Finansal suçlara karşı bütünsel bir savunma hattı

PwC Türkiye
Finansal Suçlar Birimi

pwc

Giriş

Şubat 2016'da Amerikan Merkez Bankası, Bangladeş Bankası tarafından bir gün içinde gerçekleştirilen ve toplamda 100 milyon ABD Dolar'ını aşan beş işlemi iptal etti. Para, Sri Lanka ve Filipinler'de bulunan hesaplarına gönderilmişti. Bu işlemlerin Bangladeş Bankası tarafından gerçekleştirilmediği daha sonradan anlaşılacaktı. Siber suçlular, sistemi hileli ödeme talepleriyle kandırmış ve yetkililer suçluların hesaplardaki paraları kaçırmalarını engellemek için zamanında harekete geçememişti. Sri Lanka hesaplarına gönderilen para kurtarıldı ancak Filipinler'e gönderilen 81 milyon Amerikan Doları'nın ülkenin kumar endüstrisine aktarıldığı anlaşıldı.

Bangladeş Bankası soygunu, yüz milyonlarca tüketiciyi etkileyen ve saldırganların finansal kurumlar içindeki siber güvenlik, suistimal ve kara para aklama (AML) operasyonlarındaki zafiyetlerden nasıl yararlandığını gösteren son zamanlardaki yüksek profilli veri ihlallerinden sadece bir tanesi. Siber güvenlik, suistimal ve AML fonksiyonları organizasyonlarda genellikle ayrı birimlerde yapılanmıştır. Bu durum, fonksiyonlar arasında yeterli iletişimi, veri bütünlüğü, süreç ve kaynak verimliliği açısından eksikliklere yol açmaktadır.

Siber saldırıları, dolandırıcılığı ve kara para aklamayı birbirinden bağımsız mali suçlar olarak düşünmek doğru değil. Etik olmayan bir işlem ya da siber bağlantılı bir soygun, para aklama planının ilk aşamasıdır çünkü yasadışı yollarla elde edilen suç gelirleri bu yollarla başka hesaplara taşınmaktadır.

Parayı çalma eylemi, kullanıcı cihazındaki kötü amaçlı bir yazılım ile veya kullanıcı kimlik bilgilerini çalmak için yapılan bir oltalama ('phishing') saldırısı ile siber güvenlik sistemindeki bir zayıflıktan yararlanabilir. Bangladeş Bankası örneğinde, saldırganlar ilk önce, sistem güvenliğini atlatmak ve sistemde iz bırakmamak için özel zararlı yazılımlar tasarlayarak siber zafiyetlerden yararlandılar. Daha sonra, kimlik avı ile topladıkları müşteri bilgilerini kullanarak, Bangladeş Bankası'nın ağına eriştiler ve oluşturdukları sahte hesaplarla para transferi gerçekleştirmeye başladılar. Son aşamada ise siber suçlular, elde ettikleri suç gelirlerini Filipinler'deki kumar endüstrisinde akladılar.

Finansal kurumlar siber suçlar konusunda endişe duymaktadırlar, ancak bu durumla en iyi nasıl başa çıkabileceklerini bilememektedirler.

PwC'nin 2018 Küresel Bilgi Güvenliği Anketi (GSISS) ve 21. Küresel CEO Anketi'nde, CEO'lar ve yönetim kurulları en çok endişe duydukları iş tehdidi olarak siber saldırıları tanımladılar, ancak Küresel Bilgi Güvenliği Anketi katılımcıların % 44'ünün, genel bilgi güvenliği stratejisi hakkında bilgi sahibi olmadıklarını ortaya koymaktadır. PwC'nin 2018 Küresel Ekonomik Suç Araştırması, büyük şirketlerin hemen hemen yarısının son iki yıl içinde dolandırıcılıktan zarar gördüğünü gösteriyor - bu rakam 2016'da gerçekleştirilen ankete oranla % 13 daha yüksek. Finansal kurumların mevcut riskleri daha net bir şekilde değerlendirebilmek için, şüpheli işlemleri hızlı bir şekilde tespit edip, önleyici adımlar atabilmek adına siber güvenlik, sahtecilik ve AML kontrollerini daha bütünsel yaklaşımlarla yönetmeleri gerektiğine inanıyoruz.

