Kötücül Saldırılar, Tehditler ve Güvenlik Açıkları

Bu bölümde kötücül amaçlı bir saldırı yapmak için kullanılan yazılım hakkında bilgi edineceksiniz. Bu yazılımlara kötücül yazılım (malware) denmektedir. Ayrıca saldırıların farklı türlerini öğreneceksiniz, internet yeni ve henüz oturmamış bir alandır. Bu alanda bilgilerinizi çalmaya çalışan birçok kötü insan bulunmaktadır. Eğer cihazlarınız veya hassas bilgileriniz internete açık ise kayıp veya zarar riskiniz olacaktır. Günlük yaşamınızdan farklı olarak, siber dünyada herkesin uymak zorunda olduğu yasalar yoktur. Size zarar verecek faaliyetler ve hırsızlıklar gündelik olaylardır. Bu tür olaylar şirketleri, kişileri ve hatta devletleri de etkilemektedir. 2014 yılının sonunda Sony Pictures Entertainment'in hacklenmesinde olduğu gibi, bu tür suçlar genelde cezasız kalmaktadır.

Kötücül saldırılar her yıl milyarlarca dolarlık zarara neden olmaktadır. Neyse ki, birçok şirket ve sizin gibi kişiler Bilgi Teknolojileri - BT (Information Technologies - BT) varlıklarını saldırılardan korumak için çaba sarf etmektedir. Bu bölümde, güvenlik açıklarını tanımlamayı, kurumunuzu tehditlerden korumayı ve bilgisayarınızı kötücül saldırılardan güvende tutmayı öğreneceksiniz.

Kötücül Faaliyet Artmakta

Muhtemelen siber saldırıların haberlerini izlemiş, TV'de reklamlarını görmüş veya gazetelerde manşet başlıklarını fark etmişsinizdir. Bir örnek: Yakın bir zamanda, bir üniversite öğrencisi Amerika Birleşik Devletleri başkan yardımcısı adayının e-posta hesabına sızdığı için 20 yıl hapse çarptırıldı. Benzer bir olayda, bir tekstil firması olan TJX şirketi milyonlarca müşterisinin kredi kartı numarasının çalınmasına neden olduğunu kabul etti. Bir ticari reklam filminde saf bir çalışan “zararsız” bir e-posta bağlantısına tıklayarak bütün şirkete bir virüs saldırısı başlatmaktadır. Etrafınızdaki her alanda, bilişim güvenliği çalışanlarının durdurmak zorunda olduğu kötücül saldırıları göreceksiniz. Haberler son zamanlardaki veri ihlalleri ile doludur. Hiçbir şirket veya kişi dijital verilerin veya dijital kimlik bilgilerinin çalınmasının getirdiği risklerden korunmuş değildir.

Bu tür saldırılar habercilerin ve kamunun dikkatini çekse de, çoğu zaman siber saldırıların kurbanları başlarına geleni hiç kimseye duyurmazlar. Dünya genelindeki sistemler her gün tehdit altındadır. Çoğu durumda bu tür saldırılardan haberdar olanlar yalnızca güvenlik uzmanları ve BT çalışanlarıdır. Güvenlik uzmanları, sistemleri tehditlerden korumak ve gerçekleşen kötücül saldırıların etkilerini de hafifletmekle sorumludurlar. Bilgisayar sistemlerini korumanın en etkili yollarından biri sistemdeki açıkların BT altyapısında hızlıca ve etkili bir biçimde giderilmesini sağlamaktır.

Aşağıdaki tabloda Bloomberg Business tarafından Nisan 2013 yılında belirlenen en fazla saldırı gerçekleştiren ilk 10 ülkeyi göstermektedir. 2013 yılında Çin yüzde 41 ile dünyanın en fazla saldırı gerçekleştiren ülkesidir. ABD yüzde 10 ile ikinci sıradadır. Saldırının başlatıldığı yeri bulmak zor olabilmektedir. Özellikle, botnetler kullanılıyorsa daha da zor olmaktadır. Botnet, uzaktaki bir bilgisayar korsanının (hacker) kontrol ettiği birbirine internet üzerinden bağlı bir grup bilgisayardır. Uzaktaki bilgisayar korsanı başka bir ülkede yaşasa dahi bu botnet ile birbirine bağlı bilgisayarları kullanarak bir saldırı başlatabilmektedir. Bu durumda, saldırıyı gerçekleştireni bulmak ve yakalamak zor olabilmektedir.

KAYNAK	SALDIRI PAYI (%)
Çin	%41
ABD	%10
Türkiye	%4,7
Rusya	%4,3
Tayvan	%3,7
Brezilya	%3,3
Romanya	%2,8
Hindistan	%2,3
İtalya	%1,6
Macaristan	%1,4

Bloomberg Business Verilerine Göre En Çok Saldırı Düzenleyen 10 Ülke 2013.

Neyi Korumaya Çalışıyorsunuz?

Kısaca, değerli varlıklarınızı korumaya çalışıyorsunuz. Bir varlık (asset) değer taşıyan herhangi bir şey olabilir. Bir organizasyondaki her şeyin bir değeri olsa da, varlık kelimesi genellikle ciddi değeri olan öğeler için kullanılmaktadır. Bir kurumun varlıkları aşağıdakileri içerebilmektedir:

- Müşteri verisi - İsim, adres, telefon, sosyal güvenlik numarası (Social Security Number - SSN), doğum tarihi, kart sahibinin verileri, korunan sağlık bilgisi kayıtları.
- BT varlıkları ve ağ altyapısı - Donanım, yazılım ve hizmetler.
- Fikri mülkiyet - Patentler, yazılım kodu, formüller veya mühendislik planlan gibi hassas veriler.
- Mali durum ve mali veriler - Banka hesapları, kredi kartı bilgileri ve mali işlem verileri.
- Servis kullanılabilirliği ve verimlilik - Hesaplama servislerinin ve yazılımlarının insanların ve makinelerin verimliliğini desteklemesi kabiliyeti.
- İtibar - Şirket çalışanlarının yasa ve kurallara uyumu (kurumsal uyum) ve marka imajı.

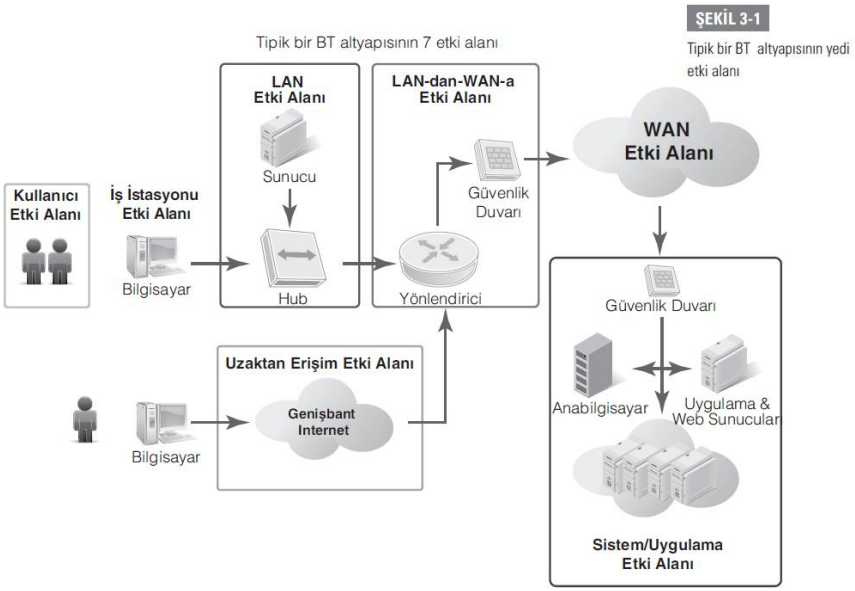
Bu varlık türlerine ayrı ayrı bakalım ve kötücül saldırılara nasıl maruz kalabileceklerini tartışalım.

Müşteri Verileri

Medya kaynakları bir veri ihlalinde çalman bilgileri haber yapmayı çok severler. Müşteri kişisel verisinin, kart sahibi bilgilerinin veya elektronik ortamda korunan kişisel sağlık hizmetleri veri unsurlarının kaybolması etkileri nedeniyle kısa sürede manşetlere taşınmaktadır. Günümüzün dijital çağında, müşterinin kişisel verileri başka bir şahıs tarafından çalınmaya ve istismara açıktır. Kimlik bilgileri çalınarak başka bir kişi taklit edildiğinde oluşan duruma kimlik hırsızlığı (identity theft) denmektedir. Müşteri kişisel verileri müşterinin adı ve soyadı, ev adresi, telefon numarası, doğum tarihi, sosyal güvenlik numarası veya kart bilgilerini içerebilir.

BT ve Ağ Altyapısı

Yazılım ve donanım bir kurumun bilişim altyapısının temel bileşenleridir. **Aşağıdaki şekilde** genel bir BT altyapısı çerçevesinin yedi etki alanım göstermektedir. Her etki alanının parçaları bir ağa veya internete bağlanabilir. BT altyapısının internete bağlı olması nedeni ile BT altyapısının hem içerisine hem de dışarısına yönelik tehditler olabilmektedir.



Veriye zarar veren yeni tehditler, zırhlı virüsler (armored virus), fidye yazılımları (ransomware) ve kötücül kripto-kilitleyici yazılımlarını (cryptolocker malware) içermektedir; bu zararları düzeltmek veya değiştirmek şirketlere zaman ve maliyete mal olabilir. Zırhlı virüsler, kodlarının tersine mühendislikle (reverse engineering) okunmasını ve kötücül yazılım için bir antivirüs oluşturmayı zorlaştıran güçlendirilmiş koda (hardened code) sahiptirler. Fidye yazılımları, bir zaman saatiyle bağlantılı yeni bir malware formudur ve kurban kuruluşu verilerinin silinmesini önlemek için fidye ödemeye zorlar. Kripto kilitleyici, deşifreleme (decryption) anahtarlarını elde etmek için kurban fidye ödeyinceye kadar kritik dosyaları veya verileri şifreleyen özel bir fidye yazılımı biçimidir. Kritik donanım ve yazılım sistemlerine yönelik kötücül saldırılar,

kuruluşlar içerisinde geniş çaplı sorunlara neden olabilir. Bu sorunlar kritik verilerin kaybolmasını veya mali bilgilerin veya fikri mülkiyetin çalınmasını içerebilir. Korunmayan BT ve ağ altyapısı varlıkları, saldırganlara ve siber suçlulara hassas kaynaklara erişmek için en geniş açıklıkları sunabilir. Bu erişim kolaylığı, internete bağlı varlıkları saldırıların en sık yapıldığı ilk nokta haline getirir. Bu durum, katmanlı bir güvenlik yapısı oluşturmak için en değerli varlıklarınızı BT altyapısının erişilmesi en zor kısımlarına koymanız gerektiği anlamına gelmektedir. Katmanlı güvenlik savunmaları yeni, çok biçimli kötücül yazılımların (polymorphic malware) gelişmişliği göz önüne alındığında kritik bir öneme sahiptir. Çok biçimli kötücül yazılım, şekil değiştirip farklı biçimlere girebileceği ya da değişebileceği için anti virüs ve kötücül yazılımla mücadele uygulamaları ile tespit edilmesi ve temizlenmesi zorlaştığından zararlıdır.

> *Şubat 2016'da Hollywood Presbiteryen Kilisesi Tıp Merkezi kripto-kilitleyici kötücül yazılım kullanan bir fidye yazılımının kurbanı oldu. Bir kripto-kilitleyici yazılım kritik önemdeki dosyaları şifreleyerek sistemi kilitler ve şifreleme anahtarını vermek için fidye talep eder. Hollywood şifreleme anahtarını elde etmek için 17000 doları Bitcoin ile ödemeyi seçti. Hastane fidyeyi ödemeye ve normal işlemlerine dönmeye karar verdi. Bu durumda, bir veri ihlali oluşmasa da kritik önemdeki dosyalar şifrelendikleri ve kullanılamaz hale geldikleri için bu olay bütün bilgisayar sistemlerinin kontrolünün tamamıyla kaybedilmesiyle sonuçlandı.*

Fikri Mülkiyet

Fikri mülkiyet (intellectual property) pek çok kurumun temel taşıdır. Fikri mülkiyet kurumun bir varlığıdır. Bu varlık, özgün bir üretim süreci veya müşteri verisi gibi gerçek bir veri de olabilir. Fikri mülkiyet örnekleri olarak patentler, ilaç formülleri, mühendislik planları, bilimsel formüller ve tarifler verilebilir. Örneğin, bir restoran zincirinin yiyecek hazırlamak ve teslimatı hızlı bir biçimde yapmak için özgün bir sürece sahip olduğunu düşünelim. Eğer piyasadaki rakipleri sahip olunan bu süreci öğrenirlerse, restoran rekabet üstünlüğünü kaybedebilir. Dijital dünyada veri en değerli varlıktır. Ne kadar veriniz varsa o kadar değerlisiniz. Ayrıca, eğer verinizin üst verisi (metadata) varsa, verinize ek değer katabilir.

Haber manşetlerinde neler okuyorsunuz? Veri ihlalleri ya da veri kayıpları hayatın her alanında her gün gerçekleşmektedir. Bu tür kayıplar, kimlik hırsızlığı, iş hırsızlığı ya da fikri mülkiyetin çalınmasını içermektedir. Veri ihlalleri sıklıkla gerçekleşmektedir. Bir bilgi sistemleri güvenliği uzmanı olarak göreviniz, varlıklarınızda bir veri ihlali olmasını önlemektir. Bu sizin bir numaralı hedefinizdir.

BT güvenliği açısından temel sorun, fikri mülkiyet hırsızlığından korunmak ve bunun rakiplere ya da kamuya açıklanmasını önlemektir. Fikri mülkiyetin çalınması, kurumun rekabet avantajını etkisiz bir duruma getirebilir. Örneğin, Alpha İlaç Şirketi isimli bir şirketin, piyasaya sürdüğünde 10 milyar dolar kazanmayı hedeflediği yeni bir ilacı 2 milyar dolar yatırım yaparak geliştirdiğini düşünün. Şirket ilacı tam piyasaya sürecekken, Beta İlaç Şirketi'nin Alpha'nın formüllerini ele geçirip kendi versiyonu olan ürünü piyasaya aceleyle sürdüğünü düşünün. Alpha, ARGE yatırımları ve yeni ilaç geliştirmek için önemli meblağlar harcamasına rağmen ilk pazar avantajını kaybedecektir. Fikri mülkiyetin korunması her kurumun en fazla önem verdiği konudur.

Mali Durum ve Mali Veriler

Mali varlıklar her kurumun en önemli varlıkları arasındadır. Bu varlıklar çeşitli biçimler alabilirler. Bunlar; banka hesapları, ticaret hesapları, alım hesaplan, şirket kredi kartları ve diğer para ve kredi kaynakları gibi finansal varlıklar olabilmektedir. Alternatif olarak, bu varlıklar gerçek mali varlıklara erişime izin veren veriler de olabilir. Mali veriler, müşteri kredi kartı numaralarını, kişisel mali verileri veya yatırım hesapları ya da bankacılık için kullanılan kullanıcı adlan ve parolalar olabilir. Diğer mali veri örnekleri, banka ve şirketlerin kendi aralarındaki finansal veri transferlerinde kullandıkları işlem verisini içermektedir. Bunlar, elektronik ödemeler ya da para transferleri için kullanılan elektronik veri değişimi (electronic data interchange – EDI) numaralarını veya otomatik takas merkezi (automated clearinghouse – ACH) işlemlerini içerebilmektedir.

Mali varlıkların kötücül saldırılar nedeniyle kaybı tüm kurumlar için en kötü senaryodur. Bu durum sadece fiziksel kayıplara neden olmamakta, ayrıca kurumun şöhretine ve marka imajına da uzun vadeli etkileri olabilmektedir.

Hizmet Kullanılabilirliği ve Verimlilik

Bilgisayar uygulamaları kurumların iş ilişkilerinin yönetiminde yardımcı olan özgün hizmetler sunarlar. Kurum her ihtiyaç duyduğunda bu kritik hizmetlerin kullanılabilir olması önemlidir. Bir hizmetin arıza veya bakımı

nedeniyle sunulamadığı süreye kesinti (downtime) denir. Kesinti, kasıtlı ya da kasıtsız olabilmektedir. Çoğu zaman, sistem yöneticileri kasıtlı kesintileri önceden planlarlar. Örneğin, sunucular işletim sistemi güncellemelerine veya yamalarına ihtiyaç duyduğunda, sistem yöneticileri sunucular üzerinde ilgili işlemleri problem çıkarmadan gerçekleştirebilmek için sistemleri kasıtlı olarak çevrim dışı (offline) duruma getirirler. Yöneticiler kasıtlı kesintiyi planladıklarında, bu planlamanın kurumdaki etkisini en aza indirmeye çalışırlar. Sistem yöneticileri kesintinin etkisini, işletmenin kritik işlemlerini aksatmayacak şekilde yönetmeye çalışırlar. Siz de, örneğin kritik bir yazılımın hafta sonu güncellenmesi ya da e-posta sistemleri gibi sistemlere yamaların gece yarısı uygulanması gibi kasıtlı kesinti senaryolarını biliyorsunuzdur.

Kasıtsız kesinti genellikle teknik arızalar, insan hataları veya saldırılar nedeniyle oluşmaktadır. Teknik arıza ve insan kaynaklı hatalar kasıtsız kesintinin en yaygın nedenleridir. Kötücül saldırılar nedeniyle oluşan kesinti daha az yaygın olsa da, araştırmalar bu saldırıların hızla arttığını göstermektedir. Kötücül saldırılar BT altyapısının yedi etki alanından herhangi birinde gerçekleşebilir ve kesintiye neden olabilir. Kötücül saldırılar genellikle, Kullanıcı, iş istasyonu, LAN ve LAN'dan WAN'a etki alanlarını hedeflemektedirler.

