Bilgi Güvenliği – Temel Kavramlar

Fatih Özavcı
Security Analyst

holden@siyahsapka.com
http://www.siyahsapka.com
http://www.dikey8.com

Sunu İçeriği

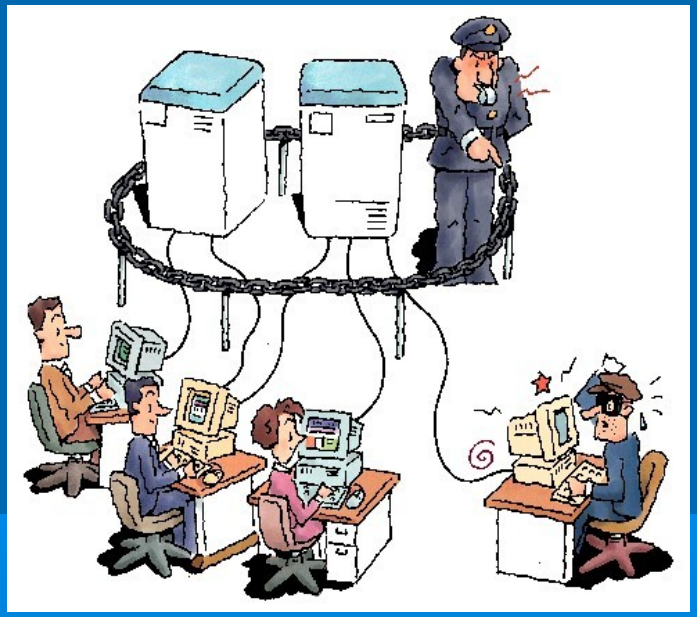
- Bilgi Güvenliği Kavramı ve Kapsamı
- Risk ve Tehditler
- Hareket Planı ve Bileşenleri
  - Güvenlik Politikaları
  - Güvenlik Uygulamaları
  - Denetleme ve İzleme
- Sistem Yöneticilerinin Genel Hataları

Bilgi Güvenliği Kavramı

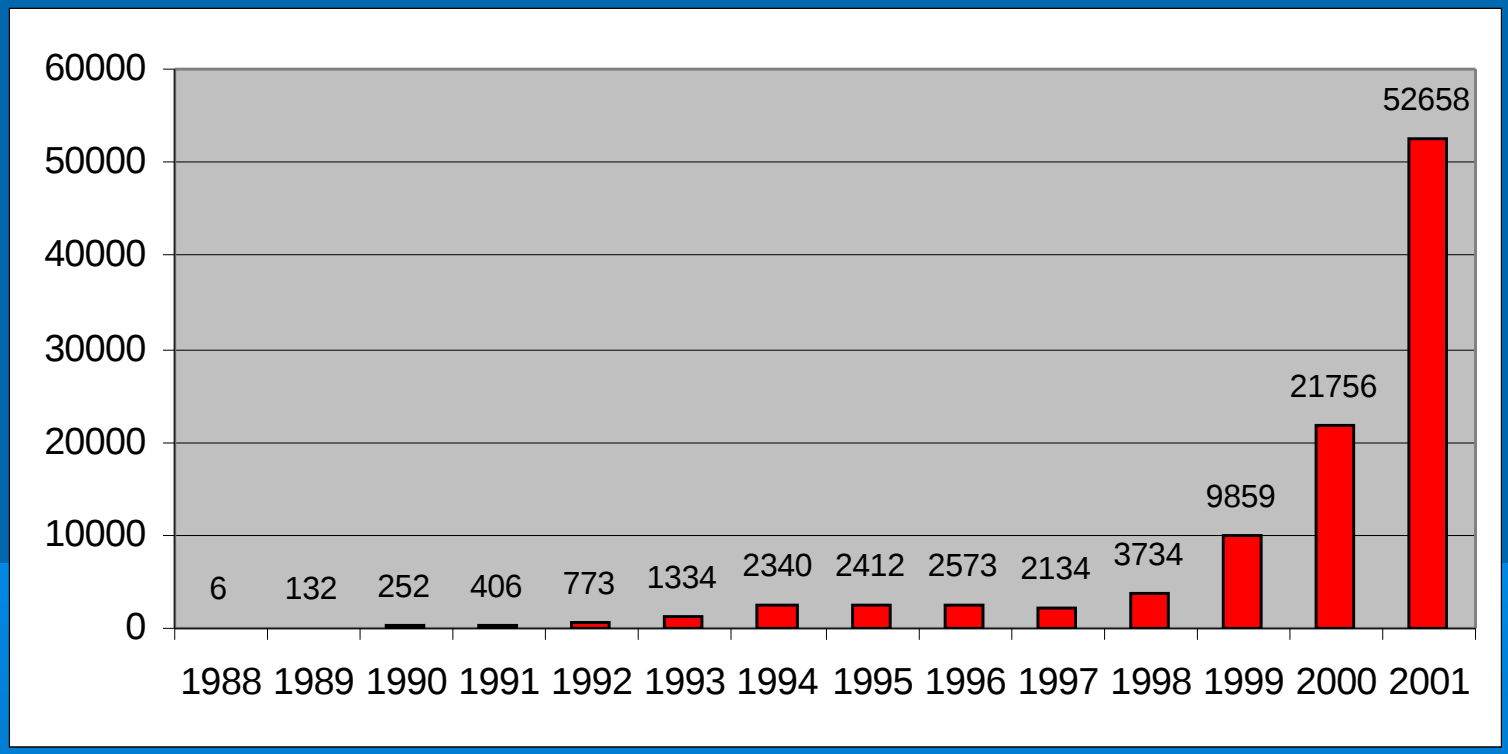
Bilişim ürünleri/cihazları ile bu cihazlarda işlenmekte olan verilerin bütünlüğü ve sürekliliğini korumayı amaçlayan çalışma alanıdır.