Hangi faaliyetler daha iyi koordine edilmeli?

Siber güvenlik, suistimal ve kara parayı aklamayı önleme programları genellikle ortak unsurlara ve kontrollere sahiptir. Çalışmalara başladıktan sonra birçok firma, belirli süreçlerin birleştirilmesi gerektiğini ve bazı süreçlerin ise aynı bilgiyi paylaşarak ayrı ayrı yürütülmesi gerektiğini fark edebilir.

Veri yönetimi, bütünsel yönetim için en kritik alanlardan biridir. Siber güvenlik, suistimal ve kara parayı aklamayı önleme programlarının geleneksel olarak birbirinden ayrı silolarda faaliyet göstermesinin nedenlerinden biri, veri kaynaklarının farklı departmanlara ait farklı sistemlerde olmasıdır.

Örneğin, AML programları müşterilerin demografik verileri ve işlem geçmişlerini saklayabilir, dolandırıcılık önleme programları olağandışı hesap hareketlerini ve hesap ayarlarında yapılan değişiklikleri kaydedebilir. Siber güvenlik uygulamaları ise cihaz, kullanıcı ve ağ ile ilgili verileri toplayabilir. Şirketler, ağdaki işlem hareketlerini ve kimlerin hangi hesaplara ve sistemlere erişim yetkisi olduğunun daha iyi anlaşılması için tüm bu bilgileri bir veri havuzunda ('data lake') saklayabilir. Üçüncü taraflardan alınan siber istihbaratlar da analiz yapılan bu veri havuzuna eklenebilir.

Tablo 1: Verinin bulunduğu yerler

Veri noktaları	Alışılagelmiş veri sahipleri	Saklama / kullanım süresi
İsimler, e-posta adresi, fiziksel adres, telefon numarası gibi kullanıcı kimlik bilgileri	AML, suistimal önleme	Yıllarca
IP adresi, coğrafi konum, üretici, işletim sistemi, uygulama tanımlayıcısı (veya kullanıcı aracısı) gibi kullanıcı cihaz bilgileri	Suistimal önleme	Aylar veya yıllarca
Oturum açma / oturum kapatma, erişim engelleme girişimleri, hesap kilitleme, şifre sıfırlama gibi sistem erişimi (müşteri ve kullanıcı) hareketleri	Suistimal önleme, siber güvenlik	Aylar veya yıllarca
Müşteri / kullanıcı işlemi, ödeme talimatı, servis uygulaması (ör. Kredi)	Suistimal önleme, siber güvenlik	Yıllarca
E-posta veya dosya aktarımı gibi veri hareketleri	Uyum, siber güvenlik	Aylar veya yıllarca
Yeni ayrıcalıklı kullanıcılar veya ayrıcalık değişiklikleri, aygıt / uygulama, yazılım ve yapılandırmadaki değişiklikler gibi sistem değişikliği olayları	Siber güvenlik, bilgi teknolojileri	Aylar veya yıllarca
Oluşturma, okuma, güncelleme, silme (CRUD) gibi veri / dosya erişim olayları	Siber güvenlik	Günler veya yıllarca

Finansal kurumların bütüncül yaklaşması gereken diğer alanlar şunları içerir:

- **İhlal/Olay yönetimi:** Kara para aklama ve suistimal uyarıları aynı yazılım ile yönetilebilir.

- **Risk değerlendirmesi:** Siber güvenlik, kara para aklama ve suistimal risk değerlendirmeleri, bir kurumun taşıdığı finansal suçlara ilişkin risklerin ortaya konması birlikte ele alınabilir.

- **Müşteri deneyimi:** Bu alandaki bütünsel yaklaşım, her ne kadar finansal suçların önlenmesini etkilemeyecek olsa da , müşterilerin aynı bilgileri birden fazla göndermesini veya onay almak için beklemelerini ortadan kaldırarak müşteri deneyimini iyileştirebilir.

