YÖNETİM BİLGİ SİSTEMLERİ

BİLİŞİM GÜVENLİĞİ

PROF. DR. İBRAHİM HALİL SEYREK

GİRİŞ

- Bilgi sistemlerinin kullanımı firmalar ve toplum için bir çok faydalar sağlamaktadır. Ancak gittikçe artan kullanımı ile birlikte, bu sistemlerin güvenliğinin sağlanması, bireylerin gizliliklerinin korunması ve bilgi teknolojileri kullanılarak işlenen suçların önlenmesi büyük önem kazanmıştır.
- Bilişim suçları, birtakım kişilerin suç amaçlı yada sorumsuzca işledikleri eylemlerden doğan, bilgi teknolojileri ve özellikle İnternetin yaygın kullanımı ve açıklarından faydalanılarak gerçekleştirilen suçlardır.
- Bu suçlar işletmelerin güvenliği ve hayatını devam ettirmesi önünde ciddi tehditler oluşturabilmektedir.

BİLİŞİM SUÇLARI TÜRLERİ

Çok farklı şekillerde bilişim suçları işlenebilmektedir. Aşağıda bu suçlar sınıflandırılmıştır:

1. Donanım, yazılım, veri ve bilgisayar ağlarının yetkisiz kullanımı, erişimi, değiştirilmesi veya bozulması
2. Bilgilerin yetkisiz bir şekilde açığa çıkarılması, yayılması
3. Yazılımların yetkisiz bir şekilde kopyalanması
4. Bir kişinin kendi donanımı, yazılımı, verileri veya ağ kaynaklarına erişimin engellenmesi
5. Bilgisayar ve ağ kaynaklarının yasal olmayan bir şekilde bilgi edinmek amacıyla kullanılması
6. Bilgisayarlar aracılığıyla yapılan dolandırıcılık
7. Yasal olmayan konularda İnternet sitesi ve içerik oluşturulması ve yayınlanması

BİLGİSAYAR KORSANLIĞI

- Bilgisayar ağ sistemlerinin yetkisiz bir şekilde kullanılmasına bilgisayar korsanlığı adı verilmektedir.
- Bilgisayar korsanları İnternet ve diğer bilgisayar ağlarına saldırarak veri ve programları çalar veya bunlara zarar verirler.

BİLGİSAYAR KORSANLARININ UYGULADIĞI BAZI YÖNTEMLER

- **Hizmetin reddedilmesi saldırısı**: Bilgisayar ve ağ kaynaklarına çok fazla istemde bulunarak bu sistemlerin tıkanmasına dolayısıyla hizmet verememesine neden olurlar
- **Tarama**: İnternete bağlı bilgisayarları uzaktan tarayarak zayıf yönlerini bulma ve bu açıkları kullanma
- **Dinleme**: İnternet üzerinde iletilen bilgileri dinleyerek kişilere ait şifreleri ve gizli bilgileri öğrenmeye çalışma
- **Sahte adresler ile bilgi toplama**: Banka veya bir kurumun gerçek adreslerine benzer adresleri kullanarak, sahte e-posta veya web adresi ile kişilere ait kredi kartı veya parola bilgilerini toplamaya çalışma
- **Truva atları**: Masum gibi görünen bir programın içerisine kötü amaçlı bir yazılım yerleştirerek kişinin sistemindeki bir takım açıklardan faydalanma
- **Sosyal mühendislik**: Firma çalışanlarını kandırarak firmanın bilgisayarlarına ait parola vb. gibi sisteme giriş yapmayı sağlayan bilgilerin edinilmesi.

BİLGİ SİSTEMLERİ GÜVENLİĞİ

- Bilgi sistemleri güvenliği, bu sistemleri oluşturan donanım, yazılım ve ağ kaynaklarına yapılan saldırıların önlenmesi yanında bu sistemlerin yedeklerinin alınarak işlemlerin devamlılığının sağlanmasını da içermektedir.
- Bilgi sistemlerini güvenliği bağlamında aşağıdaki konular ele alınacaktır.

1. Bilgi sistemlerine girişlerin denetlenmesi
2. Bilgi sistemlerine erişimin denetlenmesi
3. Bilgilerin şifrelenmesi
4. Virüsler, Truva atları ve kurtlar

BİLGİ SİSTEMLERİNE GİRİŞLERİN DENETLENMESİ

- Bilgi sistemine kimlerin giriş yapacağının belirlenmesi sistemin güvenliği için oldukça önemlidir. Bu amaçla aşağıdaki yöntemler kullanılabilir

