IIA Bülteni

İç denetçiler için günümüzün acil çözüm gerektiren sorunlarına bakış açısı Şubat 2020

HAZIRLIKLI OLMAYI YENİDEN DÜŞÜNMEK: SALGINLAR (PANDEMİLER) VE SİBER GÜVENLİK

Koronavirüs salgını, kurumların genelde gözden kaçırdığı meseleler arasında sayılan iş sürekliliği ve afete hazırlık konularının giderek daha fazla sayıda kurumun **ana gündem maddeleri hâline gelmesine neden oluyor**.

Süregelmekte olan salgının kapsamı ve süresinin belirsiz olması iş dünyası üzerinde hâlihazırda bir etki bırakmışa benziyor; örneğin kurumlar daha şimdiden personel seyahat planlarını yeniden değerlendirmeye başladılar, korku içindeki yatırımcılar ise hisselerini elden çıkarmanın peşindeler. Salgının genişlemesinin yarattığı risk, örneğin tedarik zincirlerinin, çalışan verimliliğinin ve üçüncü taraf ilişkilerinin salgından etkilenme ihtimali, hem şirket yönetici kadroları hem de iç denetim liderleri tarafından dikkate alınmak zorunda. İç denetim liderleri en azından salgın, afete hazırlık ve iş sürekliliği planlarını gözden geçirmeye ve gerekli güncellemeler konusunda tavsiyelerde bulunmaya hazırlıklı olmalılar.

Kurumlar koronavirüsün faaliyetleri üzerindeki olası etkilerini belirlemenin henüz ilk aşamalarında olmalarına rağmen, koronavirüsün tali risklerinden biri kendini göstermeye başladı bile: kriz ortasında sosyal mühendislik. Siber suçlular, bu ölümcül virüse dair giderek büyüyen kaygı ve endişelerden istifade ediyorlar. Birleşik Krallık merkezli bir tüketici teknoloji haber ve inceleme web sitesi olan TechRadar Pro'ya göre, Japonya'nın üç ayrı şehrinde, virüs hakkında yol gösterici bilgi verme süsüyle hazırlanmış kötü amaçlı yazılım içeren e-postalar rapor edilmiş. Hacker'lar, bu kötü amaçlı yazılımı virüsün yayılmasına karşı korunmak için ne yapılması gerektiği hakkında bilgi içerdiği iddiasını taşıyan e-posta eklerine gizlemişler. TechRadar Pro'nun bildirdiğine göre, koronavirüse karşı korunmanın yollarını öğrenme hevesiyle bu e-posta eklerini açan kişiler ise, onun yerine başka tür bir virüsle iştigal etmek zorunda kalmışlar.

Krizlerin yarattığı fırsatlardan yararlanma eğilimi gösteren siber suçlular giderek yaygın hâle gelecek gibi görünüyor. Kurumlar, oltalama, sahte senaryo üretme ve yemleme gibi sosyal mühendislik yöntemlerine karşı kendi savunma protokolleri ve uygulamalarını tesis etmek zorundalar.

Kurumunuzun afetlere hazırlık durumunu değerlendirmek için cevaplamanız gereken genel sorular

Aşağıda sıralanan sorular, kurumunuzun afetlere hazırlık ve iş güvenliği planlama konularıyla olması gerektiği gibi ilgilenip ilgilenmediğini belirlemek için iç denetim biriminiz tarafından sorulması gereken **genel sorulardan bazılarıdır**:

