

Türkiye’de En Sık Karşılaşılan Güvenlik Açıkları

Düzenleme Tarihi: 14/04/2005



INFOSECURE

InfoSECURE, 2000 yılından beri Türkiye'de ve yurtdışında denetim ve danışmanlık alanında Bilgi Güvenliği Denetim ve Danışmanlığı hizmetlerini şirket ve kurumlara sunmaktadır. Tek faaliyet alanı bilgi güvenliği denetim ve danışmanlığı olan InfoSECURE, bugüne dek 100'ün üzerinde güvenlik denetimi ve danışmanlığı yapmıştır. Yurtdışına güvenlik denetimi satışını birden fazla kez gerçekleştirmiştir. Halen İran ve İngiltere'deki müşterilerine hizmet vermektedir. InfoSecure deneyimli danışman ekibi ile güvenlik denetim ve danışmanlığında geniş bir yelpazede hizmet sunabilme yetisine sahiptir.

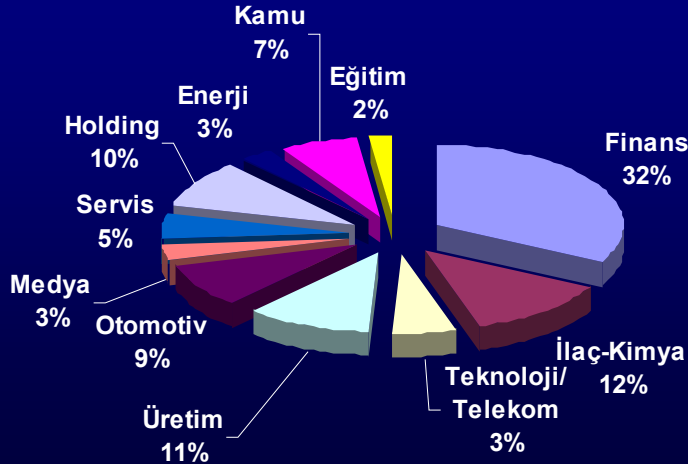
ISO 17799/BS 7799 Danışmanlığı

Güvenlik Danışmanlığı alanındaki hizmetlerimiz arasında yakın dönemde öne çıkan alan ISO 17799/BS7799 Danışmanlığı'dır. Teknolojik güvenliği sağlamak firmalar için ilk koşul olmakla birlikte, kuruluşlar güvenliğin sadece teknoloji değil, ancak insan-süreç- teknoloji üçlüsü ile sağlanabileceği gerçeğini kabul etmektedirler. gerçek anlamda ve kontrollü bilgi güvenliğinden bahsedebilmek için firmaların Bilgi Güvenliği Yönetim Sistemleri'ni (BGYS) oluşturmaları gerektiği son dönemin önemli konu maddesidir. BGYS çalışmasının ilk ve en temel adımı Bilgi Güvenliği Politikaları'nın oluşturulmasıdır. Politikalar aslında, teknoloji yatırımlarının akıllıca yapılması için de önkoşuldur. Politikaların hazırlanmasından başlayan ve yaşayan bir BGYS oluşturulmasına kadar giden süreç firmanın bir sertifika ile (ISO 17799/TSE 17799) çalışmasını belgelendirmesine kadar gider. Firma bu belgeyi alarak bilgi güvenliği kalitesini sürdürmeye de niyet etmiştir. InfoSecure, bir BGYS oluşturmaya niyet eden firmalara danışmanlık hizmeti vermektedir. Burada amacımız kısa dönemli ilişkiler değil, güvenlik politikalarının oluşturulmasından başlayıp sertifikasyona giden süreçte uzun dönemli bir danışmanlık hizmeti vermektir. Bu sadece danışman ekip ve firma birbirini tanımakta, güvenmekte, firmanın iş alanı ve kültürü ile InfoSecure'un bilgi birikimi ve deneyimi en iyi şekilde harmanlanmaktadır. En başarılı ve uzun soluklu sonuçlar bu şekilde elde edilmektedir.

