Bilgi Güvenliği

Bu bölümde;

- Bilgi güvenliğinin önemini açıklayacak,
- Bilgi güvenliğine yönelik tehditleri kavrayacak,
- Sayısal dünyada kimlik yönetimi konusunda güvenlik acısından yapılması gerekenleri listeleyecek,
- Kişisel bilgisayar ve ağ ortamında bilgi güvenliğini sağlamaya yönelik işlemleri gerçekleştireceksiniz.

BİLGİ GÜVENLİĞİ

Kişisel ya da kurumsal düzeyde bizim için büyük önem teşkil eden her tür bilgiye izin alınmadan ya da yetki verilmeden erişilmesi,
bilginin ifşa edilmesi,
kullanımı,
değiştirilmesi,
yok edilmesi gibi tehditlere karşı
alınan tüm tedbirlere **bilgi güvenliği** denir.

Bilgi güvenliğinin üç öğesi

Gizlilik

- Bilginin yetkisiz kişilerin eline geçmemesi için korunmasıdır
- Sosyal medya hesabının çalışması gibi

Bütünlük

- Bilginin yetkisiz kişiler tarafından değiştirilmesi ya da silinmesi gibi tehditlere karşı korunması ya da bozulmasıdır
- Web sayfasının başkası tarafından değiştirilmesi

Erişilebilirlik

- Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanıma hazır durumda olmasıdır.
- Web sayfasına erişimin kapatılması

Bilgi Güvenliğine Yönelik Tehditler

- Bir bilişim teknolojisi sistemine sızmak,
- sistemi zafiyete uğratmak,
- sistemlerin işleyişini bozmak
- ve durdurmak gibi kotu niyetli davranışlar;
- **siber saldırı** veya **atak** olarak adlandırılmaktadır.

BİLGİ GÜVENLİĞİ

- **Siber** ya da **siber uzay**; temeli bilişim teknolojilerine dayanan, tüm cihaz ve sistemleri kapsayan yapıya verilen genel addır.

Siber Suç:

- Bilişim teknolojileri kullanılarak gerçekleştirilen her tür yasa dışı işlemdir.

Siber Saldırı:

- Hedef seçilen şahıs, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırıdır.

Siber Savaş:

- Farklı bir ülkenin bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır.

Siber Terörizm:

- Bilişim teknolojilerinin belirli bir politik ve sosyal amaca ulaşabilmek için hükûmetleri, toplumu, bireyleri, kurum ve kuruluşları yıldırma, baskı altında tutma ya da zarar verme amacıyla kullanılmasıdır.

Siber Zorbalık:

- Bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür.

Sayısal Dünyada Kimlik ve Parola Yönetimi

Her gün sıkça kullandığımız şifre ve parola kavramlarını inceleyecek olursak "**parola**" bir hizmete erişebilmek için gerekli olan, kullanıcıya özel karakter dizisidir.

"**Şifre**" ise sanal ortamdaki verilerin gizliliğini sağlamak için veriyi belirli bir algoritma kullanarak dönüştüren yapıdır.

Sayısal Dünyada Kimlik ve Parola Yönetimi

Elde edilen bilgiler yetkisiz kişiler ile paylaşılabilir ya da şantaj amacıyla kullanabilir.

Parolası ele geçirilen sistem başka bir bilişim sistemine saldırı amacıyla kullanılabilir.

Parola sahibinin saygınlığının zarar görmesine yol açabilecek eylemlerde bulunulabilir.

Ele geçirilen parola ile ekonomik kayba uğrayabilecek işlemler yapılabilir.

Parola sahibinin yasal yaptırım ile karşı karşıya kalmasına yol açabilir.

Güçlü bir parola için;

Parola, büyük/küçük harfler ile noktalama işaretleri ve özel karakterler içermelidir.

Parola, -aksi belirtilmedikçe- en az sekiz karakter uzunluğunda olmalıdır.

Parola, başkaları tarafından tahmin edilebilecek ardışık harfler ya da sayılar içermemelidir.

Her parola için bir kullanım ömrü belirleyerek belirli aralıklar ile yeni parola oluşturulması gerekir.

Parola güvenliği için;

Parolanın başkalarıyla paylaşılmaması son derece önemlidir.

Parolalar, basılı ya da elektronik olarak hiçbir yerde saklanmamalıdır.

Başta e-posta adresinin parolası olmak üzere farklı bilişim sistemleri ve hizmetler için aynı parolanın kullanılmaması gerekir.

Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

Bu zararlı programlar,

İşletim sisteminin ya da diğer programların çalışmasına engel olabilir.

Sistemdeki dosyaları silebilir, değiştirebilir ya da yeni dosyalar ekleyebilir.

Bilişim sisteminde bulunan verilerin ele geçirilmesine neden olabilir.

Güvenlik açıkları oluşturabilir.

Başka bilişim sistemlerine saldırı amacıyla kullanılabilir.

Bilişim sisteminin, sahibinin izni dışında kullanımına neden olabilir.

Sistem kaynaklarının izinsiz kullanımına neden olabilir.

Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

Virüsler

- Bulaştıkları bilgisayar sisteminde çalışarak sisteme ya da programlara zarar vermek amacıyla oluşturur.

Bilgisayar Solucanları

- Kendi kendine çoğalan ve çalışabilen, bulaşmak için ağ bağlantılarını kullanan kötü niyetli programlardır.

Truva Atları

- Kötü niyetli programların çalışması için kullanıcının izin vermesi ya da kendi isteği ile kurması gerektiği için bunlara Truva Atı denmektedir

Casus Yazılımlar

- İnternet'ten indirilerek bilgisayara bulaşan ve gerçekte başka bir amaç ile kullanılsa bile arka planda kullanıcıya ait bilgileri de elde etmeye çalışan programlardır.

Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

Zararlı Programlara Karşı Alınacak Tedbirler

- Bilgisayara anti virüs ve İnternet güvenlik programları kurularak bu programların sürekli güncel tutulmaları sağlanmalıdır.
- Tanınmayan/güvenilmeyen e-postalar ve ekleri kesinlikle açılmamalıdır.
- Ekinde şupheli bir dosya olan e-postalar açılmamalıdır. Örneğin *resim.jpg.exe* isimli dosya bir resim dosyası gibi görünse de uzantısı *exe* olduğu icin uygulama dosyasıdır.
- Zararlı içerik barındıran ya da tanınmayan web sitelerinden uzak durulmalıdır.
- Lisanssız ya da kırılmış programlar kullanılmamalıdır.
- Güvenilmeyen İnternet kaynaklarından dosya indirilmemelidir.