KÜRESEL BAKIŞ AÇILARI VE ANLAYIŞLAR

Siber Güvenlik

KISIM I: Gelecek Nesil için Kadro Oluşturma ve Gelişim

KISM II: Yapay Zeka – Siber Güvenliğin Dostu ve Düşmanı

KISIM III: Siber Güvenlik Üçüncü Taraf Risk Yönetimi

AUDITBOARD

The Institute of Internal Auditors

İçindekiler

Kısım 1: Yeni Nesil için Kadro Oluşturma ve Gelişim

Uzmanlar Hakkında

Aneta Waberska, CISA

Aneta, AuditBoard kurumunda Bilgi Güvenliği ve Uyum Ürünleri Direktörü olarak görev yapmaktadır. BT denetimi ve uyum alanlarında 15 yıldan fazla deneyime sahiptir ve kendi sektör deneyiminden yararlanarak BT risk ve uyum kullanıcılarına hizmet veren ürün geliştirme çalışmalarına odaklanmak üzere AuditBoard bünyesine katılmıştır. Aneta kariyerine KPMG ve PwC kurumlarında başlamış olup, müşterilere SOC 1 ve SOC 2 gibi çerçeveleri uygulama ve değerlendirme konularında yardımcı olmuştur. Şirket çapında politikaların yönetilmesi ve üçüncü taraf risk yönetim programları da dâhil olmak üzere karmaşıklık düzeyi değişen uyum programlarını uygulamak ve yönetmek üzere farklı büyüklükte şirketlerle çalışmıştır. Güvenlik çerçevesi gerekliliklerini karşılayacak kontrolleri uygulamaya koymak için yönetimle yakından çalışırken uyumun şirketin stratejik hedeflerini desteklemesini sağlamak için üst düzey yöneticilerle de çalışmıştır.

Uday Gulvadi, CIA, CPA, CAMS, CISA

Uday, Stout kurumunda Uyuşmazlıklar, Uyum ve Soruşturmalar grubunda Genel Müdür olarak görev yapmaktadır ve ulusal düzeyde mevzuata uyum ve mali suçlar uygulamalarını yönetmektedir. Uday, 20 yılı aşkın tecrübesi olan bir mali suçlar, iç denetim, bilgi sistemleri denetimi ve risk danışmanlığı uygulaması lideridir. Uzmanlık alanı kurumsal risk yönetimi, AML ve yaptırım programı yönetişimi, model validasyonlar, risk temelli iç denetimler, bilgi teknolojisi ve siber güvenlik denetimi ve kontrolleri de dâhil olmak üzere en zorlu mali suçlar konusunda uyum, BT ve siber riskler, yönetişim ve risk ve uyum konularında yönetim kurullarına, denetim komitelerine ve üst yönetime danışmanlık yapmaktır. Uday'ın müşterileri dünyanın en büyük bankaları ve finans kuruluşlarından, daha küçük finansal hizmet şirketlerine kadar çeşitli firmalardan oluşmaktadır.

GİRİŞ

Siber güvenlik, büyüklüğü ne olursa olsun tüm kurumlar için önemli bir tehdit oluşturmaktadır. Yakın zamanda yaşanan örnekler, işlerin ne kadar çabuk ters gidebileceğini göstermektedir. Bir siber saldırı, Ace Hardware şirketinin bayilerine yaptığı sevkiyatları kesintiye uğratmış ve müşterilerin online siparişlerini geçici olarak devre dışı bırakmasına neden olmuştur. Şili'deki büyük bir telekom şirketine yapılan fidye yazılımı saldırısı veri merkezleri, internet erişimi ve IP üzerinden sesli iletişim gibi hizmetleri kesintiye uğratmıştır. Ayrıca, daha küçük kuruluşların da etkilenebileceğini gösteren bir örnek olarak, Kuzey Carolina'nın Cabarrus County bölgesinde bir siber saldırı doğum, ölüm, evlilik endekslerine ve arazi kayıtlarına çevrimiçi genel erişimi kesintiye uğratmıştır.

İç denetim, siber risklerin yönetilmesine yardım etme konusunda anahtar bir rol oynamaya çok uygundur ancak bu rolü yerine getirmek için ihtiyaç duyduğu kaynaklara sahip olmak zorundadır. Kurumların karşı karşıya kaldıkları siber tehditleri tanımlama ve bunlar hakkında tavsiye vermek için gereken bilgi ve becerilere sahip olması gereklidir. Deloitte'e göre, siber güvenlik değerlendirmesi yürütülürken "güncel risk ortamı hakkında uygun derinlikte teknik becerilere ve bilgiye sahip olan denetim personelini sürece dâhil etmek kritik düzeyde önemlidir."[1]

Bu özet, siber güvenlik hakkında üç kısımdan oluşan serinin birinci kısmıdır. İç denetim liderleri tehditleri ele almak için kadro oluşturmadan önce bu tehditleri anlamak zorundadır; bu nedenle, bu kısım siber güvenlik zorluklarının iç denetçiler ve onların çalıştıkları kurumlar için incelenmesiyle başlamaktadır. Ayrıca, iç denetim liderlerinin sürekli devam eden siber riskleri ele almak için ihtiyaç duydukları yetenekli kişileri ellerinde bulundurmalarını sağlamak için takip edebilecekleri seçenekleri ve stratejileri de kapsamaktadır.

[1] "Siber Güvenlik ve İç Denetimin Rolü - Acil Eylem Çağrısı (Cybersecurity and the Role of Internal Audit—An Urgent Call to Action)," Deloitte Development LLC, 2017.

Açık Bir Tehdit

Siber güvenlik hâlâ en önemli risklerden biridir

İç Denetimin Siber Güvenlik Çalışmaları Artmaktadır

Aneta Waberska (CISA), AuditBoard'un Bilgi Güvenliği ve Uyumluluk Ürünleri Direktörü **"İç denetçiler kurumun bütününe bakmalı** ve risk temelli bir yaklaşım benimsemelidir," diyor. "Siber riskler, çoğu kurum için listenin en tepesindedir."

İç denetçiler, siber risklerin oluşturdukları tehdidin farkında görünmektedir. İç Denetim Vakfının iç denetim liderleriyle yaptığı bir küresel ankete göre, siber güvenlik 2024 yılına girerken en önemli risk olarak tanımlanmıştır. 4.200'den fazla iç denetim yöneticisinin (İDY) katıldığı Risk in Focus 2024[2] anketinde siber güvenlik, Beşerî Sermaye ve İş Sürekliliği ile birlikte listenin en tepesindeki üç risk olarak belirlenmiştir ve ankete katılanların %73'ü siber güvenliği ilk beş riskten biri olarak tanımlamıştır.

İç Denetçiler Enstitüsü 2023 Kuzey Amerika İç Denetimin Nabzı yayınına göre, Kuzey Amerika'da iç denetim liderlerinin %78'i siber güvenliği kurumlarında yüksek veya çok yüksek bir risk olarak belirlemiştir.[3] Ankete katılan denetçiler denetim planlarının %10'unu siber güvenliğe ve %9'unu BT konularına ayırmıştır. Buna ilave olarak, Nabız anketinin bulgularına göre, fonksiyonların yaklaşık %70'i siber güvenlik ve BT'yi içeren yüksek riskli alanları yıllık veya sürekli olarak gözden geçirmiştir.

Aşağıda sayılanlar dikkate alınması gereken bazı siber güvenlik tehlikeleri arasında yer almaktadır:

- Suçluların kritik bilgileri çalmasını sağlayan ya da müşteri veya iş ortağı verilerini ifşa eden ihlâller.
- Kurumların ilk önce siber suçlulara fidye ödemeden önemli fonksiyonları yürütmesini ya da gerekli bilgilere erişim sağlamasını imkânsız kılan fidye yazılım saldırıları.
- Bir sisteme zarar verebilecek kötü amaçlı yazılımlar.

Siber saldırılar, işletme fonksiyonları bozulduğunda ya da müşterilerin veya iş ortaklarının bir kuruma olan güvenini kaybedip onunla iş yapmayı bırakması durumunda meydana gelen finansal kayıplar gibi bariz sonuçların ötesinde sonuçlar doğurmaktadır. Dahası, bir siber olayın ortaya çıkarılmasından sonra, kurumlar, düzenleyici raporlama gerekliliklerini karşılamak amacıyla, ne olduğunu ve ne zaman olduğunu anlamak, herhangi bir hasarı gidermek için iyileştirme çalışmaları yürütmek ve bu tür saldırılardan kaynaklanan yan sonuçların finansal ve operasyonel perspektiflerden önemli olup olmadığını tespit etmek için adli soruşturmalara zaman ve para yatırımı yapmak zorundadırlar.

Bu durumda, siber güvenlik harcamalarının hızlı bir şekilde artması şaşırtıcı değildir. 2023 yılının başlangıcında, Canalys, küresel siber güvenlik harcamasının yıl boyunca %13,2'ye çıkmasını ve potansiyel olarak 224 milyar dolara ulaşmasını beklemiştir.[4]

Stout kurumunda Uyuşmazlıklar, Uyum ve Soruşturmalar grubunda genel müdür olan Uday Gulvadi (CIA, CPA, CAMS, CISA) "Şirketler bu tehditlerin çok gerçek ticari ve mali sonuçlar doğurduğunu fark etmeye başladı," demiştir. Uday, bu tehditlerin denetim komiteleri için kesinlikle en önemli konular olduğunu ve "iç denetimden bu alanlarda adım atması ve güvence sağlaması istendiğini" söylemiştir.

