SOSYAL MÜHENDİSLİK: İHRACATÇILAR İÇİN TEHDİTLER VE SİGORTA İLE RİSK TRANSFERİ

Teknoloji, dijital güvenliğin sağlanmasında önemli bir rol oynasa da insan faktörü kritik bir unsur olmaya devam etmektedir. Farklı birçok araştırma raporunda, veri ihlallerinin %70 ila %90'ının sosyal mühendislik saldırıları veya hata içeren insan kaynaklı unsurlardan kaynaklandığı belirtilmektedir. Şirketler, çalışan eğitimi, çok faktörlü kimlik doğrulama (MFA), e-posta filtreleme araçları ve net güvenlik politikaları gibi araçlar ile kendilerini korumayı hedeflemeli, öngörülemeyen riskleri ise risk yönetimimin tamamlayıcısı olarak sigortaya transfer etmeyi değerlendirmelidir.

Sosyal Mühendislik Nedir?

Sosyal mühendislik, bireylerin veya kurumların hassas bilgilerini ele geçirmek, sistemlerine yetkisiz erişim sağlamak veya maddi zarar vermek amacıyla insan psikolojisini manipüle eden bir siber saldırı yöntemidir. Teknolojik altyapılar ne kadar güçlü olursa olsun, şirket çalışanlarının veya yöneticilerinin ikna edilmesiyle gerçekleşen dolandırıcılıklar, küresel olarak ve ülkemizde büyük mali kayıplara neden olabilmektedir.

Sosyal mühendislik süreçleri genellikle e-posta, telefon görüşmeleri, sahte web siteleri ve hatta yüz yüze görüşmeler yoluyla gerçekleştirilebilmektedir.

İhracatçıların Karşı Karşıya Kalabileceği Sosyal Mühendislik Tehditleri

Uluslararası ticaret yapan ihracatçı firmalar, sosyal mühendislik saldırılarına karşı hassas durumdadır. Karşılaşılan tehditlerden bazıları şunlardır:

- **Sahte Banka Hesap Değişikliği Bildirimi:**
  Tedarikçi veya iş ortağı gibi görünen dolandırıcılar, banka hesap bilgilerini değiştirdiğini bildirerek para transferlerinin yanlış hesaplara gitmesini sağlayabilir.

- **Sahte Tedarikçi veya Müşteri Dolandırıcılığı:**
  Dolandırıcılar, gerçek bir tedarikçi veya müşteri gibi davranarak, para transferlerini kendi hesaplarına yönlendirebilir.

- **Yöneticileri Taklit Eden E-Posta Dolandırıcılığı (CEO Fraud):**
  Saldırganlar, bir firmanın yöneticisi veya yetkilisi gibi davranarak finans ekiplerine sahte talimatlar vererek ödeme yaptırabilir.

- **Gümrük veya Lojistik Dolandırıcılıkları:**
  Sahte lojistik firmaları veya gümrük yetkilileri, ihracatçılardan çeşitli vergi veya gümrük ücretleri adı altında para talep edebilir.

- **Kargo Yönlendirme Dolandırıcılığı:**
  Saldırganlar, sevkiyat işlemlerine müdahale ederek malların başka bir yere teslim edilmesini sağlayabilir.

Elektronik Suç Sigortaları ile Sosyal Mühendislik Riskini Transfer Etmek

Sosyal mühendislik saldırılarının önlenmesi için teknik ve insan odaklı önlemler almak oldukça önemlidir. Ancak, her önleme rağmen bu tür bilgisayar dolandırıcılıkları gerçekleşebilmektedir. Bu nedenle, firmalar sigorta poliçeleri aracılığıyla bu riski belirli ölçülerde transfer edebilirler.

Elektronik Suç sigortaları bilgisayar dolandırıcılıklarına karşı teminat sunabilmektedir. Elektronik suç sigortaları sigortalanan firmanın bilgisayar sistemlerine yetkisiz giriş yapılması yolu ile para/fon transferine yol açabileceği gibi sosyal mühendislik ile ilgili de genişletmeler sunmaktadır.
Sosyal Mühendislik Dolandırıcılığı Ek Teminatı: Yanlış kişiye veya sahte hesaba yapılan ödeme kayıplarını konu almaktadır.

Bu teminatın satın alınabilmesi için kurumların uyması beklenen bir takım minimum risk güvenlik kriterleri mevcuttur. Bu tür sigorta poliçelerinin kapsamı ve limitleri poliçeye göre değişebilmektedir. Sigorta brokerleri, ihracatçı firmaların ihtiyaçlarına uygun özel sigorta çözümleri sunarak firmaların bu tür tehditlere karşı mali güvencelerini güçlendirebilir.

Hazırlayan: İpek Ünal - Partner

Integra Sigorta ve Reasürans Brokerlığı A.Ş
Yönetici Sorumluluk Sigortası (D&O), Kapsamlı Suç Sigortası ,Siber Sigorta, Meslek Sorumluluk Sigortası, Ticari Alacak Sigortası, Politik Risk Sigortası ve Kefalet Sigortası dahil olmak üzere Finansal ve Profesyonel Sigorta Branşları konusunda 18 yıllık deneyim.

+90 (212) 708 90 30

ipek.unal@integrabroker.com

Ipek Ozerdem Unal | LinkedIn