Bilgi Güvenliğinin Amacı

- Veri Bütünlüğünün Korunması
- Erişim Denetimi
- Mahremiyet ve Gizliliğin Korunması
- Sistem Devamlılığının Sağlanması



Cert/CC Yıllara Göre Rapor Edilen Olay Sayısı



Tehdit Türleri

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım
- Kötü Niyetli Hareketler

Harici Tehdit Unsurları

- Hedefe Yönelmiş Saldırılar
- Hedef Gözetmeyen Saldırılar

~ % 80 ~ % 20

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım
  - Temizlik Görevlisinin Sunucunun Fişini Çekmesi
  - Eğitilmemiş Çalışanın Veritabanını Silmesi

- Kötü Niyetli Hareketler
  - İşten Çıkarılan Çalışanın, Kuruma Ait Web Sitesini Değiştirmesi
  - Bir Çalışanının, Ağda “Sniffer” Çalıştırarak E-postaları Okuması
  - Bir Yöneticinin, Geliştirilen Ürünün Planını Rakip Kurumlara Satması

Harici Tehdit Unsurları

- Hedefe Yönelmiş Saldırılar

  - Bir Saldırganın Kurum Web Sitesini Değiştirmesi
  - Bir Saldırganın Kurum Muhasebe Kayıtlarını Değiştirmesi
  - Birçok Saldırganın Kurum Web Sunucusuna Hizmet Aksatma Saldırısı Yapması

- Hedef Gözetmeyen Saldırılar

  - Virüs Saldırıları (Melissa, CIH – Çernobil, Vote)
  - Worm Saldırıları (Code Red, Nimda)
  - Trojan Arka Kapıları (Netbus, Subseven, Black Orifice)

Saldırı Kavramı

Kurum ve şahısların sahip oldukları tüm değer ve bilgilere izinsiz erişmek, zarar vermek, maddi/manevi kazanç sağlamak için bilişim sistemleri kullanılarak yapılan her türlü hareket dijital saldırı olarak tanımlanabilir.

Saldırgan Türleri

- Profesyonel Suçlular
- Genç Kuşak Saldırganlar
- Kurum Çalışanları
- Endüstri ve Teknoloji Casusları
- Dış Ülke yönetimleri






Saldırı Yöntemleri

- Hizmet Aksatma Saldırıları
- Dağıtık Hizmet Aksatma Saldırıları
- Ticari Bilgi ve Teknoloji Hırsızlıkları
- Web Sayfası İçeriği Değiştirme Saldırıları
- Kurum Üzerinden Farklı Bir Hedefe Saldırmak
- Virüs , Worm , Trojan Saldırıları
- İzinsiz Kaynak Kullanımı

Saldırıya Uğrayabilecek Değerler

- Kurum İsmi, Güvenilirliği ve Markaları
- Kuruma Ait Özel / Mahrem / Gizli Bilgiler
- İşin Devamlılığını Sağlayan Bilgi ve Süreçler
- Üçüncü Şahıslar Tarafından Emanet Edilen Bilgiler
- Kuruma Ait Adli, Ticari Teknolojik Bilgiler

Görülebilecek Zararın Boyutu

- Müşteri Mağduriyeti
- Kaynakların Tüketimi
- İş Yavaşlaması veya Durması
- Kurumsal İmaj Kaybı
- Üçüncü Şahıslara Karşı Yapılacak Saldırı Mesuliyeti

Güvenlik İhtiyacının Sınırları

Saldırıya Uğrayabilecek Değerlerin, Kurum İçin Arzettiği Önem Seviyesi Güvenlik İhtiyacının Sınırlarını Belirlemektedir.

Hareket Planı Bileşenleri

- Güvenlik Politikası Oluşturulması
  - Sunulacak Hizmet Planının Oluşturulması
  - Erişim Seviyelerinin Belirlenmesi
  - Bilgilendirme ve Eğitim Planı
  - Savunma Bileşenlerini Belirleme
  - Yedekleme ve Kurtarma Stratejisi Belirleme
- Güvenlik Politikasının Uygulaması
  - Kullanılacak Uygulamaların Belirlenmesi
  - Uygulamaların Planlanan Biçimde Yapılandırılması
  - Bilgilendirme ve Eğitim Seminerleri
- Denetleme ve İzleme
  - Sistemin Politikaya Uygunluğunun Denetlenmesi
  - Oturumların ve Hareketlerin İzlenmesi
  - Ağa Sızma Testleri

Güvenlik Politikası

Kurumsal güvenliğin sağlanması sürecinde önemli olan her bileşenin seçimi, yapılandırılması, izlenmesi için oluşturulan ve yazılı ortama aktarılan kural ve yöntemler listesidir.