[2] "Risk in Focus 2024," İç Denetim Vakfı, 2023
[3] "2023 Kuzey Amerika İç Denetimin Nabzı (2023 North American Pulse of Internal Audit)," İç Denetçiler Enstitüsü, 2023

[4] "Siber güvenlik yatırımları 2023'te %13 artacak (Cybersecurity investment to grow by 13% in 2023)", Canalys, 18 Ocak 2023, https://www.canalys.com/newsroom/cybersecurity-forecast-2023

Zorluklar

Siber güvenlik yaklaşımı ve kadro oluşumunda olgunluk etkisi

Siber Ortamın Net Bir Şekilde Anlaşılması Esastır

İç denetimin siber risk yönetimini desteklemesine yardım edecek doğru insanları işe alabilmek ve onlara uygun gelişim fırsatları sunabilmek için kurumun kendine özgü siber güvenlik durumlarını ve risklerini her yönüyle anlamak önemlidir. Birçok faktörün ve zorluğun dikkate alınması gereklidir.

Rehber Odaklı Zihniyet

Waberska, geleneksel olarak birçok iç denetim ekibinin iç kontrolleri ve çeşitli süreçleri rehber odaklı bir perspektiften düşünmeye alıştığını belirtmiştir. Bununla birlikte, iş dünyasında sürekli devam eden dijital dönüşüm, ekiplerin siber güvenlik de dâhil olmak üzere kurum genelinde iç denetimlerin ve diğer süreçlerin dijital çözümlerle nasıl geliştirilebileceği ve iyileştirilebileceğini bilmelerini ve fark etmelerini gerektirmektedir. Aynı zamanda, giderek daha sofistike hale gelen siber suçluların dijital ortamların yaratabileceği güvenlik zafiyetlerinden yararlanmasından dolayı, iç denetçilerin bizzat dijital dönüşümün kurumlar açısından doğurduğu riskleri de anlamaları gerekmektedir.

Örneğin, bir kurum bulut üzerinde faaliyet gösteriyorsa ya da herhangi bir ileri veya yeni teknoloji kullanmayı planlıyorsa, geçmişte bu araçlarla çalışmış olan kişilere ihtiyaç duyacaktır. Waberska, ekip üyelerinin teknolojide uzman olmalarına gerek olmadığını ancak bulut ortamına veya diğer çözümlere maruziyet kalmalarının ilişkili risklere daha fazla aşina olmalarını sağlayacağını belirtmiştir. Bu becerilere sahip kişilerin istihdam edilmesine ilave olarak, denetim ekiplerinin yeni teknolojilerin var olan kadronun eğitim ve gelişim sürecine dâhil edilmesini de sağlamaları gereklidir.

İç Kontroller

İç denetçiler, kurumun karşılaştığı risklere karşı korunması için kurumda uygun kontrollerin olduğunu sağlamak üzere eğitilmektedirler. Siber riskler söz konusu olduğunda, iç kontrollerin, kurumun bilgi teknolojisinden ödün verilmemesini ve işletme fonksiyonlarının işler durumda kalmaya devam edebilmesini sağlayacak şekilde çalışmaları gereklidir.

Siber güvenlik risklerini tanımlamak ve onlar hakkında tavsiye vermek için, iç denetim ekiplerinin kurumları tarafından kullanılan teknolojilere yönelik BT güvenlik kontrollerine aşina olmaları gerekecektir. Waberska, örneğin bulutla çalışırken geçerli olan kontrollerin kurum içi veri merkezleriyle kullanılan kontrollerden farklı olacağını belirtmiştir. İç denetçilerin, siber suçun gizlilik açısından doğurabileceği tehdidi ve kurumun gizlilik programına ilişkin denetim planlarına yönelik olası etkileri göz önünde bulundurarak hangi kontrollerin uygun olacağını anlamaları da gerekecektir.

Şeffaflık Düzenlemeleri ve Veri Koruma

Kurumlardan siber güvenlik çabalarına ilişkin raporlama hakkında artık daha açık olmaları istenmektedir. İç denetçiler, hangi kuralların kendi şirketlerini etkilediğini anlamak ve uyum ihtiyaçlarını değerlendirebilmek zorunda olacaktırlar. Önemli bir örnek olarak, Ağustos ayında, ABD Menkul Kıymetler ve Borsa Komisyonu, halka açık şirketlerin bir siber saldırıya maruz kaldıklarında daha fazla şeffaflık sağlamalarını ve siber riskleri azaltma çabaları hakkında spesifik bilgileri ifşa etmelerini gerektiren Siber Güvenlik Risk Yönetim, Strateji, Yönetişim ve Olay Açıklaması hakkında nihai bir kural yayınlamıştır. Bu kural teklif aşamasındayken IIA da kural hakkında yorumlarını sunmuştur. IIA, özellikle de bir siber olayın önem derecesinin tespit edilmesi ve "siber güvenlik" teriminin daha iyi tanımlanması başta olmak üzere uygulama rehberi geliştirmek için SEC ile birlikte çalışmaya devam etmeyi planlamaktadır.

İş yapmanın giderek çok uluslu hale gelmesi ve dünya çapında siber güvenlik düzenlemelerinin sayısının artması nedeniyle, iç denetçiler, örneğin Avrupa Birliği Genel Veri Koruma Tüzüğü gibi kurumlarını etkileyebilecek tüm veri güvenliği ve gizlilik kanunlarına aşina olmak zorundadırlar. Gerçekten de Birleşmiş Milletler Ticaret ve Kalkınma Konferansına göre, 194 ülkeden 137'si verilerin ve gizliliğin korunmasını güvence altına alan kanunlar yürürlüğe koymuştur.

BT Sistemleri

Temel düzeyde dahi olsa teknolojiyi bünyesinde barındıran tüm kurumlar bir tür BT sistemine dâhildir ve bunların hepsi siber riske karşı savunmasızdır. Sistemlerin hacmi ve içerdikleri potansiyel zafiyet ve tehditler göz önünde tutulduğunda, şirketlerin ve iç denetimin hangi sistemlerin en önemli olduğunu anlamaları önemlidir. Waberska "Tüm sistemlerde aynı seviyede kontrolleri hiçbir zaman sağlayamayacağız," diye belirtmiştir. Öncelikleri belirlemek için, örneğin aşağıdakiler gibi sorular sorulması gerekecektir:

- Hangi sistemler kurumun işleyişi için kritik düzeyde önemlidir? Bu soruya kurumun bu sistemler olmadan iş yapmaya veya önemli amaçlarına ulaşmaya devam edip edemeyeceği -ve bunu ne kadar süre yapabileceği- göz önünde bulundurularak cevap verilmesi mümkündür.
- Hangi sistemler en hassas verileri işlemektedir? Bu veriler gizli kurumsal bilgileri veya kişiyi tanımlamak için kullanılabilecek bilgileri (PII) içerebilir.
- Hangi sistemler benzersiz veya ikame edilmesi zor veriler içermektedir?[5]

Üçüncü Taraflar

Küçük ve orta ölçekli kurumlar bile verilerini işleyen üçüncü taraflarla ilişki içindedirler. Bu, bir bulut uygulama veya daha büyük ölçekli kurumlar için belki yurt dışındaki bir işlem merkezi aracılığıyla gerçekleşebilir. Gulvadi, bu tedarikçilerin önemli kurumsal verileri ve müşterilere ait PII'yi işleyebildiğini ve verilerin dünyanın herhangi bir yerinde tutulabileceğini belirtmiştir. Bu nedenle, BT varlıklarının nerede oldukları ve bu varlıklar etrafında uygun kontroller olup olmadığı da dâhil olmak üzere "Bütün BT varlıklarının genel görümünü anlamak son derece önemlidir," demiştir.

Kurumların, üçüncü taraflarla veri paylaşmadan önce onların siber güvenlik süreçlerini değerlendirmeleri ve üçüncü tarafların bu verileri kullanmaya başlamalarından sonra söz konusu süreçleri izlemeleri ve bazı durumlarda, üçüncü tarafları denetleme haklarını saklı tutmaları gerekmektedir. Waberska "Eğer müşteri verilerini başka bir tarafla paylaşıyorsanız bu verileri sizin şirketinizin koruyacağı şekilde korumalarını sağlamanız gerekir," demiştir. Şirketlerin, örneğin üçüncü tarafın iç kontrollerinin riski ne kadar iyi ele aldığını görmek amacıyla değerlendirildiği SOC 2 gibi üçüncü taraf tasdik raporlarını ya da ilgili veri kategorilerinin korunmasıyla ilgili başka tipte tasdik veya sertifikasyon dokümanlarını gözden geçirmeleri gereklidir.

Güvenli Erişimin ve Kullanılabilirliğin Sağlanması

Gulvadi, bir yandan kurumun veri ve sistemleri koruyabilmesini sağlarken diğer yandan bilgi ve sistemlerin iş hedeflerine ulaşmak için gerektiğinde kullanıma hazır olmasının garanti edilmesi arasında bir denge olduğunu belirtmiştir. Bu dengeyi korumak amacıyla, kurumlar hem verileri koruyan hem de müşteri hizmetlerinin veya diğer önemli iş fonksiyonlarının ihtiyaç duydukları bilgilere erişimi külfet haline getirmeyen kontroller seçmek zorunda kalacaktırlar. Kurumun hangi sistemlerin en yüksek seviyede güvenlik gerektirdiğine karar vermesinden sonra bu seçimi yapmak daha kolay olacaktır. Bazı sistemlerin çok faktörlü kimlik doğrulaması, şifreleme protokolleri ve veri kaybı koruma yazılımı kullanılarak korunması gerekirken diğerleri bu seviyede detaylı koruma gerektirmeyecektir.

[5] "*CISA İçgörüleri – Siber, Güvenli Yüksek Değerli Varlıklar (HVA) (CISA Insights – Cyber, Secure High Value Assets (HVAs)),"* ABD Ulusal Güvenlik Bakanlığı, https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf

İç Denetim Kaynaklarının Güçlendirilmesi

Siber güvenlik kadrosunun oluşturulması hâlâ en önemli önceliklerden biridir

İç Denetimde Siber Yetenekli Kişinin İşe Alınması ve Geliştirilmesi

Bu riskler göz önünde bulundurulduğunda, iç denetim bu riskleri ele alabilen bir ekibi nasıl oluşturabilir ve koruyabilir? Cevabın detayları kuruma göre çeşitlilik gösterecektir ancak hepsi için geçerli olan birkaç tavsiye mevcuttur.

