KPMG

Bir Suistimalcinin Profili 2016

Teknoloji suistimali kolaylaştırıyor, zayıf kontroller ise körüklüyor

Haziran 2016

kpmg.com/fraudster

KPMG Türkiye

İçindekiler

Önsöz

Suistimal, şirketlerin itibarına zarar veren, milyonlara mal olan ve hayatları mahveden küresel bir sorun. Toplum üzerinde ağır ekonomik ve ahlaki yükler doğuruyor. KPMG yıllardır suistimal trendleri hakkında raporlar yayımlıyor ve elinizdeki bu rapor da tüm dünyadaki suistimalcilerin profilini çıkaran üçüncü rapor. Bu raporda, profesyonellerimiz, soruşturmalarımız sırasında elde ettiğimiz bilgilerden yola çıkarak yaklaşık 750 suistimalci hakkında detaylı bir anket gerçekleştirdi.

Suistimale kalkışan kişi tipleri, yaptıkları suistimal türü ve bu suistimallerin nasıl tespit edildiği hakkında daha fazla bilgi edinmek amacıyla, bu üçüncü anketimize bazı yeni sorular ekledik. Bu en son anket, suistimalin teknoloji boyutu ve siber suistimal hakkında bazı sorular da içeriyordu. Raporumuzun sonunda da, tehditlerin giderek gelişip değiştiği bir ortamda suistimalle en iyi şekilde nasıl mücadele edilebileceğine dair önerilerimize yer verdik.

Suistimalcinin profiliyle ilgili bu raporun amacı, müşterilerimizin bu karmaşık konuyu ve bu konunun gelecekte ne yönde değişebileceğini anlayabilmelerine yardımcı olmak. Anketimizin, suistimalciler ve bunlarla mücadele yollarıyla ilgili dünya genelindeki tartışmaya katkıda bulunacağını da umuyoruz. Bu tartışmanın sonucu, şirketleri, devletleri ve genel olarak toplumu doğrudan ilgilendiriyor.

Petrus Marais
Küresel Suistimal Önleme ve İnceleme Hizmetleri Başkanı

Phillip Ostwalt
Küresel Soruşturmalar Başkanı

Yönetici özeti

KPMG Suistimal İnceleme Uzmanları tarafından 2013 yılı Mart ayı ile 2015 yılı Ağustos ayları arasında gerçekleştirilen suistimal incelemelerinden edinilen bilgilerle hazırlanan "Bir Suistimalcinin Profili" raporunun üçüncüsünde 81 ülkeden 750 farklı suistimalci profili incelendi. Peki tipik bir suistimalcinin öne çıkan özellikleri neler?

- Erkek
- 36-55 yaşları arasında
- Şirkette 6 yıldan uzun süredir yönetici pozisyonunda çalışan

2010 ve 2013 yılındaki raporlara baktığımızda suistimalci profilinin çok büyük farklılıklar göstermediğini ancak suistimal karşıtı kontrollerin gittikçe zayıfladığını ve problemin gün geçtikçe büyüdüğünü görüyoruz. İç kontrol zayıflıklarını fırsat olarak kullanan suistimalcilerin arttığını, teknoloji kullanımının suistimallerin oluşmasında son derece etkili olduğunu ancak; suistimallerin tespiti ve önlenmesi aşamasında teknolojiden yeteri ölçüde yararlanılmadığını görüyoruz.

Türkiye'deki duruma baktığımızda, globaldeki çalışmanın sonuçları ile benzer bir şekilde, şirket varlıklarının kötüye kullanılması, zimmet ve satın alma yolsuzluklarının en çok rastlanan suistimal türleri olduğunu gözlemliyoruz. Özellikle satın alma sürecindeki suistimallerde, hayali satın almalar, ihalelerdeki yolsuzluklar, üçüncü şahıslarla çıkar amaçlı kurulan ilişkiler ve yöneticilerin kurdukları kişisel firmalara şirket kaynaklarının aktarılması Türk şirketlerinin karşı karşıya olduğu başlıca suistimal riskleri olarak öne çıkıyor.

Ekonomik ve politik gündemdeki hızlı gelişmeler, Türkiye'de faaliyet gösteren çok uluslu ve lokal şirketlerin karlılık hedeflerini karşılayabilmek için daha agresif politikalar ve stratejiler geliştirmesine neden oluyor. Bu süreçte şirketler, suistimalin önlenmesine yönelik etkin kontrolleri hayata geçirmek ya da mevcut kontrollerini iyileştirmek konusunda yeterli kaynağı ayıramıyor ve bu durum da şirketleri suistimale daha açık bir hale getiriyor.

Şirketler, temel iç kontrol süreçlerini hayata geçirdiklerinde, mevcut kontrollerin onları suistimale karşı sürekli koruyacağını varsayıyorlar. Oysa suistimal risklerini de içerecek şekilde risk yönetimi, iç kontrol çerçevesi kanalıyla sürekli izlenmesi ve değişen risklere cevap verecek şekilde uygulanması gereken bir süreçtir.

Günümüzde şirketler, suistimali önleyecek kontrollere yatırım yapmak yerine, maliyetleri azaltma kaygısıyla, gereksiz masraflar olarak değerlendirilen harcamaları kesme yoluna gidiyor ve ne yazık ki suistimali önlemeye yönelik kontroller de bu masraf kaleminde değerlendiriliyor.

Tüm dünyada olduğu gibi Türkiye'de de siber yolsuzluklar alanında bir artış olduğunu görüyoruz. Suistimalciler, teknolojinin sunduğu pek çok yeni fırsatı değerlendirmekten çekinmiyorlar. Siber yolsuzlukların tespiti ve raporlaması konusunda ülkemizde eksiklikler olduğundan bunların takibi de yapılamıyor. Araştırma, dünyadaki mevcut durumun da Türkiye'den çok farklı olmadığını ve şirketlerin aslında bu tehdidin farkında olduğunu ancak başlarına geleceğini düşünmediğini gösteriyor. Çalışma ayrıca, siber suistimal girişimlerinin başlıca amacının kişisel bilgilerle fikri mülkiyeti çalmak, üst düzey yöneticilerin e-postalarına erişmek, şirket verilerine stratejik erişim sağlamak ve DoS saldırısına yol açmak olduğunu ortaya koyuyor.

Şirketler, bir yandan suistimale karşı yaptırımların artırılmasını desteklerken diğer yandan da yolsuzlukların önlenmesi için içeride tedbir almak ve bu risklere karşı hazırlıklı olmak durumundalar. Bu amaçla, düzenli olarak risk analizleri ve iç denetimler yaptırabilir, üçüncü taraf risklerine cevap verecek bir yaklaşım izleyebilir, suistimal bildirim mekanizmalarını hayata geçirebilir ve tehditleri izlemeye ve veri analizi yapmaya olanak sağlayan teknolojik çözümleri kullanabilirler.

Her ne kadar yolsuzlukların önlenmesi için, milyonlarca işlemi hızla inceleyerek şüpheli işlemleri tespit etmeye yarayan veri analizi araçları olsa da bu etkin teknolojik araçların kullanımın %3 gibi çok az bir oranda kaldığını ve ihbar mekanizmasının suistimallerin ortaya çıkartılmasında halen en etkin yöntem olduğunu görüyoruz.

Keyifle okumanız dileğimle,

İdil Gürdil
Suistimal Önleme ve İnceleme Hizmetleri Lideri, Risk Yönetimi Danışmanlığı, Şirket Ortağı

— Suistimalle mücadele kontrolleri (iç denetim, şüpheli yönetici ve çalışanlar ve suistimalle mücadele süreçleri) yeterince güçlü değil ve bu sorun giderek büyüyor. KPMG'nin tüm dünyadan 750 suistimalciyle ilgili yaptığı araştırma; bu suistimal vakalarının en az dörtte üçünde zayıf iç kontrollerin bu duruma zemin hazırladığını ortaya koydu. 2013 yılındaki anketle kıyaslandığında, zayıf iç kontrollere bağlı olarak bir fırsat gören suistimalcilerin oranında kayda değer bir sıçrama gözlemlendi.

— Kontroller güçlü olsa bile suistimalciler bunlardan kurtulmanın bir yolunu bulabiliyor veya aşabiliyorlar. Bu noktada, özellikle çok fazla yetkiye sahip yöneticileri kontrol altına almak için (bildirimde bulunan, farklı türde ihbar mekanizmaları ve şüpheli müşteriler ve tedarikçilerin belirlenmesi gibi) birbirinden farklı yöntemler ortaya çıkıyor.

— Suistimal, tek başına yapıldığından neredeyse iki kat fazla oranda gruplar halinde yapılıyor. Bunun bir nedeni, suistimalcilerin kontrollerden kaçınmak için çoğu zaman işbirliği yapmaya ihtiyaç duymaları. Bu nedenle danışıklı işler şirketler için önemli bir tehdit unsuru. Örneğin beş veya daha fazla kişiden oluşan daha büyük gruplar tek başına veya küçük gruplar halinde hareket eden suistimalcilere göre finansal açıdan kurumlara daha fazla zarar veriyorlar.

— Erkek suistimalciler kadınlara göre daha fazla işbirliği yapıyor. Kadınların bu konudaki oranı 2010 anketine göre artmış olsa da, işbirliği yapan erkeklerin sayısının bu ankette kadınların yaklaşık beş katı olduğunu görüyoruz. Ayrıca erkek sustimalciler kadın suistimalcilere oranla şirket içerisinde daha üst seviyede yer alıyorlar.

— Suistimalci grupları çoğunlukla, hem şirket içinden hem şirket dışından kişilerden oluşuyor. İşbirliği yapanların %61'i ya şirket çalışanı değil ya da şirket çalışanı olmayan kişilerle işbirliği yapan şirket çalışanları. Bunların bazıları da eski çalışanlar. Bu durum, tedarikçiler ve müşteriler gibi şirket dışından çalışılan üçüncü taraflar ile çalışılmaya başlamadan önce, durum değerlendirmelerinin yapılması gerektiğine işaret ediyor.