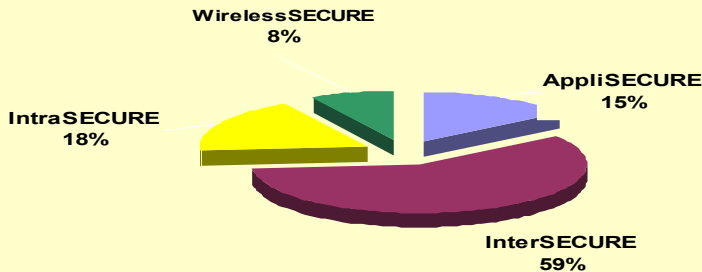
Denetim Hizmetleri

InfoSECURE denetim hizmetlerine, Internet, Intranet, kablosuz ağ ve cihazları, çok çeşitli uygulama ve veritabanları özel denetimler dahildir. Gerektiğinde saldırıya uğrayan sistemlerin "adli analizi (forensic analysis)" için yardımımıza başvurulmaktadır. Denetim hizmetlerinde yoğunluk halen şirket dışından gelebilecek tehditlere yönelik internet üzerinden yapılan denetimlerdir. Önümüzdeki dönemde beklentimiz, internet üzerinden gelecek tehditlere gösterilen hassasiyetin intranet ve kablosuz ağlara da gösterilmesidir. Internet üzerinden gelebilecek saldırılara karşı açıkların denetlenmesi hizmetine başvuran firmaların sayısında da büyük artış beklemekteyiz. Bu konuda önlem alan firma sayısı halen asıl ihtiyaca göre sınırlıdır. Konunun ciddiyetini anlayan firmalar abonelik modelimiz dahilinde düzenli olarak denetleniyorlar. Denetimlerin sıklığı "ayda 1" ile "6 ayda 1" arasında değişmektedir. Bilgilerinin değerini, prestij ve varlık kaybının riskini doğru değerlendiren firmalar "Güvenliğimi sağladım, artık denetime ihtiyacım yok" diye bir yaklaşım olamayacağını ve güvenlik konusunda sürekli tetikte olmaları gerektiğinin bilincindedir.

Denetimlerin Sektörel Dağılımı



Denetim Tipi Dağılımı



En popüler denetimler

InterSECURE: İnternet üzerinden saldırı ve sızma simülasyonu

IntraSECURE: Şirket içinden saldırı ve sızma simülasyonu

AppliSECURE: Uygulama Denetimi

WirelessSECURE: Kablosuz ağ ve cihazlardan saldırı ve sızma simülasyonu

GİRİŞ

InfoSecure Güvenlik Denetim Ekibi kurulduğu günden bu yana 100'den fazla güvenlik denetimi yapmış, birçok şirket ve kurumda güvenlik açıklarının bulunmasını ve giderilmesini sağlamıştır.

Bu çalışmalar sırasında **InfoSecure**'un karşılaştığı yaygın pek çok teknik güvenlik probleminin arasında, aşağıdaki güvenlik açıkları şirketlerimizde en sık rastlanan güvenlik problemleri olarak öne çıkmaktadır.

Türkiye'deki Şirketlerde En Sık Rastlanan Güvenlik Açıkları :

1. Hatalı Kablosuz Ağ Yapılandırması
2. Hatalı Yapılandırılmış Sanal Özel Ağ (VPN) Sunucuları
3. Web Uygulamalarında SQL Sorgularının Değiştirilebilmesi
4. Web Uygulamalarında Başka Siteden Kod Çalıştırma
5. Kolay Tahmin Edilebilir Şifrelere Sahip Kullanıcı Hesapları
6. SNMP Servisi Kullanımı
7. Güncellemeleri Yapılmamış Web Sunucusu
8. İşletim Sistemi ve Uygulamaların Standart Şekilde Kurulması
9. Hatalı Yapılandırılmış Saldırı Tespit Sistemleri
10. Güvenlik Duvarı Tarafından Korunmayan Sistemler

İÇİNDEKİLER

INFOSECURE	2
1. Hatalı Kablosuz Ağ Yapılandırması	6
2. Hatalı Yapılandırılmış Sanal Özel Ağ (VPN) Sunucuları	7
3. Web Uygulamalarında SQL Sorgularının Değiştirilebilmesi	8
4. Web Uygulamalarında Başka Siteden Kod Çalıştırma	9
5. Kolay Tahmin Edilebilir Şifrelere Sahip Kullanıcı Hesapları	10
6. SNMP Servisi Kullanımı	11
7. Güncellemeleri Yapılmamış Web Sunucusu	12
8. İşletim Sistemi ve Uygulamaların Standart Şekilde Kurulması	13
9. Hatalı Yapılandırılmış Saldırı Tespit Sistemleri	14
10. Güvenlik Duvarı Tarafından Korunmayan Sistemler	15
SONUÇ	16

