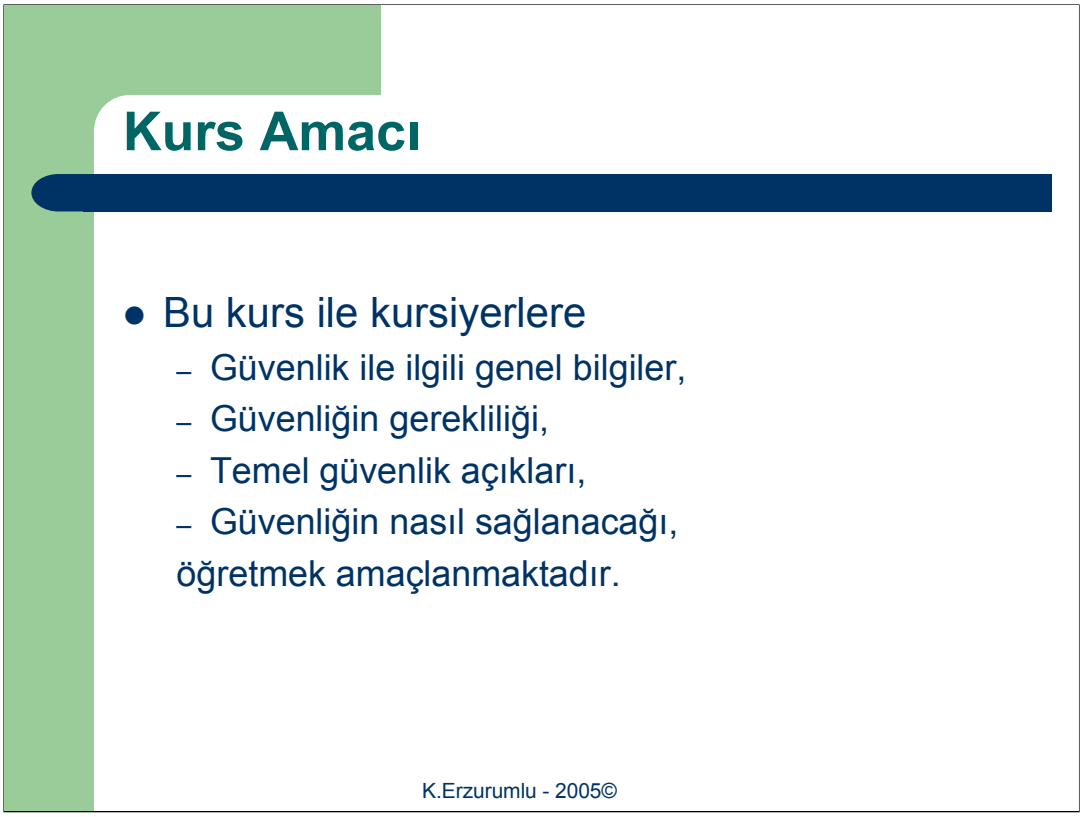
İçindekiler

Güvenliğin Temelleri

Ünite 1
Genel Kurs Bilgileri

Güvenliğin Temellerinin anlatılacağı eğitim seminerlerinin başlangıç noktası olan bu ünitede katılımcılara kurs içeriği hakkında bilgi sunulacak ve eğitim programı/takvimi hakkında bilgi verilecektir.



"Güvenliğin Temelleri" kursu ile kurs katılımcılarına genel güvenlik kavramı, bilgisayar ağları ve ağlarda güvenlik kavramlarının açıklanması amaçlanmıştır. Bu bağlamda kurs süresince uygulamalı olarak güvenlik hakkında genel bilgiler verilecektir.

Kursiyer Sorumlulukları

- Kursiyerlerden “temel bilgisayar okur-yazarlığı” ve bilgisayar ağları ile ilgili temel kavram bilgisine sahip olmaları beklenmektedir.

“Güvenliğin Temelleri” kursuna katılabilmek için kursiyerlerin temel bilgisayar okur-yazarlığı bilgisine sahip olmaları yeterlidir.

Kurs içeriğinin ilk 8 ünitesi sırası ile yukarıda listelenmiştir. Bu ünitelerin içerikleri ise;

I. Kurs Genel Bilgileri (1 Saat)

Şu an işlenmekte olan ünitedir. Bu ünite kapsamında genel kurs bilgileri verilecektir.

II. Güvenlik Nedir? (2 Saat)

Bu ünite kapsamında "Güvenlik" kavramının tanımı yapılacak, ne amaçladığı açıklanacaktır. Bu bağlamda gerekli açıklamaların yapılmasını takiben, bir genelleme yapılarak bilgisayarlar üzerinden gerçekleşen saldırıların türleri, amaçları ve kimler tarafından gerçekleştirildiği açıklanacaktır.

III. Toplum Mühendisliği (2 Saat)

Tüm kurs kapsamında anlatılacak olan konuların hepsinin temelinde toplum mühendisliği yatmaktadır. Halk dilinde "korsan" (ing. *Hacker*) olarak adlandırılan bu kişiler "bilgi kırıntıları"nı ve "insani zaafları" kullanarak karşılarındaki kişiyi kandırır ve kendilerine yardımcı olunmasını sağlarlar. Bu ünite kapsamında toplum mühendislerinin kullanmakta olduğu genel yöntemler örnekleri ile anlatılacak ve toplum mühendislerinden sakınma yollarına değinilecektir.

IV. Yetkilendirme (2 Saat)

Bu ünite kapsamında güvenliğin sağlanabilmesi için uygulanması gereken yetkilendirme yöntemleri, bu yetkilendirme yöntemlerine kullanılan ACL ve VLAN kavramları açıklanacaktır. Ünitenin son kesiminde ise kullanıcı onaylama mekanizmaları ve kullanım yerlerine değinilecektir.

V. Şifreleme Yöntemleri (1 Saat)

Güvenliği sağlamak için kullanılması zorunlu olan şifreleme işlemi

matematiksel işlemlere dayanmakta ve “geri dönüşümsüz” ve “geri dönüşümlü” (matematiksel adları ile asimetrik/simetrik algoritmalar) algoritmalar aracılığı ile yapılmaktadır. Bu ünite kapsamında bu şifreleme yöntemleri kabaca açıklanacak ve detaylara girilmeyecektir.

VI. Güvenlik Politikaları (1 Saat)

Kurum içerisinde güvenliğin sağlanabilmesi için öncelikle tam anlamı ile düşünülmüş, tasarlanmış ve yazılmış bir güvenlik politikası gereklidir. Bu başlık altında güvenlik politikası oluşturulurken dikkat edilmesi gerekenler açıklanacaktır.

VII. TCP/IP Genel Bilgileri (2 Saat)

Tam anlamı ile ileri düzey güvenlik sağlayabilmek için öncelikle TCP/IP ile ilgili temel bilgilerin bilinmesi gerekmektedir. Bu ünite kapsamında OSI katmanları, Fiziksel Adresler, ARP, Yönlendirme ve Yönlendirme protokolleri gibi giriş düzeyi TCP/IP bilgileri sunulacaktır.

VIII. Ağ Cihazları (1 Saat)

Farklı OSI katmanlarında çalışan cihazlar ve güvenlik ile ilgili yönleri bu ünite kapsamında açıklanacak ve güvenli ağ tasarımlarında ne tür cihazların kullanılması gerektiği açıklanacaktır.

Kurs içeriğinin son 8 ünitesi sırası ile yukarıda listelenmiştir. Bu ünitelerin içerikleri ise;

IX. Saldırı Türleri ve Tespit Sistemleri (1 Saat)

Toplum mühendisleri gerekli bilgilere sahip olduktan sonra, hedef sisteme saldırmak çeşitli saldırılar yürütürler. Bu ünite kapsamında bilgisayar sistemlerine yapılan saldırılar, bu saldırıların türleri ve nasıl engellenebileceği açıklanacaktır. Bu saldırı türleri ve açıklamaları tamamlandıktan sonra "Saldırı Tespit Sistemleri" (ing. *Intrudition Detection Systems*) açıklanacak ve yerel ağlarda nasıl kullanılması gerektiği detaylandırılacaktır.

X. Güvenli Ağ Tasarım/Gerçekleştirim (1 Saat)

Güvenliğin en üst düzeyde tutulduğu bir ağın ve IP planlamasının temelleri bu ünite altında detaylı olarak incelenecektir.

XI. Uzaktan Erişim (1 Saat)

Yerel ağları ve bilgisayar sistemlerini yönetmek amacı ile acil durumlarda uzaktan erişimlerde bulunmak kaçınılmazdır. Fakat uzaktan erişim mekanizması güvenlik riskleri içermektedir. Bu ünite kapsamında bu riskler sıralanacak ve ideal uzaktan erişimin nasıl yapılması gerektiği açıklanacaktır.

XII. Kablosuz İletişim (1 Saat)

Güvenlik ve kablosuz iletişim birbirlerine tamamen zıt iki terimdir. İletişimin herkese açık bir şekilde yapılması nedeni ile iletilen bilgiler güvende değildir. Kablosuz iletişim'in cazibesinin yanında bu büyük dezavantajı bu ünitede açıklanacaktır.

XIII. Yedekleme (1 Saat)

Verilerin sayısal ortamda güvenliği ne kadar sağlanmış olursa olsun, en

kötü durumda bile fiziksel arızalar için yedek alınması ve bu yedeklerin düzenli olarak saklanması hayati önem taşımaktadır. Bu ünite kapsamında “Nasıl Yedek Alınmalı ve Saklanmalı” irdelenecektir.

XIV. Güvenlik Duvarları (2 Saat)

Günümüzde yanlış bir şekilde güvenlik ile özdeşleştirilmiş olan, tek başına güvenlik için yeterli olmayan fakat onsuz da güvenliğin olmayacağı “Güvenlik Duvarları” bu ünite kapsamında açıklanacak, çeşitli marka/modellerin özellikleri sıralanacak ve örnekler ile detaylandırılacaktır.

XV. Zayıflık Testleri (1 Saat)

Sunucu sistemlerin güvenli olup olmadığını değerlendiren zayıflık testleri ile ilgili bilgiler verilip, zayıflık testleri yapmakta olan programlar hakkında önbilgi verilecektir.

Genel Bilgiler

- Dersler;
  - 1 Ders = 50 dakika,
  - Her ders sonunda 10 dakika mola,
  - Bir günde 4 saat ders,
  - Toplam 5 gün eğitim.
- Kursiyerlere;
  - Ders notları içeren belgeler,
  - Güvenlik ile ilgili e-kitaplar içeren CD verilecektir.
  - Kursiyerlerin K.Mitnick'in "Aldatma Sanatı" adlı kitabı okuması tavsiye olunur.