— Teknoloji, hem suistimalcilere hem de suistimalle mücadele eden şirketlere yardımcı oluyor. Suistimalcilerin dörtte birine yakını teknolojiden faydalanıyor. Buna karşılık şirketler, ise suistimali önlemek, tespit etmek ve buna karşılık verebilmek için teknolojiyi çok daha iyi bir araç olarak kullanmalıdır. Suistimalle mücadelede teknolojisinin anahtarı ise, milyonlarca işlemi hızla inceleyip şüpheli öğeleri arayabilen bir araç olan veri analitiği. Oysa, araştırılan suistimalcilerin tespit edilmesinde suistimalle mücadeleye yönelik proaktif veri analitiği araçlarının kullanılma oranının sadece %3 olduğu görülüyor.

— Teknoloji tabanlı suistimal faaliyetlerinin önemli bir türü olan siber suistimal tehlikesi giderek büyüyor ve pek çok şirket bu sorunun farkında olsa da bunun için fazla bir şey yapmıyor.

— Suistimal tehditlerinin sürekli değişim gösterdiği bir ortamda, şirketler düzenli risk değerlendirmeleri yapmak ve gerekiyorsa suistimali tespit etme ve önleme yöntemlerini değiştirmek zorundalar.

Bir suistimalcinin profili

Mart 2013 - Ağustos 2015 arasında 750 suistimalci için soruşturma yürüten KPMG uzmanlarıyla gerçekleştirilen küresel bir anketin sonuçlarına göre, tipik bir suistimalci 2010 ve 2013 yıllarında yapılan KPMG anketleriyle benzer karakteristik özellikler taşıyor. KPMG anketlerinde düzenli olarak ortaya çıktığı gibi; suistimal faili erkek ve 36-55 yaş arasında, mağdur kuruluşta altı yıldan uzun bir süredir çalışıyor ve operasyon, finans ya da genel yönetim bölümlerinde yönetici konumunda. 2015 anketinde ortaya çıkan, suistimalcinin diğer temel karakteristik özellikleri ise şöyle:

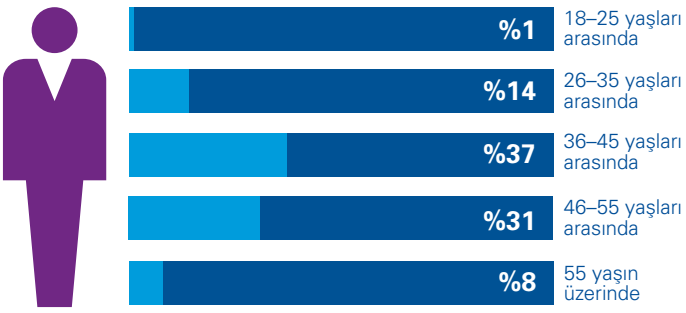
Yaş ve Cinsiyet

— Suistimalcilerin %79'u erkek olsa da, kadınların 2010 yılında %13 olan oranları %17'ye yükseldi.

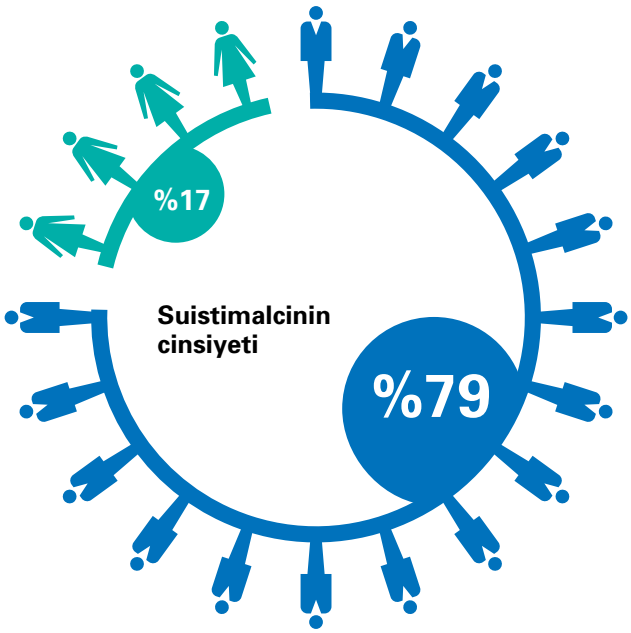
— Faillerin (erkek veya kadın) %69'u 36-55 yaş arası kişiler ve bu oran 2013 anketindeki oranla hemen hemen aynı. Kadın suistimalcilerin %45'i, en büyük grup olarak, 36-45 yaş grubunda yer alıyor.

— Suistimalcilerin %14'ü, 26-35 yaş grubunda; bu oran 2010 anketine göre %12 seviyesindeydi. Bu yaş grubundaki kadınların 2010 anketinde %24 olan oranı ise 2015 anketinde %19'a geriledi. Aynı yaş grubunun oranı erkeklerde ise aynı dönemde %9'dan %13'e çıktı.

Suistimalcinin yaşı



*Geri kalanın yaşı bilinmiyor
Kaynak: Bir Suistimalcinin Profili 2016, KPMG



*Geri kalanın cinsiyeti bilinmiyor
Kaynak: Bir Suistimalcinin Profili 2016, KPMG

İçerideki kişi, dışarıdaki kişi ve işbirliği

— Suistimalcilerin %65'i mağdur olan şirkette çalışıyor, %21'i ise eski çalışanlar. Şirket çalışanı olan suistimalcilerin %38'i şirkette altı yıldan uzun bir süre çalışmış. Bu oranlar 2013 anketindeki oranlarla aynı.

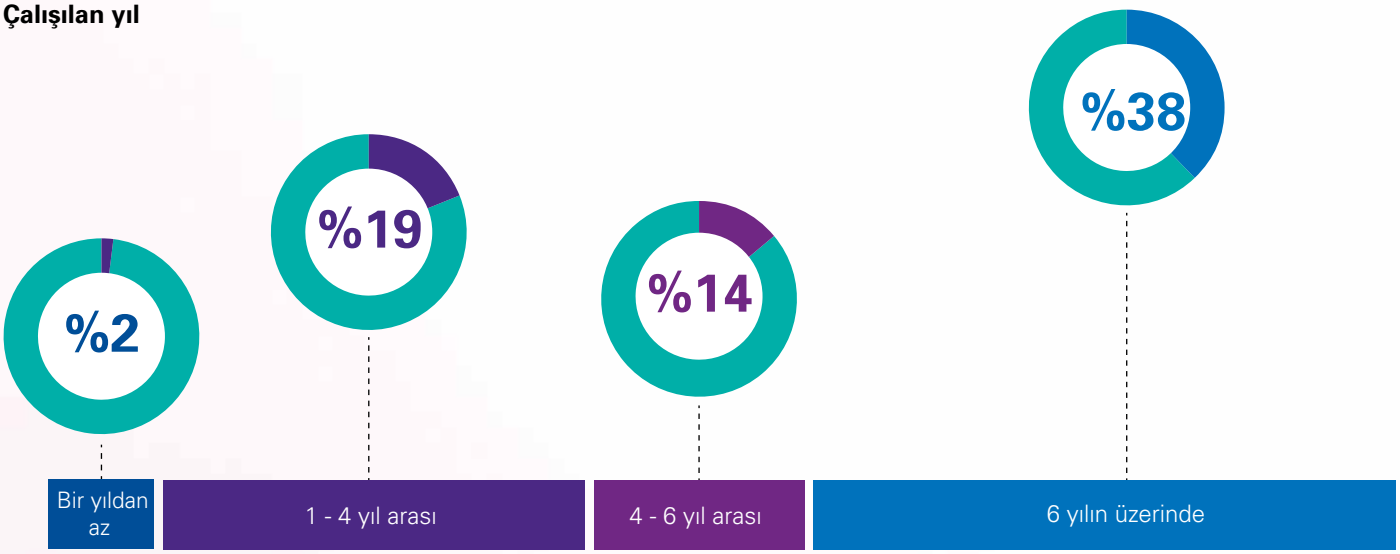
— Suistimallerin %62'sinde fail başkalarıyla suç için işbirliği yapıyor. 2013 anketi ise suistimalcilerin %70'i başkalarıyla işbirliği yaptığını gösteriyordu.

— Kadınların işbirliği yapma oranı daha düşük: Kadınların sadece %45'i suistimal için başkalarıyla işbirliği yaparken erkeklerde bu oran %66.

— Beşten fazla kişinin katıldığı işbirliklerinin 2010 anketinde %9 olan oranı 2015 anketinde %20'ye yükseldi.

— İşbirliği en çok Latin Amerika ve Karayip ülkeleri (%76) ile Ortadoğu ve Afrika ülkelerinde (%74) yaygın. Tek başına hareket eden suistimalcilerin oranının en yüksek olduğu yerler ise %65 oranla Avustralya ve Yeni Zelanda gibi Okyanusya ülkeleri ile %58 oranla ABD ve Kanada gibi Kuzey Amerika ülkeleri.

Çalışılan yıl



Kaynak: Bir Suistimalcinin Profili 2016, KPMG

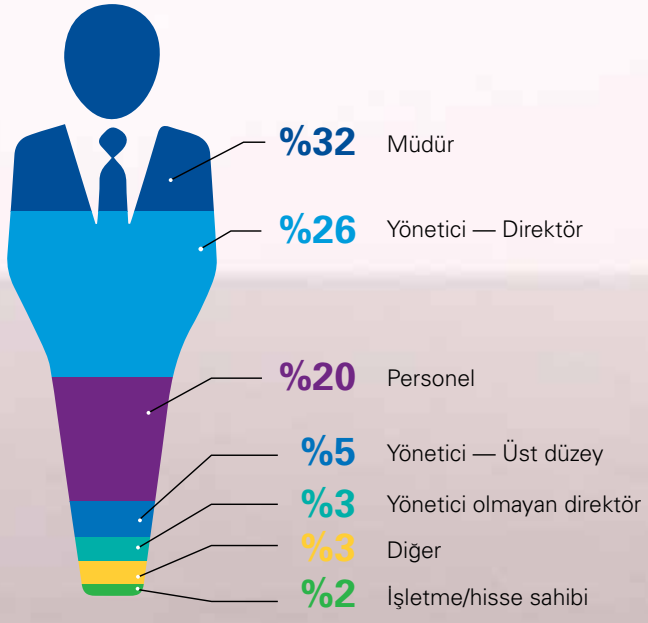
Şirketteki Pozisyon

— Suistimalcilerin %34'ü üst düzey yönetici ve direktörlerden, %32'si müdürlerden ve %20'si diğer seviyelerdeki personelden oluşuyor. (2013 anketinde bu oranlar sırasıyla %32, %25 ve %16 idi).

