Bilişimle İş Hayatı ve Güvenlik

Bilg. Müh. Berhan Soylu
berhan.soylu@emo.org.tr

Bilişim sektörü geliştikçe yeni tehlikeler türemekte ve gün geçtikçe güvenliğin önemi daha da artmaktadır.

İş hayatında bilişim deyince aklımıza ilk olarak bilgisayar teknolojisi ile haberleşme, hesap yapma ve bilgi muhafazası gelir. Bunlar temel işlevlerdir. Bu temellerin üzerlerine binen katlar ile bu teknoloji; işlerimizi hızlandıran, iyileştiren, düşünmemizi kolaylaştıran hatta bizim yerimize düşünebilen dev bir sektör haline gelmiştir. Her sektörde olduğu gibi bu sektörde de güvenlik; sektör büyüdükçe önemi artan ayrı bir meslek haline gelmiştir. Peki güvenlik neden önemlidir?

Yaşadığımız yerlerin kapısını kilitliyoruz, pencerelerde perde kullanıyoruz, önemli evraklarımızı kasamızda saklıyoruz, dışarıda arabamızın kapısını iyice kontrol edip kilitliyoruz, hatta arabamızda alarm kullanıyoruz. İş hayatında bilişim teknolojilerinde de, benzer önlemler alınmaktadır ve alınmalıdır. Çünkü güvenlik zaman, para, verimlilik, emek, bilgi gibi kriterler; iş hayatında riske atılamayacak değerlerin başında yer almaktadır. Şimdi, ne gibi güvenlik sorunları çıkabileceğini ve ne gibi çözümleri olduğunu en sık karşılaşılan şekilleri ile incelemeye başlayabiliriz.

Öncelikle basit bir senaryo ile başlayalım. Düşünelim ki bir şirketimiz var ve 5 adet bilgisayar bulunmakta. Bir tanesinde muhasebe programı bulunmakta ve bütün bilgisayarlar birbirine bağlı durumdalar. İnternet kullanılıyor, e-posta alışverişi yüksek, ofis programları kullanılıyor, gelir giderler bu ofis programları yardımı ile hesaplanıp tutuluyor, gün sonunda raporlar bilgisayarlar aracılığı ile yazıcılardan çıktı alınarak kağıtlarda muhafaza ediliyor.

Ve senaryomuzu kötüleştirelim. E-postalardan bir tanesi yüzünden bir bilgisayara virüs bulaşıyor ve bu virüs tüm bilgisayarların aynı ağ içinde olması sayesinde kolayca tüm bilgisayarlara yayılıyor. Virüs yüzünden muhasebe programı çalışmamaya başlıyor. Kullanılan bazı ileti programları çalışmamaya başlıyor, ofis uygulamaları ile işlem yapılamaz hale geliyor ve bu nedenle yazıcıdan çıktı alınamıyor. Daha da kötüsü bilgisayarlarda sakladığımız verilerin silinmesi söz konusu oluyor, hatta bilgisayarlar bir daha kullanılamaz hale geliyor. Çok uç bir örnek gibi görünse de böyle bir virüsün bulaşması artık hayatımızın bir parçası haline gelen aynı zamanda da tehlike dolu internet ortamında hiç de zor değil.

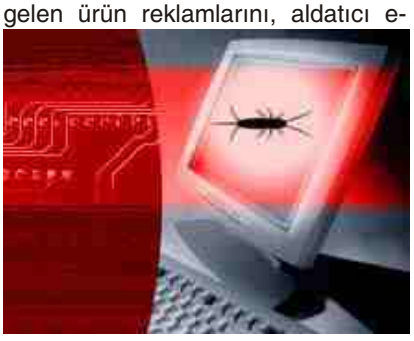
Şimdi ise bu sorunun analizini yapalım ve giderlere bir göz atalım. E-posta ile gelen virüs ilk başta yayılıyor ve ilk bulaştığı bilgisayara hasar vermeye başlıyor, sonra diğer bilgisayara bulaşıp zarar veriyor. Sorun olduğunun kesin anlaşılması ve bakım için uzman birisinin veya firmanın çağırılması en az iki gün alıyor. Kolay bir virüs olsa bile bilgisayarlar en az bir gün kullanılamaz halde bulunuyor, zor bir virüs ise tüm verilerinizin kaybolma olasılığı çok yüksek. Ortalama dört iş günü kaybınız var ve düşünün ki tüm verileriniz, eski hesaplarınız, stok veya mali bilgileriniz kaybolmuş, firmanıza ait geçmişteki her şey silinmiş ya da sadece kağıtlarda kalmış.

