TONE at the TOP®

Üst yönetime, yönetim kurullarına ve denetim komitelerine yönetişimle ilgili konularda kısa ve öz bilgiler sunar

Sayı 125 | Ekim 2024

Siber Dayanıklılıkta Yönetim Kurulunun Rolü

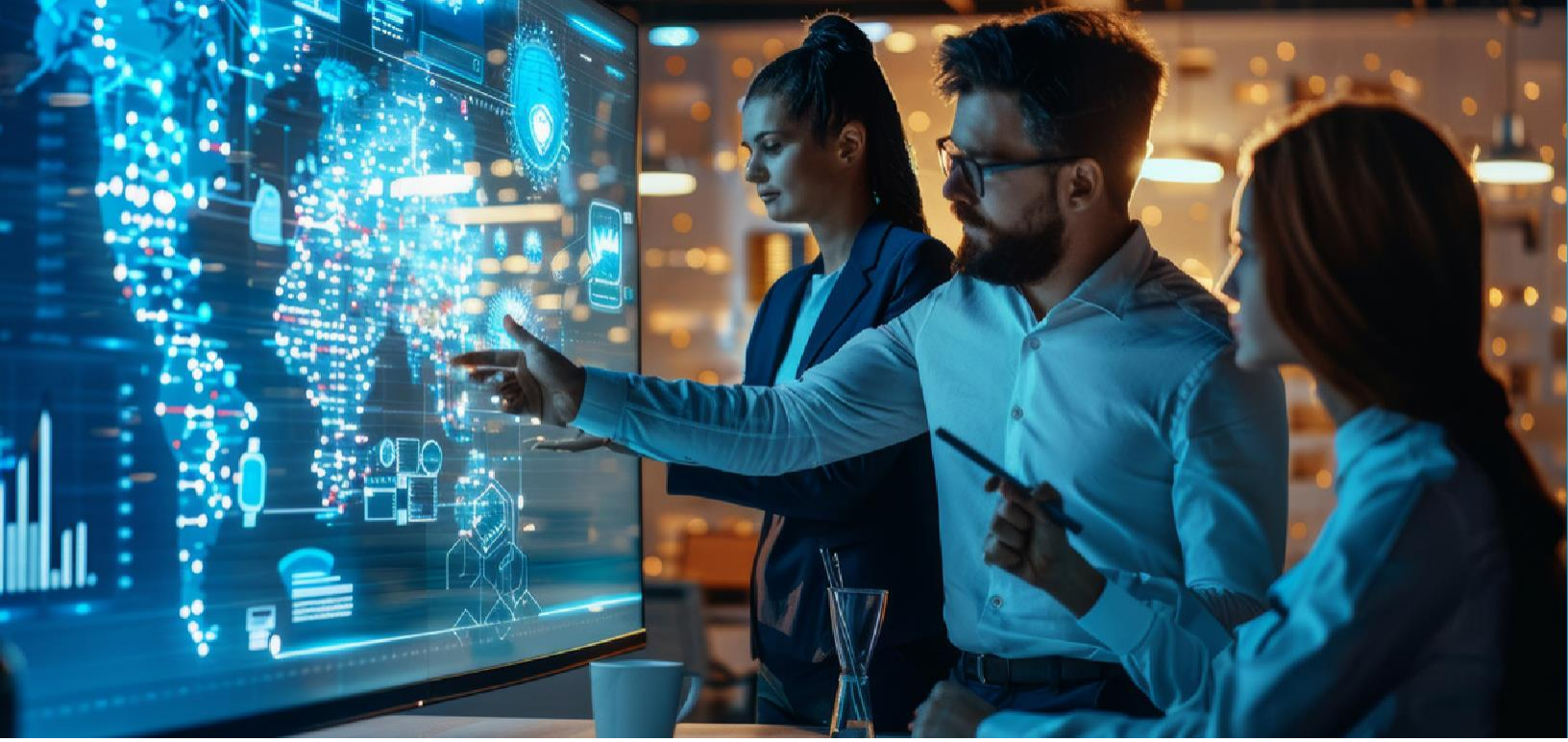
Şirketiniz bir sonraki siber saldırıya hazır mı? **2024 Cisco Siber Güvenlik Hazırlık Endeksi**'ne göre, çoğu kurum gelecekte böyle bir olayın yaşanmasını bekliyor ve iş dünyası ve siber güvenlik liderlerinin %73'ü önümüzdeki 12 ilâ 24 ay içinde bir siber olayın faaliyetlerini sekteye uğratacağını öngörüyor.

