thinktech
STM Teknolojik Düşünce Merkezi

Siber Güvenlikte İnsan Faktörü

Şirketler, gün geçtikçe, siber saldırı tehdidini daha yakından hissediyor. Teknik önlemlere ciddi yatırımlar yapıyorlar ve yüksek nitelikli, yüksek maaşlı uzmanları işe alıyorlar. Zaman zaman da kendilerini korumaları için dışarıdan uzmanlarla çalışıyorlar. Teknoloji ve yüksek maaşlı uzmanların siber güvenlik için önemli olduğu su götürmez bir gerçek ama tüm bu yatırımlar başka bir kaynak tarafından, şirketin kendi çalışanları tarafından kolaylıkla boşa çıkarılabilir. PwC'nin 2013'te hazırladığı bir ankete göre, güvenlik ihlallerinin yüzde 36'sı dikkatsizlikten kaynaklanan insan hatalarının eseri (yüzde 10'u kasti sistem kurcalamaları) ve çalışanların gazabına uğrayan küçük işletmelerin oranı yüzde 57.

Çalışanların Verebileceği Zararlar

Bu çalışanlar kimler? Bazı çalışanlar yanlış bir şey yapma niyetinde değildir. Onların yaptığı hatalar aslında şirketin suçudur. Ya yetersiz personel işe alınmıştır ya yeterince eğitilmemiştir ya da güvenlik kültürü gelişmemiştir. Bazı çalışanlar çok sadık, kendini adamış ve çalışkan olmalarına rağmen, siber risk tehdidini değerlendiremezler ve dışarıya iş çıkarırlar. Burada hata yine şirketindir. Bazı çalışanlar ise ellerindeki muazzam siber kaynakları kullanarak onarılamayacak yaralar açabilirler. Elbette bu kötü niyetli insanları suçlamak gerekir ama şirketin önlem almadaki yetersizliğini de unutmadan. Peki bu dikkatsizlik ve hatalar nelere mal oluyor? Şirketlerin bu tip önlemleri almakta yetersiz kalması başta bilgi hırsızlığı, maddi kayıplar ve prestij kaybı olmak üzere, verimlilikte azalma, zaman yönetiminde sıkıntı ve müşteri kayıpları yaşanması gibi büyük problemlere yol açabiliyor.

Neler Yapılabilir?

Yönetişim: İnsani risklerin sorumluluğunun şirket yönetiminde dağıtılmaması gerekir. Bu risklerden sorumlu bir yönetici olmalıdır.

Roller, sorumluluklar ve kaynaklar: Riskten sorumlu yöneticiyi belirledikten sonra, tüm rollerin ve sorumluların alacağı önlemler, prosedürler ve kullanacağı kaynaklar açıkça belirtilmelidir.

Kazanımlar: Yönetim şirketin kritik kazanımlarını ve zayıflıklarını anlamalıdır.

Risk: Şirket en az yılda bir kez güvenlik riski yaratabilecek çalışanlarını bulmak için resmi bir değerlendirme yapmalıdır. Yüksek seviye risk taşıyan ve bu kültüre uygun çalışanlar belirlenip gerekli önlemler alınmalıdır.

Kültür: Yönetim şirket için bir güvenlik kültürü benimsemeli, planlama yapmalıdır.

Etki: Yönetim, içerideki bir çalışandan kaynaklanan olayın operasyonel, finansal, itibari ve yasal etkisini anlamalıdır.

Yanıt: Şirket bir olay karşısında asgari zarara uğrayacak şekilde tedbirlerini almış olmalıdır. Yönetim seviyesinde bir programla hazırlık yapılmalıdır.

Şeffaflık ve farkındalık: Tüm önlemler ve prosedürler, orantılı, yasal düzenlemelerle uyumlu ve çalışanların her zaman ulaşabileceği kadar şeffaf olmalıdır. Çalışanlar yaptıkları her şeyin potansiyel sonuçlarının farkında olmalıdır.

Tedarik zinciri: Riskten sorumlu yöneticinin, tüm kazanımların arasında tedarik zincirinin de olduğunu bilmesi gerekir. Çalışanlara uygulanan prosedürlerin ve politikaların aynı şekilde tedarik zincirine de uygulanması gerekir.

Denetim: Denetim komitesi yıllık değerlendirmelerle riskleri ve bu risklere karşı hangi önlemlerin alındığını denetlemelidir.

İyi performans gösteren şirketlerin etkin ve şeffaf risk azaltma programları vardır. Örneğin 9 Ekim 2017 tarihinde İstanbul'da düzenlenen Savunma Zirvesi toplantısında bir panelde konuşan Kale Grubu Başkan Yardımcısı Osman Okyay, her tür bilgi hırsızlığını ve siber saldırıları önlemek için şirketin Ar-Ge sürecinde kullanılan bilgisayarların internet bağlantılarının ve USB girişlerinin kaldırıldığını söyledi. Uygun politikalarla şirket çapında güvenlik kültürünün yayıldığı yönetimlerde içerideki siber güvenlik zaafiyetini azaltmak mümkündür. Bunların yarattığı tahribatı sıfıra indirmek mümkün değildir ama yine de en aza indirmenin yolları bulunabilir.