi adı arasındaki bağlantıya sızmasını sağlayabilir. Bu sızıntı ile kendi belirledikleri kötü amaçlı IP adreslerine kullanıcıları yönlendirirler. Hedeflenen kaynağa hizmet veya erişim reddedildiğinde bir DDoS saldırısı gerçekleşir. Bu tür saldırılar siteyi aşırı yükler, kaynak sistemini önemli ölçü-de yavaşlatır veya kapatır. İşte tam bu noktada Blockchain teknolojisi, DNS giriş-lerini merkezi olmayan hale getirerek bu tür saldırıları ortadan kaldırır. Bu şekilde de bilgi güvenliğinin kullanılabilirlik ilkesine fayda sağlamış olur. Şu da önemli bir detaydır ki, IoT (Nesnelerin İnterneti) birkaç bağlantılı sistemi etkileyebildiğinden DDoS saldırılarının %91 oranında artmasına sebep olmuştur.

Blockchain'in en önemli güvenlik parçasından biri de hash fonksiyonlarıdır. Alınan verinin, birçok matematiksel algoritma ile şifrelenerek çıktı haline getirilmesine hashing denir. Burada amaç verinin gizlenmesidir. Web sitelerinde şifre ile giriş yaparken, yazılan şifre önce hash'e dönüştürülür, daha sonra veri tabanına yazılır. Böylece veri tabanını inceleyen kişi kullanıcının şifresini görmemiş olur. Blockchain, hash fonksiyonlarını kalıcı ve değiştirilemez olarak kaydeder. Böylece Blockchain, defterde depolananlarla karşılaştırarak kimlik doğrulamada daha verimli olduđu-nu kanıtlamış olur. Burada ise bilgi güvenliğinin gizlilik ilkesine olan faydası net bir şekilde görülmektedir.



Blockchain'in veri bütünlüğünü koruma ve doğrulama gerçekleştirme özelliği, herhangi bir siber-fiziksel altyapının durumunun doğrulanmasına yardımcı olur. Blockchain aracılığıyla kaydedilen veriler, tüm doğrulamalar için daha fazla güvence sağlar. Böylece bilgi güvenliğinin bütünlük ilkesine de destek sağlanmış olur.

Bugün en etkili olduğu düşünülen bir siber güvenlik sistemi, yarın yetersiz kalabilir. Hiçbir siber savunma sisteminin %100 güvenli olmadığını kabul etmek gerekir. Fakat şu anda, her kuruluş mevcut en başarılı siber güvenlik çözümü benimsemeyi tercih etmektedir ve burada Blockchain göz ardı edilemeyecek kadar önemlidir. Blockchain'i nesnelerin interneti, yapay zeka ve makine öğrenmesi gibi diğer derin teknolojilerle birleştirerek güçlü bir teknik altyapı oluşturulabilir.

KAYNAKÇA

<https://www.disruptordaily.com/blockchain-use-cases-cyber-security/>
<https://bootcamp.cvn.columbia.edu/blog/blockchain-guide-to-skills/>
<https://www.siberportal.org/blue-team/blockchain/blockchain-uygulama-alanlari/>
<https://markvanrijmenam.medium.com/five-blockchain-trends-for-you-to-consider-this-year-cf78017f37>
<https://devrimdanyal.medium.com/blockchain-teknolojisi-siber-riskler-ve-sorunlara-genel-bak%C4%B1%C5%9F-96d1f352d6e5>
<https://dergipark.org.tr/tr/download/article-file/396266>
<https://mediatrend.mediamarkt.com.tr/blockchain-siber-guvenligin-gelecegini-nasil-etkileyecek/>
<https://www2.deloitte.com/tr/tr/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html>
<https://www.leewayhertz.com/blockchain-and-cybersecurity/>





SIZMA TESTİ RAPORU

Sızma testi süreci boyunca taraflar arasındaki iletişime çok dikkat edilmelidir. Görüşmeler mail ile sağlanmalıdır. Rapor yazılırken özen gösterilmelidir. Rapor taslağı kişi ve kuruma göre şekil alır ancak bilgileri eksiksiz iletmek esas önemli noktadır. Raporlama yapılırken dikkat edilmesi gereken hususlar şunlardır:

- Rapor Taslağı ve İçindekiler
- Üst ve Alt Bilgi Tasarımı
- Kapak Tasarımı
- Doküman Künyesi
- Tablo ve Şekil Listesi
- Yasal Sorumluluklar
- Yönetici Özeti
- Bulgu Kartı
- Rapor İletimi

Rapor Taslağı ve İçindekiler

Raporda içindekiler listesi olmak zorundadır. Üst ve alt başlıklar, sayfa sayıları dikkatle yazılmalıdır. Taslak rapor yazılırken sürekli güncellenmelidir.

Üst ve Alt Bilgi Tasarımı

Üst ve alt bilgi, raporun tüm sayfalarına uygulanır ve raporla ilgili bilgiler içerir. Bu bilgiler; “GİZLİ” ibaresi, testin adı, versiyon numarası, testi yapan firmanın logosu veya web site linki olabilir.

Kapak Tasarımı

Kapak test raporunun görselliği açısından oldukça önemlidir. Kapak rengi, testi yapan firmanın renkleriyle uyuşmalıdır. Kapakta testi yapan firmanın adı ve logosu, testin türü ve versiyonu, testin yapıldığı tarihler ve mutlaka “GİZLİ” ibaresi bulunmalıdır.

Doküman Künyesi

Doküman künyesi, rapor hakkında genel bilgiler vermektedir. Doküman künyesinde doküman başlığı, doküman numarası, ilk yayın tarihi, revizyon numarası, son revizyon tarihi, toplam sayfa sayısı, raporu yazan kişinin adı, testi

gerçekleştiren kişinin adı, raporu gözden geçiren kişinin adı, raporu onaylayan kişinin adı, raporun gizlilik derecesi bilgileri yer almalıdır.

