Siber Güvenlikte En Yaygın Beş Yanılgı

KPMG Türkiye

kpmg.com.tr

İçindekiler

Önsöz

Siber güvenlik her kuruluş için önemli bir endişe kaynağı. Her gün gerçekleşen olaylar, bireysel fırsatçı bilgisayar korsanlarından, fikri mülkiyeti çalıp işletmeyi zarara uğratma stratejisine sahip profesyonel organize siber suç örgütlerine kadar, siber saldırganların yarattığı riski gözler önüne seriyor.

Her kuruluşun yönetim birimleri, kuruluşun riskleri anlamasını ve doğru öncelikleri belirlemesini sağlamakla sorumludur. Teknik terminoloji ve değişim hızı nedeniyle bu kolay bir görev değildir.

Bu sorunları ele almak için sadece teknolojiye odaklanmak da yeterli değil. Siber riskin etkin bir şekilde yönetilmesi, doğru teknolojileri uygulamaya koymanın yanı sıra doğru kurumsal yönetim ve destek süreçlerini hayata geçirmek anlamına da gelir.

Ancak bu karmaşıklık, şirket yönetimlerinin sorumluluğu doğrudan teknik "uzmanlara" devretmeleri için bir mazeret olmamalıdır. Liderlerin siber güvenlikle ilgili kaynak tahsisinin kontrolünü ele almaları, siber güvenlikle ilgili kurumsal yönetimi ve karar alma süreçlerini aktif bir şekilde yönetmeleri ve bilgiye dayalı, mantıklı bir organizasyon kültürü yaratmaları son derece önemlidir.

Bu çalışma, yönetimin doğru işler yapabilmesini sağlayabilecek faydalı görüşler sunuyor. Çalışma, günümüzün siber suç dünyasını inceleyerek, en yaygın beş yanılgıyı ortaya koyuyor, siber güvenlik politikalarını kişiselleştirmenin önemine değinerek, güçlü bir siber güvenlik modelinin kritik boyutlarını ele alıyor ve şirketlerin siber güvenliğin "yeni koşullarına" başarıyla uyabilmesine yardımcı olabilecek bazı sorulara yanıt veriyor.

Tanıl Durkaya
Bilgi Teknolojileri Danışmanlığı
Şirket Ortağı, KPMG Türkiye
E : tdurkaya@kpmg.com

Siber suç nedir ve kimler bu suçu işler?

Siber suç, kuruluşları zarara uğratmak ya da pek çok farklı amaç ile tetiklenebilen yasa dışı dijital faaliyettir. Bu terim pek çok hedef ve saldırı yöntemi için kullanılıyor.

"Aktörü", yani saldırıları yapan veya destekleyen kişi ya da kuruluşu anlamak etkin bir savunma için mutlaka gereklidir.

Bu aktörler dört kategoriye ayrılabilir:

1. Genellikle tek başına hareket eden ve neler yapabileceklerini gösterme isteğiyle motive olan bireysel bilgisayar korsanları,
2. Genellikle korku ve karmaşa yaratarak bir ideolojiyi veya siyasi görüşü desteklemek amacıyla hareket eden eylemciler,
3. Dolandırıcılık amaçlı e-postalardan, çalınan şirket verilerinin satılmasına kadar pek çok farklı yöntem aracılığıyla sadece maddi çıkar elde etmeyi amaçlayan organize suç örgütleri,
4. Jeopolitik konumlarını ve/veya ticari çıkarlarını geliştirmek için çeşitli faaliyetler yürüten hükümetler.

Bu farklı aktörlerin gerçekleştirdiği saldırılar, hedefin türü, saldırı yöntemleri ve etkisinin boyutu gibi bazı farklı özellikler barındırır.

01 Siber riski anlama

Veri hacmi katlanarak büyümeye devam ettikçe kuruluşların çevrim içi ağlar aracılığıyla paylaştıkları veri oranı da artıyor. Tabletler, akıllı telefonlar, ATM'ler, güvenlik sistemleri, petrol sahaları, çevresel kontrol sistemleri, termostatlar vb. oluşan milyarlarca makine birbirine bağlı ve birbirine bağlı olma hali sürekli katlanarak artıyor. Kuruluşlar mevcut BT sistemlerini giderek artan oranda çeşitliliğe sahip yeni cihazlara açıyor ve veri güvenliği üzerindeki doğrudan kontrollerini kaybediyor. Ayrıca gerek toplum gerekse şirketler bünyesindeki iş sürekliliği de bilgi teknolojilerine giderek daha fazla bağımlı hale geliyor. Bu temel süreçlerin aksaması ise, hizmetin sürekliliği üzerinde büyük etkiye sahip olabiliyor.