Güvenlik Politikasının Bileşenleri

- Sunulacak Hizmet Planının Oluşturulması
- Erişim Seviyelerinin Belirlenmesi
- Bilgilendirme ve Eğitim Planı
- Savunma Bileşenlerini Belirleme
- Yedekleme ve Kurtarma Stratejisi Belirleme

Güvenlik Uygulamaları

- Güvenlik Duvarları
- Saldırı Tespit Sistemleri
- Anti-Virüs Sistemleri
- Sanal Özel Ağ Sistemleri
- Şifreleme Sistemleri
- Sistem Güçlendirme (Hardening)
- Doğrulama ve Yetkilendirme Sistemleri
- İçerik Kontrol Yazılımları
- Yedekleme Sistemleri

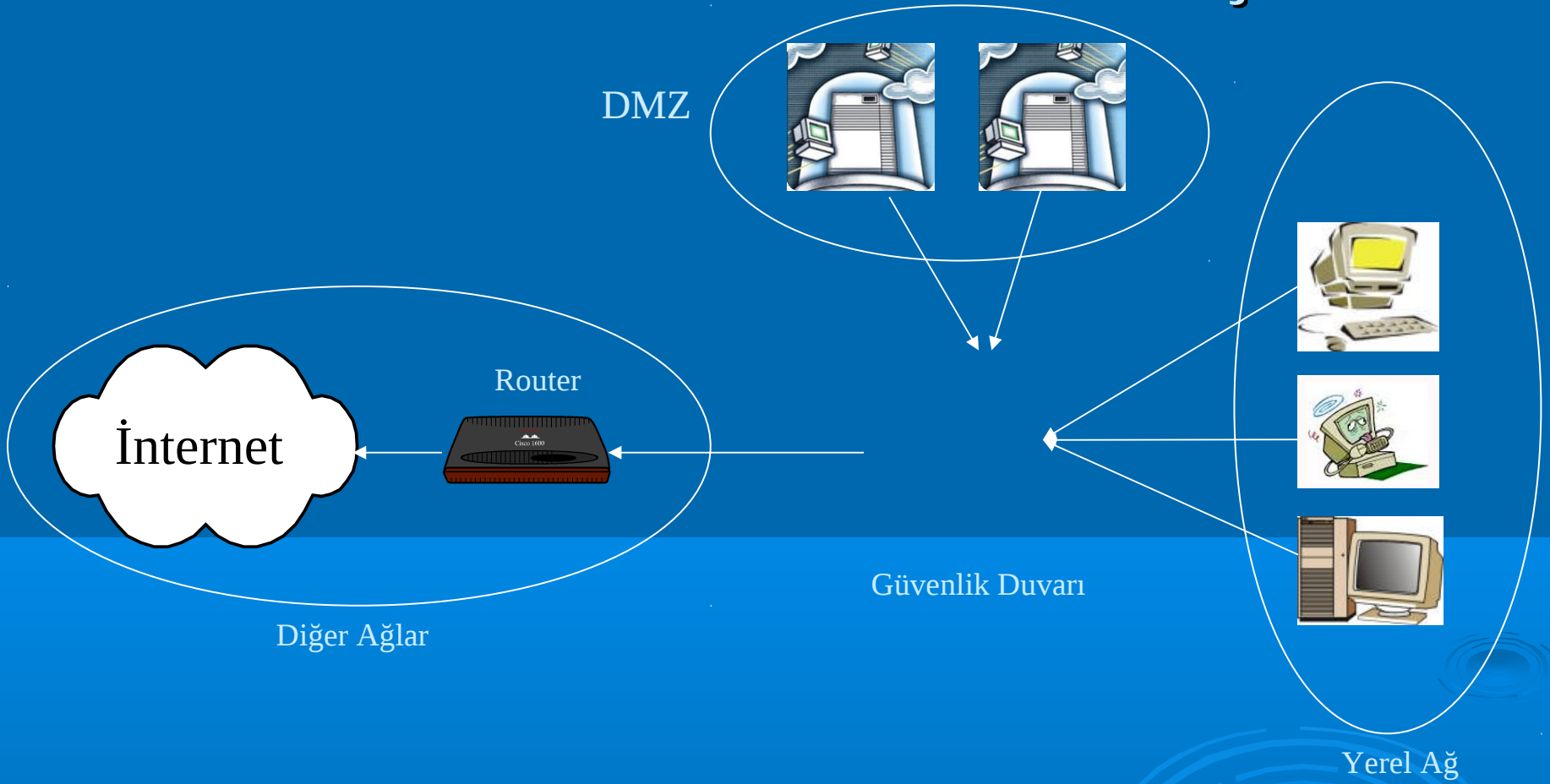
Güvenlik Duvarı

- Ağlar arası erişimleri düzenlerler
- Mimarileri
  - Statik Paket Filtreleme
  - Dinamik Paket Filtreleme (Stateful Inspection)
  - Uygulama Seviyesinde Koruma (Proxy)
- Erişimleri kural tabanlı belirlerler
- Donanım ve Yazılım olarak sunulabilirler
- Amaca özel işletim sisteminde bulunmalıdırlar
- Her türlü formatta kayıt ve uyarı sunabilirler

