



# 2006 Yılı Güvenlik Denetim Değerlendirmeleri Sonuç Raporu

Tarih : 25 Nisan 2007



## GamaSEC Hakkında

GamaSEC Bilgi Güvenlięi Denetim ve Danıřmanlık Servisleri Ekim 2005 itibariyle ITBS Ltd.řti. bünyesinde hizmet vermeye bařlamıř, Temmuz 2006 itibariyle ise baęımsız bir řirket hüviyetini kazanmıřtır. Bünyesinde GamaTEAM olarak bilinen 5 adet güvenlik danıřmanı ve denetmeninden oluřan kadrosu ile kurulduęu günden itibaren 90'ın üzerinde denetim ve danıřmanlık hizmetini bařarıyla tamamlamıřtır. Hazırlamıř olduęu ok sayıda güvenlik denetim ve danıřmanlık hizmeti ile kurumların güvenlik seviyesini arttırmak adına yapacaęı alıřmaları güçlendirmeyi hedeflemektedir.

### GamaSEC Hizmetleri

- ⇒ GamaNET İnternet Güvenlik Denetimi
- ⇒ GamaAPP Web Uygulaması Güvenlik Denetimi
- ⇒ GamaLAN Yerel Aę Güvenlik Denetimi
- ⇒ GamaAUDIT Biliřim Sistemleri Denetimi
- ⇒ GamaSCAN Otomatize Güvenlik Denetimi
- ⇒ GamaDMZ DMZ Bölgesi Güvenlik Denetimi
- ⇒ GamaVPN Sanal Özel Aę Güvenlik Denetimi
- ⇒ GamaWIRELESS Kablosuz Aę Güvenlik Denetimi
- ⇒ GamaCON Bilgi Güvenlięi Danıřmanlıęı
- ⇒ GamaREPORT Raporlama Danıřmanlıęı
- ⇒ GamaPOLICY Güvenlik Politikası Danıřmanlıęı

### GamaSEC Eęitimleri

- ⇒ Biliřim Sistemleri Güvenlik Denetimi
  - Siber Saldırıları Anlamak
  - Sistem Sızma Denetim Temelleri
  - İleri Düzey Sistem Sızma Denetimi
  - Yerel Aę Sistem Sızma Denetimi
  - Web Uygulama Güvenlięi
  - İleri Düzey Exploit Geliřtirme
- ⇒ Kurumsal Bilgi Güvenlięi
  - Kurumsal Bilgi Güvenlięi Politikası ve Standartlar
  - Kurumsal Bilgi Güvenlięi Politika Uygulamaları
  - Kurumsal Bilgi Güvenlięi Farkındalıęı
  - Kurumsal Bilgi Güvenlięi Temel Kavramlar
  - Kurumsal Bilgi Güvenlięi Teknolojileri
- ⇒ Sistem ve Aę Güvenlięi
  - Güvenli Web Uygulaması Geliřtirme
  - Sunucu Güvenlięi İyileřtirme
  - Güvenlik İhlali Müdahale

## Deęerlendirme zeti

GamaSEC Bilgi Gvenlięi Denetim ve Danıřmanlık Servisleri tarafından sunulan Internet, Yerel Aę ve Uygulama denetim hizmetleri sonucunda ok sayıda kurumda benzer gvenlik aıklarının bulunduęu saptanmıřtır. Ařaęıda denetim srecinde sıklıca rastlanan gvenlik aıkları listelenmiřtir. Raporun ilerleyen blmlerinde saptanan gvenlik aıklarının detaylı aıklamaları, zm nerileri ve referansları da yer almaktadır.

## 2006 Yılı En Sık Karřılařılan 10 Gvenlik Aıęı

1.	Hatalı Yapılandırılmıř veya Gncellenmemiř Saldırı nleme Sistemleri
2.	Web Uygulamalarında Bozuk Oturum Ynetimi
3.	Gvenlik Duvarı Tarafından Korunmayan Sistemler
4.	Web Uygulamalarında Siteler Arası Komut alıřtırma
5.	Test veya rn Deneme Amalı Kullanılan n Tanımlı Sistemler
6.	Web Uygulamalarında SQL Sorgularının Deęiřtirilebilmesi
7.	Kablosuz Aę Eriřim Noktası ve İstemcilerin Hatalı Yapılandırılması
8.	İřletim Sistemi ve Yazılımı Gncellenemeyen zel Amalı Aę Cihazları
9.	Korumasız veya Hatalı Yapılandırılmıř VoIP Sistemleri
10.	Yerel Aę Yazıcı, Switch, Ynlendirici ve Sunucu Ynetim Sistemleri