Siber suçlular bu zaafiyetlerin neler olduğunu çok iyi biliyor. Sadece maddi çıkar elde etmekten belli bir ideolojiye destek sağlamaya, casusluğa veya terör eylemine kadar farklı motivasyon kaynaklarıyla hareket eden bireysel bilgisayar korsanları, eylemciler, organize suç örgütleri ve hükümetler giderek artan sayıda ve önemde devlete ve şirket ağına saldırıyor.

Siber tehdit yıpratıcı bir etki bırakarak gerçekleştiğinde, medya siber güvenlik konusunda genellikle bir panik havası yaratıyor ve orantısız bir korku kültürüne neden oluyor.

Her kuruluş siber suçlular için kolay bir hedef olmayabilir. Örneğin küçük veya orta ölçekli bir şirket çok uluslu bir kuruluştan çok daha farklı bir risk profiline sahiptir.

Siber suç risklerinin kontrol altına alınabileceği gerçeği ise tüm hükümetler veya kuruluşlar için geçerlidir. Siber suçlular karşısında asla çaresiz değiliz ve her ne kadar işletmenize ağır hasarlar verebilseler de kendinizi bunlara karşı korumak için bazı adımlar atabilirsiniz. %100 güvenlik elde etmeniz mümkün olmasa da, siber güvenliği "işinizin olağan bir parçası" olarak görüp yatırımlarınızı riskler ve potansiyel etkiler arasında dengeleyerek, kuruluşunuzun siber suçla mücadeleye iyi hazırlanmasını sağlayabilirsiniz.

Kuruluşlar önleme, tespit etme ve yanıt verme olarak sıralayabileceğimiz üç kritik alandaki kabiliyetlerini artırarak işletmelerinin karşılaştığı riskleri azaltabilir.

Önleme

Önleme her şeyden önce kurumsal yönetim ve organizasyon ile başlar. Kuruluş bünyesinde siber suçla savaşmaya yönelik sorumlulukları belirlemek ve kilit pozisyonlardaki personel için farkındalık eğitimleri vermek gibi bazı temel tedbirleri hayata geçirmek bunun bir parçası.

Tespit etme

Bir kuruluş, kritik faaliyetleri ve olayları izleyerek teknolojik tespit tedbirlerini güçlendirebilir. İzleme ve veri madenciliği faaliyetleri birlikte yürütüldüğü takdirde, veri trafiğindeki anormal hareketleri belirlemek, saldırıların odaklandığı noktaları bulmak ve sistem performansını izlemek için mükemmel bir araç haline gelir.

Yanıt verme

Yanıt verme, başarısı önceden test edilmiş bir planın, olası bir saldırı bulgusu elde edildiği anda devreye sokulmasıdır. Kuruluş, saldırı sırasında etkilenen tüm teknolojilerini devre dışı bırakabilme becerisine sahip olmalıdır. Kuruluş, bir müdahale ve felaket sonrası kurtarma planı geliştirirken, siber güvenliğe tek başına bir çözüm olarak değil kesintisiz bir süreç olarak bakmalıdır.

	Önleme	Tespit etme	Yanıt verme
Yönetim ve organizasyon	Siber suç sorumlularını görevlendirme	Krize 7/24 hazır bir organizasyon yapısı kurma	Suistimali önlemeye yönelik analiz becerilerini kullanma
Süreçler	Siber suça yanıt testleri (simülasyonlar) Periyodik taramalar ve sızma testleri	Olay takibine yönelik prosedürler	Siber suç yanıt planı
Teknoloji	Makul güvenlik seviyesini ofis masalarında sağlama Ağ segmentasyonunu sağlama	Kritik süreçlerin kaydedilmesini sağlama Güvenlik olaylarının merkezi bir şekilde izlenmesini sağlama	Saldırıya uğrayan BT hizmetlerini devre dışı bırakma veya sonlandırma

02 En yaygın beş siber güvenlik yanılgısı

Siber güvenlik pek çokları için bir bilinmezliği ifade ediyor. Bu bilinmezlik de, siber güvenlik yaklaşımı konusunda pek çok yöneticinin yanlış kanılara sahip olmasına yol açıyor. Yıllara dayanan tecrübemiz, çoğu zaman oldukça şiddetli sonuçlar doğurabilen aşağıdaki beş güvenlik yanılgısının yaygın olduğunu gösteriyor.