Bir siber saldırının hassas verilerin açığa çıkması, operasyonların kesintiye uğraması ve üçüncü taraflarla ilişkilerin ve şirketin itibarının zarar görmesi de dâhil olmak üzere birçok potansiyel sonucu vardır. IIA'nın yayınladığı **2025 Risk in Focus** raporunda, iç denetim liderleri siber güvenliğe büyük bir farkla en yüksek risk derecesini vermektedir. Aynı zamanda, siber güvenliği iç denetimin en çok zaman ve çaba harcadığı alan olduğunu da belirtmektedirler.

Bu rapora göre, siber güvenlik liderlerin kurumlarının bundan üç yıl sonra karşılaşmasını bekledikleri en önemli risk olmaya devam ederken, dijital bozulma (yapay zekâ (AI) dâhil) geçmiş anketlerde bulunduğu noktadan hızla yükselerek ikinci sıraya yerleşmiştir. Raporda, "Yapay zekâ dünya genelinde siber güvenlik ve suistimal risklerini artırıyor" denmektedir. Siber güvenlik, yapay zekanın en fazla olumsuz etki yaratacağı alan olarak değerlendirilmiştir.

Bir saldırının gerçekleşip gerçekleşmeyeceğinden ziyade ne zaman gerçekleşeceğinin önemli olduğu bir ortamda, siber dayanıklılık şirketlerin bir olayı atlatmasına yardımcı olmak açısından kritik önem taşımaktadır. Şirketler kendilerini siber saldırılara karşı korumak için büyük çaba sarf edebilirler ancak aynı zamanda bu tür saldırılara yanıt vermeye ve bu saldırılardan kurtulmaya da hazırlıklı olmalıdırlar.

Siber dayanıklılık "siber kaynakları kullanan veya siber kaynaklar tarafından etkinleştirilen sistemlerdeki olumsuz koşulları, gerilimleri, saldırıları veya tehlikeleri öngörme, bunlara dayanma, bunlardan kurtulma ve bunlara uyum sağlama yeteneğidir. Siber dayanıklılık, siber kaynaklara bağlı olan görev veya iş hedeflerinin, mücadele edilen bir siber ortamda gerçekleştirilmesini sağlamak amacıyla tasarlanmıştır." — Ulusal Standartlar ve Teknoloji Enstitüsü.



Yönetim Kurullarından Yeni Beklentiler

Düzenleyiciler ve hissedarlar, yönetim kurulunun siber güvenlik konusundaki sorumluluğunu incelemekte ve yönetim kurulu üyelerinin kurumlarının güvenlik açıklarını gözetip denetlemesine yönelik yeni beklentiler ortaya koymaktadır. ABD Menkul Kıymetler ve Borsa Komisyonu **Siber Güvenlik Risk Yönetimi, Strateji, Yönetişim ve Olay Açıklamaları** başlıklı nihai bir kural kapsamında, halka açık şirketler için, özellikle de önemli siber güvenlik olaylarına ilişkin açıklamaları ve kayıtlı şirketlerin bu riskleri nasıl değerlendirdiği, tanımladığı ve yönettiğinin yanı sıra yönetimin bunların değerlendirilmesi ve yönetilmesindeki rolü hakkında periyodik açıklamaları ele alan gerekli ekleri ortaya koymaktadır. Bu nihai kurallar, yönetim kurullarının siber güvenlik risklerine yönelik gözetimi hakkında açıklama yapılmasını da gerektirmektedir.

"Yönetim Kurulları: Endüstriler için Nihai Siber Güvenlik Savunması (Boards of Directors: The Final Cybersecurity Defense for Industrials)" başlıklı McKinsey makalesinde, yönetim kurulları gözetim rollerinin bir parçası olarak yöneticilerin ve ekiplerinin siber güvenlik konusunda yüksek bir standart belirlemelerini sağlamalıdır. Ardından, hedeflerin gerçekleştirilip gerçekleştirilmediğini ve ekiplerin siber güvenlik konusunda sorumluluk alıp almadığını tespit ederek siber güvenlik çaba ve çalışmalarını izlemelidirler. "Yönetim kurulu, bu tür girişimlerin planlanmasını ve finanse edilmesini sağlayan son savunma hattıdır," diye belirtilmektedir.