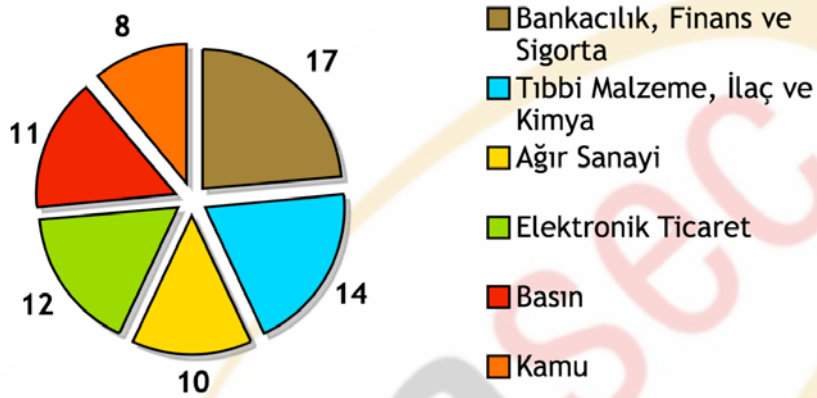
## İindekiler

<u>GAMASEC HAKKINDA</u>	<u>2</u>
<u>DEęERLENDİRME ÖZETİ</u>	<u>3</u>
<u>İİNDEKİLER</u>	<u>4</u>
<u>ARAŞTIRMA KAPSAMI</u>	<u>5</u>
<u>1 HATALI YAPILANDIRILMIŞ VEYA GÜNCELLENMEMİŞ SALDIRI ÖNLEME SİSTEMLERİ</u>	<u>6</u>
<u>2 WEB UYGULAMALARINDA BOZUK OTURUM YÖNETİMİ</u>	<u>8</u>
<u>3 GÜVENLİK DUVARI TARAFINDAN KORUNMAYAN SİSTEMLER</u>	<u>9</u>
<u>4 WEB UYGULAMALARINDA SİTELER ARASI KOMUT ALIŞTIRMA</u>	<u>11</u>
<u>5 TEST VEYA ÜRÜN DENEME AMALI KULLANILAN ÖN TANIMLI SİSTEMLER</u>	<u>12</u>
<u>6 WEB UYGULAMALARINDA SQL SORGULARININ DEęİŞTİRİLEBİLMESİ</u>	<u>13</u>
<u>7 KABLOSUZ Aę ERİŞİM NOKTASI VE İSTEMCİLERİN HATALI YAPILANDIRILMASI</u>	<u>15</u>
<u>8 İŞLETİM SİSTEMİ VE YAZILIMI GÜNCELLENEMEYEN ÖZEL AMALI Aę CİHAZLARI</u>	<u>16</u>
<u>9 KORUMASIZ VEYA HATALI YAPILANDIRILMIŞ VOIP SİSTEMLERİ</u>	<u>17</u>
<u>10 YEREL Aę YAZICI, SWITCH, YÖNLENDİRİCİ VE SUNUCU YÖNETİM SİSTEMLERİ</u>	<u>18</u>
<u>SONU</u>	<u>20</u>

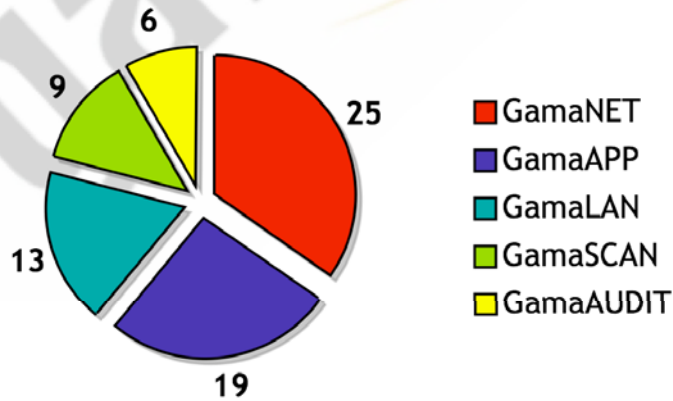
## Araştırma Kapsamı

GamaSEC Bilgi Güvenliği Denetim ve Danışmanlık Servisleri 2006 yılı içinde 72 adet güvenlik denetim hizmeti sunmuştur. Denetim hizmetleri başta elektronik ticaret, basın, finans, ilaç sanayi ve ağır sanayi şirketleri olmak üzere çok sayıda farklı sektöre sunulmuştur. En sık tercih edilen denetimler GamaNET İnternet Güvenlik Denetimi, GamaAPP Yerel Ağ Güvenlik Denetimi ve GamaLAN Yerel Ağ Güvenlik Denetimi hizmetleridir.

