Siber güvenlik: CEO'ların öngörü yanılgısı

KPMG Türkiye

kpmg.com.tr

Önsöz

Şirketlerin ve bireylerin dijital dünyaya doğru çıktıkları yolculuk ile kritik altyapılar siber dünya ile bütünleşik bir hal alıyor.

Bu yolculuk, fırsatların yanında pek çok siber riski de beraberinde getiriyor. Dijital veri hacminin her geçen gün artması, verilerin kıymetli bilgi formlarına hızla dönüşmesi, internetin hayatımızın vazgeçilmez bir parçası olması gibi birçok sebep bizim ülkemizde de siber güvenlik konusunu önemli gündem maddelerinden birisi haline getiriyor. Tehditlerin sanal olarak belirdiği ancak oluşturduğu zararın gerçek olduğu saldırıların sayısı arttıkça siber saldırılarla mücadeleye yönelik çalışmalara ağırlık veriliyor.

Geçtiğimiz yılın son çeyreğinde Türkiye olarak sıkça karşı karşıya kaldığımız siber saldırıların önümüzdeki dönemlerde de ciddi ekonomik ve sosyal sonuçlar doğuracağı tahmin ediliyor. Başta bankacılık, iletişim ve e-ticaret olmak üzere Türkiye teknoloji kullanımı alanında ileri bir noktaya ulaştı. Ama teknoloji kullanımının beraberinde getirdiği risklere baktığımızda, bu raporda yer verilen oranlardan çok da iyi olduğumuz söylenemez.

Siber saldırıların bilinen ve belirlenmiş herhangi bir stratejisinin olmaması ve her türlü zafiyetten faydalanılması eğilimi ile büyük, orta veya küçük ölçekte her şirket siber risk taşıyor. Bu nedenle siber saldırılarla mücadele konusunda süreç yaklaşımı ihtiyacı öne çıkıyor. Yalnızca bireylerin değil şirketlerin ve hatta ülkelerin de siber tehditlere yönelik birlikte hareket etmesi ile anlam kazanacağı anlaşılmalıdır.

Siber güvenlik alanında birlikte çalışmalar yürütmenin, birikim ve tecrübelerin bir araya getirilerek güç birliği oluşturmanın önemini anlatmak amacıyla KPMG, küresel olarak bu stratejik riske yaklaşımları içeren bir çalışma gerçekleştirdi.

İyi okumalar dilerim,

Tanıl Durkaya
BT Danışmanlığı, Şirket Ortağı

Küresel CEO'lar, risk ile ödül arasındaki ince çizgide yürüyor

Bir petrol ve gaz şirketinin üst düzey yöneticisi, kızının geçen haftaki futbol maçında attığı golün fotoğrafını içeren bir e-postaya tıklar. İki yıl sonra bu yönetici, söz konusu fotoğrafın bir saldırganın klavyeden girilen tüm karakterleri (gönderilen e-postalar da dahil) kaydeden kötü amaçlı bir program içerdiğini öğrenir. Siber korsanlar ekran görüntülerini düzenli olarak kaydetmiş, bilgisayar kamerasını ve mikrofonunu açmış ve üst düzey yöneticilerin birbirleriyle neler konuştuklarını öğrenmiştir. Ne tesadüftür ki, şirket bu süre boyunca petrol imtiyazlarıyla ilgili pek çok ihaleye girip hep kılpayı kaybetmiştir.

Bir ev izleme sistemleri üreticisi, müşterilerin çok işine yarayacak yeni bir özelliğin reklamını yapar: Termostatınızı, lambalarınızı ve güvenlik sisteminizi akıllı telefonunuzdan kumanda edebilmek! Ancak bu sistem, yerel bir hırsızlık çetesinin sisteme sızarak eve kolayca girebilmesine imkan tanıyacak kadar basit ve korumasızdır. Oysa bu sistemin güvenlik mekanizmasında ve oturum açma ilkelerinde yapılacak basit bir değişiklik bu tür ihlalleri önleyebilirdi.

Bir perakende şirketi, uluslararası bir hacker şebekesinin, mağazalarında kredi kartları veya banka kartlarıyla yapılan her satış işleminin bilgisini aylardır sessizce çektiğini kötü bir tecrübeyle öğrenir. Yönetim kurulu ve üst düzey yöneticiler bu durumu devletin soruşturma görevlileri aracılığıyla öğrenir ve haber şirketin konu hakkında gerekenleri yapabilmesinden önce kamuoyunda hızla yayılır. Satışlar dibe vurur, şirket toplu davalarla karşılaşır ve CEO istifa eder.

Daha etkili korunma yöntemlerine başvurmak bu olayların hepsini engellemekte elbette yardımcı olabilirdi ancak maalesef yeterli olmazdı. Ürünleri ve süreçleri korumak için daha etkili güvenlik tedbirleri uygulamak önemli olsa da, saldırganın kim olduğu hakkında daha fazla bilgi edinmek ve tespit edilen tehditleri ortadan kaldırmaya yönelik bir plana sahip olmak daha da önemlidir.

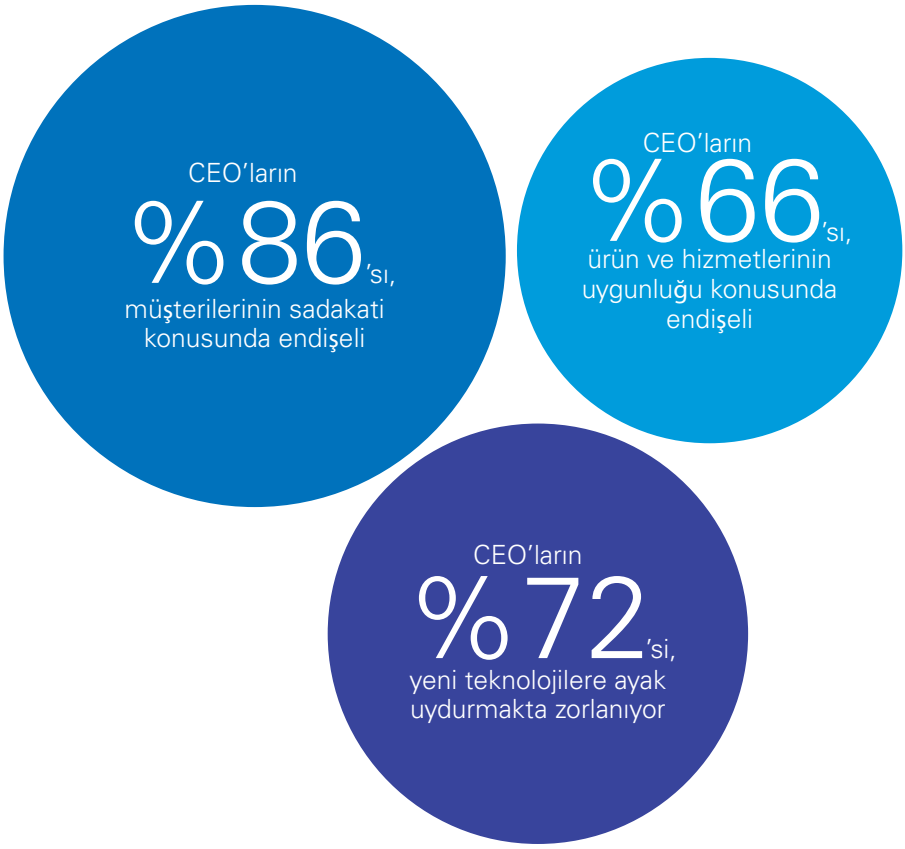
Günümüzde teknoloji, on yıl kadar önce kimsenin tahmin bile edemeyeceği yollar aracılığıyla şirketlerin müşterileriyle bağlantı kurabilmelerini sağlıyor: Akıllı cihazlar, kişiselleştirilmiş pazarlama kampanyaları ve ürünler, otomatik hale gelmiş hizmetlerin yanı sıra daha anlık ve kişiselleştirilmiş hizmetler. Bunların hepsini ve daha fazlasını artık cebimizde taşıdığımız akıllı cihazlar ile yapıyoruz. Bankalar bile artık cebimizde.