K.Erzurumlu - 2005©

Toplam 20 saat olan eğitim 5 gün sürecek ve her gün toplam 4 saat ders işlenecektir. Her 50 dakikalık dersin sonunda 10 dakika mola verilecektir.

Ders saati içerisinde kursiyerlerin cep telefonlarını kapatmaları yada sessiz konuma getirmeleri gerekmektedir.

Bütün kursiyerlerimize ders notlarını içeren belgeler ve güncel güvenlik ile ilgili e-Kitapların bulunduğu bir CD takımı hediye edilecektir.

Eğitmen

- Kerem Erzurumlu
  - H.Ü. Bilgisayar Mühendisliği 2000 Mezunu,
  - Haziran 2004'de "Yüksek Mühendis"
  - H.Ü.B.M.'de doktora programına devam etmekte,
  - İş Deneyimi;
    - H.Ü. Bilgi İşlem Daire Başkanlığı – Sistem Yöneticisi (2 Yıl)
    - YimpaşNet İnternet A.Ş. – Sistem/Ağ Yöneticisi (1 Yıl)
    - O.D.T.Ü. – Sistem/Ağ Yöneticisi (2 Yıl)
    - H.Ü. Bilgisayar Mühendisliği – Sistem/Ağ Yöneticisi (4 Yıl)
    - Mezuniyetinden itibaren vermekte olduğu özel dersler

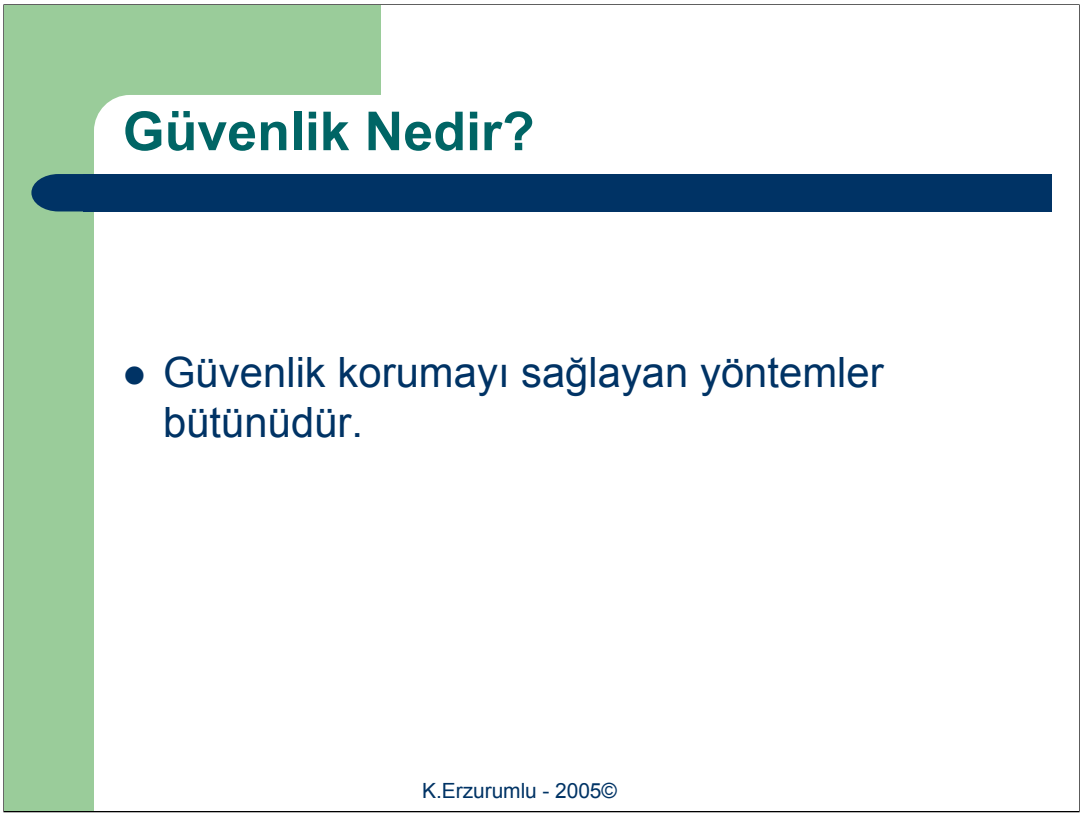
Kerem Erzurumlu'nun erişim bilgileri;
http://www.penguen.net
E-Posta: kerem@linux.org.tr
Telefon: +90 312 2977500 – 122
Fax: +90 312 2977502
GSM: +90 532 2539074

Güvenliğin Temelleri

Ünite 2

Güvenlik Nedir?

Bu ünite kapsamında “Güvenlik” kavramının tanımı yapılacak, ne amaçladığı açıklanacaktır. Bu bağlamda gerekli açıklamaların yapılmasını takiben, bir genelleme yapılarak bilgisayarlar üzerinden gerçekleşen saldırıların türleri, amaçları ve kimler tarafından gerçekleştirildiği açıklanacaktır.



Güvenlik denildiğinde çoğunlukla akla mevcut yasaları uygulayan kolluk kuvvetleri gelmektedir. Ama gerçekte "Güvenlik" kelimesi "korumayı sağlayan kurallar ve yöntemler bütünüdür." olarak algılanmalıdır. Dolayısı ile güvenlik tanımı,

•neyi koruyacağını,

•ne amaçla koruyacağını,

•kimlerden koruyacağı,

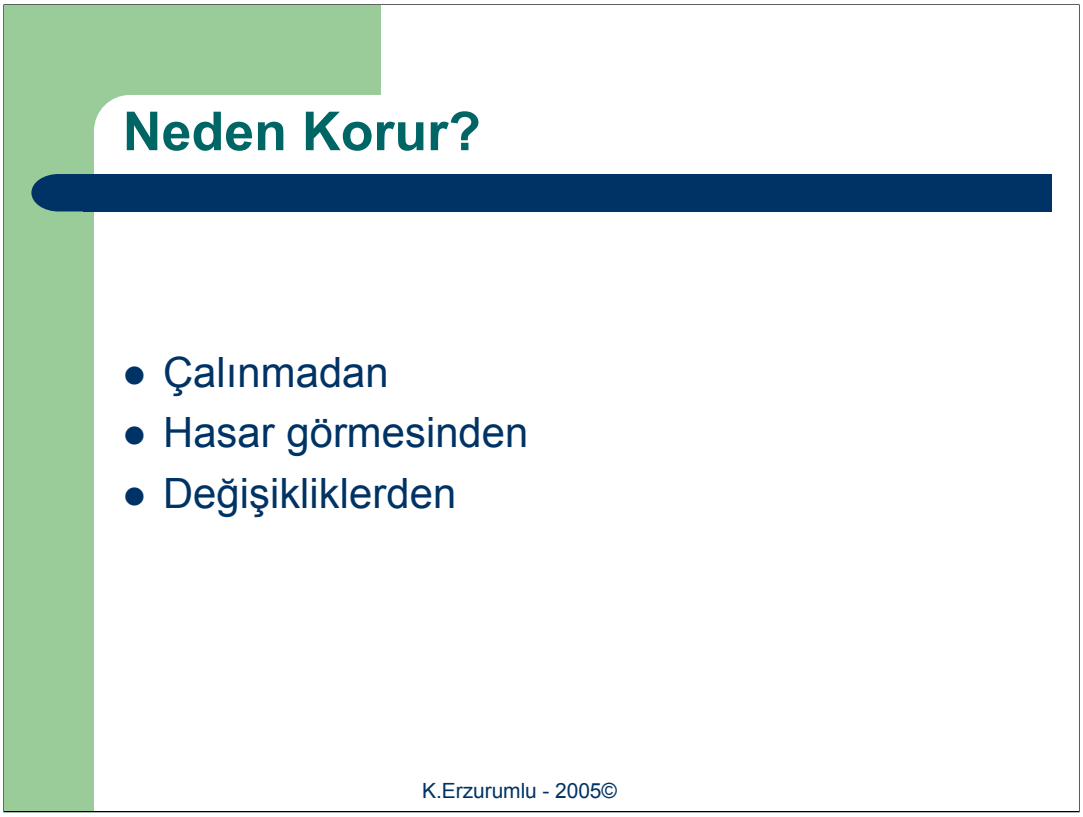
•nasıl koruyacağı içerir.

Neyi Korur?

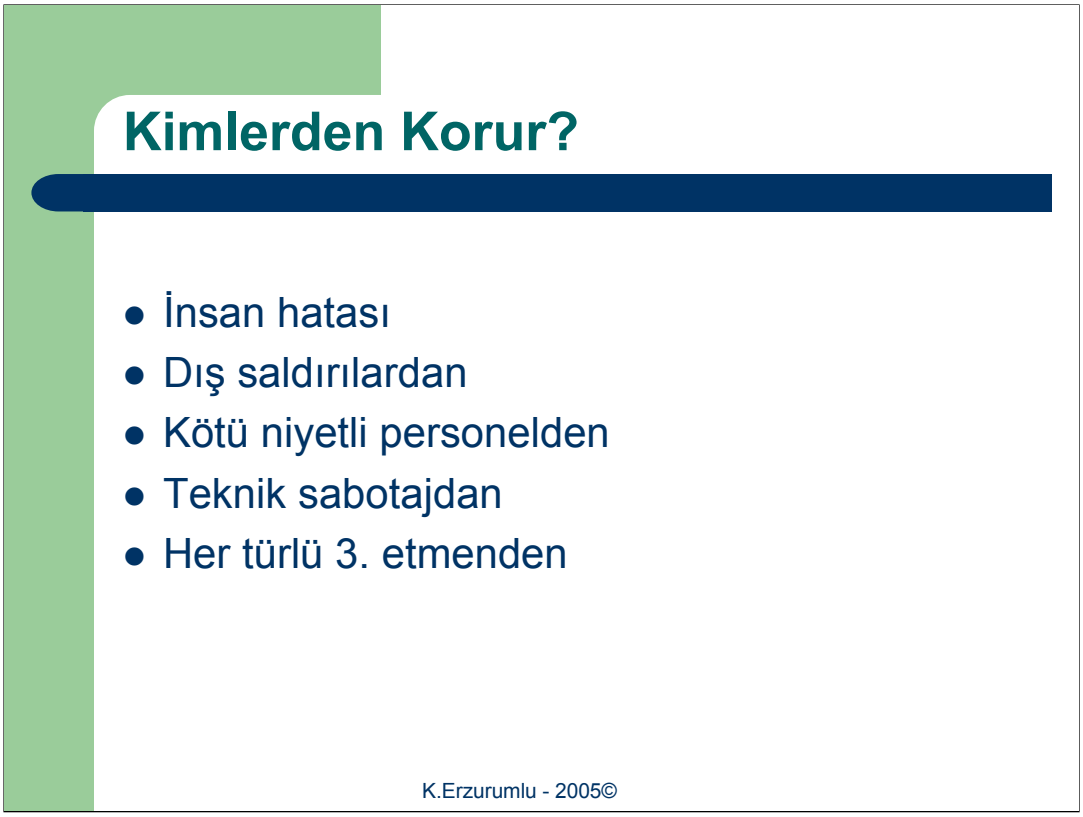
- Firmaları, firma çalışanlarını ve müşterilerini
- Evrak ve elektronik belgeleri
- Yazılım ve donanımlarınızı

K.Erzurumlu - 2005©

Güvenlik ile amaçlanan kurumlar için maddi manevi değeri olan tüm elektronik yada yazılı her türlü meteryal korunmalıdır. Bu meteryaller her kuruma göre farklılık göstermektedir. Bir e-satış sitesinde en kritik bilgi müşteri bilgileri, onların kredi kartı numaraları ve kişileirn iletmiş olduğu siparişlerdir. Bir belediye içinse Hesap İşleri Kayıtları ve Tapu/İmar bilgileri üzerlerinde yetkisiz işlem yapılması istenmeyen bilgilerdir.