Becerilerin Birleşimini Arayın

Gulvadi, iç denetim ekiplerinin siber riski ele almak için hem siber güvenliğin teknik yönüne ilişkin derin bir anlayışa hem de güvenlik hususlarının iş açısından doğurabileceği sorunları kavrama yeteneğine ihtiyaç duyduklarını belirtmiştir. Geçmişte, BT denetçileri bilgi teknolojisinin teknik yönleri konusunda güçlü olma eğilimi gösterse de genelde ilişkili risklerin kurumun iş hedeflerini gerçekleştirme becerisini nasıl etkilediğine odaklanmıyorlardı. Eğer iç denetimin iyileştirilmiş teknoloji veya kontroller ya da ilave personel alımı konusunda ihtiyaç duyduğu yatırımlar için yönetimin onayını alması gerekiyorsa, iş açısından olası etkileri açıkça ifade edebilme becerisi paha biçilmez olabilir.

Gulvadi, teknik bilgiyi iş hedefleri, süreçleri ve değer zincirleri anlayışıyla harmanlayan ekipler oluşturmak için daha fazla çaba sarf edildiğini görmektedir. Bazı durumlarda, iç denetim ekipleri her iki beceriye de sahip olanları bulurken diğer ekipler becerileri birbirini tamamlayan kişilerden oluşmaktadır. Kurum, iki tipteki personele de diğer disiplin hakkında temel çalışma bilgisi sağlamak amacıyla eğitim sunmayı düşünebilir.

Becerileri Yeni Teknolojilere Entegre Edin

Birçok iç denetim ekibi, örneklem bazında test yaklaşımından uzaklaştıkça veri analitiği, yapay zekâ ve makine öğrenimi konularında uzmanlığı olan kişileri bünyesine katmaktadır. Gulvadi "Bütün popülasyonu test etmek ve anomali tespitini iyileştirmek için yapay zekâ kullanabilirsiniz," demiştir. Yapay zekâ kullanımı verimliliği ve güvenilirliği artırmakla kalmaz, aynı zamanda iç denetçilerin yeni teknolojilerin kullanımında giderek daha sofistike hale gelen siber suçlulara ayak uydurabilmelerine de yardımcı olur.

Dış Kaynak Kullanımını Araştırın

Bazı iç denetim ekipleri, teknik veya ticari becerileri artırmak için dış kaynak kullanılan bir ekibe iş vermektedir. Siber güvenlik veya BT güvenliği konularında özel uzmanlığı olanlar, gerektiğinde bir projede veya daha uzun bir süre bazında iç denetim ekibinin bünyesine katılabilirler. İç denetim ekibinin üyeleri bu uzmanlarla birlikte çalıştıklarında, yüklenicilerin bilgi birikimlerini artırmalarına ve şirket süreç ve prosedürlerini daha iyi yönlendirmelerine yardımcı olabilirler. Aynı zamanda, kurum dışı uzmanlarla çalışmak ekip üyelerinin bilgi tabanını genişletmeye yardımcı olabilir. Dış kaynak kullanma opsiyonunun değerlendirilmesi konusunda, Gulvadi dış kaynak kullanılan kişilerin güncel ekibin becerileriyle eşleşmesini veya onları geliştirmesini sağlamak için ekip üyelerinin sertifikasyonlarının ve önceki tecrübelerinin gözden geçirilmesini tavsiye etmektedir.

İşbirliğini Göz Önünde Bulundurun

Bazen iç denetim ekibinin ihtiyaç duyduğu uzmanlık kurum bünyesinde, örneğin BT, güvenlik veya uyum gibi alanlarda mevcut olabilir. Bir yandan denetçi bağımsızlığını korurken diğer yandan iyi bir ortaklık kurmak, iç denetim ekibi üyelerine kurumun teknoloji ekosistemi ve riskleri hakkında bir dizi yeni içgörü ve bilgi sağlamaktadır. Böyle bir ortaklık aynı zamanda gelecekte verimli denetimler için de zemin hazırlamaktadır, çünkü diğer ekipler iç denetimin kurumu gereksiz risklerden koruma ve kurumun hedeflerine ulaşmasını sağlama amacını paylaştığını bileceklerdir. Açık iletişim, diğer ekiplerin iç denetim hedeflerine ilişkin endişelerini aşmalarına da yardımcı olabilir. Waberska "BT ve güvenlik ekipleri önemli sorunları düzeltmeye ve çözümler bulmaya odaklanır. Bu ekipler riskleri ve onların hafifletilmesi gerektiğini anlar. İç denetimin bu ekiplerle risklere yüksek düzeyde odaklanan bir konuşma yapabilmesi, iç denetimin çok daha etkili hale gelmesi için belirli bazı kontrollerin neden gerekli olduğunu açıklar," demiştir.

Kurum İçi İlişkiler Kurun

Spesifik bir proje üzerinde işbirliği yapmıyor olsalar bile, mevcut çalışmaları hakkında bilgi edinmek için çalıştıkları kurumların güvenlik, uyum ve BT ekiplerindeki diğer profesyonellerle ilişki kurmaktan ve bu ilişkileri sürdürmekten iç denetim ekibinin tüm üyeleri faydalanabilir. Waberska "Şirket ortamında neler olduğunu anlamak çok önemlidir," ve bu ilişkiler ekibin zamanında güncel bilgiler almasını sağlayabilir. Spesifik denetimler trendleri ve tehditleri ortaya çıkaracaktır "ancak neyin değiştiğini mümkün olduğunca erken öğrenmek daha iyidir," demiştir.

Mevcut Kaynaklardan Faydalanın

Waberska "Eğer iç denetim modern teknolojileri en azından yüksek bir seviyede öğrenmeyi ve onlara eşlik eden riskleri tanımlamayı kendine görev edinirse, var olan ve yeni ortaya çıkan riskler konusunda güncel kalacaktırlar," demiştir. Çok çeşitli siber güvenlik rehberleri, araştırmaları, sertifika programları ve örneğin IIA'nın yıllık Siber Güvenlik Sanal Konferansı gibi konuyla ilgili konferanslar hakkında bilgiler içeren IIA Siber Güvenlik Kaynak Merkezi seçenekler arasındadır. AuditBoard kurumu da kendi kaynaklar sayfasından erişilebilen çok çeşitli siber güvenlik kaynakları sunmaktadır.

İç Denetim Vakfı tarafından hazırlanan Risk in Focus 2024, siber güvenlik riskini küresel olarak araştırmaktadır ve siber güvenliğin ve diğer en önemli risklerin dünya genelinde nasıl görüldüğü ve yönetildiği hakkında benzersiz bölgesel perspektifler sunmaktadır.

Varılan Sonuçlar

2023 IIA Nabız anketi İç denetim personel kadrosunun arttığını ancak henüz COVID öncesi seviyelere dönmediğini bulmuştur. İç denetim liderlerinin, iş gücüne katılan nesillerin dijital açıdan bilgili olduğunu hatırlamaları gereklidir. Gulvadi, bu nesillerin sahip ettiği bilgi birikiminden faydalanmanın en iyi yolları üzerine düşünmenin akıllı bir yaklaşım olacağını belirtmiştir. İç denetim birimleri, yeni nesile kritik iş sorunlarını çözmeye yardımcı olacak içgörüler sunmak için YZ/ML gibi gelişmekte olan teknolojileri kullanma şansı sunarak rekabetçi bir kadro oluşturma ortamında kendilerini diğerlerinden ayıracaklardır. İç denetim ekipleri yeniden oluşturmaya veya uzmanlığını yeni zorluklar üstlenecek şekilde genişletmeye devam ettikçe bu özette ele alınan tavsiye ve içgörüleri planlama süreçlerine kullanmaları gerekecektir.

Kısım 2: Yapay Zekâ – Siber Güvenliğin Dostu ve Düşmanı

Uzmanlar Hakkında

Aneta Waberska, CISA

Aneta, AuditBoard kurumunda Bilgi Güvenliği ve Uyum Ürünleri Direktörü olarak görev yapmaktadır. BT denetimi ve uyum alanlarında 15 yıldan fazla deneyime sahiptir ve kendi sektör deneyiminden yararlanarak BT risk ve uyum kullanıcılarına hizmet veren ürün geliştirme çalışmalarına odaklanmak üzere AuditBoard bünyesine katılmıştır. Aneta kariyerine KPMG ve PwC kurumlarında olup, müşterilere SOC 1 ve SOC 2 gibi çerçeveleri uygulama ve değerlendirme konularında yardımcı olmuştur. Şirket çapında politikaların yönetilmesi ve üçüncü taraf risk yönetim programları da dâhil olmak üzere karmaşıklık düzeyi değişen uyum programlarını uygulamak ve yönetmek üzere farklı büyüklükte şirketlerle çalışmıştır. Güvenlik çerçevesi gerekliliklerini karşılayacak kontrolleri uygulamaya koymak için yönetimle yakından çalışırken uyumun şirketin stratejik hedeflerini desteklemesini sağlamak için üst düzey yöneticilerle de çalışmıştır

Terry Grafenstine, CIA, CPA, CISSP, CISA, CRISC, CGAP, CGEIT

Terry, İç Denetçiler Enstitüsü (IIA) Küresel Yönetim Kurulunun 2023–24 kıdemli başkan yardımcısı ve Pentagon Federal Credit Union (PenFed) kurumunda iç denetim yöneticisidir. Siber ve teknoloji alanlarında mesleğe yaptığı katkılardan dolayı IIA tarafından "On Yılın En İyi On Denetim Fikir Önderinden" biri olarak kabul edilmiş ve IIA'nın Seçkin Denetim Uygulayıcıları Listesine dâhil edilmiştir. Citi ve Deloitte kurumlarında liderlik rollerini üstlenmiş ve ABD Temsilciler Meclisi'nde atanmış Genel Müfettiş olarak görev yapmıştır.