Ancak yeniliği hayata geçirme becerisi güvenliğin önünde gidiyor. Ve maalesef kötü niyetli kişiler inovasyon konusunda uzman. Dünyanın en yaratıcı "pazarlarından" biri de, organize suçu ve belki de herkesten daha başarılı yer altı bilgisayar korsanlarını destekleyen "Karanlık Ağ". Her gün yeni araçlar, yeni saldırı tipleri ve yeni nakde çevirme stratejileri geliştirilip paylaşılıyor. Her şey değişiyor: Uzmanlık, riskler ve etkileri.

CEO'ların uykusunu kaçıran şeyler

Müşteri verileri, fikri mülkiyet verileri ya da şirketi yönetmek için gereken veriler gibi, verileri korumak artık pek çok işletme için "sonradan akla gelen" bir konu değil. KPMG dünyanın en büyük ve en karmaşık şirketlerinde görev yapan 1.200'den fazla İcra Kurulu Başkanı ile yaptığı ankette onların uykularını kaçıran konuları ortaya çıkardı: Katılımcıların üçte ikisi ürün ve hizmetlerinin uygunluğu konusunda endişeliyken, dörtte üçü yeni teknolojilere ayak uydurmakta zorlanıyor ve neredeyse tamamı müşteri sadakati konusunda endişeli. [1] Siber güvenlik, müşteri sadakatiyle, güvenle ve yenilikçilik ile yakından bağlantılı. Yaşanabilecek bir ihlal müşteri güvenini kökünden zedeleyebiliyor ve markanın itibarına ağır darbe vurabiliyor.

KPMG Siber Güvenlik Hizmetleri Küresel Başkanı Malcolm Marshall, "Ürün ve süreçlere etkin bir siber güvenlik seviyesi sağlanması önemli bir rekabet avantajı yaratabilir" diyerek ekliyor: "Bazı işletmeler güvenliği, parmak izi tanıma özelliğine sahip bir satış noktasına dönüştürüyor. Örneğin bankalar, hantal güvenlik süreçlerini parmak izi tanıma özelliği ile değiştirmeye başladı. Personelinizin ve müşterilerinizin kimliğini en doğru şekilde tanımlayabilirseniz çok daha güvenli ve kişiselleştirilmiş hizmetler sunabilirsiniz."



Kaynak: 2015 KPMG CEO Araştırması, Mayıs 2015.

[1] Anketin metodolojisini raporun sonunda bulabilirsiniz.

Her şirket aslında bir siber şirket

Bir işletmenin yapabileceği en büyük hatalardan biri, siber güvenliği sadece CIO'nun alanına giren bir konu olarak görmektir. Marshall bu konuda, "Elbette CIO çok önemli bir role sahip ancak giderek daha fazla sayıda işletmenin müşteriyle iletişim kanalı olarak dijital ortamdan faydalandığı günümüzde işletmeler her zaman gerçek siber güvenlik uzmanlarıyla çalışmayabiliyor" diyerek ekliyor: "Pek çok üst düzey yönetici, ürünlerine entegre edilmiş teknoloji seviyesinin farkında bile değil. Hatta bunların çoğu, siber suçluların, şirketin sunduğu ürün ve hizmetleri kötüye kullanabilecek yaratıcı ve dahiyane yöntemlere sahip olduğundan bile habersiz."

Siber suçlar klasik suçlar kadar iyi anlaşılamadı. Oysa bu suçlar ürünün saygınlığı ve itibarıyla ilgili olduğundan yönetim kurulunu doğrudan ilgilendiriyor. Örneğin kurumsal yatırımcılar, geçmişte önemli bir siber güvenlik ihlali yaşamış bir şirkete yatırım yapma konusunda daha isteksiz olabiliyor. Bu da şirketin hem hisse fiyatlarını hem de sermaye temin edebilme kapasitesini olumsuz etkiliyor.

Kısacası: Her şirket artık bir siber şirkettir ve güvenlik konusunda her zaman uyanık olmak zorundadır.

> "Kabul edelim ki siber zayıflıklar konusunda hepimiz ayakta uyuduk! Ürün ve hizmetler için gereken güvenlik tedbirlerini almak konusundaki eksikliklerimizden gerekli dersleri çıkarmadık."
>
> — Malcolm Marshall
> KPMG Siber Güvenlik Hizmetleri Küresel Başkanı

Siber güvenlik: Stratejik bir risk

Yönetim kurulu üyeleri ve üst düzey yöneticiler, siber güvenliği stratejik bir konu olarak değil taktik bir sorun olarak görüyorlardı. Bununla birlikte, siber güvenliğin kurumsal çapta bir risk arz edebileceği geçtiğimiz on yıl içinde daha iyi anlaşıldı.

Anketimize katılan CEO'ların yaklaşık üçte biri, siber güvenliğin, şirketlerini şu anda en çok etkileyen sorun olduğunu belirtti. Her beş CEO'dan biri ise, bilgi güvenliğinin en çok endişe duydukları konu olduğunu ifade etti. Operasyonel riskler ve uyum riskleri de diğer başlıca riskler arasında gösterildi. Siber risk, kontrol altına alınamadığı takdirde hızla operasyonel veya yasal bir sorun haline gelebilir.