Bir arada ele alınan faaliyetlerin finansal kurumlara daha hızlı ödeme yolları ve açık bankacılık gibi yeni teknolojileri keşfetmelerinin ve aynı zamanda bu teknolojilerin finansal suçları önlemeye nasıl yardımcı olacağına dair bir örnek: Günümüzde müşteri deneyimi, bankacılık işlemlerinin ve müşteri taleplerinin hızlı bir şekilde gerçekleşmesini gerektirir. Bu nedenle bankaların şüpheli işlemleri çok hızlı bir şekilde çözümlendirmeleri gerekir.

Bankaların, ödeme talimatlarının geçerliliğini değerlendirmek için kullanılan mobil cihaz türleri, IP adresleri ve ödeme geçmişi gibi kullanıcı trendlerine hızlıca erişebilmeleri gerekir. Bu, yalnızca daha kapsamlı ve daha bütüncül verilerle mümkün olacaktır.

Günümüzde müşteri deneyimi, bankacılık işlemlerinin ve müşteri taleplerinin hızlı bir şekilde gerçekleşmesini gerektirir. Bu nedenle bankaların şüpheli işlemleri çok hızlı bir şekilde çözümlendirmeleri gerekir.

Bu faaliyetler nasıl entegre edilebilir?

Finansal suçları önleme süreçlerinin entegrasyonu ancak tüm programın omurgası olarak hizmet verecek açık bir işletim modeli oluşturarak başarılabilir. Etkin bir işletim modeli üç temel yapıtaşından oluşur: yapı, gözetim ve yetkinlikler.

Yapı: Finansal kurumlar, finansal suçlar risk komiteleri ve tüzükleri, eskalasyon prosedürleri, organizasyon yapıları, insan kaynağı, ekip ve etkileşim yapılarından oluşan kurumsal bir yönetişim modeli oluşturmalıdır. Bu model, organizasyonun üçlü savunma hattı kapsamında rollerin, sorunlulukların ve iletişim kanallarının formal olarak belirlenmesini – ve açıkça dokümante edilmesini – içermelidir:

(a) Suistimal risklerinin izlenmesi ve yönetilmesi; (b) bağımsız risk yönetimi ve iç sistemler; (c) suistimal yönetimi faaliyetleri için bağımsız güvence sağlamakla sorumlu iç denetim fonksiyonu. Bu yönetişim yapısını geliştirirken, finansal kurumlar süreçleri konsolide ederek hangi ekiplerin birlikte çalışması gerektiğini belirleyebilir. Bu şekilde yapılanarak, kurumlar mükerrer işleri tespit edebilir ve ortadan kaldırabilir. Örneğin, para aklama ve suistimal uyarılarını incelemek için ayrı ekipler oluşturmak yerine, ortak bir ekip her ikisini de gözden geçirebilir. Daha açık veri görünürlüğü ile aynı işi yapan iki farklı ekibin birlikte çalışması verimliliği artırır.

İlk adım olarak, finansal kurumlar mevcut raporlama yapılarını gözden geçirerek iyileştirme alanlarını tespit etmeli ve üst yönetimin finansal suçlara ilişkin riskleri bütüncül olarak görebilmesini sağlamalıdır.

Gözetim: Organizasyonlar aynı zamanda farklı finansal suç disiplinlerini etkin bir şekilde yönetebilmek için kurum çapında bir yönetişim çerçevesi benimsemeli ve siber güvenlik, suistimal ve AML programlarının yönetimini, yürütülmesini ve denetlenmesini destekleyen finansal suçlar risk komiteleri oluşturmalıdır. Böylece, finansal suçları önleme stratejisinin ve politikaların bütüncül olarak uygulanmasına olanak sağlanacak ve iş birimlerinin, strateji belirlerken finansal suçlara ilişkin risk toleransını anlamasını ve dikkate almasını kolaylaştıracaktır. İlk adım olarak, finansal kurumlar mevcut raporlama yapılarını gözden geçirerek iyileştirme alanlarını tespit etmeli ve üst yönetimin finansal suçlara ilişkin riskleri bütüncül olarak görebilmesini sağlamalıdır.

