

Bilişim Güvenliği

(Sürüm 1.1)

ORACLE®
Türkiye



www.oracle.com.tr

www.pro-g.com.tr

***Bu kitapçığın hazırlanmasına katkıda bulunan
Oracle Türkiye'ye teşekkür ederiz.***

Bu kitapçık, "Pro-G Proje Bilişim Güvenliđi ve Arařtırma San. ve Tic. Ltd. Őti" tarafından hazırlanmıř olup, tüm hakları saklıdır.

Bu kitapçığın bir kısmının yada tamamının herhangi bir biçimde (fotokopi, diđer bir elektronik ya da mekanik çođaltıcı) kopyası çıkarılamaz, bilgisayar sistemlerine aktarılamaz ve bireysel kullanım dıřında kullanılamaz.

© 2003, Pro-G Bilişim Güvenliđi ve Arařtırma Ltd.

İçindekiler

1	GİRİŞ	5
2	“BİLİŞİM GÜVENLİĞİ”NDEN NE ANLAMALIYIZ?	6
2.1	BİLİŞİM GÜVENLİĞİ NEDİR?	6
2.2	GÜVENLİK PRENSİPLERİ	8
2.2.1	<i>Gizlilik (Confidentiality)</i>	8
2.2.2	<i>Veri Bütünlüğü (Data Integrity)</i>	9
2.2.3	<i>Süreklilik (Availability)</i>	10
2.2.4	<i>İzlenebilirlik ya da Kayıt Tutma (Accountability)</i>	10
2.2.5	<i>Kimlik Sınaması (Authentication)</i>	11
2.2.6	<i>Güvenilirlik (Reliability - Consistency)</i>	11
2.2.7	<i>İnkâr Edememe (Non-repudiation)</i>	11
2.3	TEHDİTLER	11
2.4	GÜVENLİK BOŞLUĞU (VULNERABILITY)	12
2.5	RISK.....	13
3	BİLİŞİM GÜVENLİĞİNİN SAĞLANMASI	15
3.1	BİLİŞİM GÜVENLİĞİ SÜREÇ ALANLARI	16
3.2	BİLİŞİM GÜVENLİĞİ TEKNOLOJİLERİ	18
3.3	EĞİTİM	19
4	YÖNETSEL ÖNLEMLER	21
4.1	RISK YÖNETİMİ	22
4.1.1	<i>Kurumsal Bilgi Kaynaklarına Değer Bıçme</i>	22
4.1.2	<i>Risk Analizi</i>	23
4.1.3	<i>Tedbirlerin Seçimi</i>	24
4.2	GÜVENLİK POLİTİKALARI.....	25
4.3	STANDARTLAR, YÖNERGELER VE PROSEDÜRLER	27
4.4	GÜVENLİK YAŞAM DÖNGÜSÜ.....	28
4.5	GÜVENLİK DENETİMLERİ	28
5	TEKNOLOJİ UYGULAMALARI	31
5.1	KRİPTOGRAFI	31

5.1.1	<i>Simetrik Algoritmalar</i>	33
5.1.2	<i>Asimetrik Algoritmalar</i>	33
5.1.3	<i>Özetleme Fonksiyonları</i>	34
5.2	SAYISAL İMZA VE PKI	34
5.3	AĞ BÖLÜMLENDİRMESİ VE GÜVENLİK DUVARLARI	36
5.4	YEDEKLEME	38
5.5	SALDIRI TESPİTİ	39
5.6	ERİŞİM DENETİMİ	41
5.6.1	<i>Tanımlama</i>	42
5.6.2	<i>Kimlik Sınama</i>	42
5.6.3	<i>Yetkilendirme</i>	43
5.7	ANTI-VİRÜS SİSTEMLERİ	44
6	EĞİTİM	46
7	BİLİŞİM GÜVENLİĞİ STANDARTLARI	48
8	ORACLE VERİTABANI GÜVENLİĞİ	50
8.1	KİMLİK BELİRLEME VE YETKİLENDİRME METOTLARI	51
8.2	KAYIT BAZINDA GÜVENLİK	53
8.3	VERİLERİN ŞİFRELENMESİ	54
8.4	KULLANICI AKTİVİTESİNİN İZLENMESİ	54
8.5	İLETİŞİM GÜVENLİĞİ	55
9	ÖZET VE SONUÇ	58
10	KAYNAKLAR	60
11	GÜVENLİK TERİMLERİ	62

1 Giriş

Özellikle 1990'lı yıllardan başlayarak yaşanan hızlı teknolojik gelişmeler ve internetin yaygınlaşmasının bir sonucu olarak bilişim güvenliği son yıllarda giderek önem kazanan bir konu haline gelmiştir. Konunun önümüzdeki dönemde kurumların öncelik listesinde giderek artan bir öneme sahip olacağı ve kurumların bilişim güvenliği alanına gereken önemi vermeye başladıkları, ilgili önlemleri alma çabası içine girdikleri bilinmektedir. Ancak, bilişim güvenliğinin sadece teknolojik önlemlerle sağlanabileceği gibi genel bir yanılısamanın olduğu da gözlenmektedir.

Bu dokümanda bilişim güvenliğinin temel kavramları, en önemli bileşenleri ele alınmaktadır. Konunun esas olarak çok boyutlu ve karmaşık bir süreç olmasından hareketle, bilişim güvenliğinin bütünsel yaklaşımlarla ele alınmamasının tehlikeleri açıklanmaktadır.

Dokümanın ikinci bölümünde bilişim güvenliğinin temel kavramları ve bileşenleri, üçüncü bölümde ise bilişim güvenliğinin nasıl sağlanabileceği ele alınmaktadır. Dördüncü bölümde kurum yönetiminin alması gereken önlemler, beşinci bölümde geliştirilmiş güvenlik teknolojileri uygulamalarının başlıcaları, altıncı bölümde de güvenlik eğitimi konusunda yapılması gerekenler işlenmektedir. Yedinci bölümde bilişim güvenliğine ilişkin uluslararası standartlar ele alınmakta, sekizinci bölümde ise Oracle veritabanı yönetim sisteminin güvenlik özellikleri açıklanmaktadır.

2 “Bilişim Güvenliđi”nden Ne Anlamalıyız?

2.1 Bilişim Güvenliđi Nedir?

1990'lı yıllarda yaşanan hızlı teknolojik gelişmelerin bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Hayatımızın birçok alanında bilgisayar ve bilgisayar ağı teknolojileri “*olmazsa olmaz*” bir şekilde yer almaktadır. İletişim, para transferleri, kamu hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan sadece birkaçıdır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir.

Bilişim sistemlerine ve bu sistemler tarafından işlenen verilere yönelik güvenlik ihlalleri inanılmaz bir hızla artmaktadır.

Bilişim sistemlerine olan bireysel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımız da o denli artacaktır. Bu duyarlılık arttıkça da bilgisayar sistemlerine ve ağlarına yönelik olarak gerçekleştirilecek olan saldırıların sonucunda; para, zaman, prestij ve değerli bilgi kaybı da artacaktır. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda ise kaybedilen insan hayatı bile olabilir.

Bilgisayar Güvenliđi Enstitüsü (Computer Security Institute - CSI) ve Federal Araştırma Bürosu (FBI) tarafından geleneksel olarak gerçekleştirilen “Bilgisayar Suçları ve Güvenlik Araştırması”nın 2001 yılı raporuna göre bilişim suçları 1997- 2001 yılları arasında her yıl neredeyse ikiye katlanacak biçimde artmıştır. Aynı araştırma, gizli bilgilerin çalınması ve finansal kayıtlarda yapılan yasadışı değişikliklerin, en çok maddi zarara neden olan iki saldırı biçimi olduğunu göstermektedir.

Bilişim güvenliđi konusunun, önümüzdeki dönemde de bilişim sektöründe giderek artan bir öneme sahip olacağı bilinmektedir.

İzleyen paragraflarda son yıllarda yaşanmış bilgisayar güvenliği ihlallerine ilişkin bazı örnekler verilmektedir.

Melissa virüsü, 26 Mart 1999 tarihinde ilk kez ortaya çıkmış, anti virüs programlarını atlatarak Windows 9x, NT işletim sistemleri altında Word 97 ve Word 2000 programlarını kullanarak bilgisayarlara zarar vermiştir. Melissa virüsü internete gönderilmiş ve milyonlarca dolar zarar yol açmış “kötü amaçlı” (malicious) bir programdır ve e-posta yolu ile yayılmıştır. Virüsün 34 yaşındaki yaratıcısı David L. Smith, evdeki bilgisayarı yardımı ile virüsü internete göndermiştir. Virüs her bulaştığı bilgisayardan 50 yeni bilgisayara bulaşma özelliğine sahiptir. Bu nedenle çok hızlı ve durdurulamaz bir şekilde yayılmıştır. Smith virüsü ilk olarak biri çalıntı diğeri kendine ait olan iki America Online hesabını kullanarak bir e-posta mesajı ile beraber bir haber grubuna (news group) göndermiştir. Söz konusu e-posta mesajında “e-postanın eklentisinin yetişkin (adult) içeriğe sahip web sayfalarına giriş parolalarını bulmayı sağlayan bir program olduğundan bahsedilmiştir. Bu e-posta mesajı açılır açılmaz kurbanın bilgisayarına virüs bulaşmaktadır. Daha sonra virüs, Microsoft Outlook programı yardımı ile kendisini, kurbanın adres defterindeki ilk 50 kullanıcıya postalamaktadır. Olay hakkında delil toplama sürecinde America Online yetkilileri de görev almışlardır. 1 Nisan 1999’da Smith, FBI ve New Jersey Yüksek Teknoloji Suçları Birimi görevlileri tarafından kardeşinin evinde yakalanmış ve göz altına alınmıştır. Smith, 2 Mayıs 2002 tarihinde 20 ay hapis cezasına çarptırılmış ve 3 yıl göz hapsi ile 100 saat kamu hizmetinde çalışma cezasını almıştır. Melisa virüsü saldırısının 80 Milyon dolar zarara yol açtığı tespit edilmiştir.

Bir **zaman bombasının** geri döndürülemez zararlar vermesine bir örnek 1996 yılında yaşanmıştır. Timothy Allen Lloyd (39), yüksek teknoloji ürünü ölçme ve kontrol cihazları üreten Omega Mühendislik şirketinde çalışan “şef bilgisayar ağı program tasarımcısı” idi. Lloyd, Omega’da 11 yıl çalıştıktan sonra 10 Haziran 1996’da şirket ile ilişkisi kesildi. Bunun üzerine Lloyd hazırladığı “zaman bombası” yardımı ile Omega’nın tüm karmaşık üretim yazılımlarını geri döndürülemez bir şekilde sildi. Bu sabotaj sonucunda şirket, satışları ve ileri tarihli anlaşmaları da göz önünde bulundurduğunda 10 Milyon dolarlık

bir kayba uğramıştır. Bu olay olduğu sırada, Amerikan Gizli Servisi tarihinde, benzer olaylar arasında yol açtığı zarar en yüksek olan sabotajlardan biri olarak kayda geçmiştir. Olay ortaya çıkarıldığında, Lloyd 41 ay hapis ile cezalandırılmıştır.

1999 yılında Kanada'da yaşanan olay ise, **elektronik sahtecilik** konusunda verilebilecek en iyi örneklerdendir. Bu olay, Kosta Rika, ABD ve Kanada makamlarının ortak çalışmaları sonucunda ortaya çıkarılmış bir dolandırıcılıktır. "www.triwestinvest.com" adlı sitede, daha önceden sadece çok zengin yatırımcılara sunulan, yıllık %120'lik bir kar marjı olan ve para kaybı riski olmayan bir yatırımdan söz edilmekteydi. Yatırımcılardan, 1000 dolarlık paketler halinde paralarını yatırmaları istenmekteydi. Bu siteye paralarını ilk yatıranlara, kâr payı ödemesi altında bir takım ödemeler de yapılarak siteyle daha fazla müşterinin ilgilenmesi sağlanmıştır. 1999 - 2001 yılları arasında bu site aracılığı ile yatırım yapan 15.000 kurbanın paraları ile Alyn Richard Waage; Mexico ve Kosta Rika'da milyon dolarlık gayri menkuller, yatlar ve helikopterler satın almıştır. Bunun yanında, dolandırdığı paraların bir kısmını gizlemek için de Kosta Rika'da paravan şirketler kurmuş ve paraların bir kısmını da bu şirketlerden kazanmış gibi göstermiştir. Waage, internet üzerinden dolandırıcılık yapmak ve bu yolla yatırımcıları kandırarak 60 Milyon \$ toplamaktan suçlu bulundu, paranın çoğu sahiplerine iade edildi.

Bu örnekler, bilişim güvenliğinin gerek tehditler ve riskler, gerekse de alınması gereken önlemler açısından ne denli önemli olduğunu göstermektedir.

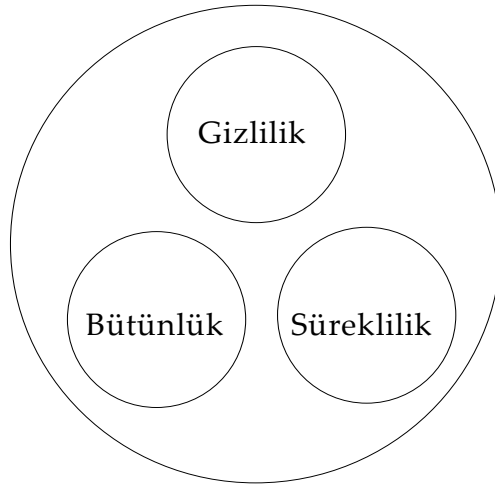
2.2 *Güvenlik Prensipleri*

Bilişim Güvenliğinin bir çok boyutu olmasına karşın, temel olarak üç prensipten söz edilebilir: Gizlilik, Veri Bütünlüğü ve Süreklilik.

2.2.1 **Gizlilik (Confidentiality)**

Bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Gizlilik, hem kalıcı ortamlarda (disk, tape, vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar, yetkileri olmayan verilere birçok yolla

erişebilirler: Parola dosyalarının çalınması, sosyal mühendislik, bilgisayar başında çalışan bir kullanıcının, ona fark ettirmeden özel bir bilgisini ele geçirme (parolasını girerken gözetleme gibi). Bunun yanında trafik analizinin, yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir.



Şekil 1 - Temel Güvenlik Prensipleri

2.2.2 Veri Bütünlüğü (Data Integrity)

Bu hizmetin amacı, veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır. Bu hizmeti, geri dönüşümü olan ve olmayan şekilde verebiliriz. Şöyle ki; alıcıda iki tür bütünlük sınaması yapılabilir: Bozulma Sınaması ya da Düzeltme Sınaması. Bozulma Sınaması ile verinin göndericiden alıcıya ulaştırılması sırasında değiştirilip değiştirilmediğinin sezilmesi hedeflenmiştir. Düzeltme Sınaması'nda

ise, Bozulma Sınaması'na ek olarak eğer veride deęişiklik sezildiyse bunu göndericiden çıktığı haline döndürmek hedeflenmektedir.

2.2.3 Süreklilik (Availability)

Bilişim sistemleri, kendilerinden beklenen işleri gerçekleştirirken, hedeflenen bir başarıml (performance) vardır. Bu başarıml sayesinde müşteri memnuniyeti artar, elektronik işe geçiş süreci hızlanır. Süreklilik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarıml düşürücü tehditlere karşı korumayı hedefler. Süreklilik hizmeti sayesinde, kullanıcılar, erişim yetkileri dahilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilirler.

Sistem sürekliliği, yalnızca kötü amaçlı bir "hacker"ın, sistem başarımlını düşürmeye yönelik bir saldırısı sonucu zedelenmez. Bilgisayar yazılımlarındaki hatalar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması, ortam şartlarındaki deęişimler (nem, ısı, yıldırım düşmesi, topraklama eksikliği) gibi faktörler de sistem sürekliliğini etkileyebilir.

Aşağıda, yukarıdaki üç temel prensibe ek olarak ikinci planda deęerlendirilebilecek izlenebilirlik, kimlik sınaması, güvenilirlik ve inkâr edememe prensiplerinden bahsedilmiştir.