Fırsat maliyeti (opportunity cost) bir şirketin kesinti nedeniyle kaybettiği para miktarıdır. Kesinti ister kasıtlı ister kasıtsız olsun, her iki türlü de sistem kullanılabilirliğini etkilemektedir. Bazı kurumlar fırsat maliyetine gerçek kesinti maliyeti de (true downtime cost) demektedir. Fırsat maliyeti genellikle kesinti nedeniyle kurumda yaşanan üretim kaybını ölçmektedir. Örneğin, büyük bir hava yolu şirketinin rezervasyon sunucularının çalışmadığını düşünün. Sunucular çalışmadığında, müşteriler bilet alamazlar. Bu kesintinin fırsat maliyetini satılamayan biletlerin toplam ücreti olarak ölçebilirsiniz. Kasıtsız kesintinin fırsat maliyeti genellikle kasıtlı kesintinin fırsat maliyetinden çok daha fazladır. Fırsat maliyeti bilgi güvenliği uzmanları için ciddi bir sorundur. Bu maliyet, siber suçlar ve kötücül saldırılarla mücadelede kaybedildiği tahmin edilen yıllık 1 trilyon doların büyük bir kısmını oluşturmaktadır.

İtibar

Bilgi güvenliği uzmanlarının korumaya çalıştıklarının en önemlilerinden biri kurumun itibarı ve marka imajıdır. Güvenlik açıkları ve zararlı saldırılar nedeniyle sahip oldukları varlıklar tehlikeye düşen şirketler kamuoyunda oluşan ciddi olumsuz sonuçlarla karşılaşmaktadırlar. Örneğin, kullanıcı kredi kartı verisinin çalınmasına ve bu verinin uluslararası ölçekte dağılmasına izin veren bir güvenlik açığı şirketin itibarına ve marka imajına ciddi zarar verecektir. Şirket çabucak önlem alsa ve sorunu etkili bir biçimde çözse de, şirkete ve markalarına yönelik kamudaki olumsuz algı uzun süre kalabilecektir. Diğer sonuçların yanı sıra, bu durum, kurumun gelir, net değer ve piyasa değerinde bir düşüşe neden olabilir.

> *Bir veri ihlali politikası ve usulü, bir veri ihlalini yönetmek için kuruluşunuzu hazırlayacaktır. Bu tür bir politika, müşteriler, düzenleyici kurumlar ve sigorta şirketleri ile iletişimi içermektedir. Eğer kuruluşunuz yasalara uygunluk gereksinimleri altındaysa, veri ihlali bildirimi için yasal zorunluluklara tabii olabilirsiniz. Hukuk personeli de dahil olmak üzere yönetici kadro, gerçekleşen bir veri ihlali ile ilgili olarak kuruluşun yönetim kuruluna özel tavsiyelerde bulunurlar. Bir veri ihlalinin düzgün bir şekilde ele alınması, ilgili hukuki tavsiyelerle birlikte yapılmalıdır.*

Kimi yakalamaya çalışıyorsunuz?

Popüler kullanımlarda ve medyada, bilgisayar korsanı (hacker) terimi genellikle bir bilgisayar sistemine yetkilendirilmeden giren birisini tanımlar. Çoğu durumda, bilgisayar korsam ağ üzerinden ya da bir yazılım çatlağı (software crack) yoluyla uzaktaki bir bilgisayarın kontrolünü ele geçirmeye çalışmaktadır. Medya ve kamuoyu ayrıca terörizm, vandalizm, kredi kartı dolandırıcılığı, kimlik hırsızlığı, fikri mülkiyet hırsızlığı veya başka birçok suç biçiminden biri için teknolojiyi kullanmaktan dolayı suçlanan kişileri tanımlamak için bilgisayar korsanı terimini kullanmaktadır. Bilgisayar dünyasında bilgisayar korsanı kelimesi genellikle, bilgisayar sistemleriyle ilgili olarak, bir şeyi nasıl değiştireceğini araştırmayı ve iğrenmeyi seven bir kişiyi tanımlamaktadır. Bilgisayar korsanları, iyi ya da kötü, uzman ve tamirci olarak kabul edilmektedirler ancak basının bu terime olumsuz bir anlam yüklemesi nedeniyle bilgisayar korsanları sıklıkla bazı tartışmalara konu olmaktadırlar.

Bilgisayar korsanlarını aşağıdaki gibi sınıflandırılabilir:

- Siyah şapka bilgisayar korsanları (Black-hat hackers): Bir siyah şapka bilgisayar korsanı, teknik hünerlerini göstermek için BT güvenliğini kırmaya çalışmakta ve yetkilendirmesiz olarak sistemlere

girmeye çalışmaktadır. Siyah şapka bilgisayar korsanları güvenlik açıklarından yararlanmak için genellikle özel yazılım araçları geliştirmekte ve kullanmaktadırlar. Siyah şapka bilgisayar korsanları genellikle sistemlerdeki açıklardan faydalanmaktadırlar fakat buldukları güvenlik açıklarını genellikle bu sistemlerin yöneticilerine bildirmeye çalışmamaktadırlar. Güvenlik kavramının aksine, bilgi işlem kaynaklarının ücretsiz ve açık olarak kullanılmasını teşvik etme eğilimindedirler.

- Beyaz şapka bilgisayar korsanları (White-hat hackers): Bir beyaz şapka bilgisayar korsanı ya da etik bilgisayar korsanı, güvenlik açıklarını tanımlamak ve sızma testi (penetration test) gerçekleştirmek için yetkisi olan bir bilgi sistemleri güvenliği uzmanıdır. Siyah şapka bilgisayar korsanları ve beyaz şapka bilgisayar korsanları arasındaki fark, beyaz şapka bilgisayar korsanlarının güvenlik zayıflıklarını düzeltmek için belirlemesi, siyah şapka bilgisayar korsanlarının güvenlik zayıflıklarını sadece eğlencesine ve bu zayıflıkları kullanmak için bulmasıdır.
- Gri şapka bilgisayar korsanları (Gray-hat hackers): Bir gri şapka bilgisayar korsanı, bir gün siyah şapka bilgisayar korsanı olabileceği gibi beyaz şapka bilgisayar korsanı da olabilecek, yetenekleri ortalama seviyede olan kişilerdir. Bir diğer ortak tanıma göre, keşfedilen güvenlik açıklarını belirleyen ancak kullanmayan, ancak yine de güvenlik açıklarım açıkça ifşa etmediği için bir ödül bekleyen bir bilgisayar korsanıdır. Bu tip bilgisayar korsanları için ortak-bir tanım bulunmamaktadır.

Bilgisayar korsanları, kırıcılardan (cracker) farklıdır. Bir kırıcının düşmanca bir niyeti vardır, gelişmiş yeteneklere sahiptir ve mali kazançla ilgilenebilir. Kırıcılar ağlara ve bilgi kaynaklarına yönelik en büyük tehdidi temsil etmektedir. Bu tehditler genellikle dolandırıcılık, veri hırsızlığı, verilerin tahrip edilmesi, erişimin engellenmesi ve diğer kötücül faaliyetleri içermektedir. Bununla birlikte, bilgisayar korsanlarının faaliyetleri de hasar ve kayba neden olabilmektedir.

> *Bir başka saldırgan türü betik keratalarıdır (script kiddies). Bir betik keratası, bilgisayar korsanı olmaya çalışan özenti (wannabe), herhangi bir yaştaki az yetenekli ya da yeteneksiz bir kişidir. Bu kişi, bir siber saldırı gerçekleştirmek için, gerçekleştirdiği adımların anlamını tam olarak anlamaksızın, sadece talimatları izlemekte ya da "yemek kitabı" yaklaşımını kullanmaktadır.* ☺

Kötücül Saldırılar, Tehditler ve Güvenlik Açıkları

Saldırı Araçları

Bir kurumun varlıklarını ve BT alt yapısını korumak için saldırganların nasıl düşündükleri konusunda biraz fikir sahibi olmanız gerekmektedir. Bir saldırının nasıl düzenlendiği ve hangi araçların kullanıldığını bilmek bir savunma planı yapmaya yardımcı olacaktır. Aslında, birçok kurum sistemleri üzerindeki zayıflıkları bulmak için saldırganların kullandığı araçların aynısını kullanmaktadır. Kendi sisteminizdeki zayıflıkları saldırganlardan önce bulmak her zaman daha iyidir ancak bu zayıflığı bir an önce gidermek daha da önemlidir.

Bilgisayar suçluları ve siber saldırganlar, kullanılabilir zayıflıkları bulmak için birtakım donanım ve yazılım araçlarını ve asıl saldırıyı gerçekleştirmek için de başka araçlar kullanmaktadır. Bu araçlar ve teknikler aşağıdakileri içerebilmektedir:

- Protokol çözümleyiciler (protocol analyzers)
- Port tarayıcılar (port scanners)
- İşletim sistemi parmak izi tarayıcıları (OS fingerprint scanners)
- Güvenlik açığı tarayıcıları (vulnerability scanners)
- İstismar yazılımı (exploit software)
- Otomatik numara çeviricileri1 (wardialers)
- Parola kırıcılar (password crackers)
- Tuşa basma kaydedicileri (keystroke loggers)

Protokol Çözümleyiciler

Bir protokol çözümleyicisi (protocol analyzer) veya paket koklayıcı (packet sniffer) (veya sadece koklayıcı-sniffer), bir bilgisayarın LAN veya kablosuz bir ağda olsun veya olmasın, ağ trafiğini izleyip yakalamasını sağlayan bir yazılım programıdır. Saldırganlar şifreleri ve açık metin verileri yakalayabilmekte ve bozabilmektedir. Protokol çözümleyicileri yazılım, donanım veya hem yazılım hem de donanım birleşimi

[1] Bir modeme bağlanan telefon numaralarını bulmak için kullanılan, genellikle başkalarının bilgisayarlarına izinsiz olarak girmek isteyen biri tarafından kullanılan bir programdır.

şeklinde olabilmektedir. Yoklayıcılar karışık modda (promiscuous mode[2]) çalışırlar; bu da her veri paketinin koklayıcı tarafından görülebileceği ve yakalanabileceği anlamına gelmektedir. Koklayıcılar çerçeve (frame) ve IP veri paketini çözmekte, şifrelenmemişse verileri açık metin olarak görmenize olanak tanımaktadır.

Port Tarayıcılar

Bir port tarayıcı (port scanner), IP sunucu cihazlarındaki etkinleştirilmiş açık portları taramak için kullanılan bir araçtır. Bir port numarasını bir hizmetle yaygın şekilde ilişkili bir kanal olarak düşününüz. Örneğin, Port 80 http web trafiği için, Port 21 Dosya Transfer Protokolü (File Transfer Protocol - FTP), ve Port 23 Telnet içindir. Artık RFC 3232 olarak bilinen Yorumlar için İstek (Request for Comments - RFC) 1700, en yaygın TCP/UDP bağlantı noktası numaralarını ve hizmetleri listelemektedir. Port tarayıcıları, IP sunucu cihazında etkinleştirilen açık portları veya uygulamaları ve hizmetleri tanımlamak için kullanılmaktadır. Bu, saldırgana saldırıda kullanılabilecek değerli bilgiler sağlamaktadır.

İşletim Sistemi Parmak İzi Tarayıcıları

Bir işletim sistemi parmak izi tarayıcısı (Operating System - OS fingerprint scanner) bir saldırganın bir IP sunucu cihazına değişik türlerde paketler göndererek gelen cevaplardan hedef cihazın işletim sistemini (Operating System - OS) tahmin etmesini sağlayan bir yazılımdır. Ağ protokolleri genel olarak standart olsa da, farklı işletim sistemi satıcıları uygun gördükleri şekilde bunları hayata geçirebilirler. İşletim sistemi parmak izi tarayıcısından gönderilen paketler, iş istasyonlarında, sunucularda ve ağ cihazlarında kullanılan çeşitli işletim sistemlerinden gelen farklılıkları ayırt edecektir. Bir IP sunucu cihazı yanıt verdiğinde, OS parmak izi tarayıcısı hangi işletim sisteminin cihaza yüklendiğini tahmin edebilmektedir. Bir saldırgan, hangi OS ve sürümün yüklendiğini bildikten sonra, uygulanabilir yazılım güvenlik açıklarını ve istismarlarını kullanabilmek için daha fazla şansı olacaktır. Bir yazılım güvenlik açığı (software vulnerability), programdaki bir hata veya zayıflıktır. Bir istismar (exploit) saldırganın bir güvenlik açığı bulduğunda yapabileceği bir şeydir.

Güvenlik Açığı Tarayıcıları

Bir güvenlik açığı tarayıcısı (vulnerability scanner) bir IP sunucu cihazında var olan güvenlik açıklarını tanımlamak ve mümkün olduğunda doğrulamak için kullanılan bir yazılım programıdır. Bu bilgiden, bir güvenlik açığı tarayıcısı veri tabanındaki bilinen yazılım güvenlik açıklarını bulduğu şeyle karşılaştırır. Güvenlik açığı tarayıcısı bilinen tüm yazılım güvenlik açıklarını listelemekte ve bunları kritik, büyük ya da küçük olarak önceliklendirmektedir.

Bilinen yazılım açıklarının ve etkilenmelerin tam ve güncellenmiş bir listesi için https://cve.mitre.org adresini inceleyiniz. Yaygın Güvenlik Açıkları ve Etkilenme (Common Vulnerabilities & Exposures - CVE) listesi, ABD Ulusal Güvenlik Bakanlığı (U.S. Department of Homeland Security) adına, Mitre Şirketi tarafından tutulmakta ve yönetilmektedir. Bu liste günümüzde Ulusal Güvenlik Açıklar Veri tabanı (National Vulnerability Database-NVD) olarak bilinmektedir.

> *NVD (https://nvd.nist.gov) Güvenlik içerik Otomasyon Protokolü'nü (Security Content Automation Protocol- SCAP) kullanarak temsil edilen ABD hükümetinin standartlara dayalı güvenlik açığı yönetim verileri deposudur. Bu veriler güvenlik açığı yönetimi, güvenlik ölçümü ve uyumluluğunun otomatikleştirilmesini sağlamaktadır. NVD, güvenlik kontrol listeleri, güvenlikle ilgili yazılım kusurları, hatalı yapılandırmalar, ürün adları ve etki metrikleri veri tabanları içermektedir.*

İstismar Yazılımları

Bir istismar yazılımı (exploit software) bilinen yazılım açıklarını, verileri ve kod betiklerini birlikte kullanarak bir IP aygıtındaki veya bilgisayar sistemindeki zayıflıkları istismar eden bir yazılımdır. Bazı tür kötücül amaçları gerçekleştirmek için kullanılabilen bir programdır. Bu kötücül amaçlar, hizmet reddi saldırıları, izinsiz erişim saldırıları, brute force parola saldırıları (brute-force password attack) ve arabellek taşması (buffer overflow) saldırılarını içerir. Unutmayınız ki, yazılım güvenlik açıkları sistemde yazılım hatası (software bug), arka kapı açığı (back door vulnerability), kısa süreli program arızası (glitch) gibi zayıflıklar yaratmaktadır.

Bir saldırgan güvenlik açıkları değerlendirmesi yaparken ve izinsiz sızma testi (intrusive penetration test) gerçekleştirirken istismar yazılımlarını kullanacaktır. Güvenlik açığı değerlendirmesi bir açığı belirleyebilir, sızma testi ise bu açığı istismar etmeye çalışarak açığın varlığını teyit edecektir. Bu nedenle, sızma testi kötücül

[2] Ağ kartının çalışma modlarından bir tanesidir. Ağ kartının, hedefi neresi olursa olsun aynı alt ağdaki (subnet) tüm paketlerin bir kopyasını kendi üzerine almasıdır.

ağ trafiğine neden olur. Sızma testi siyah şapka veya beyaz şapka bilgisayar korsanlarının bir bilgisayar sistemine veya IP cihazına sızmak için gerçekleştirdiği eylemdir. Bu hem sisteme erişimi, hem de siyah şapka bilgisayar korsanlarının çoğunun en çok istediği şey olan veriye erişimi elde etmeye yol açabilir. Bir beyaz şapka bilgisayar korsanı, izin verilirse, keşfedilen bir güvenlik açığının gerçekten var olduğunu ve bunun sistemi kritik bir riske maruz bıraktığını doğrulamak için sızma testi yapabilir. Beyaz şapka bilgisayar korsanı daha sonra sızma testi sonuç değerlendirme raporunun bir parçası olarak maruz kalman risklerin giderilmesi için yollar önerir.

Otomatik Numara Çevirici

Bir Otomatik Numara Çevirici (wardialer) telefon numaralarını arayıp karşı tarafta bir bilgisayar bulmaya çalışan bir bilgisayar programıdır. Program otomatik olarak belli bir aralıktaki telefon numaralarını arayarak çalışır. Daha sonra karşı tarafta bir modeme başarıyla bağlanabildiği numaralan kaydeder ve bir veri tabanına girer. Otomatik Numara Çeviriciler dijital telefonların, IP telefonların ve IP üzerinden arayıcı (Voice over IP - VoIP) telefonların yaygınlaşmasıyla gittikçe demode olmakta ve ortadan kalkmaktadır. VoIP'den önce, saldırganlar Otomatik Numara Çeviricileri kullanarak özel santrallere (Private Branch Excharıge - PBX) erişerek çevir sesi almaya ve böylece uluslararası telefonlan ücretsiz aramaya çalışırlardı. Ek olarak, bir saldırgan Otomatik Numara Çevirici kullanarak analog modem sinyallerini bulmaya ve uzaktaki bir BT altyapısında bulunan bir sisteme erişim izni almaya çalışır.