— Kadın suistimal faillerinin %42'si diğer seviyelerden personel (2010 yılında %46), %38'i müdürler (2010 yılında %28), %13'ü ise üst düzey yöneticiler. Erkek suistimalcilerin ise yalnızca %15'i diğer seviyelerden personel, %32'si de yönetici seviyesinde.

— Okyanusya bölgesindeki suistimalcilerin %52'si diğer seviyelerdeki personelden oluşuyorken, Ortadoğu ve Afrika ülkelerindeki suistimalcilerin %47'si müdür seviyesinde (Kuzey Amerika ülkelerinde %33), Avrupa'daki suistimalcilerin ise %39'u direktör seviyesinde yönetici.

Kıdem düzeyi



Kaynak: Bir Suistimalcinin Profili 2016, KPMG

Kişisel Özellikler

— Suistimalcilerin %38'ini oldukça saygı gören, %10'u ise çevrelerinde pek sevilip saygı görmeyen kişiler oluşturuyor.

— Üstünlük duyguları korku veya öfke duygularından daha güçlü.

Kontrolleri Atlatmak

— Zayıf iç kontroller bu dönem suistimalcilerin %61'i için katkı sağlayan bir etken olurken 2013 anketinde bu oran %54'tü. Çalışma, Avrupa'da suistimalcilerin %72'sinin, zayıf kontrollerin söz konusu suistimal için kendilerine fırsat verdiğini söylediğini ortaya koydu. Benzer biçimde, Kuzey Amerika ve Okyanusya'daki katılımcıların %59'u da bu fırsata işaret ettiler.

— Faillerin %44'ü şirketlerinde sınırsız yetkiye sahipler ve kontrolleri aşabiliyorlar. KPMG'nin araştırdığı tüm bölgelerde, suistimalcilerin büyük bir kısmı sınırsız yetkiye sahipti.

Suistimalin Genel Özellikleri

— Suistimalcilerin %24'ü için teknoloji, önemli bir kolaylaştırıcı unsur oldu. Bunun yanı sıra, anketimiz bu yıl ilk kez KPMG tarafından soruşturulan 31 siber suistimalciyi de kapsıyor.

— En yaygın görülen suistimal türünün, ağırlıklı olarak zimmet ve satın alma yolsuzlukları şeklinde gerçekleşen varlıkların kötüye kullanımı (%47); ikinci en yaygın suistimal türü ise suistimal amaçlı raporlama olduğunu görüyoruz (%22).

— Ortadoğu ve Afrika ülkelerindeki suistimallerin %24'ü enerji ve doğal kaynaklar sektöründe gerçekleşirken, Okyanusya ülkelerindeki suistimallerin %26'sı kamu sektöründe görüldü.

— Suistimallerin %66'sı bir ila beş yıl arası bir süre boyunca gerçekleştirildi (2013 anketinde %72 oranındaydı) ve %27'si mağdur olan şirkete en az 1 milyon ABD Doları zarar verdi (2013 yılına göre benzer oranlar).

— Suistimalcilerin %44'ü bir anonim bildirim, şikayet veya resmi bir ihbar hattı sayesinde, %22'si ise yönetim incelemesi sonucunda tespit edildi.

Zayıf kontroller giderek büyüyen önemli bir sorun

Kurumsal suistimal, hem yöneticiler hem de yönetim kurulları için giderek daha kalıcı ve küresel bir zorluğa dönüşüyor. Şirketlerin giderek tırmanan siber suistimal tehdidiyle karşı karşıya kaldığı ve muhasebe defterlerinde ve kayıtlarda sahtecilik gibi geleneksel suistimal biçimlerinde hiçbir azalma görülmediği bir ortamda, suistimal riskinin yönetimi de giderek daha karmaşık bir hal alıyor. Bu duruma karşılık verebilmek amacıyla pek çok şirket suistimali önlemeye, tespit etmeye ve gerekli karşılıkları vermeye yönelik güçlü iç kontrolleri hayata geçirdi. Ancak bu durumun dünya geneline yayıldığını söylemek zor. Zira anketimiz, suistimalcilerin %61'i için (Avrupa'da %72) zayıf iç kontrollerin önemli bir etken olduğunu ortaya koydu.

Bu durum, pek çok şirketin bu sorunu yönetmekte yaşadığı zorluğun ölçütüne işaret etmekle kalmıyor, finansal kaybın veya itibar kaybının önlenmesi de dahil olmak üzere, suistimalle mücadele kontrollerinin sıkılaştırılmasıyla elde edilebilecek potansiyel faydaları da ortaya koyuyor. Daha basit bir ifadeyle, sağlam iç kontroller ve gözetim süreçlerinin bulunduğu şirketlerde suistimalin gerçekleşme olasılığı da düşüyor. KPMG Singapur Suistimal Önleme ve İnceleme Hizmetleri Lideri Lem Chin Kok, "Kötü tasarlandıkları ve çalışanlar tarafından riayet edilmedikleri takdirde iç kontroller zayıflıyor. Kapsamlı bir suistimal risk değerlendirmesi ise, zayıflık ve eksiklikleri ortaya koymada son derece etkilidir" diyor.

Bu durum, suistimalcilerin önemli bir bölümünün (%14) iç kontroller ve gözetim süreçlerinden ziyade "şans eseri" tespit edildiği gerçeğinde de kendisini gösteriyor. Anket kapsamında incelenen suistimalcilerin %75'i, zayıf kontrollerin suistimale zemin sağlayan ve suistimalin fark edilmeden gerçekleştirilmesine izin veren bir etken olduğunu belirttiler.

Suistimalle mücadelede oldukça etkili kontroller ve süreçler var ve bunları öneriler bölümünde sizlere açıklayacağız.

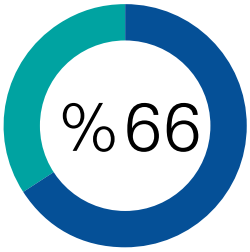
Zayıf kontroller, suistimal kurbanı olan şirketler için önemli bir sorun ve bu sorun büyümeye devam ediyor. Kontrollerin zayıf olması veya var olmaması nedeniyle suistimal suçunu işleme ya da buna teşebbüs etme fırsatını yakaladığını söyleyen kişilerin 2013 yılında %18 olan oranı önemli bir artış kaydederek %27'ye yükseldi. KPMG Meksika Suistimal Önleme ve İnceleme Hizmetleri Lideri Shelley Hayes, "Suistimalcilerin iş arkadaşlarının ters giden bir şeyler olduğunu hissettiği ancak görmezden geldiği vakalar belirledik. Diğer bazı vakalarda ise, suistimalcilerin iş arkadaşları farkında olmadan, aslında iç kontrolleri devre dışı bırakacak şekilde sadece bir iş arkadaşına yardımcı olarak suça olanak tanımışlardı" diyor.

Kötü tasarlandıkları ve çalışanlar tarafından riayet edilmedikleri takdirde iç kontroller zayıflıyor. Kapsamlı bir suistimal risk değerlendirmesi ise, zayıflık ve eksiklikleri ortaya koymada son derece etkili.

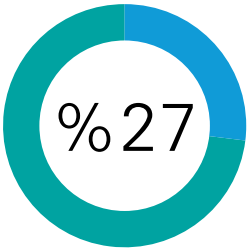
Suistimale zemin hazırlayan faktörler

Kaynak: Bir Suistimalcinin Profili 2016, KPMG

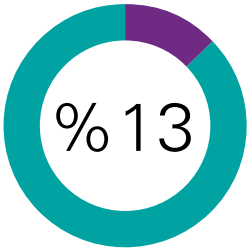
Suistimalcinin öne çıkan motivasyon kaynağı neydi?



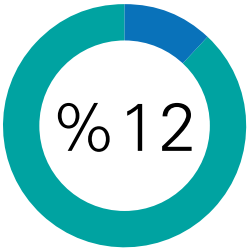
Kişisel maddi kazanç ve hırs



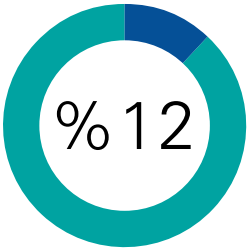
İstek/"Yapabiliyorum Duygusu"



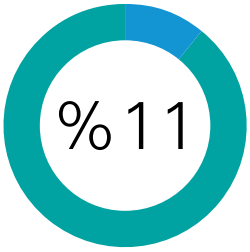
Organizasyonel kültür odaklı



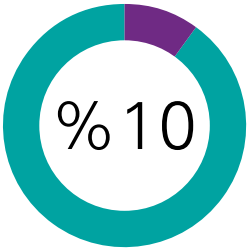
Bonus kazanmak için hedefleri tutturma/ kayıpları gizleme isteği



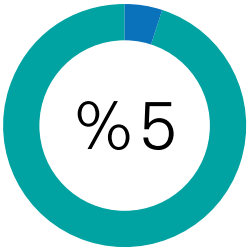
İşini kaybetmemek için bütçeyi tutturma/kayıpları gizleme isteği



Şirketi korumak için hedefleri tutturma/kayıpları gizleme isteği



Yukarıda sayılmayan diğer bir neden



Diğer motivasyonlar arasında (%5 ve altında) kendine güvenin kaybolması, düzenleyici uyum gerekliliklerinden kaçınma, oranlama odaklı, medya görünürlüğü odaklı, operasyonların aksaması vb nedenler yer alıyor

Yolsuzluğun sıra dışı özellikleri

KPMG profesyonelleri çoğu zaman suistimal ve yolsuzluğun bir arada var olduğunu, dünya genelinde düzenleyici makamların da, rüşvet ve yolsuzlukla mücadeleye giderek daha fazla odaklandıklarını belirtiyor. İncelenen 750 suçlu arasında 125'i yolsuzluk türü suistimallere karışmıştı ve bu kişiler diğer suistimal amaçlı faaliyetlere karışan kişilere göre daha farklı özellikler sergiliyor. Öncelikle yolsuzluk genellikle şirketin daha üst seviyelerinde gerçekleşiyor: Bu suçları işleyenlerin %51'i üst düzey yöneticiyken, diğer suistimal suçlarında bu oran %31. Üstelik bu suçların önemli bir bölümü C-seviye yöneticilerin ofisinde işleniyor (%26; diğer suç türlerinde %15).

