ANKARA
HACI BAYRAM VELİ ÜNİVERSİTESİ
UZAKTAN EĞİTİM UYGULAMA VE
ARAŞTIRMA MERKEZİ

İŞLETMELERDE VERİ İLETİŞİMİ

Doç. Dr. Şaban Öztürk

saban.ozturk@hbv.edu.tr

Dersin Genel Hedefleri

- Öğrencilerin veri iletişiminin temel kavramlarını, protokollerini ve teknolojilerini anlamalarını sağlamak.
- İşletmelerde kullanılan çeşitli iletişim ağlarının yapısını, bileşenlerini ve işlevlerini incelemek.
- Günümüz veri iletişimi teknolojilerini (örneğin, Ethernet, Wi-Fi, Bluetooth) ve bunların işletme ortamındaki uygulama alanlarını öğrenmek.
- Veri iletişimi ağlarının güvenliğini sağlamak ve yönetmek için gerekli stratejileri ve araçları öğrenmek.
- İşletmelerde veri iletişimi ile ilgili ortaya çıkan sorunları tanımlamak ve bu sorunlara etkili çözümler geliştirmek.

Doç. Dr. Şaban Öztürk
saban.ozturk@hbv.edu.tr

Bölüm Hedefleri

- Ağ güvenliğine ilişkin unsurların kavranması

1. Veri Güvenliği

İş dünyası ve hükümet, her zaman fiziksel ve bilgi güvenliği ile ilgilenmiştir. Organize toplumlar var olduğundan beri, fiziksel varlıklarını kilitler, bariyerler, korumalar ve ordu ile korumuşlardır.

İnternet'in yükselişi, bilgi güvenliğinin doğasını tamamen yeniden tanımlamıştır. Artık şirketler, ağlarına ve daha da önemlisi verilerine yönelik küresel tehditlerle karşı karşıyalar. Virüsler ve fidye yazılımları gibi kötü amaçlı yazılımlar uzun zamandır bir sorun olmuştur, müşterilerinin verilerini koruyamayan firmalar için büyük bir sorumluluk teşkil etmektedir. Kanunlar, ABD'de bir bilgisayara izinsiz girmek—hasar vermese bile—para cezası ve/veya hapis cezası ile cezalandırılabilen federal bir suç olmasına rağmen, bu duruma ayak uydurmakta yavaş kalmıştır. Yine de, yasaların uygulanabilir olmasına rağmen uygulanması çok zor olacak yeni bir tür sınır ötesi siber suçla karşı karşıyayız.

Güvenlik olaylarının sayısı yılda yaklaşık %30 artmaktadır. 2016 yılında yaklaşık 50 milyon şifre çalınmıştır. 1.500 ABD'li yetişkin arasında yapılan bir anket, 2016 yılında %51'inin bir tür siber güvenlik olayı yaşadığını ortaya koymuştur. İnternet'in ilk günlerinde, bir virüs yaratmak ve web sitelerine izinsiz girmek, heyecan arayan genç yetişkinler tarafından yapılırdı. O günler geride kaldı. Bugünün hedefi para.

1. Veri Güvenliği

Muhtemelen haberlerde büyük şirketlerin siber saldırıların kurbanı olduklarını ve milyonlarca müşterilerinin kredi kartı bilgilerinin çalındığını duymuşsunuzdur. Ancak, herhangi bir büyüklükteki bir şirket de saldırının hedefi olabilir. Pek çok özel ve kamu kuruluşu, bireylerin, organizasyonların ve hükümetlerin internet üzerinde faaliyet gösteren suçlulara (siber suçlular) karşı kendilerini korumalarına yardımcı olmaya odaklanmaktadır.

Son birkaç yılda bilgisayar güvenliğinde artış olmasının üç ana nedeni vardır.

Birincisi, geçmişte birinin bilgisayarına izinsiz girmek bir hobi olarak görülürdü, ancak bugün siber suçlu olmak bir meslek haline geldi. Bilgi çalmak için belirli hedeflerin bilgisayar ağlarına sızmak üzere kiralanabilecek profesyonel organizasyonlar vardır. Burada etik hacklemeden (bir şirketin güvenliğini test etmek için başka bir şirketi işe alma durumu) değil, ücret karşılığında kredi kartları, kişisel bilgiler veya fikri mülkiyet çalacak hackerlardan bahsediyoruz. Bu saldırılara hedefli saldırılar denir ve siber suçlular yalnızca teknik açıkları istismar etmeye çalışmakla kalmaz, aynı zamanda sosyal mühendislik veya oltalama e-postaları yoluyla “insanı hacklemeye” de çalışırlar. Bu hedefli saldırılar çok sofistike olabilir ve her organizasyon siber suçlular için değerli olabilecek verilere sahip olduğundan herhangi bir organizasyon kurban olabilir.

1. Veri Güvenliği

İkincisi, hacktivizm (daha büyük bir politik veya sosyal amaca dikkat çekmek için hackleme tekniklerinin kullanılması) daha yaygın hale geldi. Hacktivizm, yasa dışı hackleme tekniklerini dijital aktivizmle birleştirir ve genellikle büyük organizasyonları ve hükümetleri hedef alarak, hackerların sosyal veya politik amaçlarına dikkat çekmek için kamuya açık web sitelerini sabote eder veya tahrip eder. Örneğin, Anonymous adlı grup.

Üçüncüsü, mobil cihazlardaki artış, istismar için çok verimli bir ortam sunmaktadır. Banka hesaplarımıza erişmek, Amazon'dan alışveriş yapmak ve iş verilerimizi mobil cihazlarımız aracılığıyla kullanmak gittikçe yaygınlaştığı için, siber suçlular artık bu mobil cihazları hedef almaktadır. Bu tür saldırıları geliştirmek genellikle daha kolaydır çünkü mobil güvenlik genellikle bilgisayar güvenliğinden daha zayıftır, bu nedenle potansiyel olarak yüksek getirisi vardır.

Bu trendler, kişisel verilerin değerini artıracak ve dolayısıyla mahremiyetimize ve işletmelerin mahremiyetine yönelik potansiyel tehdit artacaktır. Bu nedenle, işletmelerin ve bireylerin varlıklarını, bu varlıklara yönelik potansiyel tehditleri ve bunları nasıl koruyabileceklerini anlamaları çok önemlidir.

2.Veri Güvenliğine Neden İhtiyaç Duyarız

Son yıllarda, organizasyonlar günlük iş iletişimleri, veritabanı bilgi erişimi, dağıtılmış veri işleme ve LAN'ların internetworking'i için veri iletişim ağlarına giderek daha fazla bağımlı hale gelmiştir. İnternet'in yükselişi ve bilgisayarlar ile mobil cihazları dünyanın her yerinde bağlama imkanı, organizasyonların varlıklarının potansiyel savunmasızlığını önemli ölçüde artırmıştır.

Güvenlik hatalarıyla ilişkilendirilen kayıplar büyük olabilir. Ortalama bir veri ihlalinin maliyeti yaklaşık 3,5 milyon dolardır, ancak bu sadece buzdağının görünen kısmıdır. İyi duyurulmuş bir güvenlik ihlalinin tüketici güveninin kaybına yol açması, kaybedilen işlerde çok daha fazla maliyete neden olabilir. Ancak bunlardan daha önemli olan, bilgisayar ağlarında çalışan uygulama sistemlerinin kesintiye uğramasından kaynaklanan potansiyel kayıplardır. Organizasyonlar bilgisayar sistemlerine bağımlı hale geldikçe, bilgisayar ağları “görev kritik” hale gelmiştir.

Müşteri gizliliğini korumak ve kimlik hırsızlığı riski, artan ağ güvenliği ihtiyacını da tetiklemektedir. Amerika Birleşik Devletleri'nde, organizasyonlar HIPAA'nın veri koruma gereksinimlerine uyum sağlamaya başlamış ve her izinsiz müşteri bilgisi açıklaması için 250.000 dolara kadar para cezası öngören bir California yasası uygulamaktadır

3. Veri Güvenliği Tehdit Türleri

Birçok insan için güvenlik, bir saldırganın bilgisayarınıza girmesini önlemek gibi izinsiz girişleri önlemek anlamına gelir. Ancak güvenlik bundan çok daha fazlasıdır. Güvenlik sağlamanın üç ana hedefi vardır: gizlilik, bütünlük ve erişilebilirlik.

Gizlilik, müşteri ve özel verilerin yetkisiz ifşasından korunmasını ifade eder. Bütünlük, verilerin değiştirilmediği veya yok edilmediği garantisidir. Erişilebilirlik, organizasyonun donanım ve yazılımının kesintisiz çalışmasını sağlayarak personel, müşteriler ve tedarikçilerin hizmet kesintisi yaşamamasını sağlamaktır.

Gizlilik, bütünlük ve erişilebilirliğe yönelik birçok potansiyel tehdit vardır. Genel olarak, güvenlik tehditleri iki geniş kategoriye ayrılabilir: iş sürekliliğini sağlamak ve yetkisiz erişimi önlemek.

4. Ağ Kontrolleri

Güvenli bir ağ geliştirmek, kontroller geliştirmek anlamına gelir. Kontroller, ağ güvenliğine yönelik tehditleri azaltan veya ortadan kaldıran yazılım, donanım, kurallar veya prosedürlerdir.