Bir siber saldırı, kurumların işlerini olağan şekilde sürdürmelerini zorlaştırmak için tasarlanır. Siber dayanıklılık, bilgi sahibi olmayı ve hazırlıklı olmayı ifade eder, böylece bir kriz durumunda seçenek ve öncelikler net olur. PwC'nin **Siber Risk Gözetimi: Yönetim Kurulunun Rolü (Overseeing Cyber Risk: The Board's Role)** yayınına göre, yönetim kurulları kurumlarının iyi hazırlanmasını sağlamak amacıyla yönetimin masaüstü tatbikatlarında periyodik olarak test ettiği belgelenmiş kriz yönetimi, olay tepkisi ve felaket kurtarma planları olup olmadığını tespit etmelidir.

Birçok yönetim kurulu, yönetimden güncel riskleri ve siber güvenlik hedeflerine yönelik kaydedilen ilerlemeyi gösteren bir siber puan kartı veya gösterge tablosu almaktadır. PwC, yönetim kuruluna sunulacak raporda yer alabilecek birkaç alana işaret etmektedir:

- *Çok yıllık stratejik plan ve cari yıl iş planı.*
- *Finansman ve çalışan temelinde bölünerek detaylandırılmış siber güvenlik kaynak tahsisi ayrıntıları.*
- *Örneğin **NIST Siber Güvenlik Çerçevesi** gibi tanınmış bir çerçeveye göre ölçülen olgunluk değerlendirmesi.*
- *Görev açısından kritik sistemlerin düzenli olarak güncellenen envanteri.*
- *Kurum için anahtar siber risklerin özeti.*
- *Kurumun deneyimlediği önemli güvenlik olaylarına ilişkin gözden geçirme.*
- *Çalışan eğitimi ve farkındalık çalışmaları hakkında bilgi.*
- *Siber sigorta politikası hakkındaki bilgiler de dâhil olmak üzere kurumun olaylara hazırlık çerçevesine ilişkin detaylar.*
- *Üçüncü taraf siber risk stratejisinin ayrıntıları.*
- *Kurumun çaba ve çalışmalarını emsalleriyle kıyaslayan bilgiler.*
- *Konuyla alakalı önemli hukuki ve düzenleyici gelişmeler hakkında detaylar.*
- *Son siber saldırılardan öğrenilmesi gereken dersler.*

Kurumu saldırılardan korumak kritik öneme sahip olsa da, yönetim kurullarının, yalnızca korumanın ancak kurumun halihazırda bildiği sorunları çözebileceğini unutmamalıdır. Ne yazık ki, yapay zekâ kullanan yeni teknoloji araçlarıyla donanan inovatif siber suçlular, zarara neden olmak için sürekli olarak yeni yollar geliştirmektedir. Bunun sonucunda, **"Artık Şirket Yönetim Kurullarının da Siber Güvenlik Sorumluluğu Var (Now Corporate Boards Have Responsibility for Cybersecurity, Too)" başlıklı** MIT News makalesinde belirtildiği gibi "siber riski düzgün bir şekilde ele alabilmek amacıyla, bir olay meydana geldiğinde şirketin faaliyetlerine devam edebilmesi için hızlı tepki vermek ve kurtarmak için şirket liderlerinin kaya gibi sağlam planları olmak zorundadır."

IIA Hakkında

The Institute of Internal Auditors (IIA), 245.000'den fazla küresel üyeye hizmet veren ve dünya çapında 200.000'den fazla Sertifikalı İç Denetçi (CIA) sertifikası veren kâr amacı gütmeyen uluslararası bir meslek birliğidir.

1941 yılında kurulan IIA, dünya çapında iç denetim mesleğinin standartlar, sertifikalar, eğitim, araştırma ve teknik rehberlik alanlarındaki lideri olarak tanınmaktadır. Daha fazla bilgi için theiia.org adresini ziyaret ediniz.

IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 ABD

Ücretsiz Abonelik

Ücretsiz abonelik kaydınızı yapmak için **theiia.org/Tone** adresini ziyaret edin.

