Veri Kaybı ve Veri Hırsızlığına Karşı Önlemler

Kurumsal Veri Güvenliği; Günümüzde verinin önemi her geçen gün artmaktadır. Kurumsal verilerinizin güvenliğini sağlamak için birçok önlemler alınması ve bilgi güvenliği ile ilgili farkındalıklar gerektirmektedir.

Ticaret Bakanlığı Houston Ticaret Ataşeliğinden alınan bir yazıda, son dönemlerde başta ABD'de veri hırsızlığının çok yaygınlaştığı ifade edilmektedir. Özellikle alıcı ya da satıcı firmaların elektronik posta kutularına sızma yapılarak, iki taraf arasındaki yazışma geçmişinin de kopyalandığı ve son e-postanın sanki önceki yazışmaların devamıymış gibi gösterildiği, elektronik posta adreslerinde de firma isimlerinin çok küçük farklarla kopyalanarak e-posta adreslerinin oluşturulduğu, bu tarzdaki bir çok yazışmayla ilgili olarak Ataşeliğimize intikal ettirilen durumlar olduğu, bu tür e-postalarda dikkat çeken hususun ödeme aşamasında banka bilgisinde değişiklik olduğu şeklinde bir mesajın iletilmesi olduğu, veri hırsızlığı yapan kişilerin önceki tüm yazışmaları da ekledikleri, çoğu zaman alıcı firmanın e-posta adresini ve adres sahibi kişinin adını dahi kullanarak ödemeyi yapacak olan kişiye ilettikleri e-posta mesajlarında banka bilgisi değişikliği ya da hesap bilgisi değişikliği olduğunu belirterek ödemenin yapılması için doğrudan kendi hesap numaralarını verdikleri ifade edilmiştir.

Yine anılan yazıda ABD bankacılık sisteminde de doğrudan bir hesaba yapılan ödemenin durdurulmasının çok zor ya da mümkün olamadığı, hukuki süreçlerin de uzun ve çok maliyetli olduğu, böyle bir durumun fark edilmesini müteakip ivedi bir şekilde ödeme yapılan banka tarafından alıcı bankaya swift mesajının iletilmesi ve aynı zamanda adli makamlara konunun intikal ettirilerek muhatap ülke makamlarına başvurulması gerektiği ifade edilmiştir. Öte yandan konunun sadece ülkemizde adli makamların girişimine bırakılmayarak muhatap ülkede de bir avukat vasıtasıyla adli sürecin başlatılmasının önemli olduğu belirtilmiştir.

Bu itibarla ihracatçılarımızın Bilgi Güvenliği farkındalıklarını artırması ve Bilgi Sistemleri zafiyetlerinin giderilmesi noktasında önleyici ve engelleyici aksiyonlar almaları Meclisimizce tavsiye edilmektedir.

Bilgi Teknolojileri ekiplerinin alması tavsiye edilen bilgi güvenliği önlemleri;

- Firewall ile dışarıdan içeriye ve içeriden dışarıya erişimlerin kısıtlanarak kontrol edilmesi
- Antivirüs ve benzeri kurumsal güvenlik çözümlerinin kullanılması
- USB Bellek/HDD erişimlerinin kullanıma kapatılması
- Bulut dosya depolama alanlarının (Dropbox, Google Drive vb.) kullanıma kapatılması
- Network katmanı ve topolojisine yönelik güvenlik önlemlerinin alınması (Vlan Segmentasyonu vb.)
- Güçlü şifre politikasının uygulanması (Belirli aralıklarla güncelleme zorunluluğu olan Min 8 karakter ve kompleks (En az bir büyük bir küçük harf ve rakam içeren şifre, belli deneme sayısı sonrası hesabı kitleme fonksiyonu vb.)
- DLP veri sızıntısı önleme ve Veri Sınıflandırma (Gizli, Hizmete Özel, Genel gibi) uygulamaları

Bireysel olarak alınması gereken önlemler ve farkındalıklar.

- En populer veri hırsızlığı yöntemlerinden biri olan **Oltalama** (Phishing) yöntemlerine karşı dikkatli ve farkında olmak önemlidir. Bunun için en bilinen korunma yöntemleri E-Posta ile gelen dosya veya linklerin emin olunmayan durumlarda açılmaması ve gönderici isminin doğru/sahte olup olmadığının kontrol edilmesidir. (Mümkünse bir mail gateway, sandbox yazılımı kullanarak bu tip e-postaların karantinaya alınması varsa içerisinde yer alan dosyaların korunmalı bir ortamda denetlenerek son kullanıcıya iletilmesi yapılmalıdır.)
- USB Drop saldırılarına karşı dikkatli olmalı, yerde gördüğünüz veya ortak alanlarda bulduğunuz USB bellek/HDD cihazlarını kontrol etmek için bilgisayarınıza takmayınız.
- Para transferi gibi önemli işlemleri yapmadan önce, E-Posta ile gelen bilgileri teyit etmek için, farklı bir iletişim kanalı üzerinden (Mobil,SMS,Whatsapp vb.) ilgili kişi/kurumlar ile görüşerek bilgileri teyit etmeliyiz.
- Şifre vb. önemli bilgileri E-Posta üzerinden veya tek bir iletişim kanalı üzerinden paylaşmayınız. Mümkünse şifre bilgisini 2 veya daha fazla iletişim kanalına bölerek karşı tarafa iletiniz.

- Önemli Sistem veya Web uygulamalarına giriş yaparken, 2FA veya MFA olarak bilinen iki veya daha fazla doğrulama gerektiren yöntemleri kullanmaya ve bu yöntemlerin mevcut sitelerde kullanım durumunu kontrol etmeye özen göstermeliyiz.
- Girmiş olduğunuz sitelerde aşağıdaki şekilde bağlandığınız site ile aranızda kaçak bir katman olmadığını (güvenli bağlantı, SSL doğrulaması) ikonu ile gözden geçirmeliyiz.
- Özellikle şifre giriş bilgilerini, link ve dosya içeren gelen e-postalarınızın adreslerinde yer alan @ işaretinden sonra yazan alan adını kontrol ediniz. Kontrol sonrası sadece güvenilir kaynaklardan gelen e-postaları açınız.
- Gelen e-postalarda benzer karakterler (“O” harfi yerine “0” (sıfır) kullanımı gibi) kullanılarak yapılan şaşırtmacalara dikkat ediniz.
- Özellikle sosyal medyada yapılan ofis içi durum paylaşımları içeren fotoğraflarda gizli verilerin, şifrelerin yer almamasına dikkat ediniz.
- Halka açık alanlarda bilgisayarınıza ya da hesaplarınıza giriş yaparken etraftan görüntülenmediğine emin olunuz. Mümkünse çok gizli şifre ve verilerinizi halka açık alanlarda girmeyiniz.