1	Yanılgı	**%100 güvenliği sağlamak zorundayız.**
	Gerçek	**%100 güvenlik doğru bir hedef olmadığı gibi bunu başarmak da imkânsızdır.**

Hemen her hava yolu şirketi uçuş güvenliğinin birinci öncelikleri olduğunu iddia etse de aslında uçuşun tamamen yok edilemeyecek yapısal bir risk barındırdığını da kabul eder. Aynı durum siber güvenlik için de geçerlidir. İster gizli kalmış ister kamuoyu tarafından öğrenilmiş olsun, hemen her büyük ve tanınmış kuruluş bir şekilde bilgi hırsızlığıyla karşılaşacaktır.

Siber suçlara karşı %100 koruma sağlamanın uygulanabilir ve doğru bir hedef olmadığı yönünde farkındalık yaratmak bile, savunmaya yönelik duruşunuz ile ilgili seçim yapabilmenize imkân tanıması bakımından daha etkin bir güvenlik politikası için atılmış önemli bir adımdır. Doğru bir savunma duruşu, kuruluşun suç girişimlerine karşı zayıflığından kaynaklanan tehdidi anlamaya (önleme), yaklaşan veya gerçekleşen bir ihlali tespit edecek mekanizmalar oluşturmaya (tespit etme) ve yaşanan olaylarla anında ilgilenerek (yanıt verme) kaybı en aza indirecek bir kabiliyet yaratmaya dayanır.

Uygulamada genellikle sistemlere izinsiz girmeye çalışan kişilere karşı geçilmez bir duvar oluşturmayı amaçlayan önleme faaliyetlerine ağırlık veriliyor. Oysa kusursuz güvenliğin bir hayal olduğunu ve siber güvenliğin "işin olağan bir parçası" olduğunun farkına vardığınızda, tespit etme ve yanıt verme konusuna da yoğunlaşmanız gerektiğini anlıyorsunuz. Bilgi hırsızlığından ana sistemlere yapılan yıkıcı saldırılara kadar değişiklik gösterebilen bir siber suç olayı yaşayan bir kuruluş, kayıpları en aza indirmek ve zayıflıkları gidermek zorundadır.

2		
	Yanılgı	**Sınıfının en iyisi teknik araçlara yatırım yaparsak güvende oluruz.**
	Gerçek	**Etkin bir siber güvenlik, teknolojiye sandığınızdan daha az bağımlıdır.**

Siber güvenlik dünyası, sisteme izinsiz giriş yapmaya çalışanları hızla tespit eden ürünler gibi teknik ürünler satan uzman tedarikçilerin hakimiyetindedir. Bu araçlar temel güvenlik için mutlaka gereklidir ve teknoloji mimarisine entegre edilmelidir ancak bütüncül ve sağlam bir siber güvenlik politika ve stratejisinin temeli değildir.

Teknolojiye yatırım yapmak, siber güvenlik stratejisinin itici gücü değil bir çıktısı olmalıdır. İyi bir güvenlik yapılanması, sağlam bir siber savunma yetkinliği geliştirmekle başlar. Genellikle BT departmanı buna öncülük etse de, nihai kullanıcının bilgisi ve farkındalığı kritik öneme sahiptir. Güvenlik ile ilgili en zayıf halka ise, hem BT profesyonelleri hem de nihai kullanıcı için insan faktörüdür. En iyi araçlara yapılan yatırımlar ancak kullanıcıların kendi ağlarını güvenli tutma konusundaki sorumluluklarını anlaması halinde karşılığını verebilecektir. Bilgisayar korsanlarının sistemlere erişmek amacıyla çalışanları manipüle ettikleri sosyal mühendislik hâlâ kuruluşların karşılaştığı başlıca risklerden biridir.