Yolsuzluğa bulaşanların %63'ü, diğer suistimal suçlarını işleyenlerin ise %47'si en az üç yıl süreyle bu suçu işledi, ancak suistimalin verdiği maddi hasar aşağı yukarı aynı. Bununla birlikte, yolsuzluk, diğer suistimal suçu türlerinden çok daha farklı bir yolla tespit edildi. Bu suçların %61'i kimliğini gizlemeden yapılan ve diğer anonim bildirim yolları aracılığıyla tespit edilirken, diğer suistimal suçlarında bu oran %33 oldu. KPMG Hindistan Suistimal Önleme ve İnceleme Hizmetleri Bölümü Şirket Ortağı Jagvinder Brar, "Yolsuzluğun bildirilmesi, ihbar mekanizmalarının ne kadar önemli olduğunun bir başka örneği" diyor.

Şirketler, suistimalin hem maddi kayıplara hem de itibar kayıplarına yol açabilen bir sorun olduğunun farkındalar. Dünya genelinde düzenleyici makamlar da, hem şirketler üzerindeki denetimi sıkılaştırıyor hem de iş ahlakı anlamında daha katı kurallar getiriyor. Büyük şirket skandallarının kamuoyu hafızasındaki tazeliğini koruduğu ABD ise bunların başında geliyor.

Kontrollerin zayıf olması neden giderek önemi artan bir sorun? Tüm dünyadaki KPMG profesyonellerinin tespit ettiği nedenlerden biri, şirketlerin ekonomik zorluklar nedeniyle daha güçlü suistimalle mücadele kontrollerine yatırım yapmamaları. İtalya ve Yunanistan gibi nakit sorunu yaşayan ülkelerde veya enerji gibi sıkıntılı sektörlerde suistimal giderek artıyor. Bir ekonomi yavaşlamaya başlayınca, kontrollerin titizlikle uygulanmadığı ekonomik canlılık döneminde gerçekleşmiş olan suistimallerin yüz üstüne çıkarılması şaşırtıcı değildir. Kontrollerin zayıf olmasının büyüyen bir sorun haline gelmesinin bir başka nedeni de, şirketlerin iş fırsatları arayışıyla yeni coğrafi pazarlarda girişimde bulunmaları ve bunların arasında yolsuzluğun yaygın olduğu ülkelerin de bulunması.

Bütçesi kısıtlı ve pazar payını artırmakta zorlanan şirketler, risk profillerini değiştirmeye yönelik etkin kontrollere yatırım yapmada biraz geri kalıyorlar. KPMG ABD Suistimal Risk Yönetimi Lideri Tim Hedley, "Bu tür şirketler sıklıkla, bunun yaratabileceği riski etraflıca değerlendirmeden, kontrolleri ortadan kaldırıyor" diyor. "Düzenli risk değerlendirmeleri, şirketlerin suistimalle mücadele mekanizmalarına yapılacak yatırımlara öncelik vermelerine ve paralarını en etkili sonuçları verecek yere harcamalarına yardımcı oluyor."

En büyük suistimaller kontrolleri atlatıyor ya da devre dışı bırakıyor

İşledikleri suçlar şirkete 5 milyon ABD doları veya daha fazla maddi zarar vermiş olan 86 suistimalciyi analiz ettik. Bu tür vakalar genellikle diğer suistimal kategorilerine göre çok daha uzun sürüyor. Üstelik, buradaki suistimalciler daha üst düzey yöneticiler olduğundan ve kontrolleri atlatmak için başkalarıyla işbirliği yaptıklarından bu vakaların tespit edilmesi de daha zor. Ayrıca daha uluslararası nitelikteler ve bu suistimaller büyük oranda sınır aşırı gerçekleştirildi (%11 oranındaki küçük çaplı suistimallere karşı %34 oranında).

Bu gruptaki suistimalciler genellikle ortalama yaşın üzerindeki kişiler. %85'i erkek ve üst düzey yöneticilerin suça bulaşmış olma ihtimali çok daha yüksek (daha küçük suçlarda bu oran %31 iken bu tür suçlarda %54). KPMG Güney Afrika Suistimal Önleme ve İnceleme Hizmetleri Bölümü, Soruşturmalar Birimi Lideri Dean Friedman, "Aslında tüm suistimalcilerde bir üstünlük duygusu olsa da, en büyük suistimalleri gerçekleştirenler daha despot ve sınırsız yetkiye sahip kişiler" diyor.

Bu da onların, başkalarını kendisine yardım etmeye daha kolay ikna etmelerini veya buna mecbur bırakabilmelerini sağlıyor. İşbirliği yapma oranı bu tür büyük suçlarda (%86) daha küçük suistimallere göre (%60) daha yüksek, ayrıca işbirliği yapanlar arasında şirket dışından kişilerin olma ihtimali de daha düşük. Bu suçların üçte birine yakını (%32) beşten fazla kişiyle işlenmiş (diğer suçlarda bu oran %18). Tahmin edilebileceği gibi, suçluların %51'i büyük küresel şirketlerde çalışıyordu (daha az maddi zarara yol açan suistimallerde bu oran %38). Ayrıca bu tür suçlara karışanların %20'si finansal hizmetlerde çalışıyordu, geri kalan suistimalcilerde ise bu oran %8.

Suistimalin en tehlikeli türlerinden biri, genellikle erkeklerden oluşan beş veya daha fazla kişiden oluşan gruplar halinde işlenenler. Bu büyük grupların gerçekleştirdiği suistimal eylemlerinin %27'si şirketlere 5 milyon ABD doları ve üzerinde zarar verdi ve beş yıldan uzun sürdü. KPMG Orta ve Doğu Avrupa Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı Jimmy Helm, "En etkin tespit yöntemleri iç denetim veya yönetim incelemesi değil, ihbar mekanizmaları ve anonim bildirimler oluyor. Tespit edilmesi en güç olanlar ise olağanüstü yetkilere sahip suistimalciler" diyor.

İnsanlar güçlü kontrolleri de atlatabiliyor

> **Suistimalcilerin %21'i**, çalıştığı şirketlerin iç kontrollerine riayet etmemeyi başarmış. Üstelik yakalanma konusunda ciddi bir endişe de duymamışlar.

Güçlü suistimalle mücadele kontrolleri son derece önemli olsa da, kesin çözüm olmadıkları da ortada. Suistimalcilerin %21'i, çalıştığı şirketlerin iç kontrollerine riayet etmemeyi başarmış. Üstelik yakalanma konusunda ciddi bir endişe de duymamışlar. Yakalanma riskini bildikleri halde yollarına devam edip şirketi suistimale uğratmışlar. Kontroller sıkı olsa bile, daima şanslarını denemek isteyen kişiler çıkacaktır. Bazı kontroller kağıt üzerinde oldukça güçlü görünebilir, ancak harfiyen uygulanmıyor veya kolayca bertaraf edilebiliyorlarsa, suistimal riskini önleme potansiyeli de azalacaktır.

Bazı suistimalciler, muhtemelen güçlü pozisyonlarda oldukları için yakalanma risklerinin düşük olduğunu düşünüyor. Bu kişiler kuralları esnetebileceklerine hatta görmezden gelebileceklerine inanıyor.

Suistimalcilerin oldukça yüksek bir bölümü (%44), sınırsız yetkiye sahip kişilerdi. KPMG İngiltere Soruşturmalar Bölüm Başkanı Alex Plavsic, "Bu bir kuruluş için iki tehlikeyi bir arada barındırıyor. Birincisi bu kişiler ister zayıf ister güçlü olsun, tüm kontrolleri aşabiliyorlar, ikincisi ise emirleri altındaki çalışanlara suistimali örtbas etmesine yarayacak görevler verme yetkisine sahip kişiler" diyor. Bu kişilerin verdiği hasarlar da genellikle daha ağır oluyor: Bu kişilerin gerçekleştirdiği suistimallerin %34'ü şirkete 1 milyon dolar ve üzeri zarar vermiş, sınırsız yetkiye sahip olmayanlarda ise bu oran %18'de kalmış.

Kişisel özellikler de yangını körükleyebiliyor. Ankete göre, profili çıkarılan suistimalciler için en sık kullanılan tanım despot kişiler olmaları ve korku veya öfke duygularından çok daha güçlü bir üstünlük duygusuna sahip olmaları. Sınırsız yetkiye sahip suistimalciler daha da despot ve üstünlük duygusu daha da yüksek kişiler oluyor.

Dış görünüşe göre, suistimalcilerin çevrelerinde arkadaş canlısı bir kişilik olarak görülme oranları, görülmeme oranlarının yaklaşık üç katı ve bu kişiler nadiren yalnız başlarına zaman geçiren kişiler olarak algılanıyorlar. Bu kişiler genellikle çevrelerinden oldukça saygı görüyor ve çoğunun gösterişli bir yaşam tarzı yok. Kısacası, suistimalci deyince insanların aklına gelen genel tanımlamalara uymayabiliyorlar.