1. Hatalı Kablosuz Ağ Yapılandırması

Açıklama :

Günümüzde kullanımı oldukça artan kablosuz ağlar, birçok kurumun yerel ağının bir parçası olmuştur. Ancak kablosuz ağ erişim noktalarının, istemcilerin ve kablosuz ağ tasarımlarının yapılandırmasında güvenlik gereksinimleri gözönüne alınmamaktadır. İstemcilerin kimlik doğrulamasının yapılmaması, kriptolu erişim kullanılmaması, kablosuz ağların güvenlik duvarı aracılığıyla erişim denetimine tabi tutulmaması ve sinyal kalitesinde kısıtlama olmaması, saldırganların kablosuz ağlara sızmasını kolaylaştırmaktadır. Kablosuz ağlara sızabilen bir saldırgan, kurum yerel ağına girebilir, sunuculara erişim sağlayabilir, tüm ağ erişimlerini izleyebilir veya değiştirebilir.

Çözüm Önerileri :

Kablosuz ağ tasarımı yapılırken, kablosuz ağın Internet gibi güvensiz bir ağ olduğu göz önüne alınmalı, güvenlik duvarının DMZ bölümünden giriş yapılması sağlanmalı, tercihen sanal özel ağ (VPN) sistemleri kullanılmalı, sinyal kalitesinde kısıtlamalara gidilmeli ve istemciler harici doğrulama sistemleri tarafından kimlik kontrolüne tabi tutulmalıdır. Kurum güvenlik politikası dahilinde, gezgin kullanıcıların sistemlerinde kurumda kullanılmamasına rağmen kablosuz ağ kartı bulunması engellenmeli ve istemci kurumda iken ağ kartının devre dışı olması sağlanmalıdır.

Referanslar :

Security Guidelines for Wireless LAN Implementation

<http://www.sans.org/rr/papers/index.php?id=1233>

Corporate Wireless LAN: Know the Risks and Best Practices to Mitigate them

<http://www.sans.org/rr/papers/index.php?id=1350>

Wireless Firewall Gateway White Paper

<http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/index.html>

2. Hatalı Yapılandırılmış Sanal Özel Ağ (VPN) Sunucuları

Acıklama :

Sanal özel ağ (VPN) sunucuları güvensiz ağlar üzerinde güvenli iletişim tünelleri oluşturmak için kullanılmaktadır. Genel kullanım alanları arasında; kurum bölgeleri arası bağlantıları, çözüm ortakları ile iletişim, veya gezgin istemcilerin yerel ağa güvenli bağlanabilmesi sayılabilmektedir. Sıkça karşılaşılan sanal özel ağ güvenlik açıkları arasında, sanal özel ağ sunucularında harici kimlik doğrulama sistemleri kullanılmaması, sunucunun yerel ağda bulunması sonucu yerel ağa doğrudan erişim, istemciler ile Internet arasında iletişim izolasyonu olmaması ve zayıf kriptolama algoritmalarının seçilmesi sayılabilmektedir. Güvenlik açığı barındıran sanal özel ağa sızabilen bir saldırgan, kurum ağına doğrudan erişim sağlayabilmekte ve yerel kullanıcı haklarına sahip olabilmektedir.

Çözüm Önerileri :

Sanal özel ağ sunucuları kendilerine ayrılmış bir DMZ bölümü ve güvenlik duvarı aracılığıyla yerel ağa bağlanmalıdır. Böylece güvenlik duvarına gelen iletişim kriptosuz olacak ve üzerinde erişim denetimi yapılabilecektir. Gezgin kullanıcıların bağlantısında ise sayısal sertifika veya tek seferlik şifre gibi kimlik doğrulama yöntemleri kullanılmalıdır. Kriptolama amaçlı kullanılacak algoritma mutlak suretle günümüzde kolayca kırılmayan algoritmalar (3DES, AES vb.) arasından seçilmelidir. Kullanılacak istemci yazılımları, Internet kullanımı ile sanal özel ağ kullanımı arasında izolasyon yapmalı ve istemcilerin Internet'te farklı kaynaklara erişimini kısıtlamalıdır. Ayrıca uzak erişimlerde sahip olunan yetkiler, yerel ağda sahip olunan yetkilerden çok daha az olacak şekilde yapılandırılmalıdır.