Ayrıca, bazı Otomatik Numara Çeviriciler hem bir bilgisayarda çalışan işletim sistemini ayırt edebilir, hem de otomatik sızma testleri gerçekleştirebilir. Bu durumlarda, Otomatik Numara Çevirici önceden belirlenmiş bir listede bulunan yaygın kullanılan kullanıcı adlarını ve şifreleri deneyerek sisteme girmeye çalışır.

Ağa sızmaya çalışan bir saldırgan Otomatik Numara Çevirici kullanarak olası hedefleri belirleyebilir. Eğer program otomatik sızma testi sağlamıyorsa, saldırgan modemi şifresiz kullanıcı adları ile veya kolay kırılacak parolalarla hacklemeye çalışabilir. Bir ağ sistemi yöneticisi ticari bir Otomatik Numara Çevirici kullanarak kurum ağında bulunan izinsiz kurulmuş modemleri tespit edebilir. Bu izinsiz modemler saldırganlara kurumun iç ağına kolay erişim izni sağlayabilir. Bulunup kontrol edilmeli ya da ortadan kaldırılmalıdırlar.

Otomatik numara çevirmek oldukça eski bir yöntem olsa da hala bilgisayara giriş noktaları bulmada faydalıdır. Birçok bilgisayar ağı ve ses sistemi telefon hatlarına bağlı modemlere sahiptirler. Bu modemler çoğu zaman destek hattına doğrudan erişim için veya ağdaki erişim kısıtlamalarını geçmeye çalışan kişiler tarafından takılmışlardır. Bugünün internet ile birbirine bağlı sistemlerinde dahi diğer bilgisayarlardan gelecek çağrılara cevap vermeye hazır bir kaç modem olabilir. Bir bilgisayara modem kullanarak başarıyla bağlanmak kurum ağının diğer kısımlarına da olası bir erişim noktası sağlayacaktır.

Parola Kırıcılar

Parola kırmanın amacı unutulan veya bilinmeyen parolaları bulmaktır. Bir parola kırıcı (password cracker) iki amaçtan birine hizmet eden yazılım programıdır. Brute force parola saldırısı (Brute-force password attack) ile bir sisteme izinsiz giriş yapmak veya bir bilgisayar sisteminde kriptografik hash ile kaydedilmiş parolaları geri kurtarmak. Kriptografik hash büyük bir miktar veriyi tek bir (uzun) sayıya dönüştüren bir algoritmadır. Matematiksel olarak hashlendiğinde, hash değeri verinin bütünlüğünü (integrity) teyit etmekte kullanılabilir. Brute force parola saldırısı denemesinde ise bir saldırgan kırılan (cracked) parola sisteme giriş izni verinceye dek her olası karakter kombinasyonunu denemektedir. Sözlük saldırıları (dictionary attacks) deneme yanılma saldırılarının bir alt kümesidir. Bir sözlük parola saldırısında (dictionary password attack), bilgisayar korsanları gerçek kelimeleri de içeren (saldırının adı da buradan gelir) kısa ve basit birleşimleri denerler çünkü bu tür parolalar çok yaygındır.

Tuşa Basma Kaydedicileri

Bir tuşa basma kaydedici (keystroke logger) kullanıcının klavyede bastığı her tuşu bir kayıt dosyasına kaydedebilen bir takip yazılım veya donanımıdır. Tuşa basma kaydedici daha sonra almak için dosyayı yerel dizine kaydedebilir veya belirli bir alıcıya gönderebilir. İşverenler tuşa basma kaydedicilerini çalışanların iş bilgisayarlarını sadece iş amaçlı kullanmalarını sağlamak amacıyla kullanabilirler. Fakat, casus yazılımları da (spyware) parola gibi bilgileri bilinmeyen üçüncü kişilere göndermek için tuşa basma kaydedicileri içerebilirler. Bir donanım parçası olarak, tuş kaydedici kullanıcının klavyesi ve bilgisayarı arasında bağlantı görevi gören pil büyüklüğünde bir cihazdır. Bu cihaz sıradan bir klavye aparatına benzediği için, bir kişinin davranışlarını takip etmek isteyen birinin bu cihazı açıkça görünür bir yerde saklaması kolaydır. Ayrıca, iş

bilgisayarlarının klavyeleri genellikle bilgisayarın arkasına takılır, bu kaydedicinin fark edilmesini daha da zorlaştırır. Kullanıcı klavye tuşuna bastıkça, kaydedici her basılan tuşu alır ve bu bilgiyi metin olarak kendi içindeki küçük bir belleğe kaydeder. Daha sonra, tuşa basma kaydedicisini takan kişi geri dönmeli ve cihazın topladığı bilgiye erişmek için cihazı fiziksel olarak kaldırmalıdır.

Bir tuşa basma kaydedici yazılım programı genellikle kötücül Truva atı (Trojan) programları gibi gizlenir. Bu zararlı yazılım bir URL adresi, PDF dosyası veya ZIP dosyası ile hedefe iletilebilir. Saldırgan bir bilgisayara ağ üzerinden erişebildiği sürece, yürütülebilir (executable) dosyalar da dâhil olmak üzere her dosyayı transfer edebilir. Çoğu saldırgan sosyal mühendislik (social engineering) kullanarak kullanıcıları bu indirilen programları çalıştırmaya ikna eder. Kullanıcıların kendileri de farkında olmadan tuş kaydedicileri casus yazılımlar olarak indirebilirler ve bunlar daha sonra saldırganlar tarafından rootkit'in bir parçası olarak çalıştırılabilirler. (Rootkitler hakkında bu bölümün devamında daha fazla bilgi edineceksiniz.) Tuşa basma kaydedici program bir kullanıcının her bastığı tuşu kaydeder ve periyodik olarak bu kayıt bilgisini programı kuran kişiye internet üzerinden gönderir.

Güvenlik İhlali Nedir?

Bilgisayarları saldırılardan korumak için atılan en girişken adımlara rağmen, saldırganlar bazen başarılı olabilirler. Gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability) prensiplerinden herhangi birinin ihlaline neden olan her olay bir güvenlik ihlalidir (security breach). Bazı güvenlik ihlalleri sunulan hizmetleri kasten sekteye uğratır. Bazıları ise kaza sonucudur ve yazılım veya donanım arızalan nedeniyle oluşur. Bir güvenlik ihlali ister kaza sonucu ister kötücül olsun, bir kurumun hem iş yapabilme kabiliyetini hem de güvenilirliğini etkiler.

Güvenlik ihlallerine neden olabilecek olaylar aşağıdakileri içerir:

- Hizmet reddi (Denial of Service - DOS) saldırısı
- Dağıtık hizmet reddi (Distributed Denial of Service - DDOS) saldırısı
- Web'de uygunsuz gezinme davranışları
- İzinsiz dinleme (Wiretapping)
- Arka kapı (backdoor) kullanarak kaynaklara erişim
- Kaza sonucu oluşan veri değişiklikleri

Hizmet Reddi Saldırıları

Hizmet reddi (Denial of Service - DOS) saldırıları sistem kesintisi (downtime) veya bir kullanıcının sisteme erişememesi ile sonuçlanır. DOS saldırıları bilişim sistemleri güvenliğinin hizmet kullanabilme ilkesini etkiler. Bir DOS saldırısı büyük miktarda gereksiz işler yaptırıp bir bilgisayarı meşgul tutarak kullanılmasını engelleyen koordine edilmiş bir saldırıdır. Bu gereksiz ve fazla iş, sistemin asıl yapması gereken işleri yapamamasına neden olur. Bir disk dolduğunda, sistem kullanıcıya hesabını açtırmadığında, bir bilgisayar çöktüğünde veya bir işlemci çok fazla yavaşladığında bunun sonucu hizmet reddidir, saldırının adı da buradan gelir. Hizmet reddi saldırıları genelde tek bir bilgisayardan başlatılır. Bir hizmet reddi saldırısını tespit edince, kolayca durdurulabilirsiniz.

İki yaygın hizmet reddi saldırı türü şunlardır:

- Mantık saldırıları (Logic attacks) - Mantık saldırıları yazılım hatalarını kullanarak uzaktaki sunucuların performansını ciddi olarak azaltır veya çökertir. Bu tür saldırıların çoğunu kullandığınız yazılımı en son yamaları yükleyip güncel tutarak engelleyebilirsiniz.
- Taşkın saldırıları (Flooding attacks) - Taşkın saldırıları kurbanın bilgisayarının işlemcisini, belleğini veya ağ kaynaklarını büyük sayıda gereksiz istek göndererek sıradan isteklere cevap veremez hale getirir.

DOS saldırılarına karşı en iyi savunmalardan biri saldırı önleme sistemi (Intrusion Prevention System - IPS) yazılımlarını veya cihazlarını kullanmaktır. Saldırı tespit sistemleri (Intrusion Detection System - IDS) yazılım ve cihazları ayrıca hizmet reddi saldırılarını tespit edebilir ve bu tür saldırılar gerçekleşirken sizi uyarırlar. Bir önlem alınmazsa, hizmet reddi saldırıları kısa sürede sunucuları, masa üstü bilgisayarları ve ağ donanımını boğabilirler ve kurumunuzdaki bilişim hizmetlerini durma noktasına getirebilirler. Bazı durumlarda, bu saldırılar bütün alt yapıyı felç edebilirler.

Çoğu DOS saldırıları bir yazılım hatası veya güvenlik açığından ziyade genel sistem mimarisindeki zayıflıkları hedef alırlar. Saldırganlar TCP ve ICMP (Internet Control Message Protocol) gibi yaygın kullanılan internet protokollerini kullanarak hizmet reddi saldırılarını başlatabilirler. Bu protokollerden birini kullanarak başlatılan hizmet reddi saldırılan bir veya daha fazla ağ sunucusunu ve cihazını gereksiz veri paketleri ile boğarak ve ağ hizmetlerinin durumu hakkında yanlış bilgiler sağlayarak çökertebilirler. Buna paket taşkını (packet flood) denir.

Paket taşkını başlatmanın popüler bir yolu SYN taşkınıdır (SYN flood). SYN başka bir cihazla TCP/ IP iletişimi başlatmak için kullanılan bir TCP kontrol bitidir. Normalde, bağlantı kurmak için SYN bitini alan cihaz (hem SYN hem de ACK bitleriyle) hemen cevap verir ve teyit bekler. Bir SYN taşkınında, saldırgan hedefteki bilgisayara bağlanmak için çok fazla bağlantı isteği gönderir fakat ACK biti asla alınmaz. Hedef bilgisayar her gelen isteği kaydeder ve belleğindeki bir yerel bağlantı tablosunda bağlantı için bir yer ayırır. Hedef bilgisayar daha sonra teyit için saldırgana geri mesaj gönderir ama saldırgan teyidi aldığını asla bildirmez. Bellekte kaydedilen bütün bu bitler çok küçüktürler, ama zaman geçtikçe birikirler ve sonunda bağlantı tablosunu saldırının kurbanı olan bilgisayarın belleğinde başka işlemler için yer kalmayıncaya dek doldururlar. Bu sırada, gerçek kullanıcılar hedefteki bilgisayara bağlanamazlar çünkü SYN taşkını bağlantı tablosunu doldurmuştur. Saldırının kurbanı olan bilgisayar var olan bağlantı istekleri zaman aşımına uğrayıncaya dek devre dışı kalır.

Bir başka popüler teknik smurfing'dir. Smurfing saldırısı hedefteki bilgisayarda ağ trafiği baskını yaratmak için doğrudan yayın (direct broadcast) kullanır.

Hem iç hem de dış saldırganlar hizmet reddi saldırıları başlatabilirler. Yine de, saldırıların çoğu bilinmeyen dış kaynaklardan gelir. Ağa sızmayı engelleme sistemleri (IPS/IDS) genellikle bu saldırıları tespit etmekte etkilidirler.

Güvenlik çalışanları saldırganların kendi sistemlerini kötücül I amaçlarla kullanamamalarını sağlamak için düzenli olarak agresif tedbirler almalıdır. Ayrıca, artık bazı web içerik sağlayıcıları ve ağ cihazı üreticileri temel yapılandırma tablolarında DOS saldırılarını engellemek için tasarlanmış yeni kurallar bulundururlar. Saldırganların bilgisayarlarınıza erişmelerini engellemek I tüm zamanınızı alabilir, fakat bu sarf edilen çabaya değecektir.

Dağıtık Hizmet Reddi Saldırıları

Dağıtık hizmet reddi saldırısı (Distributed Denial of Service Attacks - DDOS) kullanıcının sisteme erişebilmesini de etkileyen bir hizmet reddi saldırısı türüdür. Bir DDOS saldırısı bilgisayarları aşın yükler ve gerçek kullanıcıların erişimini engeller. DDOS saldırıları hizmet reddi saldırılarından kapsam olarak ayrışır. DDOS saldırısında saldırgan internete bağlı yüzlerce hatta binlerce bilgisayarı ele geçirip bu sistemlere otomatik saldırı birimleri yükler. Saldırgan daha sonra birimlere bir hedef sitesini sahte mesajlarla boğmaları talimatını verir. Bu mesajlar siteyi aşırı yükler ve asıl trafiği engeller. Burada asıl nokta saldıran birimlerin sayısıdır. Saldırgan saldırıyı birçok bilgisayara dağıtarak daha fazla zarara neden olur.

Büyük şirketler ve üniversiteler DDOS saldırıları başlatan saldırganların cazip hedefleridir. Araştırmacıların tahminlerine göre saldırganlar ağlara her hafta binlerce DDOS saldırısı başlatırlar. Bu tehdit o kadar ciddidir ki bu saldırıları durdurmak güvenlik ürünleri üretenler de dâhil olmak üzere birçok şirketin ilk önceliğidir. DDOS saldırılarını durdurmak DOS saldırılarını durdurmaktan | daha zordur çünkü farklı kaynaklardan gelirler. Bilgisayarları DDOS saldırılarından korumak farklı güvenlik seviyeleri gerektirir. Hem hizmet reddi hem de DDOS saldırıları birçok biçimde ve değişik şiddet seviyelerinde olabilirler ve milyonlarca dolarlık gelir kaybına neden olabilirler.

Web'de Uygunsuz Gezinme Davranışları

Kurumun kabul edilebilir kullanım politikasının (Acceptable Use Policy - AUP) ihlal edilmesi, mesel bir çalışanın web'de uygunsuz sitelerde gezinmesi, kendi başına güvenlik ihlali olabilir. Kurumlar hangi davranışların kabul edebilir hangisinin kabul edilemez olduğunu açıkça ifade eden bir kullanın politikasına (AUP) sahip olmalıdırlar. Kabul edilemez kullanım, yetkisiz kullanıcıların okumamaları gereken veri veya bilgiler için dosyaları veya dizinleri aramalarını veya basitçe, yasak web seslerini ziyaret etmelerini içerebilir. Kurumun kabul edilebilir kullanım politika belgesi güvenlik Maline neden olan eylemleri listeler.

İzinsiz dinleme

Saldırganlar telefon ve veri iletişim hatlarına gizlice girebilirler. Telefon dinleme (wiretapping), saldırganın hatta değişiklik yapması durumunda aktiftir. Yetkilendirilmemiş bir kullanıcının, içeriği değiştirmeden yalnızca iletimi dinlemesi durumunda ise pasif olabilir. Pasif dinleme (passive intrusion), daha sonra gerçekleşecek aktif bir saldırı için verinin kopyalanmasını da içerebilir.

Aktif dinlemenin iki yöntemi aşağıdaki şekildedir:

- Hatlar arasında dinleme (Between-the-lines-wiretapping): Bu tür dinleme gerçek kullanıcıların gönderdiği mesajları değiştirmez fakat kullanıcı duraksadığında iletişim hattına ilave mesajlar sokar.
- Hattı değiştirerek dinleme (Piggyback-entry wiretapping): Bu tür dinleme iletişim hattına girerek orijinal mesaj yakalar ve değiştirir ve mesajı sunucu (host) gibi davranan başka bir bilgisayara gönderir.

İzinsiz dinleme genellikle ses ve telefon dinlemesi ile ilişkilendirilse de, saldırganlar iletişim hattını veri iletişimini yakalamak için de kullanabilirler. Veri iletişimin yakalanması, yine de, daha çok koklama (sniffing) olarak adlandırılır (yine de Sniffing basit izinsiz dinlemeden öte, kablosuz iletişimin yakalanmasını içerir).

Arka Kapılar

Yazılım geliştiriciler, programlarında bazen arka kapı (backdoor) adı verilen gizli erişim metotları bulundururlar. Arka kapılar geliştiricilere ve destek personeline güvenlik kontrolleri ile uğraşmadan sisteme kolay giriş izni sağlarlar. Fakat sorun şu ki arka kapılar her zaman gizli kalmazlar. Bir saldırgan bir arka kapıyı keşfettiğinde, bunu kullanarak parolalar, şifreleme vb. var olan güvenlik mekanizmalarını atlatarak sisteme girebilir. Gerçek kullanıcılar kullanıcı kimliği ve parola kullanarak sisteme girerken saldırganlar arka kapıları kullanarak normal erişim kontrollerini sorunsuz geçerler.

Saldırganlar bir sistemin güvenliğini sisteme kendi arka kapı programlarını kurarak da tehlikeye atabilirler. Saldırganlar bu tür arka kapıları yöneticilerin bir bilgisayar sistemini korumak için koydukları kontrolleri aşmak için kullanırlar. Netcat adı verilen program günümüzde en çok kullanılan arka kapı araçlarından biridir.