Bu durum, siber güvenlik, tehdit istihbaratı, fiziksel güvenlik ve suistimal ile mücadele gibi unsurları bilgi güvenliği yöneticisinin sorumlulukları altında toplamak anlamına gelebilir.

Ayrıca, finansal suçlara yönelik sistemlerin entegrasyonu ile birlikte fiziksel güvenlik, özellikle iç tehdit yönetim programı ve suistimalcilerin tespiti konusunda önemli bir rol oynar. Bu alan, olay yönetim sistemi, istihbarat ve yasalara uyumluluk gibi temel alanların sinerjisi düşünüldüğünde genellikle gözden kaçırılıyor.

Yetkinlikler: Bütünleşik bir olay/ihlal yönetim sistemi ve tutarlı bir kök-neden analizi gibi standartlaştırılmış süreçlerin ve merkezi teknoloji çözümlerinin kullanımı, koordineli, verimli ve tekrarlanması kolay soruşturma sürecine olanak tanır. Ayrıca, gruplar arasında bilgi paylaşımı, bütünsel soruşturmalara imkan sağlayarak kurumları tek bir çerçeve içinde tutarlı süreçler geliştirmeye zorlayacaktır. Bu toplam riski azaltacaktır. AML, siber güvenlik ve suistimal önleyici kontrollerin bir araya gelmesi, kurumların düzenlemelerden kaynaklanan yükümlülüklerini nasıl yerine getirdiklerini yeniden gözden geçirme ve bu süreçleri pekiştirme fırsatı sunmaktadır.

Sıradaki adımlar ve doğru çözüm

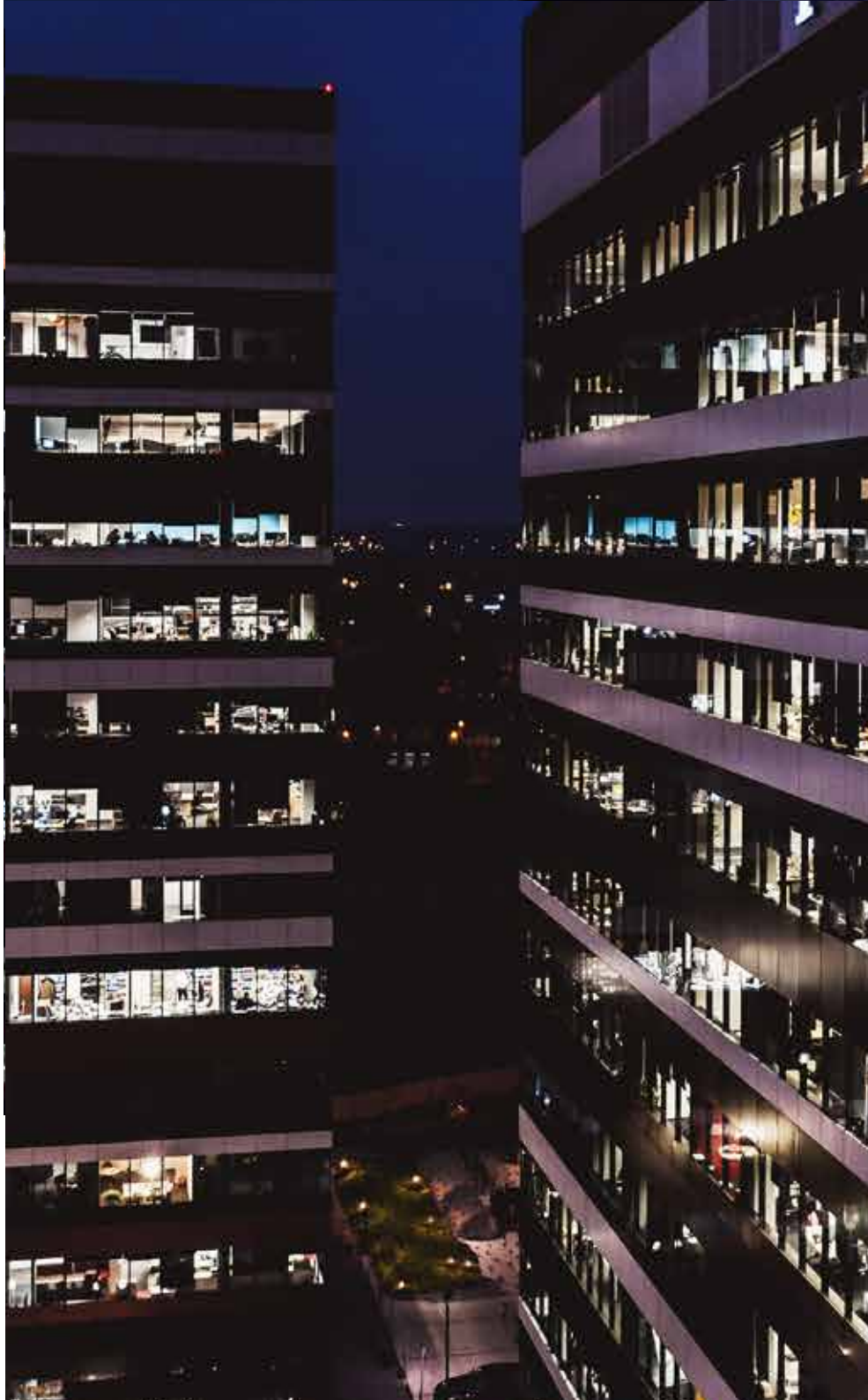
Her bir finansal kurum için en doğru çözüm; sunulan ürün ve hizmetler, coğrafi ayak izi, yerel mevzuatlar ve yasal gereksinimler, müşterilerinin demografik yapısı gibi çeşitli faktörlere bağlıdır.