2.2.4 İzlenebilirlik ya da Kayıt Tutma (Accountability)

Bu hizmetin hedefi sistemde gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır. Burada olay dendiğinde, bilgisayar sistemi ya da ağı üzerinde olan herhangi bir faaliyeti anlayabiliriz. Bir sistemde olabilecek olaylara, kullanıcının parolasını yazarak sisteme girmesi, bir web sayfasına bağlanmak, e-posta almak göndermek ya da icq ile mesaj yollamak gibi örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin örüntülerine rastlanırsa ya da bulanık mantık kullanılarak daha önce rastlanmayan ve saldırı olasılığı yüksek bir aktivite tespit edilirse alarm mesajları üretilerek sistem yöneticileri uyarılır.

2.2.5 Kimlik Sınaması (Authentication)

Ağ güvenliği açısından kimlik sınaması; alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik sına sistemleri yaygın olarak kullanmaya başlanmıştır.

2.2.6 Güvenilirlik (Reliability - Consistency)

Sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir deyiş ile güvenilirlik, sistemden ne yapmasını bekliyorsak, sistemin de eksiksiz ve fazlasız olarak bunu yapması ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir.

2.2.7 İnkâr Edememe (Non-repudiation)

Bu hizmet sayesinde, ne gönderici alıcıya bir mesajı gönderdiğini ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır ve gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır.

Bu hizmetler, zaman içinde bilgisayar sistemlerine karşı ortaya çıkmış tehditler ve yaşanmış olaylar sonucunda ortaya konmuştur. Yani her bir hizmet, belli bir grup potansiyel tehdide karşı sistemi korumaya yöneliktir, denilebilir.

2.3 Tehditler

Tehdit, bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden, olarak tanımlanabilir. Her tehdidin bir kaynağı (threat agent) ve bu kaynağın yararlandığı sistemdeki bir "güvenlik boşluğu" vardır. "Sistemi neye karşı

korunmalıyım?” sorusuna verilecek cevap bir sisteme yönelik olan tehditleri belirlemede yardımcı olacaktır.

Tehditler, tehdit kaynağı açısından bakıldığında iki gruba ayrılarak incelenebilir:

1. **İnsan Kaynaklı Tehditler:** Bu tür tehditleri de kendi içinde iki alt gruba ayırabiliriz:
 - a. Kötü niyet olmayan davranışlar sonucu oluşanlar: Bir kullanıcının, sistemi bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu sistemde ortaya çıkma olasılığı olan aksaklıklardır.
 - b. Kötü niyetli davranışlar sonucu oluşanlar: Sisteme zarar verme amacıyla, sisteme yönelik olarak yapılacak tüm kötü niyetli davranışlardır. Bu tür tehditlerde, tehdit kaynağı, sistemde bulunan güvenlik boşluklarından yararlanır.
2. **Doğa Kaynaklı Tehditler:** Bu tür tehditler genellikle önceden tespit edilemezler ve büyük bir olasılıkla olmaları engellenemez. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi bu tür tehditlere örnek olarak verilebilir.

Tehdidin geliş yönüne göre de sınıflandırma yapılabilir. Buna göre *iç tehditler*, kurum içinden kuruma yönelik yapılabilecek saldırılar, *dış tehditler* ise kurum dışından kuruma yönelik olarak yapılabilecek saldırılar olarak tanımlanır.

2.4 Güvenlik Boşluğu (Vulnerability)

Güvenlik boşluğu (Vulnerability), sistem üzerindeki yazılım ve donanımdan kaynaklanan ya da sistemi işletim kuralları ve/veya yönergelerindeki açık noktalar ve zayıf kalmış yönlerdir. Bir güvenlik boşluğu sayesinde bir saldırgan, sistemdeki bilgisayarlara ya da bilgisayar ağı üzerindeki kaynaklara yetkisiz olarak erişebilir. Bir sunucu bilgisayar üzerinde çalışan bir hizmet (örneğin web sunucu ya da e-posta alma/gönderme hizmeti), modem üzerinden içeri doğru sınırlandırılmamış arama hizmeti, bir güvenlik duvarı üzerinde açık unutulmuş bir erişim noktası (port), sunucu bilgisayarların

bulunduđu odaya giriř çıkıřlarda fiziksel eriřim denetimi eksikliđi, sunucular üzerinde belli bir politikaya dayandırılmadan belirlenen parolalar güvenlik boşluklarına örnek olarak verilebilirler.

Yazılım ya da donanımdan kaynaklanan güvenlik boşlukları, program üreticisi ya da başka bir kaynak tarafından geliştirilen bir “yama program” yardımıyla kapatılmalı ve eldeki yazılım ve donanımların üreticilerinin yayınladıđı yama listeleri sürekli olarak takip edilmelidir ve çıkan yamalar vakit geçirilmeden sisteme uygulanmalıdır.

Tehditler, bilgisayar sistemlerindeki güvenlik boşluklarına yönelik olarak tanımlanırlar. Yani bir güvenlik boşluđu ortadan kaldırılırsa ya da “yama program” yardımıyla düzeltilirse, söz konusu tehdit ortadan kaldırılır. Ařađıdaki tablodan da anlaşılacađı üzere, bir tehdidin oluřması için bir güvenlik boşluđuna ve bu güvenlik boşluđundan yararlanabilecek bir tehdit kaynađına ihtiyaç vardır.

2.5 Risk

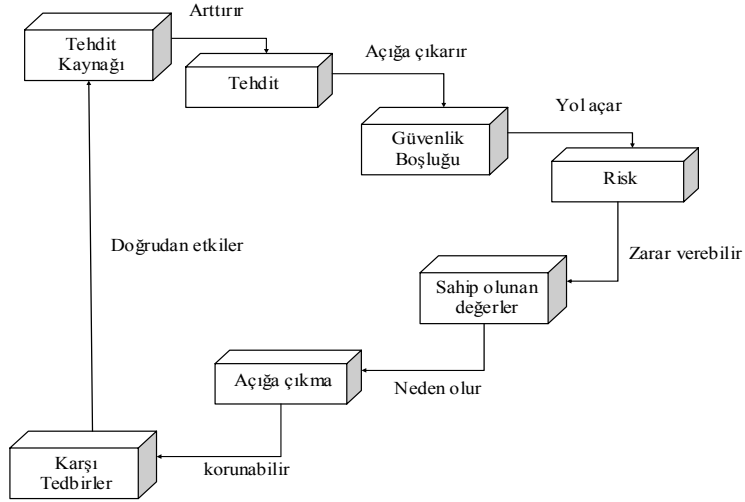
Bir tehdit kaynađının, bir sistemdeki güvenlik boşluđundan yararlanarak sisteme yetkisiz eriřimde bulunması olasılıđı, bu tehdidin *riski* olarak ifade edilir. Tehdit kaynaklarının ya da güvenlik boşluklarının azaltılması, tehdede ait riskleri de aynı oranlarda azaltacaktır.

Tablo-1’de tehdit kaynađı - güvenlik boşluđu – risk iliřkisine örnekler verilmiřtir.

Tablo-1 Tehdit Kaynağı - Güvenlik Boşluğu - Risk İlişkisine Örnekler

Tehdit Kaynağı	Etkileyebileceği Güvenlik Boşluğu	Oluşan Risk
Virüs	Antivirüs yazılımının eksikliği	Virüs bulaşması
Hacker	Sunucu bilgisayar üzerinde çalışan güçlü hizmet programları	Gizli bilgilere yetkisiz erişim hakkının elde edilmesi
Kullanıcılar	İşletim sisteminde yanlış ayarlanmış bir parametre	Sistemin çalışamaz duruma gelmesi
Yangın	Yangın söndürme cihazının eksikliği	Bina ve bilgisayar sistemlerinin zarar görmesi ve can kaybı olasılığı
Çalışanlar	Erişim denetim mekanizmalarının yetersizliği	Görev-kritik bilgilerin zarar görmesi
İş ortağı olan bir firmanın yetkilisi	Erişim denetim mekanizmalarının yetersizliği	Ticari sırların çalınması
Saldırgan	Kötü yazılmış bilgisayar programları	"tampon taşması" hatasının alınması
Kötü niyetli ziyaretçi	Güvenlik Görevlisinin olmayışı	Kıymetli cihaz ve / veya bilgilerin fiziksel olarak çalınması
Çalışan	Tutulan kayıtlardaki yetersizlik	Veri işleme programına verilen giriş verileri ve çıkış olarak elde edilen veriler üzerinde değişiklikler yapılması
Saldırgan	Güvenlik Duvarı'nın ayarlarının iyi yapılmamış olması	Bir "hizmet durdurma" saldırısının gerçekleşmesi

Potansiyel riskler, *tedbirler* yardımı ile azaltılabilirler. Bir tedbir, bir güvenlik boşluğunu ortadan kaldırır ya da bir tehdit kaynağının bir güvenlik boşluğunu kullanması riskini azaltır. Tedbirler, yazılım, donanım ya da geliştirilen bir kullanım yönergesi şeklinde karşımıza çıkabilirler. Tedbirlere, sağlam bir parola yönetim politikası, bir güvenlik görevlisi, bir işletim sistemi üzerinde akıllı kartlara dayalı bir erişim denetim mekanizması, güvenlik konusunda kullanıcıların eğitimi gibi örnekler verilebilir. Şekil-2’de yukarıda bahsedilen kavramların birbirleri ile etkileşimleri gösterilmektedir.



Şekil 2 - Temel Güvenlik Kavramlarının Birbirleri İle Olan İlişkileri
(Shon Harris, *CISSP All-in-One Exam Guide*)

3 Bilişim Güvenliğinin Sağlanması

Bilişim sistemlerinin güvenli hale getirilmesi konusu, kapsamlı ve bütünlük bir yaklaşımla ele alınmadığı takdirde, başarı kazanmak

büyük olasılıkla mümkün olmayacaktır. Bilişim güvenliğinin sağlanması üç temel açıdan ele alınabilir. Bu üç süreç alanı şunlardır:

1. Yönetmelik Önlemler
2. Teknoloji Uygulamaları
3. Eğitim ve Farkındalık Yaratma



Şekil 3 - Bilgi Güvenliğinin Sağlanmasında Bütünleşik Yaklaşım

3.1 Bilişim Güvenliği Süreç Alanları

Güçlü bir güvenlik altyapısı kurabilmek için bu üç parçayı birbiri ile bütünleştirmek ve hepsini birlikte bütünsel bir yaklaşımla ele almak gerekir. Bu bahsedilen süreç alanlarının içinde, bilgisayar ve bilişim güvenliği teknolojilerinin dışında kalan farklı alanlar da bulunmaktadır. Diğer bir deyişle, bir kurumun, kurumsal bilişim güvenliğini sağlamak amacıyla, sadece bilişim teknolojilerini devreye sokarak başarıya ulaşma şansı oldukça azdır.

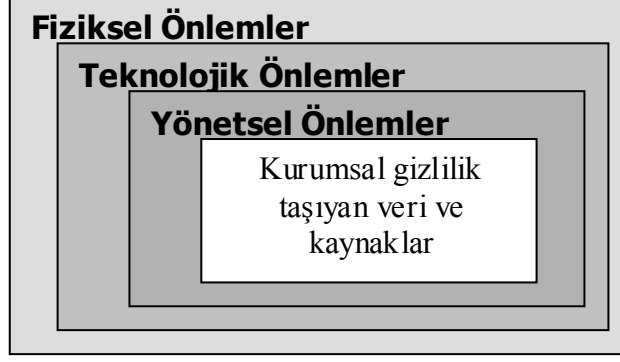
Bütün bunlara ek olarak, bu üç süreç alanından her biri, başarıya ulaşmak için diğer iki süreç alanının tam ve eksiksiz çalışıyor olmasına ihtiyaç duyar. Bu üç alan birbirileri ile ayrılmaz ve sıkı bağlara sahiptir. Birlikte çalışmalarından oluşacak sinerji, kuruma bilişim güvenliği yönünden tehdit oluşturacak tüm etkenlere karşı güçlü bir kalkan görevini üstlenecektir.

Yönetmelik Önlemler, güvenlik yönetimi ile ilgili bir dizi kuralın ortaya koyulması ve uygulanması şeklinde özetlenebilir. Hemen her konuda olduğu gibi, bilişim güvenliğinin yönetiminde de başarı; iyi bir planlama ve üst düzey politikaların doğru ve tutarlı bir şekilde belirlenmesi ile elde edilebilir. Bunun ardından, belirlenenlerin yazıya dökülmesi, yani prosedür, yönerge ve talimatlar gibi dokümanların oluşturulması gelmelidir.

Günümüzde basında ve haber bültenlerinde çok yüksek maddi kayıplara yol açan virüsleri, bilgisayar ağlarına yönelik saldırılardan zarar gören şirketleri konu alan haberler sıkça yer almaktadır. Bununla birlikte, bir sistem yöneticisinin ve güvenlik uzmanının uğraştığı işlerin, her zaman gazete haberlerinde çıkanlarla sınırlı olduğu düşünülmemelidir. Bunlar dışında, günlük ya da periyodik olarak gerçekleştirilecek bir takım işler vardır ki işte yönetmelik önlemler, bu tür işleri kapsayan ve tanımlayan bir süreç alanıdır. Bu süreç alanını oluşturan temel süreçler şunlardır:

1. Risk Yönetimi
2. Güvenlik Politikaları
3. Standartlar, Yönergeler ve Prosedürler
4. Güvenlik Denetimleri

Yönetmelik önlemlerin uygulanması, teknoloji uygulamaları ve eğitim süreçlerinin yanında fiziksel güvenlik uygulamaları ile de desteklenmelidir.



Şekil 4 - Kurumun Sahip Olduğu Değerli Varlıkların Korunması

Yönetsel önlemlerle ortaya konulan kurumun güvenlik ihtiyaçlarının karşılanmasında, teknolojik uygulamalardan da faydalanılır. Günümüzde bir bilgisayar ağına ya da tek başına bir bilgisayara yapılacak bir saldırının sonuçlanması saniyelerle ifade edilen çok kısa bir süre içinde oluşur. Bu tür saldırılara, ancak teknolojik bir takım önlemler ile karşı koyulabilir. Bunun yanında kullanılan teknolojiler, güvenlik yöneticilerinin hayatının kolaylaştırılması ve kurumun, bilişim güvenliği açısından bütün resminin görülmesi gibi yararlar da getirirler.

3.2 Bilişim Güvenliği Teknolojileri

Bilişim Güvenliğinin sağlanmasında kullanılan teknolojilerden bazıları aşağıdaki listede verilmiştir. Unutulmamalıdır ki, güvenlik uygulamalarının bütünü bunlarla sınırlı değildir. Burada en yaygın kullanılan ve en popüler teknolojilerden bahsedilmiştir:

1. Şifreleme (Kriptografi)
2. Sayısal İmza ve PKI
3. Ağ Bölümlemesi ve Güvenlik Duvarları

4. Yedekleme
5. Saldırı Tespiti ve İzleme
6. Erişim Denetimi
7. Güvenlik Derinliği
8. Anti-Virüs

3.3 Eğitim

Eğitim ve Farkındalık Yaratma süreci, bir kurumun bilişim güvenliği açısından karşı karşıya bulunduğu riskleri azaltmada kullanılması gereken ana yöntemlerden biridir. Günlük faaliyetlerini bilişim teknolojisini kullanarak gerçekleştiren kullanıcıların, güvenlik konusunda eğitimlerle bilinçlendirilmesi, onların bir güvenlik boşluğu ve kurum açısından risk oluşturacak bir etken olmaları olasılığını en aza indirecektir.

Örneğin bilişim güvenliği konusunda bilinçsiz kullanıcılardan oluşan bir kurum düşünelim. Bu kurumun coğrafi olarak farklı illere dağılmış kolları ve şubeleri olsun. Her kurumda olduğu gibi bu kurumda da şubeler ve merkez arasında; pazardaki durum, yapılan bir toplantıya ilişkin görüşler, yeni teknolojilerin kullanılması hakkında alınacak kararlar ve bunlara dayanarak stratejik yönetim planların hazırlanması, finansal durum, geleceğe yönelik tahminler ve bunlar gibi daha birçok konuda bilgi akışını gerçekleştirmek gerekir. Kurumun bu bilgi akışını, şu anda rahat ve hızlı bir teknoloji olan e-posta yoluyla gerçekleştirdiğini varsayalım.

Kurumdaki kullanıcılar, e-posta güvenliği konusunda eğitilmemişlerse, gönderdikleri e-postaların başkalarının eline geçmesinin, günümüz teknolojisi ile çok basit olduğu hakkında bilgi sahibi değillerse, gönderdikleri bilgilerin karşı tarafa ulaştırılması sırasında, araya giren bir saldırgan tarafından verilerde değişiklik yapılabileceğini bilmiyorlarsa, bu kurumun bilişim güvenliği yönünden alacağı bütün teknolojik önlemler boşa çıkacaktır.