Kurum bünyesinde barındırılmakta olan verilere saldırganlar çoğunlukla verilerin “çalınması”, “hasar görmesi” yada “ değiştirilmesini” amacı ile saldırırlar. Örnek olarak bir e-ticaret sitesinden “Kredi kartı” bilgilerinin çalınması, tahsilatı yapılmış siparişlerin değiştirilmesi göze alınamayacak prestij kaybı riskleridir.

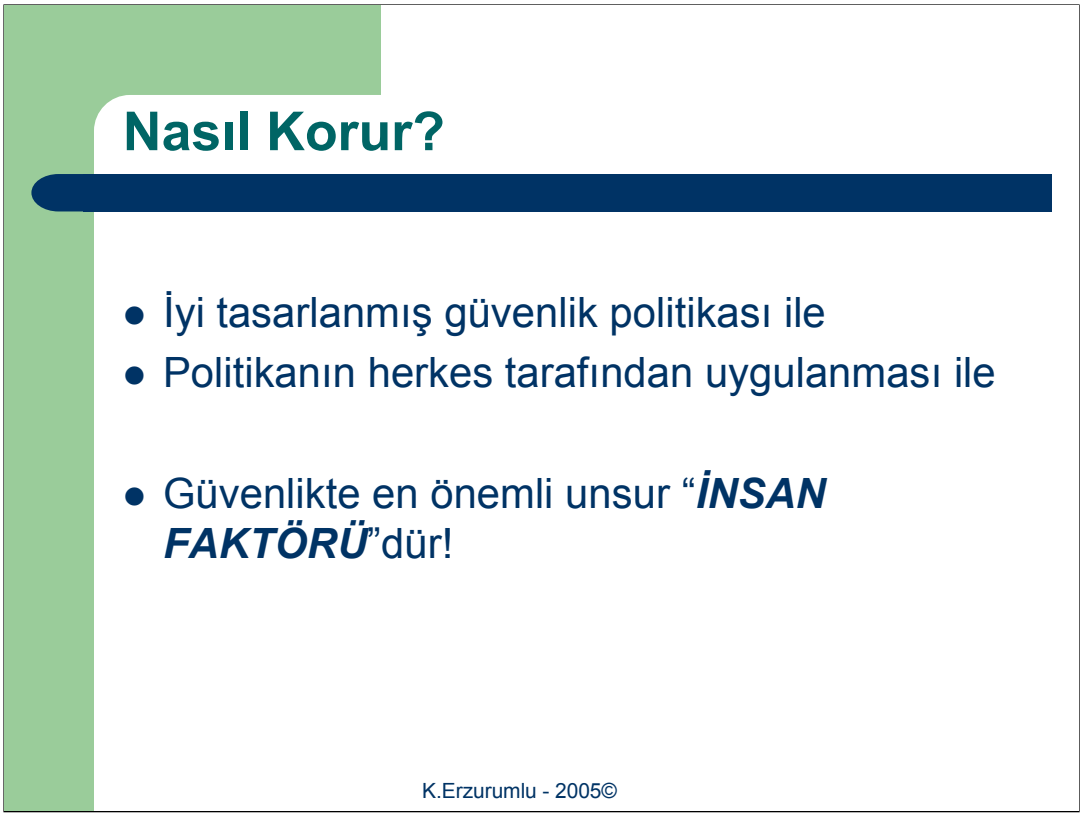


Güvenlik kapsamında korunan verilerin kimlere karşı korunduğu da çok önemlidir. Verilerin art niyetli kişilerden korunması kadar, insan hatasından da korunması gereklidir. Genel kanının aksine saldırıların büyük çoğunluğu kurumların içerisinden gerçekleşmektedir.

Korunma noktalarını kurum içi ve kurum dışı olarak gruplayacak olursak, “Dış Saldırılar” ve “Teknik Sabotaj” kurum dışı, “İnsan Hatası” ve “Kötü Niyetli Personel” kurum içi olacaktır. Diğer her türlü üçünücü etmen ise her iki kaynaklı olabilir.

Bu başlık altında bahsi geçen üçüncü etmenler yangın, sel, deprem, tsunami gibi doğal afetler olabileceği gibi, terörist saldırı, bombalama gibi insan kaynaklı fiziksel eylemlerde olabilir.

En çok dikkati çeken ise kurum içerisindeki “Kötü Niyetli Personel”dir. Kurum içerisinde maaşını beğenmeyen, müdürüne kızan, beklediği terfiyi alamayan, tartışmalar sonucu istifa eden personel genellikle kızgınlık hali ile kuruma zarar verme yolunu seçer.

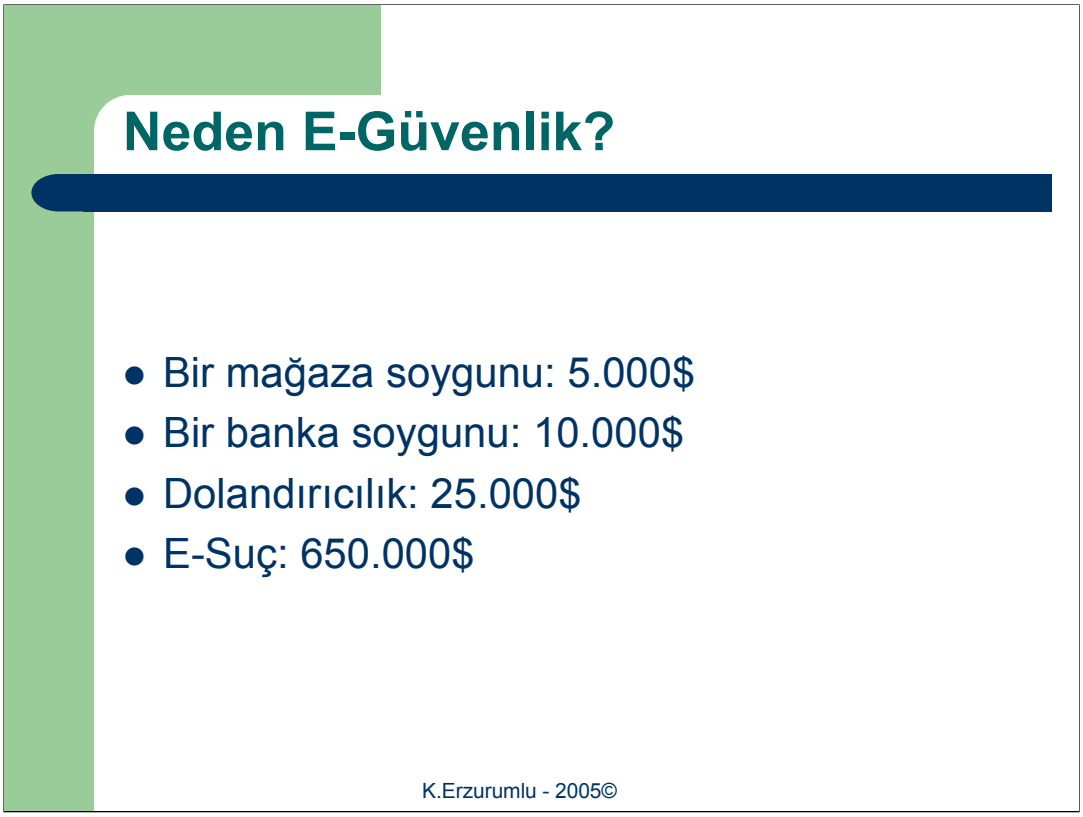


Güvenliği sağlamanın tek yolu iyi oluşturulmuş ve düşünülmüş bir "Güvenlik Politikası"'nın kurum bünyesindeki tüm çalışanlar tarafından eksiksiz uygulanması ile mümkündür. Oluşturulacak olan politika, öngörülebilecek her durumu kapsamalı ve bu durum ile ilgili açıklamalar içermelidir.

Güvenlik politikası mümkünse bölümlerden oluşmalı ve son kullanıcıya da gerekli bilgileri vermelidir. Örneğin büyük bir kurumun güvenlik politikasında aşağıdaki gibi bir tanım bulunması son derece doğaldır.

"Her Pazartesi günü iş çıkışında anti-virüs programının güncellemesi işlemi başlatılacak ve yanlızca bilgisayar ekranı kapatılarak, bilgisayar çalışır halde bırakılarak iş yerinden ayrılınacaktır."

Unutulmaması gereken en önemli konu, güvenlikte en önemli unsurun "***İNSAN FAKTÖRÜ***" olduğudur.



Elektronik Güvenlik (E-güvenlik) her geçen gün daha çok önem kazanmaktadır. Bunun başlıca nedeni e-suçlar aracılığı ile yapılan hırsızlıkların hem daha büyük tutarlarda olması hemde firma açısından daha büyük prestij kaybına neden olmasından dolayıdır. Bir banka şubesi soyulursa sigorta mekanizmaları devreye girer ve zararlar karşılanır. Bir e-suç'ta da sigorta mekanizmaları devreye girerek zararı karşılasa da, insan psikolojisi "*Bu site bir seferinde kredi kartı bilgilerimi çaldırmıştı*" düşüncesi ile güvenini kaybedecek ve ilgili siteyi kullanma isteği azalacaktır.

Benzer şekilde bir fiziksel olarak gerçekleşen bir mağaza (örneğin günümüz Türkiye'sinde bir benzinci) soygununda hırsız ortalama olarak 5.000$'lık bir nakit çalabilir. Benzer koşullardaki bir banka soygununda ise bu miktar iki katına çıkar. İngilizce'de "*white crime*" olarak adlandırılan silah kullanmadan yapılan dolandırıcılık'ta ise bu miktar 25.000$'a kadar çıkmaktadır.

