KÜRESEL BAKIŞ AÇILARI VE ANLAYIŞLAR

Siber Güvenlik

The Institute of Internal Auditors

BÖLÜM 1

Yapay Zeka ile Geliştirilmiş Bir Dünyada Siber Tehditler

Uzmanlar Hakkında

Antonio Cacciapuoti, CIA

Antonio Cacciapuoti, Intesa Sanpaolo Group'un varlık yönetim şirketi Eurizon Capital S.A. Luxembourg'da iç denetim başkanı olarak görev yapmaktadır.

Bradley Niedzielski, CPA

Bradley Niedzielski, Deloitte & Touche LLP'de denetim ve güvence ortağı ve Finans Dönüşümü ve GenAI Lideridir ve finansal hizmetler sektöründeki kamu ve özel şirketlere hizmet vermektedir.

Geçtiğimiz yıl yapay zeka (AI) alanındaki gelişmeler, kurumları bu teknolojilerin sunduğu fırsatları ve tehditleri anlamak ve ayak uydurmak için çabalamak zorunda bıraktı. Bu çabanın bir parçası olarak, şirketlerin, özellikle işletmelerin çevrimiçi bilgi ve işlemlere neredeyse tamamen bağımlı olduğu göz önüne alındığında, yapay zekanın güvenlik çabaları için oluşturabileceği artan tehlikeyi göz önünde bulundurmaları gerekiyor. Kötü aktörler, şirketlerin siber savunmalarını aşma becerilerini geliştirmek için hızla yapay zeka ile geliştirilmiş araçlara yöneldi. Bu özet, siber saldırıların
yapay zeka odaklı bir dünyada tehditlerin nasıl değiştiğini ve iç denetimin şirketlerin yeni siber güvenlik yaklaşımları geliştirmelerine nasıl yardımcı olabileceğini açıklamaktadır.

Siber Suçlarda Bir Evrim

Güçlü siber savunmalar her zaman kritik öneme sahip olsa da, kötü aktörler artık kurumların savunmalarını aşma yeteneklerini keskinleştirmek ve genişletmek için yapay zekayı kullanıyor. Eurizon Capital S.A. Lüksemburg'un iç denetim müdürü Antonio Cacciapuoti, "Yapay zeka yeni bir siber saldırı türü değil, bir evrim" diyor. Yapay zeka, hız, ölçek, karmaşıklık ve uyarlanabilirlik açısından geleneksel siber saldırılardan daha gelişmiş şekillerde kullanılmaktadır. Ayrıca, "bir virüs gibi, zaman içinde direnç kazanarak daha tehlikeli hale gelir" diyor.

Yapay zeka, dar odaklıdan geniş çaplı yıkıcıya kadar değişen saldırılarda kullanılıyor. Örneğin, New York'taki Deloitte'ta denetim ve güvence ortağı olan Bradley Niedzielski, iş dünyasındaki pek çok kişinin artık e-postalar veya raporlar için düzenli olarak yapay zeka tarafından oluşturulan belgeleri kullandığını, ancak kötü niyetli kişilerin de yapay zeka tarafından oluşturulan belgeleri suç amacıyla kullandığını söylüyor.

Bir başka cephede, oltalama saldırıları güvenlik bariyerlerini aşmayı ve değerli verilere erişim sağlamayı amaçlamaktadır. Kimlik avı yeni olmasa da FBI "belirli alıcılara göre uyarlanmış ve doğru dilbilgisi ve yazım kurallarını içeren ikna edici mesajlar oluşturma yetenekleriyle karakterize edilen, başarılı aldatma ve veri hırsızlığı olasılığını artıran" yapay zeka güdümlü kimlik avı saldırıları konusunda uyarıyor.