Kullanıcı bilinçlendirilmesi olmadan, bilişim güvenliğinden söz edilemez. Kullanıcıların eğitim ve farkındalık yaratma süreçleri ile bilinçlendirilmesi, sosyal faktörlerin bilişim güvenliği açısından oluşturdukları riskin de azaltılmasını sağlayacaktır.

Eğitim ve Farkındalık yaratma süreç alanı da aşağıdaki süreçlerle ifade edilebilir:

1. **Bilinçlendirme Eğitimleri** : Bu tür bir eğitimde, konu hakkında temel bilgilendirme ve genel bir bilgi vermek amaçlanır. Bu tür eğitimlere teknik olmayan personel ile yönetici düzeyindeki personel katılabilir.
2. **Kullanıcı Eğitimleri**: Belli bir teknolojinin ya da uygulamanın teknik olmayan kullanıcılar düzeyinde kullanımı konusunda bilgi verme amaçlı eğitimlerdir. Bilinçlendirme eğitimlerine göre daha derinlemesine bir eğitim türüdür. Katılacak kullanıcılar teknik olmayan son kullanıcılarıdır.
3. **Teknik Eğitimler**: Belli bir teknolojinin yönetilmesi, gerektiğinde yeni düzenlemelerin ve ayarların yapılması konusunda verilen derinlemesine eğitimlerdir. Kurumun güvenlik yönetiminden sorumlu personeli katılabilir.

4 Yönetmel Önemler

Bir kurumun elindeki bilgisayarlar ve bu bilgisayarlar üzerinde bulunan veriler, genellikle, kurumun kritik amaçları ve hedefleri ile doğrudan bağlantılıdır. Bu nedenle, kurumun üst yönetimi, bu kaynakların korunmasını kendine bir görev olarak almalı ve gerekli zaman, para ve insan kaynağının bu tür faaliyetlere tahsisi gerçekleştirmelidir.

Yönetmel önlemler, bilişim güvenliği açısından en yukarıdaki üst yöneticilerden en alttaki son kullanıcılara kadar, hiyerarşik bir sorumluluk yapısını ortaya koyar. Önce, nelerin hangi düzeyde bir güvenlik ihtiyacı olduğu belirlenmelidir. Yasal platformda, yürürlükte olan ve bilişim güvenliği konularını da kapsayan kanunların ve tanımlanan sorumlulukların anlaşılması ve kurumun bir bütün olarak bu sorumlulukları yerine getirmesinin sağlanması, yönetmel önlemler açısından değerlendirilmelidir.

Bu durumda, bir kurumun güvenlik yönetimi biriminin temel görevi, güvenlik yönetimine yönelik yönerge ve direktifler oluşturmak değil, öncelikle üst yönetimden güvenlik yönetimi ile ilgili gelen istekleri yerine getirmek olmalıdır. Üst yönetimin desteği olmadan, kurumsal tabanda bir işi gerçekleştirmek hayli zordur. Bu nedenle üst yönetim ile güvenlik yönetimi arasında açık bir iletişim kanalı kurulmalı ve her iki yönde de kusursuz bir bilgi akışı sağlanmalıdır. Bu sayede, yürütülen güvenlik yönetim programı üst yönetimden ihtiyacı olan desteği alır, üst yönetim de gerektiğinde devreye girerek gerekli stratejik kararları verir.

“Bilişim Güvenliği” açısından uzun soluklu bir stratejinin oluşturulması, kurumun bireylerden bağımsız olarak bir güvenlik altyapısı kurması için gerekli bir ön koşuldur. Bu amaçla geliştirilecek olan güvenlik politikalarında kullanılan dil, girilecek ayrıntı seviyesi, politikanın yazılış biçimi gibi faktörler dikkate alınmalıdır. Güvenlik politikasının yalnızca teoride ve lafta kalan bir doküman değil, bunun yerine uygulamaya dönük bir içeriğe sahip olması için gereken çaba gösterilmelidir.

Güvenlik yönetiminin yetersiz olması, kurum bazında güvenlik alanında gerçekleştirilen tüm çabaların boşa gitmesinin sebebi olabilir. Eğer üst yönetim, güvenlik gereksinimlerini tam olarak anlayamaz ise, yönetimin diğer hedeflerinin yanında pahalı, gereksiz, görünürde hiçbir yararı olmayan bir faaliyet olarak görebilir ve yeterli desteği sağlamayabilir. Böyle bir durumda, bilişim güvenliği alanındaki en güçlü teknolojiler satın alınsa bile, yönetim desteği olmadığı takdirde verimsiz ve âtil birer yatırım olarak kalacaklardır.

4.1 Risk Yönetimi

Risk, kuruma zarar verici bir olayın gerçekleşme olasılığı, olarak tanımlanabilir. Risk yönetimi ise, kurumun karşı karşıya bulunduğu risklerin tanımlanması, bu risklere değer biçilmesi, risklerin kabul edilebilir bir seviyenin altına indirilmesi ve sürekli bu seviyenin altında kalmalarını sağlayacak mekanizmaların devreye sokulmasıdır.

Yüzde yüz güvenli bir çalışma ortamı kurmak imkansızdır. Her çalışma ortamında, bir takım güvenlik boşlukları ve bunlara bağlı riskler mevcuttur. Yapılması gereken, karşı karşıya olduğumuz riskleri, doğru bir şekilde yönetmektir.

Bilişim Güvenliği açısından karşımıza çıkabilecek riskler, aşağıdaki şekilde sınıflandırılabilir:

- Fiziksel zarar
- İnsan hatası
- Donanım hatası
- Gizli verilerin ifşası/değiştirilmesi
- Verilerin yok olması
- Yazılım uygulamalarının hatalı çalışması

4.1.1 Kurumsal Bilgi Kaynaklarına Değer Biçme

Kurumsal bilgi kaynaklarına değer biçilirken, farklı açılardan bakmak gerekebilir. Örneğin, bir sunucu bilgisayarın satın alma maliyeti 5 Milyar TL ise bu kaynağa 5 Milyar TL değer biçmek doğru değildir. Değer biçme sırasında göz önünde bulundurulması gereken bir takım

hususlar şunlardır (Burada belirtilen hususların tümü her bilgi kaynağı için uygun olmayabilir) :

- ❑ Kaynağın yeniden satın alınması ya da geliştirilmesi maliyeti
- ❑ Kaynağın idamesi ve korunması maliyeti
- ❑ Kaynağın sahipleri ve kullanıcıları açısından maliyeti
- ❑ Kaynağın, kurumun rakipleri açısından maliyeti
- ❑ Fikir hakları açısından maliyeti
- ❑ Başka kurumların kaynağa sahip olma maliyeti
- ❑ Kaynağın yok olması durumunda üretimin etkilenmesi ve operasyonel açıdan yaratacağı etkiler sonucunda ortaya çıkacak olan maliyet
- ❑ Kaynağın açığa çıkması durumunda doğacak sorumluluğun maliyeti
- ❑ Kaynağın kullanılabilirliği açısından maliyeti

4.1.2 Risk Analizi

Risk analizi, risklerin gerçekleşme olasılıklarının, gerçekleşmeleri durumunda yol açacakları kayıpların doğru bir şekilde belirlenmesi ve buna göre uygun tedbirlerin devreye sokulmasıdır. Risk analizinin üç temel amacı vardır:

- Risklerin belirlenmesi
- Tehditlerin potansiyel etkisinin belirlenmesi
- Riskin gerçekleşmesi durumunda getireceği zararlar, bu riskten korunmak için seçilecek tedbir arasında ekonomik bir denge kurulması



Şekil 3 - Risk Yönetiminin Adımları

Doğrudan ve dolaylı maliyetler dikkate alınmadığında, bir kurum için, kağıt üstünde “çok güvenli” bir güvenlik altyapısı kurmak kolaydır. Ancak kurumun hedefi, kendisi için “yeterli, etkin ve yönetilebilir” bir güvenlik altyapısını oluşturmak olmalıdır. Bu yeterlilik düzeyini belirlemede risk analizi önemli bir role sahiptir. Risk analizi yardımıyla kurumlar, karşı karşıya buldukları riskleri öncelik sırasına koyabilir ve her bir riske karşı alınacak önlemlerin ve tedbirlerin getireceği maliyetleri değerlendirebilirler.

Risk analizi sayesinde kurum çalışanları bir maliyet/yarar analizi yapabilirler. Kullanılacak tedbirlerin yıllık maliyetleri ile bir tehdidin gerçekleşmesi durumunda neden olacağı zarar karşılaştırılabilir. Örneğin gizli bir bilginin değeri 100 Milyar TL ise, bu veriyi korumak için 150 Milyar TL harcamanın bir anlamı yoktur.

Risk analizi yardımı ile, kurumun bilişim güvenliği konusundaki amaçları ile diğer kurumsal amaçlar bütünleştirilebilir. Bu bütünleştirme derecesi, amaçlara ulaşmada doğrudan bir etkidir.

4.1.3 Tedbirlerin Seçimi

Tedbir, ya da başka bir deyişle “koruyucular”, maliyet-etkin ve kendisine harcanan paranın hakkını verecek şekilde seçilmelidir. Bir koruyucunun kullanımında karşılaşılabilecek maliyetler aşağıdaki tabloda gösterilmiştir:

- ❑ Çalışma ortamında yapılması beklenen değişiklikler
- ❑ Üretkenliğe Etkisi
- ❑ İdamesi için gereksinimler
- ❑ Diğer tedbirlerle uyumlu çalışabilme
- ❑ Test gereksinimleri

- ❑ Gerektiğinde onarım/yerine yenisini koyma ve güncelleme maliyetleri
- ❑ Tasarım/Planlama
- ❑ Operasyon ve Destek

4.2 Güvenlik Politikaları

Güvenlik Politikası, kurumda güvenliğin oynadığı rolün genel bir anlatımıdır. Güvenlik Politikası üst yönetim, seçilmiş bir Kurul ya da bir Komite tarafından yazılabilir. Güvenlik Politikaları, bireylerden ve teknolojiden bağımsız hazırlanmalıdır. Kurumda uygulanacak güvenlik kontrolleri, ayrıntıya girilmeden kavramsal olarak tanımlanmalıdır.

Internet Week dergisinin 2000 yılı sonunda üst düzey yöneticiler arasında yaptığı bir araştırmaya göre, araştırmaya katılanların %70'i kurumlarında güvenlik teknolojisinin kullanılmakta olduğunu bildirmiş, ancak yalnızca %38'i yazılı bir güvenlik politikasına sahip olduklarını söylemişlerdir.

Güvenlik politikasının kuruma üç yararından bahsedilebilir:

1. Kurum çalışanlarını ve üçüncü tarafları yasal sorumluluktan kurtarmak,
2. Kuruma özel gizli bilgileri; hırsızlığa, suistimale, yetkisiz kişilerin eline geçmesine, ifşaya ve değiştirilmeye karşı korumak,
3. Kurumun bilgi-işlem yeteneğini oluşturan kaynakların israfını ve boşa kullanımını engellemek.

Bir kurum için hiyerarşik olarak farklı düzeylerde güvenlik politikalarından bahsedilebilir:

1. **Kurumsal Güvenlik Politikası:** Üst yönetim tarafından, kurumda bilişim güvenliği programının çerçeve çalışması ifade edilir. Bu tür bir politika, kurumun gelecekteki tüm güvenlik faaliyetlerini kapsaması ve yönlendirmesi açısından önem taşır. Politika içerisinde; programın amaçları, verilecek

sorumluluklar, güvenliğin stratejik/taktik açıdan önemi ve uygulamada yapılacak işler, genel hatları ile kavramsal olarak tarif edilir. Kurumsal Güvenlik Politikası içerisinde, ilgili kanunlara, yasal düzenlemelere ve diğer yönerge ve prensiplere başvurular yapılabilir. Üst yönetimin, bilişim güvenliği açısından kabul edilebilir bulduğu risk düzeyi de bu tür bir politikada yer alabilir.

2. **Konuya Özel Güvenlik Politikası:** Üst yönetim, belli konularda çalışanlarını daha fazla bilgilendirmek, daha ayrıntılı bilgi vermek, bu konuyu kapsamlı bir şekilde ifade etmek istediğinde bu tür bir politika geliştirilebilir. Örneğin, e-posta gönderme alma konusunda, üst yönetimin kararlarını, haklarını, yapıp-yapamayacaklarını bu tür bir politika içerisinde ifade etmek uygun olacaktır. Üst yönetimin, gerekli görüldüğünde çalışanların e-postalarını okuyabileceği, e-postalar yoluyla gizlilik dereceli bilgilerin gönderilip alınmayacağı gibi hususlar, e-posta özel politikası içerisinde ifade edilir.
3. **Sisteme Özel Güvenlik Politikası:** Üst yönetimin, bilgisayarlar, bilgisayar ağları ve uygulamalar ve kurumsal veriler hakkında aldığı ayrıntılı kararları içerir. Bu tür bir politika içerisinde, kullanılmasına izin verilen yazılımlar, veritabanlarının nasıl korunacağı, bilgisayarlara uygulanacak erişim denetim kriterleri, güvenlikle ilgili kullanılan yazılım ve donanımların nasıl kullanılacağı gibi konular açıklanabilir.

Güvenlik politikalarını desteklemek üzere daha ayrıntılı bir takım dokümanlar oluşturulabilir. Politika ile bu dokümanların ilişkisi Şekil-6'da verilmiştir. Kurumun stratejik ve taktik hedefleri arasındaki farklılık, politika ile standart, yönerge ve prosedürler arasındaki farklılıkta da kendini gösterir. Güvenlik Politikası, kurumun stratejik bir hedeflerini içerirken; standart, yönerge ve prosedürler taktik düzeyde olan hedefler içerir. Taktik hedefler, stratejik hedefleri gerçekleştirmek amacıyla ortaya konur.

4.3 Standartlar, Yönergeler ve Prosedürler

Bir kurumun *güvenlik standartları*, o kurumdaki bilgisayar yazılım ve donanımlarının nasıl kullanılacağı hakkında bilgi verir. Kullanılan teknolojilerin ve uygulamaların, her bir kullanım sırasında tanımlanmış standartlara uygun olarak kullanılmasını garanti eder.

Yönergeler, kurumsal bir standardın belli bir uygulamada kullanılmasında güçlük çekildiğinde, yol gösterici bir takım öneriler içerecek şekilde hazırlanırlar. Standartlar, gerçek hayatta ve uygulamada karşılaşılabilecek bütün durumları ele alamayabilir. Bu durumda bir yönerge yardımı ile standartta yeterince açık olmayan "gri alanlar" açıklığa kavuşturulur.

Prosedürler, belli bir işi gerçekleştirmeye yardımcı olmak amacıyla hazırlanmış olan ve atılacak adımları ayrıntılı olarak içeren dokümanlardır. Örneğin bir yazılımın yüklenmesi, bir donanımın kurulması, yazılım ya da donanımın ayarlarının değiştirilmesi/düzeltilmesi, sistemde yeni bir kullanıcı hesabının tanımlanması, yok edilmesi gereken malzemenin nasıl imha edileceği gibi konularda prosedürler hazırlanabilir. Tanımlanmasında büyük yarar olan prosedürler şunlardır:

- Konfigürasyon Yönetim Prosedürü
- Yedekleme ve Yedekleme Ortamlarını Saklama Prosedürü
- Olay Müdahale Prosedürü
- İş Sürekliliği ve Felaket Kurtarma Prosedürü

Prosedür, yönerge ve standartlar, birbirleri ile bütünlük içinde ve birbirlerini destekleyecek şekilde hazırlanmalıdır. Örneğin bir yönergede, "kullanıcının bir sisteme girmesi için kimlik sınavından geçmesi gerektiği" yazıyorsa, ilgili prosedürde de bu tür bir kimlik sınavı için yapılması gereken faaliyetler adım adım ve okuyanın anlayacağı bir şekilde belirtilmelidir.

Prosedür, yönerge ve standartları, tek bir büyük dokümanın içine sıkıştırmak yerine, modüler bir şekilde hazırlamak, kullanım kolaylığı ve esneklik açısından daha verimli bir çalışma sağlayacaktır. Çünkü

bu türlerden her birinin kullanım alanı ve kullanacak kişiler farklılık gösterir bu şekilde dokümanların kullanıcılarına dağıtılması ve gerektiğinde güncellenmeleri kolaylaşmış olur.