GİRİŞ

Siber güvenlik iç denetçilerin dikkate alması gereken en önemli risktir ve öngörülebilir gelecekte de böyle olmaya devam edecektir. Gerçekten de Risk In Focus 2024 yayınına göre, iç denetçilerin en fazla zaman harcadığı ve efor sarf ettiği tek risk siber güvenlik riskidir. İç Denetçiler Enstitüsü (IIA) İç Denetim Vakfının rapor serisi, dünya çapında iç denetim yöneticileri ve direktörlerine çalıştıkları kurumun karşı karşıya kaldığı en önemli riskler ve tehdit tablosunun önümüzdeki üç yıl içinde nasıl değişmesini bekledikleri hakkında sorular sormuştur.

Risk in Focus 2024 bulguları, siber güvenliğin bir risk olarak ne kadar karmaşık olduğunu ve teknolojide neredeyse sürekli gerçekleşen değişimlerden kaynaklanan ilave zorlukları ve nasıl kullanılabileceğini göstermektedir. Raporun bulgularında bu da ifade edilmiştir. İç denetim liderleri, dijital bozulma tehdidinin bugün tehdit listesinde beşinci sırada yer alırken üç yıl içinde ikinci sıraya yükselmesini beklemektedir.

Siber güvenlik hakkında üç kısımdan oluşan serinin ikinci kısmı olan bu özet, yapay zekanın (YZ) siber güvenlikle ilgili zorluk ve fırsatlara nasıl katkıda bulunduğunu ve iç denetçilerin bir siber güvenlik konusu olarak ortaya çıkan ve gelişen bu risk alanı hakkında ne bilmeleri gerektiğini incelemektedir. YZ, hemen hemen tüm kurumlarda verimliliği, üretkenliği ve risk yönetimini iyileştirecek sofistike bir araç olarak büyük bir umut vadetmektedir. Bununla birlikte, etik hususlar, algoritmik önyargıya bağlı tehlikeler ve YZ kullanımına aşırı veya körü körüne güvenme gibi yeni risk yönetimi zorluklarını da beraberinde getirmektedir. YZ, siber saldırılara karşı yürütülen savaşta değerli bir araç olabilmesine rağmen kötü amaçlı aktörler de suç işlemek için YZ kullanmaktadır.

İş Başında YZ

İki Ucu Keskin Siber Kılıç

İç Denetim YZ'nin Kullanım Alanlarını ve Tehditlerini Araştırmalıdır

Yapay zekâ terimi, öğrenme, mantıklı düşünme ve zor bir problemi çözmeye çalışma gibi insan zekasını taklit edebilen teknolojiyi ifade eder. Bu terim, makine öğrenimi veya bir sistemin verilerden öğrenme ve bu öğrenimi uygulama becerisi de dâhil olmak üzere birden fazla teknoloji türünü kapsamaktadır.

AuditBoard kurumunda bilgi güvenliği ve uyum ürünleri direktörü olarak çalışan Aneta Waberska, YZ ve makine öğreniminin siber güvenlik çaba ve çalışmalarını önemli düzeyde geliştirebilme yollarından birinin tehdit tespiti ve veri analizi olduğunu söylemiştir. Siber suçlular, zayıf noktaları arayarak ve ağ savunmalarını bozarak kurumların ağına sızmaya çalışmaktadır. Geçmişte, kurumlar bu harici tehditleri bloke etmek için sistem yöneticilerine güveniyordu. Bununla birlikte, otomasyonda ve diğer teknolojilerde kaydedilen ilerleme nedeniyle, kötü amaçlı aktörlerin giriş hacminin giderek artmasının bir kişinin etkili gözden geçirme yapabilme kapasitesini aştığını söylemiştir Waberska. YZ, bu sorunu ele alabilir. YZ, yüksek hacimlerde ağ girişlerini gözden geçirerek örüntüleri fark edebilir ve zamanla bunlardan öğrenebilir, belirli bir olayın veya olaylar kümesinin kurum açısından tehdit oluşturup oluşturmadığını anlayabilir. Waberska'ya göre "YZ'nin bu ortamda en etkili kullanımlarından biri budur."

Bunlara ilave olarak, daha sofistike kötü amaçlı yazılım tespit araçları güvenlik ihlâl ve olaylarının en önemli nedenlerinden biri olan kimlik hırsızlığını engelleme becerisi de dâhil olmak üzere daha iyi yeteneklere sahiptir. Waberska'ya göre, bu -örneğin kimlik hırsızlığını amaçlayan e-postayı açarak şirket ağlarını kötü amaçlı yazılıma maruz bırakma gibi- insan hatalarının ihtimalini azaltabilir veya tamamen ortadan kaldırabilir çünkü bu araçlar bir kişinin gelen kutusuna ulaşmadan önce bu tür e-postaları filtrelemektedir. (YZ'nin siber güvenlik savunmalarını iyileştirebileceği yollardan bazıları hakkında daha fazla bilgi almak için bilgi kutusuna bakınız.)

YZ, aynı zamanda kurumun ağında halihazırda meydana gelen anomalileri hızlı şekilde arayabilir ve sorunları tanımlayabilir -ki bu insanların böylesi geniş ölçekli veriler üzerinde gerçekleştiremeyeceği bir faaliyettir. Şirket sistemlerine yetkisiz erişim bir örnektir. Eski bir çalışan, bir şifreyi paylaşarak veya yazarak farkında olmadan bir siber suçlunun erişimine izin verebilir ya da sisteme kötü niyetle yeniden girebilir. Pentagon Federal Credit Union kurumunda iç denetim yöneticisi olan Terry Grafenstine, geçmişte eski çalışanlar arasında yetkisiz erişim olup olmadığını kontrol eden bir iç denetçinin, erişimi olan ve artık erişime sahip olmaması gereken kişileri manuel olarak karşılaştırmak ve ardından BT ekibine sorunları detaylandıran bir e-posta yazmak zorunda kaldığını belirtmiştir. Öte yandan, YZ birden fazla platform genelinde arama yapabilir; bordro sistemindeki ve erişim sistemindeki verileri karşılaştırabilir ve her türlü anomali hakkında uygun ekiplere e-posta yazabilir.

Siber Güvenlik Aracı olarak YZ Kullanımı

IEEE Bilgisayar Topluluğuna göre, aşağıda sayılanlar YZ'nin kurumun siber güvenlik savunmalarını artırabileceği yollardan bazıları arasındadır:

- Kabul edilebilir faaliyetleri kıyaslamak ve anomali ve tehditleri sürekli ve gerçek zamanlı olarak tanımlamak suretiyle kötü niyetli faaliyetleri tespit etmek.
- Güvenli olmayanları ayırt etmek amacıyla dosya özelliklerini veya kod örüntülerini inceleyerek kötü amaçlı yazılım tehdit tanımasını desteklemek.
- Şirketin sıfır gün saldırıları veya diğer bilinmeyen tehditler ile baş etme becerisini iyileştirmek.
- Bir dizi kaynaktan elde edilen güvenlik bilgilerini bir araya getirmek, proaktif tehdit avcılığı yapmak ve şirket güvenliği analistlerinin iş yükünü hafifleterek tehdit yönetimine yardımcı olmak suretiyle tehdit zekasını artırmak.[6]

[6] "Siber Güvenlik ve Siber Suç için YZ: Yapay Zeka Kendisiyle Nasıl Savaşıyor? (AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself)," Gaurav Belani, IEEE Computer Society, 6 Eylül 2023.

Grafenstine, iç denetçilerin siber suçluların amacının genelde sadece verileri çalmak olmadığının, daha ziyade sistemlere sızıp verileri değiştirerek sistemleri bozmak olduğunun farkında olmaları gerektiğini söylemiştir. En geniş düzeyde, ulus-devlet kötü niyetli aktörleri ulaşım, nükleer enerji, bankacılık ve diğerleri gibi kritik altyapıları manipüle edebilir ancak bunun sonuçları her büyüklükte kurum için önemli olabilir.

Risk Yönetimi Hususları

Etik, Önyargı ve Aşırı Güven

İç Denetim Kurumların YZ Tuzağından Kaçınmalarına Yardımcı Olabilir

Birçok faydasının yanı sıra, YZ'nin da kendi risklerine ilişkin listesi vardır. Tehditlerden bazıları kurum içi tehditlerdir ancak siber saldırılar kadar zararlı olabilirler.

Etik

Bu alandaki endişelerin birçoğu, iç denetçilerin, diğer olasılıkların yanı sıra, rapor hazırlamak, kod yazmak ve tavsiyelerin ve analizin taslağını oluşturmak amaçlarıyla kullanabildikleri üretken YZ ve geniş dil modelleri ile ilgilidir. Bununla birlikte, bu araçlar kurumlar için güvenlik ve etik sorularını da beraberinde getirmektedir. Grafenstine "Çalışanların bu araçlara bir salon oyunu veya oyuncak olarak bakma riski vardır," demiştir.

Daha önceki teknolojilerde kullanılan geleneksel siber kontroller bu sistemler için de geçerlidir ancak "bu kontrolleri iyi uygulamamanın sonuçları daha büyük olur," demiştir Grafenstine. Daha detaylı tartışılacak olan diğer konuların yanı sıra, bu sistemler nasıl eğitildiklerine bağlı olarak önyargılı, yanlış veya tamamen uydurma bilgiler sunabilmektedirler. Grafenstine, şirketin kötü kaynaklardan elde edilen internet verileriyle eğitilmiş müşteriye dönük bir sohbet robotu kullanması ve bu sohbet robotunun yanlış cevaplarının müşteriler üzerinde önemli bir olumsuz etki yaratması durumunda, şirketin işi ve itibarı için maliyetli ve potansiyel olarak utanç verici sonuçlar olacağına işaret etmektedir. Bu nedenlerle, kurumun üretken YZ sisteminin eğitildiği verilerden her yönüyle haberdar olmadığı durumlarda, bu sistemin ürettiği her şeyin insanlar tarafından gözden geçirilmesi gereklidir. Grafenstine "Şirket verdiği cevaplara sahip çıkmalıdır," demiştir.