Örneğin otomatik oltalama, bir kişi veya bir grup için kişiselleştirilir ve hassas bilgileri çalmayı veya bir sisteme erişim sağlamayı amaçlar. Cacciapuoti, "Yapay zeka sosyal medyayı, iletişim kalıplarını ve bir hedef hakkındaki mevcut verileri analiz edebilir, ardından alıcıları hassas bilgileri ifşa etmeleri veya kötü amaçlı bağlantıları tıklamaları için kandırma olasılığı daha yüksek mesajlar oluşturabilir," diye açıklıyor. Aynı zamanda, geçmişte bir kişinin sesi veya özellikleri hakkındaki bilgilere dayanarak bir videoya veya aramaya güvenmek mümkün olabilirken, deepfakes (bir kişinin simüle edilmiş videoları) ve bir kişinin sesini taklit eden ses korsanlığı ile belirli hedefleri aldatmak ve manipüle etmek mümkündür.

Kurumların karşılaştığı yapay zeka ile ilgili tek tehdit bunlar değil. Cacciapuoti'ye göre, yapay zeka destekli kötü amaçlı yazılımlar, hedef ortama göre davranışlarını uyarlayabilir ve değiştirebilir, bu da geleneksel güvenlik sisteminin tespit etmesini zorlaştırır. "Temel tespitten kolayca kaçabilir ve kodunu değiştirmek için polimorfik teknikler kullanabilir ve hatta bunlardan kaçınmak için savunma önlemlerini analiz edebilir" diyor. Daha da önemlisi, bir dolandırıcılık tespit sisteminde kullanılan bir yapay zeka makine öğrenimi modeline zehirli veriler ekleyerek yapay zekanın yanlış tahminlerde bulunmasına ve bazı dolandırıcılık göstergelerini gözden kaçırmasına neden olabilir.

Akıllı veri sızdırma yöntemini kullanan yapay zeka, çalınan verileri ve fikri mülkiyeti gerçek zamanlı olarak analiz edebilir ve hangi bilgilerin sızdırma için en değerli olduğuna öncelik verebilir. Daha sonra bu bilgileri şifreleyebilir ve serbest bırakmak için fidye talep edebilir, diyor. Yapay zeka güdümlü saldırılar, geçerli kullanıcıların kimliklerini doğrulayan kimlik bilgilerini de tehlikeye atarak sistem içinde hareket etmelerini sağlayabilir.

Yapay zeka güdümlü siber saldırıların riskleri önemlidir çünkü riskler çok yüksektir. Hassas bilgilerin sızdırılması veya kötüye kullanılması, bir kuruluşun rekabetçi konumuna zarar verebilir veya veri gizliliği düzenlemelerine uymadığı için cezalara maruz kalmasına neden olabilir. Herhangi bir ihlal, müşterilerin ve iş ortaklarının kuruma olan güvenini kaybetmesine neden olabilir. Fidye yazılımı ve kötü amaçlı yazılım saldırıları operasyonları kesintiye uğratabilir ve kritik sistemleri kapatabilir.

Pek çok kullanım, kısa bir süre önce hayal bile edilemezdi, ancak bugün gerçek zamanlı olarak gerçekleşiyor. Örneğin, Hong Kong'daki çok uluslu bir firmanın bir çalışanı, bir video görüşmesinde şirketin finans müdürünün deepfake bir simülasyonu tarafından ikna edildikten sonra farkında olmadan dolandırıcılara 25 milyon dolar ödedi, CNN'e göre.

Başka bir yerde, The Drive, bir Ferrari yöneticisinin şirket CEO'su olduğunu iddia eden bir deepfake tarafından telefonla arandığını bildiriyor. Şüphelenen yönetici sadece CEO'nun cevaplayabileceği bir soru sorunca girişim engellendi. Greylock Partners tarafından aktarılan bir vakada, Kuzey Koreli bir casus bir siber güvenlik firması tarafından işe alınmak için sahte bir kimlik kullanmış ve hemen ardından firmanın kurumsal cihazlarına kötü amaçlı yazılım yüklemiştir.