Referanslar :

Virtual Private Networks: A Broken Dream?

<http://www.securityfocus.com/infocus/1461>

Introduction to Encryption

<http://www.securityfocus.com/infocus/1181>

Intranets and Virtual Private Networks (VPNs)

http://www.iec.org/online/tutorials/int_vpn/index.html

3. Web Uygulamalarında SQL Sorgularının Değiştirilebilmesi

Acıklama :

Web uygulamalarında bazı bilgilerin tutulabilmesi için SQL veritabanları kullanılmaktadır. Uygulama geliştiricileri, bazı durumlarda kullanıcılardan gelen verileri beklenen veri türü ile karşılaştırmayarak SQL sorguları içinde kullanılmaktadırlar. Genel olarak problemler, uygulama geliştiricinin SQL sorgularında anlam ifade edebilecek ‘ ; **UNION** gibi kötü niyetli karakterlere karşı bir önlem almadığı zaman ortaya çıkmaktadır. Bu durum kullanıcıya önceden planlanmamış uygulama düzeyinde erişim sağlayabilir. İçinde SQL sorgulama barındıran bir çok ürün SQL sorguları değiştirilebilmesine (SQL Injection) karşı savunmasızdır. Saldırganlar SQL sorgularını değiştirme tekniklerini web sitelerine ve uygulamalara zarar vermek amaçlı kullanılmaktadırlar. SQL enjeksiyon ile saldırgan tablo yaratabilir, değişiklikler yapabilir, veritabanı üzerinde erişim sağlayabilir veya veritabanı kullanıcısının hakları doğrultusunda sunucuda komut çalıştırabilir.

Çözüm Önerileri :

Uygulamanın tüm bileşenlerinde kullanılan değişkenler için kontroller oluşturulmalı ve değişkene atanması beklenen veri türü ile kullanıcı girdisi karşılaştırılmalıdır. Beklenen girdi türünden farklı karakterler saptanması durumunda, karakterler SQL sorgularında anlam ifade etmeyecek biçimde değiştirilmeli, silinmeli veya kullanıcıya uyarı mesajı döndürülmelidir. Tercihen uygulamanın tamamı için geçerli olacak, değişken türü ve atanabilecek girdi türünü parametre olarak alan ve kontrolleri yaptıktan sonra girdi kabul sonucu üreten sabit bir fonksiyon tercih edilmelidir.

Referanslar :

SPI Dynamics SQL Injection Whitepaper

<http://www.spidynamics.com/whitepapers/WhitepaperSQLInjection.pdf>

SQLSecurity.com

<http://www.sqlsecurity.com/faq-inj.asp>

OWASP

http://www.owasp.org/asac/input_validation/sql.shtml

Advanced SQL Injection In SQL Server Applications

http://www.nextgenss.com/papers/advanced_sql_injection.pdf

4. Web Uygulamalarında Başka Siteden Kod Çalıştırma

Acıklama :

Başka siteden kod çalıştırma (Cross-Site Scripting) açıkları, bir saldırganın hedef web sitesi aracılığıyla site ziyaretçilerinin sisteminde komut çalıştırabilmesine olanak tanımaktadır. Saldırı sonucu olarak site ziyaretçilerinin browser'larında bulunabilecek güvenlik açıklarının kullanılması, JavaScript/ActiveX ve VBScript komutlarının çalıştırılmasını mümkün kılmaktadır. Bu tür komutlar ile kullanıcıya ait site çerezleri alınabilir, kaydedilmiş şifreler çalınabilir veya browser'da bulunabilecek güvenlik açıkları ile kullanıcı sistemi ele geçirilebilir. Ayrıca elektronik ticaret veya bankacılık uygulamaları için sahte giriş ekranları oluşturularak ziyaretçilerin yanıltılması ve sonucunda kullanıcıya ait önemli bilgilerin ele geçirilmesi mümkün olabilir.