Rootkitler normal denetim metotlarından saklanabilmeleri için tasarlanan kötücül yazılım programlarıdır. Bunlar bir saldırganın bir bilgisayar sistemine erişebilmesini sağlarlar. Saldırganlar root yetkisine veya sistem yöneticilerinin erişim yetkilerine sahip olunca rootkitler kurarlar. Geleneksel rootkitler kritik programları değiştirerek saldırganlara arka kapı erişimi verirler ve saldırganların sistemde gizlenebilmelerini sağlarlar. Şirketin yazılım bileşenlerinin yerini aldıkları için rootkitler uygulama seviyesindeki Truva atı arka kapılarından daha güçlüdürler. Rootkitler hakkında bu bölümün sonunda daha fazla bilgi alacaksınız.

> *Neredeyse bütün ağ cihazı satıcıları cihazlarını varsayılan bir kullanıcı adı ve parola ile piyasaya sürerler, cihazın kurulumunda bu bilgileri değiştirmeniz gerekir. Yeni cihazların kullanımında bu kullanıcı adı ve parolayı değiştirmeyişiniz sisteminizde herkesin bildiği bir arka kapıya - ciddi bir güvenlik açığına! - neden olur.*

Veri Değişiklikleri

Kasten veya kasıtsız olarak değiştirilen veri, bilişim sistemleri güvenliğinin bütünlük (integrity) ilkesini etkiler. Bu ayrıca bir güvenlik ihlali olarak kabul edilir. Birden fazla süreç temel veri bütünlüğü koşullarına dikkat etmeden aynı anda veriyi değiştirmeye çalışırsa bitmemiş veri değişiklikleri oluşabilir. Başka bir örnek, veriyi tutacak kayıt alanının yeterince büyük olmaması nedeniyle verilerin bir kısmının kırpılarak kaybedilmesidir. Bu durum, birçok programlama dilinde oluşabilir ve tespiti zordur. Ancak, sonuçlan çok önemli olabilir. Veri değişikliği sorunlarından kaçınmanın en iyi yolu veriyi kaydetmeden önce doğrulamak ve kullandığınız programların katı veri bütünlüğü ilkelerine uymalarını sağlamaktır.

Diğer Güvenlik Zorlukları

Güvenli ve emin iletişimi sağlamanın diğer zorlukları spam, hileler, casus yazılımlar ve hatta web tarayıcılarının kaydettiği yerel bilgilerden kaynaklanabilir. Bu zorlukların birkaçının bir arada bulunduğu durumlar da mümkündür.

Spam ve Spim

Spam istenmeyen e-postadır. Spim ise istenmeyen anlık iletiler ve chat mesajlarıdır. Çoğu spam ve spim ticari reklamlardır, genellikle kolay yoldan zengin olma teknikleri, ne olduğu belirsiz ürünler ve diğer gereksiz hizmetlerdir. Spam göndermenin maliyeti azdır, çünkü alıcı spamle ilgili giderlerin çoğunu yüklenir. İnternet

servis sağlayıcıların ve internetteki hizmetlerin spam iletmesinin bir maliyeti vardır. Çok fazla sayıda istenmeyen mesajla başa çıkmak pahalıdır. İnternet sağlayıcıları bu masrafları kullanıcılara yüklerler. Ayrıca, spam mesajları kullanıcıları aldıkları mesajları inceleyip istenmeyenleri silmek için zaman harcamaya zorlar.

E-posta spam'i ve IM chat spim'i e-posta adresleri ve IM/chat hesapları bilinen kişisel kullanıcıları hedef alır. Çoğu zaman spam ve spim göndericileri özel veya herkese açık tartışma gruplarının e-posta listelerindeki veya IM chat forumlarındaki üyelere mesajlar gönderirler. Spam göndericiler için bir diğer popüler yöntem, yazılım kullanarak bilindik kullanıcı adı ve alan adlarından e-posta adresleri yaratmak ve mesajları bu adreslere göndermektir. Örneğin, bir spam programı mehmet@yahoo.com adresine veya M harfi ile başlayan tüm isimlerin yahoo.com adreslerine e-postalar gönderir. Spim aynı yöntemi takip eder, fakat e-posta değil de anlık ileti mesajları kullanır.

Spam göndericilerin çok kullandığı bir teknik içinde 'abonelikten çık' linki bulunduran bir e-posta mesajını birtakım adreslere göndermektir. Asıl amaç e-posta adresinin kullanımda olup olmadığını bulmaktır. Yani, linke tıklayan kullanıcıları abonelikten çıkarmak yerine, spam göndericiler basitçe hesabın kullanıldığına karar verirler ve hesap daha çekici bir hedef haline gelir. Benzer şekilde, spam üreten yazılımlar genellikle e-posta hesaplarının listelerini tutarlar. Yazılımı üretenler bu adreslerin sisteme isteyerek "üye olan" kullanıcılara ait olduğunu öne sürerler fakat bunlar aslında haber gruplarından ya da mail listelerinden aşırılmış adreslerdir. Spamciler sıklıkla e-posta hesaplarım istek olursa sistemden sildiklerini iddia ederler fakat neredeyse asla silmezler.

Spam artık sadece can sıkıcı bir detay değil. Spam'i engellemek bilişim güvenliği için kritik önemdedir. Son zamanlarda spam, suçluların kişisel ve şirketlere ait bilgileri elde etmesi ve Truva atı veya diğer zararlı yazılımları bilgisayarlara yüklemeleri için kullanılan bir yol haline geldi.

Siber suçlarla savaşmak için kurumlar spam ile başa çıkmalıdırlar. Bir oltalama (phishing) e-pos-tası, alıcıyı e-postanın eklerinde gömülü halde bulunan bir URL bağlantısına tıklaması için kandırmaya çalışan sahte veya düzmece bir e-postadır. Daha önceki bölümde de belirtildiği gibi, kötücül yazılımlar, Truva atları ve tuşa basma kaydediciler oltalama e-postalarına gömülmüş olabilirler. Bu e-postayı alan bir kişi farkında olmadan URL bağlantısına tıklayarak veya e-postaya ekli dosyaları açarak kötücül yazılımı etkinleştirebilir. Bu tür olaylarla savaşmak için anti virüs, casus yazılım önleyici ve kötücül yazılım önleyici uygulamalar gerekir.

> *Eğer aldığınız bir mesajın sahtekârlık içerdiğinden şüpheleniyorsanız, Snopes (www.snopes.com) adında bir web sitesini ziyaret ederek mesajı araştırabilirsiniz. Çoğu zaman Snopes'ta size gelen mesajla eşleşen bir başlık bulacaksınız. Snopes her hile hakkında tam bilgiye sahip değildir, fakat araştırmanıza başlamak için uygun bir yol sağlayabilir.*

Aldatmalar

Bir aldatma (hoax), alıcıyı kandırmak veya aldatmak için tasarlanan bazı eylemlerdir. Bu bağlamda, aldatmalar genellikle e-posta mesajlarıyla yayılırlar. Çoğu zaman, bu mesajlar çok tahrip edici yeni virüsler hakkında uyarılar içerirler. Bu aldatma mesajları sisteminize virüsler veya Truva atları gibi otomatik olarak bulaşmasa da, bunlarla uğraşmak zaman alıcıdır. Aslında, gerçek virüslerle ve Truva atı olaylarıyla uğraşmaktan daha fazla zamanı bu tür aldatmaların gerçek olmadığını açığa çıkarmak için harcayabilirsiniz.

Aldatmalar ile başa çıkmanın en iyi yolu kullanıcılardan kendilerine gelen mesajları diğer kişilere iletmemelerini istemektir. Size gelen şirin bir mesajı bir veya iki arkadaşınıza göndermeniz sorun olmaz. Fakat doğruluğu belli olmayan bir uyarıyı ya da yardım isteğini adres defterinizdeki herkese göndermek ve alıcılardan da bu mesajı kendi adres defterlerindeki herkese göndermelerini istemek, zaten herkesin gelen kutusunu gereksiz yere dolduran kargaşayı daha da artıracaktır. Bu tür e-postaları alan kişiler bildikleri herkese bu mesajları iletmemelidirler.

Çerezler

Bir web sunucuya bir kullanıcının geçmişini izlemede yardımcı olmak için, web tarayıcılar kullanıcının hard diskinde bu web sunucusunun bir çerez saklamasına izin verirler. Bir çerez (cookie), geçmişte bir web sitesine yapılan ziyaretlerden edinilmiş ayrıntıları saklayan basit bir metin dosyasıdır. Çerezler değerlidirler çünkü HTTP durumsuz (stateless) bir protokoldür, bu nedenle bir veri dosyası çerezi kullanılarak son ziyaretin küçük bir kaydı tutulur. Bu kayıtlar kullanıcının kullanıcı adı, kullanıcının girdiği kredi kartı bilgileri ve benzeri diğer

bilgileri içerebilir. Daha sonra, kullanıcı web sunucuya bir istek gönderdiğinde, sunucu kullanıcıdan bilgileri yeniden girmesini istemek yerine çereze erişebilir.

Çerezler bazen tartışmalı bir konudur, çünkü bir web sunucusunun bazı dosyaları kullanıcının hard diskinde kaydetmek için kullanıcının bilgisayarına iletmesine izin verirler. Çerezler yazı dosyaları oldukları için, yine de, genellikle kendi başlarına bir zarara neden olamazlar. Çerezler kendileri doğrudan kötücül eylemlere kalkışamazlar. Çerezler virüsleri yayamazlar veya kullanıcının hard diskindeki diğer bilgilere erişemezler. Yine de bu çerezlerin bir güvenlik sorununa neden olmayacağı anlamına gelmez. Çerezler bir kullanıcının hard diskinden bilgi toplayamasalar da, belirtildiği gibi, bazen kredi kartı detayları gibi mahrem bilgileri kaydedebilirler.

Çerezlerle ilgili asıl problem, bilgiyi şifrelenmemiş metin dosyalarında tutmalarıdır. Bu da bilgisayarınıza erişimi olan herkesin çerezlerinizin içeriğini okuyabilmesi demektir. Bir çerez bir takım kolaylık sağlayabilse de, örneğin daha önce internette aradığınız uçuşları hatırlasa da, sizin mahremiyetinizi de kolayca tehlikeye atabilir. Güvenli bir şekilde tasarlanmış çoğu web sitesi kredi kartı numarası gibi bilgileri asla bir çerezde tutmaz fakat bazı web siteleri özensizdirler. Bilgisayarınızdaki çerezlerde hangi bilgilerin tutulduğunu asla tamamıyla bilemezsiniz. Çerezlerde kişisel bilgilerin tutulmasını engellemenin en iyi yolu sadece güvendiğiniz web sitelerinin çerez bulundurmasına izni vermektir.

Web sitelerinde daha fazla gezindikçe, bilgisayarınızda muhtemelen daha fazla çerez bulacaksınız. Aslında, kullanıcılar bilgisayarlarında yüzlerce çerezle baş başa kalabilirler, bu durum can sıkıcı bir hal alabilir. Neyse ki bu çerezleri istediğiniz an silebilirsiniz. Ayrıca, her şeyden önce web tarayıcınızın çerezlere izin vermesini engelleyebilirsiniz. Talimatlar için tarayıcınızın yardım bilgilerini kontrol ediniz.

Riskler, Tehditler ve Güvenlik Açıkları Nelerdir?

Riskler, tehditler ve güvenlik açıkları beraber oluşurlar. Risk kötü bir şeyin gerçekleşme olasılığıdır. Bir tehdit (threat) bir varlığa zarar verecek veya tehlikeye atacak herhangi bir eylemdir. Bir güvenlik açığı/zaflyet (vulnerability) ise tasarımdaki veya yazılım kodundaki zayıflığın kendisidir. İstismar edilebilecek bir güvenlik açığı bir tehdittir. Eğer bir sistemde güvenlik açığı varsa, tehdit ihtimali de vardır. Bir açığın getirdiği herhangi bir tehdit olumsuz bir olayın gerçekleşmesi riskini yaratır. Tehditleri tamamen yok edemezsiniz fakat açıklara karşı kendinizi koruyabilirsiniz. Böylece, tehditler hala var olsalar da, güvenlik açıklarım kullanamazlar. Varlıkları saldırı riskinden korumanın kilit noktası mümkün olan en fazla sayıda güvenlik açığını ortadan kaldırmak veya etkilerini gidermektir. Bir BT altyapısında çok fazla tehdit ve açık bulabilirsiniz. Aşağıdaki tabloda, BT altyapısının yedi alt etki alanının her birinde bulunabilen bazı yaygın tehditleri listelemektedir.

ETKİ ALANI	**YAYGIN TEHDİTLER VE GÜVENLİK AÇIKLARI**
Kullanıcı etki alanı	Güvenlik hakkında duyarlılığın veya dikkatin eksikliği Kullanılabilir kullanım politikasının kaza sonucu ihlali Bilinçli yapılan kötücül eylemler Sosyal mühendislik
İş istasyonu etki alanı	İzinsiz kullanıcı girişi Kötücül yazılımların sisteme sokulması Kurulan yazılımdaki zayıflıklar
LAN etki alanı	Yetkisiz ağ erişimi Gizli verilerin şifrelenmeden iletilmesi Kötücül yazılımın yayılması
LAN'dan WAN'a etki alanı	Dışarıdan ağ içindeki kaynaklara yetkisiz erişim ve temas Kötücül yazılımların sisteme sokulması İnternet bağlantısı olmaması nedeniyle üretim kaybı
WAN etki alanı	Gizli bilgilerin şifrelenmeden iletilmesi Bilinmeyen kaynaklardan gelen kötücül saldırılar Hizmet reddi saldırıları Yazılımda bulunan zayıflıklar
Uzaktan Erişim etki alanı	Sistem erişimine ve gizli bilgilere Brute-force parola saldırıları Kaynaklara uzaktan yetkisiz erişim

	Uzaktan erişimde veya kaybedilen kayıt cihazlarından verinin sızması (data leakage)
Sistem/Uygulama etki alanı	Kaynaklara yetkisiz fiziksel veya mantıksal erişim (physical or logical access) Sunucu işletim sisteminde veya uygulama yazılımında zayıflıklar Hatalar, yanlışlar ve felaketler sonucu veri kaybı (data loss)

> *Tehditleri ve güvenlik açıklarını bulmak ve bunlara cevap vermek karmaşık bir süreç olabilir. Bazı durumlarda, bir tehdidi ortadan kaldırmak çok pahalı veya çok zaman alıcı olabilir. Amacınız mümkün olduğu kadar fazla tehdidin gerçekleşmesini engellemektir fakat ayrıca bazı varlıkları koruma masrafının varlıkların kendi ederinden daha fazlaya gelip gelmeyeceğini dikkatlice değerlendirmelisiniz. Varlıkların gerçek değerinden daha fazla zamanı ve parayı tehditleri fark edip engellemeye harcamamaksınız.*

Tehditler bir kişiden, bir grup kişiden veya bir kurumdan gelebilir. İster kasıtsız ister kötücül olsun, bir hesaplama cihazına (Computing Device) yönelen bir tehdit, bir kişinin veya bir kurumun varlık veya kaynaklarına olumsuz etkisi olan herhangi bir eylemdir. Bu varlık bir donanım, yazılım, veri tabanları, dosyalar, veri veya fiziksel ağın kendisi olabilir.

Güvenlik açısından bir tehdit önem arz eder. Bilgisayar güvenliğinin hedefi tehditlerle başa çıkmada gerekli metotları, teknikleri ve tavsiyeleri sunmaktır. Ağ sistemi yöneticilerine, tasarımcılara, geliştiricilere ve kullanıcılara istenmeyen sistem özelliklerinden ve zayıflıklarından kaçınmaları için gerekli olan politikaları geliştirerek bu hedefe ulaşabilirsiniz.

Tehditleri belirleyebilir, önem ve etkilerine göre sıralayabilirsiniz. Tehditleri neden olacakları para kaybı, itibara verecekleri zarar, tazminat ve ne kadar sıklıkla oluşabilecekleri gibi kıstaslarla sıralayabilirsiniz. Her kurum, kurumun yaptığı işe ve bu işe olan etkisine bağlı olarak bir tehdidi diğer bir kurumdakinden daha yüksek veya daha alçak bir sıraya koyabilir.

En yaygın tehditler, özel bir sıralama olmaksızın, aşağıdakileri içerir:

- Kötücül yazılım
- Donanım veya yazılım hatası
- Sistemin içindeki saldırgan
- Cihaz hırsızlığı
- Dışarıdaki saldırgan
- Doğal afet
- Endüstriyel casusluk
- Terörizm

Her tehdit kötücül olmayabilir. Bazı tehditler kasten olsa da, bazıları kaza sonucu oluşabilir. Kaza sonucu oluşan tehditler donanım hatalarını ve denetim eksikliği nedeniyle oluşan yazılım hatalarını içerir. Yine de, bu kaza sonucu oluşan tehditlerin sonuçları kötücül tehditler kadar zarar verici olabilir. İster kaza sonucu, ister kötücül olsun, güvenlik ihlallerini en aza indirmek için her çabayı sarf etmelisiniz. Genel hedefiniz, ağ ve bilgisayar sistemini her tür saldırıdan korumak ve kişilerin veya kurum varlıklarının hırsızlığını, tahribatını ve bozulmasını engellemektir.

Tehditlerin Hedefleri

En çok beğendiği arama motorunu kullanarak, bir saldırgan neredeyse her protokolün, işletim sisteminin, uygulamanın, cihazın veya donanım ortamının güvenliğini aşmak için gerekli yöntemleri bulabilir. Bu nedenle, bütün tehditleri yakından izlemelisiniz. Bir sonraki tehdidin nereden geleceğini asla bilemezsiniz. Saldırgan profesyonel bir siber suçlu veya bulunduğunuz binadaki bir kişi olabilir. En iyi yöntem bütün tehdit hedeflerini düzenli olarak ve dikkatlice izlemektir.

Bir izleme planı oluşturmadaki ilk adım tehdidin bilişim altyapısının yedi etki alanından hangisinde oluşabileceğini belirlemektir. Aşağıdaki tabloda, genel tehditleri ve bu tehditlerin bilişim altyapısının neresinde oluştuğunu listelemektedir.

