Uzaklarda arama, belki de içeridedir

Yatırımcı ilişkileri yalnızca yatırımcıyla mı ilgilenir? Konularımız yalnızca raporların püf noktaları, nasıl road show'a çıkarız sorusunun yanıtı, hangi iletişim aracını nasıl kurgularız sorularının yanıtlarından oluşmamalı... Umarım siz de benimle aynı fikirdesiniz, bugün kaçınılmaz parçamız internet ve güvenliğiyle ilgili aktaracaklarım var.

Bilgisayar ağlarının korunması ve güvenliğin üst düzeyde tutulması, tartışılmaz bir öneme sahip. Kurumlar, binlerce dolarlık yatırımlarla ağlarını dış dünyadaki tehlikelere karşı koruyorlar. Ancak tehlike yalnızca dışarıda değil, hatta esas tehlikenin içeride olduğunu söylemek abartısız bir gerçeğe işaret ediyor. Çünkü gerçekleştirilen yatırımlar ve alınan önlemler, şirketlerin bilgisayar ağlarını çoğu zaman dış dünyaya karşı korunaklı bir yapıya kavuşturuyor. Dışarıdan erişmek ve zarar vermek neredeyse imkansız hale geliyor. Peki ya içerisi?

Yaprak Özer
İndeks İçerik İletişim Danışmanlık CEO

İçerideki tehlikelere karşı önlem alabilmenin ilk adımı bu tehlikelerin farkında olmak. Chip tarafından derlenen bir çalışma, kurumların altyapılarını ve çok önemli bilgilerini emanet ettikleri ağlarını tehdit eden unsurları gözler önüne seriyor. Bazıları büyük tedbirler gerektirse de bazıları biraz daha dikkatle etkisiz hale getirilebilecek temel "iç tehdit"ler şöyle:

USB bellekler: Ağları en çok tehdit eden unsurların başında USB bellekler geliyor. USB bellekler bilişim dünyasının fareleri ya da sivrisinekleri olarak da adlandırılabilir. Virüslerin yayılmasına neden olan sivrisinekler gibi USB bellekler de bir bilgisayardan aldıkları zararlı yazılımı bağlandıkları her bilgisayara bulaştırabilme potansiyeli taşırlar. Bilgisayarların "otomatik çalıştır" özelliği devre dışı bırakılarak USB belleklerin, bilgisayara takıldıkları anda otomatik çalışmaları ve yazılımların aktif hale gelmesinin önüne geçebilmek mümkün.

Dizüstü bilgisayarlar: Sisteminizi dışarıdan gelebilecek saldırılara karşı korudunuz. Şirket içindeki tüm bilgisayarlarınızda güvenlik kalkanları devrede! Peki ya dışarıdan gelen misafir bilgisayarlar ya da çalışanlarınızın dizüstü bilgisayarlarının dışarıdan taşıdıklarına hazırlıklı mısınız? Üstelik dizüstü bilgisayarlar yalnızca dışarıdan taşımakla kalmıyor, bilgileri dışarıya da taşıyabiliyorlar. Dizüstü bilgisayarlarda kayıtlı, şifrelenmemiş önemli şirket bilgileri çoğu zaman kurumların sıkıntılar yaşamasına neden olabiliyor. Şirket dışına çıkan bilgisayarlar verileri de dışarıya taşımış oluyor. Tehlikenin en alt düzeye indirilebilmesi için dizüstü bilgisayarlarda taşınan verilerin şifrelenmesi büyük öneme sahip.

Kablosuz bağlantı: Kablosuz erişim noktaları, yapısı gereği, bir şifreleme kullanılsın veya kullanılmasın tam olarak güvenli değildir. Kablosuz şifreleme protokollerinin, bilinen bazı açıkları vardır. Çeşitli yazılımlar aracılığıyla bu açıklardan kolaylıkla faydalanılabilir. Tehlikeyi azaltmak amacıyla güçlü bir kablosuz ağ sunucusu ve kırılması zor bir şifre kombinasyonu kullanılmalı. Ayrıca kurumun gerçekten ihtiyacı yoksa kablosuz ağ yerine artırılmış güvenlik olanağı sunan kablolu ağlar tercih edilmeli.

USB cihazlar: USB bellekler, ağınızı USB üzerinden tehdit eden tek risk faktörü değil. Birçok cihaz, veri depolama ve çoğu işletim sistemi üzerinde bunları kullanma yeteneğine sahip. Bu cihazların temel işlevi dosya depolamak olmadığı için genellikle gözden kaçırılabilirler. Gerçekte ise ağınızdaki bir bilgisayar, bu

cihazlardaki dosyaları çalıştırabilir ve okuyabilir. Dijital fotoğraf makineleri, müzikçalarlar, yazıcılar, tarayıcılar, faks makineleri ve hatta dijital fotoğraf çerçevelerinin belleğinde gizli bir yazılım kolaylıkla ağınıza sızabilir ve sisteme zarar verebilir. Çalışma ortamına sokulabilecek cihazlar hakkında detaylı bir direktif hazırlanmalı ve sıkı bir şekilde kontrol edilmelidir.

Optik medyalar: Amerikan askeri istihbarat uzmanlarından bir kişi, gizli bilgileri halka açık ağlara sızdırma gerekçesiyle 2010 yılının Haziran ayında tutuklanmıştı. Kaynaklara göre bu bilgi sızdırma, içeriye sokulan ve üzerinde popüler bir şarkıcının adının bulunduğu müzik CD'si ile yapılmıştı. Ağa girme yetkisi olan bir kişi, şifreli veya açık gizli bilgileri, "müzik" CD'lerine aktarabilir. Yazılabilir medyalar, farklı bir içerik taşıyormuş gibi gösterilerek, ağınızdan veri çıkarmak veya ağa veri sokmak maksadıyla kullanılabilir. Optik medyalar da, en az USB bellekler kadar ağınızı tehdit eder. USB cihazlar riskinin çözümünde olduğu gibi, çalışma ortamına sokulabilecek aygıt ve araçlar dikkatle değerlendirilmeli ve kesin direktifler sıkı kontrollerle birleştirilmelidir.

İç tehditler: Şirket içindeki çalışanlar kasten veya istemeyerek, ağınızda girmemeleri gereken bir bölüme erişebilirler ve kötü amaçlarla kullanabilirler. Söz konusu çalışan, bir arkadaşı ayrıldığında, örneğin yemeğe çıktığında bilgisayarını ödünç almış da olabilir. Belki de erişemediği bir sisteme giriş için, iş arkadaşından yardım istemiştir. Erişim şifreleri düzenli olarak değiştirilmeli ve her çalışana özel giriş şifreleri bulunmalı. Her çalışanın, giriş yapabileceği alanları belirleyen yetki seviyeleri bulunmalı. *Kaynak: Chip*