Önleyici kontroller, bir kişinin hareket etmesini veya bir olayın meydana gelmesini engeller. Önleyici kontroller aynı zamanda bir caydırıcı olarak da işlev görür, çünkü birini harekete geçmekten veya ilerlemekten korku veya şüphe nedeniyle caydırır. Örneğin, bir kapıdaki güvenlik görevlisi veya güvenlik kilidi yasa dışı giriş denemesini caydırabilir.

Dedektif kontroller istenmeyen olayları ortaya çıkarır veya keşfeder. Örneğin, yasa dışı ağ girişini arayan bir yazılım bu sorunları tespit edebilir. Ayrıca bir olayı, durumu veya izinsiz girişi belgeleyerek, ilgili kişiler veya organizasyonlara karşı sonraki eylemler için kanıt sağlar veya düzeltici eylemin alınmasını mümkün kılar.

Düzeltici kontroller, istenmeyen bir olayı veya izinsiz girişi düzeltir. Bilgisayar programları veya insanlar, hataları düzeltmek veya gelecekte tekrar meydana gelmemesi için bir güvenlik ihlalini düzeltmek için verileri doğrular ve kontrol eder. Ayrıca ağ hatalarından veya felaketlerinden kurtulabilirler.

5. Risk Değerlendirmesi

Güvenli bir ağ geliştirmedeki ilk adım, bir risk değerlendirmesi yapmaktır. Bilgi sistemleri ve ağlara yönelik güvenlik risklerini analiz etmek ve önceliklendirmek için stratejiler sunan birkaç yaygın kullanılan risk değerlendirme çerçevesi bulunmaktadır.

Bir risk değerlendirmesi basit olmalıdır, böylece hem teknik hem de teknik olmayan okuyucular bunu anlayabilir. Bir risk değerlendirmesini okuduktan sonra, herkes hangi sistemlerin ve ağ bileşenlerinin saldırıya veya kötüye kullanıma yüksek risk altında olduğunu ve hangilerinin düşük risk altında olduğunu görebilmelidir.

Yaygın olarak kullanılan üç risk değerlendirme çerçevesi şunlardır:

- Operasyonel Kritik Tehdit, Varlık ve Zafiyet Değerlendirmesi (OCTAVE)
- Bilgi ve İlgili Teknoloji için Kontrol Hedefleri (COBIT)
- Bilgi Teknolojisi Sistemleri için Risk Yönetim Rehberi (NIST guide)

saban.ozturk@hbv.edu.tr

5. Risk Değerlendirmesi

Bu çerçevelerin her biri, farklı odak noktaları ile biraz farklı bir süreç sunar. Ancak, beş ortak adımı paylaşırlar:

- Risk ölçüm kriterlerini geliştirmek
- BT varlıklarının envanterini çıkarmak
- Tehditleri belirlemek
- Mevcut kontrolleri belgelemek
- İyileştirmeleri belirlemek

saban.ozturk@hbv.edu.tr

5.1. Risk Ölçüm Kriterleri Geliştirmek

Risk ölçüm kriterleri, bir güvenlik tehdidinin organizasyonu nasıl etkileyebileceğini değerlendirmek için kullanılan ölçütlerdir. Örneğin, bir hackerın şirket sunucusuna girip müşteri kredi kartı bilgilerini çaldığını varsayalım. Organizasyon üzerindeki hemen etkilerden biri finansaldır, çünkü bazı müşteriler en azından kısa vadede alışveriş yapmayı bırakabilir. Şirketin bulunduğu yere bağlı olarak, bazı ülkeler veya eyaletler kişisel bilgilerin izinsiz ifşasına ilişkin yasal düzenlemelere sahip olduğundan, yasal etkiler de olabilir. Ayrıca, şirketin itibarı üzerinde uzun vadeli etkiler de olabilir.

Her organizasyon, potansiyel iş etkilerini kendi ihtiyaçlarına göre belirlemelidir, ancak en yaygın olarak dikkate alınan beş etki alanı finansal (gelirler ve giderler), üretkenlik (iş operasyonları), itibar (müşteri algıları), güvenlik (müşteri ve çalışanların sağlığı) ve yasal (cezalar ve davalar potansiyeli) etkilerdir.

Etki alanları belirlendikten sonra, bunları önceliklendirmek gereklidir. Tüm etki alanları tüm organizasyonlar için eşit derecede önemli değildir. Bazı alanlar yüksek öncelikli, bazıları orta ve bazıları düşük olabilir. Örneğin, bir hastane için güvenlik en yüksek öncelik olabilirken, finansal etki en düşük öncelik olabilir. Tüm etkilerin yüksek öncelikli olduğunu söylemek cazip gelebilir, ancak bu, tüm etkilerin orta düzeyde olduğunu söylemekle aynı anlama gelir, çünkü harekete geçme zamanı geldiğinde aralarında ayrım yapamazsınız.

5.1. Risk Ölçüm Kriterleri Geliştirmek

Tablo, Web tabanlı bir kitapçı için örnek risk ölçüm kriterlerini göstermektedir. Gördüğünüz gibi, bu şirket için yalnızca dört etki alanı geçerlidir, çünkü bilgi sistemleri ve ağ güvenliği sorunları çalışanların veya müşterilerin güvenliğine zarar vermez.

Impact Area	**Priority**	Low Impact	Medium Impact	High Impact
Financial	High	Sales drop by less than 2%	Sales drop by 2-10%	Sales drop by more than 10%
Productivity	Medium	Increase in annual operating expenses by less than 3%	Increase in annual operating expenses between 3% and 6%	Increase in annual operating expenses by more than 6%
Reputation	High	Decrease in number of customers by less than 2%	Decrease in number of customers by 2-15%	Decrease in number of customers by more than 15%
Legal	Medium	Incurring fines or legal fees less than $10,000	Incurring fines or legal fees between $10,000 and $60,000	Incurring fines or legal fees exceeding $60,000

5.2. BT Varlıklarının Envanterini Çıkarmak

Bir varlık, değeri olan bir şeydir ve donanım, yazılım, veri veya uygulamalar olabilir. Şekil, altı yaygın BT varlık kategorisini tanımlamaktadır.
Önemli bir varlık türü, organizasyonun hayatta kalması için kritik olan bir bilgi sistemi olan görev-kritik uygulamalardır. Bu uygulamalar başarısızlığa izin verilemeyen uygulamalardır ve eğer başarısız olursa, ağ personeli diğer tüm işleri bırakıp bunu düzeltmeye odaklanır. Görev-kritik uygulamalar genellikle açıkça tanımlanır, böylece önemi göz ardı edilmez.
Bir sonraki en önemli varlık türü, organizasyonun verileridir. Örneğin, birisinin 10 milyon dolar değerinde bir ana bilgisayarı yok ettiğini varsayalım. Bilgisayar, yenisini satın alarak basitçe değiştirilebilir. Pahalı olurdu, ancak sorun birkaç hafta içinde çözülürdü.

Şimdi birisinin üniversitenizdeki tüm öğrenci kayıtlarını yok ettiğini ve kimsenin hangi dersleri aldığını veya notlarını bilmediğini varsayalım. Maliyet, 10 milyon dolarlık bir bilgisayarın değiştirilme maliyetini çok aşardı. Sadece davaların maliyeti bile 10 milyon doları aşar ve kağıt kayıtları bulup yeniden girmek için gereken personelin maliyeti çok büyük olur ve kesinlikle birkaç haftadan fazla sürer.

5.3. Tehditleri Belirlemek

Bir tehdit, organizasyona zarar verebilecek herhangi bir olası olayı ifade eder, sistemleri kesintiye uğratabilir veya organizasyona maddi zarar verebilir.

Görsel için dersin sorumlusuna ulaşınız.

5.3. Tehditleri Belirlemek

Örneğin, şirketlerin %100'ü virüs veya fidye yazılımı gibi bir veya daha fazla kötü amaçlı yazılım saldırısına maruz kaldıklarını bildirmişlerdir, ancak çoğu durumda antivirus yazılımları sorunu engellemiştir.

Diğer yaygın bir tehdit ise, çalışanları parolalarını ifşa etmeye kandırmak için bir saldırganın e-posta gönderdiği phishing gibi veya başka yollarla bilgi hırsızlığıdır.

Diğer daha az yaygın tehditler, ekipman hırsızlığı, cihaz arızası, hizmet reddi, sabotaj (bir saldırganın verileri değiştirmesi) veya yangın veya sel gibi doğal afetlerdir. Organizasyonunuzun bir tehdide maruz kalma olasılığı gerçek işinize bağlıdır. Örneğin, bir banka, bir aile işletmesinden daha fazla phishing hedef olma olasılığına sahiptir.

5.3. Tehditleri Belirlemek

Tehdit senaryosu hazırlarken, varlığı adlandırırız, tehdidi açıklarız, sonucu açıklarız (gizlilik, bütünlük veya kullanılabilirlik ihlali) ve bu tehdidin gerçekleşme olasılığını tahmin ederiz (yüksek, orta veya düşük).

Web tabanlı bir kitapçının bir varlığı (müşteri veritabanı) için bir tehdit senaryosunun bir örneğini sağlayacak tablo için dersin sorumlusuna ulaşınız.