### Denetim Hizmetlerinin Sektörel Dağılımı



### Denetim Hizmetlerinin Türlere Dağılımı



## 1 Hatalı Yapılandırılmış veya Güncellenmemiş Saldırı Önleme Sistemleri

Açıklama
<p>Kurumsal ağ altyapısı ve sunuculara yönelik saldırıları izleme, saptama veya önleme amaçlı olarak saldırı tespit/önleme sistemleri kullanılmaktadır. Saldırı tespit/önleme sistemleri, kurumsal ağın tamamını izleyebilecek, Internet ve Yerel ağ üzerinden gelebilecek saldırıları doğru noktalarda tespit edecek biçimde yapılandırılmalıdır.</p> <p>Denetimler süresince saldırı tespit/önleme sistemlerinin yerleşiminin hatalı seçildiği sıklıkla gözlenmiştir. saldırı tespit/önleme sistemlerinin, SSL/TLS/SSH gibi kriptolu ağ trafiği veya kurumsal ağın belirli bölümlerini gözlemleyemez biçimde yerleştirildiği saptanmıştır. Kurumsal web hizmetlerinin, elektronik ticaret, Internet bankacılığı veya müşteri ilişkileri uygulamalarının ağırlıklı olarak SSL/TLS üzerinden sunulması sonucunda, saldırı tespit/önleme sistemleri işleviz kalmakta, olası saldırı denemeleri veya erişimleri analiz edememektedir. Ek olarak yerleşim sorunları nedeniyle belirli ağ parçaları veya kritik sunuculara yönelik iletişimleri de gözleyememektedir.</p> <p>Saldırı tespit/önleme sistemlerinde farklı dil kodu uygulamaları, türkçe karakter sorunları veya özel uygulamaların engellenmesi nedeniyle belirli ön işlem eklentilerinin devre dışı bırakıldığı veya gözardı edildiği saptanmıştır. Bu durum sonucunda farklı dil kodu veya kripto kullanılarak yapılan saldırıların birçoğu başarılı olmaktadır.</p> <p>Aktif tepki üretmek amacıyla seçilen erişimin uzun süre kesilmesi veya anlık kesilmesi türü işlemler ise saldırı kaynağı sahteciliği yapılarak istismar edilebilmekte, erişimi önemli kurumsal bağlantılar bu yöntemle devre dışı bırakılabilmektedir.</p>
Çözüm Önerileri
<p>Saldırı tespit/önleme sistemi yerleştirilirken SSL/TLS/SSH gibi kriptolu olarak sunulacak hizmetler belirlenmeli, belirli bir sistem üzerinde kriptolu iletişim sonlandırması yapılmalı, saldırı tespit/önleme sistemi sonlandırma yapılan sistem ile servisi sunan sistem arasındaki erişimi dinleyecek biçimde yerleştirilmelidir.</p> <p>Saldırı tespit/önleme sistemlerinin güncellemeleri düzenli olarak yapılmalı, dil kodu seçenekleri etkinleştirilmeli ve ağın tamamından gelebilecek iletişimleri izleyebilecek şekilde yapılandırılmalıdır.</p>

Kaynağın sahte olabileceği protokol ve saldırı türleri incelenmeli, aktif tepki üretimi gözden geçirilmelidir. Ayrıca ağın devamlılığı için gerekli olan sistemler beyaz listeye eklenmeli, izlenmeli ancak aktif tepki ölçülü olmalıdır.

## Referanslar

IDS/IPS: Too Many Holes?

[http://www.darkreading.com/document.asp?doc\\_id=99581](http://www.darkreading.com/document.asp?doc_id=99581)

Intrusion Prevention Systems: the Next Step in the Evolution of IDS

<http://www.securityfocus.com/infocus/1670>

How to test an IPS

<http://www.iv2-technologies.com/~rbidou/HowToTestAnIPS.pdf>

IDS Evasion Techniques and Tactics

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

IDS Evasion with Unicode

<http://www.securityfocus.com/infocus/1232>

Intrusion detection system evasion techniques

[http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system\\_evasion\\_techniques](http://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques)