ETKİ ALANI	TEHDİT HEDEFİ
Kullanıcı etki alanı	Çalışanın kendi karakteri ve davranışı. Kabul edilebilir kullanım politikasının ihlalleri hedeflenir.
İş istasyonu etki alanı	İş istasyonları, diz üstü bilgisayarları, mobil cihazlar ve bunların güvenlik açıkları hedeflenir. Bu bölüm bilişim altyapısına giriş noktasıdır.
LAN etki alanı	Windows Aktif Dizin/Bölüm Kontrolörü, dosya sunucuları, yazıcı sunucuları. Ayrıca, IP veri ağı LAN bölümünün bir parçasıdır ve kimlik ve doğrulama saldırılarının hedefidir.
LAN'dan WAN'a etki alanı	DMZ VLAN'lar veya adanmış uzaktan bağlantılar genellikle burada sonlandırılır. Dünyaya açık İP cihazları, güvenlik katmanının (perimeter) güvenlik duvarları da (firewall) dahil olmak üzere, IDS/IPS ve uzaktan VPN sonlandırmaları buradadır.
WAN etki alanı	IP yönlendiricileri (router), TCP/IP yığınları ve tampon bellekleri, güvenlik duvarları, ağ geçitleri (gafeway), anahtar ar (switch) ve WAN servis sağlayıcıları hedeftirler.
Uzaktan Erişim etki alanı	Sanal özel ağ (Virtual private network - VPN), iki faktörlü kimlik denetleme (two-factor authentication, mobil ve uzaktan çalışanlar için erişim sistemleri genellikle desteklenir ve hedeftir.
Sistem/Uygulama bölümü	Web ve uygulama sunucuları, işletim sistemleri ve uygulamaları. Mahrem veriler içeren arka-uç (back-end) veri tabanı sunucuları ve veri tabanı tabloları hedeftir.

Bu listeden, bir saldırganın büyük sorunlara neden olmak için çok imkâna sahip olduğu açıkça görülmelidir. Ayrıca, çoğu tehdit hedefinin farklı kategorilerde ortaya çıktığını fark etmelisiniz. Bütün etki alanları üzerinde kapsamlı bir güvenlik planının hazırlanmasının gerekliliği açıkça görülmelidir.

Tehdit Türleri

Bilgiyi korumak için, bilginin gizliliğini (confidentialty), bütünlüğünü (integrity) ve kullanılabilirliğini (availability) korumalısınız (CIA). Üç ana tehdit türü bu prensiplerden her birini doğrudan tehdit etmektedir. Bunlar aşağıdaki şekildedir:

- İfşa (disclosure) tehditleri
- Değişim (alteration) tehditleri
- Hizmet reddi (denial) veya tahribat (destruction) tehditleri

İfşa Tehditleri

Ağ kaynakları üzerinde tutulan veya ağ kaynakları arasında iletim halinde olan gizli ve mahrem bilgilere yetkisiz kullanıcıların her erişiminde ifşa (disclosure) oluşur. İfşa, ayrıca tıbbi kayıtlar veri tabanı gibi gizli ve mahrem bilgiler içeren bir cihaz veya bir bilgisayar kaybedildiği veya çalındığı durumlarda oluşabilmektedir. Bilgi sızması (information leak) bir kişinin gerekli yetkiye sahip olmaksızın bilgiyi kasten başkalarına dağıttığı her durumdur. Saldırganların yasadışı olarak veriyi elde etmek veya değiştirmek için kullandıkları iki teknik aşağıdaki gibidir:

- Sabotaj (Sabotage) - Sabotaj mala zarar verilmesi veya normal hizmetlerin engellenmesidir. Teknik olarak, sabotaj bilişim güvenliğinin hizmet sunabilme ilkesine saldırır.
- Casusluk (Espionage) - Casusluk bilgileri, genellikle başka bir devlete yardımcı olmak için, çalma eylemidir. Teröristler ve düşman güçleri aynı zamanda mahrem devlet bilgilerini gelecekteki ataklarında kullanmak için çalmaya kalkışabilirler.

Sabotaj sessiz bir saldırı değildir fakat casusluk hiçbir görünür iz bırakmadan yapılabilir.

Çoğu kurumda, kaydedilen bilginin çok büyük bir kısmı kamuya açık değildir. Bu bilgi, kullanıcının bilgisayarında bulunan kişisel bilgileri veya büyük bir veri tabanında saklanan mahrem kayıtları içerebilir. Bu bilgilerin ifşasının etkileri farklı olabilir. Örneğin, bir kullanıcının kişisel bilgilerinin açıklanması kullanıcıyı utandırırken, bir yurttaşın mahrem kayıtlarının ifşası ciddi sonuçlara neden olabilir. Ayrıca, eğer devlet sırrını veya istihbarat dosyalarını ilgilendiriyorsa, bilginin ifşası daha fazla probleme bile neden olabilir.

Bilişim güvenliği çalışanları ifşa tehditleri ile başa çıkmak için çok fazla zaman harcarlar. Özellikle, Amerikan hükümeti kritik güvenlik alanlarında problem oluşturabilme potansiyelleri yüzünden ifşa tehditlerine çok yakından odaklanır. Bu tür tehditlerle başa çıkmanın en zor yanlarından biri yetkilendirilmemiş kişilerin korunmayan veriyi çaldıktan sonra eylemleri hakkında hiçbir iz bırakmamalarıdır. Bu nedenle, güvenlik araştırmaları ve geliştirmeleri ifşa tehditlerine ve karşı tedbirlere odaklanmıştır.

Değiştirme Tehditleri

Bir değiştirme tehdidi (alteration threat) verinin bütünlüğünü hedef alır. Bu saldırı türü, kasıtlı veya kasıtsız olarak, bir sistemde tutulan verilere yetkisiz değişiklikler yaparak sistemi tehlikeye sokar. Bu değişim veri ağ cihazında kayıtlıyken veya iki kaynak arasında transfer edilirken oluşabilir. Kasıtlı değişimler genellikle kötü niyetlidir. Kasıtsız değişimler genellikle kaza sonucudur. İnsanlar, bilgisayarların ve cihazların tutarlılığını etkileyecek hatalar yapabilirler ve çoğu zaman yaparlar. Değişimler kasıtlı olmasa bile yine de güvenlik problemleri yaratırlar.

Sistem yapılandırmasına yapılan değişiklikler bir ağ kaynağının bütünlüğünü de ihlal edebilir. Bu değişiklik yetkisiz bir kişi bir varlığı kurcaladığı zaman veya yetkisi olan bir kişi öngörülemeyen sonuçları olan bir değişiklik yaptığı zaman meydana gelebilir. Örneğin, bir kullanıcı veri tabanı dosyalarını, işletim sistemlerini, uygulama yazılımını ve hatta donanım cihazlarını değiştirebilir. Değişiklikler ağ üzerindeki bir kaynakta bilgi oluşturmayı, değiştirmeyi, silmeyi ve yazmayı içerebilirler. Bu değişiklikleri takip etmeyi veya denetlemeyi içeren teknikler geliştirmek iyi bir fikirdir. Bu sayede kimin ne zaman, nerede ve nasıl değişiklikler yaptığı hakkında bir kayda sahip olabilirsiniz. Ayrıca, değişiklik yönetim sistemleri (change managemerıt systems) kimlerin değişiklik yapabileceğini, bu değişiklikleri nasıl yapabileceklerini ve dosyaları nasıl değiştirebileceklerini sınırlandırabilir. Varlıkları sadece yetkili kişilerin ve sadece yetki verilen şekillerde değiştirebilmeleri çok önemlidir.

Önceden hazırlanmak değiştirme tehditlerinin şiddetini azaltabilir. Örneğin, sizde verinin bir kopyası veya yedeği varsa, güvenlik ihlalinin etkisi yedeğin bulunmadığı duruma göre daha az şiddetli olur. Yine de, verinin geri kazanılması (recovery) en son çaba olmalıdır. Çok daha iyi bir yöntem değiştirme saldırısının gerçekleşmesini ilk baştan engellemektir. Bilginizi korumak, bu bilgiyi tamir etmekten veya geri kurtarmaktan her zaman daha iyidir.

Ret veya Tahribat Tehditleri

Ret (denial) veya tahribat (destruction) tehditleri varlıkları ve kaynakları kullanılamaz veya ulaşılamaz hale getirirler. Veriyi yok eden veya kullanılamaz hale getiren her tehdit bilişim güvenliğinin kullanılabilirlik ilkesini ihlal eder. Bir ret veya tahribat saldırısı yetki sahibi bir kullanıcının bir kaynağa erişimini geçici veya kalıcı bir şekilde engellediğinde başarılı olmaktadır.

Bir DoS saldırısı ret veya tahribat tehdidine bir örnektir Bu bölümde daha önce öğrendiğiniz gibi, genelde kötücül olan bir DoS saldırısı, yetkili kullanıcıların bilgisayar ve ağ kaynaklarına erişimini engeller. Birçok kurum DoS saldırılarının muhtemel kurbanlarıdır. Aslında internete bağlı her cihaz DoS tehditlerine açıktır. Bu saldırı türü bloke edilen varlığın veya kaynağın önemine göre küçük veya çok büyük bir tehlike oluşturabilir. Örneğin, bir saldırganın bir sunucudaki belirli bir portu bloke ettiğini düşünelim. Eğer bu port kritik önemdeki bir kaynak için değilse etkisi çok küçük olabilir, fakat eğer port şirketinizin web sitesine kullanıcı girişinin doğrulanmasını destekliyorsa, müşterilerinizin sisteme dakikalarca veya saatlerce girmesini engelleyebilecektir. Bu durumda etkisi çok ciddi olabilecektir.

Tehdit gerçekten bir DoS tehdidi mi?

İsteklere geç cevap verilmesi her zaman hizmet reddi saldırısı yüzünden değildir. Bu durum, ağ kullanım limitinin aşılması yüzünden olabilir. Aşırı talep (oversubscription) ağın tasarlanandan daha fazla bilgisayar ve süreç tarafından kullanıldığını ifade eder. Bir başka deyişle, kullanıcılar ağı gerektiğinden fazla kullanıyorlardır. Ağ cihazı satıcıları bu tekniği müşterinin zararına olarak gelir artırmada kullanırlar. Bir başka ihtimalde, hizmet sağlayıcının kullanıcının ağdaki bazı kaynaklara ulaşamamasına neden olması olabilir. Örneğin, hizmet sağlayıcı ağdaki önemli kaynakları sistem güncellemesi veya web sitesi değişikliği gibi nedenlerle devre dışı bırakmış olabilir. Başka bir suçlu da kısma (throttling) adi verilen, yöneticilerin ağdaki trafiği yavaşlatmak ve azaltmak için kullandıkları bir teknik olabilir veya sorun basit bir kullanıcı hatası olabilir.

Bir DoS saldırısı kritik önemde olmayan bir pottu baskına uğratsa da, gelen büyük miktardaki trafik sunucuyu çökertebilir veya o kadar yavaşlatır ki sunucu gelen geçerli isteklere zamanında cevap veremez. Bu durumda, DOS saldırısı hala başarılı olmaktadır.

Kötücül Saldırı Nedir?

Bir bilgisayar sistemine veya ağa yapılan bir saldırı (attack) sistemde bulunan bir güvenlik açığını istismar ederek başarılı olur. Dört genel saldırı kategorisi vardır. Bir saldırı aşağıda belirtilen dört kategoriden hepsi veya bir kaçının birleşiminden oluşabilir:

- Uydurmalar (Fabrications) - Uydurmalar, hiçbir şeyden şüphelenmeyen kullanıcıları aldatmak için bir takım hileler oluşturmaktır.
- Engellemeler (Interceptions) - Engelleme, bir iletişime kulak misafiri olmak ve bu iletişimi yetkisiz bir kullanım için başka bir yere yönlendirmektir.
- Kesintiler (Interruptions) - Bir kesinti, bir iletişim kanalında kopmaya neden olur ve verinin iletimini engeller.
- Değişiklikler (Modifications) - Bir değişiklik, iletimde veya dosyada bulunan verinin değiştirilmesidir.

Daha önce öğrendiğiniz gibi, güvenlik tehditleri aktif veya pasif olabilir. Her iki tür de bilişim altyapısı için olumsuz sonuçlara neden olabilir. Aktif bir saldırı veri akımının (data stream) değiştirilmesini veya bilgisayar ve ağ sistemlerini yetkisiz erişimin elde edilmesini içerir. Bir aktif saldırı fiziksel bir sızmadır. Pasif bir atakta saldırgan sisteme değişiklikler yapmaz. Bu tip saldırılar sadece veri iletimini takip eder ve dinler.

Aktif tehditler aşağıdakileri içerir:

- Doğum günü saldırıları (Birthday attacks)
- Brute-force parola saldırıları (Brute-force password attacks)
- Sözlük parola saldırıları (Dictionary password attacks)
- IP adres yanıltması (IP address spoofing)
- Ele geçirme (Hijacking)
- Yeniden gönderme saldırıları (Replay attacks)
- Ortadaki adam saldırıları (Man-in-the-middle attacks)
- Yerine geçme saldırıları (Masquerading)
- Sosyal mühendislik (Social engineering)
- Oltalama (Phishing)
- Telefon şebekesine yasa dışı girme (Phreaking)
- Web sitesi trafiğinin yönlendirilmesi (Pharming)

Bu tür saldırılar sıklıkla görülür ve çok yaygındırlar. Bu saldırılar bilişim sistemleri güvenliği çalışanlarının radar ekranlarında her yıl daha da artan bir sayıda görünürler. Şimdi bu kötücül saldırıların en yaygın biçimlerinden birkaçının tanımını yapacağız.

Doğum Günü Saldırıları

Saldırganlar özetlenmiş (hash) bir parola dosyasını ele geçirince bir doğum günü saldırısı (birthday attacks) gerçekleştirilir. Bir doğum günü saldırısı, tek yönlü özetlere (one-way hashes) yapılan brute-force saldırısını kolaylaştıran bir kriptografik saldırı türüdür. Olasılık teorisindeki doğum günü problemine (birthday problem) dayanan matematiksel bir saldırı biçimidir.

Brute-Force Parola Saldırıları

En çok denenen ve çalışan saldırı metotlarından bir tanesi brute-force parola saldırılardır (brute-force password attacks). Bir brute-force parola saldırısında saldırgan çalışan bir parola buluncaya kadar farklı parolaları bir sistem üzerinde dener. Genellikle saldırgan parola, kullanıcı kimliği ve güvenlik kodunun bütün birleşimlerini bir eşleşme buluncaya dek deneyen bir yazılım programı kullanır. Saldırı kısa bir sürede ve seri olarak gerçekleşir. Bu saldırı tipine brute-force parola saldırısı denir, çünkü saldırgan basitçe bütün şifreleri denemeye çalışır. Beceri veya gizliliğe gerek yoktur -sadece kod kırılıncaya dek brute-force vardır.

Bugünün büyük ölçekli bilgisayarları ile milyonlarca parola birleşimini çok kısa bir sürede denemek mümkündür. Yeterince zaman verilir ve yeterince bilgisayar kullanılırsa çoğu algoritmayı kırmak mümkündür.

Sözlük Parola Saldırıları

Bir sözlük parola saldırısı (dictionary password attack) kullanıcıların kötü parolalar seçeceklerini göz önüne alan basit bir saldın türüdür. Bir sözlük parola saldırısında, bir parola kinci program sözlükteki bütün kelimeleri alır ve her bir kelimeyi parola olarak kullanarak sisteme giriş yapmaya çalışır.

Kullanıcılar genellikle yaygın olarak kullanılan kelimeleri parola olarak seçmek gibi kötü bir tercih yaparlar. Karmaşık parolaları zorunlu hale getiren bir parola politikası sözlük saldırılarına karşı en iyi savunmadır. Kullanıcılar rakamların ve sayıların birleşiminden oluşan parolalar kullanmalıdırlar ve parolalar kullanıcı hakkında hiçbir kişisel bilgi içermemelidir.

IP Adres Yanıltması

Adres yanıltması (spoofing) bir kişi, program veya bilgisayarın kendisini bir başka kişi, program veya bilgisayar gibi gösterip bir kaynağa erişim kazanmaya çalıştığı bir saldırı türüdür. Yaygın bir adres yanıltması saldırısı, sahte bir ağ adresi kullanarak kendisini farklı bir bilgisayar olarak göstermeye çalışmaktır. Bir saldırgan bir bilgisayarın ağ adresini hedefteki ağda bulunan yetkili bir bilgisayarın adresi ile değiştirir. Eğer hedefin yerel yönlendiricisinin yöneticisi, yönlendiriciyi dışarıdan gelen ama ağın içindeki adreslere sahip olan trafiği filtreleyip engelleyecek şekilde yapılandırmamışsa, saldırı başarılı olabilir. IP adres aldatması, bir saldırganın içerideki korunan kaynaklara erişimini sağlayabilir.

Adres çözümleme protokol zehirlenmesi (Address Resolution Protocol – ARP poisoning), adres aldatması saldırısına bir örnektir. Bu saldırıda, saldırgan değişik bir MAC adresi ile sahte ARP mesajları göndererek hedefteki bir cihazın, örneğin bir sunucunun, MAC adresini taklit eder. Bu, sunucudan gönderilen ağ trafiğinin ikiye katlanmasına neden olur. Başka bir ağ tabanlı saldırı türü Christmas (XMAS) saldırısıdır. Bu tür bir saldırı, bayrakları (flag), TCP başlık bitleri 1 olarak ayarlanmış IP yönlendiricileri ve ağ sınırındaki yönlendiricileri şaşırtmak için ayarlanmış gelişmiş TCP paketleri gönderir ve böylece IP yönlendiricisini bir yılbaşı ağacı gibi aydınlatır.