Kaynak: 2015 KPMG CEO Araştırması, Mayıs 2015.

KPMG ABD Siber Güvenlik Başkanı Greg Bell, "İhlaller zaman içerisinde şöyle bir soruna dönüşebilir: Bir siber sorunla ilgilendiğimden asıl işime odaklanamıyorum" diyerek ekliyor: "Veya bir siber sorunu çözmeye veya düzeltmeye çalışırken asıl işime ara vermem gerekiyor, bu durumda da pek çok karmaşık mevzuat sorunuyla ve hatta davalarla karşılaşabiliyorum."

Siber risk konusunda bir strateji çerçevesi oluşturmak

Yasal, itibar ve düzenleyici ortam riskleri tüm şirketler için birer endişe kaynağı. Fiziksel bir altyapıya sahip şirketler içinse bu riskler katlanarak artıyor. Bir saldırı tüm kontrol mekanizmalarını karıştırabilir, işletmenin donanımlarını kullanılamaz hale getirebilir, faaliyetlerini aksatabilir ve likidite riski yaratabilir. Son yıllarda devletlere ait petrol ve gaz şirketlerine yapılan saldırılar, enerji ve sanayi sektöründeki tüm işletmeler için adeta bir "uyanış çağrısı" oldu. Zira arkasında devlet desteği ve bolca kredi imkanı olmayan şirketler benzer saldırılara maruz kalsalardı ciddi likidite sorunları yaşayabilirlerdi.

Marshall bu konuda, "Pek çok şirket kurumsal riski değerlendirme konusunda belli bir çerçeveye sahip olsa da, siber risk hâlâ diğer risklerden farklı ele alınıyor. Oysa bu çok yanlış" diyor.

Örneğin üçüncü taraf riskini ele alalım. Başta bankalar olmak üzere pek çok şirket, üçüncü taraf risklerini zaten yıllardır dikkate alıyor. Bunlardan bazıları, pek çok tedarikçiyle çalıştığından tedarikçilerden birinin yaşayabileceği sorunlara karşı dayanıklı. Ancak konu daha derinlemesine incelendiğinde, bu tür "makul" bir riskin, farklı tedarikçilerin tek bir tedarikçiye bağımlı olması sonunda "dördüncü taraf riski" olarak adlandırılabilecek yeni bir riskle karşılaşabilir. Bu genellikle likidite riskinin değerlendirilmesinde ortaya çıkan bir risk ise de, siber dayanıklılık konusunda da aynı risk mevcut olabilir. Örneğin, tedarikçilerinizin tamamı aynı bulut hizmetleri sağlayıcısına güveniyor olsa ne olurdu?

Marshall bu konuda, "Her işletme, siber güvenliği analiz etmeye yönelik bir yapıya sahip olmalı ve bu yapı tercihen işletmenin mevcut kurumsal risk yönetimi yapısına entegre edilmeli" diyor. Bu noktada işletmelerin kullanabileceği çeşitli çerçeveler söz konusu: NIST'in ABD'de yayımladığı *Kritik Altyapıların Siber Güvenliğini Geliştirme Çerçevesi* veya Birleşik Krallık'ta yayımlanan *Siber Güvenliğin Esasları* ya da tüm dünyada en çok kabul görmüş çerçeve olan uluslararası ISO27001 standardı. Marshall, "Hangi çerçevenin seçileceği, seçilen çerçevenin nasıl entegre edilip uygulandığından çok daha az öneme sahip" diyerek ekliyor: "Önemli olan, seçilen çerçeveyi işletme bünyesindeki risk yönetiminin ana unsurlarından biri olarak benimsemek."

Düşmanınızı tanıyın

Bu süreçte atılması gereken ilk adım, kimin, işletmenin hangi kısmına, neden saldırabileceğini anlamaktır. Kısacası düşmanınızı tanımanız gerekir (güvenlik istihbaratıyla ilgili 9. sayfaya bakınız). Oluşturulacak strateji, işletmenin hangi varlıklarının en çok korunmaya ihtiyacı olduğunun ve olası bir saldırıda alınabilecek en büyük hasarın ne olabileceğinin anlaşılmasına yardımcı olacaktır. Marshall bu konuda da, "Bu, yatırımın ve koruma tedbirlerinin işletmeye en büyük zararı verebilecek alanlara odaklanmasına yardımcı olabilir" diyor.

Örneğin fikri mülkiyet, örneğin pek çok teknoloji şirketi için altın değerinde. Peki ya bir şirket bir ülkede ürün tasarımı, başka bir ülkede yazılım geliştirme ve dünyanın bambaşka bir noktasındaki üçüncü bir ülkede bulunan tedarikçilerle donanım tasarımı faaliyetleri yürütüyorsa? Bir senaryo geliştirecek olursak bu tür bir şirketin yönetim kurulu, fikri mülkiyet konusunu "sürekli endişe kaynağı arz eden" bir risk olarak tanımladı. Bu şirketin yönetim kurulu, yetkisiz bir kişinin fikri mülkiyete erişim sağlaması, yeni çıkarılacak bir ürünle ilgili planları öğrenmesi veya fikri mülkiyeti kopyalaması halinde şirketin varlığının bile tehlikeye girebileceğine karar verdi.

Şirketin zayıf noktasının, en kârlı ürünü en yüksek hacimle üreten bir tesis olduğu belirlendi. Şirketin bir danışmanı tarafından kiralanan iyi niyetli bir siber korsanı, üretim bölümündeki tüm sistemlere yaklaşık 30 saniye içinde erişebildi. Bu bilgisayar korsanı, siber güvenlik açısından, fikri mülkiyet dahil olmak üzere her şeyin kontrolünü ele geçirdi. Ayrıca, nispeten orta seviyede yeteneklere sahip başka bir siber korsanı, kalite güvence programlarından üretim sürecine kadar her sunucuyu ele geçirmeyi başardı. Bu sonuç CIO'yu pek de şaşırtmadı. Çünkü daha önce bu açıklar hakkında üretim ekipleriyle işbirliği yapmaya çalışmış ancak üretim ekipleri faaliyetlerin aksayacağı endişesiyle bu güvenlik kontrollerine sıcak bakmamıştı.

Zayıflıklar, fikri mülkiyet hırsızlığı riskinin yanı sıra, şirketin en kârlı ürünü için uygulanan kalite güvencesi programının da güvenilirliğini ortadan kaldırıyordu. Kalite güvencesi üzerindeki kontrolü kaybetmiş bir şirket ise, aleyhine açılabilecek olası bir toplu davada çok zor bir durumla karşılaşabilirdi.