Görsel için dersin sorumlusuna ulaşınız.

5.3. Tehditleri Belirlemek

Sonraki adımda, tehdidin sonuçları, adım 1'de belirlenen etki alanları ve öncelikleri (örneğin, itibar, finansal, üretkenlik, güvenlik ve yasal) kullanılarak değerlendirilir. Her senaryonun her öncelik alanındaki etkisi belirlenir ve adım 1'de tanımlanan risk ölçütleri kullanılarak yüksek, orta veya düşük olarak belirlenir. Her alanın önceliği ile tehdidin etkisi çarpılarak bir etki puanı hesaplanır, düşük bir değer için 1, orta bir değer için 2 ve yüksek bir değer için 3 kullanılarak tüm sonuçlar toplanır.

Son olarak, etki puanını olasılıkla (düşük olasılık için 1, orta olasılık için 2 ve yüksek olasılık için 3 kullanarak) çarparak göreceli risk puanını hesaplayabiliriz.

Şekil, müşteri veritabanından bilgi hırsızlığı için risk puanının 50 olduğunu göstermektedir. Mutlak sayı bize gerçekte bir şey anlatmaz. Bunun yerine, farklı tehdit senaryoları arasındaki risk puanlarını karşılaştırarak karşılaştığımız en önemli riskleri belirlememize yardımcı olur.

Web tabanlı bir kitapçının bir varlığı (müşteri veritabanı) için bir tehdit senaryosunun bir örneğini sağlayacak tablo için dersin sorumlusuna ulaşınız.

5.3. Tehditleri Belirlemek

Şekil, müşteri veritabanımıza karşı bir tornado saldırısı için tehdit senaryosunu göstermektedir. Tornado risk puanının 14 olduğunu görebilirsiniz, bu da bilgi hırsızlığının bir tornado riskinden daha büyük bir risk olduğunu göstermektedir.

Bu örneklerde, olasılığı, önceliği ve etkiyi değerlendirmek için yalnızca üç değer (yüksek, orta ve düşük) kullandık. Bazı organizasyonlar daha karmaşık puanlama sistemleri kullanır. Ve olasılığın, önceliğin ve etkinin aynı ölçekleri kullanması gerekmediğini belirtmek gerekir. Bazı organizasyonlar öncelik için 5 noktalı ölçekler, etki için 7 noktalı ölçekler ve olasılık için 100 noktalı ölçekler kullanır.

Web tabanlı bir kitapçının bir varlığı (müşteri veritabanı) için bir tehdit senaryosunun bir örneğini sağlayacak tablo için dersin sorumlusuna ulaşınız.

5.4. Mevcut Kontrolleri Belgeleme

Belirli varlıklar, tehdit senaryoları ve risk puanları belirlendikten sonra, bir organizasyonun risk kontrol stratejisini oluşturmaya başlayabilirsiniz, ki bu da bir organizasyonun riski ele almak için izleyeceği yol demektir. Genel olarak, bir organizasyon riski kabul edebilir, hafifletebilir, paylaşabilir veya erteleyebilir. Bir organizasyon riski kabul etmeye karar verirse, bu, organizasyonun hiçbir önlem almadan riskle başa çıkmaya ve belirtilen sonuçları kabul etmeye karar verdiği anlamına gelir.

Risk hafifletme, tehdidi karşılamak veya etkiyi en aza indirmek için bir tür kontrolün uygulanmasını içerir. Bir organizasyon, antivirus yazılımı kullanma, son teknoloji güvenlik duvarları uygulama veya çalışanlara güvenlik eğitimi verme gibi çeşitli kontrol türlerini uygulayabilir.

Bir organizasyon riski paylaşmaya karar verebilir. Bu durumda, risk karşısında sigorta satın alır. Örneğin, araba kazasına karşı bir riski paylaşırsınız. Benzer şekilde, bir organizasyon, bilgi hırsızlığı veya bir tornado hasarına karşı sigorta satın almayı tercih edebilir. Paylaşma ve hafifletme aynı anda gerçekleştirilebilir.

Son olarak, organizasyon riski erteleyebilir. Bu genellikle tehdit ve risk hakkında ek bilgi toplama ihtiyacı olduğunda gerçekleşir. Bu riskler genellikle yakın değildir ve gerçekleşmeleri durumunda organizasyon üzerinde önemli bir etkisi olmaz.

5.4. Mevcut Kontrolleri Belgeleme

Her tehdit senaryosu için, risk kontrol stratejisi belirlenmelidir. Organizasyon riski hafifletmeye ve/veya paylaşmaya karar verirse, belirli kontrollerin listelenmesi gerekir.

Mevcut kontroller belgelendikten sonra, bunların yeterliliğine ilişkin genel bir değerlendirme yapılır. Bu değerlendirme, riskle ilişkilendirilen bir değeri üretir, örneğin yüksek yeterlilik (kontrollerin tehdit senaryosundaki riskleri güçlü bir şekilde kontrol etmesi beklenir), orta yeterlilik (bazı iyileştirmelerin mümkün olduğu anlamına gelir) veya düşük yeterlilik (riski etkili bir şekilde hafifletmek veya paylaşmak için iyileştirmeler gereklidir).

5.5. Geliştirmeleri Belirleme

Risk değerlendirmesindeki son adım - ve nihai hedefi - hangi iyileştirmelerin gerektiğini belirlemektir. Çoğu organizasyon o kadar çok tehditle karşı karşıyadır ki, hepsini en yüksek düzeye indirgeme lüksüne sahip değildir. İlk olarak en yüksek risklere odaklanmaları gerekmektedir; en yüksek risk puanına sahip tehdit senaryoları dikkatlice incelenir ve en az orta düzeyde kontrol yeterliliğinin sağlandığından emin olunur.

Risk hafifletmeyi iyileştirmek için uygulanabilecek ek kontroller ve riski paylaşmanın yolları göz önüne alınır. Daha önce belirtildiği gibi, iş sürekliliği kaybı ve izinsiz erişimle ilişkili riskleri hafifletmek için uygulanabilecek birçok farklı kontrolü açıklamaktadır.

6. İş Sürekliliğini Sağlamak

İş sürekliliği, bir kesinti, yıkım veya felaket karşısında bile organizasyonun veri ve uygulamalarının çalışmaya devam etmesi anlamına gelir. İş sürekliliği planının iki ana bölümü vardır:

-bu olayların organizasyon üzerinde büyük bir etki yaratmasını önleyecek kontrollerin geliştirilmesi,
-bir felaket meydana gelirse organizasyonun toparlanmasını sağlayacak bir felaket kurtarma planı.

İş sürekliliğine yönelik başlıca tehditlere odaklanıyoruz: virüsler, hırsızlık, hizmet reddi saldırıları, cihaz arızası ve felaketler.

6.1. Virüs Koruması

Kötü amaçlı yazılımları, bilgisayar virüslerini ve fidye yazılımlarını önlemeye özel dikkat gösterilmelidir. Bazıları zararsız olup sadece rahatsız edici mesajlar yaratırken, diğerleri fidye ödenmediği takdirde verileri yok eden ciddi tehditler oluşturur. Çoğu durumda, bozulmalar veya veri yok edilmesi yereldir ve sadece birkaç bilgisayarı etkiler. Bu tür bozulmalar genellikle kolayca halledilebilir; virüs kaldırılır ve ağ çalışmaya devam eder. Ancak fidye yazılımları geniş çaplı tahribata yol açabilir.

Çoğu kötü amaçlı yazılım, diğer programlara veya USB sürücülerine kendini ekler. Bu dosyalar çalıştırıldığında veya USB'ye erişildiğinde, kötü amaçlı yazılım yayılır. Belge, e-posta veya elektronik tablo dosyalarında bulunan makro virüsler, enfekte olmuş bir dosya açıldığında yayılabilir. Bazı virüsler, yayılırken görünümlerini değiştirir, bu da tespit edilmelerini zorlaştırır.

Kurtçuk (worm), insan müdahalesi olmadan yayılan özel bir virüs türüdür. Birçok virüs bir dosyaya yapışır ve bir kişinin dosyayı kopyalamasını gerektirir, ancak bir kurtçuk kendisini bilgisayardan bilgisayara kopyalar. Kurtçuklar, bir bilgisayara kurulduktan sonra kendilerini diğer bilgisayarlara, bazen e-postalar aracılığıyla, bazen de yazılımdaki güvenlik açıkları üzerinden kopyalayarak yayılır.

6.1. Virüs Koruması

Virüslerin yayılmasını önlemenin en iyi yolu, bir antivirüs yazılımı kurmaktır. Çoğu organizasyon, bilgisayarlarına otomatik olarak antivirüs yazılımı yükler, ancak birçok kişi ev bilgisayarlarına bu yazılımları yüklemez. Antivirüs yazılımı, en son güncellemesi kadar etkilidir, bu yüzden yazılımın düzenli olarak güncellenmesi kritik önem taşır. Yazılımınızı otomatik olarak güncelleyecek şekilde ayarladığınızdan emin olun.