En İyi Savunma

Neyse ki yapay zeka, kuruluşların kötü aktörleri engellemesine de yardımcı olabilir. Cacciapuoti, "Yapay zekayı durdurmak için yapay zekayı kullanmak zorundasınız." diyor. Kuruluşların gelişen tehditlere ayak uydurmak için daha sofistike yapay zeka destekli siber güvenlik önlemlerini benimsemeleri gerekiyor. "Suçluların kullandığı teknoloji hakkında derin bilgiye sahip değilseniz, onları nasıl durdurabilirsiniz?" diye soruyor. Kuruluşlar, siber suçluların kullandığı araç ve stratejileri tanımalı ve siber güvenliği artırmaya yardımcı olabilecekleri birçok yolu anlamalıdır.

"Yapay Zeka Odaklı Saldırılarla Mücadele Etmek için Yapay Zeka Destekli Siber Güvenlik İhtiyacı," ISACA, gelişmiş teknolojilerin saldırıları önlemeye yardımcı olabileceği çok sayıda yol tanımlıyor:

Saldırıları Önlemenin Yolları

- Kurumsal kaynakların nasıl kullanıldığını belirlemek, açık alanları tespit etmek, bir varlık envanteri oluşturmak ve ağ trafiği eğilimlerini ve kullanıcı etkinliklerini/davranışlarını belirlemek için geniş veri kümelerini analiz etmek.
- "Olağandışı girişler, yeni bir coğrafi konumdan veya IP adresinden gelen erişim talepleri, yeni kullanıcı erişimi, dosyalar ve diğer kaynaklar üzerindeki izinlerin değiştirilmesi, büyük hacimli dosyaların çıkarılması veya silinmesi ve trafikte üstel bir artış" gibi anormalliklerin tespit edilmesi
- Şüpheli kötü aktörleri proaktif olarak kilitlemek, oturumlarını kapatmak veya başka bir şekilde engellemek ve sistem yöneticilerini faaliyetlerine karşı uyarmak için yapay zekayı kullanmak.
- Hızlı yanıt verebilmek için sistemlerin sürekli izlenmesi.
- Potansiyel güvenlik tehditlerini öngörmek ve bunları önlemeye yönelik adımlar atmak için tahmine dayalı analizi kullanma.
- Sıfırıncı gün tehditlerini veya yeni ve görünmeyen güvenlik açıklarını tespit etme ve önlem
- Yanlış pozitif potansiyel tehditlerin sayısını azaltmak.
- Yanıtları hızlandırmak ve insan hatalarını en aza indirmek için güvenlik değerlendirmelerin otomatikleştirme.
- Sürekli koruma sağlamak için yeni gelişmelere ve ortamlara uyum sağlayacak şekilde ölçeklendirme.

Cacciapuoti, kuruluşların daha derin içgörüler oluşturmak için birden fazla kaynaktan gelen verileri toplamak, analiz etmek ve ilişkilendirmek için yapay zekadan yararlanabileceğini söylüyor. Ayrıca büyük metinsel verileri analiz etmek için doğal dil işleme (NLP) kullanabilirler. Örneğin, iç denetçilerden sözleşmeleri analiz etmeleri istendiğinde, NLP sistemin analiz etmesi için önemli metinsel verileri çıkarabilir.

Yapay Zeka Konularının Ele Alınması

Bir kurum hiçbir zaman riskin %100'ünü ele alamayacağı için Niedzielski, işe farklı iş alanlarındaki tehditleri stratejik olarak değerlendirerek başlamayı öneriyor. Bu, potansiyel yapay zeka dolandırıcılık vektörlerinin belirlenmesini ve saldırıya uğrama olasılıkları ile potansiyel büyüklük ve etkilerinin değerlendirilmesini içerecektir. Bir sonraki adımın, mevcut kontrollerin etkinliğini belirlemek olduğunu söylüyor.

Bu çabanın bir parçası olarak Niedzielski, GenAI'nin gelişmiş muhakeme ve örüntü tanıma gibi gelişmekte olan yeteneklerinin, yapay zeka tarafından üretilen kimlik avı girişimleri ve derin sahtekarlıklar gibi yaygın taktikleri tanımak için kullanılmasını önermektedir. Bazı şirketler, bir aramanın dahili veya harici bir numaradan yapılıp yapılmadığını doğrulamak için protokoller ve teknolojiler kullanır.