Çoğu zaman gözden kaçırılan bir başka risk de, şirket birleşmeleri ve satın almalarında yaşanıyor. Bazı işletmeler, güvenliği ürünlerine yeterince entegre etmemiş bir şirketi satın almanın ne kadar olumsuz sonuçlar doğurabileceğini ancak yaşayınca anlayabiliyor. Kısa süre önce yaşanan bir olayda, bir şirketin, satın aldığı bir şirketle ilgili siber güvenlik zayıflıklarını düzeltmek için yaptığı harcamalar o şirketi satın alma bedelinin %25'ine varmıştı. Araçlarda kullanılacak bir ürün için siber güvenliğin ne kadar kritik olduğu hususu atlandığından, satın alan şirketin yaptığı durum tespiti mevcut zayıflıkları ortaya çıkaramamıştı.

Hazır mısınız?

Ankete katılan CEO'ların yarısı, gelecekte yaşanabilecek bir siber olaya tam olarak hazırlıklı olduğunu belirtti. Bununla birlikte anket, CEO'ların sadece yarısının bir siber güvenlik yöneticisi veya ekibi görevlendirdiğini ve yarısından azının veri paylaşımı gibi bazı dahili süreçlerde değişiklik yaptığını ortaya koydu.

Daha da şaşırtıcı olan ise, işletmelerin sadece üçte biri veri paylaşımı ve hareket işleme gibi dahili süreçlerde gerekli değişiklikleri yapmıştı. Siber korsanlar, büyük işletmelerin küçük tedarikçilerine ve hizmet sağlayıcılarına kötü amaçlı yazılımlarla sızarak aslında o büyük işletmelerin sağlam güvenlik sistemlerini de aşmış oluyorlar. Bu tür kötü amaçlı yazılımlar bir faturada veya sensör izleyicide kendilerine yer bulabiliyor.

Son yıllarda en çok ses getiren ve en şaşırtıcı ihlallerin bazıları üçüncü taraf tedarikçiler üzerinden gerçekleştirildi. Tedarik zinciri yönetiminin giderek daha da karmaşıklaştığı ve ekipmanlar ile süreçlerin birbirine giderek daha bağımlı hale geldiği dikkate alındığında, siber güvenliğin, tedarikçilerinizi ve satıcılarınızı da kapsayacak şekilde tüm tedarik zincirine yayılan bir konu olduğu daha iyi anlaşılacaktır. Elbette siber güvenliği bir rekabet avantajına dönüştürme fırsatına da sahipsiniz. Son bölümdeki örnekte de görülebileceği gibi, sağlam ve kanıtlanabilir bir güvenlik protokolü ile destekleyerek, müşterilerini açık bir ağa bağlayan her şirket önemli bir satış noktası sahibi olabilir.

Anket, katılan CEO'ların çeşitli senaryolarda önemli güvenlik tedbirlerini planlamadığını veya planlamakta geç kaldığını ortaya koydu.

Bir güvenlik yöneticisi/ekibi görevlendirmeyi planlamak

Önleyici adımlar atmış	%50
Önümüzdeki 3 yıl içinde adımlar atmayı planlıyor	%29
Bunu yapmayı planlamıyor	%21

Dahili süreçleri (veri paylaşımı, donanım kullanımı vs.) değiştirmeyi planlamak

Önleyici adımlar atmış	%45
Önümüzdeki 3 yıl içinde bunu yapmayı planlıyor	%44
Bunu yapmayı planlamıyor	%11

Mevcut teknolojileri yükseltmeyi planlamak

Sadece güncel teknolojileri yükseltmiş /önleyici adımlar atmış	%37
Önümüzdeki 3 yıl içinde bunu yapmayı planlıyor	%49
Bunu yapmayı planlamıyor	%14

Harici süreçleri (veri toplama, hareket işleme, veri paylaşımı vs.) değiştirmeyi planlamak

Önleyici adımlar atmış	%34
Önümüzdeki 3 yıl içinde bunu yapmayı planlıyor	%53
Bunu yapmayı planlamıyor	%13

ABD'de önemli yatırımlar yapıldı

Hazırlıklı olma durumuyla ilgili veriler, coğrafi konuma göre önemli farklar olduğuna işaret ediyor. Kendinizi ne kadar hazır hissettiğiniz, nerede bulunduğunuza bağlı. Örneğin ABD'deki CEO'ların %87'si şirketlerinin tam olarak hazır olduğunu belirtiyor. Saldırıya uğrayan tüketici verilerini ifşa etmekle ilgili yasal kurallar, kamuoyunda büyük ses getirmiş bazı ihlal olayları ve hükümetin veri korumayla ilgili aktif bir tutum sergilemesi, bu konudaki bilincin diğer bölgelere kıyasla daha güçlü hale gelmesini sağlamış. ABD siber suçlular için cazip bir hedef ve saldırganlar özellikle Kuzey Amerika'da "manşetlere çıkmayı" çok seviyor.