Bu noktada teknoloji ne yazık ki yardımcı olamıyor ve yöneticiler bu zorlukla baş etme sorumluluğunu almak zorunda kalıyor. Yöneticiler, bilinçli bir yaklaşım sergilemeli ve siber saldırılardan gelebilecek tehditlere karşı çalışanları eğitip farkındalık yaratmak için onlarla en iyi şekilde nasıl iletişim kurabileceklerini sorgulamalıdır. Bu genellikle mevcut organizasyon kültürünü çalışanların risklere karşı tetikte olacağı ve endişelerini üstlerine proaktif bir şekilde ileteceği bir şekilde değiştirmekle gerçekleştirilebilir.

3		
	Yanılgı	**Elimizdeki silahlar bilgisayar korsanlarının silahlarından daha güçlü olmalı.**
	Gerçek	**Güvenlik politikalarınızı, saldırganların hedeflerine göre değil kendi hedeflerinize göre belirlemeniz gerekir.**

Siber suçla savaş, kazanılması kolay olmayan yarışlara bir örnektir. Çünkü saldırganlar sürekli yeni yöntem ve teknolojiler geliştirir, savunma ise her zaman bir adım geriden gelir. Peki, bu gerçeğe rağmen saldırıları engellemek için sürekli gelişen sofistike araçlara yatırım yapmaya devam edilmeli mi?

Saldırganlar ve yöntemleri hakkında her zaman güncel bilgi ve görüşlere sahip olmak önemliyse de, yöneticilerin siber güvenlik konusunda esnek, proaktif ve stratejik bir yaklaşım benimsemeleri kritik öneme sahiptir. Bir şirketin bilgi varlıklarının paha biçilemez değeri ve bu bilgileri kaybetmenin işletme üzerindeki ağır etkileri düşünüldüğünde, siber güvenlik yatırımlarında her yeni tehdidi tespit etmek amacıyla en güncel teknoloji veya sistemlerden ziyade kritik varlıkları korumaya öncelik verilmelidir.

En önemlisi de, yöneticilerin işletmeye hangi saldırganların neden saldırmak isteyebileceğini anlamasıdır. Bir kuruluş, varlıklarının değerini bir suçludan daha farklı algılıyor olabilir. Bazı varlıklarla ilgili risk almayı diğerlerine kıyasla ne kadar kabul edebilirsiniz? İşin ve teknolojinin bir zincir halinde geliştiğini ve dolayısıyla birbirlerinin güvenliğinden doğrudan etkilendiğini de düşündüğünüzde, kilit varlıklarınız hangi sistemlerde ve kimler tarafından saklanıyor?

4

Yanılgı: **Siber güvenlik konusunda mevzuata uyum tamamen etkin bir izlemeyle ilgili bir durum.**

Gerçek: **Öğrenme kabiliyeti en az izleme kabiliyeti kadar önemlidir.**

Gerçekler, siber güvenliğin mevzuata uyumdan son derece etkilendiğini gösteriyor. Kuruluşlar bazı yönetmeliklere ve mevzuata uyum sağlamak zorunda olduklarından aslında bu anlaşılabilir bir durum. Bununla birlikte, mevzuata uyumu siber güvenlik politikasının nihai hedefi olarak görmek ters etki yaratacak bir durumdur.

Sadece dış gelişmeler ile vakaların trendlerini anlayabilen ve bunlarla ilgili görüşleri doğru politika ve stratejiler belirlemek için kullanabilen bir şirket uzun vadede siber suçla mücadelede başarılı olabilecektir. Bu nedenle, etkin bir siber güvenlik politikası ve stratejisi kesintisiz öğrenme ve gelişmeyi temel almalıdır.