Peki, firmaların şimdi atmaları gereken adımlar ne olmalı?

- Meslektaşlarınız ile bir araya gelerek bütüncül yaklaşım ve kısa vadeli faydaları hakkında fikir alışverişinde bulunun, görüş bildirin ve diyaloğu sürdürün.

- Size fayda sağlayacak teknolojileri ve araçları tanımlayın ve daha etkili çözüm yolları geliştirmek için gerekli adımları belirlemeye başlayın.

Bütüncül yaklaşıma giden yol, özellikle büyük ve karmaşık kurumlar için basit ve hızlı bir süreç değildir. Bazı fırsatlar bütüncül yaklaşım için yetkin olgunluktadır, bazıları gelecekte birbirine entegre edilmeli ve diğerleri ise ayrı kalmaya devam etmelidir. Önemli olan, kuruluşların şu anda entegrasyon hakkında neler yapabileceklerini gözden geçirmeye başlamalarıdır.



İletişim

Serkan Tarmur
Şirket Ortağı
PwC Türkiye Bankacılık ve
Sermaye Piyasaları Sektör Lideri
T: +90 212 376 5304
M: serkan.tarmur@pwc.com

Gökhan Yılmaz
CIA, CFE, CPA, CISA, CCSA, CRMA
Direktör
PwC Türkiye Ticari Anlaşmazlık
Çözümleri ve Suistimal İncelemeleri Lideri
T: +90 (212) 326 6488
M: gokhan.yilmaz@pwc.com

Cihan Vehbi Salihoğlu,
CISSP, CIPP/E, CISA, CIPT, CEH,
ISO 27001 LA
Direktör
PwC Türkiye Siber Güvenlik Hizmetleri Lideri
+90 212 326 6849
cihan.salihoglu@pwc.com

Derya Etiz
MBA, CAMS, CIPM
Kıdemli Müdür
PwC Türkiye Adli Bilişim Çözümleri Lideri
T: +90 212 355 6769
M: derya.etiz@pwc.com

Not

www.pwc.com.tr/finansal-suclara-karsi-savunma

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.
This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2018 PwC Türkiye. Tüm hakları saklıdır. Bu belgede PwC ifadesi, PwC ağını veya PwC ağının üyesi olan bağımsız ve farklı tüzel kişiliklerden oluşan PwC Türkiye'yi ifade etmektedir. Daha detaylı bilgi için www.pwc.com/structure adresini ziyaret edebilirsiniz.

2018-0315