Tüm bunların yanı sıra bir e-suçta çalınan para 650.000$ ortalamasındadır.

Neden E-Güvenlik?

- ABD firmalarının %15'i güvenlik eksikliği nedeni ile kayıp veriyor.
  - Örneğin; Microsoft, XP kaynak kodlarını çaldırdı.
- CERT'e göre saldırılarda artış var
  - 2003 ile 2004 arasında %80
- Tahminlere göre saldırıların %20'lik kısmı tespit ediliyor.

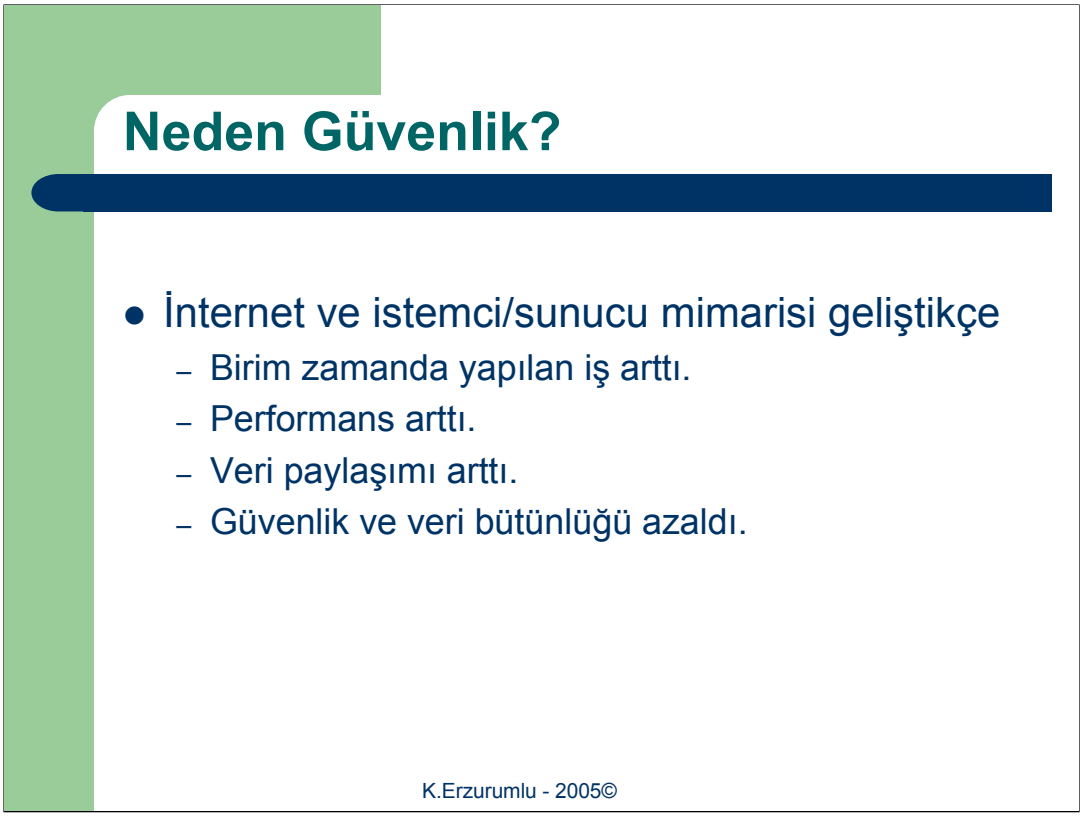
K.Erzurumlu - 2005©

CERT Amerika Birleşik Devletlerinde, kurumlar üstü bir acil durum timidir. Asıl işi bir devlet dairesinin saldırıya uğraması ve bilgi sızıntısının/bilgi değişikliğinin yaşanması durumunda müdahelede bulunarak "olay yeri inceleme" (ing. *Forensic Investigation*) yapmaktır.

Dolayısı ile CERT düzenli olarak saldırıları izler ve periodik aralıklarla güvenlik ile ilgili raporlar yayınlar.

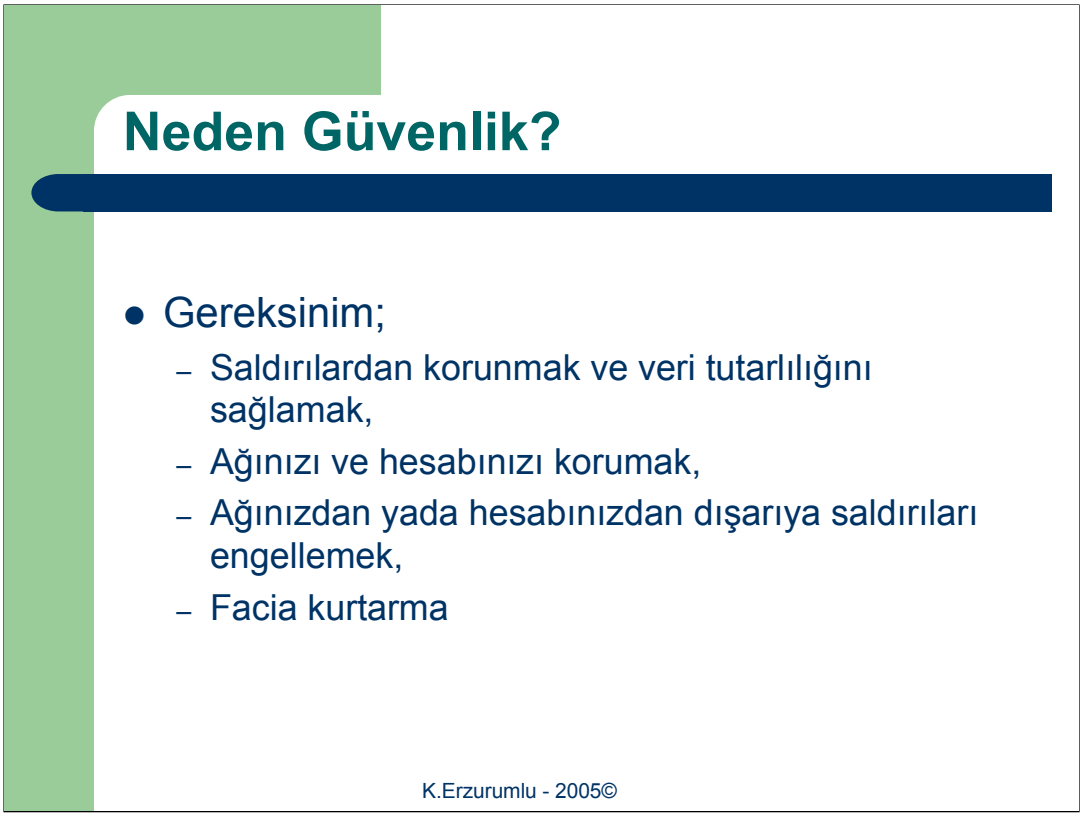
Bu raporlara göre Amerika Birleşik Devletleri'ndeki özel şirketlerin %15'i her sene güvenlik eksiklikleri nedeni ile maddi/manavi kayıplar yaşamaktadır. Bu kayıplara örnek olarak Microsoft'un 2004 yılı içerisinde Windows XP işletim sisteminin kaynak kodlarını çaldırması verilerebilir.

Bunun yanı sıra CERT yer sene gerçekleşen saldırıların bir önceki yıla oranla %80 oranında attığını tespit etmiştir. Ve bu oranlar ile birlikte CERT, gerçekleşen saldırıların yanlızca %20'sinin rapor edildiğini/açıklandığını tahmin etmektedir.



İstemci/Sunucu mimarisi ve paralelinde internet geliştikçe, bu mimarinin sunmakta olduğu "cazip" iş gücünün dağıtılması, veri paylaşımının artması fikirleri çabukça benimsendi ve uygulamaya geçildi.

Birim zamanda üretilen işin artması, insanların paralel çalışabilmesi gibi çok önemli etmenler içerse de istemci/sunucu mimarisinin en büyük dezavantajı güvenliğin ve veri bütünlüğünün azalmış olmasıdır. Dolayısı ile güvenlik ve veri bütünlüğü için ek önlemlerin alınması kaçınılmazdır.



Güvenliğin en büyük gerekliliğinin kurum için maddi/manevi değeri olan verilerin korunması olduğunu ünitenin başında dile getirmiştik. Bunun haricinde güvenlik ile sağlanacak diğer yan etmenlerde mevcuttur. Örneğin, kişisel bilgilerinizin korunması, hesabınızdan/ağınızdan dışarıya saldırılarda bulunulmaması yada facia durumlarında kurtarma gibi.

Kim Saldırıyor?

- Mevcut çalışanlar %81
- Eski çalışanlar %6
- Yabancılar %13

K.Erzurumlu - 2005©

Mevcut saldırılar incelendiğinde saldırıları gerçekleştiren kişilerin %81 oran ile mevcut çalışanlar olduğu görülmektedir. Yabancılar %13'lük oran ile mevcut çalışanları izlemektedir. Eski çalışanlar ise %6'lık bir orana sahiptir. Genellikle "*Eski Çalışanlar*" ve "*Yabancılar*" kötü niyetlidir. Mevcut çalışanlar arasında ise kötü niyetliler bulunmakla birlikte daha çok kurumun gizli bilgilerini ele geçirme/öğrenme merakı önplandadır.

Saldırganların amaçları incelenecek olursa en büyük pay %44 ile "Para Çalma"dır. Bunu %16'şarlık oranlar ile "Bilgi Çalma" ve "Yazılım Hasarı" izlemektedir. %12'lik oranla gelen "Bilgi Değişikliği"ni, %10 oranla "Servis Çalma" takip etmektedir. Son olarakda %2'lik bir oranla "Atlama Noktası" gelmektedir.

Bu bağlamda amaçlar teker teker incelenecek olursa;

Para Çalma: E-para yada kredi kartı bilgileri çalma amaçlanmaktadır. Ürün çalma da bu kategori içerisinde sayılabilir. Örneğin bir e-ticaret sitesinden 1 adet sipariş ettiğiniz üründen 10 tane teslim edilmesini sağlamak.