4.4 Güvenlik Yaşam Döngüsü

Çeşitli teknik ve yönetsel yönlerini vurgulamış olduğumuz bilişim güvenliği kavramlarının etkinliğini sağlamak, konuyu sürekli canlılığını koruyacak bir yaşayan proje olarak ele almakla mümkün olacaktır. Tehditlerin sürekli olarak yenilenmesi ve çeşitlilik kazanması, kullanılan altyapıların sık aralıklarla güncelleme, iyileştirme, genişleme ve benzeri değişikliklere uğraması ve yazılım sistemlerindeki sürekli değişimler, herhangi bir anda güvenli kabul edilebilecek bir sistemin takip eden sürede güvenli kalmasını garanti edemez. Bu nedenle, güvenlik çalışmaları bir yaşam döngüsü ile modellenmektedir.

Genel kabul görmüş yaklaşımlardan biri olan CERT (Computer Emergency Response Team) tarafından önerilen yaşam döngüsü, aşağıdaki adımları içermektedir:

- ❑ Sistem Güçlendirme (Harden / Secure)
- ❑ Hazırlık (Prepare)
- ❑ Saldırı / Sorun Tespiti (Detect)
- ❑ Tespit edilen olaya özgü önlemlerin alınması / kurtarma (Respond)
- ❑ İyileştirme, tespit edilen olayın tekrarını önleyecek önlemler (Improve)

Bu adımların tekrarlı bir biçimde gerçekleştirilmesi sayesinde, sürekli olarak potansiyel sorunlar tespit edilebilir ve zamanında önlem alınarak sistem güvenliği azami seviyede korunmaya çalışılır.

4.5 Güvenlik Denetimleri

Güvenlik denetimi, bir kurumun güvenlik altyapısının, güvenlik politikasının, prosedürlerinin ve personelinin ayrıntılı bir biçimde ele

alınması, zayıf yönlerin tespiti ve bu zayıflıkların giderilmesi için öneriler sunulmasıdır.

Başarılı bir denetim, tüm ilgili tarafların işbirliği ile gerçekleştirilebilir. Genelde güvenlikle ilgili bir denetim söz konusu olduğunda, birçok insan olumsuz bir önyargıya kapılır ve rahatsız olur. Bununla birlikte, güvenlik denetimi kurum içinde güvenlik politikasına uygun çalışılıp çalışılmadığının tespitinde kullanılacak tek yoldur.

Denetlenecek faaliyetler arasında; bilgisayarlara giriş/çıkışlar, dosya işlemleri ve sistem ve ağ erişim haklarının değiştirilmesi olarak sayılabilir. Bir denetim sırasında sorgulanabilecek konulardan bazıları şunlardır:

- Hangi veriler "salt okunur", hangileri "yazılabilir"dir?
- Önemli verileri kim/ne değiştirebilir?
- Sistem erişimini ve kaynak kullanımını ne engelleyebilir?
- Sistem üzerindeki değişiklikler nasıl yapılmaktadır?
- Sisteme nasıl erişilebilir?
- Bilgisayarlar, bilgisayar ağları ve bunların buldukları binalar fiziksel açıdan güvenli mi?
- Sistemde yapılan değişiklikler izleniyor mu?
- Sistemde aksaklık çıktığında, bunun nedenleri ortaya çıkarılabiliyor mu?
- Kullanıcı grupları tanımlanmış mı? Hangi kullanıcıların erişim yetkileri, diğerlerine nazaran daha fazla? Tüm kullanıcıların sahip olduğu haklar neler?

İki tip denetim vardır. Biri kurumun kendi personeli tarafından gerçekleştirilen "İç Denetim", diğeri ise kurum dışı, bağımsız bir kuruluş tarafından gerçekleştirilen "Dış Denetim"dir.

Başarılı bir denetim için iki temel nokta göz önüne alınmalıdır:

1. Planlama: Bir denetim planında, kurumun hangi açılardan denetleneceđi ve sonuçların nasıl deđerlendirileceđi ortaya konur.
2. Kullanılan Araçlar: Denetimin yapılmasına yardımcı olacak belge, yazılım, kamusal bir takım kriterler bu sınıfa girerler.

5 Teknoloji Uygulamaları

Bu bölümde, güvenlik tedbirlerinde kullanılan teknolojilerden bahsedilmiştir. Tüm teknolojiler burada bahsedilenlerle sınırlı değildir. Bunun yanında burada adı geçen teknolojiler, bilişim güvenliği söz konusu olduğunda ilk akla gelenlerdir. Sırasıyla Bölüm 5.1’de Kriptografi, Bölüm 5.2’de Sayısal İmza ve PKI, Bölüm 5.3’de Ağ Bölümlemesi ve Güvenlik Duvarları, Bölüm 5.4’de Yedekleme, Bölüm 5.5’de Saldırı Tespiti ve İzleme, Bölüm 5.6’da Erişim Denetimi ve Bölüm 5.7’de Anti-virüs teknolojilerinden bahsedilmiştir.

5.1 Kriptografi

Kriptografi, veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılan bir teknolojidir. Kriptografi’de veri, matematiksel yöntemler kullanılarak kodlanır ve başkalarının okuyamayacağı hale getirilir. Bu matematiksel kodlamaya “*kripto algoritması*” adı verilir. İlk bilinen kripto algoritmaları 4000 yıl kadar önce ortaya çıkmıştır. Zaman geçtikçe, kullanılan teknikler ve cihazlar gelişmiş ve her geçen gün yeni teknikler kullanılır ve yeni algoritmalar üretilir olmuştur. Bu teknoloji şu anda bilişim güvenliğinin vazgeçilmez bir parçasıdır.



Şekil 5 - Temel Kriptografi Mekanizması

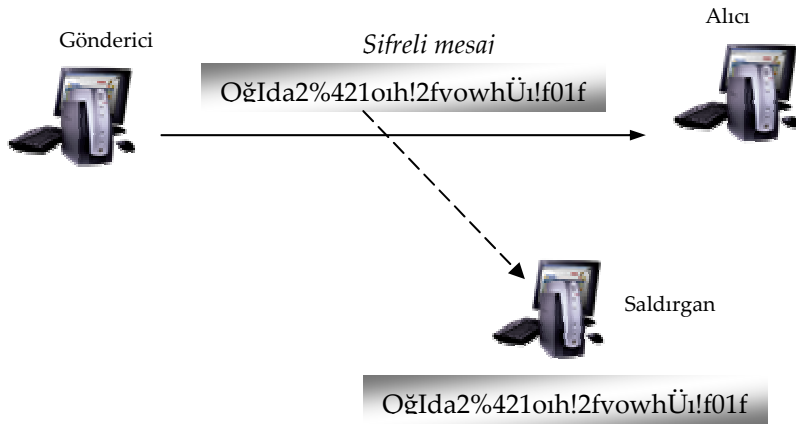
Şifrelenmemiş bir bilgiye “açık metin” (clear text) denir. Açık metin, bir insanın okuyabileceği bir yazı ya da bir bilgisayarın anlayabileceği çalıştırılabilir (.exe, .com) bir program ya da bir veri dosyası (.txt) olabilir. Bir kripto algoritması kullanılarak, herkesin okuyamayacağı bir şekilde kodlanmış bilgiye ise “şifreli metin” (ciphered text) denir. Açık metinden şifreli metne geçme işlemi “şifreleme”, şifreli metinden

açık metne geçme işlemi ise “şifre çözme” olarak adlandırılır. Şifreleme ve şifre çözme yapan bir sistem de “kriptosistem” olarak adlandırılır. Bir kriptosistemin, şifreleme ve şifre çözme yapan hem donanım hem de yazılım bileşenleri olabilir.

Algoritmalar, açık metin üzerinde yapılan karmaşık işlemlerden oluşan matematiksel formüllerdir. Bir algoritma, hem yazılımla hem de donanım bileşenleri ile gerçekleştirilebilir. Birçok algoritma, şifreleme ve şifre çözme işlemi gerçekleştirilmek amacıyla, açık metinden başka, “anahtar” denen bir değer de kullanır. Anahtar “0” ve “1”lerden oluşan uzun bir bit dizisidir. Her algoritmanın kullandığı anahtar boyları farklıdır. Genellikle anahtar boyu arttıkça, olası anahtar sayısı arttığından, saldırganın bu şifreyi çözmesi güçleşir, ama aynı zamanda da şifreleme ve şifre çözme hızı yavaşlar. Bir algoritmanın olası tüm anahtarlar olasılıklarının oluşturduğu topluluğa “anahtar uzayı” denir.

Şekil-7’de bir saldırganın hattı dinleyerek mesajı ele geçirmesi gösterilmiştir. Ancak saldırgan mesaja sahip olsa bile, mesaj kriptolu olduğundan içeriği konusunda bilgi sahibi olamaz.

Kripto sistemleri, ilk bölümde bahsedilen Gizlilik, Veri Bütünlüğü, Kimlik Sınaması ve İnkâr Edememe hizmetlerinde kullanılır.



Şekil 7 - Hattı Dinleyen Bir Saldırgana Karşı Şifrelemenin Kullanılması

Kripto algoritmaları temelde ikiye ayrılırlar: Simetrik Algoritmalar ve Asimetrik algoritmalar. Aşağıdaki bölümlerde bu iki algoritma türü sırasıyla tanıtılmıştır. Bölüm 5.1.3'de ise özetleme fonksiyonlarından bahsedilmiştir.

5.1.1 Simetrik Algoritmalar

Simetrik algoritmalarda şifreleme ve şifre çözme için aynı anahtar kullanılır. Bu anahtara gizli anahtar (secret key) denir. Bu gizli anahtar iki tarafça da (gönderici ve alıcı) bilinir.

Simetrik algoritmalar asimetrik algoritmalarla nazaran daha hızlı çalışırlar. Bununla beraber, asimetrik algoritmalarla nazaran saldırıya karşı daha az dirençlidirler. Simetrik algoritmalarla örnek olarak AES, DES, 3DES, Blowfish, IDEA, RC4 ve SAFER algoritmaları verilebilir.

5.1.2 Asimetrik Algoritmalar

Şifreleme ve şifre çözme için ayrı anahtarlar kullanılır. Bu anahtarlardan birine açık anahtar (public key), diğerine özel anahtar (private key) denir. Kullanılacak bu iki anahtar birlikte üretilirler. Bununla birlikte bu anahtarlardan herhangi birine sahip olan bir şahıs, diğer anahtarı üretemez, bu matematiksel olarak imkansız denebilecek derecede zordur.

Asimetrik algoritmalar, simetrik algoritmalarla göre daha güvenli ve kırılması zor algoritmalarlardır. Bununla birlikte, başarımları (performans) simetrik algoritmalarla göre oldukça düşüktür. Asimetrik algoritmalarla her şahsın bir anahtar çifti vardır. Bir şahsın özel anahtarı, yalnızca kendi kullanımı içindir ve başkalarının eline geçmemesi gerekir. Bu şahsın açık anahtarı ise, bu şahsa mesaj göndermek isteyen herhangi biri tarafından kullanılabilir. Gönderici mesajı, alıcının açık anahtarı ile şifreler. Alıcı, gelen mesajı kendi özel anahtarı ile açar.

Mesaj gönderebileceğimiz kullanıcıların sayısı arttıkça, elde etmemiz gereken açık anahtar sayısı da artacaktır. Sistemde 100 kullanıcı varsa, her bir kullanıcının ayrı bir açık anahtarı olacağından, tüm bu açık anahtarlar, erişilebilir olmalıdır. Bu problem de sayısal sertifikalar

teknolojisi yardımı ile çözülebilmektedir. Bölüm 5.2’de bu teknoloji açıklanmaktadır.

Asimetrik algoritmalarla örnek olarak RSA, ECC, Diffie-Hellman ve El Gamal algoritmaları verilebilir.

Görüldüğü gibi simetrik ve asimetrik algoritmaların birbirlerine göre bir takım üstünlükleri ve zayıf yönleri vardır. Her iki algoritma grubunun üstünlüklerinden faydalanarak zayıf yönlerini bir kenara bırakmak amacıyla “hibrid kriptosistemler” kullanılmaktadır. Bu tür sistemlerde hem simetrik hem de asimetrik algoritmalarla hem başarıyı hem de güvenliği yüksek şifreleme yapılabilmektedir.

5.1.3 Özetleme Fonksiyonları

Bir özetleme fonksiyonu, herhangi bir uzunluktaki metni, giriş değeri olarak alır ve sonuç olarak sabit uzunluklu bir değer üretir. Bu değere mesaj özeti (message digest) adı verilir. Burada üretilen özet, fonksiyona giren metnin karakterini taşımaktadır denilebilir. Giriş metninde yapılacak tek bir karakter değişikliği bile üretilen özetle büyük değişikliklere yol açar. Ayrıca, özetleme fonksiyonu tek yönlü olduğundan, özette asıl metne geri dönüş yoktur. Özetleme fonksiyonları, uzun metinlerin, asimetrik bir algoritma ile şifrelenmeleri sırasında, asimetrik algoritmanın başarımlı dezavantajını ortadan kaldırmak amacıyla kullanılırlar. Tüm mesaj metni değil de yalnızca mesajın özeti alınarak asimetrik algoritmayla şifrelenir. Özetleme algoritmalarına örnek olarak SHA-1 , DSS, MD2, MD4, MD5 algoritmaları verilebilir.

5.2 Sayısal İmza ve PKI

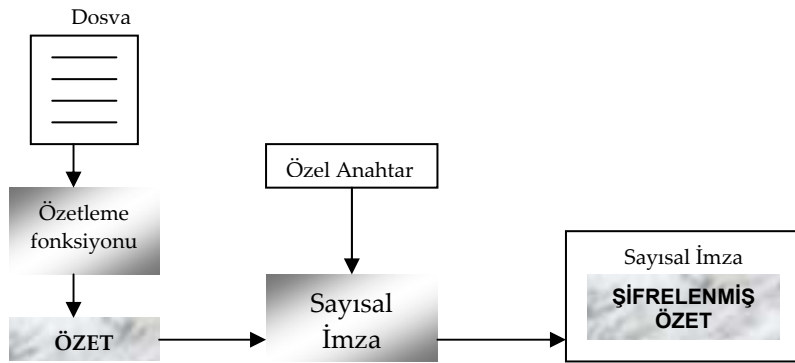
Bir sayısal imza, şifrelenmiş bir özet (hash) değeridir. Sayısal imzalar yardımıyla, alıcı taraf göndericinin kimliğinin sınavını yapar ve göndericinin kim olduğundan tam olarak emin olur. Bunun yanında, sayısal imza teknolojisi, gönderilen verilerin bütünlük sınavında da kullanılabilir. Buna göre sayısal imza teknolojisi, ilk bölümde bahsedilen Kimlik Sınavı ve Veri Bütünlüğü prensiplerinin gerçekleştirilmesinde kullanılırlar.

Sayısal imzalar, gerçek hayatta kullanılan ve elle atılan imzanın (ıslak imzanın) bilişim dünyasındaki karşılığı olarak görülebilir. Bir sayısal imza, imzaladığı içeriğin, imzalandığı andan itibaren değişmediğinin kanıtlanmasında kullanılabilir.

Sayısal imzalama, asimetrik kript algoritmaları yardımı ile yapılır. Sayısal imzalama, mesaj bir mektup zarfına konulduğunda üzerinin mühürlenmesi gibi düşünülebilir. Sayısal imzalar, bilgisayar ağları yoluyla yapılan finansal işlemlerin güvenli bir şekilde yapılması ve veritabanı bütünlüğünün kontrolü gibi kullanım alanları bulmuşlardır.

Sayısal imzalar, Açık Anahtar Altyapısı (Public Key Infrastructure – PKI) teknolojisinin de belkemiğini oluşturur. PKI, çok geniş bir coğrafi alana yayılmış kullanıcılar arasında, güvenli bir haberleşme altyapısı kurmayı hedefleyen bir teknolojidir. Açık Anahtar Altyapısı'nı oluşturan elemanlardan başlıcaları şunlardır:

1. **Sayısal sertifikalar:** Bir sayısal sertifika, gerçek hayatta kullanılan bir kimlik kartının, bilişim güvenliğindeki karşılığıdır. Bir sertifikanın içinde; sahibinin kimlik bilgileri, yetki derecesi, sertifikanın son kullanma tarihi, sahibinin kript anahtarı bilgisi yer alır. Bir sayısal sertifika, bir kullanıcının bir sisteme girerken kimlik sınamasının yapılmasında ya da kriptolu e-posta mesajlarının



Şekil 8 - Bir Mesajın Sayısal İmzası'nın Oluşturulması

gönderilmesinde kullanılabilir. Sayısal sertifikalar için ISO tarafından X.509 standardı yayınlanmıştır ve bu standart yaygın olarak kullanılmaktadır.