- Kilt paydaşlarınız kurumunuzun dayanıklılık planlarını en son ne zaman gözden geçirdiler? Kurumunuzun planları en son ne zaman ve kimler tarafından test edildi?
- Tesisinize ve/veya çalışanlarınıza ve/veya bulut sağlayıcılarınıza ve/veya tedarikçilerinize ve/veya müşterilerinize etki edebilecek doğal afetler, salgınlar veya başka olası yıkıcı olaylar mevcut planlarınızda ne şekilde ele alınıyor?
- Kurumunuz iş dayanıklılık ortakları ile olan sözleşmelerini en son ne zaman gözden geçirdi?
- İrtibat kişisi değişiklikleri, satıcılara, acil durum müdahale ekiplerine, düzenleyici kurumlara, sigorta acentelerine ve diğer kritik paydaşlara nasıl bildiriliyor?
- Kurumunuz işle ilgili kritik otomatik faaliyetleri manuel şekilde gerçekleştirme konusunda ne denli yetkin? Gereken formlar ve prosedür kılavuzları mevcut mu? İlgili faaliyetleri yürütecek uygun kadrolar var mı?
- Kurumunuz kurtarma için tayin edilen öncelik sırasının uygun olduğundan emin olmak için çeşitli farklı iş süreçlerinin kritiklik derecelerini ne sıklıkta teyit ediyor? BT, kritik altyapı bileşenlerinin iş kurtarma gereksinim ve ihtiyaçlarının karşılanmasına olanak sağlayacak hâle getirilmesini nasıl sağlıyor?
- İnternet erişimi veya hücresel erişim tamamen veya kısmen kesilseydi, bu sebeple hangi iş hedefleri tamamen veya kısmen ulaşılmaz hâle gelirdi?
- Bir doğal afet veya salgın durumunda yapılması gerekenlere istinaden çalışanlarınız ve iş ortaklarınız hangi eğitimleri aldı?
- Veri merkeziniz ve/veya bulut sağlayıcınız uzun bir dönem boyunca "ışıklar kapalı", yani hiç personel olmadan çalışabilir mi?
- Kritik iş süreçleri veya faaliyetlerinizden hangileri alternatif yerlere aktarılamaz nitelikte? Bunlardan hangilerinin, olayın zamanlaması veya süresi nedeniyle mevzuata uygunluk yönünden etkileri vardır?

Sosyal mühendislik zafiyetlerinizi değerlendirmek için cevaplamanız gereken genel sorular

Aşağıda sıralanan sorular, kurumunuzun sosyal mühendislik şemalarına/entrikalarına zafiyetini belirlemek için iç denetim biriminiz tarafından sorulması gereken **genel sorulardan bazılarıdır**:

- Sosyal mühendislik tehlikesi, kurumunuzda tatbik edilen uygulamalar, politikalar ve eğitimlerden hangilerinin kapsamına giriyor? Bunlar çalışanlara nasıl iletiliyor ve bunlar nasıl uygulanıyor?
- Sosyal mühendislik tehlikesi kurumunuz bünyesindeki bütün personel seviyelerinde tam ve eksiksiz bir şekilde anlaşılıyor mu ve tüm personele iletiliyor mu?
- Sosyal mühendisliğe karşı özellikle zafiyet taşıyan sistem ve süreçleriniz hangileri? Etkilenme potansiyeli barındıran kilit iş süreçleriniz hangileri?
- BT biriminiz, sosyal mühendislik yöntemlerine özellikle zafiyeti bulunan alanlarla ilgili hangi testleri yapıyor?
- Kurumunuz bünyesinde sosyal mühendislik yöntemlerine özellikle zafiyeti bulunan alanları denetleme planlarınız var mı?

IIA KAYNAKLARI

Kısa Bilgilendirme Yazısı

- Stratejik Kamu Varlıklarının Korunması

Çalışma Rehberleri

- Risk Yönetim Sürecinin Değerlendirilmesi
- Üçüncü Taraf Risk Yönetiminin Denetlenmesi
- Eşgüdüm (Koordinasyon) ve İtimat: Bir Güvence Haritasının Geliştirilmesi
- İş Sürekliliği Yönetimi
- GTAG: İş Sürekliliği Yönetimi
- GTAG: Siber Güvenlik Risklerinin Değerlendirilmesi

Internal Auditor dergisi

- In the Face of Nature