

SİBER DOLANDIRICILIK BÜYÜK SERMAYELİ BİR TİCARET

Siber dolandırıcılığın hackerler için oldukça karlı bir iş olduğu apaçık ortada. Buna karşılık siber dolandırıcılık saldırıları kurumlar için mali bir yıkım olmaya devam ediyor.



Yapılan son çalışma bu tehdit unsurunun ne kadar sarsıcı olduğunu ortaya koydu: Ortalama 10.000 çalışanı olan bir şirket siber dolandırıcılık saldırıları sonrasında ortaya çıkan tabloyu düzeltmek için yılda 3,7 milyon dolar harcar. Sıradan bir çalışan siber dolandırıcılık ile ilgili olaylar için yılda 4,16 saat harcar.

Aşağıdaki durumları içeren siber dolandırıcılık saldırılarının doğrudan bir sonucu olarak kurumların üstlendiği en yüksek maliyetler: Gizliliği ifşa edilmiş kimlik bilgileri ve kötü amaçlı yazılım nedeniyle ortaya çıkan veri ihlalleri ve bunun yanı sıra bütün ağa zarar vermeden önce kötü amaçlı yazılım içerme maliyeti.

Çalışanlarınız bu tehlikeye karşı yeterince hazırlıklı mı yoksa siber dolandırıcılık olaylarına davetiye çıkaracak kadar savunmasızlar mı?

“ Sıradan bir çalışan siber dolandırıcılık ile ilgili olaylar için yılda 4,16 saat harcar. ”

SİBER DOLANDIRICILIK SORUNUNUZ FARKINDALIK YARATARAK NEDEN ÇÖZÜME KAVUŞTURULAMIYOR?

Güvenlik uzmanları olarak, kişisel fikir ve görüşlerden ziyade kanıtlanmış uygulamaları daha çok önemsiyor ve dikkate alıyoruz.

Bu nedenle bir sorunun yalnızca farkında olmak sorunun kendisiyle baş edecek güç ve donanıma sahip olmak ile eş değerdir.

Kısacası farkındalık işe yaramıyor.

Kurumsal bir güvenlik perspektifinde hazır bulunuşluk her türlü risk senaryosunda farkındalığa galip gelir. Örneğin tehlikeli görünmeyen bir e-posta saldırısını açan bir çalışan siber dolandırıcılık saldırılarının mevcut olduğundan haberdar oldukları için çok donanımlı bir hackerin güçlüğüle

anlaşılan bulgularını kolayca fark edemeyebilirler.

Birçok farkındalık programı çalışanları siber dolandırıcılık konusunda bilgilendirmeye odaklıdır ve buna göre test edilir. Biz CybeReady olarak bunun sadece mücadelenin yarısı olduğuna inanıyoruz.

Siber dolandırıcılık konusunda endişeleriniz varsa, çalışanlarınızın siber dolandırıcılık saldırılarına maruz kalma ihtimalini azaltacak adımlar atmak önemlidir.

HİZMET İÇİ EĞİTİM MASRAFLARINI VE KARMAŞIKLIĞINI HAFİFE ALMAYIN

Birçok kurum eğitimle ilgili içeriği veya teknolojileri satın almak istediğinde yalnızca ön ödeme maliyetlerini inceler. Çoğunlukla harcanan paraya odaklanmak yatırımlarının önemli bir kısmını kaçırdıkları anlamına gelir. Gerçek fatura bir program uygulandığında hazırlanır.

Güvenlik eğitim programlarının maliyetlerini karşılaştırırken üç başlık altında toplamak önemlidir: Eğitim hazırlığı maliyeti, çalışanların eğitimi sırasında kaybedilen zaman ve katılım maliyeti.

BUNLARI ALT KATEGORİLERE AYIRALIM:

KATILIM MALİYETLERİ:

Bunlar herhangi bir eğitim programının makul fiyatlarıdır. Çalışanlarınızın güvenliğe bakış açısı olumlu mu? Programınızın zaman kaybı olduğunu düşündüler mi? İyi bir eğitim programı çalışanları etkileyerek içine alırken kötü hazırlanmış bir eğitim programı ise çalışanları kendinden uzaklaştırır.

ÇALIŞANLARIN EĞİTİMİ SIRASINDA KAYBEDİLEN ZAMAN:

Bu dolaylı maliyetler hem eğitim hem de bununla bağlantılı seyahat masrafları için harcanan zamanı kapsar. (Seyahat masrafları ile, bir konferans salonundaki tüm çalışanlarınız veya uzaktan giriş ile ilgili teknik sorunları gidermek zorunda olmayı kapsasın veya kapsamasın herkesin eğitime katılma süresini kastediyoruz).