2. **Sertifikasyon Otoriteleri:** Bir PKI sistemine dahil olan kullanıcılar için sayısal sertifika üretim ve saklama merkezleridir. Bir kullanıcıya mesaj gönderilirken ya da gelen bir mesajdaki sayısal imzanın doğruluğunun sınanırken, o alıcının açık anahtarına ihtiyaç duyulur. Bu açık anahtar elde etmek için, sertifikasyon otoritesinden, kullanıcının kimliği yardımı ile kullanıcının sayısal sertifikası elde edilir. Kullanıcının açık anahtarı, bu sertifika içerisinden alınarak kullanılır.

5.3 Ağ Bölümlendirmesi ve Güvenlik Duvarları

Güvenlik duvarı (firewall), bir kurumun ağ güvenliği politikasının uygulanmasında kullanılan bir teknolojidir. Güvenlik duvarları, bir bilgisayar ağundan başka bir bilgisayar ağına geçişi sınırlarlar. Birçok kurum, kendi bilgisayarlarına, internet üzerinden gelebilecek saldırılara karşı güvenlik duvarlarını kullanır. Bunun yanında, kurum içi bir ağ bölümü ile yine kurum içi başka bir ağ bölümü arasındaki geçiş sınırlamasında da güvenlik duvarı kullanılabilir. Bir güvenlik duvarı, ağ üzerindeki bir boğum noktası olarak düşünülebilir. Çünkü iki ya da daha çok ağ arasındaki tüm trafik güvenlik duvarından geçmek zorundadır. Güvenlik duvarları, yazılım olarak gerçekleştirilebildikleri gibi, yüksek trafik akışı olan noktalarda donanımla gerçekleştirilmiş güvenlik duvarları da kullanılmaktadır.

Birçok kurum güvenlik duvarlarını, arınmış bölge (demilitarized zone) kurulumu için kullanır. Bu düzenlemede güvenlik duvarının üç bacağı vardır: Birinci bacak dış ağ ile irtibatı ikinci bacak iç ağ ile irtibatı sağlar. Üçüncü bacak ise iç ve dış ağ arasında kalan "arınmış bir bölge" kurmayı sağlar. Bu üçüncü bacağın olduğu bölgeye, kurumun dışarı açık, web, e-posta ve DNS gibi bir takım hizmetlerinin sunulduğu bilgisayar kaynakları koyulabilir. Çünkü bu kaynaklar, saldırganlar tarafından ilk olarak saldırıya maruz kalması beklenen kaynaklardır. Günümüzde arınmış bölgelerin çoğunda

kurulan bir "Saldırı Tespit Sistemi" (Intrusion Detection System - IDS) yardımıyla saldırgan davranışları izlenerek gerekli tedbirler alınmaktadır.

Güvenlik duvarları, ağ adres dönüşümü (Network Address Translation - NAT) hizmeti yardımı ile, iç ağdaki bilgisayarların IP adreslerini, dışarıdaki saldırganlardan gizler.

Güvenlik duvarları, iç ağdaki bilgisayarlara vekil (proxy) hizmeti verebilirler. Bu şekilde, örneğin iç ağdaki bir kullanıcının bilgisayarı ile bu kullanıcının internet üzerinde bağlandığı web sayfası arasında doğrudan bir bağlantı kurulmaz. Bunun yerine kullanıcı ile vekil sunucu ve vekil sunucu ile internet sayfası arasında kurulan iki bağlantı söz konusudur. Vekil sunucunun görevi, kullanıcıya, kendi varlığını hissettirmeden, bağlantılar arasında verilerin taşınması ve bu sırada da tanımlanmış güvenlik politikasına göre de gelip geçen verilerin kontrol edilmesidir.

Internet üzerinde belli ağ bölümlerine ya da hizmetlere erişilmesini engellemek ya da internet üzerinden kurumsal ağlardaki kaynaklara erişimi düzenlemek için de güvenlik duvarının paket eleyici (packet filtering) hizmetinden faydalanılır. Bir paket eleyici, kendisine gelen veri paketinin 5 özelliğine bakarak paketin, diğer ağ bölümüne geçişine izin verip vermeme kararını verir. Bu özellikler şunlardır:

1. Kaynak IP adresi
2. Kaynak hizmet noktası (port)
3. Hedef IP adresi
4. Hedef hizmet noktası
5. Bağlantı tipi (TCP, UDP, ICMP, vb.)

Paket eleyicilerin karar vermede kullandıkları politika tablosu da iki tür olabilir:

1. **Tanımlı olmayanlara izin verilmesi:** Paket eleyicinin politika tablosunda tanımlı olan kurallar dışındaki tüm trafiğin geçişine izin verilir. Örneğin kurum, kendi kullanıcılarının

ICQ'ya ve IRC'ye bağlanmalarını istemiyorsa bu kurallar yazılır ve geri kalan tüm trafiğin geçişine izin verilir.

- 2. Tanımlı olmayanlara izin verilmemesi:** Paket eleyicinin politika tablosunda tanımı olan kurallar dışındaki hiçbir trafiğin geçişine izin verilmez. Bu tür çalışmaya örnek olarak, kurum, kullanıcıların yalnızca web sayfalarına bağlanmasını istiyorsa, burada web sayfalarına erişimde kullanılan HTTP protokolünün hizmet numarası (port number) olan 80 tanımlanır. Bu şekilde herhangi bir sunucu üzerinde 80 numaralı porta erişimler hariç hiçbir trafiğe izin verilmez.

Bir kurumda birden fazla güvenlik duvarı art arda konularak çalışma verimi ve sağlanan güvenlik arttırılabilir. Daha yüksek güvenlik düzeyi gerektiren kurumsal bölümlerin ağ girişlerine de gerekirse ikinci bir güvenlik duvarı koyulabilir.

5.4 Yedekleme

Bir sistemin yedeğini almak ve bunu düzenli olarak yapmak insanlara genellikle hep zor gelir; ta ki sistemlerinin devre dışı kaldığı, verileri kaybolduğu ya da bozulduğu güne kadar.

Sürekli ve tutarlı bir şekilde, çalıştığımız verilerin yedeğini almak, bir gün yaşayacağımız bir saldırı ya da doğal bir afetin sonuçlarının bizi en az şekilde etkilemesini sağlayabilir. Bir yedek alma sisteminin kurulmasının maliyeti, üretilmesi uzun zaman alan verimizi kaybettikten ya da veritabanımızdaki tüm kayıtlar silindikten sonra yeniden kazanma maliyetinden çok daha düşüktür.

Doğal olarak, sistemdeki her verinin yedeği alınmamalıdır. Bu tür bir çalışma yedekleme sistemimizin maliyetini oldukça arttıracaktır. Bu nedenle, hangi verinin bizim için kritik, önemli ve yedeği alınması gerekli veri olduğunun tespiti gerekir. Bu şekilde, farklı veri gruplarının yedekleme açısından öncelik sıraları belirlenir. Yedeği alınacak verilerin ve yedek alma sıklığının doğru tespiti ile, yedekleme sürecini, sistemin günlük işleyişini en az şekilde etkileyecek şekilde düzenlemek gerekir.

Özellikle doğal afetlere karşı, yedeklerin farklı bir coğrafi bölgede saklanması gerekir. Bu tür bir yedeklemede veriler, çevrim-içi ve çevrim-dışı şekilde aktarılabilir. Çevrim içi aktarımda veriler, farklı bölgedeki merkeze, periyodik olarak bilgisayar ağı üzerinden aktarılır. Çevrim-dışı yolu ile yapılan yedeklemede ise, veriler, yüksek kapasiteli bir saklama ünitesi (teyp, flash bellek, taşınabilir hard disk, CDROM, DVD-rom gibi) üzerine yazılarak güvenli bir şekilde yedek alınan bölgeye ulaştırılır.

Veritabanı yedeklemesi, iş-sürekliliğinin sağlanmasında önemli bir faktördür. Kurumun veritabanlarını farklı bilgisayarlarda yedeklenmiş şekilde tutmak (replicated database), bir veritabanı sunucusunda meydana gelebilecek arıza ya da sistem güncelleme gibi durumlara karşı tüm sistemi toleranslı hale getirecektir.

Sistemlerin, elektrik kesilmelerine ve güç kaynağı arızalanmalarına karşı korunması da yedekleme konusunda ele alınabilir. Elektrik kesilmesi, hem kesinti boyunca çalışmamızın durmasına neden olur, hem de çalışan sunucumuz, "shutdown" gibi bir komut verilerek değil de sanki bir anda fişi çekilerek kapatıldığından, sunucuda geri dönülemez donanım ya da yazılım arızaları meydana gelebilir.

Bu tür durumlardan korunmak amacıyla, sistemler kesintisiz güç kaynakları ve yedek güç üniteleri ile desteklenmelidir.

5.5 Saldırı Tespiti

Saldırı tespit Sistemleri (Intrusion Detection System - IDS), bilgisayarların ve bilgisayar ağlarının faaliyetlerini izlemek, kaydetmek ve olası saldırıları tespit etmek amaçlı olarak tasarlanan sistemlerdir. İki tip saldırı tespit sistemi vardır:

1. **Ağ Tabanlı (Network Based):** Bir bilgisayar ağının tamamını ya da belli bir kısmını izlerler. Ağ üzerinde herhangi bir noktadan çalıştırılabilirler.
2. **Konak Tabanlı (Host Based):** Belli bir bilgisayarı izlerler. Bu tür sistemler, izlenecek olan bilgisayar üzerinde çalışırlar. İzlenen bilgisayarı kullanan kullanıcıların yapacakları hatalardan dolayı oluşacak zararları önlemeye yöneliktirler.

Bu tür hatalar, sistem dosyalarının silinmesi, önemli ayarların değiştirilmesi gibi şekillerde karşımıza çıkabilirler.

İyi bir saldırı tespit sistemi, çok az kullanıcı müdahalesi ile çalışabilmeli, sistem kaynaklarını en az düzeyde kullanmalı, sistemde zaman içinde yapılacak değişikliklere karşı uyum sağlayabilir (adaptive) olmalı, sistemdeki normal davranış ile normal dışı davranışı ayırt edebilmelidir.

Saldırı tespit Sistemleri, temelde bilgi tabanlı ve imza tabanlı olmak üzere iki farklı mantığa göre kurulmaktadır.

Daha önce karşılaşılan saldırı şekilleri ayrıntılı olarak analiz edilerek elde edilen bilgiler, yani *saldırının imzası*, saldırı tespit sisteminin bilgi tabanına kaydedilir. Her tanımlanmış saldırının bir imzası vardır. Saldırı imzaları dışında kalan her faaliyet, normal olarak algılanır. Bu şekilde çalışan bir saldırı tespit sisteminin verimli çalışması için, sürekli saldırı imzalarını güncelleyerek sistemi, yeni saldırı tiplerini de tarayacak şekilde güncel tutmak gerekir.

Bilgi tabanlı saldırı tespitinde ise, sistem kullanıcılarının, normal davranışlarından farklı olarak gösterdikleri davranış şekillerine göre çalışma yapılır. Bu yöntem, tahmine dayalı bir sistemdir ve genellikle “uzman sistemler” ve “bulanık mantık” teknolojilerinden faydalanılır.

Bir saldırı tespit sisteminin, ağ üzerindeki faaliyetleri izlemek için ağ üzerindeki farklı noktalarda alıcı cihazlarını ve yazılımlarını kurmak gerekebilir. Bu cihaz ve yazılımların görevi, sorumlu oldukları ağ bölümü üzerinde gerçekleşen faaliyet bilgilerini, saldırı tespit sistemi merkezine aktarmaktır.

Bir Saldırı tespit Sistemi, bir hata yaptığında bu hata iki şekilde olabilir.

1. **Yanlış pozitif (False Positive):** Saldırı Tespit Sistemi, sistemdeki normal bir davranışı saldırı olarak algılayarak hata yapmıştır.
2. **Yanlış negatif (False Negative):** Bu tür bir hata, yanlış pozitive göre çok daha vahim sonuçlar doğurabilir. Bir yanlış-

negatif hatası, saldırı tespit sisteminin işini yapmadığı ve bir saldırıyı tespit edemediğinin bir ifadesidir.

Saldırı tespiti ve saldırgan davranışlarının ortaya çıkarılmasında son zamanlarda ortaya çıkarılan bir yöntem de *tuzak sistem (honey-pot)* yöntemidir. Bu yöntemde ağ üzerinde kurulan bir bilgisayar, üzerinde çalışan hizmetler ve korunmasız görüntüsü ile saldırganların ilgisini çekerek bu bilgisayara saldırmaya özendirmektedir. Bu bilgisayar, gerçek operasyonel bir sistem görüntüsü vermekte ve aynı zamanda saldırının tüm faaliyetleri kaydedilmektedir. Saldırı sonucu bu sistem devre dışı kalıp çökse dahi, tüm saldırgan davranışları kaydedilmiş olmakta, elde edilen bu veriler yardımıyla yeni saldırı imzaları ve yöntemleri keşfedilebilmektedir.

5.6 Erişim Denetimi

Bilişim güvenliğinde en önemli konularda biri, kaynaklara kimin nasıl eriştiğini kontrol etmek, bu sayede bilgi üzerinde yetkisiz değiştirme ve açığa çıkarma olaylarını engellemektir. Bu amaçla yapılan faaliyetlere genel olarak erişim denetimi (access control) denir. Bir kullanıcı bilgisayarından ağ üzerindeki bir dizine ulaşmak istediğinde ona kullanıcı adı ve parola soran bir ekranla karşılaşması, erişim denetimine örnek olarak verilebilir. Erişim denetimi, yazılım ve donanım tabanlı olarak sağlanabilir.

Erişim denetimi yardımı ile kullanıcı ve sistemlerin, diğer sistemlerle nasıl etkileşimde buldukları belirlenir. Erişim denetimi kontrolleri ile, kaynaklara yetkisiz erişimler engellenir ve yetkili kullanıcıların da yetki derecelerine göre erişimleri sınırlandırılır. Erişim denetiminde karşımıza çıkan iki önemli kavram vardır: Bunlar kullanıcıları ifade eden *özneler* ve kaynakları ifade eden *nesnelere*dir. Erişim, bir özne ile bir nesne arası veri akışı olarak ifade edilir. Özneler, bir nesne içerisindeki bir veriye erişimi talep eden varlıklardır. Nesnelere, bir bilgisayar programı, veritabanında saklanan veriler ya da bir bilgisayar olabilir. Erişim denetimi üç aşamalı olarak gerçekleştirilebilir:

1. Tanımlama (Identification)

2. Kimlik Sınama (Authentication)
3. Yetkilendirme (Authorization)

Bölüm 5.6.1’de Tanımlama, Bölüm 5.6.2’de Kimlik Sınama, Bölüm 5.6.3’de ise Yetkilendirme konusuna değinilmiştir

5.6.1 Tanımlama

Değerli bir kaynağa, yalnızca ona erişmeye hakkı olanlara erişim yetkisi verilmelidir. Bu erişim yetkisinin denetimi sırasında, kullanıcılardan iki tür bilgi istenir.

Birinci bilgi herkesin bildiği kullanıcıya ait ve kullanıcının kimliğini belirten bir bilgidir. Sosyal güvenlik numarası, çalıştığı kurumdaki sicil numarası, kullanıcının adı soyadı, sistemden tanımlanmış kullanıcı adı, kullanıcı kimliğine örnek olarak verilebilir.

İkinci tür bilgi ise, yalnızca kullanıcının bildiği özel bir bilgidir. Bu konu Bölüm 5.6.2’de ele alınmıştır.

5.6.2 Kimlik Sınama

Kimlik sınama, bir kişinin Bölüm 5.6.1’de anlatılan kimliğe sahip kişi olduğunun tespit edilmesidir. Bu ispat bir parola, bir akıllı kartın kullanımı, tek seferlik bir parola, bir sayısal imza bilgisi, biyometrik bir özelliğin belirlenmesi şeklinde karşımıza çıkabilir.