Kötü amaçlı yazılımlar genellikle internetten dosya indirerek yayılır, bu yüzden bilinmeyen kaynaklardan dosya kopyalamaktan veya indirmekten kaçının (örneğin, müzik, videolar, ekran koruyucuları) veya en azından indirdiğiniz her dosyayı kontrol edin.

Tüm dosyaları kullanmadan önce kötü amaçlı yazılımlara karşı kontrol edin (arkadaşlarınızdan gelenler bile!).

Araştırmacılar, her gün 10 yeni virüs geliştirildiğini tahmin ediyor, bu yüzden antivirüs yazılımı tarafından sağlanan virüs bilgi dosyalarını sık sık güncellemek önemlidir.

6.2. Hizmet Kesintisi (Denial-of-Service) Koruması

Hizmet kesintisi saldırısında (DoS), bir saldırgan, hedef sistemi mesajlarla doldurarak normal kullanıcıların mesajlarını işleyemez hale getirmeye çalışır. En basit yaklaşım, bir Web sunucusunu, DNS sunucusunu, posta sunucusunu vb. gelen mesajlarla doldurmaktır. Sunucu bu mesajlara yanıt vermeye çalışır, ancak o kadar çok mesaj vardır ki, bunları işleyemez.

Bir kullanıcının ağı mesajlarla doldurması durumunda, bu kişinin mesajlarını Web sunucusuna ulaşmadan önce filtrelemek mümkün gibi görünebilir. Bu işe yarayabilir, ancak çoğu saldırgan, gelen mesajlarda sahte kaynak IP adresleri kullanmalarını sağlayan araçlar kullanır.

Bir DDoS saldırısında, saldırgan binlerce bilgisayara veya akıllı cihaza (örneğin, TV'ler) girip kontrolünü ele geçirir ve bunlara DDoS ajanı (bazen zombi veya bot olarak da adlandırılır) denilen yazılımı yükler. Saldırgan daha sonra DDoS yöneticisi (bazen botnet olarak da adlandırılır) denilen yazılımı kullanarak ajanları kontrol eder. Yöneticisi, saldırganın kontrolündeki bilgisayarlara talimat verir ve bu bilgisayarlar aynı anda hedef siteye mesajlar göndermeye başlar. Bazı DDoS saldırıları, hedefe saniyede bir milyardan fazla paket göndermiştir.

6.2. Hizmet Kesintisi (Denial-of-Service) Koruması

Ağınızı DoS ve DDoS saldırılarından korumak için birkaç yaklaşım bulunmaktadır. İlk yaklaşım, ağınızı internete bağlayan ana yönlendiriciyi, gelen mesajların kaynak adreslerinin bu bağlantı için geçerli bir adres aralığında olup olmadığını doğrulayacak şekilde yapılandırmaktır (trafik filtreleme olarak adlandırılır). Örneğin, gelen bir mesajın kaynak adresi ağınızın içinden geliyorsa, bu açıkça sahte bir adrestir. Bu, yalnızca geçerli adreslere sahip mesajların ağa girmesine izin verir, ancak bu, yönlendiricide daha fazla işlem yapılmasını gerektirir ve bu nedenle gelen trafiği yavaşlatır.

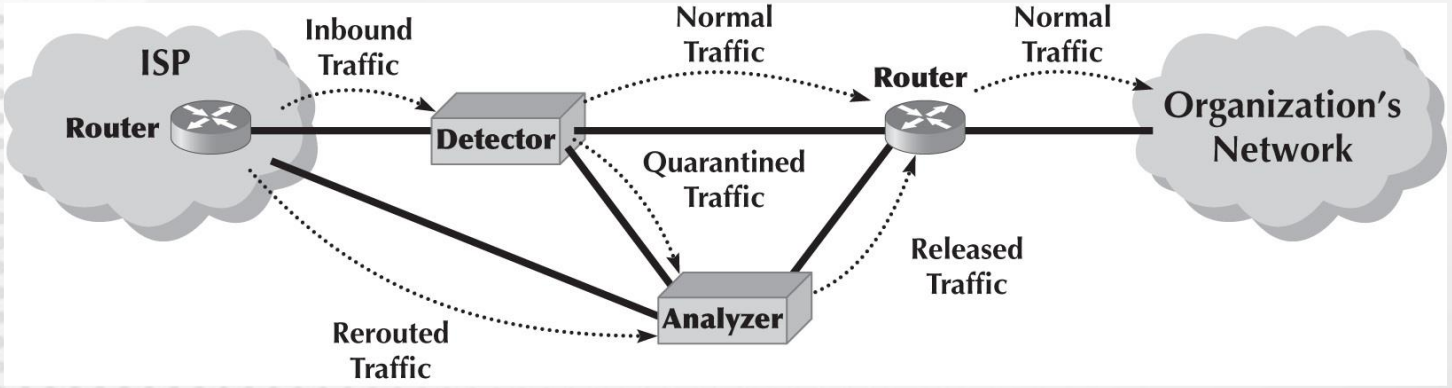
İkinci bir yaklaşım, ana yönlendiriciyi (veya güvenlik duvarını), kaynağı ne olursa olsun, ağa girmesine izin verilen DoS/DDoS saldırı paketlerinin sayısını sınırlayacak şekilde yapılandırmaktır (trafik sınırlama olarak adlandırılır).

Bir DoS/DDoS saldırısını gösteren şey, bu tür paketlerin sel gibi gelmesidir, bu nedenle her saniye belirli bir sayıdan fazla gelen paketleri atarak saldırının etkisini azaltabilirsiniz. Dezavantajı, bir saldırı sırasında düzenli müşterilerden gelen bazı geçerli paketlerin de atılacak olmasıdır, bu nedenle ağınıza ulaşamayacaklardır. Bu nedenle, ağ çalışmaya devam edecektir, ancak bazı müşteri paketleri (örneğin, Web istekleri, e-postalar) kaybolacaktır.

6.2. Hizmet Kesintisi (Denial-of-Service) Koruması

Üçüncü ve daha sofistike bir yaklaşım, ana yönlendiricinin (veya güvenlik duvarının) önüne yerleştirilen özel amaçlı bir güvenlik cihazı olan trafik anomali dedektörü kullanmaktır. Bu cihaz, trafik analizini gerçekleştirir. Normal trafik kalıplarını izler ve normal trafiğin nasıl göründüğünü öğrenir. Çoğu DoS/DDoS saldırısı belirli bir sunucu veya cihaza yöneliktir, bu nedenle anomali dedektörü belirli bir sunucuya veya cihaza yönelik ani ve anormal derecede yüksek bir trafik patlamasını tanıdığında, bu gelen paketleri karantinaya alır ancak normal trafiğin ağa akmasına izin verir. Bu, ağın genel olarak minimal bir şekilde etkilenmesini sağlar.

Anomali dedektörü, karantinaya alınan paketleri bir trafik anomali analizörüne yönlendirir. Anomali analizörü, karantinaya alınan trafiği inceler, geçerli kaynak adreslerini ve "normal" trafiği tanımaya çalışır ve karantinaya alınan paketlerin hangilerinin ağa bırakılacağını seçer. Bu süreç hiçbir zaman mükemmel değildir, ancak diğer yaklaşımlardan önemli ölçüde daha iyidir.



Kaynak: https://quizlet.com/107199403/chapter-5-introducing-the-internet-and-email-flash-cards/

saban.ozturk@hbv.edu.tr

6.3. Hırsızlığa Karşı Koruma

Çoğu zaman göz ardı edilen bir güvenlik riski hırsızlıktır. Bilgisayarlar ve ağ ekipmanları, yaygın olarak bulunan ve iyi bir yeniden satış değeri olan öğelerdir. Çeşitli endüstri kaynaklarına göre, her yıl bilgisayar hırsızlığı nedeniyle 1 milyar dolardan fazla kayıp yaşanmaktadır ve çalınan birçok ürün internet açık artırma sitelerinde satılmaktadır. Fiziksel güvenlik, hırsızlık korumasının önemli bir bileşenidir. Çoğu kuruluş, ofislerine giren herkesin belirli bir düzeyde fiziksel güvenlikten geçmesini gerektirir. Örneğin, çoğu ofiste güvenlik görevlileri bulunur ve tüm ziyaretçilerin bir kuruluş çalışanı tarafından yetkilendirilmesi gerekir.

Hırsızlık için en yaygın hedeflerden biri dizüstü bilgisayarlardır. Çalışanların evlerinden, arabalarından ve otel odalarından en çok çalınan cihazlar dizüstü bilgisayarlardır. Havaalanları da dizüstü bilgisayar hırsızlığı için yaygın bir yerdir. Seyahat eden çalışanlar için fiziksel güvenlik sağlamak zordur, ancak çoğu kuruluş, çalışanlarına dizüstü bilgisayarlarla seyahat ederken özel dikkat göstermeleri gerektiğini düzenli olarak hatırlatır. Buna rağmen, dizüstü bilgisayarlar hâlâ en yaygın olarak çalınan cihazlardır.

6.4. Cihaz Arızası Koruması

Sonunda, her bilgisayar ağ cihazı, kablo veya kiralanmış devre arızalanacaktır. Bazı bilgisayarlar, cihazlar, kablolar ve devreler diğerlerinden daha güvenilir olabilir, ancak her ağ yöneticisi arıza durumuna karşı hazırlıklı olmalıdır.