Çözüm Önerileri :

Uygulamanın tüm bileşenlerinde kullanılan değişkenler için kontroller oluşturulmalı ve değişkene atanması beklenen veri türü ile kullanıcı girdisi karşılaştırılmalıdır. Beklenen girdi türünden farklı karakterler (örn. `</;()`) saptanması durumunda, karakterler anlam ifade etmeyecek biçimde değiştirilmeli, silinmeli veya kullanıcıya uyarı mesajı döndürülmelidir. Tercihen uygulamanın tamamı için geçerli olacak, değişken türü ve atanabilecek girdi türünü parametre olarak alan ve kontrolleri yaptıktan sonra girdi kabul sonucu üreten sabit bir fonksiyon tercih edilmelidir.

Referanslar :

SPI Dynamics Cross-site Scripting Whitepaper

<http://www.spidynamics.com/whitepapers/SPIcross-sitescripting.pdf>

OWASP Cross-site Scripting Information

<http://www.owasp.org/projects/asac/owasp-iv-css-1.shtml>

5. Kolay Tahmin Edilebilir Şifrelere Sahip Kullanıcı Hesapları

Acıklama :

Ağda bulunan istemci, sistem yöneticisi veya servislere özel kullanıcı hesaplarının kolay tahmin edilebilir şifrelere sahip olması, bir saldırganın kurum ağına yönelik kullanabileceği en basit saldırı yöntemidir. Özellikle yönlendirici yönetim şifreleri veya sunucu servislerine ait kullanıcı hesaplarının şifreleri kolayca tahmin edilebilmektedir. Web temelli uygulamaların yaygınlaşması ile web temelli uygulamalar da şifre seçim hatalarından etkilenmektedir. Bir saldırganın, yönetim hesaplarını veya geçerli bir kullanıcıya ait şifreleri ele geçirmesi durumunda, kurum ağına sınırsız erişim sağlanabilmekte ve istenen ağ sistemi kolayca ele geçirilebilmektedir.

Cözüm Önerileri :

Şifre seçimi, kalitesi ve yönetimi konusunda kurum politikası oluşturulmalıdır. Başta sistem yöneticileri olmak üzere kullanıcıların şifre seçim kriterlerine uyumu, izin hizmetleri veya alan denetçileri ile sağlanmalı ve kullanıcıların daha zor tahmin edilebilir şifre seçimleri yapmaları sağlanmalıdır. Özel uygulama alanlarında (sanal özel ağ, ERP yazılımları, bankacılık uygulamaları vb.) harici doğrulama sistemleri veya sayısal sertifikalar kullanılmalıdır. Web temelli uygulamaların tasarımında, kullanıcı hesap yönetimi ve şifre seçimi konusunda, beklenen kriterlerin uygulanması zorlayıcı olmalıdır.

Referanslar :

Passwords: the Weak Link in Network Security

http://www.windowsecurity.com/articles/Passwords_Network_Security.html

Information Security: web applications

<http://www.upenn.edu/computing/security/standards/wwwsec.html>

6. SNMP Servisi Kullanımı

Acıklama :

SNMP protokolü, ağ yönetim ve izleme amaçlı olarak kullanılmaktadır. Kurumsal ağlarda, birçok sunucu veya ağ bileşeninde SNMP servisi kullanılmaktadır. Kurumlar, İnternet erişim ortamında güvenlik duvarı aracılığıyla sunucularda bulunan SNMP servisine erişimleri engellenmektedir. Ancak güvenlik duvarının önünde yer almakta olan birçok yönlendirici SNMP servisini ve SNMP servisinin yapısından kaynaklanan güvenlik sorunlarını içermektedir. UDP protokolü temelli olması, kullanıcı adı ve şifre doğrulamaları kullanmaması, SNMP protokolünün en zayıf yönlerindedir. Yönlendirici üzerinde bulunan SNMP servisini ele geçiren bir saldırgan, tüm kurumsal ağ trafiğini tünelleme ile kendisine aktarabilir, yönlendirme tablolarında değişiklik yapabilir ve kurum ağına geçiş için yönlendiriciyi atlama noktası olarak kullanabilir.

