KPMG

# Denetim komiteleri için Siber Güvenlik

**Denetim Komitesi Enstitüsü Serisi 7**

kpmg.com.tr
kpmgdenetimkomitesi.com

Şirketlerin güçlü bir siber güvenlik korunma sistemine sahip olmasında denetim komitelerine önemli bir görev düşüyor. Bu görevi yerine getirmek için yapılması gereken, ilgili teknolojileri detaylarıyla bilmek değil, yönetim ve politika belirleme alanlarında liderlik etmek. Son yıllarda hem devlet kurumları hem de özel işletmelerin karşı karşıya kaldıkları siber saldırıların sayısı ve boyutu sürekli büyüyor. Yani bu sorun "bekle ve gör" yaklaşımının ötesinde bir ilgi bekliyor.

**Öncelikle aşağıdaki sorulara cevap verebilmek gerekiyor:**

- Korunması gereken en önemli varlıklar neler?
- Bu varlıklar nasıl korunuyor?
- Bunların korunmasından kim sorumlu?
- Kabul edilebilir siber güvenlik risk seviyesi nedir?
- Büyük bir siber güvenlik olayı gerçekleşse şirket nasıl tepki verirdi?

**Bu sorulara verilecek hazır cevaplarınız yoksa, bilin ki yalnız değilsiniz. Ancak, siber güvenlik konusunda denetim komitelerinden beklentiler gün geçtikçe artıyor.**

# Tehdit nereden geliyor?

Sanal dünya, organize suç örgütleri açısından oldukça cazip bir ortam. Suçlular bilgisayar sistemlerindeki açıkları kullanarak bilgisayarlara uzaktan erişip onları uzaktan kontrol edebiliyor, klavye vuruşlarını ve ekran görüntüsünü kaydedebiliyor ve bilgisayar kullanıcılarını manipüle ederek hassas bilgilere erişebiliyor. Sanal dünyada saldırganlar saldırılarını birden fazla ülke veya bölge üzerinden yönlendirerek gerçek konumlarını gizleyebiliyor, bu da yapılan soruşturmaları ve kanunların uygulanmasını zorlaştırıyor.

Kötü niyetli çalışanlar, hassas şirket bilgilerini kolaylıkla toplayıp şirket dışına çıkarabildikleri gibi, şirketin veri tabanlarını bozacak veya ağ operasyonlarını sabote edecek kötü amaçlı yazılımları sisteme bulaştırabiliyorlar.

Şirketlerin rakipleriyle ilgili siber casusluk faaliyeti gerçekleştirmesi de sıkça rastlanır hale geldi. Saldırılarda genellikle fikri mülkiyet haklarıyla korunan hassas bilgiler hedef alınıyor. Büyük şirketlerin aylarca saldırı altında oldukları halde bunu fark etmedikleri ve sonuçta çok büyük miktarda hassas veri hırsızlığının gerçekleştiği durumlar da görülebiliyor.

Siyasi eylemler de artık sanal dünya üzerinden yapılır hale geldi. Sabotajlar ve hizmet dışı bırakma saldırıları gittikçe daha sık gerçekleşiyor. Geçmişte bu tür saldırıların çoğu Anonymous gibi "hacktivist" olarak tanımlanan gruplara atfedilirdi, ancak son zamanlarda siyasi gayeler güden ve Orta Doğudaki çatışmalarla bağlantılı gruplar da etkinliğini artırmaya başladı.

# Siber güvenlik ihlalinin sonuçları

Siber güvenlik ihlalleri:

- Suistimal, hırsızlık ve gasp yoluyla finansal sistemleri ve varlıkları,
- Casusluk yoluyla fikri mülkiyet haklarını ve ticari sırları,
- Karalama, hakaret, suçlama, sırları ifşa etme gibi yollarla markayı ve internetteki varlığını ve
- Sabotaj veya operasyonlarda kesintiye neden olma yoluyla iş sürekliliğini etkileyebilir.

# Denetim komitesinin rolü

Kurumsal Yönetim İlkelerine göre şirketlerin iç kontrol ve iç denetim sistemlerinin gözetim sorumluluğu, denetim komitesine aittir.