"Bu gelişmiş teknolojiler, ilgili riski en aza indirmeye yardımcı olabilir" diyor. Ancak bazı durumlarda, örneğin bir arayanın veya toplantı katılımcısının deepfake olup olmadığına hemen karar vermek gibi, çalışanların içgüdülerine güvenmeleri veya örneğin bir CEO'nun neden aradığını ve para transferi istediğini sorgulamaya hazır olmaları gerekebilir. Bu gibi durumlarda, çalışanlar içgüdülerine güvenmeye ve kişiyi şirket numarasından geri aramaya ya da aradığı iddia edilen kişi aynı ofisteyse, kim olduğunu doğrulamak için koridorda yürümeye teşvik edilmelidir.

İç denetim, risk yönetimi, BT, siber güvenlik ve diğer ilgili işlevler gibi alanlardan profesyonellerden oluşan çok disiplinli bir ekip, yapay zekadaki gelişmeleri izleyebilir ve risk yönetimi, güvenlik protokolleri ve dolandırıcılık tespit sistemlerinde sürekli güncellemeler sağlayabilir. Niedzielski'ye göre ekip, hangi kontrollerin hasarı en iyi şekilde önleyeceği veya sınırlandıracağı gibi konuları göz önünde bulundurarak çabaları belirlemek ve bunlara yanıt vermek için birlikte çalışabilir.

Ayrıca şirketlerin deneyimlerini düzenli olarak paylaşmalarını ve başkalarının karşılaştığı YZ güvenlik açıklarını tartışmalarını öneriyor. "Sadece başarılı çabalar değil, aynı zamanda bir şeylerin yanlış gittiği zamanlar ve şirketin bundan nasıl ders çıkardığı" tavsiyesinde bulunuyor. "Bilgi paylaşımı, eğitim ve uygun risk değerlendirmeleri, yapay zeka kaynaklı dolandırıcılık riskini en aza indirmeyi mümkün kılacaktır."

Niedzielski, bu ortamda, çalışanların potansiyel şüpheli faaliyetler konusundaki farkındalığını artırmak ve ihlalleri gidermek için uygun eylem planlarını pekiştirmek için eğitimin en önemli öncelik olması gerektiğini söylüyor. Cacciapuoti, gerçek dünyadaki durumlarda gerçek zamanlı olarak siber güvenlik eğitimi sağlamak için yapay zeka simülasyonlarının kullanılmasının da mümkün olduğunu belirtiyor. Yapay zeka, siber eğitimde bireysel çalışan davranışını analiz edebilir ve iyileştirme için içgörüler sağlayabilir.

İç Denetimin Katkısı

Cacciapuoti, iç denetimin, kurumun çabalarının yapay zekânın zorluklarıyla eşleşmesini sağlamaya yardımcı olabileceğini söylüyor; buna riskleri azaltırken potansiyelden yararlanmak da dâhil. "İç denetim kapsamlı bir risk değerlendirmesi yapmalı, yapay zeka sistemlerini güvenlik, etik ve uygunluk açısından denetlemeli ve güvenli inovasyonu desteklemelidir" diyor. "Yapay zeka tehditleriyle başa çıkabilecek kadar sağlam bir siber stratejinin şekillendirilmesine katılabilir."Buna ek olarak, iç denetim tipik olarak önemli bir savunma hattı olsa da, Cacciapuoti, yapay zeka söz konusu olduğunda, risk yönetiminde dinamik bir yaklaşım

> "Yapay zeka asla iç denetçilerin yerini almayacak, ancak güçlü bir yardımcı olabilir."
>
> **- Antonio Cacciapuoti, CIA**

benimseyerek bir saldırı hattı olarak da hizmet etmesi gerektiğini söylüyor. "Doğrudan saldırmak varken neden riskin gelmesini bekleyesiniz ki?" diye sorar. Bu, uygun yönetişim kontrolleri ve sürekli iyileştirme sağlarken kurumun fırsatları en üst düzeye çıkarabilmesi için yeni teknolojileri kullanmada ön planda olmak anlamına gelir.