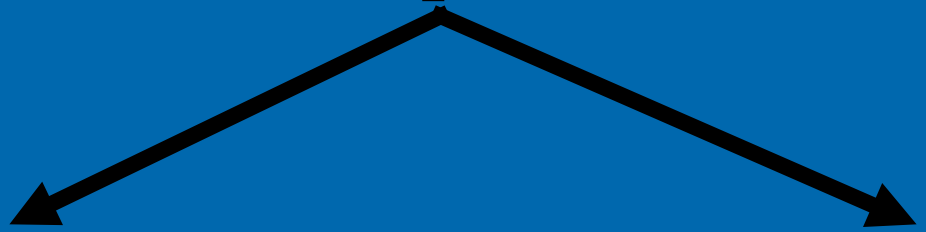
Güvenlik Duvarı / Neler Yapabilir – Yapamaz

- Erişim Denetimi Yapabilir
- NAT Yapabilir
- Bridge (Köprü) Moda Geçebilir
- Paket İçeriği Kontrol Edebilir
- Trafik Yönetimi Yapabilir
- Üçüncü Parti Yazılımlar İle Beraber Çalışabilir
- Saldırıları Engelleyemez
- Virüsleri Engelleyemez
- Zayıflıkları Saptayamaz, Yamalayamaz
- Ağlar Arası İletişimde Şifreleme Yapamaz

Güvenlik Duvarı Örnek Yerleşimi



Saldırı Tespit Sistemleri



- Ağ Temelli
- Sunucu Temelli
- Uygulama Temelli
- Anormallik Saptama Temelli
- Saldırı İmzası Arama Temelli

Saldırı Tespit Sistemleri (Ağ Temelli ve Saldırı İmzası Arama)

- Belirli bir ağ parçasını dinleyerek saldırıları tespit etmeye çalışırlar
- Tanımlı olan imzalar ile saldırıları belirler ve engelleyebilirler (Worm saldırıları dahildir)
- Birden fazla yardımcı ile çalışarak, merkezi yönetim ve raporlama sağlayabilirler
- Güvenlik Duvarı ve Yönlendirici üzerine, saldırı sonucu dinamik kurallar koyabilirler
- Köprü (Bridge) modunda çalışarak kendilerini gizleyebilirler
- SMS, Pager, WinPopup, Sistem Kaydı, XML ve Veritabanı gibi uyarı ve kayıt çıktıları sağlayabilirler

Siyah Şapka Güvenlik Çözümleri

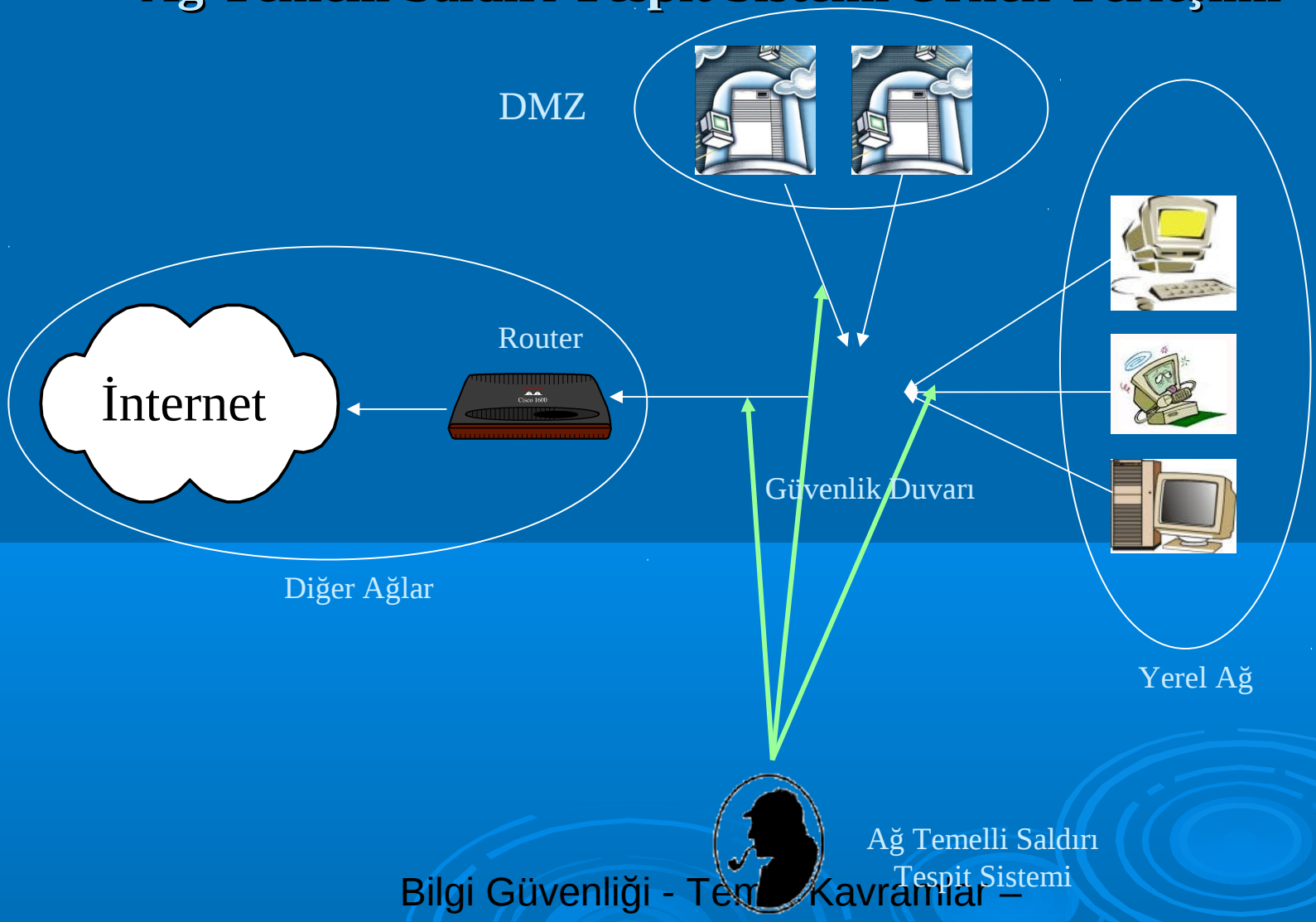
Saldırı Tespit Sistemleri (Sunucu Temelli ve Saldırı İmzası Arama)