KPMG'nin tüm dünyada gerçekleştirdiği 2015 Küresel Denetim Komitesi Anketi'nin verileri, denetim komitesi üyelerinin %40'ının siber güvenlik ile ilgili risklere daha fazla zaman ayırmaları gerektiğini düşündüklerini ortaya koydu. "Siber güvenlik konusunda kendilerine sağlanan bilginin kalitesi" hakkında değerlendirme yapmaları istendiğinde, katılımcıların sadece yüzde 10'u kalitenin çok iyi olduğunu, yüzde 49'u genellikle iyi olduğunu ama zaman zaman sorunların yaşandığını, yüzde 41'i ise gelişime ihtiyaç olduğunu belirtti. Bu oran, ankette test edilen 12 risk alanı içinde kaydedilen en yüksek memnuniyetsizlik oranı.

Dünyanın dört bir tarafında hükümetler siber güvenliğin sadece kamu sektörü kurumları, askeri kurumlar ve kritik ulusal altyapı kuruluşları için değil, özel sektör şirketleri için de gittikçe artan bir öneme sahip olduğunun farkında.

Ülkeler siber güvenliklerini sağlamak amacıyla idari yapılanmalar gerçekleştirmekte, teknik önlemler almakta ve hukuki altyapılar hazırlamaktalar. Konunun önemi dikkate alınarak ülkemizde de "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Siber Güvenlik Kurulu" oluşturulmuştur. Siber Güvenlik Kurulu'nun ilk toplantısında "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilmiştir. Söz konusu eylem planı kapsamında temel görevi koordinasyon ve işbirliği olan Ulusal Siber Olaylara Müdahale Merkezi (USOM) 27 Mayıs 2013 tarihinde kurularak, faaliyetlerine başlamıştır. Yine söz konusu eylem planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulması öngörülmüştür.

> "Bilgisayar korsanlarının hedefinde sadece bankalar yok."

## Başkalarının riski

Şirketler, kendilerinin siber suçlular açısından önemli bir hedef olmadıkları düşüncesiyle, korunma tedbirlerine yeterince yatırım yapmayabiliyorlar. Stratejik ve Uluslararası Araştırmalar Merkezi'nin kısa süre önce yayınladığı "Net Kayıplar: Siber Suçların Küresel Maliyeti" raporuna göre, internetteki yolsuzluk ve casusluk faaliyetleri, 375 ila 575 milyar dolar arası bir kayba yol açtı. 20'den fazla ülkede ATM'lerden 45 milyon dolar çalan küresel bilgisayar korsanı ağı gibi örnekler daha çok ön plana çıkıyor, ancak bilgisayar korsanlarının hedefinde sadece bankalar yok. Geçtiğimiz yıllarda bir çok üretim ve hizmet şirketinin de sofistike ve istikrarlı siber saldırılara maruz kaldığı, sistemlerine izinsiz girildiği, milyonlarca müşterinin kişisel bilgilerinin çalındığı gibi haberler basına yansımıştı. Bu ve benzeri saldırılarda hem büyük mali sonuçlar ortaya çıkmış, hem de ciddi itibar kayıpları yaşanmıştı.

Bu örnekler, farklı gayelerle hareket eden siber suçlular açısından bütün şirketlerin cazip birer hedef olabileceğini gösteriyor.

Casusluğun sadece James Bond filmlerinde olduğunu düşünürüz, ancak rakiplerden kaynaklanan casusluk faaliyetlerine karşı kendini korumak günümüzde birçok şirket için günlük hayatın bir parçası haline geldi. Siber saldırılarda fikri mülkiyet hakları sistematik bir şekilde hedef alınıp çalınıyor. 2015 yılının Aralık ayı içerisinde yapılan yurtdışı kaynaklı olduğu iddia edilen saldırılar neticesinde Türkiye'de özellikle ".tr" uzantılı sitelere girmek isteyenler etkilendi. 14 Aralık 2015'te başlayan ve yaklaşık 10 gün süren bu saldırılar e-ticaret sitelerini ve bazı bankaların web sitelerini, internet üzerindeki pos sistemlerini geçici olarak kullanılmaz hale getirdi.