ChatGPT gibi üretken YZ programlarının kullanımı 2022'nin sonlarında piyasaya sürülmelerinden bu yana hızla artarken kamuya açık üretken YZ'de bilgi yayınlamak, tıpkı bir bilgisayar korsanlığı olayının yapabileceği gibi, şirket veya müşteri verilerini ve kişiyi tanımlayan bilgileri ifşa edebilir ve önemli bir risk unsurudur. Çalışanlar şirket bilgilerini içeren sorguları kamuya açık üretken YZ programlarına gönderdiğinde, program bu bilgileri saklayacak ve potansiyel olarak kurum dışındaki diğer sorgulara yanıt vermek için kullanacak ve kamuya ifşa edecektir. Grafenstine, bunun yalnızca gizli bilgileri kamuya açık hale getirmekle kalmayabileceği, aynı zamanda kötü niyetli kişilerin kamuya açık üretken yapay zekada keşfettikleri ayrıntıları kimlik avı veya diğer araçlarla şirket sistemlerine girmek için kullanabilecekleri uyarısında bulunmuştur.

YZ Çıktısına Körü Körüne Aşırı Güvenmek

Tüm meslek sahipleri, kullandıkları araçlardan ve elde ettikleri bilgilerden nihai olarak sorumludurlar. Bu durum, doğrulanmamış veri veya içeriği çok fazla bel bağlamaları halinde kendi standartlarını ihlâl edebilecek olan iç denetçiler için özellikle doğrudur. "Güvenilir olmak bizim işimiz," demiştir Grafenstine.

Algoritmik Önyargı

Makineler spesifik algoritmalar temelinde öğrenecek şekilde eğitilirler ve ürettikleri bilgiler bu algoritmalardan kasıtlı olarak veya olmayarak etkilenebilmektedir. Örnek olarak, algoritmalar, belirli bir rolde mevcut çalışanlar ağırlıklı olarak erkekse işe alma kararında kullanılan kadınlara ait özgeçmişleri filtreleyebilir ya da mevcut ipotek sahiplerinin çoğu beyazsa beyaz alıcılardan gelen ipotek başvurularını tercih edebilir.[7] Grafenstine "Bu sistemler kasıtlı olarak kötü niyetli olmaya çalışmıyor ancak önyargıları var," demiştir.

[7] "Önyargılı AI algoritmaları azınlıklar için hayatın neredeyse her alanına zarar verebilir (For minorities, biased AI algorithms can damage almost every part of life)," The Conversation, www.theconversation.com, 24 Ağustos 2023.

Yapay Zekayı Korumak ve Ona Karşı Korunmak

İç Kontroller Kritik Düzeyde Önemlidir

YZ Sistemlerinin Bütünlüğünün Korunması, Erişim

YZ'nin kendisi üzerinde güvenlik ve onu kullanma becerisi, kurumlar ve iç denetçiler için dikkate alınması gereken diğer ciddi hususlardır. YZ kaynaklarına kimin erişim sağlayabileceği, kod değiştirme yetkisinin nasıl korunduğu ve kimin test alanından üretime bilgi iletmesine izin verildiği konularında kontroller bulunması gereklidir. Grafenstine bir iç denetçi olarak "YZ algoritmasının değiştirilip değiştirilmediğini ya da birinin bir sürecin ortasında bu algoritmayı bozarak değiştirip değiştiremeyeceğini anlayabileceğimden emin olmak istiyorum," demiştir. İç denetçilerin müdahalenin potansiyel kapsamından da haberdar olmaları gereklidir. Grafenstine "Eğer şirket yapay zekanıza erişim sağlayabilirsem tek bir işlemi değiştirmekle kalmam," demiştir. Bunun yerine, kötü niyetli aktör kurumun bütün veri havuzuna veya veri deposuna ya da YZ'nin erişimi olan her şeye girebilir.

> "YZ'den yararlanan bir çözümü uygulamaya koymuş olmanız, artık kurşun geçirmez olduğunuz anlamına gelmez."
>
> Aneta Waberska

Aynı zamanda, YZ'nin siber suçluların kötü amaçlı yazılımları hızlı şekilde yaratmasını, saldırıları otomatize etmesini ve sahte resim veya mesajlar yaratmak için, örneğin video veya resimleri dijital olarak değiştiren deepfake ve YZ ses oluşturucular gibi araçlar kullanarak onların dolandırıcılık veya sosyal mühendislik saldırılarının etkinliğini iyileştirmesini kolaylaştırdığının farkında olmak da önemlidir. IEEE Bilgisayar Topluluğunun bir makalesine göre "Siber tehdit ortamı giderek daha tehlikeli hale gelmektedir ve YZ bunda büyük bir rol oynamaktadır."[8]

Waberska, iç denetçilerin YZ'yi ofansif ve defansif bir araç olarak görmeleri gerektiğini belirtmiştir. "YZ'den yararlanan bir çözümü uygulamaya koymuş olmanız, artık kurşun geçirmez olduğunuz anlamına gelmez," demiştir. Önceki saldırılar genelde tek bir bilgisayar korsanı tarafından tek bir kuruma yönelik yürütülürken YZ daha büyük ölçekte saldırılar gerçekleştirerek birden fazla kurumu vurabilmektedir. YZ, geçmiş programlardan öğrenerek kötü amaçlı yazılımı geliştirebilir ve bu bilgiyi daha iyi ve daha güçlü kötü amaçlı yazılımlar oluşturmak için kullanabilir; tüm bunları herhangi bir geliştiriciye ihtiyaç duymadan kendi başına yapabilir. Waberska "Eğer YZ kurumunuza zorla girmeye çalışıyorsa mevcut çözümünüzden çok daha güçlü olabilir," demiştir. İç denetçiler, kurumlarının bu riskleri anlamasını ve bunları ele almaya hazırlıklı olmasını sağlayabilirler. İç denetim ekibi çözümleri uygulamaya koyamaz ancak bahsi geçen tehditleri dikkate alıp almadıklarını ve çözümleri uygulayıp uygulamadıklarını görmek için güvenlik ekibiyle bilinçli ve bilgiye dayalı bir görüşme yapabilirler. Waberska "Kurumların yeni çözümler benimsemesi zaman alacaktır ancak tehditlerin farkında olmak ve kendini korumak için plan yapmak önemlidir," demiştir.

İnsan Unsuru Unutulmamalı

Kurumlar kurum dışı siber tehditleri uzaklaştırmak için vites artırırken iç denetçilerin kendi çalışma arkadaşlarının sebep olduğu, dikkatsizlikten kaynaklanan tehditlerin yarattığı tehlikeyi unutmamaları gereklidir. Örneğin kimlik avı girişimleri, insanların bir siber suçlunun sisteme girmeye ya da önemli bir şifreyi veya gizli veriyi elde etmeye çalıştığını fark edemedikleri bir insan hatasından dolayı başarılı olmaktadır. Waberska "İç denetçilerin, kurumun kullanıcıları bu tehditler konusunda nasıl eğittiğine bakmaları gereklidir," demiştir. Özellikle de çalışanlar kimlik avı e-postalarının evrim geçirdiğini anlamayabilirler. Bir zamanlar yazım yanlışları veya garip yazı stilleri gibi kırmızı bayrakları fark etmekken kolaydı ama şimdi çok daha sofistike ve gerçekçi kimlik avı e-postları yazmak için YZ kullanılmaktadır. "Bu e-postalar çok gerçek görünüyor ve kötü niyetli aktörlerin onları oluşturması çok daha kolay," demiştir Waberska.

[8] "Siber Güvenlik ve Siber Suç için YZ: Yapay Zeka Kendisiyle Nasıl Savaşıyor (AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself)," Gaurav Belani, IEEE Computer Society Tech Trends, 6 Eylül 2023.

Varılan Sonuçlar

Siber saldırı tehdidi dijital dünyada iş yapmanın daimî bir özelliğidir ve YZ ve onun evrim geçiren kullanımı bu tehdide karşı yürütülen risk yönetimi savaşında yeni ve provokatif bir dönüm noktası sunmaktadır. İç denetçilerin aşağıdaki konularda oynayacağı önemli bir rol vardır:

- Liderlerin ve önemli ekiplerin YZ ile ilişkili faydaların ve tehlikelerin farkında olmasını sağlama.
- YZ'nin kurum bünyesinde çeşitli siber güvenlik çaba ve çalışmalarını nasıl geliştirebileceğini belirleme ve bu konuda tavsiyeler verme.
- YZ destekli siber saldırı araçlarına karşı güncellenmiş savunmaları dikkate alma ihtiyacına ilişkin farkındalığı teşvik etme.
- Şirketin YZ teknolojilerini anlaması ve kullanması konusunda güvence sağlama.

YZ ve ilişkili teknolojiler, değerli kaynaklar olarak hizmet edebilirler ancak nihai cevap değildirler. Waberska "Teknolojideki gelişmeler, onları akıllı ve güvenli bir şekilde nasıl kullanacağınızı bildiğiniz sürece iyi olabilir. Karşılığında ne aldığınızı değerlendirirken mesleki muhakemenizden faydalanmanız gerekir."

Grafenstine, muhafazakâr olmanın iç denetçiler için bir değer olduğunu ancak sürekli hayır diyen bir "ret makamı" olmamaları gerektiğini de akıllarında tutmalarını söylemiştir. İç denetçilerin teknolojiyi takip etmemeye bağlı riskler hakkında içgörüler de dâhil olmak üzere iyi kontrol ve risk tavsiyesi sağlamaları gereklidir. "Teknolojiyi benimsememek muazzam bir risktir ancak bunu dikkatli bir şekilde yapmalıyız," demiştir.

Kısım 3: Siber Güvenlik Üçüncü Taraf Risk Yönetimi

Uzmanlar Hakkında

Richard Marcus, CISA, CRISC, CISM, TPECS

AuditBoard kurumunda Bilgi Güvenliği Başkan Yardımcısı olarak görev yapan Richard Marcus ürün, altyapı ve kurumsal BT güvenliğine odaklanmanın yanı sıra AuditBoard kurumunun kendi kurum içi uyum girişimlerine de liderlik etmektedir. Bu sıfatla uyum, risk değerlendirmesi ve denetim kullanım durumlarını karşılamak için platformun güçlü özellik setinden yararlanarak güçlü bir AuditBoard ürünü kullanıcısı haline gelmiştir.