Sonraki bölümde de göreceğimiz gibi, bir işbirlikçiden faydalanan suistimalciler, daha da güçlü kontrolleri atlatabilmeleri bakımından özellikle büyük bir tehdit oluşturuyorlar. Suistimalle mücadele mekanizmalarının sıkı olduğu şirketlerde, işbirliği yapan suistimalcilerin %16'sı bu sıkı kontrolleri atlatabilmiş veya suistimali kendi adına işlemesi için başka çalışanların aklını çelebilmiş.

Bu analiz, suistimalle mücadele kontrollerinin zayıf veya güçlü olması arasında hiçbir fark olmadığına yönelik görüşü desteklemiyor, hatta tam aksini destekliyor. Açık noktalara rağmen, bir suistimalin iç kontroller aracılığıyla tespit edildiği vakaların oranında artış gözlendi: 2013'te %68 olan bu oran 2015'te %72'ye yükseldi.

Ne tür mekanizmalar işbirliğini tespit edebildi? İşbirliğinin söz konusu olduğu 456 örneğin %52'si ihbarlar, diğer anonim bildirimler ve tedarikçilerin ya da müşterilerin şikayetleri sonucu tespit edildi. İç denetim gibi diğer yöntemler ise, muhtemelen şirketin bu tür bir fonksiyona yönelik yeterli kaynağa sahip olmaması (personel veya bütçe bakımından) veya iç denetim kontrollerinin rutin bir düzende yapılması ve suistimalcilerin de bunları iyi biliyor olması nedeniyle çok daha az etkili oldu. Kimliğini gizlemeden ve anonim bildirimde bulunanlar da, sınırsız yetkiye sahip suistimalcilerin tespit edilmesinde aynı derecede önem taşıyor.

KPMG Avustralya Suistimal Önleme ve İnceleme Hizmetleri Bölümü, Soruşturmalar Birimi Lideri Robin Tarr, "Bu durum, etkili bir ihbar hattı mekanizmasının ve tüm personeli bu mekanizmanın ne zaman, neden ve nasıl kullanılacağı konusunda eğitmenin önemine işaret ediyor" diyor. Ancak bu noktada, iç denetim gibi diğer suistimalle mücadele prosedürlerinin de güçlendirilmesi gerektiği unutulmamalı. Şirketler, farklı kontrol türlerinin etkin bir şekilde çalıştığından emin olmalılar.

Yalnız kurtlar ve sürü halinde avlanan suistimalciler

Pek çok kişinin gözünde, kurumsal suistimalciler, suçu işlemek için sadece kendi ustalıklarına ve kurnazlıklarına güvenen yalnız kurt imajı sergilerler. Oysa, ankete göre, gruplar halinde çalışan suistimalcilerin sayısı bu yalnız kurtların neredeyse iki katı. 2015 anketindeki suistimalcilerin %62'si bir veya birkaç kişiyle işbirliği yapmışken, 2010 anketinde bu oran %59 idi. İlginçtir, başkalarıyla işbirliği yapma konusunda bölgeler arasında belirgin farklılıklar var. İşbirliği özellikle Latin Amerika (%74) ile Ortadoğu ve Afrika ülkelerinde (%76) yaygın. KPMG Hollanda Suistimal Önleme ve İnceleme Hizmetleri Bölümü'nden Jack De Raad, "Suistimalciler, kontrolleri atlatmak için bir yardımcıya ihtiyaç duydukları veya gerekli bilgi, beceri ve yetki seviyelerine sahip olmadıkları için işbirliği yoluna gidiyorlar" diyor. Bunun aksine, Kuzey Amerika (%58) ve Okyanusya ülkelerinde (%65) suistimalcilerin büyük bir kısmının kendi başlarına hareket ettiğini belirledik.

İşbirliği yapanlar kimler? İşbirliği yapan kişiler, tek başına hareket eden suistimalcilere göre genellikle daha kıdemli ve şirkette daha uzun süredir çalışan kişiler. İş birliği yapanların %40'ı üst düzey yöneticiler ve direktörler iken, tek başına hareket edenlerde bu oran sadece %28. Ayrıca, işbirliği yapanların yalnızca %35'inin sadece şirket içi kişilerden oluşması da bir başka ilginç gerçek. Geri kalan kısım ya mağdur olan şirketin bir çalışanı değil ya da şirket dışından bir veya birkaç kişiyle işbirliği yapan bir şirket çalışanı.

KPMG ABD Üçüncü Taraf Risk Yönetimi Lideri Graham Murphy, "Bu durum şirketlerin işbirliği karşısında ne kadar savunmasız olduklarını ve kontrol mekanizmalarını özellikle tedarikçiler ile satış temsilcileri gibi üçüncü taraflarla olan ilişkiler üzerine odaklanarak tasarlamaları gerektiğini ortaya koyuyor" diyor. "Tedarikçiler, iş ortakları ve kurumsal müşteriler hakkında uygun seviyede durum tespitleri yapılmasını sağlayan güçlü bir üçüncü taraf risk yönetimi programı, üçüncü tarafların güvenlik incelemesine tabi tutulması ve gözetiminde kritik öneme sahip bir araç."

İşbirliği yapanlar, genellikle tek başına hareket edenlerden daha ağır hasarlar veriyorlar. İşbirliği yapmış suistimalcilerin %34'ü çalıştıkları şirketlere 1 milyon Amerikan Doları ve üzerinde zarar vermişken, tek başına çalışanlarda bu oran %16. İşbirliği yapanlar daha yüksek tutarda maddi kazanç sağlıyor, üstelik daha uzun bir süre boyunca tespit edilemiyorlar.

Bunların tespit edilme yöntemleri de daha farklı. Tek başına hareket edenler ağırlıklı olarak ya iç denetimle ya da tesadüfen, yönetim incelemesi sonucunda yakalanıyor. İşbirliği yapanlar

> "**Beş veya daha fazla işbirlikçiden oluşan grupların** tespit edilmesinde en etkili yöntem **kimliğini gizlemeden (%24) ve anonim bildirimler (%24)** oldu, bu da diğer tespit yöntemlerinin büyük işbirliği gruplarını tespit etmede etkisiz kalabileceğine işaret ediyor."

içinse temel tespit yöntemleri kimliğini gizlemeden yapılan bildirimler, yönetim incelemesi ve anonim bildirim oluyor. Beş veya daha fazla işbirlikçiden oluşan grupların tespit edilmesinde en etkili yöntem kimliğini gizlemeden (%24) ve anonim bildirimler (%24) oldu, bu da diğer tespit yöntemlerinin büyük işbirliği gruplarını tespit etmede etkisiz kalabileceğine işaret ediyor.

Tek başına hareket eden suistimalciler işbirliği yapanlara göre genellikle daha alt pozisyonlarda görev yapıyorlar. Zayıf

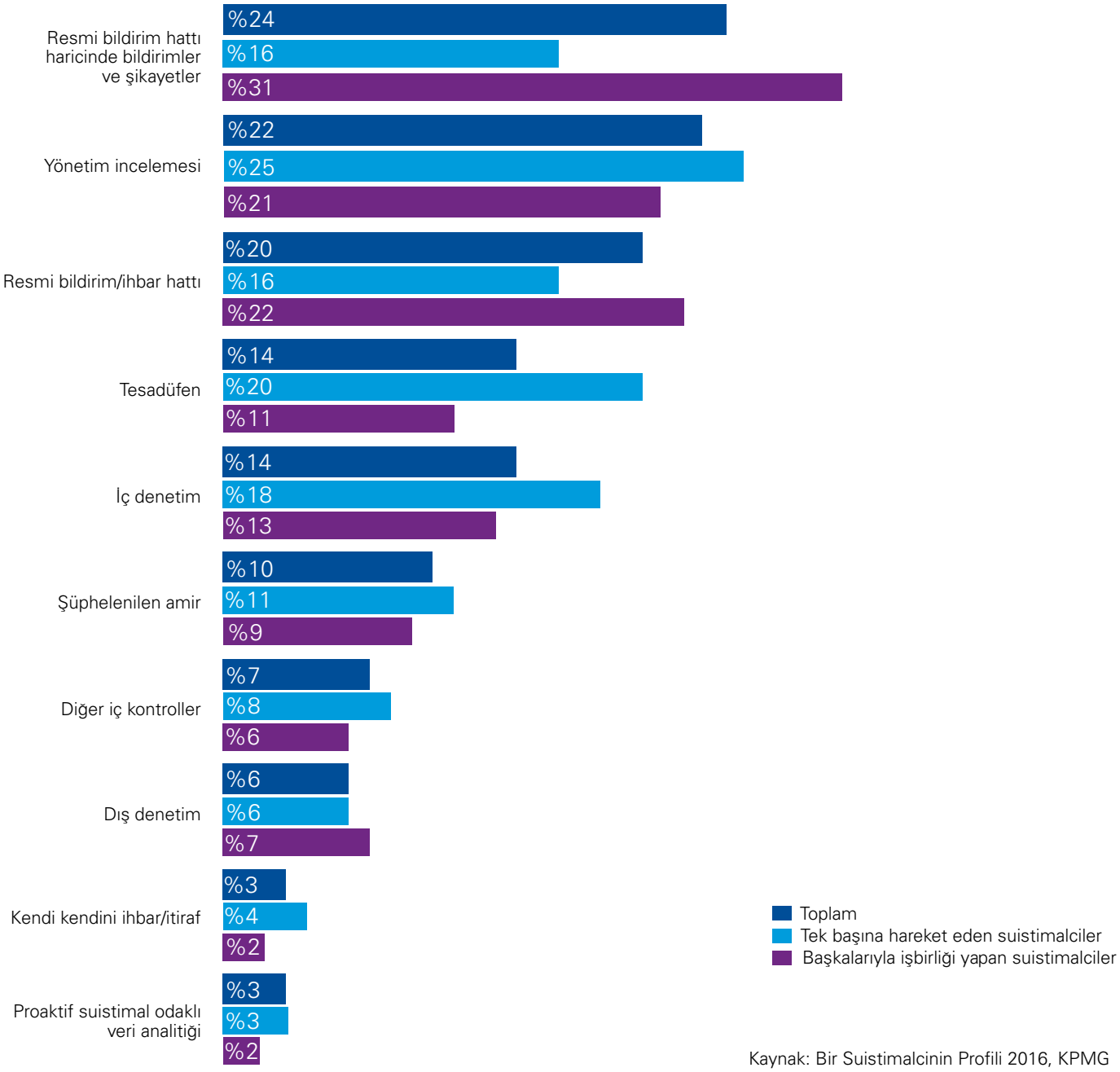
iç kontroller, işbirliği yapanlardan (%58) ziyade tek başına hareket edenler (%66) için önemli bir faktör. Bunun sonucu olarak, tek başına hareket edenlerin tesadüfen tespit edilme oranı işbirliği yapanlara kıyasla daha yüksek (sırasıyla %19 ve %10).