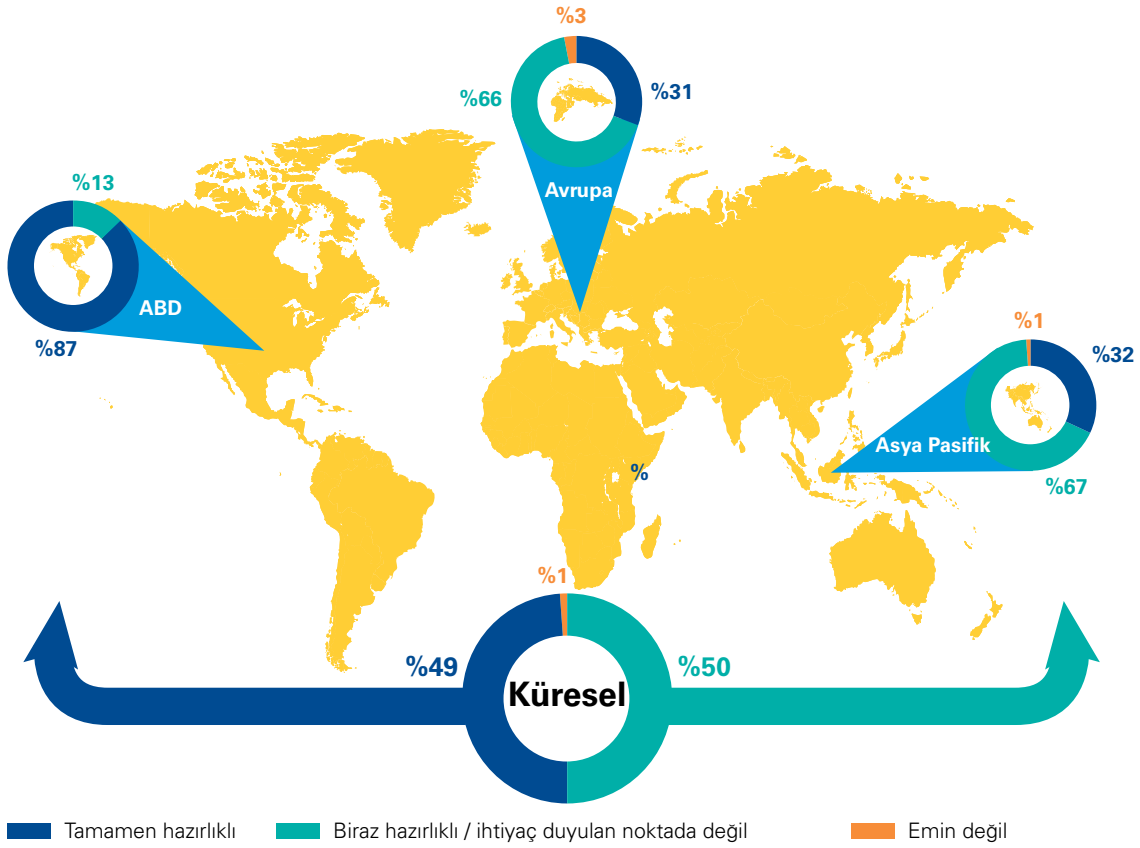
Bell bu konuda, "Pek çok şirket, olası saldırıları önlemek için ciddi yatırımlar yaptı" diyerek ekliyor: "Ancak, yakın zamana kadar, saldırıyı önlemeye çok fazla odaklanılıyor, saldırıdan korunmaya ve buna yanıt vermeye ise yeterince odaklanılmıyordu." CEO'lar şu soruyu sormaya başladı: Bell bu noktada şu soruyu soruyor: "Bir siber saldırıyla karşılaşırsak bunu nasıl daha hızlı tespit edebilir ve nasıl etkin bir şekilde yanıt verebiliriz?" İşletmelerin bu tür bir saldırıya ne kadar hazır oldukları, saldırıdan en az zararla ve hızla kurtulabilmek ile kalıcı ve daha ağır hasarlar yaşamak arasındaki ince çizgiyi oluşturuyor.

> "Bunun temel nedeni ise çoğu zaman tahmin yanılgıları. Saldırganların kararlılığını ve becerilerini tahmin etmede yanılmak."
>
> — Malcolm Marshall
> KPMG Siber Güvenlik Hizmetleri Küresel Başkanı

Avrupa'daki Tedbir Seviyesi

Avrupalı katılımcıların üçte birinden az bir kısmı olası bir siber saldırıya hazırlıklı olduklarını belirtti. Pek çok Avrupalı işletme ise değişim sürecinde. KPMG Almanya Siber Güvenlik Başkanı Uwe Bernd-Striebeck, "Snowden'ın açığa çıkması pek çok Avrupalı CEO'yu mevcut siber stratejilerini ve güvenlik tedbirlerini yeniden gözden geçirmeye itti" diyerek ekliyor: "Pek çok Avrupalı şirketin yerli güvenlik şirketlerine yöneldiğini ve ABD menşeli güvenlik araçlarını Avrupa menşeli araçlarla değiştirdiğini veya yakın bir gelecekte bunları yapmayı planladığını görüyoruz.

Bölgedeki çoğu şirket, siber güvenlik yolculuğunun henüz başında veya ortalarında. Bu şirketler, en etkili korumayı sağlayacak ve siber olaylarla yeterince baş edebilmelerine imkan tanıyacak düşük maliyetli ve etkili güvenlik çözümleri arıyor. Güvenliğe önemli yatırımlar yapmış olsalar da, Avrupalı CEO'lar, ABD'li CEO'lara kıyasla biraz daha temkinli olduklarından siber güvenlik konusunda tam anlamıyla hazır olduklarını belirtmekten kaçınıyor."



Kaynak: 2015 KPMG CEO Araştırması, Mayıs 2015.

Asya: Tehdit ortamına yanıt verebilmek

KPMG Asya Siber Güvenlik Başkanı Dani Michaux, "ABD'deki işletmelerin olası tehditlere karşı hazırlıklı olma çabalarını hızlandıran davranışlar Asya Pasifik bölgesinde görülmedi veya ilerleme kaydetmedi" diyor. CEO'ların sadece %32'si işletmelerinin siber cephede tam anlamıyla hazır olduğunu belirtti. Hükümetler bu konuda ülke çapında daha aktif bir rol oynayıp konuyu yakından takip ediyor, gizlilik kanunları gözden geçiriliyor ve işletmeler artan tehdit ortamına artık daha iyi yanıtlar verebiliyor.

Asya Pasifik bölgesindeki işletmelerin siber risk konusundaki değerlendirmeleri ve olgunluk seviyeleri arasında önemli farklar var. Siber riski yeni yeni kabul edip anlamaya başlayan işletmeler olduğu gibi; siber güvenliğin işletmeyi korumak ve büyütmek için kritik öneme sahip olduğunu yönetim kurulu ve CEO seviyesinde kabul edip gerekli tüm tedbirleri almış işletmeler de mevcut.

Pekin'in ABD teknolojisini ikame etme çabaları ve Çin'deki güvenlik ürünleri ve hizmetleri konusunda bazı katı yönetmelikleri yürürlüğe sokması, Asya'nın bu en büyük siber güvenlik pazarında önemli değişimlere yol açtı.

KPMG Avustralya Siber Güvenlik Başkanı Gordon Archibald, "Avustralyalı pek çok CEO ve yönetim kurulu aslında siber güvenliğin önemini biliyor ancak bu konudaki farkındalıkları çoğu zaman harekete geçilmesini sağlayabilecek seviyede olmuyor" diyor. Bunun nedenlerinden biri, neler yapılması gerektiği konusunda belli bir netlik bulunmaması. Archibald şunları ekliyor: "Bu aslında bazen sorunu net bir şekilde tanımlamak için gereken enerjiyi sağlayamayan yöneticilerin sorunlarından biri. Neyi korumaya çalışıyorum, riskler neler ve bu varlıklar ne kadar iyi korunuyor gibi sorulara yanıt bulmakta zorlanıyorlar." Bu yöneticiler tehdidin farkında ancak bunun işletme ve yeni gelişen teknolojiler üzerindeki potansiyel etkilerini her zaman göremiyorlar.

Kime sahip olduğunuz ne bildiğiniz kadar önemli

Bu sorunlar bir araya geldiğinde yetenek tarafında "kusursuz fırtınayı" yaratıyor ve zaten hakim olan yetenek açığı önümüzdeki yıllarda daha da kötüleşecek gibi görünüyor. Gelecekte karşılaşılabilecek bir siber olaya hazırlıklı olmadıklarını söyleyen anket katılımcısı CEO'ların önümüzdeki 3 yıl boyunca çalışan sayısını artırma ihtimallerinin daha yüksek olduğunu düşünüyoruz. Ayrıca, bu katılımcıların yarısı aynı dönem boyunca yetenek açığında bir artış bekliyor.

