ÜNİTE 2: BİLİŞİM GÜVENLİĞİ

Giriş

Günümüzde; virüsler, bilgisayar korsanları (hackers), elektronik sahtekarlık, sistemlere izinsiz erişimler, bireysel veya kurumsal bilgilerin çalınması, sızdırılması ve özel hayata dair bilgi ve görsellerin ele geçirilip paylaşılması gibi konular güvenlik sorunu olarak hayatımıza girmektedir. Bilginin üretilmesi ve paylaşılması yaygınlaştıkça bilgisayar ve ağlara olan bağımlılık da giderek artmıştır. Paylaşılan bilgi ve verilerin güvenliği ve korunması konusunda yaşanılan kötü tecrübeler bilgi ve verinin korunması anlamındaki duyarlılığı arttırmıştır. Başlangıçta sıralanan bu sorunlara çareler aranmış ve çözümler geliştirilmiştir.

Bilişim Güvenliği ve Temel İlkeleri

Günümüz koşullan farklı kültürden bireyler ve kurumlarla rekabeti gerektirmektedir. Bilişim teknolojileri sayesinde insanlar farklı ürünleri karşılaştırabilmektedir. Diğerleri ile iletişim kurabildiğimiz, haberleşebildiğimiz ve paylaşımda bulunabildiğimiz teknolojiler güvenlik ve güvenliğin sağlanması sorunlarını da beraberinde getirmektedir. Bilgi ve iletişim teknolojilerini kullanırken olası tehdit ve tehlikelerin önceden farkına varılması ve gerekli önlemlerin alınmasını gerektiren bir konu olarak tanımlanan bilişim güvenliğinin amacı teknolojinin kendisine, bilgiye ve veriye yetkisiz bir biçimde erişilmesi, kullanılması, değiştirilmesi, ifşa edilmesi, ortadan kaldırılması, başkalarının eline geçmesi, zarar verilmesi gibi tehditlerin bilinciyle hareket etmek, gerekli önlemleri almak ve bu konudaki olası zararları ve kayıpları önlemektir. Bilişim güvenliği konusu gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) şeklinde üç temel ilkeden oluşmaktadır (S: 40, Şekil 2.1). Öte yandan izlenebilirlik veya kayıt tutma (accountability), kimlik sınaması (authentication), güvenilirlik (reliability-consistency) ve inkar edememe (non-repudiation) şeklinde ilkeler de odaya atılmaktadır (S: 40, Tablo 2.1). Gizlilik: Veri gizliliği ve kullanıcı gizliliği şeklinde iki başlık altında incelenebilecek olan gizlilik ilkesi, kullanılan sistemin ve sistemdeki verilerin yetkisiz kişilerin eline geçmesine, izinsiz erişilmesine ve kullanılmasına karşı korunmasıdır. Bütünlük: Veri bütünlüğü ve sistem bütünlüğü olmak üzere ikiye ayrılan bütünlük ilkesi, sistemi ve sistemde bulunan veriyi olması gerektiği şekilde muhafaza etmektir. Erişilebilirlik: Erişilebilirlik ilkesi, bilginin her an ulaşılabilir ve kullanılabilir olmasını gerektirmektedir. Kurum içi veya dışından gelecek saldırılar, bilinçsiz, yanlış ve dikkatsiz kullanımlar ile yangın, yıldırım veya deprem gibi çeşitli etkenler erişilebilirliğe zarar verebilir. İzlenebilirlik: İzlenebilirlik ilkesi, kullanıcıların sisteme girişleri, alınıp gönderilen e-postalar, çeşitli servis ve yazılımların çalıştırılması, durdurulması gibi bilgisayar sistemi ya da ağ üzerindeki her türlü olayların daha sonra incelenebilecek şekilde kayıt altında olması ile ilgilidir. Kimlik Sınaması: Kimlik sınaması ilkesi, sistemi kullanmak üzere yetkilendirilen kişinin, sistem veya herhangi bir program sorguladığında, aynı kişi olduğunu belgelemesi ile ilgilidir. Parmak izi veya diğer biyometrik kimlik tanıma uygulamaları da günümüzde örnek verilebilmektedir. Güvenilirlik: Güvenilirlik ilkesi, sistemin öngörülen ve kendisinden beklenen performansı ile ortaya çıkan sonuçların tutarlılığı ile ilgilidir. İnkar Edememe: Özellikle internet üzerinden ticaret ve bankacılık işlemlerinde oldukça önemli bir konu olan inkar edememe ilkesi, bilgilerin ve verinin paylaşıldığı kullanıcılar arasında doğabilecek anlaşmazlıkların, güvenli bir şekilde nasıl çözüldüğü ile ilgilidir.