- Özel dosyaları, sistem kayıtlarını ve sürücülerini izleyerek, değişiklikleri rapor edebilirler
- Tanımlı olan imzalar ile saldırıları belirlerler
- Sistemde aktif bulunan işlemleri takip edebilirler
- Gerekli görüldüğü durumlarda erişimleri engelleyebilir, servis durdurabilir ve başlatabilirler
- SMS, Pager, WinPopup, Sistem Kaydı, XML ve Veritabanı gibi uyarı ve kayıt çıktıları sağlayabilirler

Saldırı Tespit Sistemleri Neler Yapamaz

- Erişim Denetimi Yapamaz
- Tanımlanmamış Saldırıları Saptayamaz
- Virüsleri Saptayamaz
- Zayıflıkları Saptayamaz, Yamalayamaz
- Ağlar Arası İletişimde Şifreleme Yapamaz
- Yoğun Ağ Trafiğinde Performansları Düşer
- Şifrelenmiş Veriyi İnceleyemez

Ağ Temelli Saldırı Tespit Sistemi Örnek Yerleşimi



Sunucu Temelli Saldırı Tespit Sistemi Örnek Yerleşimi

Pine ile e-posta okuma

/etc/shadow Dosyasını Okuma

Kernel'da Bellek Taşırmaya Çalışma

Sunucu Temelli Saldırı Tespit Sistemi

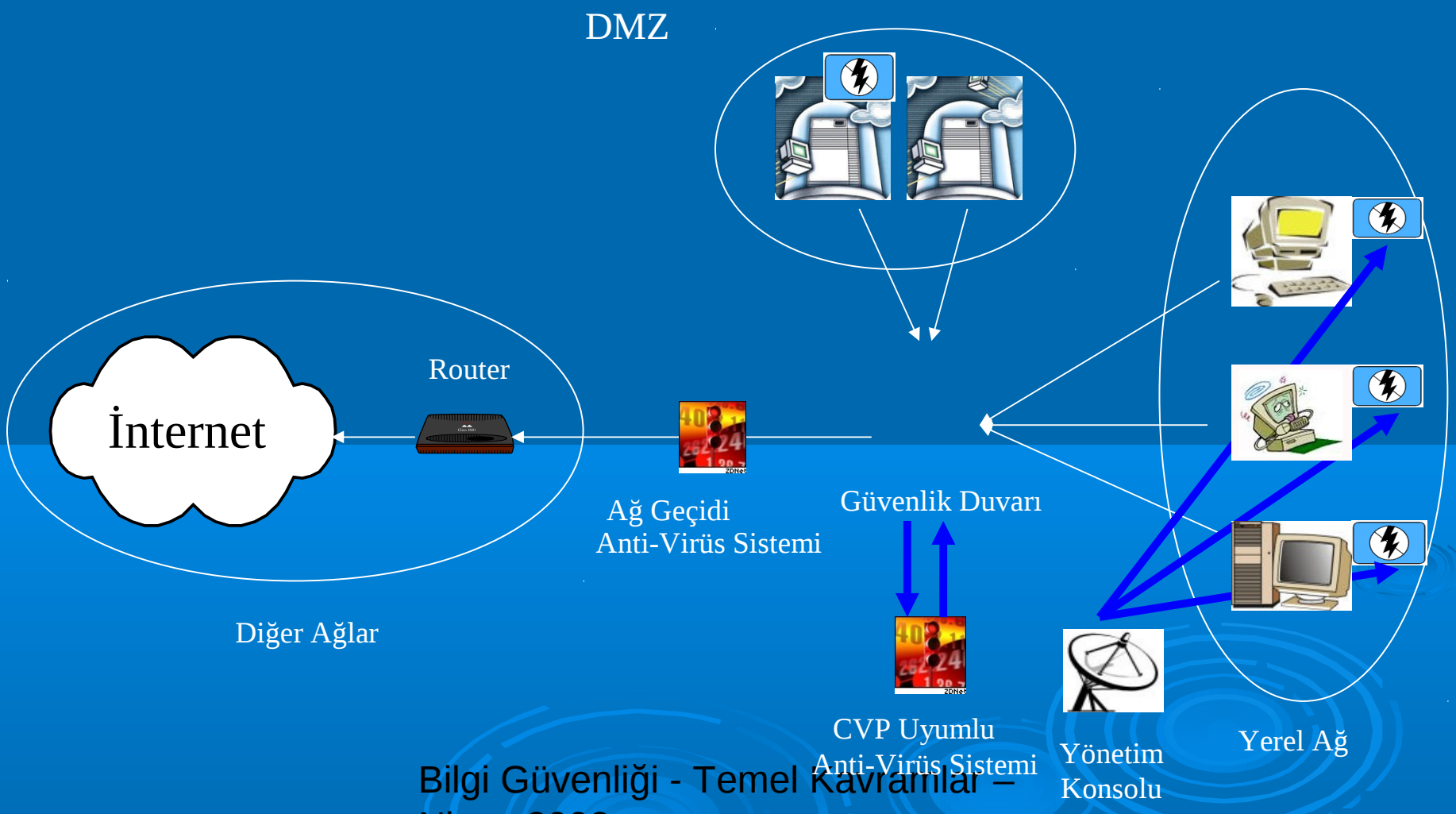
Anti-Virüs Sistemleri

- Virüs, Worm ve Trojanları tanımlı imzaları ile saptarlar
- İmzaları tanımlanmanmış virüsleride çeşitli yöntemler ile saptayabilen örnekleri mevcuttur
- Virüs imzaları bir veritabanında tutulur ve İnternet aracılığıyla düzenli olarak güncellenir
- Ağdaki tüm sistemleri korumadıkça anlamlı değillerdir
- Bir ağ parçasını, belirli bir trafiği, bir sunucu yada bir istemciyi koruyabilirler

Anti-Virüs Sistemi Neler Yapabilir – Yapamaz

- Tanımlanmamış Virüsleri Saptayabilir
- Tek Merkezden Yönetilebilir
- Ağ Geçidi Olabilir
- Bridge (Köprü) Moda Geçebilir
- Güvenlik Duvarları İle Beraber Çalışabilir
- Worm Saldırılarını Engelleyemez
- Şifrelenmiş Dosyalarda Virüs Saptayamaz
- Erişim Denetimi Yapamaz
- Saldırıları Saptayamaz
- Zayıflıkları Saptayamaz / Yamalayamaz

