e-Güvenlik Zirvesi

5 Nisan 2002 tarihinde, Ankara'da güvenlik zirvesi toplandı. Ancak, bu zirvenin katılımcıları genelkurmay üyeleri değil, bilgisayar güvenliği alanında hizmet veren şirketlerdi.

Son yıllarda sanal alemde yaşanan saldırıların sayısının artmasıyla birlikte, Internet'te güvenlik konusu da gündeme oturdu. 2001 yılı bilgilerine göre ülkemizde 52.658 adet güvenlik sorunu bildirimi, 2437 adet güvenlik açığı tespiti ve 50.000 virüs saldırısı yaşandı. ABD'de yaşanan her sorun ve saldırı, günü gününe Türkiye'ye ulaşıyor. Kırılma yoğunluğu sıralamasında İsrail 1., Türkiye'yse 6. sırada. Saldırıya uğrayan sitelerin dağılımıysa oldukça şaşırtıcı; devlet kurumlarına ait siteler en güvenli yerler gibi görünse de, aslında oldukça sık saldırıya uğruyorlar. Türkiye'deki tüm saldırılar arasında com.tr uzantılı sitelere yapılan saldırıların oranı %41; bu rakam gov.tr uzantılı siteler için %31. Bu ikisini, üniversiteler ve askeri siteler takip ediyor. Saldırıyı düzenleyenlerin profiliyse, oldukça geniş bir yelpazede. Eğlence amaçlı saldırı yapanlar, oldukça büyük bir kesimi oluşturuyor. Politik amaçlı saldırı yapan suç örgütleri, yabancı haber alma servisleri, siber savaş denemesinde bulunan örgütler ve kurumların kendi içindeki saldırganlarsa diğer tehdit unsurları.

Internet'in amacının dünyadaki tüm insanların birbirleriyle iletişim kurması ve bilgi alışverişinde bulunması olduğu göz önüne alınırsa 6 milyar birimlik bir ağın güvenliğiyle karşı karşıya olduğumuz ortaya çıkıyor. Bu kadar kapsamlı bir ağın güvenliğini sağlamak için, öncelikle hangi çerçevede bir güvenlikten söz edildiğinin net olarak belirlenmesi gerekiyor. Bu çerçeveyi belirleyen kilit sözcükler, bilgiye izinsiz ve yetkisiz ulaşımın engellenmesi. Ancak bu çerçevenin genelde net olarak belirlenememesi, insanların gereksiz yere Internet'ten korkmalarına neden oluyor. Internet bazı kesimler için hala yeni ve yabancı bir ortam olma özelliğini koruyor. Bu nedenle de insanları Internet'ten korkutmak, oldukça kolay. Ancak bir kez korktuklarında da, bu insanların bir daha Internet'i kullanmalarını sağlamak neredeyse olanaksız. Bu nedenle Internet'te güvenlik önlemleri alırken, oldukça özenli ve dikkatli davranmak gerekiyor. Çözüm bilgisayarlarımızı Internet'ten izole etmekten değil, Internet'e planlı ve güvenli bir biçimde açılmanın yöntemlerini öğrenip, bunları uygulamaktan geçiyor.

Günümüzde herkes hem kendisini, hem de yaptığı işi tanıtmak amacıyla Internet'te bir yeri olsun istiyor. Internet'e bağlı bilgisayar sayısı ve bu bilgisayarlardan kurulan web sitesi sayısı, her geçen gün artmakta. Bu sayılar arttıkça, Internet üzerinden gerçekleştirilen saldırıların sayısı ve çeşidi de hiperbolik olarak artıyor. Hatta eskiden tamamen güvenli kabul edilen işletim sistemleri bile, yavaş yavaş saldırılardan etkilenir hale geliyor. Örneğin yapılan saldırılara karşı Windows'dan daha güvenli olarak bilinen bir ortam olan Linux bile, eski güvenilirliğini kaybetti. Bugüne kadar Internet'e yayılıp da Windows işletim sistemine bulaşan virüsler, Linux ortamında çalışan bilgisayarları etkilememişti. Ancak Mart 2002'de her iki ortama da yayılabilen bir virüsün ortaya çıkmasıyla, Linux ortamı da saldırılara karşı güvenli olmaktan çıktı.

Internet üzerindeki e-ticaret ve bankacılık işlemleri, en çok güvenlik gerektiren alanlar. Özellikle Elektronik Fon Transferi (EFT) işlemlerinde, güvenlikle ilgili pek çok sorun yaşanabiliyor. Bu işlemler aktarım sayısı ele alındığında genel aktarımın % 0,2 sini oluşturuyor. Ancak aktarılan trilyonlarca lira paranın, değer olarak, genel dağılımın %85'ini oluşturuyor olması, EFT'leri çok önemli hale getiriyor. Bu tür işlemlerin güvenliğinde, öncelikle kurulacak ateş duvarının (firewall) mimarisi çok önemli. Hangi girişlerin yapılıp, hangilerinin yapılamayacağının tanımının yapıldığı yer olan ateş duvarları, kurum dışından gelecek saldırılar kadar, kurum içinden yapılan saldırı girişimlerini de tanımlayabilecek nitelikte olmalı. Asıl tehdit kurum dışındanmış gibi görünse de, rakamlar bunun aksini söylüyor. İçeriden kaynaklı saldırıların tüm saldırılara oranı, % 60. Kendi ücretlerini değiştirmek isteyen ya da belli bir nedenden dolayı çalıştıkları şirkete kızgın olan çalışanlar grubu, bu tür saldırıların potansiyel düzenleyicileri. Bilgisayarınızın güvenliğinde, üzerinde kurulu olan işletim sisteminin payı da oldukça büyük. Zayıf ve ayakta kalamayacak bir sistemle çalışıyorsanız, alacağınız diğer önlemler pek işe yaramıyor. Antivirüs yazılımları da, güvenliğin önemli bir unsuru. Kullanılacak yazılım, virüsleri bilgisayarınıza girmeden önce tanımlayabilecek türde bir virüs yazılımı olmalı. En önemli şeyse, sizin Internet'e çıkarken neye, ne kadar izin verdiğiniz. Bunu doğru şekilde belirleyemezseniz, yukarıdaki önlemlerin hiçbiri etkili olamıyor.

