BİLGİ GÜVENLİĞİ AKADEMİSİ

www.guvenlikegitimleri.com

Güvenlik Mühendisliği

Huzeyfe ÖNAL
Bilgi Güvenliği AKADEMİSİ
honal@bga.com.tr

www.bga.com.tr

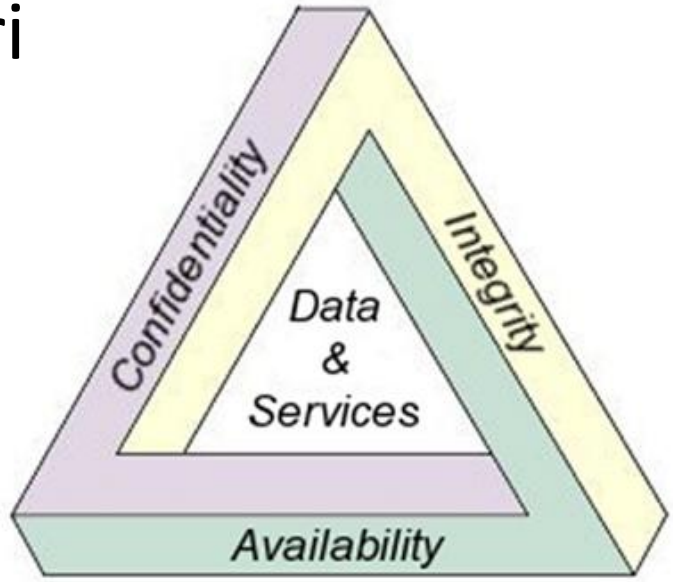
Sunum içeriği

- Güvenlik kavramı
- Türkiye’de güvenliğe yaklaşım
- Güvenlik bileşenleri
- Güvenlik konusunda kariyer imkanları

Güvenlik Kavramı

– “CIA”

- Var olan maddeyi, bilgiyi koruma ihtiyacı
- Koruma yöntemleri ve çeşitleri
- Fiziksel Güvenlik
- Sanal Güvenlik



Türkiye’de Güvenliğe Yaklaşım

- 2000’li yılların başından itibaren gelişme gösteren bir sektör
  - 2000’li yıllarda Güvenlik duvarı kullanan şirket oranı %10
  - Günümüzde bu durum ~ %90 civarlarında
- Bilgisayarların ve bilgisayarlı iletişimin artması ile paralel ilerleme
- Hazır ürünleri al-sat şeklinde ilerleyen bir ticari yapı
  - Bunun etkisi ile hazır ürünleri kullanan, ezberci güvenlik yöneticileri
- Arge çalışmaları yok denecek kadar az.
- Gelecekte çok da farklı olmayacağı bugünden belli olan, sektörün kaymağı niteliğinde

Güvenlik Çeşitleri

- Eskiden bilişim güvenliği tek başına ele alınan bir olguydu
- Zamanla kendi içerisinde alt dallara ayrıldı
  - Ağ güvenliği
  - Web Uygulama Güvenliği
  - İşletim sistemi güvenliği
- UNIX/Linux sistem güvenliği
- Windows sistem güvenliği
  - Veritabanı Güvenliği

False Sense Of Security

Ağ Güvenliği

- Şirketlerin dış dünyaya açılan kapısı
  - Ülkeler için sınır güvenliği mahiyetinde.
  - Katmanlı Güvenlik Mimarisi
- Eve ulaşımda ilk aşama bahçe kapısı,
  - Bahçe duvarlarına izinsiz girişimi engelleme için çit yerleşimi
  - Evin giriş kapısı, kapı kilitleri
  - Evin pencereleri , pencere korkulukları
  - Eve izinsiz girişleri belirleyen Alarm sistemleri…
- En hassas ve önemli güvenlik bileşeni
  - Ağ güvenliği bileşeni olmadan diğer bileşenler işe yaramaz

Ağ Güvenliği Bileşenleri

- Yönlendirici Cihazlar (Router)
- Güvenlik Duvarları (Firewall)
- Saldırı Tespit ve Engelleme Sistemleri (IDS / IPS)
- Anormallik tespit sistemleri (ADS)
- Kablosuz ağ cihazları
- WAF (Web Application Firewall)
- Tüm bu sistemleri yönetecek mühendisler
  - Genelde unutulsa da en önemli bileşen ☺

Yönlendirici Cihazlar

- En temel ağ bileşeni
- Amaç: ağlar arası paket yönlendirme
- Temel paket filtreleme işlemleri
  - Ip ve port bazında filtreleme yapabilir.
  - Katmanlı güvenlik anlayışının ilk bileşeni.