Cinsiyet karşılaştırmasına baktığımızda, işbirliği yapma konusunda erkekler ve kadınlar arasında önemli bir fark olduğunu görüyoruz. Erkekler işbirliği yapmaya kadınlardan daha meyilli (sırasıyla %66 ve %45). Ancak kadınlar da eskiye kıyasla daha fazla işbirliği yapıyorlar. Hem kadın hem erkeklerden oluşan işbirliği gruplarının 2010 yılında %34 olan oranı 2015 yılında %47'ye yükseldi.

Bu noktada, anket örnekleminde erkek sayısının kadın sayısının yaklaşık beş katı olduğu ve kadın suistimalcilerin kuruluşta erkeklerden daha alt pozisyonlarda olduğu da dikkat çekiyor. Kadınların yaş aralığı da daha düşük. 26-45 yaş arası erkeklerin oranı %50 iken aynı yaş aralığındaki kadın oranı %63. Ayrıca, maddi sıkıntı içinde olan kadınların oranı da erkeklerden fazla (tüm anket örneklemi içinde sırasıyla %14 ve %4).

Ancak zaman içinde, suistimal amaçlı eylemler konusunda cinsiyetler arasında görülen farklar, kadınların çalıştıkları şirketlerde yükselmeye başlamalarıyla birlikte giderek azalıyor. Yönetim seviyesindeki kadın suistimalcilerin 2010 yılında %28 olan oranı 2015 yılında %38'e yükseldi, ayrıca kadınların işbirliği yapma oranları da artıyor. KPMG İngiltere Rüşvet ve Yolsuzlukla Mücadele Lideri Annabel Reoch, "Suistimalcinin şirket içindeki seviyesi ne kadar yüksekse, başkalarını suça ortak olmaya ikna etme olasılığı da o kadar artıyor" diyor.

Suistimaller nasıl tespit edildi?



Kaynak: Bir Suistimalcinin Profili 2016, KPMG

Şirket içi suistimalciler ve şirket dışından kişiler

Tek başına hareket edenler ile işbirliği yapan suistimalciler karşılaştırıldığında önemli farklar ortaya çıkıyor. Aynı durum, şirket içinden işbirliği yapanlar ile şirket dışından işbirliği yapanların karşılaştırılması için de geçerli. Ancak bu noktada, analiz edilmesi gereken üç farklı grup olduğundan durum biraz daha karmaşık: tamamen şirket içindekiler (%35), tamamen şirket dışındakiler (%18) ve ikisinin karışımı (%43). KPMG Kanada Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı Stephan Drolet, "Şirketler, hem şirket içini hem de şirket dışını dikkate alan suistimalle mücadele mekanizmaları tasarlamak zorundalar. Üstelik, şirket içinden tek başına bir suistimalcinin, şirket dışından büyük bir grupla işbirliği yapabiliyor olması ihtimalini de göz önünde bulundurmaları gerekiyor. Yani şirketlerin tedbir alması gereken pek çok farklı permütasyon var" diyor.

Anket sonuçları arasındaki en ilginç tezatlardan biri de, sadece şirket içinden suistimalcilerin verdiği maddi zararın, sadece şirket dışından veya karışık grupların verdiği zarardan daha fazla olması. Birinci grubun gerçekleştirdiği suistimallerin yaklaşık %42'si en az 1 milyon Amerikan Doları maddi zarara yol açmışken, diğer iki grupta bu oran sırasıyla %32 ve %25. Sadece şirket içinden olan grubun, finansal raporlama suistimali yaptığı vakaların oranı (%35) şirket dışından veya karışık gruplara (%16) göre çok daha fazla.

Ayrıca, tespit yöntemi bakımından da belirgin farklar var. Kimliğini gizlemeden ve anonim bildirimler, karışık grupların tespitinde sadece şirket içinden gruplara göre daha yaygın tespit yöntemleri olarak (sırasıyla %49 ve %37) öne çıkıyor.

"Şirketler, hem şirket içini hem de şirket dışını dikkate alan suistimalle mücadele mekanizmaları tasarlamak zorundalar. Üstelik, şirket içinden tek başına bir suistimalcinin, şirket dışından büyük bir grupla işbirliği yapabiliyor olması ihtimalini de göz önünde bulundurmaları gerekiyor. Yani şirketlerin tedbir alması gereken pek çok farklı permütasyon var."

1 milyon Amerikan Doları ve üzerinde kayba yol açan suistimallerin oranı

Suistimallerin **%42** 'si tamamen içeriden suistimalciler tarafından gerçekleştirildi

Suistimallerin **%32** 'si içeriden ve dışarıdan suistimalci grupları tarafından gerçekleştirildi

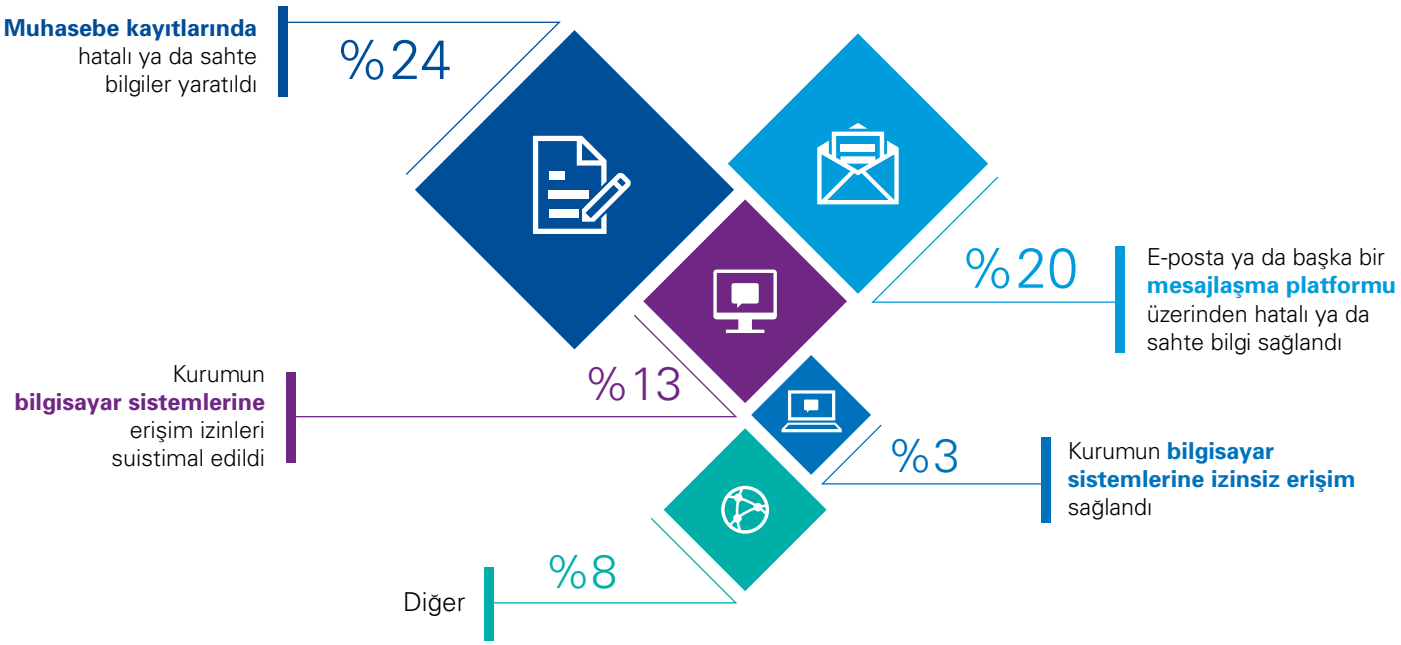
Suistimallerin **%25** 'i dışarıdan suistimalciler tarafından gerçekleştirildi

Teknoloji suistimalciler için hem araç hem de engel

Teknoloji adeta iki ucu keskin bir kılıç. Teknolojik ilerlemeler, şirketlerin suistimalle mücadele konusunda daha güçlü mekanizmalar geliştirebilmelerine yardımcı olurken suistimalciler için de içeri sızabilecekleri açıkları bulmada bir araç olabiliyor. Ancak anketimiz, teknolojinin suistimali tespit etmekten çok işlemek amacıyla kullanıldığını ortaya koyuyor. Suistimalcilerin %24'ü için teknoloji kolaylaştırıcı bir etken oldu.