## 2 Web Uygulamalarında Bozuk Oturum Yönetimi

Açıklama
<p>Web uygulamalarında kullanıcı ve grup yönetimi, iletişim takibi ve yetkilendirme amaçlı olarak oturum takip sistemleri kullanılmaktadır. Birok web uygulama geliřtiricisi, geliřtirme yaptığı platformun oturum takip özelliğini kullanmakta ve oturum takibini yetkilendirme için yeterli bulmaktadır.</p> <p>ok sayıda uygulama bileřenin olduğu durumlarda, bazı uygulama bileřenlerinde oturum takibi yapılması için gereken kod bloęu eklenmesi unutulmakta, yönetim sistemi ve kullanıcılar aynı oturum yapısını kullanmakta, kullanıcılara oturum sonlandırma imkanı sunulmamakta, iletişimin zaman aşımı deęerleri belirlenmemekte veya oturum deęeri tahmin edilebilmektedir.</p> <p>Bozuk veya tahmin edilebilir oturumlar kullanılarak uygulama kaynaklarına yetkisiz erişim, veritabanına yetkisiz erişim veya dięer kullanıcıların haklarının ele geçirilmesi mümkün olmaktadır. Ayrıca bozuk oturumların takip edilmemesi sonucu oluşan istisnalar ve üretilen hatalar uygulama yapısı hakkında önemli olabilecek bilgilere erişim sağlamaktadır.</p>
özüm Önerileri
<p>Uygulamaların tüm bileřenleri gözden geçirilmeli, oturum takibi için gerekli olan kod bütünlüğünün tüm bileřenlerde sağlandığı, oturum zaman aşımı ve sonlandırma tanımlarının doęru biçimde yapıldığı teyit edilmelidir. Mümkünse geliřtirme yapılan platformun sunmuş olduğu oturum takip ve yetkilendirme sistemlerine ek olarak ikincil takip kriterleri eklenmeli, olası platform zaafiyetlerine karşı korunma sağlanmalıdır.</p>
Referanslar
<p>OWASP Top Ten - Broken Access Control <a href="http://www.owasp.org/index.php/Broken_Access_Control">http://www.owasp.org/index.php/Broken_Access_Control</a></p> <p>OWASP Top Ten - Broken Authentication and Session Management <a href="http://www.owasp.org/index.php/Broken_Authentication_and_Session_Management">http://www.owasp.org/index.php/Broken_Authentication_and_Session_Management</a></p> <p>OWASP Top Ten - Insecure Configuration Management <a href="http://www.owasp.org/index.php/Insecure_Configuration_Management">http://www.owasp.org/index.php/Insecure_Configuration_Management</a></p>

### 3 Güvenlik Duvarı Tarafından Korunmayan Sistemler

Açıklama
<p>Birçok kurum çalışanları ürün denemeleri, şirket içi bağlantı testleri veya dosya paylaşım yazılımları kullanımı gibi özel amaçlarla kurmuş oldukları sistemleri, ağa dahil olmadığı ve risk oluşturmayacağı düşüncesiyle, güvenlik duvarı ve yönlendirici arasına yerleştirmekte, doğrudan yönlendiriciye bağlanmaktadır.</p> <p>Ağ dışında yer aldığı düşünülen ilgili sistem, güvenlik duvarı veya diğer kurumsal önlemlerden faydalanamakta, çoğunlukla ciddi güvenlik zaafiyetleri barındırmaktadır. Dosya paylaşım yazılımlarının zaafiyetleri, kritik servislere doğrudan erişime imkan sağlanması veya uzak yönetim servislerinin bulunması nedeniyle sistemlerin yönetimi kolayca ele geçirilebilmektedir.</p> <p>Sistemlerin ele geçmesi durumunda -her ne kadar ağ dışında oldukları düşünülse de- yönlendirici ve güvenlik duvarı arasında akmakta olan tüm kurumsal Internet trafiği dinlenebilmekte, aynı ağ parçasında olmaları nedeniyle güvenlik duvarı veya yönlendiriciye doğrudan saldırı yapılabilmesi mümkün olmaktadır.</p>
Çözüm Önerileri
<p>Kurum bünyesinde yer alan her sistemin kurum ağının parçası olduğu unutulmamalı, kurumsal güvenlik önlemlerini alabilecek şekilde uygun yapılandırmaların yapılması sağlanmalı ve yerleşimleri bu doğrultuda belirlenmelidir. İlgili sistemlerde tehlike arzedecek yazılımların kullanılmaması, uzak yönetim ve diğer arabirimlere erişimin engellenmesi gerekmektedir. Eğer böyle bir sistemin kullanımı gerekli ise özel bir DMZ ağına yerleştirilmeli, aynı ağ üzerinde herhangi bir sistem ile doğrudan veya dolaylı iletişimi fiziksel olarak engellenmeli, izleme sistemleri etkinleştirilmeli, eğer yapılabiliyor ise tercihen harici bir ağ bağlantısı sağlanarak gerekli ihtiyacın giderilmesi sağlanmalıdır.</p>
Referanslar
<p>Hardening Bastion Hosts  <a href="http://www.sans.org/reading_room/papers/index.php?id=420&amp;c=80c9dec08d4b581d738caceb89082798">http://www.sans.org/reading_room/papers/index.php?id=420&amp;c=80c9dec08d4b581d738caceb89082798</a></p> <p>Intrusion Detection FAQ: What is a bastion host?  <a href="http://www.sans.org/resources/idfaq/bastion.php">http://www.sans.org/resources/idfaq/bastion.php</a></p>

SANS Top 20 - C3. P2P File Sharing Applications  
<http://www.sans.org/top20/#c3>