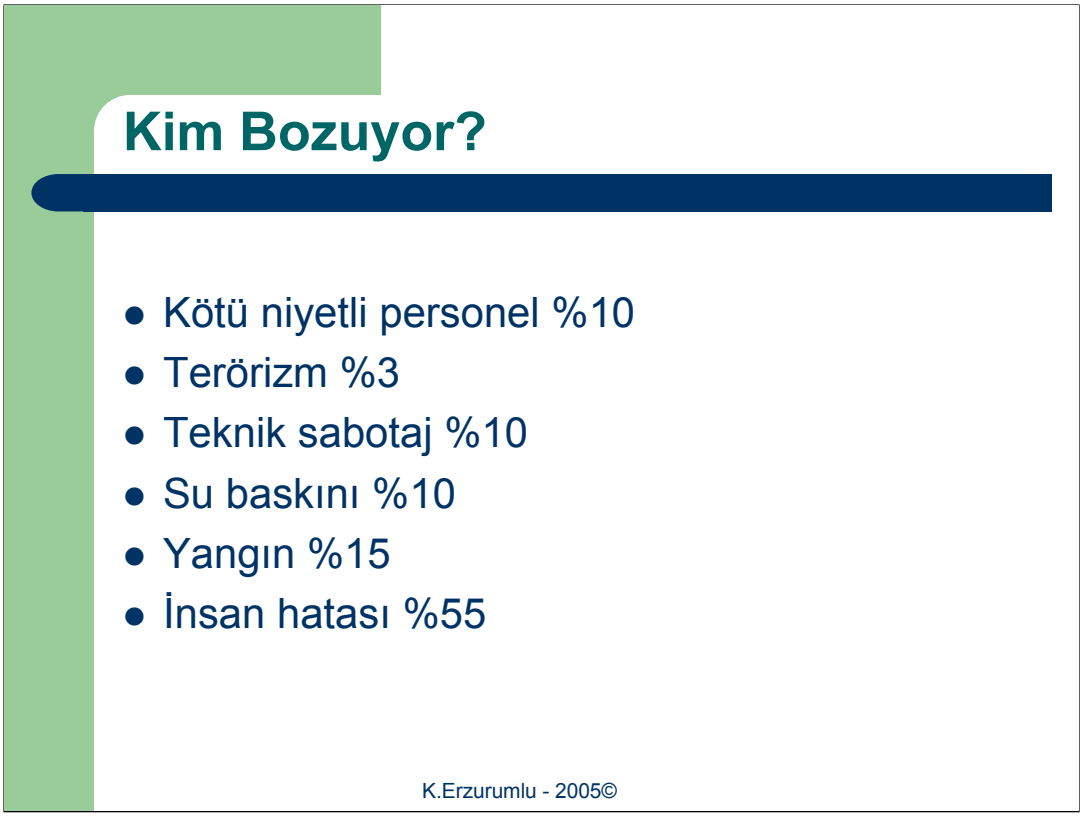
Bilgi Çalma: Giderek dijitalleşen dünyamızda bilgi güç sağlamaktadır. Kişinin amacı belli bir kişinin/ürünün/projenin/şirketin gizli bilgilerine ulaşmaktır.

Yazılım Hasarı: Kurumun çalışmakta olan uygulamalarına zarar vermek amaçlanır. Bu sayede iş akışı duracak/aksayacaktır.

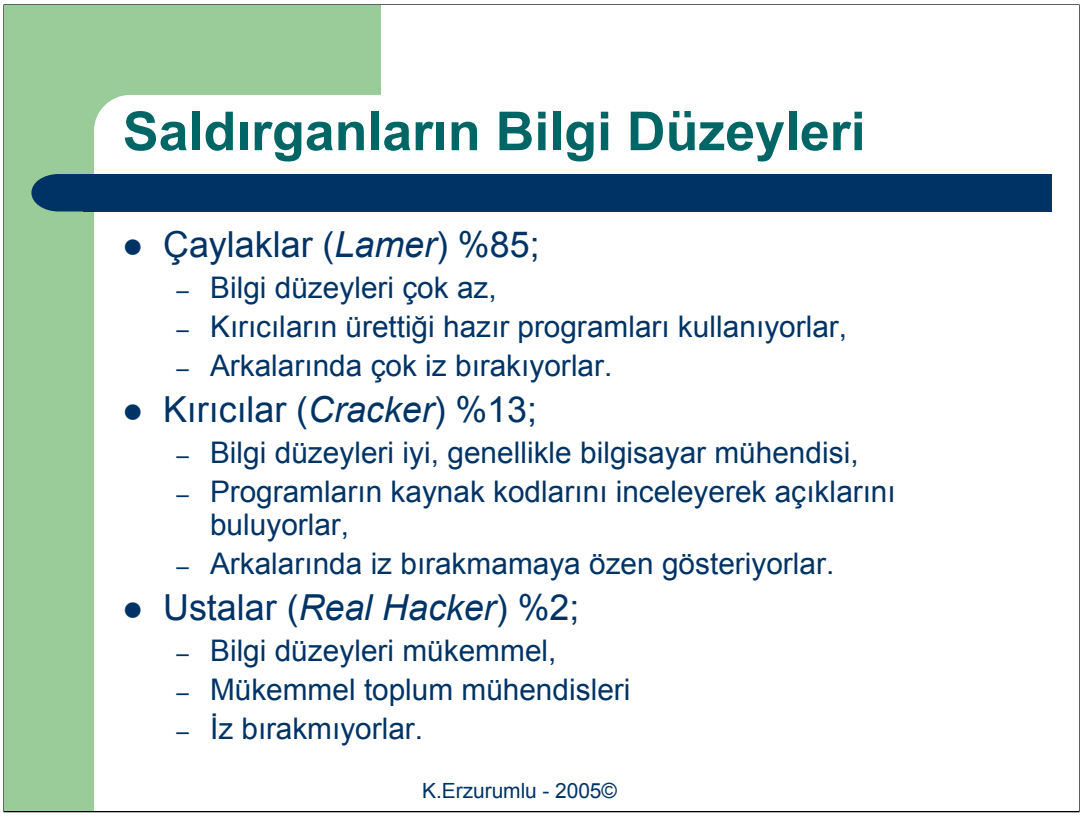
Bilgi Değişikliği: Mevcut veriler üzerinde oynama yapılması amaçlanmaktadır. Örneğin imara açık olmayan bir arazinin imara açılması gibi.

Servis Çalma: Ücretini ödemeden bir hizmetten faydalanmak amaçlanmaktadır. Örneğin aylık ücretini ödemeden ADSL kullanmak gibi.

Atlama Noktası: Saldırgan bir sonraki hedefe saldırırken izlerini kaybettirmeyi amaçlar. Bu nedenle tüm saldırıları sizin sunucunuzu/bilgisayarınızı kullanarak yapar.



Bu bağlamda gerçekleştirilmekte olan bilgi değişiklerini kimler gerçekleştiriyor sorusu gündeme gelmektedir. Şu ana kadar oluşmuş genel istatistiki bilgiler yukarıda verilmiştir.



Saldırganlar bilgi düzeylerine göre 3 farklı gruba ayrılmaktadır. Bu gruplar kısaca Çaylaklar, Kırıcılar ve Ustalar olarak anılır.

Çaylaklar genellikle kendilerini gizlemeye uğraşmayan, çoğu zaman buldukları hazır yazılımları kullanan ve ingilizce "*Lamer/Script Kiddie*" olarak tanımlanan kişilerdir. Bilgisayar hakkında fazla bir bilgileri olmamakla birlikte yanlızca kaba bilgilere sahiplerdir.

Kırıcılar ise konsunda daha uzmanlaşmış kişilerden oluşmaktadır. Asıl amaçları yazılımların açıklarını bulmaktır. Bu nedenle açık kaynak yazılımları satır satır incelerler. Uzak sistemlere saldırdıklarında arkalarında iz bırakmamaya özen gösterirler.

Ustalar ise bu konuda uzmanlaşmış kişilerden oluşur. Arkalarında iz bırakmazlar ve yakalamak son derece zordur.

Genelde çaylaklar son derece basit ve engellenmesi kolay saldırılar yapmaktadır. Ufak ve düzenli kontroller bu kişilerin saldırılarını engellemek için yeterlidir. Kırıcılar ve Ustaları engellemek içinse çok daha fazla dikkat ve özen gerekmektedir.

Güvenlik Düzeyleri

- ABD Savunma Bakanlığı öncülüğünde "Güvenilir Bilgisayar Değerlendirme Kriterleri" oluşturulmuştur.
- En önemli kural;
  - ***"Hiç kimse herşeyi yapmaya yetkili değildir!"***
    - Kişiye güvenilebilir ama kişinin hesabına "**ASLA!**"
      - Kullanıcı adı/şifresi çalınabilir,
      - Anahtarı çalınabilir,

K.Erzurumlu - 2005©

Güvenlik tasarlanırken en önemli kural "***Kimse herşeyi yapmaya yetkili değildir***" ilkesidir. Zira kişi son derece güvenlilir olabilir fakat kullanıcının kullanıcı adı ve şifresi aynı güvenlilirlikte değildir.

Güvenlik Düzeyleri

- Güvenilir Bilgisayar Değerlendirme kriterleri bilgisayarları işledikleri ve sakladıkları verilere göre sınıflandırmayı önerir.
  - Güvenilmez bilgisayarlar,
  - Terminaller,
  - Veri Ambarları,
  - Sunucular...
- Her bir sınıf için güvenlik kuralları ve erişim yetkileri tanımlanmalıdır.

K.Erzurumlu - 2005©

Güvenlik polikası oluştururken genel bir politika yazmak yerine ağda mevcut bilgisayarları depoladıkları verilere ve yapmakta oldukları işlere göre sınıflandırarak, her sınıf için ayrı bir kurallar kümesi ve değerlendirilmesi en uygun yöntemdir. Bu yöntem ilk başlarda yapılacak işleri arttırırken, takip eden süre içerisinde sistem yöneticilerini rahatlatacaktır.

Güvenliğin Temelleri

Ünite 3
Toplum Mühendisliği

Tüm kurs kapsamında anlatılacak olan konuların hepsinin temelinde toplum mühendisliği yatmaktadır. Halk dilinde “korsan” (ing. *Hacker*) olarak adlandırılan bu kişiler “bilgi kırıntıları”nı ve “insani zaafları” kullanarak karşılarındaki kişiyi kandırır ve kendilerine yardımcı olunmasını sağlarlar. Bu ünite kapsamında toplum mühendislerinin kullanmakta olduğu genel yöntemler örnekleri ile anlatılacak ve toplum mühendislerinden sakınma yollarına değinilecektir.

Toplum Mühendisliği Nedir?

- İnsanları kandırma/aldatma sanatıdır.
- Bir çok örneği mevcuttur;
  - Telefon aracılığı ile hedefi kandırmak,
  - Kurum ağlarına sızmak,
  - Ve akla hayale sığmayacak bir çok yöntem...

K.Erzurumlu - 2005©

Toplum mühendisliği temelinde insan psikolojisini ve zayıf yönlerini kullanarak, insanları kendi çıkarları doğrultusunda kullanma sanatıdır. Toplum mühendisleri ünite kapsamında da detaylı örnekleri ile sunulacağı üzere birçok yöntemi bir arada kullanırlar. Bu yöntemlerden başlıcaları telefon görüşmeleri yapmaktır. Bu görüşmeler sayesinde elde edeceği ufak bilgileri başka kurbanları kandırmak için kullanırlar.