Geçtiğimiz günlerde ise bilgisayar korsanları tarafından internete sızdırılan veri tabanındaki 49 milyon 611 bin 709 vatandaşın kişisel bilgilerinin Türk vatandaşlarına ait kimlik bilgileri olduğu iddia edildi.

Bu iddialar pek çok farklı kaynak tarafından doğrulandı. Bu olaylar, sorumluların tespit edilebileceği altyapının önemini de gündeme getiriyor.

Bir ülkenin kritik ulusal alt yapısının parçası olan şirketler, başka ülkelerin veya teröristlerin hedefi haline gelebilir. Uluslararası ilişkilerde gerilimin yükseldiği dönemlerde siber saldırı sayısında da artış yaşanıyor. Geçtiğimiz yıllarda ABD'yi, İsrail'i, Pakistan'ı, Hindistan'ı ve Güney Kore'yi hedef alan siyasi güdümlü saldırılar bunun örnekleri.

Siyasi veya sosyal bazı hedefler için bilgisayar korsanlığı yapan "hacktivistler" de şirketleri hedef alabiliyor. Böyle durumlarda saldırganlar şirketin mali açıdan kıymetli verilerine erişmek veya üretiminde kesintiye neden olmaktan ziyade, şirketin itibarına zarar vermeyi veya şirketi strateji değişikliğine zorlamayı hedefliyor.

Organize suç örgütleri de şirketlere şantaj yapmak için siber saldırı gerçekleştirebiliyor. Borsalar ve internet üzerinden ticaret yapılan platformlar bu tür saldırıların hedefi olabiliyor.

Şirketlerin sadece asli faaliyetlerini yürüten birimleri değil, insan kaynakları, finans ve iş geliştirme gibi destek birimleri de dahil olmak üzere bütün birimleri siber saldırıya maruz kalabilir. Otomasyonun yaygın bir şekilde kullanılması sonucu, bilgisayarlar günümüzde sadece bilgi işlemde değil, endüstriyel süreçlerin, binaların ve altyapıların kontrolünde de ilk bakışta fark edilmeyen önemli bir rol oynuyor.

Saldırganlar şirketin sistemlerine bir müşterinin veya tedarikçinin BT altyapısı vasıtasıyla sızabilecekleri gibi, çalışanların ev bilgisayarları veya cep telefonları vasıtasıyla da sızabilirler. Satın alma veya birleşme gibi yeniden yapılanma sürecinden geçmekte olan şirketler, piyasanın hassas olması, çalışanların moral durumu, ağ ayarlarının yeniden yapılması ve şirket dışından danışmanların da sürece dahil olması gibi nedenlerle saldırıya daha açık hale gelebilir.

Siber güvenlik sadece teknik bir konu değil. Siber güvenliğin sağlanması için siber olaylara karşı hazırlıklı olmayı, korunmayı, böyle olayları tespit etmeyi ve gerektiğinde tepki vermeyi içeren entegre bir yaklaşımın benimsenmesi şart.

## Güvenlik ve maliyet arasında doğru dengeyi tutturmak

"Mutlak güvenlik" çok gerçekçi bir yaklaşım olmayabilir. Yeterli kaynaklara sahip kararlı bir düşman, bilgi güvenliğinde, fiziksel güvenlikte veya çalışanlarda zayıf bir nokta bulup en güçlü güvenlik sistemlerini bile eninde sonunda aşabilir. Şirketler önemli varlıklarını siber saldırılardan koruyacak önlemleri alırken bunun maliyetini de hesaba katmak zorunda.

Siber tehditlerin şirketin risk yönetimi ve kurumsal yönetim çerçevesinin bir parçası olarak ele alınması ve şirketin önemli varlıklarına veya iş süreçlerine yönelik siber saldırı riskine, risk değerlendirmelerinde yer verilmesi gerekir.

Birçok şirket, siber saldırıyla baş edebilme kabiliyetlerini test etmek için saldırı senaryoları üzerinde çalışıyor. Bu senaryolarda olası bir saldırganın saldırma nedenleri ve neyi başarmak istediği, saldırının hangi şartlarda gerçekleştirilebileceği ve saldırganın kullanabileceği teknikler ele alınıyor.