Giriş parolası, en yaygın kullanılan kimlik sınama biçimidir. Kullanım kolaylığının yanında, başkalarının eline geçmesi kolay olduğundan güvenlik boşluğu oluşturmaya aday bir teknolojidir. Bununla beraber parolamızla ilgili uyulacak birkaç basit kural, parolamızın başkalarının eline geçmesini engelleyecektir:

1. **Parola Değiştirme:** Parolaları çok uzun süre kullanmamalı, belli aralıklarla değiştirmeliyiz.
2. **Sisteme Girişi Sınırlama:** Eğer bir kullanıcı kimliği yanlış parolayla defalarca sisteme girmeye çabalyorsa, bu parolamızı tahmin etmeye yönelik bir çalışma olabilir. Sistem, belli bir sayıda yanlış girişten sonra bu kullanıcının

erişim hakkını askıya alarak, kendini ve asıl bu kimliğe sahip olan kullanıcıyı korumuş olur.

3. **Parola Seçimi ve Saklama:** Kesinlikle boş parola kullanılmamalıdır. Parola en az 6 karakter olmalı içinde, harf, rakam, diğer özel karakterler (% , ! , ? , = gibi) grubundan en az birer karakter içermelidir. Parola, bilinen ya da tahmin edilebilecek bir kelimedenden (soyad, evcil hayvan adı, şehir adı gibi) ya da sözlüklerde bulunan sözcüklerden oluşmamalıdır.

Biyometrik tanıma, bir kişinin vücudunda bulunan ve yalnızca ona has özellikler taşıyan bir özelliğin sisteme tanıtılmasıdır. Bu özelliklere el ayası, el geometrisi, retina taraması, iris taraması, parmak izi, ses, yüz şekli, tuşlara basma hızı gibi örnekler verilebilir.

Sisteme verilecek özel bilgi olarak sahip olunan bir akıllı kart ya da jeton (hardware token) da kullanılabilir. Son yıllardaki hızlı gelişimleri ile akıllı kartlar, hem fiziksel hem de mantıksal erişim denetim sistemlerinde yaygın kullanım alanı bulmaktadırlar. Bir akıllı kart, kullanıcıya özel bir takım veriler taşır. Tek bir akıllı kart, çoklu-uygulama desteği sayesinde birden çok uygulamada kullanılabilir, böylece cüzdanımızın bir kart cennetine dönüşmesinden kurtuluruz. Örneğin bir üniversite kampüsü içerisinde, hem kapıdan girerken, hem otopark ücretini öderken, kütüphaneden ödünç kitap alırken, genel kullanımlı bir bilgisayara giriş yaparken, yemekhanede ücret öderken ve daha sayısız birçok uygulamada kullanılabilen akıllı kartlar mevcuttur.

Yukarıda belirtilen kimlik sına yöntemlerinden birden fazlasının birlikte kullanılması, erişim denetim güvenliğini arttıracaktır.

5.6.3 Yetkilendirme

Aslında yetkilendirme ile kimlik sınaması birbirine karıştırılabilir. Yetkilendirme, sisteme kendini kimliği ile tanıtmış ve kimlik sınaması yapılmış (yani belirttiği kimliğe sahip olan kişi olduğunu ispatlamış) kullanıcılara, sistem kaynaklarına erişim izni verilmesidir. Kullanıcı, kimlik sınaması yapıldıktan sonra, ağ üzerindeki bir kaynaktaki bir dosyaya erişmek istediğinde, öncelikle bu kullanıcının bu kaynağa

erişim yetkisi olup olmadığı sınıranır. Eğer yetkisi varsa, kaynağa erişmesine izin verilir. Yani bir kullanıcı, kimlik sınaması yapıldıktan sonra, tüm kaynaklara erişme yetkisine sahip olmaz. Erişim yetkisi, kendisine verilen yetki düzeyi ile sınırlıdır.

5.7 *Anti-Virüs Sistemleri*

Bilgisayar virüsleri, “Kötü amaçlı program kodu” olarak tanımlanabilir. Korumasız bir bilgisayar ve bilinçsiz bir kullanıcı, bir bilgisayara virüs bulaşması için yeterlidir. Çünkü e-posta yoluyla gönderilen, kullanıcılara cazip öneriler sunan (erişkin sitelerine ücretsiz erişim hakkı ya da kılını kıpırdatmadan para kazanma gibi) ve tek yapmaları gerekenin ekteki programı kurmak olduğunu iddia eden e-postalar yoluyla virüsler, gerçek hayattaki virüslerden farksız bir hızla yayılmaktadırlar. Anti-virüs yazılımları, bilinen virüsleri tanıyabilen ve temizleyebilen programlardır. Bir anti-virüs yazılımı yalnızca bildiği tür virüsleri tanıyabilir. Yeni ortaya çıkmış bir virüsü tanıması imkansızdır. Örneğin 1999 yılında ortaya çıkan “Melissa” ve 2000 yılının ortaya çıkan “IloveYou” virüsleri anti-virüs programları kendilerini tanıyana kadar ciddi zararlara ve maddi kayıplara yol açmışlardır.

Bir virüsün kimliğine o *virüsün imzası* da denir. Bir kurum, elindeki anti-virüs yazılımlarını, üreticilerinin yeni yayınladığı virüs imza listeleri ile sürekli güncellemelidir. Yeni virüslere karşı da kullanıcı bilinçlendirmesi yoluyla önlem alınabilir. Kullanıcılar, tanımadıkları kimselerden gelen, cazip öneriler içeren e-postaları açmamalı, gerektiğinde sistem ve güvenlik yöneticilerini vakit kaybetmeden konu hakkında bilgilendirmelidirler. Bunun yanında anti-virüs programları, artık güvenlik duvarları ve e-posta sunucuları ile birlikte çalışabilmektedir. Bu şekilde tedbirlerin bütünleşik çalışması sonucu, virüs bulaşma riski en aza indirilmeye çalışılmaktadır.

Bu bölümde ele alınan teknolojilerin, birbirleri ile etkileşimli çalışacak şekilde kullanılması sonucu, kurumun daha etkin korunması gerçekleştirilebilir. Saldırmanın karşısına her bir engeli ya da tedbiri aştığında çıkarılacak olan yeni bir tedbir, sistemin saldırınlara karşı caydırıcılığını arttıracak ve sistemin verdiği güvenlik hizmetlerini tamamlayıcı olacaktır.

6 Eğitim

Bir kurumda bilişim güvenliğinin yerine getirilmesi amacıyla, politikalar, prosedürler oluşturulabilir. Bu prosedürleri yerine getirebilmek için yüksek miktarlarda paralar harcanarak tedbirler konulabilir. Tüm bunlarla birlikte, harcanan bu kadar paranın ve hazırlıkların anlamlı olabilmesi için, sistem içerisinde yer alacak olan kullanıcıların eğitilmesi ve kurulan güvenlik sistemi ile ilgili bilinçlendirilmesi gerekir. Eğitim programının amacı, kurumdaki her bireyin, güvenlik programının bir bütün olarak kurum için ve her bir birey için önemini kavraması olmalıdır.

Eğitimler, kurum içinde en azından üç farklı grup için tasarlanmalıdır: Yöneticiler, orta kademe yöneticiler ve teknik grup.

Yönetici eğitimleri, mümkün olduğu kadar kısa tutulmalıdır. İçerik olarak, kurumsal kaynaklardan, bunların değerinden, korunması ve saldırılara karşı alınan tedbirler için yapılan harcamadan bahsedilmelidir.

Orta kademe yöneticilere verilecek eğitimlerde, üst düzey yöneticilere verileden farklı bir eğitim içeriği hazırlanmalıdır. Her orta kademe yöneticinin sorumlu olduğu bölümün, kurumsal güvenlik açısından önemine yer verilmeli, kurumsal güvenlik programının sürdürülmesi ve başarı kazanması için kendi sorumluluklarında çalışan personelin güvenli bir çalışma ortamında çalışması amacına nasıl katkıda bulunabilecekleri aktarılabilir.

Teknik bölümlerde çalışan insanlar için ise, güvenliğin onların günlük faaliyetlerini nasıl etkileyeceğine yönelik bir eğitim verilmelidir. Diğer gruplara göre, teknik gruba, üzerinde çalıştıkları sistemlerin nasıl etkileneceği, olası güvenlik ihlallerinin neler olabileceği bilgilerini içeren daha ayrıntılı bir eğitim verilmelidir.

Her üç grubun üyeleri de bir güvenlik ihlali ile karşılaşmaları durumunda, ne yapacakları, kime bilgi verecekleri konusunda bilgilendirilmelidirler. Hiçbir çalışan, bir saldırı ile karşılaştığında bununla kendisi mücadele etmeye ya da saldırıya karşı koymaya uğraşmamalıdır.

Kurulan güvenlik sisteminin ortadan kalkması durumunda kullanıcıların nasıl etkilenecekleri, sistemin yararı konusunda kullanıcıları bilinçlendirmek açısından uygun bir yöntem olacaktır. Bu tür eğitimlerde, uygun ve uygunsuz davranışlara birçok örnek verilerek, sistemin kullanışı ile ilgili bilgiler, örneklerle desteklenebilir. Bu örnekler arasında, yetkisiz bir personelin kurumun giriş/çıkış kontrollü bir bölgesinde neden bulunduğu sorgulanması, e-postaların beklenen kullanım şekilleri, internetin doğru bir şekilde kullanılması, şirkete ait bilgi ve belgelerin kullanım şekilleri gibi konular olabilir.

Eğitimlerin sonunda, kullanıcılara, güvenlik konusunda aldığı eğitimde gördüğü konular hakkında bilgi sahibi olduğuna ve kurumun güvenliğini ihlal yönünde bir faaliyette bulunmayacağını taahhüt ettiğine dair bir belge imzalatılabilir.

7 Bilişim Güvenliği Standartları

Kurumsal ölçekte bilişim güvenliğinin sağlanması, teknik bir problem olmanın yanısıra, yönetsel bir problemdir. Bilişim güvenliğini sağlamaya yönelik tedbirler, teknolojiler, bunların kurum içinde kullanımı, işletilecek süreçler ve bunların sahipleri gibi pek çok konuda kalıcı ve etkin kararların verilmesi, bu karar ve bilgilerin belgelerle desteklenmesi ve konunun bir yaşam döngüsü bakışıyla canlı tutulması gereklidir. Bu amaçla çeşitli standartların oluşturulması ve uygulanması bir yöntem olarak benimsenmiştir.

BS 7799, güvenlik politikası geliştirme ve güvenlik denetlemesi yapma konularını kapsayan uluslararası bir standarttır. Bu Standart, 10 alt bölümden oluşur. Her bölümde, o bölümde anlatılan konunun, kurumsal güvenlik politikasına nasıl dahil edileceği ve bu faaliyetlerin nasıl denetleneceği ile ilgili bilgiler vardır.

ISO, BS 7799'u baz alarak ISO 17799 standardını hazırlamıştır.

Aşağıdaki listede, standardın her bölümünün kısa birer tanıtımı yer almaktadır:

İş Sürekliliğinin Planlanması: Kritik iş kaynakları tanımlanır ve bu kaynaklara zarar vermeye ve onların sürekliliğini etkilemeye yönelik olan faaliyetlerle mücadele için tedbirler alınır. Burada bahsedilen zarar, küçük ya da büyük bir zarar olabilir.

Sistem Erişim Denetimi: Erişim denetimine ihtiyacı olan kaynaklar belirlenir. Yetkisiz gerçekleşen faaliyetler tespit edilmeli ve uygun bir şekilde kotarılmalıdır.

Sistem Geliştirme ve Sürdürme: Bilginin gizliliği, bütünlüğü ve kimlik sınaması korunmalıdır. Tüm bilişim faaliyetleri güvenli bir şekilde gerçekleştirilebilmelidir. Uygulama yazılımların ve bunlara ilişkin verinin güvenliği de göz önünde bulundurulmalıdır.

Fiziksel Güvenlik ve Çevre Güvenliği: Kuruma ait bina ve benzeri yerlere giriş çıkışlar kontrol altında tutulmalıdır. Bu sayede verilerin, bilgisayar ve bilgisayar ağlarına ilişkin cihazların çalınmasını ve zarar görmesi engellenir.

Uygunluk: Yasal olarak yapılmıř düzenlemelere, kurumsal olarak ortaya konulan politika ve kurallara uygunluk saęlanmalıdır.

Kurum alıřanlarının Gvenlięi: Kullanıcılar, potansiyel tehditler ve kurumsal gvenlik politikasını desteklemek zere nasıl davranılacağı hakkında bilgi sahibi olmalıdırlar.

Gvenlik Organizasyonu: Kurum iinde bilgi gvenlięinin ynetimi yapılmalıdır. Bilgi-iřlem hizmetleri, bařka bir firma yardımıyla dıř kaynaktan alınıyor olsa bile, kuruma zel bilgiler, yine kurum iersinde korunmalıdır.

Bilgisayar ve Aę Ynetimi: Bilgi iřlem ve iletiřim kaynakları korunmalı ve bu kaynakların btnlę ve sreklilięi saęlanmalıdır.

Kaynak Sınıflandırması ve Kontrol: Bilgi kaynakları iin uygun sınıflandırma yapılmalı ve her sınıflandırma dzeyi iin gerekli koruyucular devreye sokulmalıdır.

Gvenlik Politikası: Kurumsal gvenlik programının temeli olarak bir gvenlik politikası oluřturulmalıdır.

8 Oracle Veritabanı Güvenliđi

Veri, bir kurumun belki de en deđerli varlıđıdır. Bugün herhangi bir sebeple tamamen kullanılmaz hale gelen bir demirbaşı yenilemek mümkünken, yitirilmiş bir verinin kurum için kimi zaman telafisi mümkün olmayabiliyor. Dolayısıyla, kurumlara ait verinin güvenliđli ortamlarda saklanması; sadece yetkili kullanıcılara ve bu kullanıcıların yetkileri dahilinde sunulması büyük önem arz etmektedir.

Veri güvenliđi, aslında bilgi işlem kadar eski bir kavramdır. Ancak özellikle internet/intranet kullanımının yaygınlaşması, pek çok kurum yada kuruluşun internet üzerinde e-iş modelini benimsemesi dođal olarak veri güvenliđine de yeni bir boyut getirmiş durumda. E-iş modelinin bilgi işleme yansımasıysa, kritik verinin kurum dışı kullanıcılara (müşteriler, iş ortakları, tedarikçiler, vs.) açılması sonucu kullanıcı sayısı ve çeşitliliđinde görülen artış, artan veri trafiđi ve platformu oluşturan yapı taşlarındaki farklılıklar (veri tabanı sunucuları, web/uygulama sunucuları, ađ yapısı, son kullanıcı ortamları, vb.) olarak karşımıza çıkıyor. Bunlarsa geleneksel veri güvenliđi mekanizmalarının zaman zaman yetersiz kalmalarına yol açabilmektedir.

E-iş modeli ve internet mimarisi aşıđıdaki kriterleri kurumsal güvenlik mekanizmaları için önem arz eder hale getiriyor:

- ❑ Kullanıcıların kimlik belirleme işlemi, kullanıcının nereden bağlantı kurduđuna bađlı olmaksızın etkin bir şekilde yapılabilmesi.
- ❑ Veriye erişim en az kullanıcı bazında kontrolü sağlayacak şekilde detaylandırılabilmesi.
- ❑ İletişim sırasında veri, ađ üzerinde yetkisiz kişiler tarafından dinlenebilme olasılıđına karşı, korunabilmesi.
- ❑ Güvenlik sistemi kolay kurulabilir ve yönetilebilir olmalı.

Oracle Veri Tabanı Yönetim Sistemi (VTYS) yukarıda sayılan kriterleri sağlamak adına kullanıcılarına pek çok özellik sunmaktadır:

8.1 Kimlik Belirleme ve Yetkilendirme Metotları

Sistem güvenliğinin temel kilometre taşı, kullanıcıların kimliklerinin doğru belirlenmesi ve yetkilendirme işlemidir. Eğer sistemdeki bir kullanıcının kimliği belirlenemiyorsa kişilerin yaptıklarından sorumlu olması mümkün olmayacağından, kaos kaçınılmaz son olacaktır.

