BİLGİ GÜVENLİĞİ

- 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.

1.3.2 Bilgi Güvenliği Nedir?

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 Güvenliği üç temel öğeden meydana gelir

1-Gizlilik

2-Bütünlük

3-Erişilebilirlik

1-Gizlilik

Bilginin yetkisiz kişiler tarafından görünmesi engellemek için gizlenmesi gerekmektedir.

Örnek: E-posta veya kullanıcı hesap bilgilerinin bir başkaları tarafından ele geçirilmesi gizlilik ihlaline girer. Bu gibi bilgiler gizlenmelidir.

2-Bütünlük

Bilginin yetkisiz kişiler tarafından değiştirilmesi veya silinmesi bilgi bütünlüğüne zarar verir.

Bilgi güvenliği için bütünlüğün sağlanması ve tehditlere karşı korunması gerekmektedir.

Örnek: Bir web sayfasında yer alan bilgilerin saldırgan tarafından değiştirilmesi, bütünlük ilkesinin bozulmasına örnek verilebilir.

3-Erişilebilirlik

Erişilebilirlik ise bilginin ihtiyaç duyulduğunda ulaşılabilir ve kullanıma hazır durumda olmasıdır.Bilgi Güvenliği için bilgiye istediğimiz zaman erişebilmeliyiz.

ÖRNEK: Bir web sitesine erişimin saldırı sonucunda engellenmesi erişilebilirlik ilkesinin ihlal edilmesine örnek olarak verilebilir.

BİLGİ:DDOS(Distributed Denial Of Service-Dağıtık hizmet engelleme) saldırıları internet sitelerine ulaşılmasını engeller

1.3.2 Bilgi güvenliğine yönelik tehditler

Siber ve Siber Uzay nedir?

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

Siber güvenlik; siber ortamda yaşanabilecek suç, saldırı, terörizm, savaş, gibi tüm kötü niyetli hareketlere karşı alınacak tedbirler bütünüdür.

Bilgi Güvenliğine Yönelik Tehditler

- Bilişim teknolojileri güvenliğinde başlıca tehdit, korsan, hacker yada saldırgan olarak adlandırılan kötü niyetli kişiler ve bu kişilerin yaptıkları saldırılardır.
- Bir bilişim(bilgi ve iletişim) sistemine sızmak, sistemi zafiyete uğratmak, sistemlerin işleyişini bozmak ve durdurmak gibi kötü niyetli davranışlar; **siber saldırı** veya **atak** olarak adlandırılmaktadır.

Siber ortamda yaşanabilecek kötü niyetli hareketler aşağıda tanımlanmıştır:

Siber Suç: Bilişim teknolojileri kullanılarak gerçekleştirilen her tur 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 hükümetleri, 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.

Siber Alemde Parola ve Kimlik Yönetimi

Parola ve Şifre nedir

Parola: Bir hizmete erişebilmek için gerekli olan, kullanıcıya özel karakter dizisidir.

Örnek: E-mail hesabımıza ve diğer sosyal medya hesaplarına girmek için kullandığımız parolalar

Şifre: Ortamdaki verilerin gizliliğini sağlamak için veriyi belirli bir algoritma kullanarak dönüştüren yapıdır.

Örnek:https// ile web sayfası ve sunucu arasındaki veriler şifrelenerek aktarılmaktadır.

Bilişim Sistemlerine Erişim

Bir bilişim sistemine erişimin belli kurallar çerçevesinde yapılması amacıyla o sistemi kullanmak isteyen kişilerin kullanıcı adı ve/veya parola ile erişim yetkisine sahip olduklarını ispatlamaları gerekmektedir. Buradaki kullanıcı adı ve parola, bilgiye erişim yetkisinin kanıtı olarak kullanılmaktadır.

Bilgi: Kullanıcı adı o sistemde benzersiz olmalıdır. E-mail, T.C numarası gibi

Kullanıcı adı ve parolanın başka kişilerin eline geçmesi durumunda yaşanabilecek durumlar

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

Parola Nasıl Olmamalı?