Bir arızanın iş sürekliliğini etkilemesini önlemenin en iyi yolu, ağa yedeklilik sağlamaktır. İş sürekliliği üzerinde ciddi bir etkisi olabilecek herhangi bir ağ bileşeni için, ağ tasarımcısı ikincil, yedek bir bileşen sağlar. Örneğin, İnternet bağlantısı organizasyon için önemliyse, ağ tasarımcısı, organizasyonun, her biri farklı bir ortak taşıyıcı tarafından sağlanan en az iki İnternet bağlantısına sahip olduğundan emin olur, böylece bir ortak taşıyıcının ağı çöktüğünde, organizasyon diğer ortak taşıyıcının ağı üzerinden hala İnternet'e ulaşabilir.

Bu aynı tasarım ilkesi, organizasyonun iç ağları için de geçerlidir. Temel omurga önemliyse (ve genellikle öyledir), organizasyonun her biri farklı cihazlar tarafından hizmet verilen iki temel omurgası olmalıdır.

Yedeklilik pahalı olabilir, bu nedenle çoğu organizasyon, ağın tamamını korumanın gerekli olmadığına karar verir. Çoğu organizasyon, temel omurga ve İnternet bağlantılarına yedeklilik sağlar, ancak hangi dağıtım omurgalarının (yani, bina omurgaları) ve erişim katmanı LAN'larının yedeklilik sağlayacağını seçerken çok dikkatli olurlar.

6.4. Cihaz Arızası Koruması

Bir sunucunun başarısız olması durumunda, sunucu çiftliğindeki diğer sunucuların çalışmaya devam ettiği ve çok az etkinin olduğu görülür. Bazı organizasyonlar, bir bileşenin başarısız olması durumunda bile devam edecek şekilde tasarlanmış çok sayıda yedek parçaya sahip olan hataya dayanıklı sunucular kullanırlar. Bağımsız Disklerin Redundant Dizisi (RAID), adından da anlaşılacağı gibi, birçok ayrı disk sürücüsünden oluşan bir depolama teknolojisidir. Bir dosya bir RAID cihazına yazıldığında, bu dosya birkaç ayrı, yedekli diske yazılır.

Enerji kesintileri ağ arızalarının en yaygın nedenlerinden biridir. Kesintisiz Güç Kaynağı (UPS), güç kesintilerini algılayan ve bağlı cihazların pili bitene kadar çalışmasına izin veren bir cihazdır. Ev kullanımı için UPS'ler ucuzdur ve genellikle 15 dakikaya kadar güç sağlar - yeterli bir süre içinde çalışmanızı kaydetmenize ve bilgisayarınızı kapatmanıza olanak tanır. Büyük organizasyonlar için UPS'ler genellikle bir saatlik bir pil ömrüne sahiptir ve görev önemli sunucuların, anahtarların ve yönlendiricilerin organizasyonun yedek jeneratörünü etkinleştirebilene kadar çalışmasına izin verir.

6.5. Doğal Afet Koruması

Bir felaket, organizasyonun bir bölümündeki büyük bir kısmı ağ ve bilgi işlem altyapısını yok eden bir olaydır. Felaketler genellikle doğal kuvvetler tarafından (örneğin, kasırgalar, seller, depremler, yangınlar) tetiklenir, ancak bazıları insan kaynaklı olabilir (örneğin, kundaklama, bombalar, terörizm).

İdeal olarak, bir felaketten kaçınmak istersiniz ki bu da zor olabilir. Örneğin, bir depremi nasıl önlersiniz? En temel adım yine yedekliliktir; kritik verilerinizi en az iki farklı yerde saklayın, böylece bir felaket bir yeri vurduğunda verileriniz güvende olur.

Diğer adımlar, önlenecek felakete bağlıdır. Örneğin, bir selin etkisinden kaçınmak için, ana ağ bileşenleri ve veriler hiçbir zaman nehirlerin yanına veya bir binanın bodrum katına yerleştirilmemelidir. Bir tornado etkisini önlemek için, ana ağ bileşenleri ve veriler yeraltında olmalıdır. Yangın etkisini azaltmak için, tüm önemli veri merkezlerine bir yangın söndürme sistemi kurulmalıdır.

6.5. Doğal Afet Koruması

Bir felaketten kaynaklanan sorunları düzeltmede kritik bir unsur, çeşitli felaketlere yanıt düzeylerini ele alan ve tüm verilerin, uygulama yazılımlarının, ağ bileşenlerinin ve fiziksel tesislerin kısmi veya tamamen kurtarılmasını sağlayan felaket kurtarma planıdır.

Bazı firmalar, iş sürekliliği planı terimini tercih ederler. Felaket kurtarma planının en önemli unsurları, organizasyonun verilerini kurtarmasını ve bir ağın bir kısmının çökmesi durumunda uygulama yazılımını yeniden başlatmasını sağlayan yedekleme ve kurtarma kontrolleridir. En basit yaklaşım, tüm kurumsal verilerin ve yazılımların yedek kopyalarını düzenli olarak almak ve bu yedek kopyaları dış mekanda depolamaktır. Çoğu organizasyon, tüm kritik bilgilerin günlük yedeklerini alırken, daha az önemli bilgileri (örneğin, e-posta dosyalarını) haftalık olarak yedekler.

Sürekli veri koruması (CDP), firmaların düzenli yedeklemelerin yanı sıra veya onun yerine kullandığı başka bir seçenektir. CDP ile seçilen sunuculardaki tüm verilerin ve işlemlerin kopyaları, işlem gerçekleştiği anda CDP sunucularına yazılır. CDP, belirli zamanlarda verilerin anlık görüntülerini alan geleneksel yedeklemelerden veya diskin içeriğini saniyeden saniyeye kopyalayan disk yansıtmanın ötesinde daha esnek bir yapıya sahiptir. CDP, verilerin köken sunucudan mil uzaklıktaki bir konuma saklanmasını ve tüm işlemlere zaman damgası basarak organizasyonlara verileri belirli bir zaman noktasına geri yükleyebilme imkanı sağlar.

6.5. Doğal Afet Koruması

Birçok organizasyonun bir felaket kurtarma planı bulunsa da, planlarını sadece birkaçı test eder. Bir felaket kurtarma tatbikatı, bir yangın tatbikatına oldukça benzer bir şekilde, felaket kurtarma planını test eder ve çalışanlara gerçek bir felaket durumunda neyin işe yaradığını ve neyin işe yaramadığını öğrenme fırsatı sunar. Düzenli felaket kurtarma tatbikatları olmadan, bir planın test edildiği tek zaman, gerçekten kullanılması gerektiğinde olur.

Organizasyonlar genellikle bireysel kullanıcılardan daha iyi önemli verileri yedeklerler. Bilgisayarınızdaki verileri ne zaman yedeklediniz? Bilgisayarınız çalınsa veya yok edilse ne yapardınız?

7. İzinsiz Müdehale Önleme

Sızma, güvenlik sorunlarının ikinci ana türüdür ve genellikle en fazla dikkat çeken türdür. Kimse ağlarına bir korsanın girmesini istemez. Bilgisayar ağlarına yetkisiz erişim sağlamaya çalışan dört tür korsan vardır.

İlk olarak, bilgisayar güvenliği hakkında sınırlı bilgiye sahip olan rastgele korsanlar bulunur. Onlar sadece internette dolaşıp karşılarına çıkan herhangi bir bilgisayara erişmeye çalışırlar.

İkinci tür korsanlar güvenlik konusunda uzmandır, ancak motivasyonları avın heyecanıdır. Arkadaşları için hava atmayı veya ağ sahiplerini utandırmayı seven bir zorluk olduğu için bilgisayar ağlarına girerler. Bu korsanlar "hacker" olarak adlandırılır ve genellikle veri ve yazılım sahipliğine karşı güçlü bir felsefeye sahiptirler. Çoğu az zarar verir ve genellikle kendi kârlarını artırmak için çok çaba sarf etmezler.

Üçüncü tür korsan en tehlikelidir. Bu, belirli amaçlar için kurumsal veya devlet bilgisayarlarına sızmış profesyonel hackerlerdir; casusluk, dolandırıcılık veya kasıtlı imha gibi.

Dördüncü tür korsan da oldukça tehlikelidir. Bunlar, ağa meşru erişime sahip olan ancak kullanmaya yetkili olmadıkları bilgilere erişen kuruluş çalışanlarıdır. Bu bilgiler, kendi kişisel kazançları için kullanılabilir, rakiplere satılabilir veya çalışanın ek gelir elde etmesi için sahtekarlıkla değiştirilebilir.

7. İzinsiz Müdehale Önleme

Sızma, güvenlik sorunlarının ikinci ana türüdür ve genellikle en fazla dikkat çeken türdür. Kimse ağlarına bir korsanın girmesini istemez. Bilgisayar ağlarına yetkisiz erişim sağlamaya çalışan dört tür korsan vardır.

İlk olarak, bilgisayar güvenliği hakkında sınırlı bilgiye sahip olan rastgele korsanlar bulunur. Onlar sadece internette dolaşıp karşılarına çıkan herhangi bir bilgisayara erişmeye çalışırlar.