Cacciapuoti'ye göre, iç denetim fonksiyonu içinde, "yapay zeka asla iç denetçilerin yerini almayacak, ancak güçlü bir yardımcı olabilir". İç denetimin yapay zekâdan şu konularda faydalanabileceğini söylüyor:

- Büyük hacimli verileri analiz edin ve testlerdeki örnekleri tüm popülasyon boyutuna çok yakın olacak şekilde genişletin.
- İç denetim uzmanlarının daha üst düzey görevlere odaklanabilmeleri için tekrarlayan görevleri üstlenerek test prosedürlerini otomatikleştirin ve kilit kontrolleri izleyin.
- Periyodik denetimlere güvenmek yerine verileri sürekli olarak izlemek için yapay zeka algoritmalarını kullanın, olağandışı etkinlikleri çok daha erken tespit edin ve ele alın.
- Gelecekteki sonuçları öngörmek ve daha bilinçli kararlar ve öneriler almak için tahmine dayalı analitiği kullanın.
- İç denetçilerin nihai raporlarını hazırlarken kullanabilmeleri için çalışma kağıtlarını hızlı bir şekilde özetleyin.

Yapay zeka, tüm kontrol fonksiyonlarında bulguların daha düzgün ve verimli bir şekilde yönetilmesini sağlar. Cacciapuoti, "Çok büyük bir şirkette, birden fazla fonksiyondan dikkate alınması gereken çok sayıda angajman vardır" diyor. Yapay zeka, iç denetçilerin mükerrerliği önlemek için verileri tek tip bir şekilde bir araya getirmesini sağlar.

Niedzielski, riskleri azaltmak ve değerden yararlanmak için iç denetçilerin teknolojideki gelişmelerle ilgili bilgilerini sürekli güncellemelerini öneriyor. "Her gün yeni bir şey oluyor" diyor. Potansiyel risklere karşı reaktif değil proaktif yanıtlar belirlemeye odaklanmalıdırlar. Dünya yeni teknolojilerden yararlanmaya çalışırken, iç denetçilerin de kurumsal bütünlüğü korumak için yönetişim ve yeni düzenlemelere ve etik standartlara uyum konusuna odaklanmaları gerektiğini söylüyor.

Yapay Zeka Destekli Siber Tehditler: Hızlı Bilgiler

- Güvenlik uzmanlarının %97'si, yapay zekanın tükenmişliğe neden olmaya devam etmesi nedeniyle, kuruluşlarının yapay zeka kaynaklı bir siber güvenlik olayı yaşayacağından endişe duyuyor.
- Güvenlik uzmanlarının %75'i, yapay zeka destekli siber tehditlerdeki artış nedeniyle geçen yıl siber güvenlik stratejilerini değiştirmek zorunda kaldı.
- Güvenlik ekiplerinin %73'ü önleme öncelikli yeteneklere daha fazla odaklanmak istiyor.
- Kurumların %61'i geçtiğimiz yıl deepfake vakalarında artış gördü.

Kaynak: GenSiber Güvenlikte Yapay Zeka: Dost mu Düşman mı? Voice

Niedzielski'ye göre "İç denetçiler kendilerini kötü bir aktörün yerine koymalıdır". "Kötü bir aktörün kuruluşa nasıl sızacağını sormayın, kuruluş hakkında bildiklerinize dayanarak kötü bir aktör olsaydınız ne yapacağınızı sorun. Kuruluşa yalnızca niceliksel değil, niteliksel bir bakış açısını da dikkate alın."

İç denetçilerin tek başlarına hareket etmemeleri gerektiğini söyleyen Cacciapuoti, riski önlemek ve azaltmak için kontrol fonksiyonları, uyum, risk yönetimi, dış denetçiler ve düzenleyiciler de dahil olmak üzere tüm güvence sağlayıcılar ve paydaşlarla koordinasyon kurulmasını öneriyor. "Yapay zeka araçları ve siber güvenlik uzmanları arasındaki işbirliğinin yanı sıra güçlü bir yönetişim çerçevesi, bu ortamda gezinmek ve yeni ve ortaya çıkan risklere yanıt vermek için gereklidir" diyor.