En büyük zorluklardan biri de, yetenek açığının büyük ölçekte olması. Küresel tahminler, siber güvenlikle ilgili pozisyonların %23'ünden fazlasını doldurmanın 6 aydan uzun süreceğini, %10'luk bir kısmın ise doldurulamayacağını öngörüyor. ABD İş Gücü İstatistikleri Bürosu ise, Ağustos 2015 itibarıyla siber güvenlik alanında yaklaşık 300.000 boş pozisyonun doldurulamadığını tahmin ediyor. Bu yetenek açığı, teknik uzmanlıklarını işletme, yönetim, risk veya sosyal bilimler gibi diğer alanlardaki ek becerilerle de güçlendirmiş siber güvenlik profesyonelleri konusunda daha da akut bir hal alıyor.

Marshall, "Doğru BT yeteneklerini bulmak çoğu işletme için zor. Teknolojiyi müşteri deneyimine entegre etmeyi içeren projelerde ise bu daha da zor bir iş" diyerek ekliyor: "Arka planda iyi güvenlik uzmanlarına sahip olmak gerektiği konusunda herkes hemfikir. Ancak yeni ürünler tasarlamak, yeni teknolojiler entegre etmek ve yeni pazarlara güvenle girebilmek için, tasarımcılarla ve pazarlamacılarla birlikte ön saflarda görev yapan iyi güvenlik uzmanlarına sahip olmanız lazım. Müşteri deneyiminin bir kabus değil keyif kaynağı olmasını sağlayabilecek yeteneklere sahip olmalısınız."

İşi bilen siber yöneticiler

İşletme bünyesinde siber güvenlikten kimin sorumlu olduğu her zaman sorulan bir soru olmuştur. Ankete katılan on CEO'nun dördü önümüzdeki yıllarda CIO'nun görevinin daha önemli hale gelmesini beklediğini belirtilmişse de, pek çok CIO henüz üst düzey yönetici seviyesinde değildir veya bir iş ortağı olarak saygı görmüyor. Bu noktada, güvenlikten sorumlu tek yöneticinin CIO olması halinde işletmenin geri kalanının güvenliği her tür davranış ve sürece entegre etmek yerine güvenlikle ilgili tüm sorumluluğu BT fonksiyonuna bırakması riskinin doğacağı asla unutulmamalıdır.

Marshall, "Siber güvenlik daha geniş çapta bir saygıyı hak ediyor" diyerek ekliyor: "Bir yönetim kurulu üyesine ve CIO dışındaki bir üst düzey yöneticiye, siber güvenliğin hem riskler hem de fırsatlar bakımından tüm işletmeye nasıl entegre edildiğini denetleme sorumluluğu verilmesini tavsiye ediyoruz."

Bu sayede, güvenliğin sadece bir BT konusu olmadığı mesajı herkese net bir şekilde verilecektir.

İyi yönetilen pek çok şirkette bir Bilişim Güvenliği Başkanı (CISO) vardır. Bu kişi günümüzde genellikle CIO'ya raporlama yapar. Ancak, şirketler siber güvenliği tüm işletmeyi etkileyen bir iş riski olarak görmeye başladıkça bu durum da değişiyor. Bazı CISO'lar artık COO, CFO, baş hukuk müşaviri ve hatta bazı durumlarda CEO gibi en üst düzey yöneticilere raporlama yapıyor. Satın alma, birleşme ve ürün tasarımı ile ilgili siber risklerin bilincinde olan bir şirket, sorumluluğun en üst düzey yöneticilere kadar yayılması gerektiğini kabul edecektir.

Raporlama yapısı, sağlam bir güvenlik profilinin sadece bir parçası. Pek çok şey bu görevleri yerine getiren kişilere bağlı. Marshall, "Bu sadece konunun uzmanına bırakılamayacak kadar önemli bir konu" diyerek ekliyor: "Konunun uzmanı yetenekli kişilere ilham verip onlara yön gösterebilecek güçlü bir lidere sahipseniz CISO olarak bir güvenlik uzmanına ihtiyacınız yok demektir."

Kaynak: 2015 KPMG CEO Araştırması, Mayıs 2015.

Bell ise şunları söylüyor: "CISO, üst düzey yöneticilerle ve yönetim kuruluyla anlamlı görüşmeler yapabilecek kapasitede olmalı." Çoğu CISO, bu incelikli teknoloji risklerini açıklamak zorunda kalıyor ve işletme odaklı bir dinleyici kitlesi bunu fazla terminolojik bulabiliyor. Bell şunları ekliyor: "İşletmede bir siber güvenlik sorununu içeren iş riskleri hakkında sizinle konuşabilecek bir siber güvenlik liderine sahip olursanız çok daha etkili bir görüşme yapabilirsiniz."

Doğru araçlar

İşletmeler, doğru insanların yanı sıra doğru araçlara da yatırım yapmak zorunda. Saldırıya uğradıklarını anlayabilmek için öncelikle ve en önemlisi görüş imkanı elde edebilmeleri gerekir. Görüş imkanı olmadığı takdirde güvenlik açıklarını ve altyapıdaki zayıflıkları belirlemek imkansızdır. Aldıkları hasarı fark edene kadar yıllar boyunca sayısız saldırıya uğramış işletmelerin sayısı hiç de az değil.

Şirketlerin uzmanlıklarını artırabilmelerinin bir yolu da, sorunları ve anormallikleri belirleyip olağan dışı veya şüpheli faaliyetleri ortaya koyabilmek için güvenlik istihbaratına sahip olmak. İstihbarat iki şekilde yardımcı olabilir. Birincisi, bir erken uyarı sistemi zayıflıkların neden olduğu tehdit penceresini, yani saldırının tespit edilmesiyle ortadan kaldırılması arasındaki süreyi kısaltır. İstihbarat ayrıca, küresel tehditler hakkında, bir şirketin tek başına oluşturabileceğinden daha büyük bir resim oluşturur. Güvenlik bir ekosistemdir ve işletmeler hem içeride hem de dışarıda neler olup bittiğini bilmek zorundadır.