Internet Güvenliğiyle İlgili 10 Yanlış İnanış

1. Internet güvenliği için ateş duvarı (firewall) gereksizdir.
2. Yalnızca ateş duvarı kullanımı, güvenlik için yeterlidir.
3. Şifre kullanımı, sistemi korur.
4. Asıl tehdit kurum dışındadır. Bu nedenle kurum içi güvenlik tedbiri almak gereksizdir.
5. Hackerlar, web sayfalarına saçma sapan yazılar yazan, zararsız çocuklardır.
6. Zaten bana kimse saldırmaz.
7. Şirket içindeki sunucular, saldırıya uğramaz.
8. Sistemimdeki kullanıcılara, tamamen güvenebilirim.
9. Bilgisayar güvenliği bir lükstür.
10. Bana bir şey olmaz. Kötü şeyler, hep başkalarının başına gelir.

Bugünlerde en çok üzerinde konuşulan teknolojilerden biriyse, VPN (Virtual Private Networks). Uzaktan erişim ve algılama anlamına gelen bu yöntem, bağlantıya geçtiğiniz nokta ile bağlanılan yer arasındaki bilgilerin şifrelenmesini sağlıyor. İlk ortaya çıktığında güvenlik alanındaki çoğu sorunun üstesinden gelen bu teknoloji, yaygınlaştıkça etkisini de yitirdi. Çünkü VPN yaygınlaştıkça, saldırganlar da kendilerine bununla baş etmek için yeni yöntemler buldular. Örneğin, sisteminde VPN bulunan bir şirketin iç ağına girmeyi başardılar. Bunun temel nedenlerinden biri, VPN teknolojilerinin genelde kullanıcı tarafını desteklemiyor olması. Örneğin bir banka tarafından yapılan finansal bir işlem söz konusu olduğunda, VPN kullanıcıyı değil de bankanın haklarını koruyor. Oysa ki kullanıcı tarafında da ciddi güvenlik önlemlerine gereksinim var. Hatta yalnızca kullanıcının makinesinin korunması, tek başına yeterli değil. Tam bir güvenlik için, dijital imza ya da sertifika yoluyla o makineyi kullanan kişinin de doğrulanması gerekiyor.

Saldırıların çoğu, yaşanmadan önce akıl almaz ve gerçekleşemezmiş gibi gelen örnekler. Bu da, kişilerin gerekli ve yeterli önlemleri almayı ihmal etmelerine neden oluyor. Örneğin bir barajı kontrol eden bir sistem kırılabilir mi sorusu, çoğumuz için belki de oldukça komik. Ancak 1999 yılında California'da birçok barajı komuta eden bir merkezin kırılması sonucunda yaşananlar, pek de komik değildi. Bilginin hakimi (Infomaster) isimli bir saldırgan, California'nın kuzey bölgesindeki tüm barajların komuta sistemini ele geçirerek, bu bölgeye verilen tüm suyu kontrol altına aldı. 1999 yılında, oldukça sıkı güvenlik önlemleriyle korunan ABD Dış İşleri Bakanlığı sitesi kırıldı. Bu olayın sonrasında bakanlık gerekli önlemleri almadığından, olayın şaşkınlığını üzerinden atamadan bir yıl içinde tekrar kırıldı. Tedbirsizlik ve vurdumduymazlık açısından, ülkemizde de durum pek farklı değil. Türkiye'deki şirket ve kurumların %65'inin ateş duvarı bile yok. %90'ında sızma tespit sistemi kurulu değil ve %98'inin elektronik güvenlik politikası yok. Gelişen teknolojiyle birlikte yalnızca kendi olanaklarımızın değil, ortalığı karıştırmak isteyen kişilerin gereksinim duyduğu bilgi miktarının da azaldığını unutmamakta yarar var. Internet'e bağlanırken içimizin rahat olması için, bilgisayarımızdan dünyaya açılan kapımızı genişlettikçe, kapıdaki güvenlik görevlilerini de daha özenli seçmemiz gerekiyor. Günümüzde var olan bilginin yalnızca % 0 - %20'lik bir bölümü, Internet üzerinden ulaşılabilir durumda. Yani hala ulaşamadığımız birçok bilgi var. Bu durumun nedenlerinden biri, insanların neyi nasıl Internet'e koyacaklarını hala bilmiyor olmaları. Ancak asıl neden, Internet'in yapılan saldırılar etkisiyle güvensiz bir ortam olarak görülmesi ve bu nedenle kişilerin ellerindeki bilgileri bu ortama açmak istememeleri. Bu da gösteriyor ki, Internet daha güvenli bir ortam haline geldikçe, yalnızca bize ait bilgilerin güvenliğiyle ilgili olarak rahatlamakla kalmayıp, daha fazla sayıda bilgiye de ulaşabileceğiz.

Ayşenur Topçuoğlu