Tehlikeli Mi?

- Kesinlikle!
- Saldırıların büyük çoğunluğu toplum mühendisliği aracılığı ile olur.
  - Filmlerde görülen bilgisayar “kırmaları” yanlızca amatörler tarafından kullanılır,
  - Bilgi toplayarak karşıdakine karşı inandırıcı olmak,

K.Erzurumlu - 2005©

Sinema ve televizyon filmlerinde görülmekte olan “basamakların sırayla bulunması” kırma sahneleri ne yazıkki gerçek hayatta geçerli değildir. Bilgisayar korsanlarının büyük ve tehlikeli olan çoğunluğu toplum mühendisi olup, saldırılarından önce detaylı bilgiler ele geçirirler ve bu bilgilerini kullanarak çoğunlukla başarılı saldırılar gerçekleştirirler.

Toplum mühendislerinin en büyük amacı mümkün olduğu kadar çok bilgi toplamaktır. Çünki kurum hakkında ne kadar çok bilgi toplarsa karşısındaki kişiyi kandırması daha kolaylaşacaktır.

Örnek Senaryo – I

- Görüşme 1 – Aranan yer bir banka şubesi

BSP: İyi günler, ben Ayşe nasıl yardımcı olabilirim?

TM: İyi günler Ayşe Hanım, ben polisiye bir roman yazıyorum fakat bir noktada takıldım, romanında gerçekçi olmasını istiyorum. Bir-iki soru sormamda sakınca var mı?

- Tabiki.
- Kredi kartı başvurusu gelince bu bir merkezde inceleniyor değil mi?
- Evet.
- Peki bu merkezin teknik adı nedir?
- Kredi Kartları Merkezi.
- Peki bu merkezi arayınca neler soruluyor?
- Şubemizin kodu ile istenilen kişinin adı soyadı doğum tarihi.
- Yardımlarınız için çok teşekkür ederim. Gün içerisinde sizi tekrar arayabilir miyim?
- 13:00 ile 14:00 arası bir toplantıda olacağım. Onun dışında yardımcı olmaya çalışırım.

Örnek senaryo bağlamında bir toplum mühendisliği çalışmasını irdeleyelim. Burada TM Toplum Mühendisini, BSP ise Banka Şubesi Personelini ifade etmektedir.

Örnek Senaryo – I

- Görüşme 2 – Aranan yer şube, saat 13:30

TM: İyi günler, ben Kredi Kartları Merkezinden Hasan arıyorum, Ayşe Hanım ile görüşebilir miyim?

BSP: Ayşe Hanım toplantıda, buyrun ben yardımcı olayım. Ben Hüseyin.

- Sabah Ayşe Hanım ile bir kişi için konuşmuştuk, fakat işlemin ortasında bilgisayarım arızalanmış ve tamamlayamamıştık. İşlemi sizinle yapabilir miyiz?
- Tabiki, dinliyorum.
- Öncelikle şube numaranıza ihtiyacım var.
- Şube numaramız AF9754
- Teşekkürler. Ayşe Hanım banden sabah "Veli Deli" hakkında bilgi istemişti. Hay allah kahretsin, bilgisayarım yine çöktü. Kahretsin, ben bilgisayarımı düzeltince sizi tekrar arayabilir miyim Hüseyin Bey?

Örnek Senaryo – I

- Sonuç, Toplum mühendisi;
  - İlk konuşmada “Kredi Kartı Merkezi” adını,
  - İkinci konuşmada geçerli bir “Şube Numarasını”,
  - Üçüncü konuşma “Kredi Kartı Merkezi Numarasını”

  öğrenir.
  - Adını,
  - Soyadını,
  - Doğum Tarihini

  Bildiği bir kişinin Kredi Kartları ile ilgili durumunu öğrenebilir.

K.Erzurumlu - 2005©

İlk konuşma esnasında telefonu açmış olan Ayşe, telefondaki kişinin beyanatına güvenerek o kişinin bir yazar olduğuna güvendi ve kendisine sormuş olduğu soruları cevaplamakta bir sakınca görmedi. Zira toplum mühendisinin sormuş olduğu soruların cevapları şube içerisinde rutin konuşmalar esnasında kullanılmakta olan, şube personelleri için “rutin” terimlerdi. Dolayısı ile bu terimleri bir yazara vermekte hiçbir sakınca görmedi. Zira Ayşe’ye göre tek başına bu bilgiler zararlı değildi. Gerçekten de tek başına bu bilgiler zararlı olmamasına rağmen bir sonraki adım için önem arz ediyordu.

Toplum mühendisi ikinci aramasında ilk aramasından edindiği bilgileri kullanarak hedefini şaşırtma yoluna gitti. Ayşe Hanım’ın ofisinde olmayacağını bile bile –ilk görüşmede bu bilgiyi edinmişti- onu aradı ve telefona çıkan kişi olan Hüseyin Bey’den yardım istedi. Hüseyin Bey ise iş yerindeki bir arkadaşına yardım etmek amacı ile toplum mühendisinin sorduğu şube numarası sorusuna cevap verdi. Normal koşullar altında bu numara gelen aramalarda değil, giden aramalarda kullanılırdı. Yani Kredi Kartı Merkezi arandığında. Hüseyin bu noktada yanılmış ve dışarıdan gelen bir aramada bu kritik bilgiyi kullanmıştı.

İkinci görüşmede gerekli kritik bilgiyi elde eden toplum mühendisi için yapılacak son bir aşama kalmıştı. O da Kredi Kartı Merkezi’nin telefon numalarından birine ulaşmak. Bir toplum mühendisi için rutin sayılabilecek bir konuşma ile (Bir banka şubesini arayıp, ben Kredi Kartı Merkezinden arıyorum ... bir anket yapmak istiyoruz ... hangi telefon numaramızı kullanıyorsunuz?) ihtiyacı olan son bilgiyede ulaşır.

Bu aşamadan sonra artık istediği kişinin kredi kartı bilgilerine ulaşabilir duruma gelmiştir.

Örnek Senaryo – II

- Giriş: Bir cep telefonu markası 1 YTL'ye telefon kampanyası başlatmıştır. Koşul telefonu alan kişinin 2 yıl Y hattını kullanması zorunluluğudur
- Görüşme 1, Aranan yer: Zincir elektronik satış mağazası, X şubesi.

TM: İyi günler,

SP: İyi günler, nasıl yardımcı olabilirim?

- Dün 1 YTL'ye cep telefonu için bir kişi ile görüşmüştüm ama adını hatırlayamıyorum şimdi.

- Ahmet bey olmalı. O kampanya ile o ilgileniyor.

- Hah evet Ahmet'ti. Kendisini ve şubenizi müşteri tutumunuzdan dolayı genel müdürlüğünüze tebrik etmek istiyorum. Tam şube adınızı ve Ahmet Bey'in soy adını alabilir miyim? Bir hata yapmak istemiyorum da.

- Şubemiz X şubesi, şube kodumuzda Y. Ahmet Hüseyin.

- Teşekkür ederim.

Başka bir örnek senaryo bağlamında bir toplum mühendisliği çalışmasını irdelemeye devam edelim. Burada TM Toplum Mühendisini, SP ise Şube Personelini ifade etmektedir. Bir cep telefonu şebekesi belli bir marka cep telefonunu 1 YTL'den satacağını duyurmuştur. Telefonu almak için gerekli koşul 2 yıl boyunca kendi şebekesi bir miktar yüksek fiyat ile kullanmasıdır.

Toplum Mühendisimiz ise telefonu beğenmiş fakat telefon şebekesinin kurallarını beğenmemiştir. Cep telefonunu tek başına almak için bir plan yapar ve uygulamaya koyar.

Örnek Senaryo – II

- Görüşme 2, Aranan yer: Zincir elektronik satış mağazası, Z şubesi

SP: İyi günler, ben Nuran, nasıl yardımcı olabilirim?

TM: İyi günler. Ben X şubesinden Ahmet Hüseyin. 1 YTL'ye cep telefonu kampanyasında bir müşteriye telefon sattım, hattın sözleşmelerini imzaladık fakat telefon stokta kalmamış, telefonu veremedim, sizde telefon varsa, müşterimi yollasam ona satabilir misiniz?

- Tabiki. Müşterinize gelince Nuran Tarcan'ı bulmasını söyleyin. Müşterinin adı nedir?

- Ali Haydar. Birazdan kendisini size göndereceğim. Yardımlarınız için çok teşekkürler.

Örnek Senaryo – II

- Sonuç, Toplum mühendisi;
  - İlk konuşmada bir "yetkili" adını,
  - İkinci konuşmada geçerli bir "1 YTL'ye telefon satacak kişiyi",

  öğrenir.
  - Tek yapacağı gidip, kendini Ali Haydar olarak tanıtarak 1 YTL'ye cep telefonunu almaktır.
  - Tabiki istediği hattı kullanarak ☺

K.Erzurumlu - 2005©

Toplum mühendisinin planı basittir. Önce bir yetkilinin adını öğrenip, sonra o yetkilinin adını kullanarak başka bir mağazaya "Ben bir müşteriye hattı sattım ama telefonu satamadım, telefonu gelsin alsın" diyerek telefonu elde edebilecektir.

Örnek Senaryo – III

- Kişinin cep telefonu çalar, arayan numara “gizli”dir.

TM: İyi günler, Hasan Kaçan ile mi görüşüyorum?

- Evet, buyrun,
- Ben XYZ bankası müşteri hizmetlerinden arıyorum. Hem hizmet kalitemiz hakkında bir anket yapıyoruz. Aynı zamanda müşterilerimizin bilgilerini de güncelliyoruz. Müsait misiniz acaba?
- Buyrun.
- Öncelikle bankamız şubelerini/internet şubesini/telefon bankacılığını ne sıklıkla kullanıyorsunuz?
- Şubelerinizi ayda 1, internet şubenizi 10 günde bir. Telefonu kullanmıyorum.

[Bu kısımda bir müşteri memluniyeti anketi soruları var]

- Anketimize katıldığınız için teşekkür ederiz, şimdi bilgilerinizi güncelleyelim. Müşteri numaranız?
- 1234567

[Bir sürü ıvır zıvır sorunun arasında doğum tarihi, nüfus cüzdanı numarası, anne kızlık soyadı gibi bilgileri de sorar]

- Teşekkür ederim yardımcı olduğunuz için.
- Ben teşekkür ederim.

K.Erzurumlu - 2005©

Günümüzde sıkça yaşanan internet bankası mağdurluğunun bir örneğini toplum mühendisliği kapsamında irdeleyelim.