BÖLÜM 2

Siber Yılmazlığın Sağlanması

Uzmanlar Hakkında

DC Chang, CPA, CDPSE, CISSP, CRISC, CISA

DC Chang, Dallas, Teksas'taki United Airlines'ta Dijital Teknoloji ve Siber Güvenlik Denetim Direktörü olarak görev yapmaktadır.

Michael Echols, CISSP

Michael Echols, Washington DC'deki Max Cybersecurity LLC'nin CEO'sudur.

Justin Headley, CPA, CISSP, CISA, CRISC

Justin Headley, Warren Averett'in Birmingham, Alabama'daki Risk Danışmanlığı & Güvence Hizmetleri Grubu'nda kıdemli yöneticidir.

Kuruluşlar siber saldırıları önlemek için yeterli araçlara sahip olduklarından emin olmak için çalışırken, bir şekilde ihlal veya saldırılarla karşılaşacakları neredeyse kesindir. Bunu akılda tutarak, işletmeler aynı zamanda bir siber saldırıya yanıt verme ve bu saldırıdan hızlı bir şekilde kurtulma becerilerine de odaklanmalıdır. Bu özet, saldırılara karşı yılmazlığın en iyi nasıl anlaşılacağını ve aşılanacağını tartışmakta ve iç denetçinin bir kurumun tepkisini güçlendirmedeki rolünü açıklamaktadır.

İyileşme için Sahnenin Hazırlanması

En iyi haliyle, siber yılmazlık sadece korkunç bir duruma verilen bir tepki değildir. Max Cybersecurity LLC CEO'su Michael Echols'a göre bu, bir kuruluşun operasyonlarını sürdürebilmesini sağlayan planlama, süreçler, analiz, eğitim, kritik hizmetler ve yönetim gibi uygulamalardan oluşan bir sürekliliktir. Bu uygulamalar, bir saldırıdan sonra kurumsal işlevlerin geri yüklenmesini veya sürdürülmesini mümkün kılar, ancak bir sorun ortaya çıkmadan çok önce uygulamaya konmaları gerekir.

Örneğin Echols, tüm yönlendirmelerini web sitesi üzerinden alan bir hukuk firması müşterisiyle çalıştı. Genellikle her gün çok sayıda yönlendirme alıyordu, ancak bir noktada, firma herhangi bir yönlendirme almadığını fark edene kadar iki ila üç gün geçti ve nihayetinde saldırıya uğradığını fark etti. firmanın ana iş kaynağı (kritik bir işlev) olduğu için, web yönlendirmelerindeki olağandışı bir düşüş hakkında "firmanın sürekli izleme ve bir tür bildirim için zaten bir süreci olması gerekirdi" diyor.

Belirlenecek sorunlar - web trafiğindeki düşüş gibi - her işletme için farklı olacaktır ve muhtemelen birden fazla olacaktır. Echols, birçok durumda kuruluşların güç kaynaklarını etkileyecek bir olaya hazırlıklı olmak isteyeceklerini, örneğin ana işletmeden bağımsız jeneratörleri devreye sokmak için adımlar atacaklarını, böylece saldırıdan etkilenmeyeceklerini söylüyor.

> Siber yılmazlık, "siber kaynakları kullanan veya bu kaynaklar tarafından etkinleştirilen sistemlerdeki olumsuz koşulları, stresleri, saldırıları veya tehlikeleri öngörme, bunlara dayanma, bunlardan kurtulma ve bunlara uyum sağlama yeteneğidir. Siber yılmazlık, siber kaynaklara bağlı olan görev veya iş hedeflerinin tartışmalı bir siber ortamda gerçekleştirilmesini sağlamayı amaçlamaktadır."
>
> **- ABD Ulusal Standartlar ve Teknoloji Enstitüsü**

United Airlines Dijital Teknoloji ve Siber Güvenlik Denetim Direktörü DC Chang'e göre, bundan sonra olacaklara hazırlanmak için mevcut siber güvenlik ortamını bir bağlama oturtmak gerekiyor. Yirmi yıl önce, kuruluşların kendi veri merkezleri vardı ve siber güvenlik bir dereceye kadar sunucuları fiziksel kapıların ve pencerelerin arkasına kilitleme meselesiydi. Günümüzde veriler, dünyanın dört bir yanındaki kötü aktörlere karşı savunmasız olabilen sanal bir ortamda saklanmaktadır.