Ele Geçirme

Ele geçirme (Hijacking) saldırganın iki makine arasındaki iletişimi ele geçirdiği ve bu makinelerden biri gibi davrandığı saldırı türüdür. Ele geçirme saldırısının birkaç türü vardır:

- Ortadaki adam ele geçirmesi (Man-in-the-middle hijacking) - Bu tür saldırılarda, birazdan detaylıca tartışacağımız gibi, saldırgan bağlantıyı ele geçirerek kendisini bağlantının herhangi bir ucundaki kişi olarak sunmak için bir program kullanır. Örneğin, Ayşe ve Ahmet iletişim kurmak istediğinde, saldırgan Ahmet ile konuşurken Ayşe gibi, Ayşe ile konuşurken de Ahmet gibi davranır. Ne Ayşe ne de Ahmet saldırgan ile konuştuklarının farkında değillerdir. Saldırgan böylece önemli miktarda bilgi edinebilir ve hatta Ayşe ve Ahmet arasında veri akarken bu veriyi değiştirebilir. Bu saldın türü, saldırganın mesajlara erişebilmesini veya mesajları yeniden iletmeden önce değiştirebilmesini sağlar. Ortadaki adam saldınları sistemin içindeki bir tehditten gelebilir. Bu içerideki tehdit (insider threat) bir çalışandan, sözleşmeli birisinden veya kurum içerisindeki güvenilir birisinden gelebilir.
- Tarayıcı veya URL ele geçirmesi (Browser or URL hijacking) - Bir tarayıcı veya URL ele geçirme saldırısında kullanıcı istediğinden farklı olarak, genellikle saldırgan tarafından oluşturulmuş, sahte bir web sitesine yönlendirilir. Bu, kullanıcıya saldırganın siteyi değiştirdiği izlenimini verir, fakat aslında saldırgan sadece kullanıcının tarayıcısını farklı bir siteye çekmiştir. Bu tür bir saldırı aynı zamanda yazım hatası (typo squatting) olarak bilinir. Saldırganlar bu saldırıyı kullanarak kullanıcıları kandırıp parola gibi gizli bilgileri oltalayabilirler.
- Oturum ele geçirme (Session hijacking) - Oturum ele geçirmede saldırgan iki ağ bilgisayarı arasında var olan bir bağlantıyı ele geçirmeye çalışır. Bu saldırının ilk adımında saldırgan bağlantıyı izlemek için LAN üzerindeki bir ağ cihazının, örneğin bir güvenlik duvarının veya başka bir bilgisayarın, kontrolünü eline alır. Bu, saldırganın alıcı ve verici tarafından kullanılan sıralı numaraları öğrenmesini sağlar. Bu numara sıralamasını öğrendikten sonra, saldırgan sistemde iletişim halindeki taraflardan birinden geliyormuş gibi görünen bir trafik oluşturur. Bu gerçek kullanıcılardan birinin oturumunu çalar. Çalınan oturumu başlatan asıl kullanıcıdan kurtulmak için saldırgan iletişim halindeki cihazlardan birine çok fazla sayıda paket göndererek aşırı yükler ve böylece cihazın oturumu biter.

Yeniden Gönderme Saldırıları

Yeniden gönderme saldırıları (replay attacks) bir ağda veri paketlerini ele geçirip bunları yetkisiz bir durumu oluşturmak için yeniden sisteme göndermeyi içerir. Çoğaltılmış (duplicate), doğrulanmış (authenticated) IP paketlerinin alımı servisleri aksatabilir ya da bazı diğer istenmeyen sonuçlara neden olabilir. Saldırganlar eski mesajları veya eski mesajların bazı kısımlarını sistem kullanıcılarını kandırmak için yeniden gönderme saldırılarında kullandıkları zaman sistemler ele geçirilebilir. Bu durum, saldırganların bir sisteme yetkisiz girişlerine izin veren bilgiler elde etmelerine yardımcı olabilir.

Ortadaki Adam Saldırıları

Bir ortadaki adam saldırısı (man-in-the-middle attack) pek çok ağ türü tarafından kullanılan çok atlamalı (multi-hop) süreçten faydalanır. Bu tür saldırıda, saldırgan iki taraf arasındaki mesajları diğer tarafa iletmeden önce ele geçirir.

Web yanıltması (web spoofing) kullanıcının belirli bir web sunucusuyla güvenli bir oturuma sahip olduğunu düşündüğü bir tür ortadaki adam saldırısıdır. Gerçekte, güvenli oturum web sunucusuyla değil saldırganla kurulmuştur. Saldırgan daha sonra web sunucusuyla güvenli bir bağlantı kurar ve görünmeyen bir ortadaki adam gibi davranır. Saldırgan kullanıcı ile web sunucusu arasındaki trafiği idare eder. Böylelikle, kullanıcıyı parolalarını, kredi kartı bilgilerini ve diğer gizli bilgilerini vermesi için kandırır.

Saldırganlar ortadaki adam saldırılarını bilgi çalmak, DoS saldırıları düzenlemek, iletilen veriyi bozmak, bir kurumun iç bilgisayar ve ağ kaynaklarına ulaşmak ve ağdaki oturumlara yeni bilgileri sokmak için kullanabilirler.

Yerine Geçme

Yerine geçme (masquerading) saldırısında, bir kullanıcı veya bilgisayar başka bir kullanıcı veya bilgisayar yerine geçer. Yerine geçme saldırıları, genellikle IP adres aldatması veya yeniden gönderme gibi aktif saldırı biçimlerinden birini içerir. Saldırganlar doğrulama sıralarını (authentication sequences) kaydedip bunları yeniden sisteme sokarak uygulamalara veya işletim sistemlerine girebilirler. Örneğin, bir saldırgan zayıf bir web uygulamasına gönderilen kullanıcı adlarını ve parolaları izleyebilir. Saldırgan, bu ele geçirilen giriş bilgilerini kullanarak web uygulamasına girebilir ve kullanıcıymış gibi davranabilir.

Ortam Dinleme

Ortam dinleme (eavesdropping) veya koklama (sniffing), ağdaki bir birimin ağ ara yüzünü karışık (promiscuous) modunda ayarlaması ve geçen bütün paketleri daha sonra analiz etmek üzere kopyalaması halinde oluşur. Karışık mod, bir ağ cihazının adresi kendi ağ adresiyle eşleşmese dahi gelen her ağ paketini yakalayıp okumasına izin verir. Diğer kullanıcıları uyarmaksızın, sisteme donanım ve yazılım ekleyerek iletim ortamının o bölümündeki bütün paketleri izlemek ve analiz etmek mümkündür. Ortam dinleme saldırıları uydu, kablosuz, mobil ve diğer iletim metotlarını içerir.

Sosyal Mühendislik

Saldırganlar bir BT altyapısındaki kaynaklara erişmek için sıklıkla sosyal mühendislik (social engineering) denen bir aldatma tekniğini kullanırlar. Neredeyse bütün olaylarda, sosyal mühendislik yetkili kullanıcıları kandırarak yetkisiz kullanıcıların istediği şeylerin yaptırılmasını içerir. Sosyal mühendislik saldırısının başarısı insanların yardımcı olma dürtülerine bağlıdır.

Sosyal mühendislik, güvenlik ihlali konularında insan faktörünü devreye sokar ve bir silah olarak kullanır. Çalman veya taklit edilen çalışan veya satıcı kimlikleri güvenlikli yerlere giriş hakkı sağlayabilir. Saldırgan daha sonra önemli varlıklara erişim elde edebilir. Çalışanların, teknik servise veya sözleşmeli çalışanlara yardımcı olma isteğinden faydalanarak, bir saldırgan bir kurumun güvenliğini aşabilir ve erişim hakkı kazanabilir.

Bir kurumun dışarıyla iletişim kuran ilk çalışanları, örneğin resepsiyonistler ve yönetici asistanları, çoğu zaman sosyal mühendislik saldırılarının hedefleridir. Kurumun yapısı hakkında biraz bilgisi olan saldırganlar, yeni, eğitim almamış çalışanları ve güvenlik politikasından pek anlar gibi görünmeyen kişileri de hedef alacaktır.

Sosyal mühendislik saldırılarını durdurmak zor olabilir, fakat saldırıların etkisini azaltmak için bazı teknikler vardır:

- Çalışanların güvenli bir ortam konusunda temel bir eğitim almalarını sağlayınız.

- Bir bilgisayar kullanım ve güvenlik politikası geliştiriniz.
- İç ve dış teknik destek süreçleri hakkında katı bir politika uygulayınız.
- Bütün çalışanların kimliklerinin doğrulanmasını gerektiriniz.
- Dizinlerde, ilan sayfalarında, web sitelerinde ve kamuya açık veri tabanlarında bulunan herkesin erişebileceği verinin miktarını sınırlandırınız.
- Uzaktan erişim kullanıyorsanız çok dikkatli olunuz. Kimlerin ağınıza girdiğini bilmek için çok güçlü kimlik doğrulama teknikleri kullanınız.
- Güvenli mail alma ve gönderme teknikleri için çalışanlarınıza eğitim veriniz.
- Gizli veya hassas dokümanları ince şeritlere ayırarak yok ediniz.

Oltalama

Dolandırıcılık internet üzerinde gün geçtikçe büyüyen bir sorundur. Oltalama (Phishing} bir saldırganın kurbanını kredi kartı numaraları, parolalar, doğum tarihi, banka hesabı numarası, ATM şifresi veya Sosyal Güvenlik Numarası gibi gizli bilgilerini vermek için kandırdığı bir dolandırıcılık türüdür.

Oltalama saldırıları e-posta veya anlık iletiler ile kimlik hırsızlığı yapmaya çalışmaktır. Bu mesajlar, güvenilen bankalar veya finansal kurumlar gibi gerçek kaynaklardan geliyormuş gibi görünürler ve kişisel bilgiler için acil bir istek içerirler. Oltalama mesajları genellikle (banka, kredi kartı gibi) önemli hesap bilgilerinin hemen değiştirilmesini ister. Mesaj kurbana istenen bilgiyi ya doğrudan göndermesi ya da verilen bir linke tıklayarak girmesini talimat verir. Linke tıklamak kurbanı sahte bir web sitesine götürür. Bu web sitesi resmi siteye tıpatıp benzer, fakat saldırganın kendi yaptığı bir sitedir. Bu sayfaya girilen kişisel bilgiler asıl kuruma değil saldırgana gider.

Oltalama saldırılarının bir başka türü de hedef odaklı oltalamadır (spear phishing). Hedef odaklı oltalama, e-posta veya anlık iletiler kullanarak belirli bir kurumu hedef alır, gizli veriye yetkisiz erişimi hedefler. Sıradan oltalama mesajlarında olduğu gibi hedef odaklı oltalama mesajları da güvenilir bir kaynaktan geliyormuş gibi görünür.

Her tür oltalama saldırısından korunmanın en iyi yolu şüpheli bir e-postadaki linke tıklamamaktır. Bir e-posta veya anlık ileti ile istendi diye kişisel bilgileri önünüze gelen bir web sitesine girmek çok kolay olabilir. Eğer bu isteğin doğru olduğunu düşünüyorsanız herhangi bir bilgiyi girmeden önce şirketin müşteri hizmetleri destek hattını aramalısınız. Eğer şirketi arayacaksınız, şüpheli mesajda verilen hiçbir telefon numarasını kullanmayınız. Mesajda verilen web adresi doğru görünse dahi, mesajdaki linke tıklamak yerine web adresini tarayıcınıza kendiniz yazarak giriniz.

Bir Oltalama Dolandırıcılığı Nasıl Tespit Edilir?

Sadece gelen e-posta mesajında tıkladığınız linke bakarak oltalama dolandırıcılığını tespit etmek zor olabilir. Fakat göndericinin adresindeki bazı ipuçları dolandırıcılığı ortaya çıkarabilir. Şunlara dikkat ediniz:

- Oltalama yapanlar genellikle gerçek adreslerdeki karakterleri benzer karakterler ile değiştirirler. Örneğin, Paypal.com adresindeki küçük L harfi yerine 1 (rakam olarak) kullanabilirler (Paypa1.com).
- Oltalama hileleri o kadar gelişti ki artık oltacılar gerçek bağlantıları hatta asıl sitenin güvenlik sertifikasını kullanıyormuş gibi görünebilirler. Bir bağlantıya tıklamadan önce bağlantının sizi nereye götüreceğine dikkat ediniz. Eğer alan adı tuhaf görünüyorsa bağlantıya tıklamayınız. Bunun yerine, asıl web sitesinin müşteri hizmetlerini veya teknik destek hattını arayarak bağlantının geçerli olup olmadığını sorunuz. Bu yaklaşım zaman alabilir fakat bağlantılara hiç kontrol etmeden tıklamaktan daha güvenlidir.
- Bazı oltacılar gerçek şirketlerin adresine benzeyen alan adlarını satın alırlar - örneğin walmartorder. com gibi. Asıl şirket Wal-Mart'tır fakat şirketin alan adında order kelimesi geçmemektedir.
- Bir başka taktik de aynı alan adını .com uzantısı yerine .org uzantısıyla kullanmaktır. Bu alan adını kullanan dolandırıcılar daha sonra milyonlarca e-posta gönderip müşterilerden hesap bilgilerini, doğum tarihlerini, Sosyal Güvenlik numaralarını ve diğer bilgilerini doğrulamalarını isterler. Kaçınılmaz bir şekilde, bazı bilgisayar kullanıcıları bu mesajlara cevap verirler. Bütün alan adını dikkatlice kontrol ediniz!

Oltalama Dolandırıcılığını Önleme Çalışma Grubu (Anti Phishing Working Group - APWG) sahtekârlık ve kimlik hırsızlığı gibi e-posta dolandırıcılıklarının neden olduğu sorunları ortadan kaldırmaya çalışan endüstri tabanlı

küresel bir yasa uygulama birliğidir. Daha fazla bilgi edinmek için APWG web sitesini www.antiphishing.org adresinde ziyaret edebilirsiniz. Ayrıca, Federal Ticaret Komisyonu (FTC) web sitesi (www.ftc.gov) tüketiciler için oltalama aktivitelerini ve kimlik hırsızlığı sorunlarını bildirebilecekleri bir form ve e-posta adresi bulundurmaktadır.

Web Sitesi Trafiğinin Yönlendirilmesi

Web sitesi trafiğinin yönlendirilmesi (pharming) alan adı değiştirerek kişisel ve finansal bilgileri elde etmeye çalışan bir saldırı türüdür. Fakat web sitesi trafiğinin yönlendirilmesi saldırısı kurbanlarını geçerli sitelere benzeyen sahte sitelere çekmek için mesajlar kullanmaz. Bunun yerine alan adı sunucusunda (Domain Name Server - DNS) bulunan bir alan adını "zehirler". Bu sürece DNS zehirlenmesi (DNS poisoning) denir. Sonuç olarak, bir kullanıcı zehirlenmiş sunucunun web adresini kendi adres çubuğuna girdiğinde saldırganın sitesine ulaşır. Kullanıcının tarayıcısı hala gerçek web adresini gösterir ki bu durum web sitesi trafiğinin yönlendirilmesinin tespitini zorlaştırmakta ve sonuçlarım daha da ciddi hale getirmektedir. Oltalama e-posta ve anlık ileti yoluyla kişileri teker teker dolandırmaya çalışırken; web sitesi trafiğinin yönlendirilmesi, alan adını değiştirerek büyük insan gruplarını dolandırır.

Kötücül Yazılım Nedir?

Bütün yazılımlar iyi amaçlara hizmet etmezler. Bazı yazılımlar bir veya daha fazla hedef bilgisayara sızar ve bir saldırganın talimatlarını izlerler. Bu talimatlar zarar vermeyi, güvenlik yetkilerini yükseltmeyi, mahrem verileri ifşa etmeyi ve hatta veriyi silip değiştirmeyi içerebilir. Bu tür yazılıma kötücül yazılım (malicious software) veya kısaca malware denir. Kötücül yazılımın amacı sistemi zarara uğratmak ve çalışmasını aksatmaktır. Kötücül yazılımın etkileri bir masaüstü bilgisayarını yavaşlatmaktan çökertmeye, kredi kartı numaraları hırsızlığına ve daha kötü şeylere kadar uzanabilir. İnternette gezinmek, e-posta okumak, müzik veya diğer dosyaları indirmek kişisel bir bilgisayara kötücül yazılım bulaştırabilir - bu genellikle kullanıcının bilgisi olmadan gerçekleşir.

Kötücül yazılım iki temel kategoride yer alır: bulaşıcı (infecting) programlar ve saklanan (hiding) programlar. Bulaşıcı programlar aktif olarak kendilerini diğer bilgisayarlara kopyalamaya çalışırlar. Bunların asıl amacı bir saldırganın talimatlarını yeni hedeflerde çalıştırmaktır. Bu tür zararlı yazılımlar aşağıdakileri içerir:

- Virüsler
- Solucanlar (worms)

İsimlerinin ima ettiği gibi, saklanan programlar bilgisayarda saklanırlar ve saldırganın talimatlarını fark edilmeden gerçekleştirirler. Saklanan kötücül programlar aşağıdakileri içerir:

- Truva Atları (Trojan Horses)
- Rootkitler (Rootkits)
- Casus yazılım (Spyware)

Virüsler

Bir bilgisayar virüsü kendisini başka bir bilgisayardaki bir programa kopyalayan veya iliştiren bir yazılım programıdır. Virüsün amacı programı asıl geliştiren kişinin tasarlamadığı talimatları çalıştırmak için diğer bilgisayarı kandırmaktır. Kullanıcılar virüs bulaşmış dosyaları ağdaki diğer bir bilgisayardan, bir flash bellekten veya internetteki bir hizmetten kopyalar. Bundan farklı olarak kullanıcılar evdeki bilgisayarlarında bulunan virüsleri getirip, internete ve diğer ağ hizmetlerine erişimi olan taşınabilir bilgisayarlarında çalışabilirler.