Anti-Virüs Sistemleri Örnek Yerleşimi



Sanal Özel Ağ Sistemleri

- Birden fazla sistem veya ağın, güvensiz ağlar üzerinden, güvenli iletişimini sağlayan ağ bileşenleridir
- Donanım ve yazılım olarak bulunabilirler
- IPSec, PPTP, L2TP, SSH gibi protokolleri kullanarak iletişimin şifrelenmesini sağlarlar
- Harici onaylama sistemleri ile beraber kullanılmaları önerilmektedir

Sanal Özel Ağ Sistemleri Neler Yapabilir – Yapamaz

- Erişim Denetimi Yapabilir
- Veri Trafiğini Farklı Algoritmalarla Şifreleyebilir
- Üçüncü Parti Yazılımlar İle Beraber Çalışabilir
- Saldırıları Engelleyemez
- Virüsleri Engelleyemez
- Zayıflıkları Saptayamaz, Yamalayamaz

Şifreleme Sistemleri

- İnternet ortamında verilerin güvenli şekilde aktarımını, bütünlüğünü ve gönderenin doğruluğunu sağlamaktadırlar
- Mail, Dosya, Disk ve Veri trafiğini şifreleyebilmektedirler
- Des, MD5, 3Des, Sha-1 gibi çeşitli algoritmalar kullanmaktadırlar

Sistem Güçlendirme (Hardening)

- Sunucuların Ele Geçirilme İhtimallerini Azaltmak veya Ele Geçirildiğinde Saldırganın Hareket Alanını Kısıtlamak İçin Yapılır
- Kritik Dosyalara ve Donanımlara Erişim Kısıtlanır
- Kullanıcı ve Grupların Yetkileri ve Şifre Politikaları Düzenlenir
- Sisteme Var Olan Tüm Yamalar Uygulanır
- Gerekli Olmayan Yazılımlar ve Servisler Sistemden Çıkarılır
- Sistem İzleme Politikaları Belirlenir ve Uygun Kayıt Tutma Mekanizması Seçilir

Doğrulama ve Yetkilendirme Sistemleri

- Tek Merkezden Doğrulama ve Yetkilendirme Yapılması Hedeflenmektedir
- Kullanıcı ve Yetki Doğrulaması Yapılır
- Sertifika, Biometrik Cihazlar, Tek Kullanımlık Şifreler, Doğrulama ve Yetkilendirme Sistemleri Tarafından Kullanılabilir
- Güvenlik Duvarları ve Sanal Özel Ağ Sistemleri İle Bütünleşik Çalışabilirler