John A. Wheeler

John A. Wheeler, küresel işletmelerin daha fazla risk görünürlüğü ve anlayışı elde etmelerine yardımcı olan üst düzey yönetici danışmanlık firması Wheelhouse Advisors kurumunun kurucusu ve CEO'sudur. Müşterilerine stratejik rehberlik ve teknoloji çözümleri sunmak için risk yönetimi, siber güvenlik, dijital iş, operasyonel risk ve entegre risk yönetimi alanlarındaki uzmanlığından yararlanmaktadır.

GİRİŞ

Dünya giderek daha fazla birbirine bağlı hale gelmektedir ve endüstri de bunun bir istisnası değildir. Günümüzde, neredeyse tüm büyük iş sektörleri bir şekilde üçüncü taraflara bel bağlamaktadır. Önceki nesillerde, bu durum, öncelikli olarak, bir tarafın mal veya hizmetler için başka bir tarafa bel bağladığı fiziksel bir perspektiften kaynaklanmış olabilir. Bu hâlâ doğru ve geçerli olsa da şimdi taraflar arasındaki bu bağlantı dijital dünyayla iç içe geçmiş haldedir.

Doğal olarak, bu trendin -özellikle de etkinlik, üretkenlik ve sürdürülebilirlik taahhütlerini daha iyi karşılama konusunda- birçok faydası olmasına rağmen, dikkate alınması zorunlu olan riskler de vardır. Deloitte kurumunun hazırladığı 2022 Küresel Üçüncü Taraf Risk Yönetim Anketine göre, ankete katılanların %73'ü şu anda üçüncü taraf bulut hizmet sağlayıcılarına yüksek düzeyde bağımlıdır ve bu oranın önümüzdeki yıllarda %88'e yükselmesi beklenmektedir.[9] Bununla birlikte, bu tür ilişkilerin başarılı olabilmesi için, aktarılan verilerin siber saldırılara, veri ihlâllerine veya başka ilişkili siber olaylara karşı mümkün olduğunca güvende olacakları konusunda kurumlar arasında samimi bir güven olması zorunludur. Kurumların bu güveni kazanabilmeleri için bu amaca adanmış ve kapsamlı bir üçüncü taraf risk yönetimi (TPRM) programının olması gereklidir; bu program üçüncü taraf tedarikçileri sisteme alırken ve onları ilişkinin yaşam döngüsü boyunca sürekli olarak izlerken durum tespiti yapmaktadır.

Bununla birlikte, gerçek şu ki şirketler çoğu zaman yeterli durum tespiti yapmadan güven duymaktadırlar. AuditBoard kurumunda Bilgi Güvenliği Başkan Yardımcısı olan Richard Marcus "Tüm üçüncü taraflar — tedarikçi, ürün bileşeni tedarikçisi, ortak veya müşteri — kurumunuz için yeni siber riskler teşkil edebilir. Güçlü üçüncü taraf risk yönetimine yönelik ihtiyaç zamanla artmaktadır ve birçok kurum buna ayak uyduramamaktadır," demiştir.

Siber güvenlik hakkında üç kısımdan oluşan bu serinin son kısmı olan bu Küresel Bilgi Özeti, üçüncü taraflar ile ilişkili siber risklerin ne kadar önemli hale geldiğinin altını çizecek ve iç denetçilerin üçüncü taraf siber risk yönetiminde nerede durabileceklerini ele alacaktır.

9. 2022 Global Third-Party Risk Management Survey, Deloitte, 2022, https://www.deloitte.com\content\dam\Deloitte\us\Documents\TPRM_Survey_Report_Interactive.pdf.

Muazzam Bir Zorluk

Siber Riskler Üçüncü Taraf Risk Yönetimi Tartışmalarına Damgasını Vuruyor

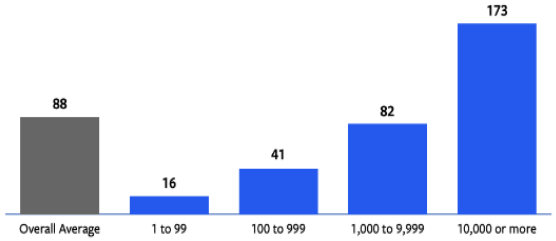
Yükselişteki risk

CyberRisk Alliance kurumunun yayınladığı yakın tarihli bir raporda (AuditBoard sponsor olmuştur), ABD merkezli 209 güvenlik ve BT lideri ve yöneticisinin, güvenlik yöneticisinin ve uyum profesyonelinin katıldığı bir anket yapılmıştır. Bu anket, üçüncü taraf siber riskinin ne kadar muazzam boyutlara ulaştığını ortaya çıkarmıştır. Anketten elde edilen içgörüler aşağıdaki gibidir:

- Şirketlerin ortalama olarak 88 üçüncü taraf ortağı (yazılım tedarikçileri, BT hizmeti tedarikçileri, BT hizmeti ortakları, iş ortakları, brokerler, alt yükleniciler, fason üreticileri, distribütörler, temsilciler ve bayiler de dâhil) vardır. Bu sayı kurumun büyüklüğüne göre önemli ölçüde çeşitlilik göstermektedir ve 1-99 personeli olan şirketlerin ortalama 16 ortağı bulunurken, 10.000 veya daha fazla personeli olan şirketlerin ortalama 173 ortağı vardır (bakınız: Şekil 1).
- Ankete katılanların %57'si, son 24 ayda bir BT güvenlik olayının (bir saldırı veya ihlâl) kurbanı olduklarını rapor etmiştir. Buna ilave olarak, kurumlar son iki yılda ortalama iki kez üçüncü tarafla ilişkili güvenlik olayı yaşamıştır.
- Böyle bir olay deneyimleyenlerin %52'si saldırının kaynağının bir yazılım tedarikçisi olduğunu belirtirken, %39'u olaydan bir iş ortağının, alt yüklenicinin veya BT hizmeti sağlayıcısının sorumlu olduğunu söylemiştir (bakınız: Şekil 2)[10].

Şekil 1

Ortalama Üçüncü Taraf Sayısı, Kurum Büyüklüğüne göre



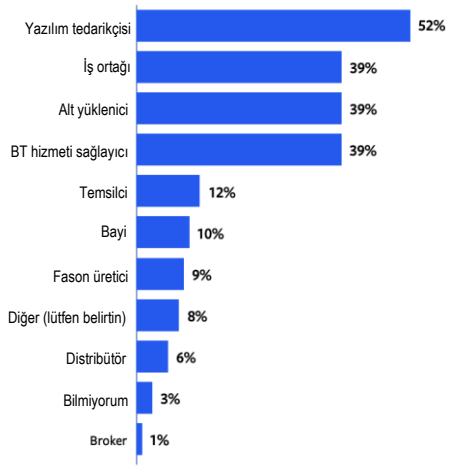
Soru: Kurumunuz şu anda yaklaşık kaç üçüncü tarafla sözleşme yapmıştır? Tüm tedarikçileri (yazılım tedarikçileri ve BT hizmet tedarikçileri de dâhil), iş ortaklarını, brokerleri, alt yüklenicileri, fason üreticileri, distribütörleri, temsilcileri ve bayileri ekleyiniz.

Not: Şekil 1 ve Şekil 2'deki grafikler ve veriler, CyberRisk Alliance ve Auditboard kurumlarının yayınladığı "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," yayınından (sayfa 9 ve sayfa 18) alınmıştır; Ocak 2023.

Şekil 2

Bu saldırıların veya ihlâllerin kaynak(lar)ı aşağıdakilerden hangisidir?

İlgili olanların tümünü seçiniz.



10. "Üçüncü Taraf Riski: Daha Fazla Üçüncü Taraf + Sınırlı Tedarik Zinciri Görünürlüğü = Kurumlar için Büyük Riskler (Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations)," CyberRisk Alliance and AuditBoard, Ocak 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

Değişime Ayak Uydurmak

Wheelhouse Advisors kurumunun kurucusu ve CEO'su olan John Wheeler'a göre, bu sorunların temel nedenleri çeşitlidir ancak hızlı bir şekilde değişen iş modelleri ve üçüncü taraf risk yönetimi süreçlerinin bu değişime uyacak şekilde güncellenememesinin bir kombinasyonundan kaynaklanmaktadır. Wheeler "Tecrübelerime göre en büyük, en önemli riskler büyük değişimlerden kaynaklanıyor. Büyümeye yönelik zorlu görev, şirketleri yeni dijital ürün ve hizmetler yaratmaya teşvik ederek büyük bir değişime yol açıyor," demiştir.

Bu noktada, Wheeler AuditBoard kurumunun "2023 Dijital Risk Raporu: Yaygın Risk, Kalıcı Parçalanma ve Hızlanan Teknoloji Yatırımı" yazısını kaleme almıştır. ABD merkezli 130'dan fazla risk liderinin katıldığı bir ankette, katılanların %21'i üçüncü taraf dijital riskini yönetip izlerken kalitatif veya kantitatif risk değerlendirmesi yapmadığını ve %56'sı kantitatif değerlendirmelere kıyasla sınırlı olan kalitatif değerlendirme yaklaşımlarına itimat ettiğini belirtmiştir.[11]

ÜÇÜNCÜ TARAF RİSKİNİ YÖNETMEK İÇİN MANUEL TEKNOLOJİLERE BEL BAĞLAYAN KURUMLARIN YÜZDESİ

AuditBoard 2023 Dijital Risk Raporu Yaygın Risk, Kalıcı Parçalanma ve Hızlanan Teknoloji Yatırımı

Wheeler, üçüncü taraf siber riskleri gibi dijital riskleri yönetenlerden %44'ünün -ki bu oran hayret vericidir- bunu yapmak için hâlâ manuel teknolojilere (hesap tabloları, e-postalar, ortak sürücüler ve Sharepoint) bel bağlamasının da eşit düzeyde endişe verici olduğunu belirtmiştir. "Bu, çok zaman tüketen bir yaklaşım," demiştir. "Gerçek şu ki parçalanmış, esnek olmayan ve uyum odaklı eski yönetişim, yani GRC [yönetişim, risk ve uyum] yazılımı dijital riske ayak uydurmaya ihtiyaç duyan birbirine bağlı risk yeteneklerini sağlayamaz ve sonuç olarak, çoğu kurum hâlâ kısmen manuel süreçlere dayanmaktadır."