Bir bilgisayar virüsü biyolojik bir virüse benzer şekilde çalışır. Bir programa "bulaşır" ve bulaştığı programın kendisini diğer bilgisayarlara kopyalamasına neden olabilir. Virüs herhangi bir programa bağlı olmadan var olamaz ve bir hedeften diğerine bulaşıcı bir biçimde yayılır.

Kaydedilen ilk bilgisayar virüsü araştırmacı Bob Thomas tarafından 1971 yılında yazılan Creeper virüsüydü. Creeper kendisini ağdaki diğer bilgisayarlara kopyalayıp ekranlarında "Benim adım Creeper, yakalayabiliyorsanız yakalayın beni!” mesajını gösteriyordu. Thomas bu kendini çoğaltan, deneysel virüsü ağdaki bilgisayarların bu tür programlardan nasıl etkilendiklerini görmek için tasarladı. Creeper sisteme sokulduktan kısa bir süre sonra araştırmacılar Creeper'ı bulmak ve yok etmek için Reaper programını ortama saldılar.

Günümüzde bilinen yüz binlerce virüs her tür programa bulaşmaktadır. Virüslerin asıl endişelendirici yanı kendilerini sıklıkla kullanılan programlara bulaştırmalarıdır. Kullanıcılar bu virüslü programları çalıştırdıklarında, aslında kendi parolaları ve yetkileri ile virüs kodunu çalıştırmaktadırlar. Virüs yetkilerini artırmak zorunda kalmaz; virüs bulaşmış programı çalıştıran kullanıcı virüse kendi yetkilerini ve izinlerini kullandırtmış olur.

Zamanla, virüsler daha akıllı hale geldiler. Örneğin, bazı virüsler kötücül yazılımı tespit eden programların virüs tanıma fonksiyonlarını devre dışı bırakarak kendilerini koruyabilirler. Virüsler bulaştıkları dosyaların boyutlarını artırdıkları için kolayca tespit edilebilirler. Buna önlem olarak bazı virüsler bulaştıkları dosyaların boyutlarını virüs bulaşmadan önceki kadar göstererek denetimden kurtulmaya çalışırlar. Böylece, hiçbir şey değişmemiş gibi görünür.

Solucanlar

Bir solucan (worm) kullanıcıların girdilerine veya eylemlerine ihtiyaç duymadan kendisini çoğaltarak kopyalarını, genellikle bir ağ üzerinden, diğer bilgisayarlara gönderebilen bağımsız (self-contained) bir programdır. Solucanın amacı, basitçe, ağı gereksiz yere kullanarak ağın bant genişliğini azaltmak veya başka zararlı eylemlere kalkışmak olabilir. Solucanla virüs arasındaki fark solucanın bulaşmak için üzerinde yaşayacağı bir programa ihtiyaç duymamasıdır. Solucan tek başına (standalone) bir programdır.

Dünyada “kontrolsüzce’’ yayıldığı tespit edilen ilk solucan Morris solucanıydı. Robert Tapan Morris bu solucanı 1988'de yazdı. Motris solucanı bir arabellek taşması (buffer overflow) açığına saldırmaktaydı. Morris solucanın asıl gayesi Unix işletim sistemi sürümlerine sahip olan bilgisayarlara bulaşarak internette yayılmak ve bu sayede internetin boyutlarını tahmin etmekti. Yine de, solucan yazarının tahmininden daha hızlı yayıldı. Sonunda, solucan bilgisayarlara birçok defa bulaştı ve bulaştığı bilgisayarları kullanılamayacak kadar yavaşlattı. Morris solucanı medyanın ilgisini çeken ilk kötücül yazılım oldu ve Amerika Birleşik Devletlerinde 1986 Bilgisayar Kullanımı ve Sahtekârlığı Yasası (US. 1986 Computer Use and Fraud Act) kapsamında verilen ilk cezayla sonuçlandı.

Truva Atları

Bir Truva Atı (Trojan borse), aynı zamanda Truva da denir, kendisini faydalı bir programmış gibi gösteren kötücül bir yazılımdır. Adı meşhur Truva atından gelir. Bu hikâyede, Truva ile 10 yıldır savaşta olan Yunanlar büyük bir tahta at yapıp Truvalılara "hediye" olarak verirler. Truvalılar atı, bir barış teminatı olarak görüp, şehrin içine alırlar. O gece Truvalılar uyurken atın oyuk karnında saklanan Yunanlı askerler dışarı tırmanırlar ve şehir kapılarını açıp Yunan ordusunun kalan kısmını şehre alırlar. Yunanlılar o gece Truva’yı tamamıyla mağlup ederler.

Benzer bir şekilde, Truva atı programlan dış görünüşlerini kullanarak kullanıcıları kendilerini çalıştırmaları için aldatırlar. Bu programlar faydalı işler yapıyormuş gibi görünürler, fakat aslında kötücül kod içerirler. Program çalışmaya başladığında, saldırı talimatları kullanıcının izni ve yetkisi olmadan yürütülür.

İlk bilinen Truva atı programı 1974’te yaratılan Animal’dır. Animal kendisini basit bir soru cevap oyunu olarak gösterip kullanıcılara bir hayvan adı seçtirir ve adı tahmin edebilmek için sorular sorardı. Ancak, soru sormaya ek olarak, program kendisini kullanıcının yazma yetkisinin olduğu bütün dizinlere kopyalardı.

Günümüz Truva atları kendilerini kopyalamaktan çok daha fazlasını yapmaktadırlar. Truva atları mahrem bilgileri saklayan, bilgisayarlara arka kapılar açan veya aktif olarak dosya indiren veya gönderen programlar içerebilirler. Yapabilecekleri şeylerin listesi neredeyse sınırsızdır.

Rootkitler

Rootkitler diğer kötücül yazılımlara göre daha yeni bir türdür. 1990 yılma dek görülmediler. Bir rootkit bir veya daha fazla programı değiştirerek veya bunların yerine geçerek saldırısının izlerini gizler. Rootkitler izlerini gizlemek için genellikle işletim sisteminin parçalarını değiştirseler de, aslında bilgisayarın boot komutlarından işletim sisteminde koşan uygulamalara dek her seviyede var olabilirler. Rootkitler bir defa kurulduklarında, başka saldırılar başlatmaları için saldırganların sızılmış bilgisayarlara kolay bir şekilde erişimlerini sağlar.

Rootkitler birçok işletim sistemi için yazılmışlardır, bunlara Linux, Unix ve Microsoft Windows dâhildir. Çok fazla türde rootkit olduğu için ve bir defa makineye kurulduklarında kendilerini çok iyi gizledikleri için, rootkitleri tespit etmek ve kaldırmak çok zor olabilir. Buna rağmen, rootkitleri tespit etmek ve kaldırmak

güvenli bir sistem için çok önemlidir. Host tabanlı bir saldırı tespit programı (host based-IDS) rootkit aktivitesini tespit etmede yardımcı olabilir.

Sisteminizde bir rootkit tespit ederseniz, en iyi çözüm işletim sistemini orijinal kaynağından yeniden kurmanızdır. Bu, kullanıcı ve uygulama verilerini daha önce aldığınızı var saydığımız kopyalardan yeniden kurmanız ve yenilemenizi gerektirir. Eğer sisteminizin dokümanlarını iyi tutmadıysanız, bunları yapmak daha zor olabilir. Bir saldırganın rootkit kurmasını sağlayacak yetkisiz bir erişimi engellemek, kurulmuş bir rootkiti kaldırmaya çalışmaktan daha etkilidir.

Rootkitler genellikle diğer kötücül programlarla beraber çalışırlar. Örneğin, malware.exe isimli bir programın Windows üzerinde çalıştığını düşününüz. Basit bir rootkit Windows Görev Yöneticisini başka bir yönetici ile yer değiştirerek malware.exe isimli dosyanın gösterilmemesini sağlayabilir. Sistem yöneticileri artık kötücül programın çalıştığını bilemezler.

Casus Yazılım

Casus yazılım (spyware) özellikle bilginin gizliliğini (confidentiality) tehdit eden bir kötücül yazılım türüdür. Bu yazılım kullanıcının izni olmadan internet bağlantısı üzerinden bilgi toplar. Casus yazılım internetten indirilen, ücretsiz olan kamuya açık yazılım (freeware) veya paylaşılan (shareware) yazılım programlarının, Truva atına benzer bir şekilde, gizli bir bileşeni olarak gelir. Casus yazılım ayrıca uçtan uca (peer-to-peer) dosya paylaşımı ile de yayılır. Casus yazılımlar 1990'la-nn sonundan beri varlar ve 2000'den sonra daha popüler oldular, internetin hızlı büyümesi saldırganların hiçbir şeyden haberi olmayan daha fazla kullanıcının bilgisini toplamasını kolaylaştırdı.

Casus yazılım bir defa kurulduktan sonra, kullanıcının internet üzerindeki davranışlarını gözetler. Casus yazılım e-posta adresi ve hatta parolalar ve kredi kartı numaraları gibi bilgileri de toplayabilir. Casus yazılım daha sonra elde ettiği veriyi yazılımı yazan kişiye iletir. Yazılımı yazan kişi bu bilgiyi, basitçe, reklam veya pazar araştırması için kullanabilir ama isterse bu bilgiyle kimlik hırsızlığını kolaylaştırabilir.

Bilgi çalmaya ek olarak, casus yazılım hem elde ettiği veriyi üçüncü partilere iletmeye çalışırken internet bağlantısını kullanarak hem de bilgisayarın kaynaklarını kullanarak kullanıcıdan çalma gerçekleştirir. Birden fazla casus yazılım çalıştıran bilgisayarlar temiz bilgisayarlara göre oldukça yavaş çalışırlar. Ayrıca, casus yazılım bellek ve diğer sistem kaynaklarını kullandığı için sistemlerde düzensizliğe ve hatta çökmelere neden olabilir.

Casus yazılım bağımsızca yürütülebilen (executable) bir program olduğu için, aşağıda verilen listedekileri de içeren bazı işlemleri gerçekleştirebilmektedir:

- Basılan tuşları izlemek,
- Sabit diskteki (hard disk) dosyaları taramak,
- Sohbet (chat) programları ve kelime işlemciler (word processors) gibi diğer uygulamaları izlemek,
- Diğer casus yazılım programlarını kurmak,
- Tarayıcı çerezlerini okumak,
- Web tarayıcıdaki varsayılan ana sayfayı değiştirmek.

Reklam Yazılımı

Reklam yazılımı (Adware) casus yazılıma benzer fakat kişileri ayırt edebilecek bilgileri (Kişisel Tanımlama Bilgisi, Personally Identifiable Information - Pil) iletmez. Pil kişileri ayırt etmeye yarayan bilgilerdir. Pil örnekleri sürücünün ehliyet numarası. Sosyal Güvenlik numaraları (TC Kimlik Numarası) ve kredi kartı numaraları vb. bilgileri içerir. Reklam yazılımının topladığı bilgiler pazarlama kampanyalarını geliştirmek için kullanılır. Örneğin, reklam yazılımı, satın alma alışkanlıklarına göre uyarlanmış açılır pencereler (pop-up) sağlamaya yardımcı olabilir veya pazar araştırması amacıyla kullanılabilir.

Bir açılır pencere (popup) tarayıcıda en üstte açılan bir pencere türüdür. Bu pencereler genellikle reklam içerir. Açılır pencereler tam anlamıyla reklam yazılımı olmasalar da, çoğu reklam yazılımı kullanıcılarla iletişim kurmak için bu pencereleri kullanır. Bazı yazılım ürünleri açılır pencereleri engellemek için bir seçenek sunar.

Casus ve reklam yazılımları, hızlı ve artan bir şekilde bilgisayarlar için oldukça yaygın tehditlere dönüştüler. Bazı uzmanlar bilgisayarların %90'dan fazlasına bu yazılımların çoktan bulaşmış olduğunu tahmin ediyor.

Neyse ki, bazı yazılım sağlayıcıları casus ve reklam yazılımlara karşı yazılımlar üretmektedirler. Aslında, anti virüslerin ve genel kötücül yazılımla mücadele programlarının çoğu casus ve reklam yazılımları da tespit edip kaldırıyor. Kurumunuzun ihtiyaçları doğrultusunda bu programları inceleyip size en uygun olanını bulmak zor olduğu kadar önemli de bir görevdir.

Saldırıların Genel Türleri Nelerdir?

Saldırganın hedefine ve amacına bağlı olarak birçok saldırı türü saldırganın gereksinimine ve yeteneğine uygun olabilir. Bu saldırılar üç kategoride özetlenebilir:

- Kullanılabilirliğe yönelik saldırılar - Bu saldırılar, hayati önemdeki bir sistemin, uygulamanın veya verinin erişimini ve çalışmasını etkiler.
- İnsanlara yönelik saldırılar - Bu saldırılar, hile ve zorlama ile diğer bir kişinin bilgi paylaşmasını veya bir eylemi gerçekleştirmesini (örneğin, şüpheli bir URL linkine tıklamasını veya bilinmeyen bir e-posta adresinden gelen e-posta eklentisini açmasını) içerirler.
- BT varlıklarına yönelik saldırılar - Bu saldırılar, sızma testleri, yetkisiz erişim, yetkilerin artırılması, parola çalınması, veri silinmesi veya bir veri ihlali gerçekleştirmeyi içerirler.

Sosyal Mühendislik Saldırıları

Sosyal mühendislik, kişileri zorlayarak veya kandırarak bir şeyi yaptırma veya bir bilgiyi ifşa etmesini sağlama sanatıdır. Günlük hayatımızda bunu her zaman kullanırız. Çocuklar ebeveynlerinden izin almak veya istedikleri bir şeyi yaptırmak için sosyal mühendisliği kullanırlar. Bir eş olarak, eşinizi sizin yapmanız gereken küçük işleri yapmaya ikna edebilirsiniz. Suçlular ve sahtekârlar da bundan farklı değildir: Sosyal mühendislik taktiklerini insanlardan kendileri veya başkaları hakkında bilgi almak için kullanırlar. Bu, kimlik hırsızlığı için kişisel bilgileri toplamada anahtar noktadır. Bilgisayar korsanları ayrıca, bilişim sistemleri ve uygulamaları hakkında bilgi vermeye ikna etmek için seçilen çalışanlar üzerinde sosyal mühendislik taktiklerini denerler ve bu sayede erişim izni kazanırlar.

Bilgisayar korsanları ve sisteme giren kişiler kurbanlarına çok farklı sosyal mühendislik taktikleri uygularlar. Kurumunuza veya size karşı kullanılabilecek sosyal mühendislik taktiklerinin bir özeti aşağıda listelenmektedir:

- Otorite (Authority) - Kurumdaki yüksek bir pozisyonu kullanarak bir kişiyi bilgiyi vermeye ikna etmek veya zorlamak.
- İttifak/sosyal kanıt (Consensus/social proof) - "Herkes böyle yapıyor" diyerek bir şeyi yapmanın doğru ve kabul edilebilir olduğunu söylemek.
- Çöp karıştırma (Dumpster diving) - İnce kıyılarak çöpe atılmış belgelerden kimlik hırsızlığı için kullanılabilecek hassas ve gizli bilgiler bulmaya çalışmak.
- Yakınlık/Beğenme (Familiarity/liking) - Kurbanla sık sık iletişim kurup yakınlık ve aşinalık kurmak (örneğin, bir kargo görevlisi zamanla ofis çalışanı ile samimiyet kurabilir) ve bu sayede tanınan kişiye yardımcı olması için kurbanı cesaretlendirmek.
- Hileler (Hoaxes) - Yanlış veya sahte bir izlenim yaratarak bir kişiye bir şey yaptırmak veya kişiyi bilgi vermeye ikna etmek.
- Taklit (Impersonation) - Bir kişinin (mesela bir teknik destek çalışanı, bir kargocu veya bir banka temsilcisi) yerine geçmek.
- Korkutma(Intimidation) - Güç kullanarak bir kişiye bir şey yaptırmak veya bir şeyi açıklamasını sağlamak.
- Yetersizlik(Scarcity) - Bir şeye sahip olmamakla veya bir şeye erişim hakkını kaybetmekle korkutarak kişiye bir iş yaptırmak veya bir bilgiyi açıklamaya zorlamak.
- Omuz sörfü (Shoulder surfing) -Veri giren kişinin omuzunun üstünden bilgisayar ekranına bakmak.
- Öndeki kişinin yakınından gitmek (Tailgating) - Bir kişinin hemen arkasından yürüyerek güvenli bir kapıdan veya giriş bölgesinden gizlice geçmek.
- Güven (Trust) - Zaman içinde bir güven bağı oluşturup daha sonra bu güven bağı ile kişiye bir şey yaptırmak ya da kişiden bir bilgiyi öğrenmek.

- Aciliyet/Öncelik (Urgency) - Öncelikli veya acil stres durumunu kullanarak birisinden bilgi almak veya bir işe zorlamak (örneğin, ara holde bir yangın olduğunu söylemek ön kapıdaki güvenlik görevlisini masasından ayırabilir).
- Telefonla kişisel bilgilerin el geçirilmesi (Vishing) - Telefonla bir oltalama saldırısı gerçekleştirerek, (tatlı sözlerle) konuşarak kişisel bilgi edinmeye çalışmak veya kurbanı bir işe zorlamak.
- Balina avı (Whaling) - En üst düzey kullanıcıyı veya en değerli çalışanları, yani "büyük balık" veya "balina" gibi görülen kişileri hedef almak (çoğu zaman hedef odaklı oltalama (spear phishing) denir).