EĞİTİM HAZIRLIĞI MALİYETİ:

Bu doğrudan maliyetler arasında, danışmanlar gibi dış taraflara ödenen paralar, yazılım lisansları ve programın çalıştırılması, öğrenme yazılımının performansının izlenmesi ve her şeyin düzgün şekilde çalışıp çalışmadığının kontrol edilmesi gibi zamana bağlı maliyetler bulunur.

Sağlık, sigorta ve bankacılık gibi çeşitli endüstrileri temsil eden dünyanın önde gelen kuruluşlarından bazıları CybeReady'e ve şirket genelindeki siber dolandırıcılığa karşı hazırlık eğitimine güveniyorlar.

CybeReady tamamen bölgenize, sektörünüze ve markanıza uygun benzersiz bir hizmet düzeyine sahip Siber Dolandırıcılığa Hazırlık programları sunar.



HAZIRLIKLILIK ANALİTİK RAPORU

Zayıf noktalarınızı keşfedeceksiniz. Çalışanlarınızı siber dolandırıcılık yapmaya teşvik eden etmenleri, hangi departmanların savunmasız olduğunu ve diğer risk faktörlerini görme imkanı sağlamak oldukça önemlidir. CybeReady zamanla meydana gelen iyileştirmeleri gösteren ayrıntılı verilerle kararlarınızı desteklemenizi sağlar.



EKSİKSİZ HİZMET

Hizmet döngüsünü kapatıyoruz. Şirketin ustalıkla tasarlanmış ve düzenlenmiş hazırlık programı her yolu denedi. Sürekli olarak siber dolandırıcılık girişimlerinde bulunan, çalışanları bu girişimlere karşı kendilerini nasıl koruyacakları konusunda eğiten ve çalışanlarınız için tuzak olarak tanımlanabilecek beklenmeyen olaylara ilişkin yanıtlar sağlayabilecek yıllık bir çözümle kurumsal hazırlığınızı takip edebilirsiniz.



SAHTE SALDIRI SIKLIĞI

Eğitimimiz gerçeği taklit eder. Tek bir simülasyon yerine CybeReady hem harici (tatiller, konferanslar) hem de dahili etkinlikler (yazılım güncellemeleri, emeklilik planlamaları) için bir dizi saldırı başlatır. Artık çalışanlarınızı herhangi bir hacker'in çeşitli siber dolandırıcılık girişimlerine karşı hazırlayabilirsiniz.



KURULUM GEREKTİRMEZ

Zahmetli işleri bize bırakabilirsiniz. CybeReady'nin bulut tabanlı hizmeti yüklenecek yazılım, satın alınacak donanım ve bakım yapılacak herhangi bir ekipman olmadığı anlamına geliyor. Müşterilerimiz 48 saat sorunsuz bir şekilde ve gizli tuzaklarla karşılaşmadan bir uzman liderliğindeki sürecin içerisinde yer alabilir.



TAMAMEN İSTEĞE GÖRE UYARLANMIŞ İÇERİK

Şablonların robotlar için olduğunu düşünüyoruz. Çalışanların yalnızca en titiz davranış eğitimleri ile hazır olduğundan emin olabilirsiniz. CybeReady, sektöre özgü ustaca oluşturulmuş, birim ve mevkilere yönelik mesajlara kadar değişen zorluk seviyelerinde gerçeğe yakın çeşitli siber dolandırıcılık saldırıları konusunda uzmandır. İçeriğin tamamı müşteriye ve simülasyona özgüdür ve dilsel ve kültürel olarak ihtiyaçlarınıza göre uyarlanmıştır.

NEDEN CYBEREADY?

Geleneksel bilgi güvenliğinin, en kritik varlık (insanlar) tarafından ortaya çıkarılan risklere nadiren hitap eden başarısız bir kuruluş olduğunu düşünüyoruz.

CybeReady, kurucularının yeni bir paradigmanın geliştirilmesine öncülük eden Bilgi Güvenliği'nin "İnsan Genomu"nu araştırdığı yıllardaki işbirliğinin sonucudur: Çalışanların Siber Hazırlığı.

Ekip insan merkezli riskleri yönetmek için gerekli süreç ve çözümlere derinlemesine bir anlayış ve bakış açısı getiriyor ve bu durum da oldukça etkili hazırlık programının gelişmesine öncülük ediyor. Geleneksel farkındalık programlarının aksine CybeReady çalışanların sebep olduğu bilgi güvenliği riskleri konusunda uzmandır.

CybeReady hazırlık çözümünü Shakespeare'in en unutulmaz sözlerinden biri ile özetleyerek hazırladı:

"BÜTÜN MESELE HAZIR OLMAKTA."