Yönetim kurullarının muhtemel senaryoları değerlendirirken her türlü ihtimali dikkate almaları ve şirketin siber güvenliğini farklı yönlerden test edebilmek için birden fazla senaryo kullanmaya hazırlıklı olmaları gerekiyor.

## Siber güvenliğin iyi olması ne demek?

Şirket ağlarını korumak üzere gerekli anti-virüs yazılımlarını kurmak, güvenlik duvarı oluşturmak, siber olay yönetimi politikası oluşturmak ve kullanıcı eğitimine ve farkındalığa önem vermek gibi temel konularda hata yapmamak önemli. Bu adımlar tabi ki bütün saldırıları durdurmaz, ancak birçoğunu engelleyeceği de kesin.

Siber güvenlik önlemlerinin merkezinde, yönetim kurulunun sorumluluğunda olan bilgi riski yönetimi yatar, yani şirketin en önemli bilgi varlıklarının neler olduğunu anlamak ve bu varlıklara yönelik riskleri yönetmek.

Siber güvenliği artırma projelerinde, insan faktörünü, kültürü, iş süreçlerini ve teknik güvenlik tedbirlerini beraberce ele alacak bütüncül bir yaklaşım benimsenmeli.

Siber güvenlik sadece teknik bir konu değil. Siber güvenliğin sağlanması için siber olaylara karşı hazırlıklı olmayı, korunmayı, böyle olayları tespit etmeyi ve gerektiğinde tepki vermeyi içeren entegre bir yaklaşımın benimsenmesi şart.

Çalışanlar farkında olmadan en büyük güvenlik açığını oluşturuyor olabilirler, bu yüzden doğru davranışları teşvik etmek için teknik eğitim ve farkındalık eğitimi verilmesi büyük önem taşıyor. Siber güvenlik sisteminin etkinliğini takip edecek bir yönetim yapısının oluşturulması ile, siber tehditleri takip ederek daha iyi risk kararlarının alınmasını sağlayacak bir araştırma sisteminin kurulması da en iyi uygulamalar arasında.

## Bizim görüşümüz: bugünün ve yarının görünümü

Şirketlerin hassas verilerine erişmek için şirket çalışanlarını hedef alan sofistike organize suç örgütlerinin sayısında büyük bir artış var. Asıl siteyi taklit ederek ziyaretçileri tuzağa düşüren ve zararlı programlar içeren "Truva atı" sitelerinin sayısında da büyük bir artış var. Bu siteleri kullanan korsanların amacı kullanıcıların kötü niyetli yazılım yüklemesini sağlayarak şirket ağlarına erişim sağlamak.

Gelecekte ne gibi yeni tehditler ortaya çıkarsa çıksın karşılaşacağımız en büyük zorluk, gittikçe hayatın her alanına yayılan mobil cihaz ve benzer teknolojilerin güvenliğini sağlamak olacak. Bulut bilişim hizmetlerinin güvenliğinin sağlanması da gittikçe daha fazla önem kazanacak. Son olarak, sanal dünyanın daha saldırgan hale gelmesi de önemli bir konu. Bu durum, şirketler ve tüketiciler gibi kullanıcılar açısından internetin değerini azaltma potansiyeline sahip.

> Daha hızlı tepki vermeye odaklanmak gerekiyor.

## Değerleri korumak

Şirketin siber güvenlik konusundaki yeterliliğinin bağımsız bir şekilde değerlendirilmesi birçok farklı yolla yapılabilir. Örneğin, şirketin siber güvenliğini hem teknik güvenlik tedbirleri açısından, hem de genel bilgi riski yönetimi ve siber güvenlikle ilgili yönetim çerçevesi açısından ele alarak sistematik bir şekilde inceleyen siber olgunluk değerlendirmesi gerçekleştirilebilir.

Belirli güvenlik süreçlerine ve kontrol tedbirlerine odaklanarak bunların bağımsız bir şekilde değerlendirilmesi, test edilmesi ve sertifikalandırılması yoluna da gidilebilir. Bu adımların her biri şirketin siber güvenliğini artırabilir, ancak şirket ile ilgili kabul edilebilir risk seviyesinin ne olduğunu tartışmak ve bu konuda bir karara varmak sonuçta yönetim kurullarının görevidir.