Chang, "Artık dijital olduğumuz için takip etmemiz gereken binlerce ve binlerce pencere ve kapı var ve bunlar her gün ekleniyor ve çıkarılıyor" diyor. Kuruluşların bir kriz anında ihtiyaç duyacakları yılmazlığı geliştirebilmeleri için dijital hızlanmanın hızının ve kapsamının farkında olmaları gerekir.

Yönetişim ve Kültür

Warren Averett'in Risk Danışmanlığı & Güvence Hizmetleri Grubu'nda üst düzey yönetici olan Justin Headley'e göre yönetişim, siber yılmazlığın oluşturulmasında kilit bir role sahiptir. "Çalışanların zayıf bir parola kullandıkları veya şüpheli

bağlantılara tıkladıkları için zayıf nokta olduğunu sürekli duyuyoruz" diyor. "Ancak liderler bu işe inanmamışsa, çalışanların da üzerlerine düşeni yapmasını bekleyemezsiniz."

Birçok açıdan siber güvenlik tamamen bir teknoloji meselesi değil, bir kültür meselesidir. Echols, "Kuruluştaki insanların %90'ının fikrini değiştirirseniz ve bir kişi e-postadaki bir bağlantıyı açarsa, bu şirketi batırabilir" diyor. Siber güvenlik bilincine sahip bir kültür, kurumun beklentilerini netleştirir ve tüketiciler ile iş ortaklarına güven verir. "Bankalar siber dirençli hale gelen ilk gruplardan biri oldu" diyor, çünkü paydaşlarının güvenine güveniyorlar.

Headley, liderlerin siber güvenlik ipuçları içeren üç aylık e-postalar veya ilkel yıllık güvenlik eğitimleri gibi standart yaklaşımların ötesine geçen bir siber güvenlik kültürünü teşvik etmelerini öneriyor. Kurumunun attığı adımlar arasında çalışanlara kendi sahte kimlik avı e-postalarını göndermek ve ardından gömülü şüpheli bağlantılara tıklayanlara eğitim vermek yer alıyor. "Siber yönetişimin sadece teoride değil, uygulamada da nasıl işlediğini göstermeniz gerekiyor" diyor.

Liderler ayrıca bir saldırıda atılması gereken belirli adımları da sağlayabilir. Headley'e göre, "Bir kuruluş, bir ihlalde izlenecek pratik, tekrarlanabilir politikalar ve prosedürler varsa, bir saldırıyı durdurabilir ve iyileşebilir." Bu adımlar test edilirken liderler de dahil olur ve aksaklıkların giderilmesinde rol alırlarsa, siber güvenlik stratejilerinin başarılı olmasında büyük rol oynayabilecek bu çabaya bağlılıklarını göstermiş olurlar.

- İhlallerin %68'i, bir kişinin sosyal mühendislik saldırısına kanması veya hata yapması gibi kötü niyetli olmayan bir insan unsurunu içermektedir.
- Kullanıcıların oltalama e-postaları tarafından kandırılması için geçen ortalama süre 60 saniyeden azdı.
- İhlallerin %15'i yazılım tedarik zincirleri, barındırma ortakları da

Kaynak: Verizon Business 2024 Veri İhlali Soruşturma Raporu

Düzenlemelerin Etkisi

Kesinleşmiş kural uyarınca, Siber Güvenlik Risk Yönetimi, Strateji, Yönetişim ve Olay Açıklaması, ABD Menkul Kıymetler ve Borsa Komisyonu, halka açık şirketlerin önemli siber güvenlik olaylarını açıklamalarını ve siber riskleri nasıl değerlendirdikleri, belirledikleri ve yönettikleri konusunda periyodik açıklamalar yapmalarını zorunlu kılarak kuruluşlar için beklentileri yükseltmiştir. Chang, bu kuralın "gezegendeki her kuruluşun göz önünde bulundurması gereken önemli bir meselenin altını çizdiğini" söylüyor.