Çözüm Önerileri :

İnternet erişimine açık sistemlerde SNMP servisinin kullanılmaması tavsiye edilir. SNMP protokolünün kullanılması gerekli ise yönlendirici/sunucu üzerinde bulunan paket filtreleme seçenekleri ve erişim denetim kuralları aracılığıyla sadece bağlanması istenen sistemlere izin verilmelidir. Ayrıca SNMP erişimi için zor bir iletişim kelimesi tanımlanmalı ve iletişim TCP protokolü temelli veya yönlendirici/sunucu destekliyor ise kriptolu veri trafiği üzerinden yapılmalıdır.

Referanslar :

CERT Advisory CA-2002-03,
"Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)"
<http://www.cert.org/advisories/CA-2002-03.html>

CIAC Information Bulletin M-042,
"Multiple Vulnerabilities in Multiple Implementations of SNMP"
<http://www.ciac.org/ciac/bulletins/m-042.shtml>

7. Güncellemeleri Yapılmamış Web Sunucusu

Açıklama :

Birçok kurum, ağlarında bulunan web sunucu yazılımlarını düzenli olarak güncellememektedir. Microsoft IIS veya ASF Apache web sunucu yazılımlarının eski sürümleri birçok güvenlik açığı barındırmaktadır. Web sunucularının düzenli güncellenmemesinin sebeplerinden en önemlisi, bu yazılımların parçası olduğu ticari ürünlerin kullanılıyor olmasıdır. Web sunucuda yapılacak sürüm değişikliği veya güncellemeler, ürün firması tarafından desteğin kesilmesine neden olabilmektedir. Her iki web sunucusunda da saptanan güvenlik açıkları, web sunucusunun servis dışı kalmasına veya tüm sunucunun ele geçirilmesine neden olmaktadır. Önceden belirlenmiş yapılandırma ile kurulan web sunucuları, gerekli olmayan birçok bileşeni bünyelerinde barındırmakta ve gelecekte bu bileşenlere ait ortaya çıkabilecek güvenlik açıklarından etkilenebilmektedir.

Çözüm Önerileri :

Web sunucu yazılımlarının düzenli güncellenmeleri oldukça önemlidir, ayrıca gerekli olmayan tüm bileşenler (WebDAV, HTTP Trace, Frontpage Uzantıları, Yazıcı desteği, Index oluşturma desteği ve örnek CGI uygulamaları) sistemden çıkarılmalıdır. Böylece gelecekte söz konusu bileşenler için duyurulacak güvenlik açıklarından etkilenilmeyecektir. Microsoft IIS web sunucusu için Microsoft URLScan aracı kullanılmalı ve tüm web istekleri içeriklerine göre süzülmalıdır. Microsoft IIS veya ASF Apache'nin parçası olduğu ticari ürünler kullanılıyor ve güncellemeler yapılması durumunda üretici firmanın desteğinin kesilmesi söz konusu ise alternatif yöntemler kullanılmalıdır. Bir ters proxy aracılığıyla güvenlik açığı barındıran web sunucusuna doğrudan erişimin kısıtlanması, uygulama katmanında kullanılacak içerik denetim sistemleri, uygulama güvenlik duvarları veya saldırı tespit sistemleri verimli sonuçlar üreten çözümlerdendir.

Referanslar :

Secure Internet Information Services 5 Checklist - Microsoft

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/default.asp>

Securing Apache: Step-by-Step

<http://www.securityfocus.com/infocus/1694>

Apache HTTP Server: Security Tips

http://httpd.apache.org/docs/misc/security_tips.html

8. İşletim Sistemi ve Uygulamaların Standart Şekilde Kurulması

Açıklama :

İşletim sistemleri ve uygulamalar temel kullanım standartları doğrultusunda öntanımlı bir yapılandırma ile kurulmaktadır. Öntanımlı yapılandırma, etkin kullanımda gerekmeyecek birçok desteği içermekte ve ürünün kullanımının kolaylaştırılması için sunulmaktadır. İşletim sistemi ve uygulamaların öntanımlı kurulumlarında kolay tahmin edilebilir şifreler, güvenlik açığı içermekte olan bileşenler ve örnek uygulamalar kolay kurulum sebebiyle tercih edilmektedir. Bu şekilde kurulan işletim sistemi ve uygulamalar genel özelliklere sahip olmakta, yayınlanmış ve kullanılmayan bileşenlerinde içermekte olduğu güvenlik açıklarından etkilenmektedir. Yazılımlarda bulunan yayınlanmış güvenlik açıkları, kullanımlarının güvenlik tehditi içerebileceği öngörülmemiş uygulamalar ve gerekli olmayan servisler sonucu, sistemin tamamen ele geçirilmesi veya servis dışı bırakılması mümkün olmaktadır.