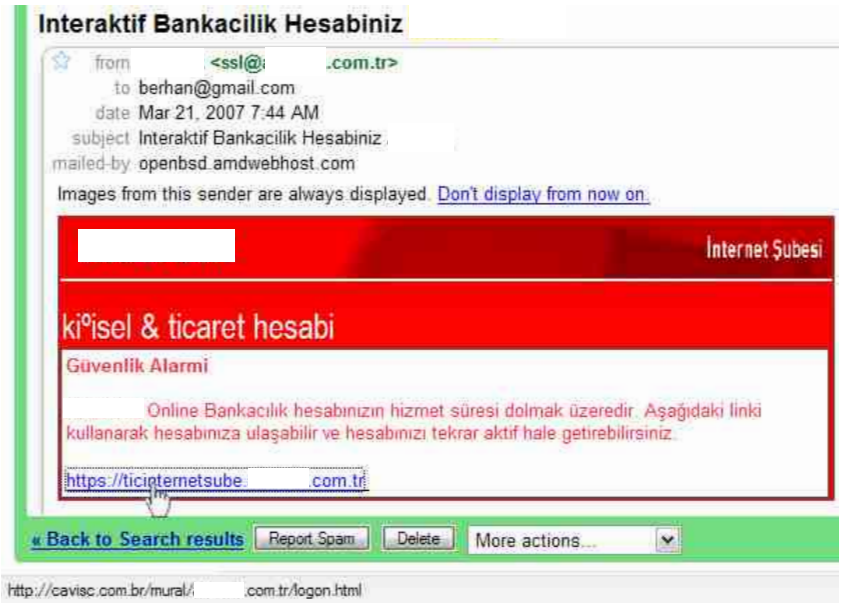
Oysa, bilgisayarlarda anti-virüs yazılımı kullanılsaydı ya da diğer bazı merkezi anti-virüs çözümleri uygulansaydı bu tarz bir sorunla karşılaşmamızın yüzdesi çok daha az olacaktı. Tabii güvenlikte sigorta niteliği taşıyan veri yedekleme çözümü ise atlamamamız gereken diğer bir önlem haline

geliyor tüm şirket verilerimizin kaybolmasına karşın.

Şimdi farklı bir senaryo düşünelim. Örneğin şirketimizin mali planlarını, nakit akışımızı, kullanılan yazılımların lisans bilgilerini, bir takım şifrelerimizi (her ne kadar yanlış da olsa) ve kişisel bilgilerimizi bilgisayarımızda tutuyoruz. Dışarıdan bir kişi herhangi bir korumanız olmadığı için sisteminize kolayca girip sizin için ve başkaları için değerli bilgileri alabilir, buna ek olarak bilgilerinize zarar verebilir. Şifrelerinizin artık bilinmesi ile siz daha fark etmeden sizin yetkilerinizi yani şifrelerinizi kullanarak büyük maddi ve manevi zararlar görmenize yol açabilir. Yine bir olasılık ile şirketinizi veya kişileri paravan olarak kullanabilir. Bu tarz saldırıları, güvenlik ihlallerini fark edip engelleyebilecek, bu tarz izinsiz girişlere açık kanalları kapatabilecek güvenlik duvarları kullanarak veya bu tarz ihlaller için tasarlanmış donanımlar sayesinde böyle bir felaketi önlemiş oluruz.