İçerik Kontrol Yazılımları

- Web Sayfalarının İçeriğinin Kontrol Edilmesini Hedeflerler
- Porno, Oyun, Siyasi ve Tehdit İçerebilecek Siteleri Filtrelemektedirler
- Bir Veritabanı Aracılığıyla Düzenli Olarak Site Adresleri Güncellenir
- Güvenlik Duvarları veya Proxy Yazılımları İle Bütünleşik Çalışabilirler

Yedekleme Sistemleri

- Merkezi Olarak Veri ve Sistem Yedeklemesi Hedeflenmektedir
- Artımlı Yedekleme, Toplam Yedekleme Gibi Farklı Politikalarla Yedekleme Yapılmaktadır
- Özel Donanımlar İle Ağ Üzerindeki Tüm Sistemlerinin Yedeklenmesi Sağlanabilmektedir
- Yedekler Düzenli Olarak Kontrol Edilmeli ve Kayıt Ortamı Sürekli Olarak Değiştirilmelidir
- Yedeklerin Fiziksel Güvenliği Sağlanmalıdır

Denetleme ve İzleme

- Ağın, Belirlenen Güvenlik Politikalarına Uygunluğu Test Edilmeli ve Düzenli Olarak Erişimler İzlenmelidir
- Merkezi Kayıt Sistemleri Kurulmalıdır
- Güvenlik Uygulamaları Tarafından Tutulan Kayıtlar Düzenli Olarak İzlenmelidir
- Denetleme ve İzleme İşlemleri Düzenli Olarak Raporlanmalı ve Geçmişe Dönük Karşılaştırmalar Yapılmalıdır

Denetleme ve İzleme Uygulamaları

- Ağ İzleme Yazılımları
- Zayıflık Tarama Sistemleri
  - Ağ Temelli Zayıflık Tarama Sistemleri
  - Sunucu Temelli Zayıflık Tarama Sistemleri
  - Uygulama Temelli Zayıflık Tarama Sistemleri
- Kayıt Tutma ve Raporlama Yazılımları
- Ağa Sızma Testleri