Çözüm Önerileri :

İşletim sistemi ve uygulama kurulumlarında, kurulum seçenekleri özelleştirilmeli, yönetim şifreleri zor tahmin edilebilir olmalı, gerekli olmayan servisler durdurulmalı ve örnek uygulamalar sistemden çıkarılmalıdır. Ürün geliştiricisi tarafından sağlanan tüm güvenlik yamaları ve yapılandırma önerileri yazılımlara uygulanmalıdır. Kurulumlarda minimalist bir yaklaşım belirlenmeli ve gerekli olmayan tüm erişim yetkileri kısıtlanmalıdır. Ayrıca düzenli olarak üretici tarafından yayınlanmış güvenlik duyuruları ve güncel güvenlik e-posta listeleri takip edilmeli, yönergeler izlenmelidir.

Referanslar :

Windows Server 2003 – Secure by Default | The Register
http://www.theregister.co.uk/2003/04/28/windows_server_2003_secure_by/

Securing & Optimizing Linux: The Ultimate Solution v2.0
<http://www.openna.com/products/books/sol/solus.php>

9. Hatalı Yapılandırılmış Saldırı Tespit Sistemleri

Acıklama :

Saldırı tespit sistemleri etkin güvenlik için vazgeçilmez uygulamalardır; ancak hatalı yapılandırılmaları durumunda saldırganların ağ iletişimini aksatabilmesi için en önemli araçlardandır.

Tespit edilen saldırılara kontrolsüz tepkiler verilmesi durumunda,

- saldırganlar saldırı tespit sisteminin türünü ve özelliklerini saptayabilir,
- çokça yapılan saldırı ile kayıt veritabanlarını doldurabilir,
- sunuculara yönelik servis engelleme saldırısı yapabilir,
- ağda gereksiz veri trafiği oluşturabilir,
- saldırılarını gizleyebilir,
- sahte saldırılar ile kritik görevdeki yönlendirici ve alan adı sunucularına erişimi kesebilir
- veya güvenlik duvarı aracılığıyla saldırgan engelleme yapıyor ise güvenlik duvarının kural tablosunu taşıyabilir.

Öntanımlı yapılandırmalarda, saldırı tespit sistemleri saldırı önleme yapmamaktadırlar, ancak optimizasyon yapılmamış birçok sistemde kontrolsüz olarak saldırı önleme yapılmaktadır. Güncelleme ve tanımlamaları doğru yapılmamış, güncel yamaları uygulanmamış sistemlerde, farklı veri ve iletişim türleri seçilmesi durumunda saldırı tespit edilememektedir.

Çözüm Önerileri :

Ağ üzerinde bir süre saldırı tespit sistemi izleme durumunda çalıştırılmalı ve gelen veri trafiği türüne bağlı olarak saldırı tespit sistemi kural ve tepki optimizasyonu yapılmalıdır. Saldırı tespit sisteminin saldırı türlerine göre tepki vermesi sağlanmalı, zorunlu kalmadıkça tepki üretilmemelidir. Güvenilir sistemler tanımı oluşturulmalı, önemli yönlendiriciler ve alan adı sunucuları ile kritik güvenlik sistemleri güvenilir olarak tanımlanmalıdır. Tepkiler öncelikle ICMP/TCP/UDP paketleri ile üretilmeli, çok sayıda saldırı olması durumunda tek bir işlem olarak ele alınmalı ve sürekli saldırılarda saldırgan sistem güvenlik duvarı tarafından engellenmelidir. Paket ve iletişim analiz seçenekleri için önerilen yama ve yardımcı yazılımlar kullanılmalı, ürün geliştiricilerinin hazırlamış oldukları rehber dökümanlarla karşılaştırılarak yapılandırmalar gözden geçirilmelidir.