Oracle9i, muhtelif kimlik belirleme teknolojilerini desteklemektedir:

Birinci yöntem kullanıcı kimliklerinin VTYS tarafından belirlenmesidir. Oracle VTYS'de tüm kullanıcıların kullanıcı adları ve şifreleri vardır. İşletim sisteminde tanımlı olan bir kullanıcı VTYS'ye bağlanabilmek için kendi kullanıcı adını ve şifresini veri tabanına sunmak durumundadır. Oracle VTYS'nin şifre yönetim mekanizması, şifre güvenliğini sağlamak için aşağıdaki işlevselliğe sahiptir:

- ❑ Şifrelere minimum uzunluk kısıtlaması konabilir.
- ❑ Şifrelerin tahminini güçleştirmek adına kullanıcı şifrelerinde alfabetik karakterlerin yanı sıra sayı ve sembol kullanımı da zorunlu hale getirilebilir.
- ❑ Belirli sayıda hatalı giriş denemesinden sonra bir kullanıcının VTYS hesabı geçici olarak kullanıma kapatılabilir.
- ❑ Kullanıcının soyadı, kurum adı gibi kolay tahmin edilebilecek şifrelerin kullanılması engellenebilir.
- ❑ Şifreler belirli bir kullanım süresinin ardından sistem tarafından geçersiz hale getirilebilir.
- ❑ Kullanıcıların şifre geçmişi tutularak, geçmişteki bir şifrenin bir süre için (yada sonsuza dek) bir daha kullanılması engellenebilir.
- ❑ Şifre uygulama kuralları, kurum, kullanıcı grupları yada tek tek kullanıcılar bazında ayarlanabilmektedir.

Oracle VTYS ayrıca, ağ kimlik belirleme servisleri, akıllı kart, biyometrik kimlik belirleme gibi muhtelif teknolojileri de desteklemektedir. Bu yöntemler şifrelerden daha güçlü güvenlik mekanizmalarıdır. Örneğin akıllı kart kimlik belirlemede iki faktörden

yararlanır. Bunlar kullanıcıya ait bir nesne (kart) ile sadece kullanıcının bildiği bir bilgidir (kişisel numara - PIN). Yine, Oracle VTYS tarafından sunulan Kerberos, RADIUS, vb. destekli güvenlik mekanizmaları benzer şekilde sistem güvenliğini artırıcı yapı taşları olarak karşımıza çıkmaktadırlar.

Oracle VTYS, dağıtık veri tabanı ortamlarında kullanıcıların tek bir noktadan sisteme girişlerini (single sign-on) desteklemektedir. Secure Sockets Layer (SSL) üzerinden X.509 (versiyon 3) sertifikalarının kullanımı yoluyla sağlanan bu fonksiyon ile kurum içindeki kullanıcıların kimlikleri şüpheye yer vermeyecek şekilde belirlenebilmektedir. Kullanılan SSL teknolojisi ayrıca veri güvenliğinin ve tutarlılığının da garantilenmesini sağlamaktadır. Oracle VTYS'deki LDAP (Lightweight Directory Access Protocol) desteği sayesinde, kurum içindeki farklı veri kaynaklarına erişme hakkına sahip kullanıcıların yetkileri tek bir noktadan belirlenebilmekte ve yönetilebilmektedir. Böylelikle, dağıtık yapıdaki kullanıcıların yönetimi kolaylaştırılmaktadır.

İnternet ortamında sıklıkla gözlemlenen bir problem de uygulama sunucusu üzerinde çalışan web tabanlı uygulamaların veri tabanı ile yüksek önceliklere sahip tek bir VTYS kullanıcısı üzerinden bağlantı kurmasıdır. Böyle bir ortamda gerçek web kullanıcılarının tanımı uygulama sunucusunda yapılmak durumundadır. Bu yaklaşım ise, verinin saklandığı ve güvenlik mekanizmalarının belki de kullanıcı bazında düzenlenmesini gerektiren veri tabanı ortamında kullanıcı bilgisinin kaybolmasına neden olabilmekte, yada sistem denetiminin yapıldığı kayıtlara (AUDIT) bu bilgiler yansıtılmamaktadır.

Oracle VTYS, internet/intranet ortamlarında son kullanıcı bilgisinin de saklanabilmesi ve denetimlerin kolaylıkla ve yüksek detayda yapılabilmesini sağlamak adına klasik veri tabanı bağlantı mekanizmasına bir yenilik getirmektedir. Bu yöntemle tek bir veri tabanı bağlantısı kullanılarak VTYS üzerinde farklı kullanıcı oturumları yaratmak mümkün hale gelmiştir. İnternet/intranet ortamındaki son kullanıcı web sunucusundaki bir uygulamayı çalıştırdığında, web sunucusu VTYS'ye çalıştırılan uygulama için bir "uygulama bağlantısı" kurmakta ve bu bağlantıyı kullanarak,

kendisine bağlanan "son kullanıcı adına" VTYS'de bir "oturum" yaratmaktadır. Bir başka son kullanıcı aynı uygulamayı çalıştırdığında ise, VTYS'de yeni kullanıcı adına bir oturum yaratılırken yeni bir bağlantıya gerek kalmadan daha önce yapılmış olan "uygulama bağlantısı" kullanılmaktadır. Bu mekanizma ile gerek "uygulama bağlantısı" gerekse "adına oturum yaratılmış olan son kullanıcı" bilgileri denetlenebilmektedir. Gerek uygulama bağlantılarının gerekse son kullanıcı oturumlarının denetim kayıtlarının tutulabilmesi, internet/intranet ortamlarının uçtan uca güvenliğinin sağlanmasında yeni bir çığır açmaktadır.

8.2 Kayıt Bazında Güvenlik

Kurum içindeki ve dışındaki kullanıcılara kritik sistem verilerine erişim hakkının verilmesi, iş akışlarını hızlandırmak, daha iyi servis vermek gibi avantajlara sahip olmakla birlikte, güvenlik açısından dikkat edilmesi gereken bir açık kapı olabilir. Kurumlar veriyi yetkisiz kişilerden gizlerken aynı zamanda veriyi, çoğu zaman kullanıcı bazında ayırabilmek durumundadırlar. Oracle 9i, Sanal Kişisel Veri Tabanı özelliği (Virtual Private Database) ile, güvenlik kavramına yeni bir standart getirmektedir: kullanıcıların kritik verilere direk erişimini sağlayan, sunucu merkezli kayıt bazında güvenlik mekanizması.

Sanal Kişisel Veri Tabanı özelliği, VTYS'deki kayıtların tutulduğu tablolara erişimin kullanıcı bazında ayarlanabilmesini sağlamaktadır. Kullanıcılar veri tabanına ne şekilde erişirlerse erişsinler bir tabloda sadece kendilerinin görmelerine izin verilmiş olan kayıtlara ulaşabilmektedirler. Bu filtreleme işlemi VTYS Yöneticisi tarafından veri tabanı düzeyinde tanımlanmaktadır. Böylelikle daha önce olduğu gibi güvenliğin veriye ulaşan tüm uygulamalarda ayrı ayrı kodlanması gereği ortadan kalkmaktadır. Karmaşık ve hataya açık olan bu eski yöntemlere gereksinim 'kayıt bazında güvenlik' yaklaşımıyla ortadan kalkmıştır. Ayrıca uygulamayı kullanmak yerine bir başka yöntemle, örneğin bir raporlama aracıyla, veri tabanına ulaşan kullanıcının bu güvenlik mekanizmasını aşması engellenmiş olmaktadır.

Sanal Kişisel Veri Tabanı özelliği kapsamında, tablolara eklenen filtreler dinamik olarak kullanıcı bazında ayarlanabilmekte, ayrıca aynı kullanıcının, sisteme bağlandığı gün, saat, yada son kullanıcı terminaline bağlı olarak farklı kayıtlara erişmesinin sağlanması da mümkün olmaktadır. Böylelikle sözgelimi, kullanıcının hafta içi iş saatlerinde ulaşabildiği veri ile hafta sonu evinden sisteme bağlandığında ulaşabileceği veri farklı olabilmektedir.

8.3 Verilerin Şifrelenmesi

Bugün, klasik bir VTYS'ye bakıldığında veri tabanının yöneticisi durumundaki kullanıcının yetkilerinin, o veri tabanındaki tüm kullanıcılara ait nesne ve verilere sınırsız erişim hakkı sağladığı görülmektedir. Kurumlar, veri tabanlarında tutulan kritik verinin, veri tabanı yöneticisi de dahil hiçbir yetkisiz kullanıcı tarafından görülememesini arzu edebilmektedirler.

Oracle9i, bu amaca yönelik olarak veri tabanındaki verilerin şifrelenebilmesini sağlayabilmektedir. Belli bir anahtar değere bağlı olarak VTYS'deki kayıtların tamamı yada bir kısmı şifrelenerek saklanılabilmekte, çevrim içi yada çevrim dışı olarak tutulan bu kayıtlar ancak şifreleme sırasında kullanılan anahtar tekrar kullanıldığında açılabilir. Dolayısı ile bir kullanıcıya ait kritik veriler (kredi kartı numarası, güvenli sisteme geçiş şifresi, vb.), VTYS yöneticisi dahil tüm kullanıcılardan gizlenebilmektedir.

8.4 Kullanıcı Aktivitesinin İzlenmesi

Oracle VTYS, güvenlikle ilgili izleme amacıyla 'integrated security auditing' adı verilen bir yeteneğe sahiptir. Bu yetenek ile, basit bir AUDIT (DENETLE) komutu, veri erişimlerini, güncellemeleri ve işlem başlama/işlem kapatma işlemlerini her bir oturum, nesne ve kullanıcı için denetlemektedir. Kullanıcı, tarih, zaman, nesne ve işlem, bir veri tabanı tablosuna veya dış denetleme çizelgesine kaydedilmektedir. Oracle VTYS'de, her bir kullanıcı için sistem haklarının denetlenebilmesi mümkündür. Böylelikle, sistem yöneticisi VTYS'de süregelen şüpheli faaliyetleri izleyebilmektedir. Aşağıdaki durumlarda denetlemeler yapılabilir :

Default olarak denetlenen durumlar;

- Veritabanının başlatılması
- Veritabanının kapatılması
- Administrator yetkisi ile veritabanına bağlantılar

İstek üzerine denetlenen durumlar;

- Cümle (Statement) bazında denetleme

Belirli bir nesne türünü ilgilendiren herhangi bir VTYS komutu çalıştırıldığında denetleme mekanizması devreye girer.

- Yetki (Privilege) bazında denetleme

Belirli bir VTYS yetkisini kullanmayı gerektiren bir komut çalıştırıldığında denetleme yapılmasını sağlar.

- Nesne (Object) bazında denetleme

Belirli bir kullanıcı nesnesini ilgilendiren bir komut çalıştırıldığında denetleme yapılması amacıyla kullanılır.

Bu denetlemeler başarılı ya da başarısız (WHENEVER SUCCESSFUL / WHENEVER NOT SUCCESSFUL) durumlar için de yapılabilmektedir. Yani bir kullanıcı, yetkisi dışında bir işlem yapmaya çalışırsa, bunun da denetlenmesi mümkün olmaktadır.

Yukarıda anlatılanlara ek olarak, Oracle VTYS, ince ayarlanmış denetleme özelliğini de (Fine-Grained Auditing) sunmaktadır. Fine-Grained Auditing ile, bir kullanıcı tablosuna yapılan tüm erişimlerin denetlenmesi yerine, ancak tablodaki güvenlik düzeyi yüksek içeriğe erişilmesi durumunda denetleme yapılabilmektedir. Sözelimi günlük işlem hacmi 100 milyar TL'den fazla olan kayıtlar sorgulandığında, ya da kayıtların kredi kartı kolonları listelendiğinde VTYS otomatik olarak denetleme yapabilmektedir.

8.5 İletişim Güvenliği

Bilindiği gibi açık ağlar doğaları gereği güvenli değildirler. Çünkü, hat üzerinde akan veri paketleri, dost yada düşman herkes tarafından okunabilmektedir. Bu sebeple kritik verinin sunucudan son

kullanıcıya, son kullanıcıdan sunucuya ve/veya sunucudan bir başka sunucuya aktarılması sırasında yabancı kişiler tarafından görülmesinin veya değiştirilmesinin engellenmesi, yani şifrelenebilmesi büyük önem taşımaktadır.

E-iş modelini benimseyen bir kurumun veri akışına bakılırsa; genelde, bir veri kaynağında tutulan veri, bu veri kaynağına bağlı bir uygulama sunucusu üzerinde çalışan bir uygulama aracılığıyla son kullanıcı durumundaki kişilerin kişisel bilgisayarlarına taşınmakta, yine bu kişiler tarafından üretilen bilgi ise aynı hat üzerinden veri kaynağına gönderilmektedir. Böyle bir mimaride veri kaynağı ile uygulama sunucusu arasındaki iletişim hattı ve uygulama sunucusu ile son kullanıcı arasındaki hat dışarıdan dinlenebilme tehlikesine açıktır. Oracle9i ve Oracle9i Application Server ürünleri her iki iletişim hattının da SSL ile şifrelenebilmesini sağlamakta, ayrıca gerek son kullanıcı bilgisayarıyla uygulama sunucusu gerekse uygulama sunucusu ile veri tabanı arasındaki hatlara güvenlik duvarlarının (firewall) yerleştirilebilmesini desteklemektedir.

Sonuç olarak, internet/intranet mimarisi kurumlara, iş akışlarını elektronik ortama taşıyarak kurumsal proseslerini hızlandırma, son kullanıcılara daha iyi hizmet verme, artan veri akışı sonucu oluşan "bilgiyi" kurumsal karar alma sürecinin daha sağlıklı hale gelmesinde kullanılabilecek gibi pek çok avantaj sunmaktadır. Ancak, bu şekilde biriken verinin korunması, sadece yetkili kişilere, yetkileri dahilinde sunulmasının garanti edilmesi, veri altyapısının gerek iç gerekse dış tehditlere karşı güvenlik altına alınması ise bu mimarinin kurumlar için getirdiği, üzerinde çok ciddi düşünülmesini gerektiren yeni zorlukları. Oracle, gerek veri tabanında gerekse internet platformunu oluşturan diğer ürün gruplarında kurumsal güvenliğe son derece önem vermektedir. Bu yüzdendir ki, Oracle VTYS ürün ailesi bağımsız kuruluşlar tarafından 15 farklı güvenlik sertifikası ile ödüllendirilmiştir. Bu yazıda anlatılan güvenlik mekanizmaları (iletim hatlarının şifrelenebilmesi, gelişmiş kimlik belirleme mekanizmaları, son derece detaylı olarak ayarlanabilen veriye erişim kısıtlamaları, güvenlik duvarı desteği, vb.) kurumların veri güvenliği ihtiyaçlarını detaylı, esnek ve güçlü bir şekilde karşılamak üzere geliştirilmiş Oracle güvenlik teknolojisinin ana hatlarını

oluřturmaktadır. Gemiřte olduĐu gibi gnmzde de Oracle, kurumların gvenlik ihtiyalarını karřılamak adına teknolojinin en geliřmiř rnlerini sunan alıřmalarını durmaksızın srdrmektedir.

9 Özet ve Sonuç

Bilişim sistemlerine bağımlılığımız gün geçtikçe arttığından, bu sistemlerin ve bunlar üzerinde işlenen, üretilen, saklanan ve iletilen bilginin güvenliğinin önemi de bağımlılığa paralel olarak artmaktadır. Bilişim sistemlerinin ve bu sistemler tarafından işlenen bilgilerin güvenliğinin sağlanması ancak tüm kurum çalışanlarının kolektif çabası ile mümkün olabilir.

Temel güvenlik prensipleri olan gizlilik, veri bütünlüğü ve süreklilik kavramlarının anlaşılması ve kurum için hedef olarak konulması gerekir. Bu hedefe ulaşmak için, yönetsel önlemler, teknolojik uygulamalar ve eğitim süreçleri tanımlanmalı ve bu süreçler, uygulamadan alınacak geri besleme ile sürekli olarak iyileştirilmelidirler. Üst yönetim, kurumun bilişim güvenliğini sağlamada yönetsel katkılar sağlamalıdır. Kurumu tehdit eden riskler ve bunların kabul edilebilir bir düzeyin altına indirilmesi için gerekli mekanizmalar belirlenmelidir. Kurumun yazılı güvenlik politikası oluşturulup, buna bağlı olarak uygulamaya dönük ve daha ayrıntılı yönerge ve prosedürler yazılmalıdır. Bu yazılan dokümanlardaki uygulamalar, yapılacak iç ve dış güvenlik denetimleri ile sürekli izlenmeli, uygulamadaki ya da dokümanlardaki hatalar bu şekilde tespit edilmeli ve düzeltilmelidir.