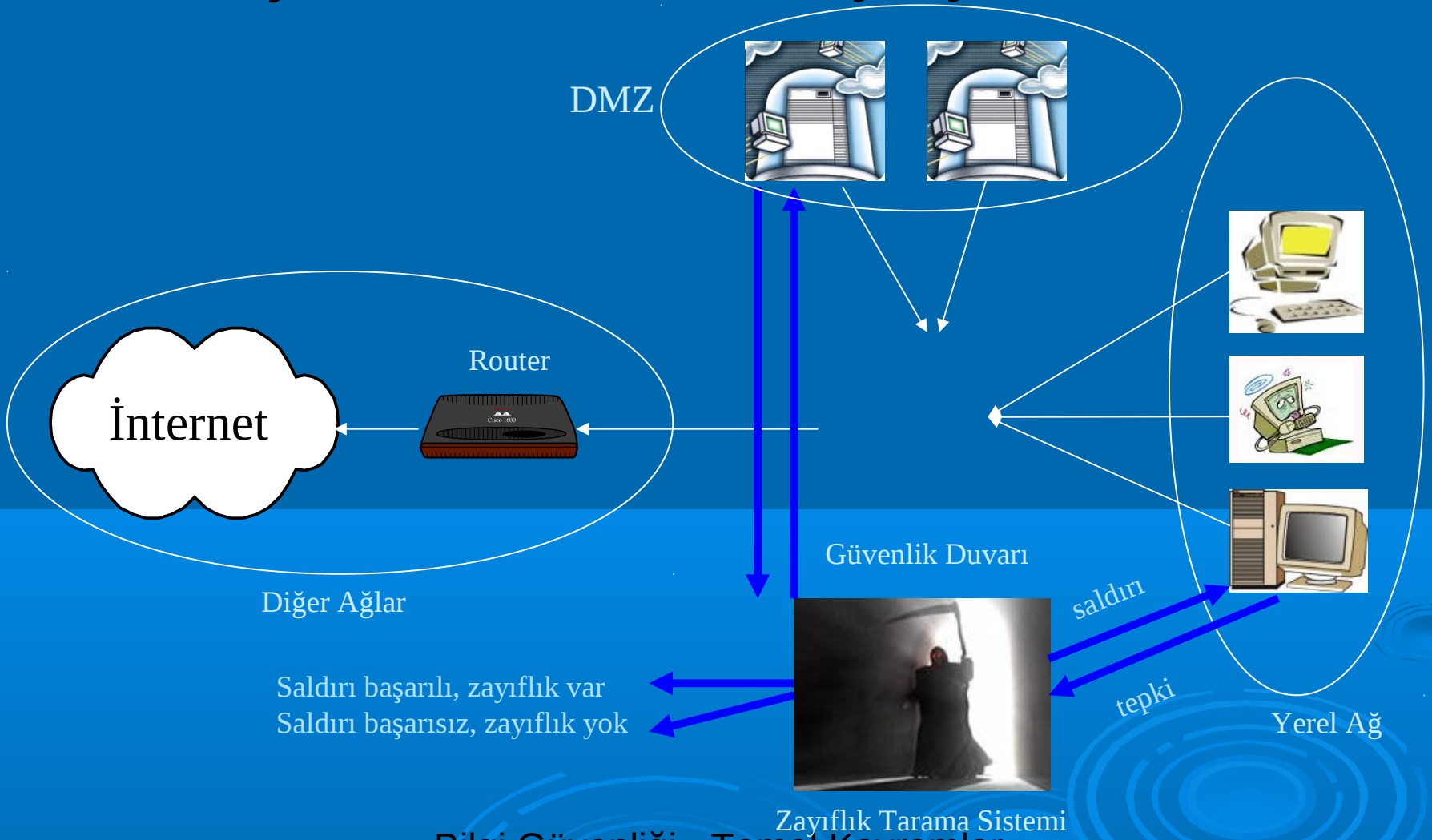
Ağ İzleme Yazılımları

- Ağ üzerinde Sniffer gibi çalışarak aktif olan protokollere dair istatistikler tutmaktadırlar
- Ağda Sorun Gidermeyi ve Performans Arttırıcı İpuçlarını Sistem Yöneticisine Vermeyi Hedeflerler
- Ayrıca ağ üzerindeki şifrelenmemiş verileri ve protokolleri yakalamayı ve incelemeyi sağlarlar

Zayıflık Tarama Sistemleri

- Yayınlanmış, bilinen uygulama ve sistem zayıflıklarını test eden araçlardır
- Veritabanlarında bulunan zayıflıkları hiçbir özel yöntem uygulamadan test etmektedirler
- Zaman içerisinde oluşabilecek zayıflıkları düzenli takip etmeyi sağlarlar
- Script dilleri sayesinde yeni zayıflıklar kolayca tanımlanabilir
- 3 farklı mimaride çalışabilirler : Ağ Temelli, Uygulamaya özel ve Sunucu Temelli

Zayıflık Tarama Sistemi Çalışma Prensibi



Kayıt Tutma ve Raporlama Yazılımları

- Merkezi Kayıt Sunucusu Oluşturmayı Hedeflemektedirler
- Ağ Üzerinde Kayıt Aktarımını Şifreli Olarak Sağlayabilirler
- Farklı Sistemlerde Tutulan Kayıtları Özelleştirebilir ve Gruplayabilirler
- Raporları Belirli Özelliklerine Göre Grafiklerle İfade Edebilirler

Ağa Sızma Testleri

- Kurum Dışı Kişiler Tarafından, Bir Saldırganın Uyguladığı Yöntemler İle Ağa Saldırılması Anlamına Gelmektedir
- Denetleme ve İzleme İşlemlerinin Son Adımıdır
- Tüm Ağ ve Servis Yerleşimi Tamamlandıktan Sonra Yapılmalıdır
- Çeşitli Yazılımların Kullanımına Ek Olarak İnsan Unsuru Öne Çıkmaktadır

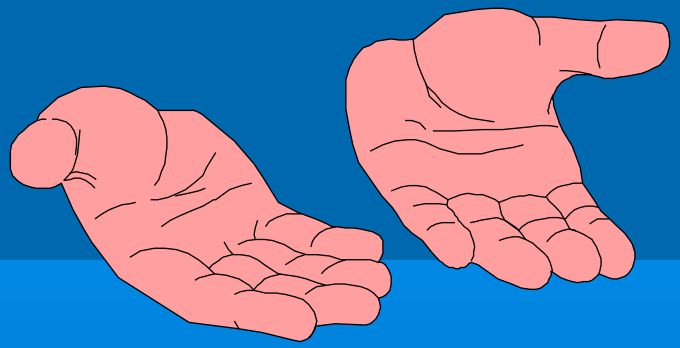
Sistem Yöneticilerinin Yaptığı En Büyük Hatalar

- Sistemde gerekli önlemleri uygulamadan ve yapılandırmayı tamamlamadan, sistemi internete bağlamak
- Sisteme kurulan uygulamaları varsayılan yapılandırmaları ve varsayılan şifreleri ile kullanmak
- Sisteme gerekli güncelleme ve yamaları (yayınlandığı halde) uygulamamak ve eski sürümlerle çalışmak
- Sistemi yönetirken güvensiz protokoller kullanmak (telnet, nfs vb.)
- Kullanıcıdan emin olmadan şifresini vermek
- Sistemde yapılması gerekli olan yedeklemeleri yapmamak, alınan yedekleri kontrol etmemek
- Sistemin hizmeti sırasında gerekli olmayan servisleri çalıştırmak (nfs, telnet, ftp, portmap, finger vb.)
- Güvenlik duvarı yapılandırırken tüm paketlere izin vermek
- Anti-Virüs Yazılımlarının, İçerik Kontrol Yazılımlarının ve Saldırı Tespit Sistemlerinin veritabanlarını güncellememek veya bu yazılımları kullanmamak
- Çalışanları güvenlik politikası konusunda bilinçlendirmemek, tehlikeli durumlarda ne yapabileceği konusunda eğitmemek
- Sistemi, eğitimini tamamlamamış çalışanlara emanet etmek

Kaynaklar

CERT – http://www.cert.org
SANS – http://www.sans.org
Security Focus – http://www.securityfocus.com
Siyah Şapka – http://www.siyahsapka.com
Dikey8 – http://www.dikey8.com
Olympos – http://www.olympos.org
Güvenlik Haber – http://www.guvenlikhaber.com

Sorular ?



Teşekkürler ....