İkinci tür korsanlar güvenlik konusunda uzmandır, ancak motivasyonları avın heyecanıdır. Arkadaşları için hava atmayı veya ağ sahiplerini utandırmayı seven bir zorluk olduğu için bilgisayar ağlarına girerler. Bu korsanlar "hacker" olarak adlandırılır ve genellikle veri ve yazılım sahipliğine karşı güçlü bir felsefeye sahiptirler. Çoğu az zarar verir ve genellikle kendi kârlarını artırmak için çok çaba sarf etmezler.

Üçüncü tür korsan en tehlikelidir. Bu, belirli amaçlar için kurumsal veya devlet bilgisayarlarına sızmış profesyonel hackerlerdir; casusluk, dolandırıcılık veya kasıtlı imha gibi.

Dördüncü tür korsan da oldukça tehlikelidir. Bunlar, ağa meşru erişime sahip olan ancak kullanmaya yetkili olmadıkları bilgilere erişen kuruluş çalışanlarıdır. Bu bilgiler, kendi kişisel kazançları için kullanılabilir, rakiplere satılabilir veya çalışanın ek gelir elde etmesi için sahtekarlıkla değiştirilebilir.

7.1. Güvenlik Politikası

Bir felaket kurtarma planı, aksaklık, yıkım ve felaketten kaynaklanan riskleri kontrol etmek için ne kadar kritikse, güvenlik politikası da izinsiz girişten kaynaklanan riskleri kontrol etmek için o kadar kritiktir. Güvenlik politikası, korunması gereken önemli varlıkları ve bunları korumak için gerekli olan önemli kontrolleri açıkça tanımlamalıdır. Çalışanların ne yapıp ne yapmamaları gerektiğine dair bir bölüm içermelidir. Ayrıca, özellikle bilgisayar bilgisi az olan son kullanıcılar olmak üzere, çalışanların ana güvenlik kuralları hakkında rutin olarak eğitilmesi ve mevcut güvenlik kontrollerinin düzenli olarak test edilip iyileştirilmesi için net bir plan içermelidir.

7.2. Çevre Güvenliği ve Güvenlik Duvarları

İdeal olarak, dışarıdan gelen saldırganları ağınızın çevresinde durdurmak istersiniz, böylece içerdeki sunuculara ulaşamazlar. Çoğu ağda üç temel erişim noktası bulunur: İnternet, LAN'lar ve WLAN'lar. Son anketler, izinsiz girişlerin en yaygın erişim noktasının İnternet bağlantısı olduğunu, ardından LAN'lar ve WLAN'ların geldiğini göstermektedir. Dış saldırganlar en çok İnternet bağlantısını kullanırken, iç saldırganlar LAN veya WLAN'ı kullanma olasılığı daha yüksektir. İnternet izinsiz girişlerin en yaygın kaynağı olduğu için, çevre güvenliğinin odak noktası genellikle İnternet bağlantısıdır, ancak fiziksel güvenlik de önemlidir. Bir güvenlik duvarı, bir kuruluşun İnternet bağlantısını güvence altına almak için yaygın olarak kullanılır. Güvenlik duvarı, bir ağdan akan paketleri inceleyen ve kuruluşun ağına erişimi kısıtlayan bir yönlendirici veya özel amaçlı bir cihazdır. Ağ, kuruluş ile İnternet arasındaki her ağ bağlantısına bir güvenlik duvarı yerleştirilecek şekilde tasarlanmıştır.

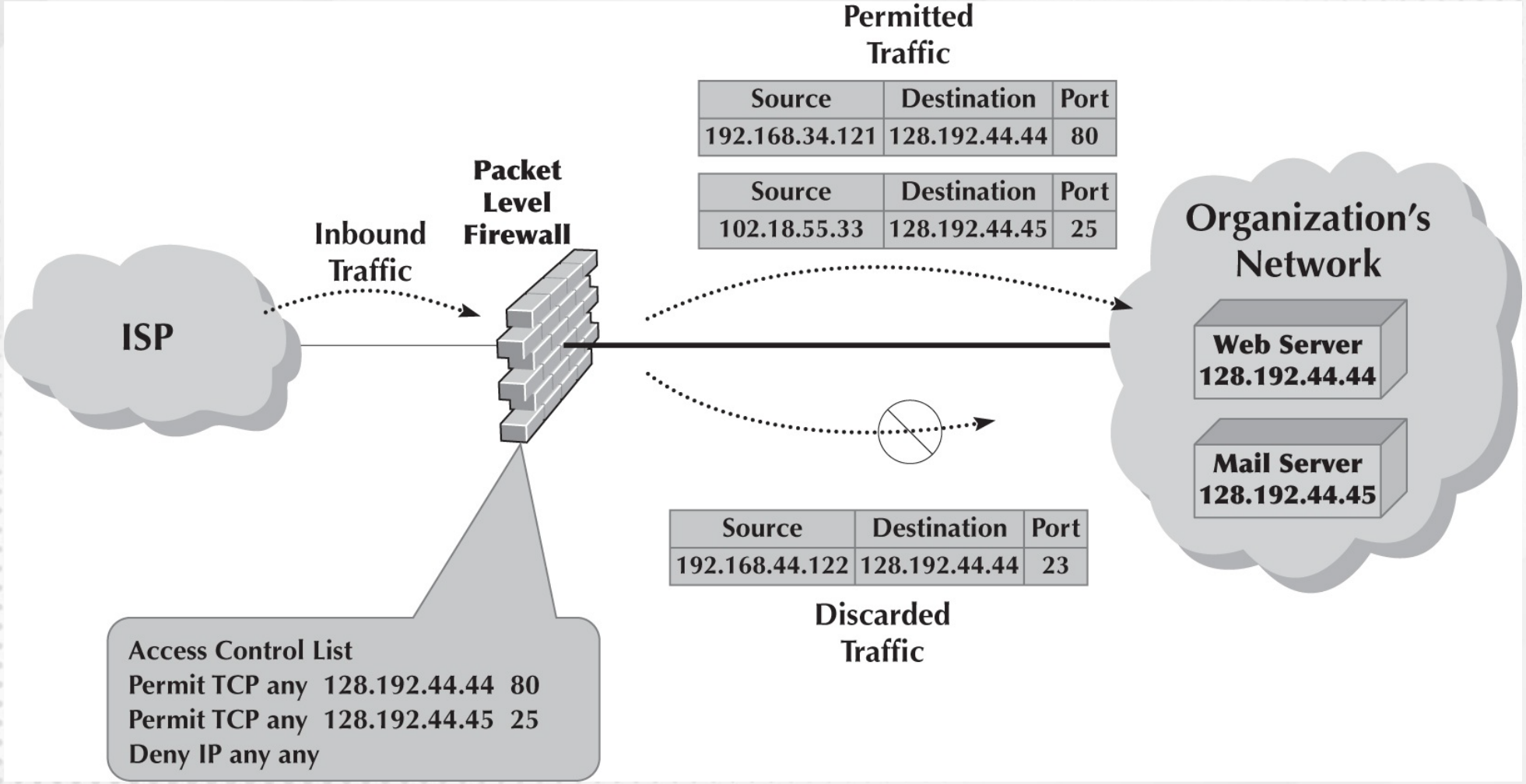
saban.ozturk@hbv.edu.tr

7.2. Çevre Güvenliği ve Güvenlik Duvarları

Bir paket düzeyinde güvenlik duvarı, üzerinden geçen her ağ paketinin kaynak ve hedef adresini inceler. Sadece kabul edilebilir kaynak ve hedef adreslere sahip paketlerin organizasyonun ağına girişine veya çıkışına izin verir. Genel olarak, adresler sadece taşıma katmanında (TCP portu kimliği) ve ağ katmanında (IP adresi) incelenir. Her paket bireysel olarak incelendiğinden, güvenlik duvarı önceki paketlerin ne olduğunu bilmez. Sadece paketin içeriğine göre giriş veya çıkış izni verir. Bu tür güvenlik duvarı en basit ve en az güvenli olandır çünkü paketlerin içeriğini veya neden gönderildiklerini izlememekte ve genellikle paketleri daha sonra analiz etmek üzere kaydetmemektedir.

Ağ yöneticisi, paket düzeyinde güvenlik duvarı için, ağ içine hangi paketlerin kabul edileceğini ve hangi paketlerin reddedileceğini bilmesi için bir dizi kural (erişim kontrol listesi [ACL] olarak adlandırılır) yazabilir.

7.2. Çevre Güvenliği ve Güvenlik Duvarları



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/2evaluate-following-statements-regarding-internet-structure-select-statements-correct-may--q52114071

7.2. Çevre Güvenliği ve Güvenlik Duvarları

Bir uygulama düzeyinde güvenlik duvarı, paket düzeyinde bir güvenlik duvarından daha pahalı ve kurulumu ile yönetimi daha karmaşıktır çünkü uygulama düzeyindeki paketin içeriğini inceleyip bilinen saldırıları arar. Uygulama katmanı güvenlik duvarlarının işleyebildikleri her uygulama için kuralları vardır. Örneğin, çoğu uygulama düzeyinde güvenlik duvarı Web paketlerini (HTTP), e-posta paketlerini (SMTP) ve diğer yaygın protokolleri kontrol edebilir. Bazı durumlarda, organizasyonun geliştirdiği uygulama yazılımının kullanılmasına izin vermek için özel kurallar yazılması gerekebilir.