Bilgisayar Sistem Ve Ağ Güvenliğini Tehdit Eden Kötü Amaçlı Yazılımlar

Masaüstü gibi sabit sistemlerde ya da taşınabilir sistemlerde sistem güvenliğinden bahsetmek için elektronik ortamlarda bulunan bilgi ve verinin bütünlüğünün korunması, izinsiz erişilip değiştirilmemesi, silinmemesi ve paylaşılmaması gerekmektedir. Birbirine ağlar aracılığı ile bağlı bulunan bilgisayar sistemlerinin ve ağ güvenliğinin sağlanabilmesi için kötü amaçlı yazılımlardan (malware) haberdar olmak gerekmektedir. Bilgisayar sistemlerine zarar vermek, bilgi çalmak, kötü amaçla kullanmak, kullanıcıları rahatsız etmek ve benzeri nedenlerle hazırlanmış yazılımlara genel olarak kötü amaçlı yazılımlar denir. Kötü amaçlı yazılımlar aşağıdaki başlıklarda açıklanmaktadır:

Virüsler: Kendilerini çoğaltmak ve belirli bir zamanda kendilerini çalıştırmak şeklinde işlevleri bulunan virüsler, kullanıcının izni veya bilgisi olmaksızın sistemin işleyişini değiştiren ve kendisini diğer program veya dosyaların içinde gizleyen programlardır. Farklı şekillerde bulaşıp yayılabilen binlerce farklı türdeki virüs, kullanıcının fark edemeyeceği küçük hasarlardan, sistemlerin çökmesine veya verilerin zarar görmesine kadar geniş bir yelpazede zarar verebilmektedir. Başlıca virüs türleri; dosya sistemi virüsleri, ön yükleme (boot sector) bölümü virüsleri, makro yazılım virüsleri, web komut dosyası (web scripting) virüsleri, ağ virüsleri ve yazılım bombalarıdır(s:43, Tablo 2.2). Genellikle ".exe" veya ".com" uzantılara sahip dosyalarla bulaşan dosya sistemi virüsleri en sık rastlanılan virüslerdendir. Virüsün bulaştığı dosyalar çalıştırıldığında, virüs etkin duruma geçerek diğer program dosyalarına da yayılarak programlandığı gibi sisteme zarar vermeye başlar. Ön yükleme (Boot Sector) virüsleri, bilgisayar sistemindeki sabit diskin ilk sektörü olan, hangi bilginin nerede olduğuna dair verileri içeren ve bilgisayar sisteminin bir tür adreslemesinin yer aldığı "Master Boot Record" (MBR) bölümünü etkiler. Makro yazılım virüsleri makrolar içeren (Microsoft Office'in Word, Excel, PowerPoint uygulamaları gibi) çeşitli program ve uygulamalarca oluşturulan dosyalara bulaşırlar. Makro virüsleri programlar tarafından kullanılan çeşitli komut setlerinin yerine geçerek, kodlandıkları kötü amaçlı yazılımları sisteme geçirmiş olurlar. Bilinen en ünlü ve zarar verici makro virüsü, 1999 yılında David Smith tarafından geliştirilen virüstür. Smith, virüse Melissa ismini vermiştir. Eklenti olan word belgesi sisteme indirildikten sonra, kendini kullanıcının e-posta hesabında çoğaltarak listedeki ilk 5ü kişiye otomatik olarak posta göndermek üzere programlanmıştır. Bu makro virüsün sebep olduğu hasar toplam 80 milyon dolar olarak rapor edilmiş ve 1 milyondan fazla bilgisayar sistemine bulaştığı ifade edilmiştir. Web üzerinde gezinti yapan hemen herkes web komut dosyası virüsleri ile karşılaşabilmektedir. Web sayfalarında bulunan reklam ve benzeri paylaşımlardan bulaşan bu tür virüslerin bulaştığı bilgisayar sistemlerinde genel bir yavaşlama fark edilebilir. "Script" ön adlı olan ve Javascript gibi ileri programlama dilleri ile yazılan web komut dosyası virüsleri sosyal ağlar, kullanıcı görüş ve yorumları, e-posta gibi yoğun katılımcı sayası olan sitelerde yaygın olarak görülmektedir. Ağ virüsleri, yerel ağlarda veya İnternet üzerinde, bilgisayar sistemleri arasında paylaşılan kaynaklar ya da klasörler üzerinden yayılarak, ağdaki diğer sistemlere de bulaşan virüs türleridir. Ağ virüsleri, herhangi bir sisteme bulaştıklarında ağ üzerindeki savunmasız sistemi bularak tüm ağa yayılırlar. Bu tür virüslerin, diğerlerinden farkı banka hesapları, elektronik posta, sosyal ağ hesapları ve diğer kişisel bilgi ve verileri de bulup, diğer şahıslarla paylaşabilmeleridir. Yazılım bombaları, gerekli şartlar oluşana dek bekleyen ve bu şartlar oluştuğunda özel bir takım yazılımları etkinleştiren yazılımlardır. Solucanlar: Virüslerden farklı olarak genellikle işletim sistemlerinin hata ve açıklarını kullanarak ağ üzerinden sistemlere bulaşan solucanlar, daha çok e-posta ile gönderilen ekler, çeşitli web siteleri ve ağ üzerinden paylaşılan dosyalar aracılığıyla yayılırlar. Kullanıcılar tarafından bir programın çalıştırılması gerekmeden solucanlar kendileri ağları tarayarak, güvenlik açığı