KPMG Capital, şirketlerin siber saldırıları önceden engelleyebilmesine, ortaya çıkan tehditleri izleyebilmesine ve olası zafiyetleri belirleyebilmesine yardımcı olan canlı saldırı istihbaratı çözümlerinde lider Norse Corporation'ın özsermaye hisselerini yakın zaman önce satın aldı. Norse kurucu ortağı ve CEO'su Sam Glines, "Norse beş yıldan beri internetin kötü çocuklarını takip ediyor" diyerek ekliyor: "İstihbarat, saldırılar, saldırganlar ve saldırma yöntemleri hakkındaki bilgileri sizin ağınıza veya iş ortaklarınızın ağlarına saldırılmadan önce size sunarak aygıtlarınızın, sistemlerinizin vs. korunmasını sağlayabilir."

Marshall ise şunları söylüyor: "Müşteriler son derece gelişmiş ve karmaşık siber tehditlerle karşı karşıya. KPMG üye şirketleri, Norse ile birlikte çalışarak hızla değişen tehdit ortamını izleyebilecek ve bu sayede hem saldırganların kullandığı taktikler hem de bunlara karşı yapılabilecekler konusunda bazı erken uyarılara ve faydalı görüşlere sahip olmamızı sağlayacak."

Tehdit istihbaratının paylaşılması

Şirketler, kendi güvenlik tehditleriyle ilgili bilgileri benzer şirketlerle ve rakiplerle paylaşarak kendi istihbaratlarını genişletebilir. Teoride bu mantıklı bir fikirse de, kendisi hakkındaki bilgileri rakipleriyle paylaşmak pek çok şirketin henüz kabul edebileceği bir şey değil. Şirketlerin çoğu, zayıflıklarını kamuoyu ile paylaşmak istemez ve kanunlarca zorunlu kılınmadığı sürece yaşadıkları ihlalleri asla kendiliğinden duyurmaz. Finans kuruluşları bunun bir istisnasıdır: Finans altyapısı birbirine o kadar bağlıdır ki finans şirketleri bir saldırıya maruz kaldıkları takdirde birlikte batacaklarını veya yüzeceklerini düşünür. Ancak diğer sektörlerin çoğunda bu tür bir paylaşma kültürü yoktur.

Şirketlerin bununla başa çıkmalarındaki bir başka yöntem de, genellikle iyi niyetli bilgisayar korsanlarına görev verilen işbirliğine dayalı ağlardır. İyi niyetli korsanlar, bilgilerini iyi niyetle kullanarak şirketlerin sistemlerindeki zayıflıkları bulmalarına yardımcı olan kişilerdir. Bunlara görev veren yöneticiler çoğu zaman şirketlerinin sistemlerine bir iki dakika içinde nasıl girebildiklerini görüp şaşkınlığa uğrarlar.

Eksiksiz güvenlik diye bir şey aslında yoktur. Şirketler, güvenlik duvarları ya da sızma girişimi önleme sistemleri gibi tepkisel teknolojilere yoğun bir şekilde güvenmek yerine, siber güvenlik konusunda proaktif ve tahminsel bir yaklaşım benimsemelidir. Zayıf noktaları sürekli test etmek kötü niyetli kişilerin bir adım önünde olmanın bir yoludur. Güvenlik istihbaratı aracılığıyla tehdit ortamını anlamak ve düşmanınızı tanımak da başka bir yoldur. Önleyemeyeceğiniz bir saldırıyı en azından tespit etmeye çalışın. Tespit de edemeyeceğiniz bir saldırı içinse, olabildiğince kısa sürede yanıt verebilmeye hazırlıklı olun.

Ağınıza kim saldırıyor?

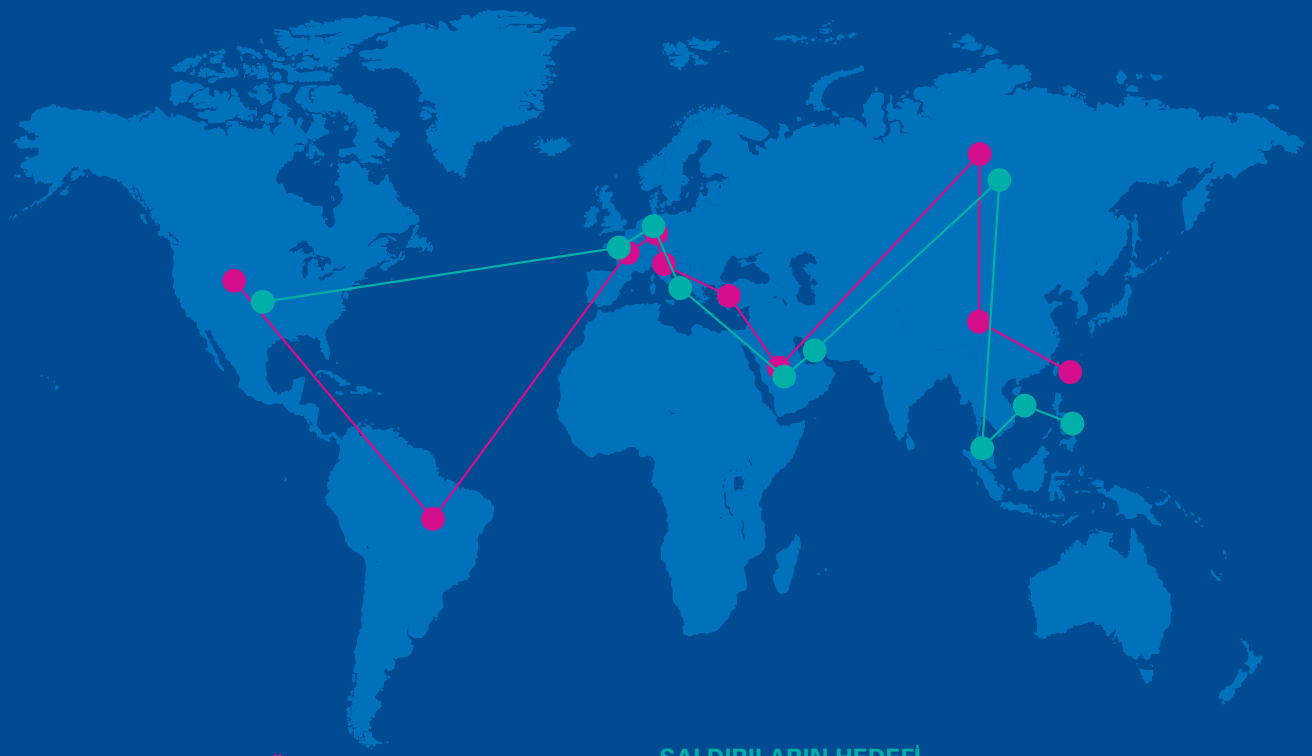
Norse Intelligence Service'teki siber analistler, karşı konulamaz hedefler gibi görünecek küresel bir sensör ağı oluşturup bu ağa kimin saldıracağını beklemeye koyularak bu soruya yanıt aramaya çalıştı. Glines, "İnternetin en belalı sokaklarında dolaştık ve saldırılmak için belamızı aradık" diyerek ekliyor: "Kendimizi kötü çocuklara bir telefon şirketi, ATM ve nükleer santral olarak tanıttık. Bu, yolun ortasına bir Ferrari park edip camları açık, kontak anahtarını da aracın üstünde bırakarak kimin aracı çalacağını beklemek gibi bir şey."