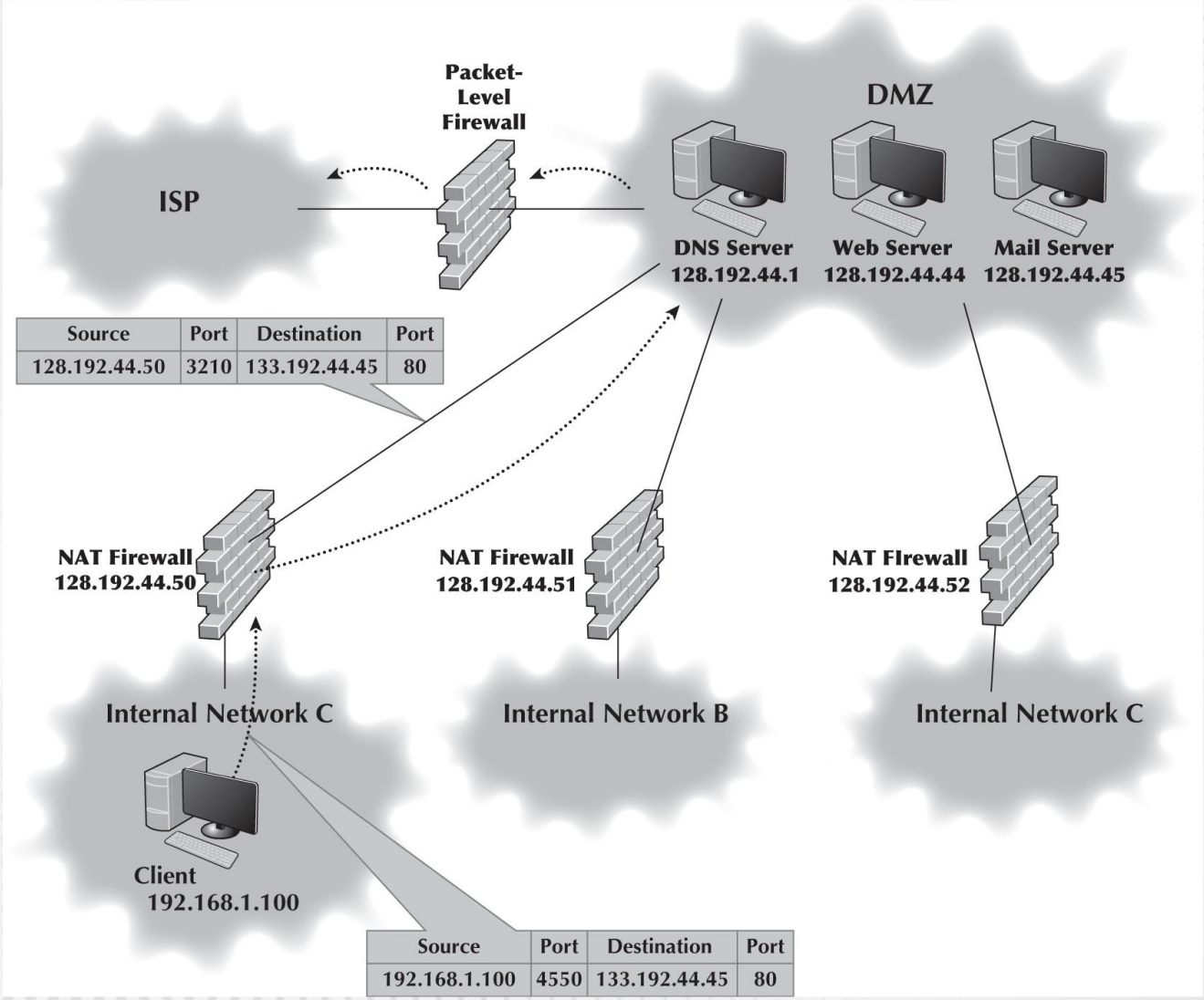
Birçok uygulama düzeyinde güvenlik duvarı, dış kullanıcıların çalıştırılabilir dosyalar yüklemesini yasaklar. Bu şekilde, saldırganlar (veya yetkili kullanıcılar) fiziksel erişim olmadan herhangi bir yazılımı değiştiremezler. Bazıları, yazılımlarındaki değişikliklere yalnızca satıcı tarafından izin verir. Diğerleri, kendi yazılımlarını aktif olarak izler ve herhangi bir değişiklik tespit ettiklerinde dış bağlantıları otomatik olarak devre dışı bırakır.

7.2. Çevre Güvenliği ve Güvenlik Duvarları

Ağ adresi çevirisi (NAT), İnternet'ten görülebilen bir dizi genel IP adresi ile organizasyon dışındaki kişilerden gizlenen ikinci bir dizi özel IP adresi arasında çeviri yapma sürecidir. NAT, şeffaftır; yani hiçbir bilgisayar bu işlemin olduğunu bilmez. NAT çeşitli nedenlerle yapılabilir, ancak en yaygın nedenler IPv4 adres tasarrufu ve güvenliktir. İnternetteki dış saldırganlar organizasyonunuz içindeki özel IP adreslerini göremezlerse, bilgisayarlarınıza saldırı yapamazlar. Bugün, çoğu yönlendirici ve güvenlik duvarında, ev kullanımı için tasarlanmış ucuz yönlendiriciler de dahil olmak üzere, NAT yerleşik olarak bulunur.

NAT güvenlik duvarı, organizasyon içinde kullanılan özel IP adreslerini İnternet'te kullanılan vekil (proxy) IP adreslerine çevirmek için bir adres tablosu kullanır. Organizasyon içindeki bir bilgisayar İnternet'teki bir bilgisayara eriştiğinde, güvenlik duvarı giden IP paketindeki kaynak IP adresini kendi adresiyle değiştirir. Ayrıca, TCP segmentindeki kaynak port numarasını, adres tablosunda organizasyonun iç ağındaki gerçek gönderen bilgisayarın IP adresini bulmak için kullandığı benzersiz bir numara olarak ayarlar. Dış bilgisayar isteğe yanıt verdiğinde, mesajı güvenlik duvarının IP adresine gönderir. Güvenlik duvarı gelen mesajı alır ve paketin içeri girmesine izin verilip verilmeyeceğini kontrol ettikten sonra, hedef IP adresini iç bilgisayarın özel IP adresiyle değiştirir ve TCP port numarasını doğru port numarasıyla değiştirir ve iç ağda iletir.

7.2. Çevre Güvenliği ve Güvenlik Duvarları



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/2evaluate-following-statements-regarding-internet-structure-select-statements-correct-may--q52114071

saban.ozturk@hbv.edu.tr

7.3. Sunucu ve İstemci Koruması

Fiziksel güvenlik ve güvenlik duvarlarına rağmen, bir ağdaki sunucular ve istemci bilgisayarlar, güvenlik açıkları nedeniyle güvende olmayabilir. Bir güvenlik açığı, yetkisiz erişime izin veren bir hatadır. Birçok yaygın kullanılan işletim sistemi, potansiyel saldırganların iyi bildiği büyük güvenlik açıklarına sahiptir. Pek çok güvenlik açığı belgelenmiş olup, satıcılar tarafından bunları düzeltmek için "yamalar" mevcuttur, ancak ağ yöneticileri tüm bu açıkların farkında olmayabilir veya sistemlerini düzenli olarak yeni yamalarla güncellemeyi unutabilirler.

Bir güvenlik açığı keşfedildiğinde, hızla İnternet üzerinde dolaşıma sokulur. Yarış, hackerlar ve güvenlik ekipleri arasında başlar; hackerlar bulgularını diğer hackerlarla paylaşır ve güvenlik ekipleri bulguları diğer güvenlik ekipleriyle paylaşırlar. Güvenlik açığına sahip yazılımın geliştiricisi genellikle güvenlik açığını düzeltmek için hızla çalışır ve deliği düzeltmek için bir yama üretir.

7.4. Trojan

Yetkisiz erişim elde etmede önemli bir araç, Truva atıdır. Truvalar, kullanıcıların bir bilgisayara uzaktan erişmesine ve uzaktan yönetmesine olanak tanıyan uzaktan erişim yönetim konsollarıdır. Herhangi bir yerden bilgisayarınızı kontrol etmenizi sağlayacak ücretsiz bir yazılım gördüğünüzde dikkatli olun; yazılım aynı zamanda bir saldırganın bilgisayarınızı herhangi bir yerden kontrol etmesine izin verebilir!

Truvalar daha sık olarak, farkında olmayan kullanıcıların İnternet üzerinden indirdikleri diğer yazılımların içine gizlenmiştir (adları orijinal Truva atına gönderme yapar). İnternet müzik sitelerinde paylaşılan müzik ve video dosyaları Truvaların yaygın taşıyıcılarıdır. Kullanıcı bir müzik dosyasını indirip oynattığında, dosya normal şekilde çalınır ve eklenmiş olan Truva yazılımı sessizce küçük bir programı yükler ve saldırganın kullanıcının bilgisayarını tamamen kontrol etmesini sağlar, böylece kullanıcı herhangi bir kötü şeyin olduğundan habersizdir. Saldırgan daha sonra basitçe kullanıcının bilgisayarına bağlanır ve kullanıcı ile aynı erişim ve kontrollere sahiptir. Birçok Truva, en iyi antivirüs yazılımları tarafından tamamen algılanamaz.