Güvenlik Duvarları-I

• Olmazsa olmaz güvenlik bileşenlerinden

– Yönlendirici benzeri koruma yetenekleri

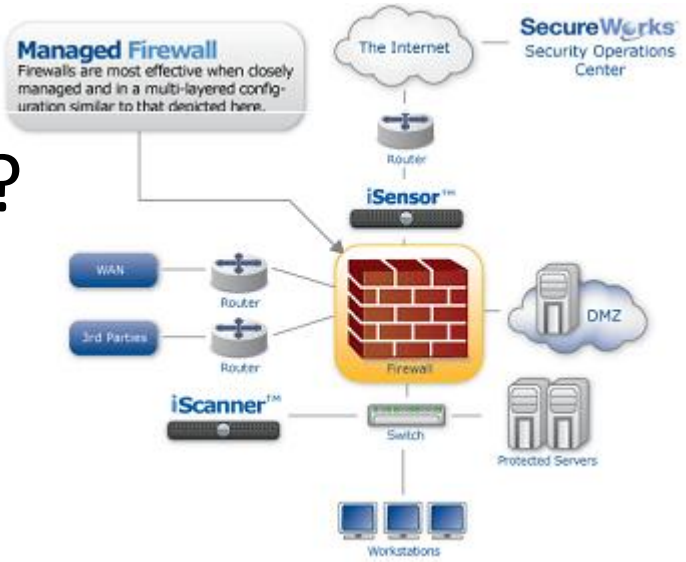
• İp, port, tcp bayrakları, anormal bağlantıları sonlandırma yeteneği vs.. sonlandırma yeteneği vs..

– Yönlendirici ile güvenlik duvarı benzer işlevleri yapsalar da temelde her ikisinin görevi de farklıdır!!

<u>* Çeşitleri:</u>

• Paket filtreleme, proxy firewallar, uygulama seviyesi firewallar, donanım firewallar, yazılım firewallar, masaüstü firewallar, web uygulama firewalllar.

Güvenlik Duvarları-II



- Güvenlik duvarları ne yapamaz?

– Paket içeriği kontrolü yapamaz,

yapmamalıdır!

- Bu sebeple karmaşık saldırılara karşı etkisiz

eleman rolü oynarlar

Güvenlik duvarları ile çalışma

- Açık kaynak kod öncesi çağlarda böyle bir imkan yoktu !

- Güvenlik duvarları genellikle donanımsal sistemlerdi.
  - Donanımsal ve yazılımsal güvenlik duvarları farkı?
- Günümüzde ?

Linux/UNIX tabanlı Güvenlik Duvarı

- Modern güvenlik duvarları ile yarışabilir düzeyde
- Kullanım için bir maddi/manevi kısıtlama yok (Özgür yazılım)
  – Evdeki iki bilgisayarı koruma amaçlı da olabilir
  – 5000 kullanıcılı bir şirketi koruma amaçlı da…
- Güvenlik duvarı çalışma şeklini ve arkasında yatan mantığı kavramak için ideal tercih.
- Linux Iptables
- OpenBSD Packet Filter
- IPF

Saldırı Tespit ve Engelleme Sistemleri

- Router ve Firewall sistemlerin yetersiz kaldığı durumlar:
  - Eskiden saldırılar daha çok network tabanlı olurdu.
  - Router ve firewalların kullanımı ile birlikte siyah şapkalılar yöntem değiştirdiler ve uygulama spesifik saldırı devri başladı.
  - Mesela 25. portta çalışan Sendmail uygulamasının X bileşenini etkileyen bir saldırı .
- Sendmail uygulamasına gönderilen ehlo komutuna parametre olarak 1000 adet A verirsek sistem çalışamaz duruma gelir(örnek)
- 25. portunuz dışarıya açık olmak zorunda
  - Firewall devre dışı kaldı…
  - O portta çalışan ve uygulamadan anlayan, paketlerin içeriğine bakabilen bir sistem ihtiyacı doğdu.
- Gerçek dünyadaki karşılığı, evlere ya da araçlara takılan “alarm sistemi”.