buldukları sisteme girerler ve oradan da içinde bulundukları bilgisayar sisteminin veri kaynaklarını kullanarak diğer sistemlere yayılmaya çalışırlar. Truva Atları: Kullanıcılara kendisini faydalı bir yazılım olarak göstererek, bilgisayara indirilmesini sağlar. Ancak yanlarında getirdiği yazılımı yazan kişinin çalıştırarak karşı bilgisayara zarar vermek üzere hazırladığı, zararlı programı içeren dosya çalıştırıldığında sistemde dışarıdan gelecek etkilere yönelik bir kapı (port) açmış olur. Casus Yazılımlar (Spyware): "adware" olarak da isimlendirilen casus yazılımlar, İnternet tarayıcı programlarının yazılım açıklarından faydalanarak, kullanıcıların Web'de gezinmeleri sırasında bulaşabildikleri gibi, kullanıcıların kaynağı belirli olmayan veya başka amaçlara hizmet ediyormuş gibi görünen programları çalıştırmasıyla sisteme bulaşırlar. Casus yazılımlar sisteme sızarak kullanıcıların ne tür web sitelerinde gezindiği bilgilerini toplar ve bu bilgileri bir merkeze iletir. Çöp e-Posta (Spam): Spam veya yığın mesaj olarak da adlandırılan çöp e-postalar, kullanıcıların izni ya da isteği olmadan kendilerine gönderilen ve genellikle reklam içerikli olan rahatsız edici elektronik postalardır. Bazı virüs türleri de e-posta adres defterinizde bulunan adreslere sürekli spam mesajlar atmaya başlayabilir.

Kötü Amaçlı Yazılımlara Karşı Korunma

Kötü amaçlı yazılımlardan korunmanın en temel yolu, bilgisayar sisteminde etkili bir antivirüs (virüs koruma) programını bulundurmak ve çalıştırmaktır. Bunun dışında casus yazılımlar için belirli aralıklarla sistem taraması yapmak, güvenilir görünmeyen e-posta eklerini ve bağlantılarını çalıştırmamak ve güvenilir görünmeyen web sitelerinde gezinmemek kötü amaçlı yazılımlara karşı alınabilecek önlemlerden sadece birkaçıdır. Antivirüs ve Casus Önleyici (Antispyware) Yazılımlar: Bilgisayar sistemlerini virüslere karşı koruyan programlara antivirüs, casus yazılımlara karşı koruyan programlara da casus önleyici (antispyware) yazılımlar denir. Antivirüs ve casus önleyici yazılımlar kötü amaçlı yazılımlar bilgisayar sistemine girip bulaşmaya çalıştıklarında fark ederek, engel olan yazılımlardır. Sürekli güncellenebilen bu tür önleyici programlar sistem her açıldığında otomatik başlayacağı için anlık kontrollerde bulunabilmektedir. Antivirüs ve casus önleyici yazılımların kullanıcılara sağladığı yararlar sayfa 48'de sıralanmaktadır. Kötü Amaçlı Yazılımlardan Korunmak İçin Alınabilecek Önlemler: Bilgisayar sistemine antivirüs ve casus önleyici programları kurmak çoğu zaman kötü amaçlı yazılımlardan korunmak için tek başına yeterli olmayabilmektedir.