1-Sadece rakamlardan oluşmamalı

2-Başkalarının kolayca tahmin edebileceği qwery,123456 gibi parolalar kullanılmamalı

3-Doğum yılı, mezuniyet yılı gibi şeyler parola olarak kullanılmamalı

Parola Nasıl olmalı?

- 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.

Örnek Parolalar

Als@nc@k+Tw€
+Al@t_Fb.
Y1Lw@z-Tw

Anahtar kelime oluştururken;

- G yerine 6,
- g yerine 9,
- Ş yerine $
- a yerine @
- i, l yerine 1 gibi karakterler kullanılabilir.

Parolanın Güvenliği Acısından, Aşağıdaki Kurallara Dikkat Edilmelidir

- Parolanın başkalarıyla paylaşılmaması son derece önemlidir.
- Parolalar, basılı ya da elektronik olarak hicbir yerde saklanmamalıdır.
- Başta e-posta adresinin parolası olmak üzere farklı bilişim sistemleri ve hizmetler için aynı parolanın kullanılmaması gerekir.

1.3.3. Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

Bilişim sistemlerinin calışmasını bozan veya sistem içinden bilgi çalmayı amaçlayan Virüs, Solucan, Truva Atı ya da Casus yazılım gibi kötü niyetlerle hazırlanmış yazılım veya kod parçaları zararlı programlar olarak adlandırılır.

Zararlı Yazılımların Etkileri

- 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.

Zararlı Yazılımları Tanıyalım

«**Virüsler**: kullanıcının izni ya da bilgisi dahilinde olmadan bilgisayarın çalışma şeklini değiştiren , dosya ve programların yapısını bozan - silen, kendini diğer dosyaların içerisinde gizlemeye çalışan aslında bir tür bilgisayar programıdır.»

Virüsler bilgisayara e-posta, Depolama Aygıtları, Yerel ağ ve İnternet üzerinden bulaşabilir.

Bilgisayarın yavaşlaması, programların çalışmaması, dosyaların silinmesi, bozulması ya da yeni dosyaların eklenmesi , hatalar ve uyarılar virüs belirtisi olabilir.

Solucanlar(Worms); kendi kendine çoğalan ve çalışabilen, bulaşmak için ağ bağlantılarını kullanan kötü niyetli programlardır. Sistem için gerekli olan dosyaları bozarak bilgisayarı büyük ölçüde yavaşlatabilir ya da programların çökmesine yol açabilir. Ayrıca sistem üzerinde arka kapı olarak adlandırılan ve saldırganların sisteme istedikleri zaman erişmelerini sağlayan güvenlik açıkları oluşturabilir.

Truva Atları: Bilgisayarı içten ele geçirmeyi hedefler. Asıl amacı kullanıcının bilgisayarına sızmak ve bir süre sonra bilgisayarı uzaktan ele geçirmektir.

Truva atları bilgisayar korsanlarının bilgisayarınızdaki kişisel ve gizli bilgilerinize ulaşmalarına imkân tanıyan gizli kapılar da yaratırlar.

Bulaşma yolları çeşitlidir,

- Güvenilir olmayan sitelerden dosya veya program indirilmesi
- Yasal olmayan kopya yazılımların kullanılması ile bulaşabilirler.

Casus Yazılımlar, Bu tür zararlı yazılımlar genellikle kullanıcı hakkında bilgi toplamayı amaçlayan yazılımlardır.

- Kullanıcıların hangi siteleri sıklıkla ziyaret ettiği, kimlere e-posta gönderdiği, kimlerle sohbet ettiği hangi programları kullandığı ile ilgili bilgileri sizin izniniz olmadan toplar ve casus yazılım sahibine iletir.
- Güvenilir olmayan web sitelerinden bulaşabilir.

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 şüpheli bir dosya olan e-postalar açılmamalıdır. Örneğin *resim.jpg.exe* isimli dosya bir
- resim dosyası gibi görünse de uzantısı *exe* olduğu için uygulama dosyasıdır.
- Zararlı icerik barındıran ya da tanınmayan web sitelerinden uzak durulmalıdır.
- Lisanssız ya da kırılmış programlar kullanılmamalıdır.
- Güvenilmeyen İnternet kaynaklarından dosya indirilmemelidir.
- Güvenlik duvarı aktif hale getirilmelidir.