## 4 Web Uygulamalarında Siteler Arası Komut Çalıştırma

Açıklama
<p>Siteler arası komut çalıştırma açıkları, web uygulamasının kullanıcılarına yönelik olarak düzenlenebilecek saldırılara imkan veren güvenlik açıklarıdır. Bu tip açıklar bir web uygulamasının verilen http cevabında kullanıcı tarafından sağlanmış bir girdiyi kontrol etmeden kullanmasıyla oluşur.</p> <p>Siteler arası komut çalıştırma açıkları kullanılarak istemcilere ait olan oturum bilgileri çalınabilir, sahte formlar veya bilgiler gösterilerek yanıltılmaları sağlanabilir. Siteler arası komut çalıştırma açıkları sadece istemcilere yönelik saldırılar için kullanılmamaktadır. Açığın farklı kullanım yöntemleri ile kurum itibarını zedeleyecek biçimde sayfa görünümü değiştirilerek e-posta ile dağıtımının sağlanması ve iç içe IFRAME kullanımları ile istemciler tarafından dağıtık servis engelleme saldırıları düzenlenmesine imkan sağlamaktadır.</p>
Çözüm Önerileri
<p>Siteler arası komut çalıştırma saldırıları genellikle hedef olan kişinin web tarayıcısındaki güvenlik açıkları ve çalıştırılan kodun içeriği ile sağlanır. Bu nedenle uygulamalara sağlanan girdi parametreleri kontrol edilmeden kullanılmamalıdır.</p> <p>Genel bir kural olarak, kullanıcı tarafından sağlanan girdiler incelenmeli, girdinin geçerliliği bir kural karşısında kontrol edilmeli ve uygun olmayan parametreler filtre edilmelidir. Tercihen engelleme türü olarak 'Beyaz Liste' yaklaşımı kullanılmalı, izin verilen karakterlerin dışındaki tüm karakterler engellenmelidir.</p>
Referanslar
<p>SPI Dynamics Cross-site Scripting Whitepaper  <a href="http://www.spidynamics.com/whitepapers/SPIcross-sitescripting.pdf">http://www.spidynamics.com/whitepapers/SPIcross-sitescripting.pdf</a></p> <p>Cross Site Scripting Faq  <a href="http://www.cgisecurity.com/articles/xss-faq.shtml">http://www.cgisecurity.com/articles/xss-faq.shtml</a></p> <p>iMPERVA Cross Site Scripting  <a href="http://www.imperva.com/application_defense_center/glossary/cross_site_scripting.html">http://www.imperva.com/application_defense_center/glossary/cross_site_scripting.html</a></p>

## 5 Test veya Ürün Deneme Amaçlı Kullanılan Ön Tanımlı Sistemler

Açıklama
<p>Kurumların ağ yenileme veya geliştirme amaçlı olarak incelemekte oldukları cihazları, doğrudan veya dolaylı olarak Internet erişimine açık biçimde kurumsal ağlarına dahil ettikleri saptanmıştır. Test veya deneme amaçlı olarak alınan ürünlerin büyük bölümü, bilinen yapılandırma hatalarına, güncelleme sorunlarına ve kolay ele geçirilen hesaplara sahiptir. Cihazların üretici yazılımlarına ek olarak, açık kaynaklı veya ücretsiz yazılımları gömülü olarak barındırabileceği, eski sürüm olmaları nedeniyle normal sürümlerde bulunan güvenlik açıklarından da etkilenebileceği unutulmamalıdır.</p> <p>Ön tanımlı yapılandırmalar, tahmin edilebilir kullanıcı ve yönetim hesapları ile güncellenmemiş yazılımlar barındıran cihazlar kolayca ele geçirilebilmekte veya sistemlere erişime imkan vermektedir. Ele geçirilen cihazlar, güvenlik duvarı dışında olsa dahi özellikleri nedeniyle ağa farklı erişim imkanları sağlayabilmekte veya paket yakalamak suretiyle Internet erişimini dinleyebilmektedir.</p>
Çözüm Önerileri
<p>Test veya deneme amaçlı sistemler için güvenlik duvarı üzerinde özel bir DMZ alanı oluşturulmalı, önemli olabilecek sistemlere erişimleri doğrudan veya dolaylı olarak engellenmelidir. Ayrıca yazılım güncellemeleri ve yapılandırma özelleştirmelerinin yapıldığı doğrulanmalı, olası güvenlik zaafiyetlerine karşı düzenli olarak izlenmelidir.</p>
Referanslar
<p>Security Configuration Guides  <a href="http://www.nsa.gov/snac/">http://www.nsa.gov/snac/</a></p>