Okuyucu Geribildirimi

Sorularınızı/yorumlarınızı gönderiniz: **Tone@theiia.org.**

İç Denetim: Siber Güvenlikte Güvenilir Ortak

Yönetim kurullarının, iç denetim birimlerinin siber güvenlik çalışmalarına katabileceği değerin farkında olmaları gerekir. İç denetim siber güvenlik stratejisi, yönetişimi ve kontrolleri hakkında özgün, objektif, bağımsız güvence ve danışmanlık hizmetleri sunmaktadır. PwC makalesi "Birçok şirket, dayanıklılık ve müdahale dâhil olmak üzere siber süreç ve kontrolleri gözden geçirmek için iç denetçilerden yararlanmaktadır" diye belirtmektedir.

İç denetim birimleri, siber olaylara müdahale ve kurtarma süreçlerini de kapsayan çeşitli yöntemlerle siber dayanıklılık çalışmalarına katkı sağlayabilir. Geçen yılki Risk in Focus raporunda, iç denetçilerin katabileceği değerlerden bazıları sıralanmaktadır ve bu liste bugün de geçerliliğini korumaktadır:

- Siber savunma yanıtlarının alakalı ve güncel olmasını sağlamak amacıyla yönetim kurulu da dâhil olmak üzere kurumun önemli bölümlerinde farkındalığın, bilgi ve beceri düzeyinin değerlendirilmesi.
- Risklerin ve tavsiyelerin açık bir şekilde iletilmesini ve gerektiğinde en üst düzeye taşınabilmesini sağlamak amacıyla bilgi güvenliğinden sorumlu genel müdür yardımcısı, bilişimden sorumlu genel müdür yardımcısı ve yönetim kurulu arasındaki raporlama hatlarının değerlendirilmesi.
- Kimlik avı test simülasyonları ve diğer farkındalık artırma faaliyetlerinin sıklığının, zamanlamasının ve etkinliğinin, çalışanların katılım düzeylerinin ve çalışanların eğitim ve takip süreçlerine ne kadar iyi entegre olduğunun değerlendirilmesi.
- Hem yönetim kurulunu yönetişim sorumlulukları konusunda eğitmek hem de risk azaltma süreçlerinin tam ve etkili olup olmadığını test etmek için senaryo pratiklerinin kullanılması.
- İç kontrol ortamının etkinliğinin ve kontrollerin birinci ve ikinci hatlara ne kadar iyi yerleştirildiğinin IIA'nın Üçlü Hat Modeli'ne göre ve çalışanların rahatsız edici veya müdahaleci bulduğu ve göz ardı etmesi, unutması veya atlatması muhtemel uygulamalara özellikle dikkat edilerek değerlendirilmesi.
- Kurumun yönetişim yapısının üçlü hat boyunca iş birliğini ne kadar iyi sağladığının değerlendirilmesi.
- Kurumun siber güvenlik ve teknoloji düzenlemelerindeki küresel gelişmeleri ne kadar iyi izlediğinin ve iç kontrollerin gelecekteki gereksinimleri karşılamak için değiştirilebilmesine ne kadar hazır olduğunun belirlenmesi.