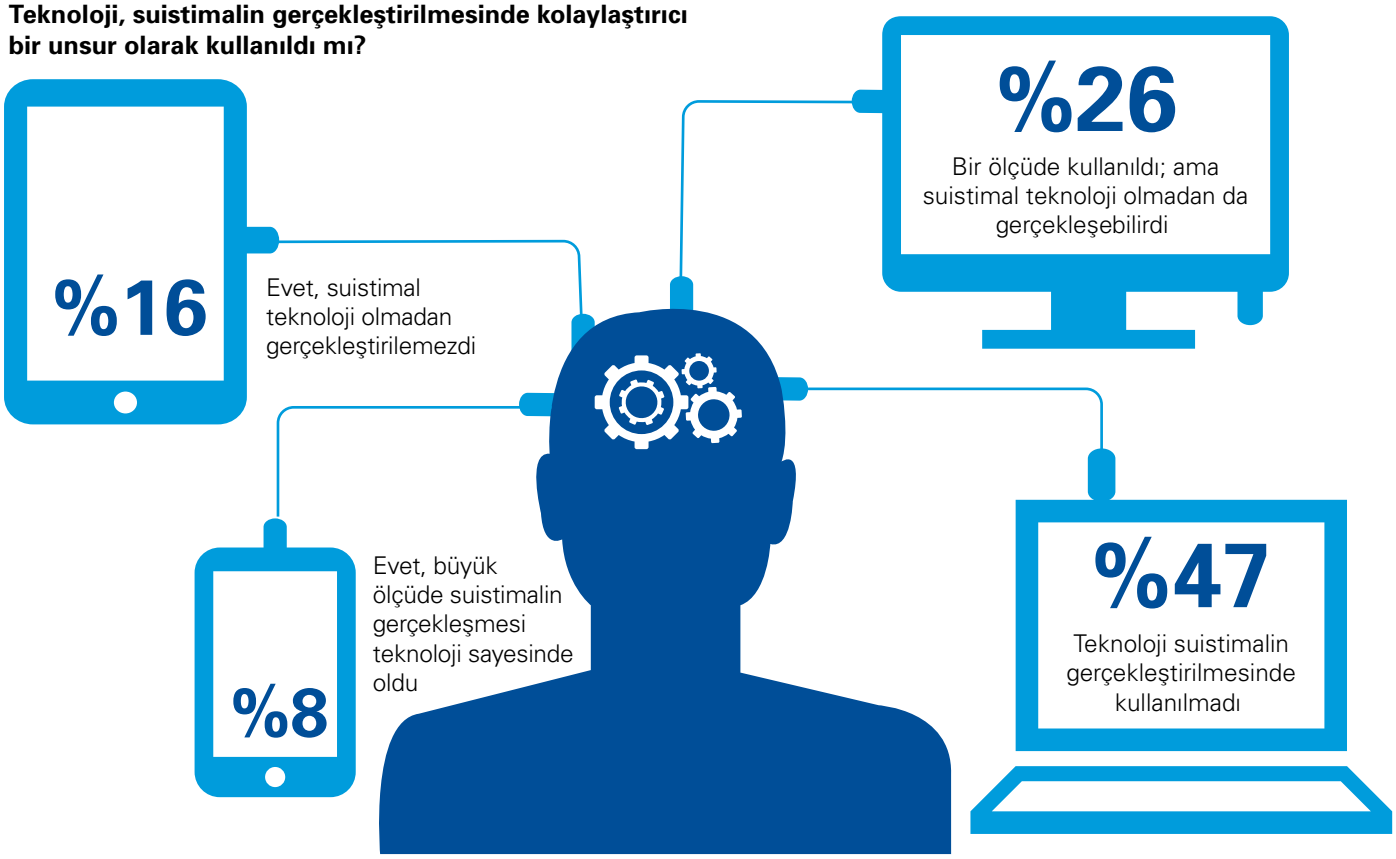
Teknolojiden faydalanılan suistimal örnekleri arasında gizli bilgilere elektronik yollardan izinsiz olarak bilgi teknolojileri altyapılarına erişmek ve yapılan suistimalin kamufle edilmesi amacıyla sahte muhasebe girişleri yapmak sayılabilir. İlginç bir şekilde, teknolojiden faydalanılan suistimallerde en düşük oran Avrupa'da (%18), en yüksek oran ise sırasıyla Okyanusya (%30), Kuzey Amerika (%29) ve Ortadoğu ile Afrika'da (%28) görüldü.

Suistimalin gerçekleşmesinde teknoloji nasıl kullanıldı?



Kaynak: Bir Suistimalcinin Profili 2016, KPMG

Teknoloji, suistimalin gerçekleştirilmesinde kolaylaştırıcı bir unsur olarak kullanıldı mı?



Kaynak: Bir Suistimalcinin Profili 2016, KPMG

Şirketlerin büyüklüğü ve coğrafi çeşitliliği dikkate alındığında, suistimalle mücadelede en önemli teknolojik araçlardan birinin veri analitiği olduğu görülüyor. Giderek daha fazla sayıda şirket, her gün gerçekleşen milyonlarca satış ve satın alma işlemi arasındaki olağan dışı işlemleri aramak için veri analitiği çözümleri kullanmaya başladı. Ancak görünüşe göre şirketler veri analitiğini tam anlamıyla uygulamaya almış değiller. Suistimallerin sadece %3'ü olağan dışı ve şüpheli faaliyetler içinde suistimal işlemlerini aramaya yönelik proaktif veri analitiği yoluyla tespit edildi.

Teknolojiden faydalanılan suistimallerde, suistimalci genellikle daha genç oluyor (%60'ı 26-45 yaş arasında kişiler). KPMG ABD Küresel Soruşturmalar Lideri Phil Ostwalt, "Daha yaşlı suistimalciler teknolojiden çok kişisel ilişkilerine güveniyorlar. Daha genç ve teknoloji meraklısı olan çalışanlar şirket içinde yükselmeye başladıkça, teknolojinin kullanıldığı suistimallerde de artış görülebilir" diyor. Teknolojiden faydalanan suistimalcilerin yaklaşık %24'ü en yaygın yakalama yöntemiyle yani tesadüfen yakalandı, teknolojiden faydalanılmayan suistimallerde ise bu oran %11. Bu da, şirketlerin teknolojiye bağlı suistimallerle mücadelede teknolojiyi daha güçlü bir şekilde kullanabileceklerinin bir başka kanıtı. Tesadüfen tespit, çoğu zaman mevcut kontrollerin etkisiz olduğunu acı bir şekilde hatırlatıyor.

"Teknoloji adeta iki ucu keskin bir kılıç. Teknolojik ilerlemeler, şirketlerin suistimalle mücadele konusunda daha güçlü mekanizmalar geliştirebilmelerine yardımcı olurken suistimalciler için de içeri sızabilecekleri açıkları bulmada bir araç olabiliyor."

Siber suistimal bir tehdit olarak kendini göstermeye devam ediyor

Tüm dünyadaki KPMG ofislerinin en sık bahsettiği yeni ve gelişen tehdit siber suistimal. Pek çok KPMG profesyoneli, şirketlerin aslında bu tehdidin farkında olduğunu ancak başlarına geleceğini düşünmediğini söylüyor. Bu nedenle çoğu zaman saldırıya uğradıklarından bile haberleri olmuyor, bu da olası tehditlere karşı hiç de hazırlıklı olmadıklarının bir göstergesi. KPMG ABD Siber Soruşturmalar Lideri Ron Plesco, "Yöneticiler aslında bilgisayar korsanlarının ve suç örgütlerinin şirketlere ne kadar büyük zarar verebileceklerinin farkındalar; neredeyse her gün medyada bu türden olayları okuyorlar. Ancak, söz konusu tehdit için çeşitli önlemler almış olsun veya olmasınlar, böyle bir şeyin günün birinde kendilerinin başına da gelebileceğine çoğu zaman inanmıyorlar" diyor.

KPMG anketinde sadece 31 siber suistimal faili yer alsa da, bu buz dağının sadece görünen yüzü olabilir. Tespit edilememiş pek çok vaka olabilir. Ne de olsa siber güvenlik daha birkaç yıldır kamuoyunun gündemine geldi, oysa çok daha uzun bir süredir fark edilmeksizin gerçekleşiyordu.

750 vakalık örneklem içinde 31 vaka küçük bir rakam gibi görünse de, sonuçlar yine de ilginç. Bunların büyük bir kısmı (13 kişi), mağdur şirketin genellikle dışarıdan suç ortaklarıyla işbirliği yapan çalışanları. Dokuzu organize suç gruplarıyla ilişkili, yedisi ise tamamen şirket dışından bireysel bilgisayar korsanları.

Anket, siber suistimallerin başlıca amacının kişisel bilgiler, fikri mülkiyet ve üst düzey yöneticilerin e-postalarını çalmak, şirket verilerine stratejik erişim sağlamak ve DoS saldırılarına yol açmak olduğunu ortaya koyuyor. ABD Federal Soruşturma Bürosu (FBI), "iş e-postası suçlarında" ciddi bir artış olduğunu ve tüm dünyada 12.000'den fazla kişinin bundan mağdur olduğunu belirtiyor.[1] Bu suç türünde, suistimalci kişi bir şirket çalışanına üst düzey bir yönetici tarafından gönderilmiş süsü verilen bir e-posta göndererek o çalışana yurt dışındaki bir banka hesabına para göndermesi talimatını veriyor. FBI, şirketlerin 2013-2015 arasında bu yolla 1,2 milyar ABD Doları civarında zarara uğradıklarını belirtiyor.

KPMG Kanada Siber Suçlarla Mücadele Ülke Başkanı Kevvie Fowler, "Pek çok şirket siber suçlarla mücadele edebilecek becerilere sahip değil, bu nedenle güçlü iç kontrollere ve veri analitiğine ihtiyaçları var. Şirketler ayrıca, hızla değişen tehdit ortamı hakkında güncel bilgilere sahip olmak için birbirleriyle sürekli bilgi ve fikir alışverişinde bulunmak zorunda" diyor.

1 http://www.ic3.gov/media/2015/150827-1.aspx

> Yöneticiler aslında bilgisayar korsanlarının ve suç örgütlerinin şirketlere ne kadar büyük zarar verebileceklerinin farkındalar; neredeyse her gün medyada bu türden olayları okuyorlar. Ancak, söz konusu tehdit için çeşitli önlemler almış olsun veya olmasınlar, böyle bir şeyin günün birinde kendilerinin başına da gelebileceğine çoğu zaman inanmıyorlar.