Siber güvenliğin hızla değişen niteliği, şirketlerin suçlulardan bir adım önde olmak için hem stratejik anlamda hem de finansal anlamda daha fazla yatırım yapmaları gerektiği anlamına geliyor. Siber güvenliği güçlendirmek demek birbiri ardına daha fazla güvenlik duvarı dikmek olmamalı, bunun yerine tepki verme hızını artırmaya ve yeni gelişen tehditlerle baş etmek için gerekli kabiliyetleri güçlendirmeye odaklanmak gerekiyor. Olası zararları en aza indirmek için, herhangi bir ihlal olduğunda bunu gecikmeden fark edebilmek de büyük önem taşıyor.

Bazı şirketler bu konuyu çok ciddiye alarak siber riskleri anlamak için yatırım yapıyorlar ve risk azaltma konusunda pragmatik bir yaklaşım benimsiyorlar. Bazı şirketler ise konuya gereken önemi vermeyerek fikri mülkiyet haklarının rakiplere kaptırılması, müşterilerin gözündeki itibarlarının zarar görmesi ve mali kayıplar da dahil olmak üzere pek çok alanda ciddi bir risk alıyorlar.

# Denetim komitelerinin dikkate alması gereken siber güvenlik konuları

**Siber tehditler şirketin risk yönetimi sürecinin bir parçası olarak ele alınmalı ve denetim komitesi aşağıdaki kontrolleri gerçekleştirmeli:**

- Şirket siber saldırılardan korumak istediği en kıymetli bilgi varlıklarının hangileri olduğuna karar verdi mi? (örneğin, finansal veriler, operasyon verileri, çalışanlarla ve müşterilerle ilgili bilgiler, fikri mülkiyet hakları)
- Yurtdışındaki faaliyetler de dahil olmak üzere şirketin varlıklarına yönelik tehditleri anlamak için gerekli bilgi toplama süreçleri var mı?
- Siber saldırı risklerinin seviyesini tespit etmek ve şirket açısından kabul edilebilir risk seviyesinin ne olduğuna karar vermek için kullanılan bir yöntem var mı?
- Siber saldırılara karşı hazırlanmak, sistemleri korumak, saldırıları tespit etmek, saldırılara tepki vermek ve saldırının sonuçlarını yönetmek için gerekli kontroller mevcut mu?
- Siber güvenlik kontrollerinin etkinliği takip ediliyor mu? Gerektiğinde bağımsız kuruluşlarca test edilmesi, incelenmesi ve onaylanması sağlanıyor mu?
- Değişen siber tehditlere ayak uydurmak için güvenlik sistemi sürekli iyileştiriliyor veya gerekiyorsa dönüştürülüyor mu? Bu amaçla performans ölçümleri yapılıyor mu?

# İletişim:

**KPMG Türkiye**
**Denetim Komitesi Enstitüsü**

**Şirin Soysal**
KPMG Türkiye
Denetim Komitesi Enstitüsü Başkanı,
Şirket Ortağı
T: +90 216 681 90 19
F: +90 216 681 90 90
E: ssoysal@kpmg.com

**Kuğu Alper**
KPMG Türkiye
Denetim Komitesi Enstitüsü Koordinatörü
T: +90 216 681 92 99
F: +90 216 681 90 90
E: kalper@kpmg.com

**İstanbul**
Rüzgarlıbahçe Mh. Kavak Sk. No:29
Kavacık 34805 Beykoz / İstanbul / Türkiye
T: +90 216 681 9000

**Ankara**
The Paragon İş Merkezi Kızılırmak Mah. Ufuk
Üniversitesi Cad. 1445 Sok. No:2 Kat:13
Çukurambar 06550 Ankara / Türkiye
T: +90 312 491 7231

**İzmir**
Heris Tower, Akdeniz Mah. Şehit Fethi Bey Cad.
No:55 Kat:21 Alsancak 35210 İzmir / Türkiye
T: +90 232 464 2045

**kpmgdenetimkomitesi.com**
**kpmg.com.tr**
**kpmgvergi.com**