Bu çalışmamız, saldırganların kimler olduğu, IP adreslerinin nereye ait olduğu, nasıl faaliyet gösterdikleri ve genellikle nelere baktıkları konusunda Norse'a son derece faydalı görüşler sağladı. Bu bilgiler Norse müşterilerinin kendi ağlarındaki risk seviyesini değerlendirebilmelerine ve tehdit içeriğini görebilmelerine yardımcı olabilir.

Sistem şu şekilde çalışıyor: Norse sensörleri ve otomatik takip gezginleri müşterinin sistemindeki ağ tehditlerini erkenden tespit edip şüpheli faaliyetler hakkında gerçek zamanlı uyarılar veriyor. Bir sızma tespit edildiğinde ise, istihbarat ünitesi saldırının arkasında kimlerin olabileceği hakkında bazı ipuçları sunuyor. Belli bir devlet mi? Bir korsan şebekesi mi? Rakiplerden biri mi? Saldırganlar geçmişte nerelere erişmeyi veya zarar vermeyi denemiş?

Glines şöyle devam ediyor: "İşe koyulalım, sizin için bu bilgileri toplayalım ve sisteminizi geliştirelim diyoruz. Bu sayede, saldırganlar sizin peşinize düştüğünde kim olduklarını, neden size saldırdıkları ve sizden ne almak istedikleri konusunda bilgi sahibi olup duruma daha hazırlıklı olabileceksiniz. Dijital düşmanlarınızı yenebilmek için en az onlar kadar saldırgan ve girişimci olmak zorundasınız."

Hacme göre ilk 10 siber saldırı kaynağı ve hedefi



SALDIRILARIN KAYNAĞI

- Çin
- ABD
- Suudi Arabistan
- Almanya
- Rusya
- Hollanda
- Fransa
- Brezilya
- Türkiye
- Tayvan

SALDIRILARIN HEDEFİ

- ABD
- Birleşik Arap Emirlikleri
- Suudi Arabistan
- Almanya
- Fransa
- Rusya
- Filipinler
- Liechtenstein
- Hong Kong
- Singapur

Kaynak: Norse İstihbarat Ağı, 2015. Bu, kurumsal sunuculardan ve mobil aygıtlardan endüstriyel SCADA ekipmanlarına ve sağlık hizmeti sistemlerine kadar binlerce farklı cihaz türünün kullanıldığı 50'den fazla ülkedeki milyonlarca IP adresinden oluşan küresel bir ağ. Bu ağ, saniyede 30.000'den fazla saldırıya maruz kalıyor. Hedeflenen ülkeler ve hedef alan ülkeler ile ilişkili coğrafi istatistiklerde saldırı verileri temel alınıyor.

Siber güvenliğin dört altın kuralı

Temel kontrolleri doğru uygulayın.

Saldırıların %75'inden fazlası, temel kontrollerin bulunmamasına bağlı zayıflıkları hedef alıyor.

Elinizdeki mücevhere iyi bakın.

Kendinizi savunmak için yapacağınız harcamaları, en kritik varlıklarınızı koruyabileceğiniz şekilde önceliklendirin.

Düşmanlarınızla ilgili "ev ödevlerinizi" ihmal etmeyin.

Size kimin, neden ve nasıl saldırabileceğini anlamak için gereken yatırımları yapın. Bu sayede en olası senaryoları öngörebilir ve saldırıya uğraması en muhtemel varlıklarınızı koruyabilirsiniz.

Siber riski, işletmenizi daha yakından incelemeye yönelik bir fırsat olarak görün.

Güvenlik ve dayanıklılık, bir işletmenin hemen her bölümünü etkileyebilir. BT güvenliğini ve işletme dayanıklılığını korumaya dönük stratejiler, işletmenin fikri mülkiyeti korumaktan üretkenliği artırmaya ya da müşterileri daha çok memnun etmenin yollarını bulmaya kadar daha geniş kapsamlı hedefleriyle uyumlu olmalıdır.

En yenilikçi şirketler, siber güvenliğin sadece yönetilmesi gereken bir risk değil aynı zamanda bir müşteri deneyimi ve gelir fırsatı olduğunun bilincine vardı. Bu şirketler, siber güvenlik konusunda hazır olmayı bir maliyetten rekabet avantajına dönüştürmenin yollarını arıyor, güvenliği henüz tasarım aşamasındayken ürün ve hizmetlerine entegre ediyor ve siber güvenliğin sadece bir BT konusu olmadığını, tüm işletme ve işletme ekosistemi boyunca elde edilmesi gerektiğini kabul ediyor.

Metodoloji

Bu raporda yayımlanan anket verileri, Avustralya, Çin, Fransa, Almanya, Hindistan, İtalya, Japonya, İspanya, Birleşik Krallık ve ABD'den 1.276 CEO ile yapılan bir ankete dayanmaktadır. Aralarında otomotiv, bankacılık, sigortacılık, yatırım yönetimi, sağlık hizmetleri, teknoloji, perakende/tüketici pazarları ve enerji/şebeke hizmetlerinin de bulunduğu başlıca dokuz sektörü kapsamaktadır. 347 CEO yılda 500 milyon $ ila 999 milyon $ arasında gelire sahip şirketlerde, 626 CEO yılda 1 milyar $ ila 9,9 milyar $ arasında gelire sahip şirketlerde, 303 CEO ise yılda 10 milyar $ ve üzeri gelire sahip şirketlerde görev yapmaktadır.

Katkıda bulunanlar

Malcolm Marshall
Siber Güvenlik Küresel Lideri

Greg Bell
ABD Siber Güvenlik Lideri

Dani Michaux
Asya Pasifik Siber Güvenlik Lideri

Uwe Bernd-Striebeck
Almanya Siber Güvenlik Lideri

Gordon Archibald
Avustralya Siber Güvenlik Lideri

Samuel Glines
Norse Corporation Kurucu Ortağı ve CEO'su

İletişim:

Hakan Aytekin
Danışmanlık, Şirket Ortağı
T : + 90 216 681 90 00
E : hakanaytekin@kpmg.com

Tanıl Durkaya
Bilgi Teknolojileri Danışmanlığı
Şirket Ortağı
T : + 90 216 681 90 00
E : tdurkaya@kpmg.com

kpmg.com.tr

Download on the App Store

ANDROID APP ON Google play