7.5. Encryption

İstilayı önlemenin en iyi yollarından biri şifrelemektir, bu da matematiksel kurallar olarak bilinen algoritmaları kullanarak bilgiyi gizlemenin bir yoludur. Aslında, kriptografi daha genel ve uygun bir terimdir. Şifreleme bilgiyi gizlemenin işlemidir, şifre çözme ise onu okunabilir biçime geri döndürme işlemidir. Bilgi okunabilir biçimdeyken açık metin olarak adlandırılır; şifrelenmiş biçimdeyken şifreli metin olarak adlandırılır.

Şifreleme bir bilgisayarda depolanan dosyaları şifrelemek veya bilgisayarlar arasında iletilen verileri şifrelemek için kullanılabilir. Birçok firma her ikisini de kullanır çünkü dosyaları şifrelemek işletim sistemindeki basit bir ayarla yapılır. Örneğin, Windows kullanıyorsanız, dizüstü bilgisayarınız çalındığında verilerinizi korumak için şifreleyebilirsiniz.

7.5. Encryption

Ağ çevresi ve ağ içi güvenliğin sağlandıktan sonra, bir sonraki adım, yalnızca yetkili kullanıcıların ağa ve ağın içindeki belirli kaynaklara girmesinin sağlanmasıdır. Buna kullanıcı kimlik doğrulama denir.

Kullanıcı kimlik doğrulamanın temeli, ağ yöneticisi tarafından atanmış olan her kullanıcının hesap için kullanıcı profili üzerinedir. Her kullanıcının profili, hangi verilere ve ağ kaynaklarına erişebileceğini ve erişim türünü (salt okunur, yazma, oluşturma, silme) belirtir.

Kullanıcı profilleri, giriş günlerini, günün hangi saatlerinde giriş yapabileceklerini, fiziksel konumları ve izin verilen yanlış giriş denemelerinin sayısını sınırlayabilir. Bazıları, ağ etkinliği gerçekleştirmemişse (örneğin, kullanıcı öğle yemeğine gitmiş ve ağdan çıkış yapmayı unutmuşsa) oturumu otomatik olarak sonlandırır. Kullanıcı oturumu açıkken gün boyunca düzenli güvenlik kontrolleri, kullanıcının hala ağa erişime izinli olup olmadığını belirleyebilir. Örneğin, ağ yöneticisi kullanıcının oturumunu açıkken profilini devre dışı bırakmış olabilir veya kullanıcının hesabı fonları tükenmiş olabilir.

7.7. Sosyal Mühendisliği Önleme

Sisteme sızmanın, hatta usta hackerlar için bile en yaygın yollarından biri, sadece sorarak güvenlik sistemini aşmaktır; buna sosyal mühendislik denir. Örneğin, saldırganlar genellikle habersiz kullanıcıları arar ve bir teknisyen veya üst düzey yönetici gibi davranarak bir şifre isterler. Ne yazık ki, çok sayıda kullanıcı yardımcı olmak ister ve istenen bilgileri basitçe sağlar. İlk bakışta, birinin tamamen yabancı birine şifresini vermesinin saçma olduğuna inanmak gibi görünse de, yetenekli bir sosyal mühendis iyi bir dolandırıcı gibidir: insanları manipüle edebilir.

Çoğu güvenlik uzmanı artık sosyal mühendislik saldırılarını test etmez; deneyimlerinden sosyal mühendisliğin herhangi bir organizasyonda sonunda başarılı olacağını bilirler ve dolayısıyla saldırganların normal kullanıcı hesaplarına kolayca erişebileceklerini varsayarlar.

Phishing (oltalama), çok yaygın bir sosyal mühendislik türüdür. Saldırgan basitçe milyonlarca kullanıcıya, banka hesabının yetkisiz bir erişim girişimi nedeniyle kapatıldığını ve bunu yeniden etkinleştirmek için giriş yapmaları gerektiğini söyleyen bir e-posta gönderir. E-posta, kullanıcıyı bankanın web sitesi gibi görünen sahte bir siteye yönlendiren bir bağlantı içerir. Kullanıcı sahte siteye giriş yaptıktan sonra, saldırganın kullanıcının kullanıcı adı ve şifresi olur ve dilediği gibi hesabına girebilir.

7.8. Sızma Önleme Sistemleri

Sızma önleme sistemleri (IPS'ler), bir sızmanın tespit edilmesi ve durdurulması için tasarlanmıştır. İki genel türde IPS vardır ve birçok ağ yöneticisi her ikisini de kurmayı tercih eder.

İlk tür, ağ tabanlı bir IPS'tir. Ağ tabanlı bir IPS ile bir IPS sensörü önemli ağ devrelerine yerleştirilir. Bir IPS sensörü, sadece o devredeki tüm ağ paketlerini izleyen ve sızıntıları bir IPS yönetim konsoluna rapor eden özel bir işletim sistemini çalıştıran bir cihazdır.

İkinci tür IPS, adından da anlaşılacağı gibi, bir ana bilgisayara veya sunucuya kurulan bir yazılım paketidir. Ana bilgisayar tabanlı IPS, sunucudaki faaliyetleri izler ve sızıntıları IPS yönetim konsoluna rapor eder. Bu tür IPS'lerin bir sızmanın devam ettiğini belirlemek için kullandığı iki temel teknik vardır; çoğu IPS her iki teknikten de faydalanır.

İlk teknik, yanlış kullanım tespitidir ve izlenen etkinlikleri bilinen saldırı imzalarıyla karşılaştırır. Bir saldırı imzası tanındığında, IPS bir uyarı verir ve şüpheli paketleri reddeder. Elbette, yeni saldırılar icat edildikçe saldırı imza veritabanını güncel tutma sorunu vardır. İkinci temel teknik ise anormallik tespitidir ve kararlı ağlarda iyi çalışır, çünkü izlenen etkinlikleri "normal" etkinlik setiyle karşılaştırır.

7.9. Sızma Kurtarma

Bir sızma tespit edildikten sonra, ilk adım sızan kişinin yetkisiz erişim sağladığı yolu belirlemek ve diğerlerinin aynı şekilde içeri girmesini önlemektir. Bazı organizasyonlar saldırganı kapıyı kapatmak ve güvenlik sorununu düzeltmekle yetinirler. Yaklaşık olarak organizasyonların %30'u, sızan kişinin faaliyetlerini kaydederek ve polisle işbirliği yaparak kişileri yakalamak için daha agresif bir yanıt verirler.

Bazı organizasyonlar, saldırganları yakalamak için tuzaklama teknikleri kullanarak kendi adımlarını atmışlardır. Amaç, saldırganın gerçek ağından dikkatini çekmek ve yalnızca sahte bilgiler içeren cazip bir sunucuya yönlendirmektir. Bu sunucu genellikle bir bal kabağı olarak adlandırılır. Bal kabağı sunucusu, saldırganı izlemek için sofistike izleme yazılımına sahip yüksek derecede ilginç, sahte bilgiler içerir ve bu bilgilere yalnızca yasadışı şekilde saldırarak ulaşılabilir. Bu bilgiye sahip olmak, ardından sızmanın nihai hukuki kanıtı haline gelir.

8. Uygulama

İyi bir güvenlik net bir felaket kurtarma planı ve sağlam bir güvenlik politikası ile başlar. Muhtemelen en iyi güvenlik yatırımı, kullanıcı eğitimidir: bireysel kullanıcıları veri kurtarma ve sosyal mühendisliği yenme yolları konusunda eğitmektir. Ancak bu, teknolojilere ihtiyaç duyulmadığı anlamına gelmez.

Gelecek yıllarda, iki faktörlü kimlik doğrulama ve şifreleme yöntemlerinin çok daha popüler hale gelmesini bekliyoruz.

Sürekli içerik filtreleme, tüm gelen paketlerin (örneğin, Web, e-posta) tarandığı bir yöntem haline gelebilir, böylece ağın hızını önemli ölçüde yavaşlatabilir. Tüm sunucu dosyaları ve istemci bilgisayarlarıyla iletişim şifrelenmiş olacak, bu da iletimleri daha da yavaşlatacak.

Son olarak, tüm yazılı güvenlik politikaları sıkı bir şekilde uygulanmalıdır. Güvenlik politikalarının ihlalleri hatta bir "başkaldırı suçu" haline gelebilir (yani, bir ihlal ve işten atılırsınız anlamında).

Değerlendirme Soruları

1) İzinsiz Müdehale Önlemeye Yönelik Unsurları sıralayınız? Her birini açıklayınız.

Kaynaklar

1) Stallings, W. (2007). Data and computer communications. Pearson Education India.

2) Forouzan, B. A. (2007). Data communications and networking. Huga Media.

3) Stallings, W., & Case, T. L. (2012). Business Data Communications-Infrastructure, Networking and Security.

4) Freer, J. (1996). Computer communications and networks. CRC Press.

5) Walrand, J., & Parekh, S. (2022). Communication networks: a concise introduction. Springer Nature.