Bu koruyucu ve denetleyici programların yanında kullanıcıların da alması gereken bazı önlemler ve atması gereken bazı adımlar bulunmaktadır (s:49-50, Maddeler). Kişisel Güvenlik Duvarı (Firewall): Evimizi çevreleyen duvarlara ve bu duvarların bir parçası olan kapıya benzetebileceğimiz kişisel güvenlik duvarları, İnternet üzerinden gelen verileri denetleyerek, kullanıcının oluşturduğu ayarlar çerçevesinde ağ yoluyla bilgisayar sistemlerine sızıp yayılmaya çalışan kötü amaçlı yazılımları engelleyen, kullanıcının izin verdiği verilerin de geçmesine olanak tanıyan yazılımlardır (s:51, Şekil 2.2). Güvenlik duvarları, bu geçiş olanağını kullanıcıların belirlediği kurallar ve ayarlar ile sisteme gelen ve giden veri (paket) trafiğini kontrol ederek sağlamaktadır.

İnternette Güvenliği Sağlama

İçinde bulunduğumuz bilgi çağının en önemli faktörlerinden biri olan internet çok sayıda tuzak, yanlış bilgi, yönlendirme ve kötü niyetin de merkezi durumundadır. Oysa kullanıcılar için internet; özgürlük, bilgiye erişimdeki sınırsızlık, hız ve esnekliktir. Bu ortamdaki bilginin ve kaynağın sürekli sorgulanması, doğru ve güvenilir bilgiye ulaşıldığından emin olunması gerekmektedir. İnternette ulaşılan bilginin çoğunun kaynağının belirsiz olduğu unutulmamalıdır. İnternette

Güvenilir Bilgiye Ulaşma: İnternette karşılaşılan her bilginin güvenilir, doğru ve samimi olmayabileceğini düşünmek ve buna göre hareket etmek, okunulan veya karşılaşılan bilgi ve bilgi kaynaklarını sorgulamak, bilgileri farklı kaynaklardan da kontrol etmek gerekmektedir(s:52, Maddeler). E- Ticaret (Elektronik Ticaret) Güvenliğini Sağlama: İnternet üzerinden yapılan alış-verişler olarak tanımlanabilen e- Ticaretteki en önemli güvenlik sorunu, alıcı ve satıcının diğer ticaret şekillerinde olduğu gibi yüz yüze olmamalarıdır. Türkiye'deki alt yapı tarafların sayısal sertifika ve imza gibi teknolojileri kullanmasını henüz olanaklı kılmamaktadır. Diğer güvenlik sorunu ise alıcıların web sitelerinden alışveriş yapmak için vermek zorunda oldukları kredi kartı ve ödeme şekliyle, kişisel bilgilerdir. Hem istemci (bilgi alan) hem de sunucu (bilgi gönderen) bilgisayarda bir kimlik sınama/doğrulama (authentication) sürecini olanaklı kılan SSL (Secure Sockets Layer) teknolojisi ile güvenli alışveriş sağlanmış olur. Sosyal Ağlarda Güvenliği Sağlama: Sosyal ağlar, kişilerin bir takım sembolik jestler ve hareketleri de kullanarak, İnternet üzerinde sanal bir toplum yaşamı içinde kendilerini tanımlamasına, internet teknolojilerini kullanarak diğer insanlarla iletişim ve etkileşim içine girmesine, paylaşmasına ve dolayısıyla kendilerini ifade etmesine olanak tanıyan ağlarıdır. İnsan sosyal topluluklar içinde yaşamaya ve paylaşmaya ihtiyaç duymuştur. Sosyal ağların yoğun olarak kullanıldığı günümüzde hayran kitlelerini oluşturan sosyal medya hesapların paylaştıkları, yazdıkları ve bildirdikleri önemli, güncel ve güvenilir olarak algılanabilmektedir. Nitekim kurumlar da farkındalık oluşturmak amacıyla sosyal medya kullanımına önem vermektedir. Zararlardan kaçınmak amacıyla sosyal ağları kullanırken bazı önemli noktaların dikkate alınması gerekmektedir (s:55, Maddeler).