SG506 BİLGİSAYAR VE AĞ GÜVENLİĞİ

ZEYNEP ÇELİK

1. ÖDEV

Bilgisayar güvenliğindeki üç temel kavram vardır. Bunlar Confidentiality (Gizlilik), Integrity (Bütünlük) ve Availability (Erişilebilirlik) olarak belirtilen CIA üçlüsüdür.

Confidentiality (Gizlilik) : Bu prensip bilginin yetkisiz kişilerin eline geçmesini engellemeyi amaçlamaktadır. Bilgi hem bilgisayar sistemlerinde, hem disk, disket, cd, dvd ve benzeri saklama ortamlarında hemde ağ üzerinde gönderici ve alıcı arasında taşınırken yetkisiz erişimlerden korunmalıdır.

Gizliliği tehdit eden saldırılara örnek olarak casus yazılımları örnek verebiliriz. Casus yazılım bilgisayarlara ve internete bağlı diğer cihazlara bulaşan; tarama alışkanlıklarınızı, ziyaret ettiğiniz web sitelerini ve çevrimiçi satın alma işlemlerinizi gizlice kaydeden kötü amaçlı bir yazılımdır. Bazı casus yazılım türleri parolalarınızı, oturum açma kimlik bilgilerinizi ve kredi kartı ayrıntılarınızı kaydeder. Bu bilgileri daha sonra kendi kişisel çıkarları uğruna şantaj için kullanabilir veya üçüncü bir tarafa satabilirler.

Diğer tüm kötü amaçlı yazılım türleri gibi casus yazılım da bilgisayarınıza izniniz olmadan yüklenir. Genellikle kendi isteğinizle indirdiğiniz (dosya paylaşım programları ve diğer ücretsiz veya paylaşılan yazılım uygulamaları gibi) yasal yazılımlarla birlikte gelir.

Ayrıca kötü amaçlı web sitelerini ziyaret ederek veya virüslü e-postalardaki bağlantılara ve eklere tıklayarak, bu yazılımları istemeden de indirebilirsiniz. Casus yazılım, yüklediğiniz anda işletim sisteminize bağlanır ve arka planda sessizce çalışmaya başlar.

Integrity (Bütünlük) : Bu prensibin amacı veriyi olması gerektiği şekilde tutmak ve korumaktır. Var olan bilginin bozulmasını, değiştirilmesini, yeni veriler eklenmesini, bilginin bir kısmının veya tamamının silinmesini engellemeyi hedefler.

Bütünlüğü tehdit eden saldırılara örnek olarak Truva atı (trojan) verilebilir. Truva atı meşru görünen ancak bilgisayarınızın kontrolünü ele geçirebilen bir tür kötü amaçlı kod veya yazılımdır. Verilerinize veya ağınıza zarar vermek, bozmak, çalmak veya başka zararlı eylemler uygulamak için tasarlanmıştır. Diğer bilgisayar virüslerinden farklı olarak diğer dosyalara veya bilgisayarlara bulaşarak kendi kendine çoğalmaz.

Trojan, diğer kötü amaçlı yazılımları kullanır ve amacını gizlemek için uzantı halinde gelir. Fark edilmeden hayatta kalmayı başaran virüs; bilgisayarınızda sessizce durabilir, bilgi

toplayabilir, güvenliğinizde delikler açabilir veya yalnızca bilgisayarınızı ele geçirebilir. Kısacası, insanları kandırmak ve zarar vermek için zararsız gibi davranan kötü amaçlı bir programdır.

Availability (Erişilebilirlik) : Bilginin her an ulaşılabilir ve kullanılabilir olmasını amaçlayan prensiptir. Bilişim sistemlerinin kendilerinden beklenen işi sürekli bir şekilde tam ve eksiksiz olarak yapmasını amaçlamaktadır.

Erişilebilirliği tehdit eden saldırılara örnek olarak DDoS saldırılarını örnek verebiliriz. Distributed Denial of Service (Dağıtık Hizmet Engelleme) kısaca DDoS, bir sistemi belirli kapasite sınırlarının üstünde veriye maruz tutma yoluyla düzenlenen saldırılar sonucu kullanıcıların sisteme veya siteye girişinin engellenmesidir. Başlangıçta DoS yani yalnızca tek bir kaynaktan hedefe saldırı yapılmasıyla ortaya çıkan saldırı türü, zamanla çok sayıda kaynaktan tek hedefe doğru yapılarak şiddeti artmıştır.

Her sistem kurulurken kullanıcı sayıları, hat kapasitesi, anlık istek sayısı gibi unsurlar için belli değerler öngörülür ve bu değerlerin biraz üstündeki bir yükü kaldırabilecek şekilde tasarım yapılır. DDoS ise sistemin kaldırabileceği yükün çok üzerinde anlık kullanıcı sayısı, anlık istek ile sistemi yorup cevap veremez hale getirerek veya hattı doldurarak sistemin erişilebilirliğini engellemeye yönelik bir saldırı türüdür.