- Kuruluşlar, tehditlerin nasıl ortaya çıktığını ve bunları nasıl öngörebileceklerini anlamak zorunda. Uzun vadede bakıldığında bu yaklaşım daha da sağlam güvenlik "duvarları" oluşturmaktan daha düşük maliyetlidir. Bu sadece altyapının izlenmesinden ibaret değildir: tehdidin ve kısa, orta ve uzun vadeli risklerin anlaşılabilmesi için içsel ve dışsal hareketlerin akıllı bir şekilde analiz edilmesiyle ilgilidir. Bu bakış açısı, yatırımlardan tasarruf etmek de dâhil olmak üzere kuruluşların mantıklı güvenlik yatırımı seçimleri yapmasını sağlamalıdır. Oysa uygulamada pek çok kuruluş stratejik bir yaklaşım benimsemez ve kendilerine gelen içsel verileri toplayıp kullanmaz.
- Kuruluşlar, yaşanan olayları bunlardan ders alabilecekleri şekilde değerlendirmek zorundadır. Uygulamada ise eylemler ağırlıklı olarak gerçek zamanlı olaylara göre şekillendirilir ve çoğu zaman kaydedilip değerlendirilmez. Bu da kuruluşun yeni şeyler öğrenip gelecekte daha etkin güvenlik tedbirleri uygulama kabiliyetine zarar verir.
- Aynı durum saldırıların izlenmesi için de geçerlidir. Pek çok durumda kuruluşlar bazı izleme kabiliyetlerine sahiptir ancak bulgular organizasyon çapında paylaşılmaz. Elde edilen bilgilerden ya hiç ya da yeteri kadar ders alınmaz. Ayrıca, izleme faaliyetleri kurumsal istihbaratla da desteklenmelidir. İzlemek, sadece neyi izlemek istediğinizi anladığınız takdirde olası saldırıları belirlemede etkin bir araç haline gelir.
- Kuruluşlar, siber güvenlik risklerini değerlendirip raporlamak amacıyla kurum çapında bir yöntem geliştirmek zorundadır. Bunun için, mevcut risk seviyeleri ile bunların artışlarını belirleyecek protokollere ve yönetim kurulunu stratejik siber riskler ve ana faaliyet üzerindeki etkileri hakkında faydalı bilgilerle donatacak yöntemlere ihtiyaç vardır.

5

Yanılgı: **Kendimizi siber suçtan korumak için en iyi profesyonelleri işe almamız gerekiyor.**

Gerçek: **Siber güvenlik sadece bir departmanın işi değil, kurumsal bir anlayıştır.**

Siber güvenlik genellikle alanında uzman profesyonellerden oluşan bir departmanın sorumluluğu olarak görülüyor. Bu düşünce yapısı yanlış bir güvenlik algısıyla sonuçlanarak organizasyonun daha geniş zemine yayılan sorumluluklar almamasına yol açabilir.

Bu noktadaki asıl zorluk, siber güvenliği genele yayılan temel bir yaklaşıma dönüştürebilmektir. Örneğin siber güvenlik, bazı durumlarda ücretlendirme politikalarıyla bile bağlantılandırılan bir İK politikası olmalıdır. Bu aynı zamanda, çoğunlukla yapıldığının aksine sadece güvenlik projelerinin sonunda değil, yeni BT sistemleri geliştirme sürecinde de siber güvenliğe en yüksek önemi vermek gerektiği anlamına gelir.

03 Çözüm kişiselleştirmekten geçiyor

Yerel bir girişimci ile çok uluslu küresel bir şirketin karşılaşabileceği siber suç riskleri birbirinden çok farklıdır. Yerel bir girişimci, siber suçu tespit etmek veya önlemek için gereken kaynaklara veya uzmanlığa sahip olmayabilir. Çok uluslu küresel bir şirket suçlular için daha cazip bir hedeftir, zira daha göz önündedir, BT'ye daha fazla bağımlıdır ve çok daha değerli varlıklara sahiptir.

Ancak her iki işletme de kuruluş yapısını, risk iştahını ve sahip olduğu bilgileri temel alarak özelleştirilmiş bir siber güvenlik yaklaşımı benimsemelidir. Bir kuyumcunun, varlıklarını korumak amacıyla stratejik, gerçekçi ve özelleştirilmiş bir yaklaşım kullanarak gerekli güvenlik seviyesine nasıl ulaştığını değerlendirin. Ardından bunu siber güvenlikle ilgili mevcut genel kurumsal yaklaşımla karşılaştırın.