## 6 Web Uygulamalarında SQL Sorgularının Deęiřtirilebilmesi

Aıklama
<p>Web uygulamaları verimlilik ve veri barındırma amacıyla SQL veritabanları kullanmaktadır. Programcılar bazı durumlarda kullanıcılardan gelen verileri bir kontrole tabi tutmadan SQL sorguları içinde kullanmaktadırlar. Genel olarak problemler uygulama geliřtiricinin SQL sorgularında anlam ifade edebilecek giriřlere karřı bir önlem almadığı zaman ortaya çıkmaktadır.</p> <p>İinde SQL sorgulama barındıran bir ok ürün SQL sorgularının deęiřtirilmesine karřı savunmasızdır. Saldırganlar SQL sorguları deęiřtirme tekniklerini Web sitelerine ve uygulamalara zarar vermek amaçlı kullanmaktadırlar. SQL sorguları deęiřtirme ile saldırganlar tablo yaratabilir, deęiřiklikler yapabilir, veritabanı üzerinde eriřim saęlayabilir.</p> <p>Hata sayfalarının özelleřtirilmesi veya genel bir hata sayfası kullanımı yöntemiyle SQL veritabanı hata mesajları kapatılması güvenlik aığının kullanımını önlememektedir. Ancak deneme ve yanılma sürecin bir parası olacağı için aığın kullanımını bir miktar zorlařtırmaktadır.</p>
özüm Önerileri
<p>Gönderilen girdilerin farklı dil kodları ile gelebileceęi göz önünde bulundurularak istemci cevabı dil kodunun sabitlenmesi ve bu doęrultuda filtreleme yapılması gerekmektedir. Özellikle tek bir karakter ile devre dıřı bırakacak önlemler almanın ( Örneęin \ veya " karakteri kullanılarak yapılacak deęiřimler) aynı karakterin kullanılması durumunda anlamsız hale gelebileceęi dikkate alınmalıdır. Tercihen engelleme türü olarak 'Beyaz Liste' yaklařımı kullanılmalı, izin verilen karakterlerin dıřındaki tüm karakterler engellenmelidir.</p> <p>Ayrıca kayıtlı prosedür (Stored Procedure) kullanımı ile SQL sorgularının dinamik olarak deęiřtirilmesi büyük ölçüde engellenecektir.</p>
Referanslar
<p>SQL Injection  <a href="http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf">http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf</a></p>

Advanced SQL Injection

[http://www.nextgens.com/papers/advanced\\_sql\\_injection.pdf](http://www.nextgens.com/papers/advanced_sql_injection.pdf)

iMPERVA SQL Injection

[http://www.imperva.com/application\\_defense\\_center/glossary/sql\\_injection.html](http://www.imperva.com/application_defense_center/glossary/sql_injection.html)

Security Focus - Penetration Testing for Web Applications (Part Two)

<http://www.securityfocus.com/infocus/1709>

OWASP Top Ten - Injection Flaws

[http://www.owasp.org/index.php/Injection\\_Flaws](http://www.owasp.org/index.php/Injection_Flaws)



## 7 Kablosuz Ađ Eriřim Noktası ve İstemcilerin Hatalı Yapılandırılması

Aıklama
<p>Gün getike kablosuz ađ kullanımı yođunlařmakta ve birok kurumsal ađın parası olmaktadır. Kablosuz ađ kullanımı bazı durumlarda kolaylık getirir de, eriřim dođrulama zorlukları, eriřim sahtecilikleri ve protokol zaafiyetleri nedeniyle ciddi güvenlik aıkları oluřturmaktadır.</p> <p>Kablosuz ađın taklit edilebilmesi, donanım adresi temelli eriřimlerin sahtecilikle ařılabilmesi, kablosuz ađ kartı srclerinin zaafiyeti, eriřim noktalarının yapılandırma, yazılımsal veya protokol zaafiyetleri istismar edilerek ađlara eriřim sađlanabilmektedir. Kablosuz ađ aıklarının istismarı ile istemcilerin sistemleri ele geirilebilmekte, kablosuz ađ trafiđi analiz edilebilmekte, kablosuz ađın devre dıřı kalması sađlanabilmekte veya ađa yetkisiz eriřim mmkn olabilmektedir.</p>
özm Önerileri
<p>Donanım adresi temelli veya basit kriptolu dođrulama yöntemleri yerine sertifika veya tek seferlik řifre temelli dođrulama yöntemleri kullanılmalıdır. Kullanılan protokoller güncellenmeli, eriřim noktası yapılandırması gözden geirilerek sadece yetkili istemcilerin giriři sađlanmalı, istemcilerin ađ kartı srcleri güncellenmeli ve tercihen bir kablosuz ađ eriřim izleme sistemi kullanılmalıdır.</p>
Referanslar
<p>ISS - Wireless LAN Security <a href="http://www.iss.net/documents/whitepapers/wireless_LAN_security.pdf">http://www.iss.net/documents/whitepapers/wireless_LAN_security.pdf</a></p> <p>Wikipedia - Wireless security <a href="http://en.wikipedia.org/wiki/Wireless_security">http://en.wikipedia.org/wiki/Wireless_security</a></p>