Doküman künyesindeki raporu gözden geçiren kişi kesinlikle raporu yazmayan biri olmalıdır. Gözden geçiren kişi raporu detaylı bir şekilde kontrol edip raporu yazan kişiye geri bildirim vermelidir. Dört göz kontrolü süreci uygulanmalıdır. Raporu onaylayan kişi ya takım lideri ya da yönetici olmalıdır.

Doküman künyesindeki bilgiler detaylı olarak ifade edilerek kuruma hitap yazılmalıdır.

Tablo ve Şekiller Listesi

Rapor yazılırken sıklıkla tablo ve şekil kullanılmaktadır. Karmaşık yapıyı önlemek için tablo listesi ve şekil listesi oluşturulmalıdır. Şekiller tablosu oluşturulurken önemli husus eklenen resimlere “Resim Yazısı” eklemektir.

Yasal Sorumluluklar

Yasal sorumluluklar kısmı, tarafları yasal olarak koruyan ve raporun en kritik kısmıdır. Bu sebeple yasal sorumluluklar detaylı olarak ifade edilmelidir. Yasal sorumluluklar içeriği hazırlanırken bahsedilmesi gereken noktalar vardır. Bunlar; tüm bulguların %100 tespit edilememiş olması, testi yapan kurumun tüm zafiyetleri bulmayı garanti etmediği, olası saldırganların farklı bakış açısı ve tekniklerle tespit edilememiş zafiyetler bulabileceği, test yapıp rapor teslim edildikten sonra yapılan değişiklikler sebebi ile yaşanabilecek hack olaylarından testi yapan firmanın sorumlu tutulamayacağıdır.

Yönetici Özeti

Yönetici özeti bölümünün en önemli özelliği teknik dilden uzak olmasıdır. Özet sade ve anlaşılır bir dille yazılır. Yönetici özetinde zafiyetler, bulgulara ait detaylı özet, bulguların oranlarını açıklayan grafikler, testin kapsamı hakkında bilgiler bulunmalıdır.

Bulgu Kartı

Bulgu kartı hazırlanırken bulgunun adına, risk derecesine, zafiyetin etkisine, erişim ortamına, kullanıcı profiline, kullanılan araçlara, zafiyet türüne, etkilenen sistemlere, zafiyetin tanımına, zafiyetin detaylarına, çözüm önerilerine, referanslar ve iyi uygulama örneklerine yer verilmelidir. Bulgu adı verilirken

bulguyu en iyi tanımlayan alan seçilmelidir. Bulgu risk dereceleri acil, kritik, yüksek, orta, düşük olmak üzere 5 adettir. Bulgular risk seviyesine göre sıralanmalıdır.

- Acil (risk seviyesi:5) Acil öneme sahip açıklıklar, niteliksiz saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Depolanmış XSS, SQL enjeksiyonu ve RFI/LFI, ayrıca müşteri bilgisi ifşasına yol açabilecek açıklıklar bu kategoriye girerler.

- Kritik (risk seviyesi:4) Nitelikli saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Ayrıca yansıtılan ve DOM tabanlı XSS açıklık vektörleri bu kategoriye girer.

- Yüksek (risk seviyesi:3) Uzaktan gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan ataklara sebep olan açıklıkları içermektedir.

- Orta (risk seviyesi:2) Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan ataklara sebep olan açıklıkları içermektedir.

- Düşük (risk seviyesi:1) Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

Zafiyetin etkisinde risk seviyesine göre etkileri detaylı bir şekilde belirtilmelidir. Örnekleri şunlardır; bilgi açığa çıkarma, oturum bilgilerini çalma, yerel ağa sızma, hizmet kesintisi saldırıları.

Erişim ortamında testin gerçekleştirildiği yer bilgisi belirtilmektedir. Kurum dışı bir test gerçekleştirildiyse “İnternet”, kurum içi bir test gerçekleştirildiyse “İntranet” olarak işlenir.

Kullanıcı profilinde internet, intranet, sistem veya diğer şeklinde test yapılırken kullanılan kullanıcı bilgilerine yer verilir. Kullanılan araçlarda zafiyet tespiti yapılırken kullanılan araçların bilgisi yer alır.

Zafiyet türü, zafiyetin etkilediği bileşenleri içermektedir. Etkilenen sistemler yazılırken zafiyetin bulunduğu bileşenler port numarası ile belirtilmelidir.

Zafiyetin tanımı ve detayları yazılırken zafiyet tanım olarak açıklanır ve zafiyetin nasıl tespit edildiği tüm detayları ile açıklanır.

Çözüm önerileri bulgunun giderilmesi için detaylı olarak açıklanır. Referanslar ve iyi uygulama örnekleri, çözüm önerilerini destekleyici web adresleri başlıklar ile paylaşılır.

Rapor İletimi

Sızma testi raporları gizli olan dosyalardır. Bu sebeple taraflar arası iletimi yapılırken güvenli bir yol izlenmelidir. Dosya şifre ile korunmalıdır. Şifre kolay tahmin edilebilir olmamalı ve şifreli bir iletişim kanalı üzerinden yazılı veya sesli olarak iletilmelidir, sms kullanılabilir. Dosya yalnızca ilgili kişiye iletmeli ve herkese açık sunuculara yüklenmemelidir. Dosya iletdikten sonra taraflar arasında iletim teyit edilir ve rapor iletdiyse rapor dosyası sunucudan silinir. İletim tamamlandıktan sonra testi yapan firma imha prosedürü başlatır.

KAYNAKÇA

<https://www.disruptordaily.com/blockchain-use-cases-cyber-security/>