Hırsızlığa karşı korunmaya dair kuyumcu perspektifi	Siber güvenliğe dair kurumsal perspektif
Hangi varlıkları koruyacağımı biliyorum ve gerekli tedbirleri aldım.	Korunması gereken varlıklarla ilgili net bir fikrim olmadan bazı tedbirler alıyorum.
Hırsızlığı işimin barındırdığı risklerden biri olarak görüyor ve %100 güvenlik istiyorsam bu işi yapmamam gerektiğini düşünüyorum.	Siber suçu değişik bir konu olarak görüyor ve %100 güvenlik elde etmeye çalışıyorum.
Bir insanın değerli malları çalıp gitmesini önlemeye yönelik tedbirlere odaklanıyorum.	Bir insanın işletmeye girmesini önlemeye yönelik tedbirlere odaklanıyorum ve bilgi çalmasını önlemeye yönelik tedbirleri unutuyorum.
Güvenlik hizmeti tedarikçilerinin beni etkilemesine izin vermiyor, kendi satın alma kararlarımı kendim veriyorum.	Güvenlik politikam piyasadaki araçlara dayanıyor ancak tam olarak neye ihtiyacım olduğunu bilmiyorum.
İşler ters gittiğinde veya böyle bir tehlikeyle karşılaştığımda bundan dersler alıyorum.	İşler ters gittiğinde veya böyle bir tehlikeyle karşılaştığımda paniğe kapılıyorum.
Hırsızlık riskinin azaltılması konusunda çalışanlarımı eğitiyor ve bir yanlış yaptıkları zaman onlarla konuşuyorum.	Siber güvenliğin büyük ölçüde uzman profesyonellerle ilgili bir konu olduğunu düşünüyor ve kuruluşun geri kalanına bu konuyla ilgili bir yük yüklemek istemiyorum.
İşimin sürekliliğini desteklediklerinden gerekli araçlara yatırım yapıyorum.	Yasal açıdan zorunlu olduğu ve medyada her gün yeni güvenlik olayları yayımlandığı için güvenlik araçlarına yatırım yapıyorum.

04 Siber olgunluğun altı boyutu

Yönetim olarak, kuruluşunuzun siber güvenlik yaklaşımının yeterli olup olmadığını bilmek istersiniz. KPMG olarak, bir kuruluşun siber olgunluğu hakkında kapsamlı bir bakış açısı sunan altı temel boyutu ele alıyoruz.

Liderlik ve kurumsal yönetim

Yönetim kurulu risk hakkında gerekli durum tespitini yapıyor, riski sahipleniyor ve etkin şekilde yönetiyor mu?

İnsan faktörü

Doğru kişileri, becerileri, kültürü ve bilgiyi destekleyip bunlardan faydalanılmasını sağlayan güvenlik kültürünün seviyesi ve entegrasyonu nedir?

Bilgi güvenliği risk yönetimi

Bilgiyle ilgili risk yönetiminin tüm kuruluşunuz, hizmet sunduğunuz ve hizmet aldığınız ortaklarınız tarafından kapsamlı ve etkin bir şekilde yapılmasını sağlamaya yönelik yaklaşımınız ne kadar sağlıklı?

İş sürekliliği

Bir güvenlik olayına karşı gerekli hazırlıkları yaptınız mı? Başarılı bir kriz ve paydaş yönetimi aracılığıyla böyle bir olayın önlenmesi veya etkilerinin en aza indirilmesi kabiliyetine sahip misiniz?

Operasyonlar ve teknoloji

Belirlenmiş riskleri ele almak ve olası olumsuz etkileri en aza indirmek için uygulanan kontrol tedbirlerinin seviyesi nedir?

Kanun ve mevzuata uyum

İlgili düzenlemelere ve uluslararası sertifikasyon standartlarına uyuyor musunuz?

Bu altı temel boyutun da gerektiği gibi ele alınması bütüncül bir siber güvenlik modeliyle sonuçlanarak kuruluşa şu avantajları sağlar:

- Dışarıdan bir siber saldırganın kuruluşa saldırması riskinin en aza indirilmesi ve başarılı saldırıların etkilerinin sınırlandırılması
- Karar alma sürecini kolaylaştırmak için siber suç trendleri ve olayları hakkında daha fazla ve doğru bilgi alınması
- Siber güvenlik konusundaki mesajın tüm çalışanlara net bir şekilde iletilmesi suretiyle herkesin sorumluğunu öğrenmesi ve bir olay yaşandığında veya böyle bir şüphe olduğunda ne yapacağını bilmesi
- Siber güvenlik konusunda hazırlıklı olan ve gerekenleri yapan bir kuruluşun tüm paydaşlarına daha fazla güven vermesinden dolayı kurumsal itibarın artırılması
- Siber güvenlik hakkında daha fazla yeterlilik bilgisi
- Kuruluşun siber güvenlik alanında benzer şirketlerle karşılaştırılması

05 Eyleme geçmeye hazır mısınız?

Siber güvenlik mutlaka gündeminizde olmalıdır. Yöneticileriniz, yönetim kurullarınız, hissedarlarınız ve müşterileriniz bu sorunla yeterince ilgilenmenizi bekliyor.