Risk ve tehditlere karşı mücadelede kullanılacak tedbirler ve teknolojiler konusunda bilgi sahibi olunmalıdır. Bu teknolojilerden seçilenlerin maliyet-etkin bir şekilde kurumun bilişim altyapısına dahil edilmesi sağlanmalıdır.

Kullanıcı eğitimleri, en az uygulanan teknolojiler ve yönetsel önlemler kadar önemsenmelidir. Kurumdaki farklı kullanıcı gruplarına, onların bilişim güvenliğine hedeflenen katkıları doğrultusunda farklı içerikte eğitimler hazırlanmalı ve verilmelidir. Doğal olarak, üst yönetim, orta kademe yöneticiler ve teknik personele verilecek eğitimler farklı olacaktır.

Alınan yönetsel önlemler, uygulanan teknolojiler ve verilen güvenlik eğitimlerinin üçü birlikte ele alınarak değerlendirilmeli ve bu üç

sürecin birlikte çalışmalarından ortaya çıkacak sinerjiden faydalanılmalıdır. Bu üç alan birbirileri ile ayrılmaz ve sıkı bağlara sahiptir. Birlikte çalışmalarından oluşacak sinerji, kuruma bilişim güvenliği yönünden tehdit oluşturacak tüm etkenlere karşı güçlü bir kalkan görevini üstlenecektir.

Uluslararası standartlar, uzun deneyimlerin ve çalışmaların ürünü olarak ortaya çıkarılmış dokümanlardır. BS 7799 / ISO 17799, güvenlik politikası geliştirme ve güvenlik denetleme yapma konularını kapsayan uluslararası standartlardır. Kurumun bilişim altyapısı kurulurken gerektiğinde bu standart dokümanlarına başvurulabilir.

Kurumsal güvenlik politikasının belirlenmesi ve bu doğrultuda yönetsel, operasyonel ve teknik denetimlerin yerleştirilmesi ve tüm kurum çalışanların düzenli ve kesintisiz eğitiminin ve bilinçlendirilmesinin sağlanması, bilişim güvenliğinin sağlanması için en uygun yaklaşım olacaktır. Unutulmaması gereken bilişim güvenliğinin bir son durum değil, hiç bitmeyen bir süreç olduğudur. Bilişim güvenliğinin sağlanmasına yönelik çabalar bitmeyen ve devamlı iyileştirmeler ile güncel tutulması gereken bir faaliyet olmalıdır.

Kurumsal bilişim güvenliği çok bileşenli, önemli ve yönetimi zor bir süreçtir. Bu nedenle ve olası saldırıların sonuçlarının yaratacağı tahribat nedenleri ile yöneticiler tarafından özellikle önem verilmesi gereken bir alandır.

10 Kaynaklar

Aşağıdaki kaynaklar, bilişim güvenliği alanında başvurulabilecek çok çeşitli kaynakların bir kısmını oluşturmaktadır. Önerimiz özellikle elektronik kaynakların etkin kullanımını sağlayacak yöntemlere öncelik verilmesidir.

Pro-G web sitesi (www.pro-g.com.tr) üzerinde "Araştırma" başlığı altında Pro-G Kütüphanesi için bir açık-metin arama arayüzü sunulmaktadır. Üç bin kadar elektronik makale ve kitabın yer aldığı kütüphane üzerinde anahtar sözcükler ile arama yapmak ve seçilen kaynaklar için çevrim içi istekte bulunmak bu arayüz sayesinde mümkün olmaktadır.

- ❑ NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook", October 1995
- ❑ Avolio, F.M., "A Multidimensional Approach to Internet Security." ACM Networker Magazine, 2 (2), pp. 15-22, Apr/May 1998.
- ❑ Lau, O., "The Ten Commandments of Security". Computers & Security 17 (2), pp. 119-123, 1998.
- ❑ NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems", December 1998.
- ❑ Baskerville, R., "Information Systems Security Design Methods: Implications for Information Systems Development", ACM Computing Surveys, 25 (4), pp. 375-414, December 1993.
- ❑ Özgüt, A., "Bilişim Güvenliğinden Ne Anlıyoruz?", TBD BIMY-10 Bildiriler Kitabı, Nisan 2003.
- ❑ Dayıoğlu, B., "Ağ ve İşletim Sistemi Güvenliği", TBD BIMY-9 Bildiriler Kitabı, Nisan 2002.

- ❑ Pro-G Web Sitesi, <http://www.pro-g.com.tr>
- ❑ Oracle Web Sitesi, <http://www.oracle.com>
- ❑ CERT/CC Web Sitesi, <http://www.cert.org>
- ❑ SANS Enstitüsü Web Sitesi, <http://www.sans.org>
- ❑ SecurityFocus Web Sitesi, <http://www.securityfocus.com>
- ❑ Dikey8 Web Sitesi, <http://www.dikey8.com>
- ❑ Olympos Web Sitesi, <http://www.olympos.org>

11 Güvenlik Terimleri

Aşağıdaki terimler, bilişim güvenliği alanında Türkçe terimler üretme yolunda yürüttüğümüz çalışmanın güncel bir ara sonucudur. Sunulan liste, İngilizce terimlerin harf sırası ile verilmiştir.

Erişim (Access): Bilgiyi işlemek ya da bir sistem tarafından işlenen bilgiyi edinmek üzere bir sistem ile etkileşime ya da etkileşime geçme becerisi ve yöntemi.

Erişim Denetim Listesi (Access Control List): Erişime izinli sistem varlıklarının kimliklerinin listelenmesi yolu ile bir sistem kaynağına erişimi sağlayan mekanizma.

Hesap (Account): Bir bilgisayar ya da ağ üzerinde, hesap adı, parolası ve kullanım kısıtları gibi bilgiler içeren kullanıcı erişim alanı kaydı.

Eylem (Action): Bir kullanıcı ya da süreç tarafından bir sonuca ulaşmak amacıyla atılan adım.

Anormallik (Anomaly): Normalden ya da sıradandan farklılık gösteren ve bu nedenle tatminkar olmayan bir kural ya da işlem.

Anonim (Anonymous): Bilinmeyen ya da gizlenmiş bir isim taşıma durumu.

Asimetrik Şifreleme (Asymmetric Cryptography): İki farklı anahtarın söz konusu olduğu (açık ve gizli anahtar), algoritmanın farklı adımlarında anahtarların değişmeli kullanıldığı modern bir şifreleme dalıdır.

Saldırı (Attack): Yetkisiz biçimde bir takım sonuçlara ulaşmak amacıyla bir saldırgan tarafından gerçekleştirilen bir dizi adım.

Saldırgan (Attacker): Bir amaca ulaşabilmek üzere bir ya da daha fazla saldırıyı deneyen birey.

Yetkilendirilmiş (Authorized): Sahibi ya da yöneticisi tarafından onaylanmış.

Arka Kapı (Back Door): Sistem ve sistem kaynaklarına sıradan prosedür dışında bir yöntem ile ulaşılmasını sağlayan, sistem tasarımcıları ya da işletmenleri tarafından bilerek bırakılmış olan ya da kamunun yaygın bilgisi dahilinde olmayan yazılım ya da donanım mekanizması.

Sınır Değer (Boundary Value): Bir sistem ya da bileşen için tanımlanmış en küçük ya da en büyük girdi ya da çıktı değeri.

Atlatma (Bypass): Bir hedefe erişim için alternatif bir yöntem izleyerek bir süreci geçersiz kılma.

Bileşen (Component): Bir bilgisayarı ya da bir ağ oluşturan parçalardan birisi.

Mahremiyet (Confidentiality): Bilgilerin yetkilendirilmemiş kişiler, varlıklar ya da süreçlerce erişilemez olmasını sağlayan nitelik.

Yapılandırma Zafiyeti (Configuration Vulnerability): Sistemin yapılandırmasındaki bir hatadan kaynaklanan zafiyet. Sistem hesaplarının öntanımlı parolaları ile

bırakılması, yeni dosyalara "herkes-yazabilir" izni ile açılması ya da zafiyeti olan hizmetlerin aktif hale getirilmesi yapılandırma zafiyetlerine birer örnektir.

Koordineli Saldırı (Coordinated Attack): Saldırının bütünlük doğasını gizlemek ve daha hızlı ilerlemek adına, paralel oturumlar kullanma ve bir patlatmanın birden çok adıma bölünerek gerçekleştirilmesi.

Hizmet Kesintisi (Denial Of Service) : Sistem kaynaklarına yetkilendirilmiş erişimlerin engellenmesi ya da sistem işleyişinin yavaşlatılması.

Tasarım Zafiyeti (Design Vulnerability): Mükemmel bir uygulamanın bile önleyemediği, bir donanımın ya da yazılımın tasarımına ya da belirtimine ilişkin zafiyet.

Dizin (Directory): Bilgi sağlayan bir veritabanı ya da başka bir sistem.

Bilginin Açığa Vurulması (Disclosure Of Information): Bilginin erişmek için yetkilendirilmemiş herhangi birisine ulaşması.

Dağıtık Araç (Distributed Tool): Birden çok bilgisayar sistemine dağıtılabilen ve daha sonra tüm sistemlerden tek bir hedefe koordineli bir saldırı gerçekleştirmek için kullanılan, saldırganın kimliğinin de gizlenebildiği araç.

Olay (Event): Bir hedefe yönlendirilmiş ve sonuçta hedefin durumunu değiştirmeyi amaçlayan eylem.

Patlatma (Exploit): Sistemdeki bir zafiyetten faydalanarak, bir biçimde, bir amacı gerçekleştirmeye çalışmak.

Sel (Flood): Kapasitesinin sınırını zorlamak amacı ile bir hedefe sık, ardışık erişim.

Gerçekleştirme Zafiyeti (Implementation Vulnerability): Tatminkar bir tasarıma sahip yazılım ya da donanımın uygulanması ya da gerçekleştirimi sırasında yapılan bir hatadan kaynaklanan zafiyet.

Olay (Incident): Saldırganların, saldırıların, amaçların, sitelerin ve zamanlamanın farklılığı nedeniyle diğer saldırılardan ayırt edilebilen bir saldırı grubu.

Bütünlük (Integrity): Yetkilendirilmemiş biçimde ya da kaza ile verilerin değiştirilmediğini, yok edilmediğini ya da kaybedilmediğini gösteren nitelik.

Saldırı (Intrusion): Bir kaynağın bütünlüğünü, gizliliğini ya da bulunurluğunu bozmayı hedefleyen her türlü eylem.

Saldırı Tespiti (Intrusion Detection): Yetkilendirilmemiş biçimde bilgisayar sistemlerini kullanmaya çalışan bireyleri (kullanıcılar ya da otomatik saldırganlar) ya da erişim hakkına sahip olan ancak yetkilerini kötüye kullanmaya çalışan bireyleri tespit etme.

Amaç (Objective): Bir olayın gerekçesi ya da nihai hedefi.

Sızma (Penetration): Bir sistemin güvenlik mekanizmalarının başarı ile atlatılması.

Yoklama (Probe): Karakteristik özelliklerini belirlemek üzere bir hedefe erişim.

Süreç (Process): Programın çalıştırılabilir halini, verilerini, yığıtını, program sayacını, yığıt göstergesini ve diğer yazmaçlarını içeren bütün halinde çalışır durumdaki bir program.

Arta Kalan Risk (Residual Risk): Güvenlik önlemleri uygulandıktan sonra kalan risk bölümü.

Risk (Risk): Belirli bir tehditin sistemin belirli bir zafiyetinden faydalanarak sisteme zarar verme ihtimali.

Risk Analizi (Risk Analysis): Güvenlik risklerinin, bu risklerin ölçüklerinin ve önlem alınması gereken alanların belirlenmesi süreci.

Risk Yönetimi (Risk Management): Sistem kaynaklarını etkileyebilecek belirsiz olayların belirlenmesi, denetlenmesi, yok edilmesi ya da en aza indirgenmesini kapsayan süreç. Risk analizi, fayda-maliyet analizi, seçim, gerçekleştirim, sınama, önlemlerin güvenlik değerlendirmesi ve komple güvenlik gözden geçirmesini içerir.

Tarama (Scan): Hangilerinin belirli karakteristiğe sahip olduğunu görmek üzere bir hedef kümesine sıra ile erişim.

Güvenlik (Security): Art niyetli eylemlerden ve etkilerinden korunmak üzere alınan ve sürdürülen koruyucu önlemlerin sonucunda oluşan durum.

Güvenlik Değerlendirmesi (Security Evaluation): Hassas bilgilerin işlenmesinde kullanılan sistemlerin güvenilirlik düzeyini değerlendirme ve belirleme işlemi.

Şaşırtma (Spoof): Ağ iletişimde kendisini başka bir varlık olarak göstererek saklanma.

Çalma (Steal): Bir kopyasını kaynak yerinde bırakmadan bir hedefin denetimini ele geçirme.

Hedef (Target): Bir bilgisayar, mantıksal ağ varlığı (hesap, süreç ya da veri) ya da fiziksel varlık (bileşen, bilgisayar, ağ ya da ağlar ağı).

Araç Takımı (Toolkit): Betikler, programlar ve bağımsız ajanlardan oluşan ve zafiyetlerden faydalanmak üzere derlenmiş yazılım paketi. Yaygın biçimde görülen rootkit'ler araç takımına bir örnektir.

Truva Atı (Trojan Horse): Kullanışlı ve masum görünen, ancak yetkisiz veri toplama, değiştirme ve yok etmeye izin veren gizli program parçaları taşıyan program.

Yetkilendirilmemiş (Unauthorized): Sahibi ya da yöneticisi tarafından onaylanmamış.

Zafiyet (Vulnerability): Bir sistemde yetkilendirilmemiş eylemlere izin veren zayıflık.

Kurt (Worm): Bağımsız olarak çalışabilen, işler durumdaki kopyalarını ağ üzerindeki başka bilgisayarlara aktarabilen ve zarar verecek biçimde sistem kaynaklarını tüketen bilgisayar programı.

Güvenliđiniz

Geleceđinizdir...

Yođun AR-GE alıřmaları ve akademik arařtırmalar ile elde ettiđimiz birikimimizi yerli biliřim gvenliđi rnleri ve hizmetlerine dnřtrerek geleceđinize ıřık tutuyoruz.



<http://www.pro-g.com.tr>



Pro-G Bilişim Güvenliği ve Araştırma Ltd.

Ürünlerimiz

ARES-Sensor: Ağ temelli saldırı tespit sistemidir. Ağ üzerinden gerçekleştirilen saldırıları gerçek zamanlı olarak kayıt edebilir ve durdurabilir.

ARES-Console: Merkezi alarm konsolu, tüm güvenlik sistemlerinin alarmlarını merkezi olarak kayıt eder ve çok boyutlu incelenmesine imkan sağlar.

ARES-Honeypot: Saldırganları cezbetmeye ve yanıltmaya yönelik bir tuzak sistemdir. Sinsi ve dikkatli saldırganları tespit etmek için kullanılır.

ARES-LogHunter: Heterojen bir ağ ortamında üretilen her türlü log'u merkezi bir biçimde veritabanına depolar, yedekler ve çok boyutlu analizine imkan verir.

ARES-Integrity: Heterojen bir ağ ortamında sunucular üzerindeki kritik dosya ve dizinlerdeki değişiklikleri tespit eder ve alarm üretir.

Ares-Wall: Durum korumalı inceleme ve entegre bant genişliği yönetimi gibi becerilere sahip gelişmiş bir güvenlik duvarı sistemidir.

Profesyonel Hizmetlerimiz

- Güvenlik Denetimleri
- Penetrasyon Testleri
- Stratejik Bilişim Güvenliği Planlaması
- Güvenlik Mimarisi Tasarımı
- Ürün Seçimi ve Kurulumları
- Olay Müdahalesi ve Delil İnceleme
- Güvenlik Yönetimi

Eğitim Hizmetlerimiz

- Bilişim Güvenliği'nin Temelleri
- Güvenlik Duvarları
- Saldırı Tespiti
- Saldırı Teknikleri ve Araçları
- UNIX Güvenliği
- Web Güvenliği
- Linux Sistem Yönetimi
- Ağ Teknolojileri ve TCP/IP