Tam olarak bir güvenlik sorunu sayılmasa da güvenlik yöntemleri ile çözülebilen ve çok sık karşılaşılan sorunlar arasında yer alan istenmeyen e-postalar; zamanımızdan ve yerimizden çalarak verimimizi büyük ölçüde düşürmektedirler. Buradaki senaryoda ise bu tarz istenmeyen e-posta (spam mail, phishing, vb…)'lar yer almaktadır. Düşünelim ki elektronik postalarımızı alıp verirken kullandığımız yazılımlar (Microsoft Outlook, Mozilla Thunderbird, vb…) veya internet üzerindeki istemci arayüzleri (Hotmail, Mynet, Gmail, Yahoo, vb…) bu tarz istenmeyen e-postalar ile dolup taşıyor. Bu tarz e-postalara örnek olarak; istemediğimiz halde gelen ürün reklamlarını, aldatıcı e-





postaları verebiliriz. Çok fazla sayıda gelen bu e-postaların her birine göz atmak ve onu silmek için geçen zamanımızın 30 saniye olduğunu varsayalım. Tabii işimize geri dönmek için harcadığımız zamanı da 1 dakika varsayalım. Günde ortalama 70 adet bu tarz e-postalardan geldiğini varsayarsak yaklaşık 1 saat 45 dakikamızı aldığını görürüz. Bu ise haftada 10,5 saat eder ki bir günlük mesaisinden fazlasına karşılık gelir. Yani her hafta bir günümüzü boşuna harcamış oluyoruz. Bunun yanında phishing isimindeki kandırmaca içeren e-postaların bize getirdiği maddi zararı da eklersek pek de göze alınmaması gereken bir risk halini almaktadır. Phishing e-postaları genelde bankalardan bizlere gelen e-postalara birebir benzeyen ve içinde bahsettiği işlemi gerçekleştirmek için bağlantılar (link) bulunduran, bu bağlantılar sonunda ise bize bankacılık şifremiz gibi özel bilgileri soran sahte ağ sayfaları(web sitesi) ile özel bilgilerimizi ele geçirmeye çalışan kişilerin yolladıkları e-postalardır.

Yukarıdaki şekilde bana gelen bir phishing e-postası yer almaktadır. Açıklama olarak hizmet süresinin dolacağını ve hesabımı tekrar aktif hale getirmek için aşağıdaki linki kullanmamı söylemektedir. E-posta detaylarında ise göreceğimiz gibi "mailed-by" kısmında ...bank ile ilgisi olmadığını kolayca tahmin edebileceğimiz bir adres bulunmaktadır. **Ayrıca bizden tıklamamızı istediği ...bank ile ilgiliymiş gibi görünen bağlantının üzerine fare imlecimizi getirdiğimizde internet tarayıcımızın (Internet Explorer, Firefox, Opera, vb…) sol alt köşesinde aslında o bağlantının nereye gideceğini görebiliriz. Bağlantı "cavisc.com.br" ile başlayan bir adrese gitmektedir ve tıklamaktan kaçınmalıyız.**

Önlem ise e-posta adresimizi bu şekilde dikkatli kullanmaktan ve istenmeyen posta filtreleyicileri kullanmaktan geçmektedir.

Bu şekilde daha birçok felaket senaryosu üretebiliriz. Bilişim sektörü geliştikçe yeni tehlikeler türemektedir, gün geçtikçe güvenliğin önemi daha da artmaktadır. Unutmayalım ki felaketleri, felaket sonrası yapılan çözümler değil önceden alınan önlemler engeller. En güvenli bilgisayarın kapalı bilgisayar olduğunu düşünürsek -ki onun da güvencesi yoktur örnek olarak çıkan yangınlara veya hırsızlıklara karşı- hiçbir önlem veya çözüm yüzde yüz etkili olamamaktadır. Gerekli önlemleri uzmanların danışmanlığı ve yardımı ile alalım, önemli bilgilerimizin yedeklerimizi aksatmadan tutalım ve bu, zaman ile yapılan yarışta yolumuza daha güvenli devam edelim. Unutmayalım ki önce güvenlik…