Deloitte.

SİBER GÜVENLİ ŞİRKET OLMAK

Ali Kamil UZUN

İş dünyamızın kurumsal varlıkları olan şirketlerimizin akıllı teknoloji ile donatılmış çalışma ortamı sayesinde şirket yönetici ve çalışanlarının bilgiye erişimi ve iletişim konforu her geçen gün hızla gelişmektedir. Bu gelişimin hızı gün geçtikçe artmakta; ölçeğimiz ve sektörümüz ne olursa olsun bizi etkilemektedir.

Bulut bilişimin olanakları ile verilerin dijital ortamda depolanabilmesi, uzaktan erişim, hızlı ve kolay transfer ile dünyamız üzerinde güneşin batmadığı bilgi toplumuna dönüşmüştür. Dijital devrim 7/24 yaşayan bir iş dünyası yaratmıştır.

Teknolojinin nimeti olan bilgi toplumunda mobil iletişim araçlarının akıllı teknolojilerle sağladığı akıl almaz iletişim imkanları sayesinde zaman ve mekan sınırlamaları olmaksızın iş ve sosyal yaşamımızı sürdürüyoruz..

Sosyal yaşamı hareketlendiren, iletişimin dilini değiştiren gelişmeler, iş yaşamında da değişim ve dönüşüm yarattı. İş yapış biçimi ile birlikte iş süreçleri değişti. Çalışma ortamının şirket duvarları ile sınırlı mekan anlayışı, yerini her yerden erişimin olduğu mobil çalışma ortamına bıraktı.

Söz konusu değişim ve dönüşüm, iş dünyası ve şirketler için yeni iş fırsatları, yeni ürün ve hizmet tasarımı, hızlı büyüme ve rekabet avantajı imkanları sağlarken tehdit oluşturabilecek önemli riskleri de beraberinde getirmektedir.

Değişimi Güvenli Yaşıyor muyuz?

Stratejik kararlarımız için kullandığımız rapor bilgilerimiz; müşteri, fiyat, maliyet bilgilerimiz; satış bilgilerimiz, ticari sırlarımız…vb şirketimize özel bilgi ve raporlarımız bir zamanlar kilit altında kasa ve evrak dolaplarında saklanarak fiziksel güvenliği sağlanırdı. Günümüzde bu bilgiler fiziksel ortam yerine elektronik ortamda saklanmakta, şirketlerin iletişim ağında bulunan kullanıcılara tanınan erişim yetkileri çerçevesinde güvenliği sağlanmaya çalışılmaktadır. Şirketimizin iletişim ağındaki güvenlik uygulamalarının güçlü olması tehdit altında olmadığımızı göstermez. Siz bu satırları okurken birileri iletişim ağınızdaki zayıflıkları araştırıyor, şirket verilerine sızmak için çalışıyor olabilir.

Teknolojinin hızla gelişim, sunduğu iletişim fırsatları ile büyüme ve rekabet avantajları sağlanırken, bu gelişim aynı zamanda şirket verilerine kötü niyetli erişim için riskler de taşımaktadır. Güvenlik zincirimizi kırmaya, iletişim ağımıza sızarak bilgilerimize erişmeye imkan sağlayan virüs ya da casus yazılımlar, şifre dolandırıcılığı, internet sitelerinin çökertilmesi gibi sonuçları yıkıcı, maddi zarar ve itibar kaybı doğuran tehdit konuları, nimetlerinden yararlandığımız teknolojinin külfetini oluşturan riskleri olarak karşımıza çıkmaktadır.

Siber güvenlik uzmanları, kötü niyetli kişilerin cep telefonumuzdaki ve tablet bilgisayarımızdaki e-postalarımızı görüntüleyebilecekleri, şifrelerimize ve şirketimizin değerli bilgilerine erişebilecekleri, telefon kameramızın uzaktan yönetilmesini sağlayabilecekleri yazılımlara dikkat çekmektedirler. Siber güvenlik zincirindeki en zayıf halkanın ise şirket çalışanları olduğunu tecrübelerimiz göstermektedir.

Şirketlerimizin stratejik yönetim kararlarının alındığı yönetim kurulu seviyesinde de kritik bilgilerin bulunduğu dosya ve raporların güvenliğinin tam olarak sağlandığından emin miyiz?

Şirket yönetim kurulu üyeleri konumları gereği şirketin en hassas bilgilerine sahip olmalarının yanı sıra işleri gereği şirket dışı mekan hareketlilikleri, akıllı mobil iletişim araçlarını kullanma sıklıkları nedeniyle güvenlik zincirinin riski yüksek halkasını oluşturmaktadır.

Söz konusu riskin yönetilmesi, siber güvenliğin sağlanarak şirket bilgilerinin korunması için gerekli görülen kritik önlemler aşağıda açıklanmaktadır.

1. Şirketlerin siber güvenliği için öncelikle yönetim kurulu seviyesinde bilgi güvenliğini sağlamak üzere riskleri ve kilit kontrolleri anlamak için çalışmalar yapılması gerekmektedir.

2. Siber güvenlik için kurumsal yönetim politikaları oluşturulmalıdır.

3. Şirket için hassas bilgilerin bulunduğu dosya ve raporlar envanterinin oluşturulması, kimlerin erişimine açık olduğunun değerlendirilmesi, kontrol ve güvenlik prosedürlerinin gözden geçirilmesi sağlanmalıdır.

4. Hassas bilgilerin yer aldığı dosya ve raporlara erişimin kontrol ve yönetimine ilişkin politika ve prosedürler geliştirilmelidir.

5. Konuya ilişkin uzmanlar yardımıyla sızma testleri ve güvenlik denetimleri yaptırılmalıdır.

Yukarıda önerilen hususların yanı sıra şirket yönetici ve çalışanlarının bilgi güvenliği konusunda sürekli bilgilendirilmesi ve eğitimi sağlanmalıdır.

Uzun lafın kısası;

Teknolojinin başını çektiği, baş döndürücü bir değişim çağındayız. Bu değişimi takip etmemiz, kurumlarımıza ve günlük yaşantımıza taşımamız gerekiyor. Kurumlarımızda yaşanan bu gelişimin sağladığı konforu yaşamamız, çağın olmazsa olmaz bir gerekliliğidir. Bu konforu yaşarken, değişim getirdiği belirsizlikleri önceden en aza indirmemiz gerekiyor. Bunu sağlamanın ilk koşulu ise, şirket yönetim kurullarının bilgi güvenliklerini tehdit eden siber risklere odaklanarak şirket yönetici ve çalışanlarını bu konuda yönlendirmeleridir.

Ali Kamil UZUN, CPA, CFE, MA, CRMA, CAC

Deloitte Türkiye Yönetim Kurulu Danışmanı

(akuzun@deloitte.com)

Makale, Turcomoney Dergisi Nisan 2014 sayısında yayınlanmıştır.