Bu durum özellikle kötü niyetli aktörlerin gün geçtikçe daha sofistike hale gelen saldırı modelleri açısından endişe vericidir. Marcus "Son birkaç on yılda ihlâllerin nasıl meydana geldiğinin kök nedenlerine bakarsanız çoğunun ön kapıda, uygulama veya altyapı katmanlarında meydana geldiğini görürsünüz. Dolayısıyla, güvenlik ekiplerinin zaman ve kaynak yatırımı yapması gereken burasıdır. Ancak saldırganlar zekidir. En az direnç gösterecek yolu arayacaklardır ve bu da çoğu zaman üçüncü taraf siber güvenlik önlemlerindeki boşlukların neden olduğu arka kapılar olacaktır," demiştir.

Düzenleyici Baskılar

Sürekli değişen ve yakın zamanda riskin hızına uyacak ivmeyi yakalayan düzenleyici ortam, kurumların üçüncü taraf siber riskleri konusunda hissettikleri baskılara katkı yapan faktörlerden biridir. ABD federal hükümetinin tedarik zinciri ortaklarına getirdiği yeni zorunluluklar bu değişiklikler arasında yer almaktadır ve bu zorunluluklar birçok sektörde etkisini göstermektedir. Marcus "Veri güvenliğine ilişkin daha fazla şeffaflık gerektiren federal zorunlulukların sadece federal hükümetle iş yapan şirketleri etkileyebileceğini düşünebilirsiniz ancak tedarik zincirinde aşağı doğru akan ve hiyerarşi veya hizmet sağlayıcılar aracılığıyla kademelere ayrılan üçüncü ve dördüncü taraf gereklilikleri vardır. Bu durum birçok endüstriye nüfuz eden hesap verebilirlik kültürü yaratmaktadır," demiştir.

Düzenleyici organlar da üçüncü taraf siber güvenlik risklerini ele almak için daha resmi adımlar atmaya başlamışlardır. Bu, ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) tarafından yakın zamanda çıkartılan yeni kuralları, örneğin tescil olanların önemli siber güvenlik olaylarını açıklamasını şart koşan yeni kuralları içermektedir. Marcus "Yeni kurallar veya yönetmelikler şirketiniz için doğrudan doğruya geçerli olmasa bile bu kurallar siber güvenlik kültürüne nüfuz eder. Şeffaflık ve hesap verebilirlik beklentisini yaratan kültürel bir değişimdir," demiştir.

11. "2023 Dijital Risk Raporu: Yaygın Risk, Kalıcı Parçalanma ve Hızlanan Teknoloji Yatırımı (Digital Risk Report 2023: Pervasive Risk, Persistent Fragmentation, and Accelerating Technology Investment)," John A. Wheeler, Auditboard, Temmuz 2023, https://www.auditboard.com/resources/ebook/digital-risk-report-2023/.

İç Denetim Yaklaşımı

İpuçları, Stratejiler ve Odak Alanları

Siber eylem kültürünün oluşturulması

Kurumlar bu eksikliklerden habersiz değildir. Gerçekten de bu farkındalık her zaman kurum çapında bir anlayışa ve eyleme dönüşmese bile çoğu bir şekilde bunların farkındadır. Her ne kadar üçüncü taraf siber güvenliğin teknik ayrıntılarını doğrudan doğruya ele alabilmek için yeterli siber güvenlik bilgisine sahip olduğunu iddia edebilecek iç denetim fonksiyonlarının sayısı az olsa da bu riskin yönetimine karılan çeşitli paydaşların (örneğin hukuku, satın alma, BT ve üçüncü tarafların kendisi) bakış açılarını birleştirmek için eşsiz oldukları pozisyonlardan faydalanabilirler. Buna ilave olarak, iç denetçiler, bu bakış açısının düzenli ve doğru olarak raporlandığından emin olmak için denetim komitesi ve yönetim kurulu ile kurdukları doğrudan etkileşimi kullanabilirler.

Wheeler, bu bakış açısının CEO'lar ve kurum liderleri için uygun eylemleri teşvik etmek açısından son derece kritik olduğunu ve risk yönetimi fonksiyonlarının bunu ifade edebilecek kadar anlamak için çaba göstermesi gerektiğini söylemiştir. "CEO'lar kurumun hem içinden hem de dışından, dinamik olarak değişen bütün teknoloji varlıkları ekosistemi boyunca gerçek zamanlı içgörülere ihtiyaç duyar. Bu süreç sayesinde dijital ürün ve hizmetleri hakkında daha iyi bir anlayışa sahip olacaktırlar," demiştir.

Bununla birlikte, kurum bünyesinde birlik olmak yeterli değildir. Bu süreç kurumun dışındaki paydaşları da içermek zorundadır. Marcus "Her üçüncü taraf ilişkisinde tedarikçi ilişkisini sürdürmekten, tedarikçi irtibat bilgisini tutmaktan ve sözleşme şartlarını yönetmekten sorumlu olan bir atanmış ilişki sahibi veya sorumlu kişisi olması gereklidir. Üçüncü taraf ilişkileri bir tedarikçiden diğerine farklılık gösterir – bazı tedarikçiler kurumunuza ilave hizmetler sunan atanmış bir müşteri destek veya başarı ekibi sağlarken diğerleri 'al-kullan' yaklaşımı benimser. Kurumunuz ve çalıştığı üçüncü taraflar arasındaki iletişim hatlarının açık ve net tutulması, etkili üçüncü taraf risk yönetiminin önemli ancak genelde göz ardı edilen bir bileşimidir," demiştir.

Bu tür bir kültür yaratmak önleyici eylemleri teşvik etmekle kalmaz, aynı zamanda bir siber saldırı veya ihlâl meydana geldiğinde verilecek tepkilerin hızını da artırmaktadır. CyberRrisk Alliance raporunda, ankete katılanların %20'si bir saldırı veya ihlâli değerlendirmek için bir hafta veya daha uzun süre gerekebileceğini belirtmiş ve sürenin uzamasını, tedarikçilerin veya ortakların bunları raporlamasını veya bunların sorumluluğunu üstlenmesini sağlamadaki zorluklara bağlamıştır.[12] Kurum içinde ve kurumun tedarik zinciri boyunca pozitif ve şeffaf bir siber kültürün yaratılması bu süreleri haftalardan saatlere düşürerek süreçte meydana gelebilecek kayıp ve zararları büyük oranda azaltmaktadır.

"Bütün üçüncü taraf risk yönetim süreci," demiştir Marcus "herkesin üçüncü taraf risklerinin farkında olduğu bir hesap verebilirlik kültürü etrafında inşa edilmelidir."

Risk seviyesine dayanan sürekli bir izleme yaklaşımı

İç denetim, yaklaşımı belirlemenin ötesinde, siber risklerle ilgili olduğu için üçüncü taraf risk yönetimi programının hazırlanmasında ve sürekli olarak değerlendirilmesinde değerli bir kaynak olabilir ve olması gereklidir.

"İç denetimin birincil sorumluluğunun, tıpkı çoğu vakada olduğu gibi, TPRM programının etkinliğini değerlendirmek olduğunu söyleyebilirim," demiştir Marcus. "Bu, kurumda kullanılmakta olan tüm üçüncü tarafların eksiksiz bir envanterini veya resmini, bu üçüncü tarafların kurumu maruz bırakabileceği riskleri anlamayı ve kurumun bu üçüncü taraf kurumlardaki kontrollerin gücünü nasıl değerlendirdiğini anlamayı içerebilir."

12. "Üçüncü Taraf Riski: Daha Fazla Üçüncü Taraf + Sınırlı Tedarik Zinciri Görünürlüğü = Kurumlar için Büyük Riskler (Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations)," CyberRisk Alliance and AuditBoard, Şubat 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

Yine, teknik analiz için konunun uzmanlarından faydalanmak gerekmesine rağmen, iç denetimin kullandığı risk yönetim ilkelerinin birçoğu bu konu için de geçerlidir.

Örneğin, iç denetimin genellikle ısı haritaları veya diğer araçlar kullanılarak görselleştirilen risk analizine ilişkin sağlam bir anlayışı olması gereklidir. Bu tür taktikler, kimin veya neyin önceliklendirilmesini daha iyi anlaması gereken ve üçüncü tarafların sürece dâhil edilip izlenmesinden sorumlu olan paydaşlar için bir rehber olarak kullanılabilir.

"TPRM programı için en önemli başarı faktörü, risk seviyesine dayanan sürekli devam eden izleme faaliyetlerini yapılandırmak ve resmileştirmektir," demiştir Marcus. "Daha yüksek riskli üçüncü taraflara daha fazla ve daha sık dikkat edilmelidir ve daha düşük riskli üçüncü taraflara daha az sıklıkta daha az dikkat edilmelidir."

Marcus, söz konusu üçüncü taraf kendi içinde yüksek riskli olmasa bile, ilişkinin doğasının -örneğin aktarılan verilerin türü (örneğin gizli veriler, müşteri verileri, özel veriler) gibi- risk kategorizasyonunu yükseltebileceğini veya düşürebileceğini belirtmektedir.