Referanslar :

IDS Evasion Techniques and Tactics

<http://www.securityfocus.com/infocus/1577>

Understanding IDS Active Response Mechanisms

<http://www.securityfocus.com/infocus/1540>

Evaluating Network Intrusion Detection Systems

http://www.giac.org/practical/michael_wilkinson_gcia.doc

10. Güvenlik Duvarı Tarafından Korunmayan Sistemler

Açıklama :

Güvenlik duvarları, kurumların güvenlik sürecinde en önemli bileşenlerdendir. Doğru yapılandırılmamış veya tasarım hatası içermekte olan güvenlik duvarları, istenen güvenlik seviyesini sağlayamamaktadır. Özel istemci veya sunuculara verilmiş sınırsız erişim hakları, güvenlik duvarının önünde bulunan sunucu ve istemciler ile erişim denetim kuralları özelleştirilmemiş güvenlik duvarları, saldırganların kurum ağına sınırsız olarak erişimine imkan tanımaktadır. Yayınlanmış güvenlik açıklarının takip edilmemesi veya yapılandırma hatası sonucu güvenlik duvarı tarafından korunmayan bir sistem, saldırganın kurum ağına girebilmesi için atlama noktası olabilmektedir.

Cözüm Önerileri :

Güvenlik duvarı tasarımı yapılırken, kurum ağına bulunan ve Internet üzerinden hizmet sunacak sistemler DMZ bölümüne taşınmalı, yönlendirici ile güvenlik duvarı arasındaki ağa fiziksel giriş imkanları önlenmeli ve güvenlik duvarı üzerinde düzenli kontroller yapılarak, özel haklar sağlayan kurallar devre dışı bırakılmalıdır. Özel amaçlar için güvenlik duvarının dışına yerleştirilmesi gereken sistemlerin, yapılandırmaları özelleştirilmeli, gerekmeyen servisler durdurulmalı, güvenlik yamaları tamamlanmalı ve güvenlik duvarı üzerinden ağa erişimlerinde hiçbir özel erişim kuralı belirlenmemelidir.

Referanslar :

Design the firewall system

<http://www.cert.org/security-improvement/practices/p053.html>

Firewalls and Internet security

<http://secinf.net/info/fw/steph/>

SONUÇ

Raporda yer alan açıklanmış güvenlik açıkları hatalı programlama, hatalı yapılandırma ve güncelleme yapılmamasından kaynaklanmaktadır. Güvenlik göz ardı edilerek, işlevsellik ve hız temelli yapılan işlemler, beraberinde çok sayıda güvenlik açığını getirmektedir. Özellikle sistem ve uygulama yapılandırma sürecinde birçok ürün ve uygulamanın özel yetkiler için değiştirilmesi, özel izinler tanımlanması, kontrolsüz tepkiler üretilmesi ve örnek uygulamaların sistemde bırakılması ile sıkça karşılaşılmaktadır. Bu güvenlik açıklarının kullanılması sonucunda kurumsal ağda birçok yetki kazanılabilmekte ve ağ kaynakları yerel kullanıcılar ile eşit biçimde kullanılabilir.

Her güvenlik açığının altında çözüm önerileri ve bazı referans dökümanlar yer almaktadır. Bu şekilde birçok güvenlik problemine karşı korunma sağlanması mümkün olabilecektir. Kapsamlı bir korunma için kullanılmakta olan güvenlik uygulamaları incelenerek en iyi verim alınacak biçimde yapılandırılmalı, sunucu ve uygulamaların öntanımlı yapılandırmaları özelleştirilmeli, şifre politikası oluşturulmalıdır. Ayrıca günümüzde çokça kullanılan kablosuz ağlar, sanal özel ağlar ve web temelli uygulamaların yapıları incelenmeli, güvenlik seviyeleri artırılmalı ve sistem kaydı tutulması sağlanmalıdır.

Güvenlik seviyesinin düzenli olarak izlenmesi, sunucu yazılımlarının güvenlik açıklarının takibi, zaman içerisinde oluşabilecek güvenlik açıklarına karşı korunma ve bilinmeyen güvenlik tehditlerinin analizi için düzenli olarak güvenlik denetimi yaptırılmalıdır. İnternet ve İnternet üzerinden yapılabilecek denetimler ile veritabanı sunucuları, yerel ağda bulunan cihazlar, istemci sistemlerinin yapılandırılması ve İnternet üzerinden paylaşılan kaynakların güvenliği analiz edilebilecektir.