Sadece sorunu biliyor olmanız eylem için hazır olduğunuz anlamına gelmez.

Üst yönetimin liderliğinde stratejik, özelleştirilmiş ve kapsamlı bir siber güvenlik programı geliştirmek, en yaygın beş siber güvenlik yanılgısına düşmemek konusunda size yardımcı olacaktır.

1. "%100 güvenliği sağlamak zorundayız"
2. "Sınıfının en iyisi teknik araçlara yatırım yaparsak güvende oluruz"
3. "Elimizdeki silahlar bilgisayar korsanlarının silahlarından daha güçlü olmalı"
4. "Siber güvenlik konusunda mevzuata uyum tamamen etkin gözetimle ilgili bir durum"
5. "Kendimizi siber suça karşı korumak için en iyi profesyonelleri işe almamız gerekiyor"

Siber güvenlik konusunda bütüncül bir yaklaşım benimsediyseniz ve yaklaşımınız hakkında şu soruları yanıtlayabiliyorsanız **harekete geçmeye hazırsınız demektir!**

1. **Kendi şirketinizin ve iş yaptığınız kuruluşların karşılaşabileceği risklerin büyüklüğünü biliyor musunuz?**
   - Kuruluşunuz potansiyel siber suçlular için ne kadar cazip bir hedef?
   - Kuruluşunuz; iş ortaklarının, tedarikçilerin ve diğer kuruluşların sunduğu hizmetlere ne kadar bağımlı durumda ve ilgili BT süreçleri birbirleri ile ne derinlikte bütünleşmiş durumda biliyor musunuz?
   - Hem süreçler hem de sistemler bazında siber güvenlik bakımından kritik varlıklarınızı net olarak ortaya koydunuz mu?
   - %100 güvenlik diye bir şey olmadığı gerçeğini dikkate aldığınızda, bu süreçlerle ve/veya sistemlerle ilgili ne kadar risk almaya hazır olduğunuzu düşündünüz mü?
   - İş ortaklarınız da sizinle aynı risk iştahına ve siber güvenlik tedbirlerine sahip midir, farkında mısınız?
   - Siber güvenlik yatırımlarınız için net olarak olay ve/veya bazlı incelemeler geliştirdiniz mi?

2. Kurumsal yönetim süreçleriniz ve stratejileriniz, organizasyonun kültürü ile birlikte etkin bir risk yönetimine imkân sağlayabiliyor mu?

- Etkin bir siber güvenlik anlayışına organizasyon kültürünüzün katkısını (veya zararını) ölçebilir misiniz?
- Yönetim kurulunuz siber güvenliğin önemi hakkında çalışanlarla en son ne zaman iletişim kurdu?
- Bir kriz veya vaka durumunda harekete geçmek için hazır mısınız? İlgili mesajların nasıl ve kim tarafından iletilmesi gerektiğini biliyor musunuz?
- Siber güvenlik politikanız hakkında paydaşlarınıza güvence sağlayabiliyor musunuz?

3. Siber güvenlik bütçeniz ne kadar büyük olmalı ve bu bütçeyi nasıl harcamalısınız?

Kuruluşunuzun risk profiline bağlı olarak, siber güvenlik bütçeniz toplam BT bütçenizin yaklaşık %3'ü ila %5'i arasında olmalıdır. Günümüzde bu bütçenin önemli bir kısmı genellikle teknolojik çözümler uygulamaya ve geçmişte yaşanmış sorunları çözmeye harcanıyor. Yanıtlamanız gereken temel soru şu:

- Toplam BT bütçenizin en az %3'ü ila %5'i siber güvenliğe ayrılmış mı?
- Siber güvenlik bütçenizin ne kadarı geçmişte yaşanmış sorunları çözmek için harcandı?
- Daha iyi güvenlik sistemlerine yönelik yapısal yatırımlara ne kadar yatırım yapıldı?
- Sistemlere ve uygulamalara ne kadar yatırım yapıldı?
- Farkındalık ve kültür değişimine ne kadar yatırım yapıldı?

İletişim:

Hakan Aytekin
Danışmanlık, Şirket Ortağı,
KPMG Türkiye
E : hakanaytekin@kpmg.com

Tanıl Durkaya
Bilgi Teknolojileri Danışmanlığı
Şirket Ortağı, KPMG Türkiye
E : tdurkaya@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