IDS(Intrusion Detection Systems)

- Güvenlik duvarlarının yetersizliği sonrası IDS kavramı ortaya çıktı
- Alarm sistemlerinde öncelikli hedef saldırının belirlenmesidir, saldırının engellenmesi değil.
- Çalıştığı konuma göre isimlendirilirler
  - Host tabanlı IDS sistemler
  - Ağ tabanlı IDS sistemler
- Açık kaynak kodlu IDS yazılımı: Snort

IPS(Intrusion Prevention Systems)

• Sadece belirlemek yetmez, engellemek lazım düşüncesinin ve piyasanın istekleri sonucu ortaya çıkmış bir teknoloji.

• Günümüzdeki ağ koruma katmanlarında en güvenilir bileşen(?)
• İç rahatlatıcı, sihirbazımsı özellikleri vardır.
  – Kutuyu koy ve rahatla…
• Yeterli önem verilmediği takdirde etkisiz eleman rolünü iyi oynarlar

• Karmaşık web ataklarına karşı yeterli koruma sağlayamıyor

Anormallik Tespit Sistemleri (ADS)

- IDS sistemlere temel oluşturur
- Bilimsel olarak eski ancak uygulama olarak yeni
- Makine, servis, uygulama ve ağ temelli
- Anormal aktiviteler
- Açık kodlu bir çözüm ? Ourmon
- Cisco Anomaly Detection System, IBM ISS ADS

Web Güvenliği

- Interneti internet yapan teknoloji:web sayfaları
- Internet üzerinden işlem yapan her firmanın mutlak surette ihtiyacı olan bir sistem
- Şirketlerin en hassas ve korunmasız alanları
  - Zincirin en zayıf halkası da denilebilir
- Basit bir hata diğer tüm önlemleri geçersiz kılabilir.
  - Örnekler…

Web Güvenliği Bileşenleri

- Güvenli kod yazımını bilen çalışanlar.
  - Programlama/Yazılım mühendisliği derslerindeki öğretiler??
- Kullanılan dil ve veritabanı özellikleri
- Web uygulama güvenlik duvarları
  - Son çare
  - Normal güvenlik duvarlarından farklıdır.

Bilişim Güvenliği Alanında Kariyer İmkanları

- Sektörün en gözde dallarından
  - Bir şeyleri ortaya koyduktan sonra koruma ihtiyacı dürtüsü…
- Sektör tecrübeli elemanlara ihtiyaç duyuyor…
- Memnuniyet oranı en yüksek çalışanlar ☺
- Yazılım mühendisliğinden farklı olarak tecrübe kolay kazanılmıyor
  - Uygulama alanları dar!!
  - Yardım alınabilecek yerli ve tecrübeli kaynak eksikliği

BT Güvenliği Kariyeri Yolunda Bir Mühendisin Yol Haritası

- Gelecekteki hedefi belirleme ve bu konuda sebat etme.
- Hedefe daha önce varmış tecrübeli çalışanlardan destek isteme, istişare. çalışanlardan destek isteme, istişare.
- Öğrenilmesi gerekenleri ve öğrenilmesi iyi olanların listesini çıkarma
  - Önem sırasına sokma.
  - Paket analizi öğrenmeden IDS kullanmaya kalkmak!

BT Güvenliği Kariyeri Yolunda Bir Mühendisin Yol Haritası

- Linux bilme zorunluluğu
  - İstisnalar kaideyi bozmaz!
  - Bu yolda iyi bir eleman olmanın kaçınılmaz şartı: Linux ve özgür yazılımları kullanabilme.
  - İş ortamlarında kullanılan sistemlerin çalışma yöntemlerini anlamanın en iyi yolu.
- Pratik geliştirme için uygulama ortamları
  - Sanal uygulama ortamları
  - Vmware, Xen vs.
- Kitap, makale okumaları, ilgili e-posta listelerinin takibi.
  - enderunix, linux.org.tr, Netsec (netsec.lifeoverip.net)

Kaynaklar

- Kaynak siteler
  - http://csirt.ulakbim.gov.tr
  - www.olympos.org
  - www.enderunix.org
  - www.lifeoverip.net
  - http://netsec.lifeoverip.net
  - www.bilgiguvenligi.gov.tr
  - www.beyazsapka.org
- Güvenlik Eğitimleri
  - http://www.bga.com.tr

Teşekkür Ederiz...