Örnek Senaryo – III

- Sonuç kurbanımız,
  - Kişi ertesi gün internet şubesine girdiğinde tüm hesaplarının eksi bakiyeli olduğunu,
  - Kredi kartlarından limitinin sonuna kadar naktin hesabına aktarıldığını,
  - Tüm birikimlerinin çeşitli bankalara EFT yapıldığını

  öğrenir.
  - Banka ile konuşur, banka "Gün gece 1:12'de şifrenizi unutmuşsunuz ve bizi aramışsınız. Tüm kişisel bilgileriniz doğrulanmış ve şifrenizi değiştirmişsiniz" der.
  - Savcılığa suç duyurusunda bulunulur. ☹

Kurbanımız telefonla arayan kişinin beyanatına güvenerek kişinin kendi bankasından aradığına inanır ve sorulan tüm sorulara eksiksiz cevap verir. Dolayısı ile gerekli tüm bilgilere sahip toplum mühendisi kişinin hesaplarını "boşaltır". Ne yazıkki yapılabilecek tek şey savcılığa suç duyurusunda bulunmaktır.

Güvenliğin Temelleri

Ünite 4
Yetkilendirme

Yetkilendirme

- Kimin ne yapabileceğine,
- Kimin ne yapamayacağına karar verilmesidir.

İdeal Yetkilendirme

- Her kişi için tek tek yetkiler belirlenir.
  - En etkili ve güvenli yöntemdir,
  - Yönetimi en zor olandır.

Rol Tabanlı Yetkilendirme

- Benzer yetkilerle donatılacak olan kişiler bir “grup”ta toplanır.
- Yetkiler gruba verilir,
- Grubun üyesi yetkilerin tamamına sahip olur.
  - Bir kullanıcı birden çok gruba üye olabilir.
- Yönetimi çok daha kolaydır.

Rol Tabanlı Yetkilendirme

- Grup bazında yerel ağın izole olması istenir.
  - Grup içindeki trafik grup içinde kalır,
  - “Dinlemeler” büyük ölçüde önlenir,
  - Erişimlerin izinlerinin ayarlanması kolaylaşır.
- Gerekli ise anahtar cihazlarda ACL kullanılır.

ACL

- “Access Control List”
  - “Erişim Kontrol Listesi”
- IP Tabanlı çalışır,
- Kimin nereye erişebileceğini
  - Belirler,
  - Denetler.

ACL

- ACL tanımları üretici firmaya göre değişir;
  - Cisco için;
  - access-list 102 permit ip 193.140.236.0 0.0.0.255 10.0.0.0 0.255.255.255 telnet
- 2 ve 3 katman cihazlarda bulunur.

VLAN

- “Virtual Local Area Network”
  - “Sanal Yerel Ağ”
- Bir birimin tüm elemanları;
  - Yan yana odalarda değil,
  - Aynı katta değil,
  - Aynı binada değil,
  - Eleman sayısı anahtardaki uç sayısından çok az.

VLAN

- Birden çok birimin aynı anahtarı aynı anda kullanması,
- Maliyetlerin azaltılması,
- Yönetim kolaylığı,
- VLAN ile ayrılmış bir anahtar 2 farklı anahtar gibi davranır.

VLAN Çeşitleri

- Uç Tabanlı
  - Her anahtarda;
    - X numaralı uç A Ağına,
    - Y numaralı uç B Ağına dahildir

    Tanımlamaları yapılır.
  - Avantaj;
    - Ayarlaması kolaydır.
  - Dezavantaj;
    - Yönetimi zordur,
    - Saldırılara açıktır.

VLAN Çeşitleri

- MAC Tabanlı
  - Her anahtara bir VMPS sunucu adresi verilir.
  - Yerel ağda bulunan her MAC adresi ve dahil olduğu VLAN sunucuya kaydedilir.
  - Anahtar bir uç bağlantısı bulduğunda o MAC adresinin dahil olduğu VLAN'ı sunucudan öğrenir.
  - Avantajı;
    - Yönetim işleri tek bir noktaya toplanıyor,
  - Dezavantajı;
    - Yerel Ağ'a bir miktar tük getiriyor.

VLAN Ana Bağlantıları

- Bir anahtar 2 VLAN barındırsa dahi tek bir "up-link" ile 2 yerel ağ bağlantısıda taşınabilir.
- Bu işleme "trunking",
- Bu işlemi yapan uca "trunking port" denir.

Güvenliğin Temelleri

Ünite 5
Şifreleme Yöntemleri

Şifreleme Yöntemleri

- İkiye ayrılır;
  - Asimetrik Yöntemler
  - Simetrik Yöntemler

Ortak Yönler

- Tüm şifrelemeler anahtar kullanır;
  - Anahtar bir yada birden çok olabilir.
  - Anahtarın uzunluğu güvenlik düzeyini belirler.

Asimetrik Yöntemler

- Veri bir anahtar ile şifrelenir.
- Şifrelenmiş veriden geri dönüş yoktur.
- Kullanıcı parolası gibi veriler için kullanılır.
  - Unix Crypt
  - Windows Crpyt

Unix Crypt

- 56 bit şifrelemele yapar,
- Anahtar olarak 2 harf kullanır;
  - “ab”, “1B”, “/c” gibi...
- crypt(“armut”,“ab”)= “abgQgKUl1Kvnw”
- crypt(“armut”,“ac”)= “ac6FemVd5McS6”

Windows Crypt

- Unix crypt ile benzer çalışır,
- Anahtar kullanmaz.

Simetrik Yöntemler

- Veri anahtar(lar) kullanılarak şifrelenir,
- Şifrelenmiş veri anahtar kullanarak geri dönüştürülebilir,
- Kullanım alanları
  - Bilgisayar Ağları,
  - Güvenli veri gönderimi,

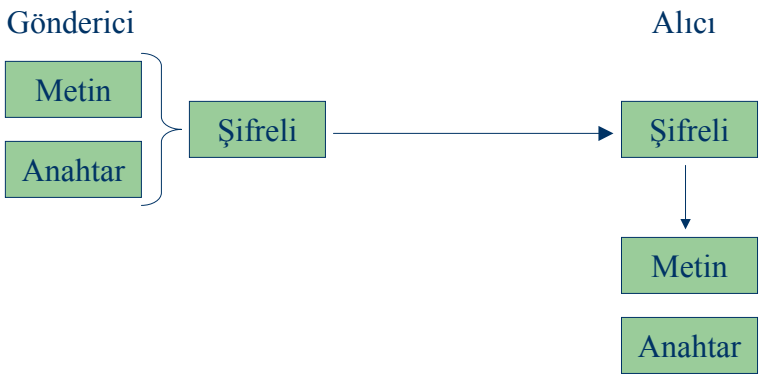
Simetrik Yöntemler

- Ağırlıkla matematiksel işlemler,
- Asal sayılar temel alınır,
- 2 alt türü mevcuttur;
  - Konvensiyonel Yöntemler
  - Modern Yöntemler

Konvansyonel Yöntemler

- Bir çok algoritma mevcuttur;
  - DES,
  - IDEA,
  - BlowFish
  - RC5
  - CAST
  - RC2
- Bir coğu “Önceden Paylaşımlı Anahtar” (Pre-Shared Key) yöntemi ile calışır.

Konvansyonel Yöntemler



Modern Yöntemler

- Açık Anahtar Yöntemleri olarak bilinir;
  - RSA
  - Diffie
  - ECC
- Bir anahtar çifti ile kullanılır,
  - Gizli Anahtar
  - Açık Anahtar

Modern Yöntemler

- Veri 2 şekilde şifrelenebilir,
  - Gizli anahtar ile,
  - Açık anahtar ile.
- Gizli anahtar ile şifrelendi ise açık anahtar ile,
- Açık anahtar ile şifrelendi ise gizli anahtar ile çözülebilir.

Modern Yöntemler

- Gizli anahtar ile şifreleme kimlik onaylama için kullanılır.
  - Bir mesajdan özet çıkartılır,
  - Özet gizli anahtar ile şifrelenir,
  - Alıcı mesajın özetini tekrar çıkartır,
  - Açık anahar ile gelen özeti çözer,
  - Çözülen anahtar ile gelen anahtar aynı ise kimlik doğrulanmış olur.

Modern Yöntemler

- Açık anahtar ile şifreleme güvenli iletişim için kullanılır.
- Bir kullanıcının açık anahtarı ile şifrelenen veri yanlızca o kullanıcı tarafından çözülebilir.

Modern Yöntemler

- SSL bir modern yöntemdir,
- Bankalar ile güvenli iletişim bu şekilde olur,
  - İletişim başlangıcı ile banka açık anahtarını kullanıcıya gönderir,
  - Kullanıcı açık anahtarını bankaya gönderir,
  - Banka veri göndereceğinde kullanıcı anahtarı ile şifreler,
  - Kullanıcı veri göndereceğinde banka anahtarı ile şifreler.

Güvenliğin Temelleri

Ünite 6
Güvenlik Politikaları

Güvenlik Politikaları

- Güvenliği sağlayan cihazlar değildir.
- Güvenliği sağlayan “İyi Tanımlanmış Güvenlik Politikası”nı uygulayan “insan”lardır.

Bölümleri

- Güvenlik Politikası
  - Sunucu Grupları,
    - VT Sunucuları,
    - İnternet Sunucuları,
    - Hizmet Sunucuları
  - Kişisel Bilgisayarlar,
  - Ağ Cihazları

  için gruplar halinde oluşturulmalıdır.

Detayları

- Öngörülebilen tüm durumlar için tasarlanmalı,
- Tüm durumlar karşısındaki hareketleri tanımlamalıdır.

Örnek Kurallar

- “Her bilgisayar sistemine virüs koruma yazılımlarının son sürümleri yüklenmeli ve çalıştırılmalıdır.”
- “Her kullanıcı Pazartesi sabahı ilk iş olarak vürus koruma programlarını ve işletim sistemlerini güncellemelidir.”

Güvenliğin Temelleri

Ünite 7
TCP/IP Genel Bilgileri

TCP/IP Genel Bilgileri

- TCP/IP bilgisayarların birbirleri ile konuşma yöntemidir.
- Her bilgisayarın bir IP'si bulunur.

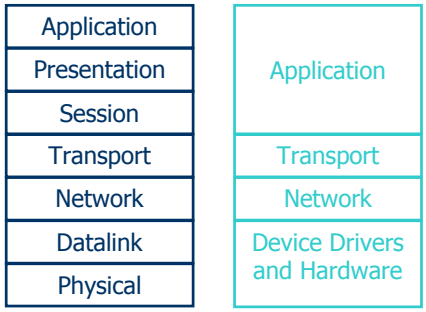
OSI Katmanları

- Tasarım aşamasında veri iletişimi için OSI katmanları kullanılır.