Kablosuz Ağ Saldırıları

Kablosuz ağ saldırıları kablosuz ağ üzerinde trafiği izlemek, paket yakalamak ve sızma testleri yapmak gibi saldırıları içerir. Hem kamuya açık hem de özel alanlardaki artan kablosuz ağ kullanımını göz önünde bulundurursak mobil kullanıcı her zaman tehdit altındadır. Kablosuz ağlar bilişim alt yapınızda ağa erişim noktası olarak ele geçirilebilirler. Gerekli kablosuz ağ güvenlik kontrollerinin hayata geçirilmesi, kablosuz ağlarda oluşacak risklerin, tehditlerin ve güvenlik açıklarının giderilmesi için anahtar bir rol oynar. Bilgisayar korsanları ve ağa sızmaya çalışan kişiler tarafından kablosuz ağlara sızma ve saldırma girişimlerinde birçok farklı taktik kullanılmaktadır.

Kablosuz ağ saldırılarının bir özeti aşağıdaki gibidir:

- Bluejacking - Bluejacking, kullanıcının telefonu ve kulaklığı arasındaki Bluetooth kablosuz iletişim bağlantısının kırılması ve ele geçirilmesidir.
- Bluesnarfing - Bluetooth cihazları arasındaki paket trafiğinin izlenip kopyalanmasıdır.
- Kötü ikiz (Evil twin) - Özel veya herkese açık bir kablosuz ağmış gibi davranarak ağa bağlanmaya çalışan her kullanıcının paketlerini izlemek.
- IV saldırısı - İletilmekte olan bir şifrelenmiş IP paketinin başlangıç vektörünü (Initialization Vector - IV) değiştirerek zaman içerisinde genel şifreleme anahtarını kırma çabasıdır.
- Frekans bozumu/Araya girme (Jamming/Interference) - Kablosuz erişim noktaları ile aynı frekansta radyo dalgaları göndererek kablosuz iletişime karışmak ve bozmak, böylece normal kullanıcılara verilen hizmeti sekteye uğratmak.
- Yakın alan iletişim saldırısı (Near field communication attack) - Çok yakın mesafeden (bir kaç santimetreden) mobil işletim sistemli iki cihazın iletişiminin arasına girmek.
- Paket koklamak (Packet sniffing) - Bir kablosuz ağın IP paketlerini yakalamak ve Wireshark gibi araçlar kullanarak TCP/IP paket verilerini analiz etmek.
- Yeniden gönderme saldırıları (Replay attacks) - Kimlik doğrulama işlemi yapıyormuş gibi önceki bir IP paket akışını bir sunucuya yeniden göndererek sunucuyu kandırmak.
- Sahte erişim noktaları (Rogue access points) - Yetkisiz bir ağ cihazını kullanarak, hiçbir şeyden şüphelenmeyen kullanıcılara kablosuz ağ hizmeti sunmak.
- War chalking - Kablosuz erişim noktalarının ve ağlarının fiziksel ve coğrafi konumlarının bir haritasını çıkarmak.
- War driving - Fiziksel olarak bölgelerin veya iş merkezlerinin etrafında dolaşarak açık ve herkes tarafından kullanılabilir ağ bağlantıları sunan kablosuz erişim noktaları ve ağları aramak.

Bu belirli saldırılara ilaveten, bilgisayar korsanları hedef tarafından kullanılan kablosuz şifreleme tekniklerindeki zayıflıkları da kullanabilirler: WEP (Wireless Encryption Protocol - Kablosuz Şifreleme Protokolü), WPA (Wi-Fi Protected Assets - Wi-Fi Korumalı Varlıklar) ve WPS (Wi-Fi Protected Setup - Wi-Fi Korumalı Kurulum).

Web Uygulama Saldırıları

Web uygulama saldırıları (application attacks), internete açık ara yüzü bulunan web sunucularına, uygulamalara ve veri tabanlarına sızma testleri yapmayı içerir. E-ticaret, müşteri veya üye web siteleri ve portallarının sayısının hızlı artışı nedeniyle gizli verilere, hassas verilere ve fikri eserlere erişim çok fazladır. Bilgisayar korsanları ve sisteme sızmak isteyenler, uygulamalara sızmak ve saldırmak için çok farklı taktikler kullanmaktadırlar.

İnternet üzerinde herkesin erişimine açık olan web uygulamaları, aşağıdakileri içeren web uygulama saldırıları ile karşılaşmaktadır:

- Rastgele/uzaktan kod yürütmek (Arbitrary/remote code execution) - Yetkili erişime veya sistem yöneticisinin erişim haklarına sahip olunursa, saldırgan uzaktaki sistemde keyfi olarak komutlar çalıştırabilir ya da bir komutu yürütebilir.
- Arabellek taşması (Buffer overflow) -Arabelleğin kabul edebileceğinden fazla veriyi göndermeye çalışmak, daha fazla açığın oluşabileceği bir durum yaratılmasıdır.
- İstemci-tarafı saldırısı (Client-side attack) - Bir iç ağda bulunan kullanıcının iş istasyonunda veya diz üstü bilgisayarında bulunan kötücül yazılımı kullanarak, internetteki (korunan ağın dışındaki) kötücül bir sunucu veya uygulama ile birlikte hareket etmek.
- Çerezler (Cookies) ve eklentiler (Attachments) - Çerezleri ve diğer eklentileri (veya içerdikleri bilgileri) güvenliği ihlal etmek için kullanmaktır.
- Çapraz site betikleme (Cross site scripting - XSS) - Bir web uygulama sunucusuna betikler enjekte edip, saldırıları istemci tarafına yöneltmektir. Bu saldırıda, web uygulamasına değil de sunucunun kullanıcılarını kullanarak sunucuya erişen diğer bilgisayarlara saldırı başlatılır.
- Dizin gezme/komut enjekte etme (Directory traversal/commandinjection) - Bir web uygulama sunucusunu istismar ederek, root dosya dizinine korunan ağın dışından erişim sağlamak, sunucuda komut çalıştırmak ve sunucudaki verilerin kopyasını almaktır.
- Başlık manipülasyonu (Header manipulation) - Çerezleri ve tarayıcı URL adres bilgilerini çalmak ve başlığı geçersiz ve yanlış komutlarla değiştirerek güvensiz bir iletişim veya eylem yaratmaktır. Tamsayı taşması (Integer overflow) - Sistemin izin verdiği en büyük tamsayıyı aşan bir matematiksel arabellek taşması oluşturmaktır. Bu, finansal veya matematiksel uygulamaların donmasını veya bir güvenlik açığı oluşturmasını sağlayabilir.
- Hafifletilmiş Dizin Erişim Protokolü'ne enjeksiyon (Lightweight Directory Access Protocol - LDAP) -Sahte ya da taklit kimlikler yaratarak, ve LDAP komutlarını ve paketlerini yanlış ID'ler için kimlik doğrulaması yapmak ve bir web uygulamasına kimlik doğrulaması yapmak.
- Yerel paylaşılan nesneler (Local shared objects - LSO) - Tarayıcının yapılandırma ayarları ile silinemeyen flash çerezlerini (adlarını Adobe Flash Oynatıcısından alırlar) kullanmak. Flash çerezler ayrıca kullanıcının sildiği veya engellediği sıradan tarayıcı çerezlerini yerlerine geri koyabilirler.
- Kötücül eklentiler (Malicious add-ons) - Yasal programların veya uygulamaların üzerinde ek kötücül yazılım çalıştıran takılabilir (plug-in) ve eklenti (add-on) yazılımları kullanmaktır.
- SOL enjeksiyonu (SQL injection) - Yapısal Sorgulama Dili (Structured Query Language - SQL) komutları enjekte ederek arka uç (back-end) SQL veri tabanından bilgi ve veri almaktır.
- Suyun başı saldırısı (Watering-hole attack) - Hedefteki bir kullanıcıyı sıklıkla ziyaret edilen bir web sitesine çekerek, kullanıcının bu web sitesine yüklenmiş kötücül kod veya yazılıma farkına varmadan tıklayarak bir saldırı başlatmasını sağlamaktır.
- XML enjeksiyonu (XML injection) - XML etiketlerini (tags) ve verilerini bir veri tabanına enjekte ederek veri almaya çalışmaktır.
- Sıfırıncı-gün (Zero-day) - Henüz belirli bir savunmanın bulunmadığı yeni bir güvenlik açığını veya yazılım hatasını kullanma.

Önlem Nedir?

Kurumunuzu bilgisayar saldırılarından korumanın basit önlemleri yoktur. Güvenlik açıklarım tespit eden, saldırıları engelleyen ve başarılı saldırıların etkilerine başarıyla cevap verebilen karşı önlemler üzerinde yoğunlaşmaksınız. Bu kolay değildir fakat hiçbir şey yapmamaktan daha iyidir. Bilgisayar ve ağ saldırılarıyla başa çıkmak BT alanında iş yapmanın bedelidir.

Zeki saldırganlar ve izinsiz giren kişiler, bilgisayarlara ve ağ kaynaklarına saldırmak için yeni metotlar icat etseler de, bu metotların çoğu zaten bilindiktir ve birkaç uygun araçla yok edilebilirler. En iyi strateji, güvenlik açıklarını tespit etmek ve saldırıları daha olmadan engellemek için açıkların sayısını azaltmaktır.

Saldırıları önlenmek en büyük önceliğiniz olmalıdır. Buna rağmen, bazı saldırılar başarılı olacaktır. Sizin bu saldırılara olan tepkiniz saldırının kendisi kadar saldırgan, proaktif ve reaktif (tepkisel) olmalıdır. Saldırılara, bilgisayar ve ağ kaynaklarını hızlıca yenileyerek, kuruntunuzun savunmasındaki boşlukları kapatarak ve

suçluları cezalandırmak için gerekli kanıtları toplayarak karşılık verebilirsiniz. Elbette, bir saldırıdan öğrendiğiniz dersleri ağı benzer saldırılardan korumakta kullanmalısınız.

Saldırılara karşılık vermek için planlama, politika oluşturma ve olay yeri inceleme amaçlı çalışmalar yapmanız gerekir. Neyse ki, güvenlik güçleri, olay yeri inceleme uzmanları, güvenlik danışmanları ve bağımsız çalışan uzman ekipler size hem güvenlik ihlaline cevap vermede hem de suçluları yakalamada yardımcı olabilirler. Ayrıca birçok kurum güvenlik ihlalleri ile başa çıkmak üzere uzman ekipler bulundurur. Bu güvenlik olay müdahale ekipleri (security incident response team - SIRT) ihlalleri tespit etme ve bunların verdiği zararı en aza indirip saldırının kanıtlarını sonraki adli safhalar için koruyabilme konularında bilgilidirler.

Gelecek bölümleri okudukça birçok karşı önlem hakkında bilgi sahibi olacaksınız. Başlangıç olarak, bu bölüm size BT altyapınızı korumak için alabileceğiniz en yaygın bir kaç önlemi tanıtacak. Bu önlemlerden bazılarını aynı zamanda tehditlere, güvenlik açıklarına ve devam eden kötü niyetli saldırılara müdahale etmek için de kullanabilirsiniz.

Kötücül Yazılımı Önlemek

Kötücül yazılım hem kişisel ağlara hem de şirket ağlarına saldırılar için bir platform sunar. Kötücül yazılım karşıtı önlemler bu saldırılara karşı ilk savunma hattıdır. Bulunduğunuz ortama zararlı yazılımların sokulmasını engellemek için adımlar atmalısınız. Kötücül yazılıma engel olmak, kötücül yazılımın verdiği zararı telafi etmekten her zaman daha iyidir. Kötücül yazılıma engel olmak için bir güvenlik programı geliştirmelisiniz.

Kötücül yazılımı engellemek için atılabilecek altı genel adım aşağıda listelenmektedir:

- Kullanıcıların sisteminize kötücül yazılım yüklemelerini engellemek için bir eğitim (bilgi güvenliği farkındalığı) programı oluşturunuz.
- Kötücül yazılım problemleri hakkında düzenli olarak bilgi verici bültenler yayınlayınız.
- Kötücül yazılım karşıtı uygulamalar kurulmamışsa, bilinmeyen veya güvenilmeyen hiçbir kaynaktan dosya transferi yapmayınız. (Bu kötücül yazılım karşıtı programlar hakkında birazdan bilgi alacaksınız.)
- Üretim ortamına dâhil etmeden önce, yeni programları ve şüpheli dosyalan önce karantina altına alınmış -ağınızın hiçbir yerine bağlı olmayan- bir bilgisayarda test ediniz veya açınız.
- Anti-malware yazılım kurunuz. Bu yazılımın ve verisinin güncel olduğundan emin olunuz. Kötü niyetli kullanıcıların sisteme kötücül yazılım sokmalarına engel olmak ve var olan kötücül yazılımları tespit etmek için düzenli olarak güvenlik taraması yaptırınız.
- Güvenli bir giriş ve kimlik doğrulama sistemi kullanınız.

Kötücül yazılımlar ile başa çıkmada başka bir önemli taktik kötücül yazılım konusundaki gelişmeleri yakından takip etmektir. Haftalık bilgisayar dergilerini okuyarak veya US-CERT veya Ulusal Siber Güvenlik İttifakı (National Cyber Security Alliance - NCSA) gibi organizasyonlara katılarak en son kötücül yazılımlar hakkında bilgi alabilirsiniz. Ayrıca önemli anti-virüs yazılımlarının düzenli olarak yayınladığı klavuz ve whitepaper ları inceleyebilirsiniz.

Ayrıca, sisteminizdeki anti-malware (kötücül yazılımla mücadele programını) kullanarak, iş istasyonlarına ve mail sunucularına sokulan bütün dosyaları tarayınız. (Bu tür yazılımların genel adı anti-virüs yazılımlarıdır fakat bugünün anti-virüs yazılımları genellikle sadece virüslerle uğraşmazlar. Bu nedenle, anti-malware demek daha doğrudur.) Çoğu yönetici anti-malware programlarını ağın birçok noktasında kullanır. Bu programlar aşağıdakileri içerir:

- BitDefender - www.bitdefender.com
- Kaspersky Antivirüs - www.kaspersky.com
- Webroot Antivirüs- www.webroot.com
- Norton Antivirüs - www.symantec.com/norton/antivirus.com
- Eset Nod32 Antivirüs - www.eset.com
- Avg Antivirüs - www.avg.com
- G DATA Antivirüs - www.gdatasoftware.com
- Avira Antivirüs - www.avira.com
- McAfee Endpoint Protection - www.mcafee.com
- Trend Micro - www.trendmicro.com
- Microsoft Security Essentials - www.microsoft.com/security_essentials

Bazı anti-malware yazılımları bir dosya tarafından gerçekleştirilen eylemleri inceleyerek dosyanın kötücül yazılım olup olmadığına karar verir. Bu tür anti-malware programları sezgisel (heuristic) analiz denen bir yöntem kullanarak programların kötücül yazılım gibi "davranıp davranmadıklarını" inceler. Diğer bazı programlar, programlan ve dosyaları bilinen kötücül yazılımlarla karşılaştırarak kötücül yazılım tespit ederler. Sorun şudur ki, bu yazılımlar yeni yaratılmış kötücül yazılımların davranışlarını hemen tanıyıp karşı tedbirler alamayabilirler. Anti-malware programı, imza veri tabanını bu yeni türleri içerecek biçimde güncellemelidir. Saldırganlar sürekli yeni kötücül yazılımlar yarattıkları için, anti-malware programınızın güncel olması çok önemlidir. Etkili bir yöntem sisteme her giriş yaptığınızda anti-malware programını güncelleyip sistemde tarama yaptırmaktır.

Unutmayınız ki sisteminizdeki bir kötücül uygulamayı tespit edip imha etseniz dahi, bu kötücül yazılım kurumun başka bir kısmında sisteme yeniden bulaşmak veya saldırmak için pusuda bekliyor olabilir. Bu durum özellikle ortak çalışma alanları için geçerlidir; virüs içeren dosyalar ana sunucuda tutulup ağ üzerinden dağıtılıyor olabilir. Bu bulaşma-tespit-kaldırma-imha süreci siz kötücül yazılımı bütün sistemden atıncaya dek defalarca tekrarlanabilir. Sisteminizin herhangi bir yerinde kötücül yazılım bulursanız, depolama cihazları da dâhil olmak üzere bütün sisteminizi taramalısınız.

Sisteminizi Güvenlik Duvarları ile Korumak

Bir güvenlik duvarı (firewall) ağ üzerinden geçen trafiği inceleyip, sizin yapılandırma ayarlarında belirlediğiniz kurallara göre geçen trafiği reddeden veya kabul eden bir program veya bu amaç için ayrılmış bir donanım cihazıdır. Bir güvenlik duvarının temel görevi, farklı güven seviyelerine sahip olan bilgisayar ağları arasındaki trafik akışını düzenlemektir, iç ağın internetle buluştuğu yer olan LAN'dan WAN'a bölümü ile WAN bölümü arasındaki trafik gibi.

Birçok ticari güvenlik duvarı bulunmaktadır. Önemli güvenlik duvarı üreticileri aşağıda listelenmiştir:

- Palo Alto Networks - www.paloaltonetworks.com
- Cisco Systems - www.cisco.com
- SonicWall - www.sonicwall.com
- Watch Guard Technologies - www.watchguard.com
- Check Point- www.checkpoint.com
- ZyXel - www.zyxel.com
- NetGear - www.netgear.com
- Juniper Networks - www.juniper.net
- DLink - www.dlink.com
- MultiTech Systems - www.multitech.com

Siber Saldırı haritaları:

- https://cybermap.kaspersky.com
- https://threatmap.checkpoint.com
- https://threatmap.fortiguard.com
- https://threatbutt.com/map
- https://talosintelligence.com/fullpage_maps/pulse
- https://www.fireeye.com/cyber-map/threat-map.html
- https://horizon.netscout.com