Suistimalle nasıl mücadele edilmeli?

Bu rapor, tüm dünyadan KPMG soruşturma uzmanlarının 750 suistimalciyle ilgili bir ankete verdikleri yanıtlardan ortaya çıkan temel bulguları ortaya koyuyor. Şirketlerin yanıt bulması gereken en önemli soru, "Suistimalcilerle nasıl mücadele etmeliyiz?" sorusu. Verileri analiz ettiğimizde dört temel öneri ortaya çıkıyor:

Teknolojiyle karşılık verin — Anketimiz, çok sayıda suistimalcinin, suistimal girişiminde bulunmak amacıyla teknolojiden faydalandığını ortaya koyuyor. Ancak, şirketlerin de suistimalcilerle mücadelede teknolojiden faydalandığına dair çok az somut örnek bulabildik. KPMG firmaları, şirketlerin dikkatli bir fayda/maliyet analizi yaparak suistimalle mücadeleye yönelik analitik çözümler benimsemesini öneriyor. Yani ateşe ateşle karşılık vermeliler. Tehdit izleme sistemlerinin ve veri analitiğinin kullanımı giderek yaygınlaşıyor ve bu araçlar kişisel davranışları izleyerek ve bilgisayar kullanımını, resmi kayıtları ve sosyal medyayı analiz ederek normal olmayan veya şüpheli davranışları ortaya çıkarabiliyor.

Şirketler, veri analitiğinin ve biriktirdikleri devasa miktarda veriyi derinlemesine inceleme gücünün sunacağı avantajlardan faydalanma konusunda genellikle istekliler. Ancak çoğu zaman, mevcut sistemlerine iyi entegre edilemeyen ve neticede "çöpe atılan", piyasada hazır bulunan standart çözümleri satın alıyorlar. Oysa, şirketin önemli gözetim ve tespit ihtiyaçlarının büyük bir kısmına etkin yanıt verebilecek kapsamlı ve özelleştirilmiş çözümlere yönelmeleri gerekiyor. Hatta mevcut sistemlerinde bile bazı yazılım bazlı çözümler bulunuyor olabilir. Veya verilerini üçüncü taraf bir hizmet sağlayıcıya gönderebilirler. Seçenek ne olursa olsun, gözü tüm dünyada her saniye gerçekleştirilen işlemlerin üzerinde olacak otomatikleştirilmiş bilgisayar programları aracılığıyla gözetim ve denetim gerçekleştirmek uzun vadede etkili olabilir.

Tetikte olun ve riskleri düzenli olarak değerlendirin — İş dünyası sürekli büyüyor ve suistimalciler de sürekli olarak, sistemi kötüye kullanmak için yapılan değişikliklerden faydalanmaya çalışıyor. Yeni düzenlemeler, yeni pazarlar ve elbette yeni teknolojiler, kontrolleri atlatma konusunda suistimalcilere sürekli yeni fırsatlar sunuyor. Şirketler bu değişim hızına nasıl ayak uydurabilirler? Yeni gelişen suistimal risklerine karşı en etkili savunma mekanizmalarından biri de, tüm şirketi kapsayan bir risk değerlendirme süreci kapsamında düzenli olarak suistimal risk değerlendirmesi yapmak. Bu tür formel değerlendirmeler her yıl yapılmalı ve şirketin yasal ortamı ile operasyonlarında meydana gelebilecek değişiklikler dikkate alınarak gerektiğinde daha sık güncellenmeli. Özellikle şirketin risk, operasyonlar, mevzuat uyum, hukuk ve diğer konularda pek çok profesyonelle çalıştığı durumlarda, ilk adım olarak tüm şirket ortamının bir stres testine (faaliyet temelli kontroller ve işletme düzeyindeki kontroller bakımından) tabi tutulması akıllı bir girişim olacaktır.

Şirketin tercihine bağlı olarak siber güvenlik değerlendirmeleri ayrı olarak da yapılabilir, ama sonuçta mutlaka genel suistimal riski değerlendirmesine entegre edilmelidir. Siber güvenlik alanındaki değişimin hızı dikkate alındığında, özellikle aynı sektörde faaliyet gösteren ve benzer tehditlerle karşı karşıya olan diğer

Tavsiyeler:

Tetikte olun ve riskleri düzenli olarak değerlendirin

Teknolojiyle karşılık verin

İş ortaklarınızı ve üçüncü tarafları iyi tanıyın

İç tehditlere karşı uyanık olun

Kaynak: Bir Suistimalcinin Profili 2016, KPMG

şirketlerle deneyim paylaşımı yapılması da son derece faydalı olacaktır.

İş ortaklarınızı ve üçüncü tarafları iyi tanıyın — Şirketler söz konusu suistimal olduğunda sadece kendi içlerine odaklanmamalı, iş ortaklarını ve kendileri adına iş yapan üçüncü tarafları da yakın gözetim altında tutmalılar. Şirketler dünya geneline yayıldıkça, kendileri adına distribütör, satış acentesi ve yerel ülke temsilcisi olarak hareket eden üçüncü taraflarla da daha fazla çalışmaya başlıyorlar. Bu tür bir üçüncü tarafla çalışmaya başlamadan önce risk temelli bir durum tespiti yapmak hem bir en iyi uygulama niteliğindedir hem de pek çok uyum programının temelidir.

Şirketler ayrıca, tedarikçilerin kendilerine sözleşmeye uygun bir şekilde fatura kestiğini düzenli olarak gözden geçirmeli ve bu tür sözleşmelerde genellikle bulunan "denetim yapma hakkı" maddesini mutlaka kullanmalılar. Teknoloji, şirketlerin bir tedarikçi hakkında yalnızca sözleşme imzalanmadan önce değil, sonrasında da tedarikçinin sözleşmeden doğan yükümlülüklerini yerine getirip getirmediğini denetlemek için düşük maliyetli bir durum tespiti yapmasına imkan tanıyor.

İç tehditlere karşı uyanık olun — Anketimizde sürekli karşılaşılan şaşırtıcı sonuç, şirketlerde 6 yıldan uzun süredir çalışmakta olan üst düzey yönetici suistimalcilerin sayısı oldu. Çok sık olarak bu tarz bir davranışta bulunacak son kişi olacaklarının beklendiğini duyuyoruz. Fakat çoğu zaman belirtiler vardır. Suistimalciler hata yapabilir. Eğer bir şeyler doğru görünmüyorsa, durun, ara verin ve düşünün. Çalışanların suistimal risklerinin farkında oldukları ve nasıl cevap vereceklerini anladıkları bir toplum geliştirmek oldukça önemlidir. Çalışanları, şirketin yardım hattı gibi raporlama mekanizmalarını kullanmaları için cesaretlendirin ve eğitin. Personellerin olumsuz bir bulgu ile karşılaştıklarında işleri için endişelenmeyecekleri bir güven ortamı yaratın. Alarm sesi duyulduğunda, eylemi sorgulamak ve soruşturmak için uygun aksiyonları alın. Elbette sadece bu adımlar suistimalcileri durdurmaya yetmez; suistimal, onu uzak tutmak için bir risk farkındalığı kültürü gerektiren, yakalaması zor ve sinsi bir düşmandır. Tüm çalışanlar ve iş ortakları uyanık davrandığında ve işlerini dürüst bir şekilde yaptıklarında suistimal tehlikesi dinecektir. Bu, uğruna çabalamaya değecek bir amaç.

Metodoloji

Çalışmamız, tüm dünyadaki KPMG suistimal önleme ve inceleme profesyonellerine, Mart 2013-Ağustos 2015 arasında soruşturdukları suistimalcilerle ilgili bilgilerin sorulduğu bir ankete dayanıyor. Bu profesyoneller, mağdur şirketin daveti üzerine vakayı soruşturduktan sonra her bir suistimalci hakkında detaylı bir anket formu doldurdular. Soruşturma sıklıkla suistimalciyle görüşme yapılmasını da içerdiğinden, KPMG hem failin hem de işlediği suçun detaylı bir profilini çıkarmasına yardımcı oldu. Bu rapor ise, suistimal vakalarının değil, soruşturulan bu 750 suistimalcinin bir analizine dayanıyor (bazı vakalarda birden fazla suistimalci bulunuyordu). 2010 yılında 348 olan suistimalci sayısı 2013 yılında 596'ya yükseldi. 2015 anketindeki suistimal vakaları, 81 ülkede (Porto Riko ve Hong Kong dahil) gerçekleşti.

*Belirtilen oranlar, yuvarlamalar nedeniyle %1 farklılık gösterebilir.

Katkıda bulunanlar

Masako Asaka
Jagvinder Brar
Sandra Cusato
Nick D'Ambrosio
Matt Dixon
Laura Dobrotka
Stephan Drolet
Déan Friedman
Renee Gooden
Matt Hansen
Shelley Hayes
Jimmy Helm
Muhammad Hoosain
Tom Keegan
Victoria Malloy
Jack Martin
Kemi Okhumale
Kajen Subramoney
Daniel Viray
Tracey Walker
Estelle Wickham

İletişim:

İdil Gürdil
Suistimal Önleme ve İnceleme
Hizmetleri Lideri, Risk Yönetimi
Danışmanlığı, Şirket Ortağı
KPMG Türkiye
T: +90 216 681 90 00
E: igurdil@kpmg.com

İstanbul
Rüzgarlıbahçe Mah. Kavak Sokak No:29
Kavacık 34805 Beykoz / İstanbul / Türkiye
T: +90 216 681 90 00

Ankara
The Paragon İş Merkezi Kızılırmak Mah.
Ufuk Üniversitesi Cad. 1445 Sokak No:2 Kat:13
Çukurambar 06550 Ankara / Türkiye
T: +90 312 491 72 31

İzmir
Heris Tower, Akdeniz Mah. Şehit Fethi Bey Cad.
No:55 Kat:21 Alsancak 35210 İzmir / Türkiye
T: +90 232 464 20 45

kpmg.com.tr