## 8 İşletim Sistemi ve Yazılımı Güncellenemeyen Özel Amaçlı Ağ Cihazları

Açıklama
<p>Kurum ağ devamlılığı, servis çeşitliliği veya güvenliği amacıyla kullanılan özel ağ cihazlarının büyük bölümü, üreticileri tarafından geliştirilmiş yazılımlar barındırmaktadır. Ağ kameraları, yönlendiriciler, kablosuz erişim noktaları, modemler, ağ yazıcıları, güvenlik duvarları, saldırı tespit sistemleri ve anti-virüs sistemleri belirtilen türde cihazlara örnek verilebilir. Birçok cihaz üretici yazılımlarını sadece asıl hizmet amaçları için kullanmakta, işletim sistemi veya yönetim servisleri için açık kaynak kodlu veya ücretsiz olarak temin edilebilen yazılımları gömülü biçimde kullanmaktadır.</p> <p>Cihazların büyük bir bölümünde, amaca uygun yazılımların dışında kalan diğer yazılımlar veya işletim sistemleri güncellenememektedir. Bu durum, ilgili yazılımların veya işletim sistemlerinin zaafiyetlerini barındırmalarına, farklı bir kullanım türü ile beraber aynı açıklardan etkilenmelerine neden olmaktadır. Farklı kullanım veya açığın özel kullanımları ile ele geçirilebilen cihazlar ile kurumsal ağa yetkisiz erişim sağlamak, kritik sistemleri ele geçirmek veya hizmet dışı bırakmak mümkün olmaktadır.</p>
Çözüm Önerileri
<p>Ağ cihazı veya sistemi seçimi yapılırken yazılım güncelleme imkanları sorgulanmalı, kullanılan harici yazılımlar ile ilgili güvenlik duyuruları takip edilmeli ve üreticiden yazılımların yeni sürümünü geliştirmesi yönünde taleplerde bulunulmalıdır.</p> <p>Yazılım güncellemesi mümkün olmayan cihazlarda sadece gerekli sistemlerin erişimine imkan verilmeli, proxy veya güvenlik duvarları aracılığıyla ilgili yazılımlara ve servislere doğrudan erişim engellenmelidir.</p>
Referanslar
--

## 9 Korumasız veya Hatalı Yapılandırılmış VoIP Sistemleri

Açıklama
<p>Kurumsal iletişim altyapısında yer alan VoIP (Voice over IP) cihazları merkezi veya noktalar arası ses iletişimi için kullanılmaktadır. Kurumsal telefon santrallerine bağlantıları olması, yerel ağ veya Internet üzerinden erişilebilir olmaları nedeniyle iletişimin önemli bir bölümünde etkin konumda bulunmaktadır.</p> <p>VoIP cihazının ön tanımlı yapılandırmada bırakılması, ses görüşmeleri daveti veya kayıt sahteciliği, protokol zaafiyetleri, kriptolu iletişim tercih edilmemesi, yönetim arayüzlerine erişim veya istemcilerin hatalı yapılandırılması nedeniyle ciddi güvenlik açıkları barındırmaktadır.</p> <p>Ele geçirilen veya güvenlik önlemleri atlatılan bir VoIP cihazı ile ağa yetkisiz erişim sağlanabilir, telefon görüşmeleri dinlenebilir, iletişim altyapısı izinsiz kullanılabilir veya iletişim servisi durdurulabilir. Ayrıca kriptosuz iletişim kullanılması, ağda paket yakalanması veya ortadaki adam saldırısı yapılması durumunda ses iletişiminin kolayca çözümlenebilmesine olanak sağlamaktadır.</p>
Çözüm Önerileri
<p>VoIP cihazları ön tanımlı yapılandırmaları özelleştirilmeli, yönetim arabirimlerine erişim kısıtlanmalı, tercihen kriptolu iletişim tercih edilmeli ve ses iletişim taleplerine özel doğrulama yöntemleri kullanımı tercih edilmelidir. Ayrıca Internet üzerinden erişime açılması durumunda DMZ alanında yer almalı, ele geçirilmesi durumuna karşı iletişim ve erişim izlemeleri etkinleştirilmelidir.</p>
Referanslar
<p>Ensure successful VoWLAN: Understand security in VoIP networks  <a href="http://www.commsdesign.com/design_corner/showArticle.jhtml?articleID=193400223">http://www.commsdesign.com/design_corner/showArticle.jhtml?articleID=193400223</a></p> <p>Intrusion Prevention: The Future of VoIP Security  <a href="http://www.tippingpoint.com/pdf/resources/whitepapers/503160-001_TheFutureofVoIPSecurity.pdf">http://www.tippingpoint.com/pdf/resources/whitepapers/503160-001_TheFutureofVoIPSecurity.pdf</a></p> <p>Security in SIP-Based Networks  <a href="http://www.cisco.com/warp/public/cc/techno/tyvdve/sip/prodlit/sipsc_wp.pdf">http://www.cisco.com/warp/public/cc/techno/tyvdve/sip/prodlit/sipsc_wp.pdf</a></p>