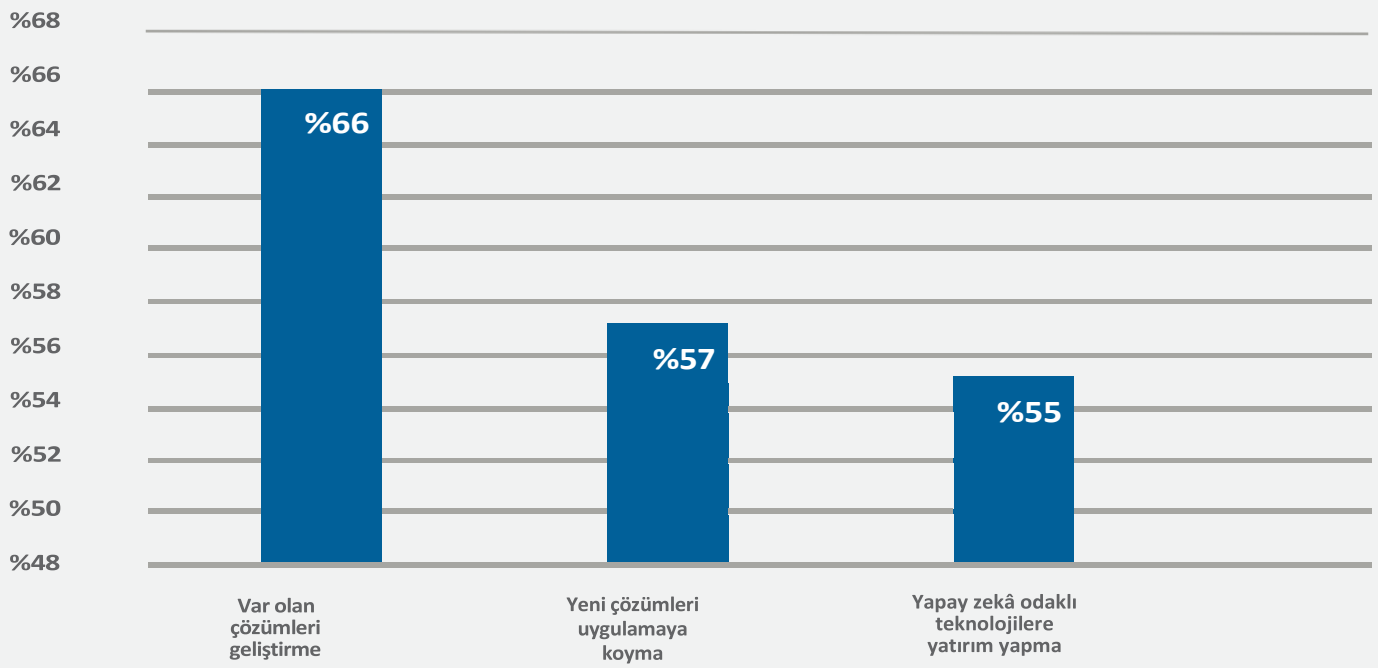
Kapsamı Genişleyen ve Gelişen Risk

Yeni teknolojiler hızla gelişirken, ortaya çıkan birçok araç siber saldırıların yapılmasını daha da kolaylaştırmaktadır. Federal hükümetin Siber Güvenlik ve Altyapı Güvenliği Dairesi Başkanı Jen Easterly'ye göre, yapay zekâ ve benzeri araçlar siber güvenlik çalışmalarını geliştirebilmelerine rağmen, kimlik avı ve spam, şantaj ve terörizm, yanlış bilgi aktarımı ve seçimlere müdahaleyi de kolaylaştırabilmektedir. Ayrıca, üretken yapay zekanın siber saldırganlara yeni fırsatlar sunduğunu ve daha az sofistike siber suçluların tahribat yaratmasına olanak tanıdığını da belirtmektedir. Yönetim kurulu üyeleri, siber saldırıları önlemenin en iyi yolu hakkında önemli bilgi ve tavsiyeler almak ve siber saldırıların meydana gelmesinin ardından müdahalelerinin çevikliğini değerlendirmek için iç denetim ekiplerine başvurmalıdır. İç denetçiler, kurumun bir saldırıdan en iyi şekilde kurtulmasını sağlamaya yardımcı olabilecek kontrol ortamına ve tanımlanan risklere ilişkin bağımsız değerlendirmeler sunabilir.

YÖNETİM KURULU ÜYELERİNE SORULAR

- Diğer kurumların nasıl karşılık verdiği de dâhil olmak üzere yeni siber tehditleri nasıl izliyoruz?
- Kurum kendi siber dayanıklılığını nasıl ölçüyor ve değerlendiriyor?
- Bu bilgileri saldırılara karşı hazırlıklarımızı ve potansiyel müdahalelerimizi uyarlamak için nasıl kullanıyoruz?
- Felaket kurtarma planlarımız neler? Bu planlar geçmişte ne kadar etkili oldular? Bu deneyimlerden ne öğrendik?
- Siber dayanıklılık stratejileri konusunda hangi birimlerin doğrudan sorumluluğu var?
- Siber dayanıklılığa duyulan ihtiyacı ve bu konuda oynayabilecekleri rolü bütün çalışanlar anlıyor mu?

Şirketler siber güvenliklerini nasıl geliştiriyor?



Kaynak: 2024 Cisco Cybersecurity Readiness Index.