Bu göreve yardımcı olmak amacıyla, AuditBoard, aşağıdaki üç risk kademesi kategorisiyle ilgili incelemelerin nasıl yapılandırılacağı konusunda bir başlangıç noktası olarak aşağıdaki örneği (Şekil 3) kullanmaktadır:[13]

Şekil 3

Risk Kademe Özellikleri	Kademe 1 – Yüksek Risk	Kademe 2 – Orta Risk	Kademe 3 – Düşük Risk
Veri Erişimi	**Gizli**	**Kişiye özel**	**Halka açık veya Yok**
Gözden geçirme sıklığı	**1 yıl**	**2 yıl**	**3 yıl**
Gözden geçirme gereklilikleri	**Yerinde denetim** **Kontrol soru formu** **Sertifikasyon incelemesi**	**Sertifikasyon incelemesi**	**Yok**

Not: Şekil 1 ve Şekil 2'deki grafikler ve veriler, Auditboard kurumunun yayınladığı "Effective Third-Pary Risk Management: Key Tactics and Success Factors" yayınından (sayfa 8) alınmıştır; 2022.

Üçüncü taraf güvenlik incelemesi işe alma ve alıştırma sürecinde bitmez; algılanan risk seviyesi esas alınarak sürekli gözden geçirilmesi gereklidir. Paydaşların düzenli gözden geçirme taahhütlerinden ve bu tür gözden geçirmeleri yürütmek için kullandıkları süreçlerden haberdar olmalarını sağlamak, iç denetim risk evreninin tam ortasında yer almalıdır. Bu tür süreçlere ilişkin fikirler aşağıda satılanları içerebilir:

- SOC 2 gibi uyum sertifikalarının ve raporlarının kontrol edilmesi. Uyum sertifikasyonlarını kontrol etmek için yaygın çerçeveler arasında SOC 2, ISO 27001 ve NIST SP 800-161 yer alır.
- Standartlaştırılmış soru formlarının kullanılması. Bunların arasında Standartlaştırılmış Bilgi Toplama Soru Formu (SIG) veya Cloud Security Alliance kurumundan CCM ve CAIQ yer alabilir.
- Güvenlik kontrolü soru formları.

Yazılım Çözümlerini Benimseme

Bu kadar çok değişkeni bir arada tutmak için, hem iç denetimin hem de diğer risk yönetim fonksiyonlarının manuel süreçlerden uzaklaşarak yazılım çözümlerine yönelmeyi önceliklendirmeleri gereklidir. "İç denetim, üçüncü taraf risk yönetim süreçlerini daha verimli hale getirecek teknolojilere yatırım yapılmasını destekleyebilir," demiştir Marcus. "Birçok durumda, ölçek verimliliği bunu

13. "Etkili Üçüncü Taraf Risk Yönetimi: Önemli Taktikler ve Başarı Faktörleri (Effective Third-Party Risk Management: Key Tactics and Success Factors)," AuditBoard, Ocak 2022, https://www.auditboard.com/resources/ebook/effective-third-party-risk-management-key-tactics-and-success-factors/?utm_campaign=effective-third-party-risk-management-key-tactics-and-success-factors-0122022&utm_medium=download-image&utm_source=blog.

gerektirmektedir. Üçüncü taraf risk uygulamalarını uygulamaya koyduğum ilk kurumlardan birini hatırlıyorum: Beş veya altı tedarikçi için risk değerlendirmesi yaptık ve ardından, bu süreci tüm tedarikçileri kapsayacak şekilde genişletmeyi düşündük. Bununla birlikte, bu şirkette 17.000 tedarikçi olduğunu gördüğümüzde çok şaşırdık. Yüzlerce, binlerce veya on binlerce tedarikçinin ölçeklendirilmesini kolaylaştıracak teknoloji destekli bir platform olmadan bunu yapabilmenin hiçbir yolu yoktur."

Buna ilave olarak, bu tür çözümler iç denetimin diğer üçüncü taraf risk fonksiyonlarıyla daha yakın işbirliği yapması için mükemmel bir fırsat sunmaktadır. "İşbirliğinin önündeki engellerin birçoğu veri paylaşımını ve iş akışı sorunlarını içerir," demiştir Marcus. "İki ekibin tedarikçi tablosunu -aynı panoyu, aynı tedarikçi veri tabanını vb. kullanarak- birlikte değerlendirebildikleri bir teknoloji platformunun mevcut olması birlikte daha verimli çalışmalarına ve ortak sonuçlara yönelmelerine izin vermektedir".

İşe almanın yanı sıra işten çıkarmaya da odaklanma

Üçüncü taraf ilişkileri nadiren sonsuza kadar sürer. Bununla birlikte, bir ilişkinin resmi olarak bitmesi her zaman taraflar arasındaki veri hatlarının kapandığı anlamına gelmemektedir. Her ne kadar bariz gibi görünse de bu unutulan hatlar kurumların üçüncü taraf siber güvenlik sistemlerinde bulunan en büyük açıkların bazılarından sorumludur ve kasıtlı veya kasıtsız olarak istismar edilmeye hazır "dijital arka kapılar" oluşturmaktadırlar. Bu, iç denetçilerin üçüncü taraf gözden geçirme uygulamalarını değerlendirirken gözden kaçırmaması gereken bir husustur.

"İşten çıkarma aşamasında detay odaklı çalışmak elzemdir," demiştir Marcus. "Günümüzün iç içe geçmiş dijital ekosisteminde, kaldırılması veya devre dışı bırakılması gereken üçüncü taraf hesaplarının, hizmetlerinin veya kullanıcılarının gözden kaçırılması kolaydır. Erişim ayrıcalıklarının iptal edilmesi, kullanıcı hesaplarının devre dışı bırakılması ve üçüncü taraflarca verilen tüm yazılım veya uygulamaların kaldırılması gerekir. Bu, iç denetimin kesinlikle incelemesi gereken bir konudur."

Varılan Sonuçlar

Kurumların geleceği siberdir. Her geçen yıl, bu trendin kalıcı olacağı açıkça görülmektedir ve siber güvenliğin daha uzmanlaşmış beceri setleri gerektirmesi iş dünyasının paydaşların kendilerini eğitmelerini bekleyeceği anlamına gelmemektedir. Siber güvenlik sürekli bir öğrenme serüvenidir ve üçüncü taraf ilişkilerine katılan tüm tarafların da siber güvenliği bu şekilde değerlendirmesi gerekir.

Neyse ki kurumların bu gerçeği kabul ettiklerine dair olumlu işaretler vardır. CyberRisk Alliance Business Intelligence raporunda, üç katılımcıdan neredeyse iki tanesi üçüncü taraf saldırısı riskini önlemek veya hafifletmek için kullandıkları en yaygın önlemin personel eğitimi olduğunu belirtmiştir.[14] Üçüncü taraflarla ilişkili riskler hiçbir zaman son bulmayacak bile olsa, politika ve müdahaleler bu risklerin de diğer herhangi bir yerleşik risk gibi kolay yönetildiği bir noktaya ulaşacaktır. O zaman bugün değil ancak oraya yaklaşıyoruz ve etkili iç denetim risk yönetimi güvencesi kurumların oraya güvenli bir şekilde ulaşmasına yardımcı olacaktır.

14. "Üçüncü Taraf Riski: Daha Fazla Üçüncü Taraf + Sınırlı Tedarik Zinciri Görünürlüğü = Kurumlar için Büyük Riskler (Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations)," CyberRisk Alliance and AuditBoard, Şubat 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

IIA Hakkında

İç Denetçiler Enstitüsü (IIA) 235.000'den fazla küresel üyeye hizmet veren ve dünya çapında 190.000'den fazla Sertifikalı İç Denetçi (CIA) sertifikası vermiş olan, kâr amacı gütmeyen uluslararası bir meslek kuruluşudur. 1941 yılında kurulan IIA, dünya çapında iç denetim mesleğinin standartlar, sertifikalar, eğitim, araştırma ve teknik rehberlik alanlarında lideri olarak tanınmaktadır. Daha fazla bilgi için, lütfen theiia.org adresini ziyaret ediniz.

AuditBoard Hakkında

AuditBoard denetim, risk, uyum ve ÇSY yönetimini dönüştüren lider bulut tabanlı platformdur. Fortune 500 listesinde yer alan kurumların %40'ından fazlası AuditBoard'dan yararlanarak işletmelerini daha fazla netlik ve çeviklikle ileriye taşımaktadır.

AuditBoard G2, Capterra ve Gartner Peer Insights'ta müşterileri tarafından en yüksek puanları almıştır ve kısa süre önce Deloitte tarafından üst üste beşinci yıl Kuzey Amerika'nın en hızlı büyüyen teknoloji şirketlerinden biri olarak gösterilmiştir. Daha fazla bilgi için: AuditBoard.com.

Sorumluluğun Reddi Beyanı

IIA bu dokümanı bilgi ve eğitim amaçlı yayımlamaktadır. Bu materyalin spesifik münferit koşullara kesin ve nihai cevaplar vermesi beklenmemelidir ve bu nedenle sadece akran bilgisine dayalı düşünce liderliği olarak kullanılmak üzere amaçlanmıştır. Resmi IIA Rehberi değildir. IIA, herhangi bir spesifik durumla doğrudan ilgili konularda bağımsız uzman tavsiyesi almanızı önerir. IIA, herhangi bir kimsenin bu rehberi tek referans kaynağı olarak kullanması durumunda hiçbir sorumluluk kabul etmezl.

Global Knowledge Briefs are intended to address topics that are timely and relevant to a global internal audit audience, and each topic covered is vetted by members of Küresel Bilgi Özetlerinin küresel bir iç denetim kitlesi için güncel ve ilgili konuları ele alması amaçlanmaktadır ve ele alınan her konu IIA'nın gönüllü Kuzey Amerika İçerik Danışma Komitesi üyeleri tarafından incelenmektedir. Konu uzmanları, öncelikli olarak IIA'nın Küresel Rehberlere Katkıda Bulunanlar listesinden belirlenmekte ve seçilmektedir.

Küresel Rehberlere Katkıda Bulunanlar listesine eklenmek üzere başvuruda bulunmak için şu adrese e-posta atınız: Standards@theiia.org. Gelecek Küresel Bilgi Rehberleri için konu önerisinde bulunmak için: Content@theiia.org.

Telif Hakkı

Ocak 2024

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101