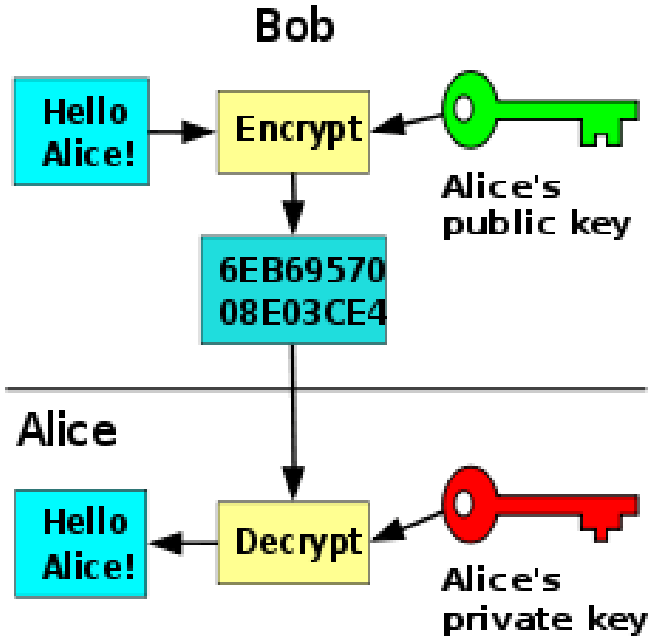
1. **Şifre kullanma**: Kullanıcının kimlik denetimi için gerçekleştirilir. Kolayca tahmin edilmemeli ve belirli aralıklarla değiştirilmelidir.
2. **Akıllı kart kullanımı**: Kişiye ait bilgileri içeren bir kart olup karta sahip olmayanların sisteme erişmeleri engellenir
3. **Fiziksel özelliklere dayalı tanıma sistemleri**: Parmak izi, ses, göz bebeği, vs. yi kimlik tanıma amaçlı kullanan sistemlerdir.

BİLGİ SİSTEMLERİNE ERİŞİMİN DENETLENMESİ

- Bilgi sistemlerine giriş yapan kimselerin bu sistemlerdeki bütün bilgileri erişim hakları yoktur. Ayrıca erişebildikleri veri üzerinde yapabilecekleri işlemler de (okuma, yazma, değiştirme gibi) kullanıcının yetkisine bağlı olarak sınırlı olabilir. Bu amaçla kullanıcıların yetkilerinin belirlenmesi ve izinli olmadıkları verilere ulaşmaları ve yetkilerinde olmayan işlemleri gerçekleştirmeleri engellenmelidir.
- Sistemin güvenliği açısından hangi kullanıcının hangi tarih ve saatte hangi verilere ulaşıp üzerinde ne tür işlemler yaptığı sistemde özel günlük dosyalarına kaydedilmelidir.

BİLGİLERİN ŞİFRELENMESİ

- Bilgilerin hızlı bir şekilde iletilmesi bu bilgilerin yetkisiz kimselerin eline geçmesini kolaylaştırmıştır. Yetkisizi kişilerin bilgilere erişimini engellemek için bilgiler şifrelenebilir. Böylece bu bilgiler yanlış kişilerin eline geçmiş olsa bile şifreli olduğu için içerikleri bu kişiler tarafından görülmeyecektir



VİRÜSLER, TRUVA ATLARI VE KURTLAR

- Bilgisayar virüsü kullanıcı istemeden kendini bilgisayara kopyalayan ve genellikle zarar verme amacıyla geliştirilmiş yazılımlardır. Tanımdan da anlaşılacağı üzere bilgisayar virüslerinin özellikleri şunlardır:

1. Çalışabilmek için kendisinden başka bir yazılıma ihtiyaç duyarlar
2. Kendilerini kopyalayarak çoğalırlar, yani bulaşıcıdırlar
3. Çoğu zaman zarar vericidirler. Örneğin diğer programları çalışmaz hale getirebilirler, dosyaları silebilirler, bilgisayar sistemine zarar vererek tamamen çalışmaz hale getirebilirler.

- **Bilgisayar kurtları** bilgisayar virüslerinden farklı olarak kendi başlarına çalışabilirler ve başka bir programa ihtiyaç duymazlar
- **Truva atı** ise kendini kullanıcıya faydalı bir program gibi gösterir ancak aktif hale geldiğinde bir takım zararlar vermeye başlar, örneğin kullanıcının bilgilerini İnternet üzerinden başkalarına gönderir, veya sistem üzerinde bir takım açıklar yaratarak uzaktan bu açıkların kötüye kullanılmasına zemin hazırlar. Genellikle e-postalara eklenen dosyalar ile yayılır

VİRÜSLER, TRUVA ATLARI VE KURTLAR

- Bilgisayar virüslerine karşı alınabilecek bazı önlemler:
  - Anti-virüs yazılımları kullanın. Anti-virüs yazılımları kullandığınızda bu yazılımların güncel olmasına ve virüs veritabanlarını sürekli olarak güncel tutmaya özen göstermelisiniz.
  - Internet üzerinden e-posta, vb. çeşitli yollarla gelen ve güvenmediğiniz dosyaları açmayın
  - Flash bellek, CD, DVD gibi taşınabilir depolama araçlarının bilgisayarınızda kullanmazdan önce bunların virüs içermediğinden emin olun veya kullanmazdan önce virüs taramasından geçirin

BİLGİSAYAR AĞLARI VE GÜVENLİK DUVARLARI

- Bir bilgisayar ağına dışarıdan yapılan yetkisiz bilgi girişlerinin engelleyen ve sistemin içine giren ve sistemden dışarı çıkan veri trafiğini belirli kurallar doğrultusunda filtreleyen donanım ve yazılımlardır. Güvenlik duvarları dışarıdan iç ağa yapılan çeşitli saldırıları ve kötü amaçlı yazılımları tanıyarak bunların içeriye girmesine engel olur. Güvenlik duvarları dışarıdan gelen tehditleri engellemenin yanında içeriden dışarıya çıkan trafiği de denetleyebilir. Böylece örneğin çalışanların mesai saatleri içerisinde işle ilgili olmayan sitelere bağlanması veya sohbet programları gibi izin verilmeyen bir takım uygulamaları çalıştırması engellenebilir.