## 10 Yerel Ađ Yazıcı, Switch, Yönlendirici ve Sunucu Yönetim Sistemleri

Aıklama
<p>Kurumsal ađda yer alan ađ yazıcıları, yönlendiriciler, switch'ler ve sunucular için özel merkezi yönetim yazılımları kullanılmaktadır. Kullanılan yazılımların büyük bölümü SNMP arayüzü veya özel bir aracı yazılım ile yönetim imkanı sağlamaktadır. Ek olarak cihazların tekil yönetimi amacıyla Telnet, SSH, SNMP veya HTTP servisleri kullanılmaktadır.</p> <p>Yönetim yazılımlarının kullanmakta oldukları protokollerde bulunan zaafiyetler, yetersiz erişim denetimi ve doğrulama tercihleri veya yazılımların barındırmış oldukları zaafiyetler nedeniyle ađda bulunan sistemlere tek merkezden yetkisiz erişim mümkün olabilmektedir. Erişime ek olarak kullanılan protokollerde bulunan zaafiyetler nedeniyle anonim olarak çok sayıda kritik bilgiye erişim sağlanabilmektedir.</p> <p>Ađ cihazlarının ve sunucuların tekil yönetim arayüzleri ise bir dięer güvenlik zaafiyetini doğurmaktadır. Yazılım güncellemelerinin yapılamaması, ön tanımlı yapılandırma kullanımı ve cihazların dięer ađlara erişime geçit olabilmeleri nedeniyle ađda çok sayıda sisteme yetkisiz erişim mümkün olabilmektedir. Ayrıca cihazların kritik görevlerde olması durumunda kritik servislerin engellenmesi imkanıda bulunmaktadır.</p>
Çözüm Önerileri
<p>Her bir kurumsal ađ bileşeni önemsiz gibi görünse bile önemli bir sistem gibi düşünölmeli, yapılandırmaları bu doğrultuda yapılmalı, yönetim hesapları gözden geçirilmeli ve gerekli olmayan yönetim servisleri durdurulmalıdır.</p> <p>Merkezi yönetim yazılımları düzenli olarak güncellenmeli, kullanılan protokollerin güncel ve güvenli sürümleri kullanılmalı, tercihen harici erişim doğrulama yöntemleri ve erişim izleme sistemleri tercih edilmelidir.</p>
Referanslar
<p>CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol  <a href="http://www.cert.org/advisories/CA-2002-03.html">http://www.cert.org/advisories/CA-2002-03.html</a></p>

Secunia - Cisco IOS

<http://secunia.com/search/?search=cisco+ios>

Secunia - IBM Tivoli

<http://secunia.com/search/?search=ibm+tivoli>

Secunia - CA eTrust

<http://secunia.com/search/?search=etrust>

Secunia - Compaq Management

<http://secunia.com/search/?search=compaq+management>



## Sonu

**GamaSEC** Bilgi Gvenlięi Denetim ve Danıřmanlık Servisleri tarafından sunulan denetim hizmetleri sonucunda birok kurumun ortak gvenlik aıklarına sahip olduęu saptanmıřtır. Saptanan gvenlik aıklarının byk blm aę altyapısı tasarımlarından veya sistem ynetim zaafiyetlerinden oluřmaktadır.

Kurumsal aę bnyesinde yer alan her sistemin nemli olduęu ve sunmakta olduęu hizmetin kurum iin gerekli olduęu gz nnde bulundurularak yapılacak gvenli aę tasarımları, birok gvenlik aıęının oluřmasını nlemektedir. alıřanların kullanılan teknolojiler konusunda eęitilmesi ile verim artıřı saęlanabilecek ve sistemlerin ynetim zaafiyetleri kolaylıkla giderilebilecektir.

Aęırlıklı olarak kurumsal veya mřteriler arası bilgi paylařımı, elektronik ticaret ve Internet bankacılıęı amalı kullanılan yazılımların, tasarım ařamasından bařlamak zere gvenlik kriterlerinin yerine getirilmesi ve ekibin gvenli yazılım geliřtirme eęitimi ile desteklenmesi sonucunda daha kaliteli ve gvenli olması mmkn olmaktadır.

Kurumsal aęlarda ve sistemlerdeki deęiřimler gz nnde bulundurularak dzenli olarak baęımsız denetimler yaptırılması, olası gncel gvenlik zaafiyetlerinin analiz edilmesi ve aę iyileřtirmelerinin yapılması, kurumun ihtiya duyulan gvenlik seviyesinin saęlanmasına yardımcı olacaktır.

Kurumsal ihtiyalar doęrultusunda hazırlanacak Bilgi Gvenlięi Ynetim Sistemi ile yařayan bir gvenlik olgusu oluřturulması, ynetiminin ve geliřiminin saęlanması birok kurum iin gereklilik haline gelmiřtir. Gvenlięin kurumun bir parası haline gelmesi ve alıřanların kurum gvenlik yaklařımı konusunda bilgilendirilmesi, iř devamlılıęı ve gvenlik risklerinin en aza indirgenmesini saęlayacaktır.