7	Uygulama	• Son kullanıcı programlar için arabirim
6	Sunum	• Uygulama katmanı veri dönüştürücü
5	Oturum	• Sistemler arası anlaşma
4	İletim	• Güvenli iletişim sorumlusu
3	Ağ	• Ağlar arası veri iletimi
2	Veri-Bağ	• Fiziksel katman için arabirim
1	Fiziksel	• Donanımsal katman

OSI

TCP/IP Katmanları



OSI TCP/IP

IP

- TCP yada UDP iletişimini sağlar.
- 32 bitten oluşan bir sayıdır.
- 8'li gruplar halinde ifade edilir.
  - 193.140.236.6 gibi

ARP

- Aynı ağdaki iki bilgisayarın iletişim kurabilmesi için öncelikle birbirlerinin MAC adresini bilmesi gerekir.
- Bu amaçla ARP sorgusu yapılır.
- Amaç belirli bir IP adresinin MAC adresini öğrenmektir.

ARP

- A B'ye veri gönderecekse;
- ARP istemi; IP(A),MAC(A),IP(B),MAC(HERKES)
- İstemi alan tüm makinalar
  - IP(B) ben miyim?
  - Evetse
    - IP(B),MAC(B),IP(A),MAC(A)
  - Hayırsa
    - Gözardı et.

RARP

- ARP'ın tersine kullanılır,
  - MAC adresinden IP adresine ulaşmak.
- Disksiz makinalar IP almak için kullanır.

IP Adresleri

- IP adresleri Ağ ve bilgisayar bölümlerinden oluşur.
  - Ağ [193.140.236] bilgisayar [3]
  - Her ağ parçası kendi ağ IP'sine ihtiyaç duyar.
  - Bilgisayar kısmının bitleri değiştirilebilir.
  - Ağ kesimine ayrılan bitleri artırarak farklı ağlar yaratılabilir.

Ağ Sınıfları

- Öntanımlı 3 ağ türü vardır;
  - A, B ve C sınıfları
  - A sınıfı
    - Ağ maskesi 255.0.0.0
    - 126 ağ ve ağ başına 16,777,216 bilgisayar adresi
    - İlk 8 bit'in değeri 1 ile 126 arasında
  - B Sınıfı
    - Ağ maskesi 255.255.0.0
    - 16384 ağ ve ağ başına 65,536 bilgisayar adresi
    - İlk 8 bit'in değeri 128 ile 191 arasında
  - C sınıfı
    - Ağ maskesi 255.255.255.0
    - 2,097,152 ağ ve ağ başına 254 bilgisayar adresi
    - İlk 8 bit'in değeri 92 ile 223 arasında

Adanmış IP Adresleri

- İnternet'te kullanılmazlar,
- Kurumların kendi içinde kullanımı için ayrılmıştır;
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

Ağ Maskeleri

- Ağ maskeleri IP adresinden ağ adresini bulmak için kullanılır.

	Decimal Notation	Binary Notation
	255.255.255.0	11111111 11111111 11111111 00000000
&	192.168.4.3	11000000 10101000 00000100 00000011
=	192.168.4.0	11000000 10101000 00000100 00000000

Ağ Maskeleri

- Noktalı yada bit sayısı olarak yazılabilir.
  - Adres: 192.168.4.3 Maske: 255.255.255.0
  - 192.168.4.3/24
- Öntanımlı C sınıfı için;
  - Ağ Maskesi 255.255.255.0
  - 254 bilgisayara izin verir.
    - İlk IP ağ tanımlayıcısı
    - Son IP broadcast adresi

Ağ Maskeleri

- 8 bitlik gruplar halinde olmak zorunda değildir.
- 255.255.255.192 geçerlidir;
  - 16,382 bilgisayara izin verir.
- 255.255.255.128 geçerlidir;
  - 126 bilgisayara izin verir.

TCP ve UDP

- TCP
  - Güvenilir,
  - Sağlam,
  - Veri bütünlüğü sağlayan,
  - Yavaş bir iletişim türüdür.
- UDP
  - Güvenilmez,
  - Bozulabilir,
  - Veri bütünlüğü garanti etmeyen,
  - Hızlı bir iletişim türüdür.

Kapı Numaraları

- Bilgisayardaki her servis için tek bir adres sağlar.
- 1 ile 65535 arasıdır.
- 1 ile 1023 arası iyi bilinen kapılardır.
- IANA bu dağılımı sağlar.

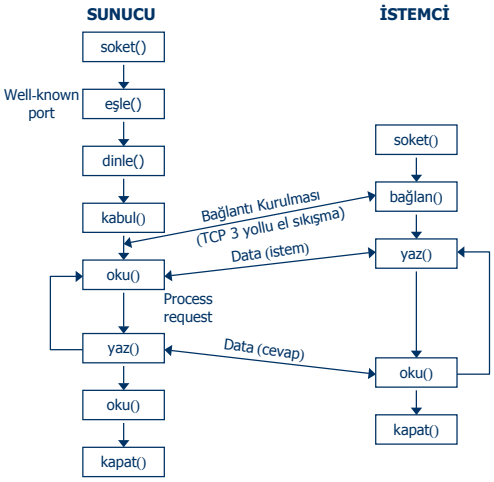
Bazı İyi Bilinen Kapılar

name	Port	name	Port
ftp-data	20/tcp	nntp	119/tcp
ftp	21/tcp	ntp	123/udp
telnet	23/tcp	netbios	137-139/tcp/udp
smtp	25/tcp	imap2	143/tcp
time	37/tcp	bgp	179
dns	53/tcp/udp	ldap	389
tftp	69/udp	rlogin	513/tcp
http	80/tcp	rshell	514/tcp
pop3	110/tcp	syslog	514/udp
sunrpc	111/tcp/udp	rip	520/udp

Soketler

- Soket = IP Adresi + Kapı Numarası
  - 192.168.4.3:1110
- Her veri iletimi yapan program bir sokete el koyar ve o soket üzerinden işlem yapar.

TCP Veri İletişimi



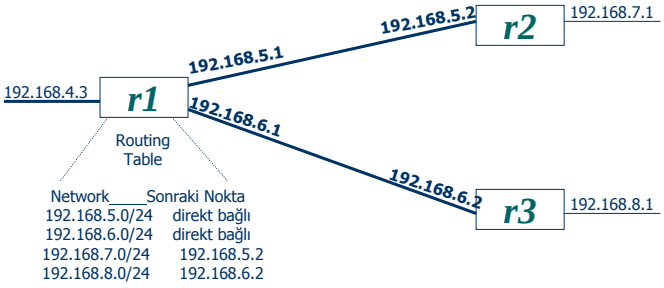
Yönlendirme

- İki farklı bilgisayar ağı arasında paket iletimi için kullanılır.
  - Yönlendirici cihazlar yapar,
  - Yönlendirici cihaz,
    - Gömülü/adanmış bir sistem olabilir.
    - Birden çok arabirimi olan bilgisayar olabilir.

Yönlendirme

- En basit kullanımda;
  - Yönlendirici almış olduğu paketi hedefe uygun olan sonraki yönlendiriciye gönderir.
  - Bu hedef yerel ağa ulaşana kadar devam eder.
  - Yerel ağ bazıda da ARP sorgusu ile hedefine ulaştırılır.
- Yönlendiriciler hedef için en iyi yolun hangisi olduğunu bulmak için “Yönlendirme Tablosu” kullanır.

Yönlendirme



- Yönlendirme tabloları elle yada otomatik güncellenir.

Güvenliğin Temelleri

Ünite 8
Ağ Cihazları

Ağ Cihazları

- 1. Katman: HUB, Yineleyici, Köprü
- 2. Katman: Anahtar
- 3. Katman: Yönlendirici
- 4. Katman: Güvenlik Duvarı, IDS
- 5. Katman: Güvenlik Duvarı, IDS
- 6. Katman: Güvenlik Duvarı, IDS
- 7. Katman: Güvenlik Duvarı, IDS

1. Katman

- HUB
  - Bir portuna gelen veriyi tüm portlarına kopyalar,
  - Çok büyük güvenlik riski içerir,
  - Herkes herşeyi dinleyebilir durumdadır.
- Yineleyici
  - Fiziksel kabloların mesafe sınırını uzatmak için kullanılır,
- Köprü
  - Farklı fiziksel katmanlar arası iletimi sağlar,

2. Katman

- Anahtar
  - Hangi portunda hangi MAC adresi olduğunu bilir,
  - Hedef paketi yanlızca gitmesi gerekene gönderir,
  - Büyük ölçüde güvenlik sağlar.

3. Katman

- Yönlendirici
  - Ağlar arası iletişimi sağlar,
  - Dinamik yönlendirme tablosu günleme protokollerinin açıkları mevcuttur,

Güvenlik Duvarları

- Tüm katmanlarda birlikte çalışır,
- Temel olarak ACL gibi çalışır,
- Farkı eklentiler ile genişletilebilmesidir.

Saldırı Tespit Sistemleri

- Takip eden ünitede açıklanacaktır.

Güvenliğin Temelleri

Ünite 9

Saldırı Türleri ve
Tespit Sistemleri

Saldırı Türleri ve Tespit Sistemleri

- Saldırganlar 3 türlü saldırı gerçekleştirir;
  - Standart kapı taraması,
  - Standart zayıflık taraması,
  - Standart hedef taraması,

Kapı Taraması

- Bir bilgisayar üstünde hangi servislerin verildiğini bulmak için kullanılır.
- Gizli yapılırsa tespiti zordur.
- Diğer durumlarda tespit edilmesi kolaydır.

Zayıflık Taraması

- Belirli bir zayıflık için tüm ağdaki bilgisayarların teker teker taranmasıdır.
- Tespit edilmesi kolaydır.

Standart Hedef Taraması

- Ağda hangi bilgisayarların çalıştığını bulmaya yönelik bir taramadır.
- Gizli olarak yapılabilir.

Saldırı Tespit Sistemleri

- Intrusion Detection Systems (IDS)
- Tüm saldırılar belirli paketler ile olur.
- Tüm paket trafiği içinde benzer paket bulunur ve iletişimi engellenirse zarar önlenir.

Saldırı Tespit Sistemleri

- Örnek;
  - Web sunucusu üzerindeki “pf.cgi” açığı için
  - İstemci mutlaka “GET /cgi-bin/pf.cgi” istemini göndermelidir.
  - Paket içeriğinde bu geçiyorsa bu bir saldırıdır.

Saldırı Tespit Sistemleri

- Avantajları
  - Saldırı veritabanı güncel olduğu sürece
  - Güvenli
  - Sağlam
  - Başarılı

Saldırı Tespit Sistemleri

- Dezavantajları
  - Saldırı imzaları iyi tanımlanmaz ise normal iletişimleri de engeller,
  - Genellikle bulduğu “alarmların” büyük kısmı sahte alarmdır.
  - Saldırı veri tabanını güncel tutmak bir problemdir.