Headley, diğer gerekliliklerin yanı sıra, kuralın kuruluşları siber uygulamalarının operasyonel olmasını sağlamaya zorladığını söylüyor. BT fonksiyonunun genellikle bir silo içinde çalıştığını ve işleyişini tam olarak anlamayan liderlerin zımni güvenine sahip olduğunu belirtiyor. "Bunun değişmesi gerekecek" diyor. Orada kurum içi ve müşteri verilerinin nasıl ele alınacağı ve siber endişelerin nasıl giderileceği konusunda kurum çapında bir anlayış olmalıdır.

Echols, pek çok düzenlemede olduğu gibi, "her şey şeffaflığa bağlı olacak" diyor. "Önemli bir ihlal olduğunda, şirketin bu ihlale nasıl tepki vereceğine dair net bir süreci olmalıdır."

Yapay Zekayı Karışıma Eklemek

Yapay zeka (AI), siber sorunların önlenmesinde ve bir saldırı sonrasında yılmazlığın artırılmasında paha biçilmez bir araç olabilir. Headley, yeni nesil güvenlik duvarları ve nokta koruma sistemleri gibi teknolojilerin veri trafiğini sıralamayı ve

araştırılması gereken anormallikleri bulmayı kolaylaştırdığını söylüyor. "Yapay zeka kullanımı son birkaç yılda oyunun kurallarını değiştirdi ve şirketlerin saldırıları tespit etme ve bunlara yanıt verme konusunda daha iyi olmalarına yardımcı olmaya devam edecek."

Yapay zeka aynı zamanda kuruluşlara karşı bir silah olarak da kullanılabilir. Echols, "Göz ardı edilmiş güvenlik açıklarınız varsa, yapay zeka bilgisayar korsanlarının bunları bulmasına yardımcı olacaktır" diyor.

Headley'e göre, diğer hususların yanı sıra, kuruluşların yeni araçlarla elde edilecek daha fazla verimlilik dürtüsünü güvenlik ve gizliliği koruma ihtiyacı ile dengelemesi gerekecek. Yeni teknolojiler, kuruluşların, genellikle programlara hassas bilgiler vermeyi içeren tekrarlanabilir görevleri ortadan kaldırmasına yardımcı olur. Aynı zamanda, "bu teknolojilere yönelik hedefli saldırılar görmeye devam ediyoruz çünkü kötü aktörler insanların teknolojiyi tam olarak anlamadığını biliyor" ve bu da programların içerdiği hassas verileri özellikle savunmasız hale getirebilir.

Yılmazlık oluştururken, kuruluşların çalışanlarını gelişen teknolojiler konusunda eğitmeleri ve teknoloji kullanımının kuruluşun risk iştahına uygun olmasını sağlamaları gerekecektir. Headley, "Bir şirket en iyi teknolojilere ve becerilere sahip olabilir, ancak bir kullanıcı yine de bilmeden veya bazen bilerek bir GenAI aracı kullanarak ön kapıdan veri sızdırabilir" diyor.

Kuruluşlar geleneksel siber saldırı yaklaşımlarını ihmal etmemeye de dikkat etmelidir. Echols, birçok siber sorunun, yanlış yapılandırmalar veya yerleşik bir uygulamanın takip edilmemesi gibi yeni olmayan sorunlardan kaynaklandığını söylüyor. Birçok ihlalin, hiç düzeltilmemiş bilinen güvenlik açıkları veya yüklenmemiş yamalarla ilgili olduğunu söylüyor. Sonuç olarak, son kullanıcıların yeni ve mevcut tehditler konusunda eğitilmesi özellikle önemlidir. "Denetçiler, ilgisizliğin yarattığı gizli güvenlik açıklarını ortaya çıkarmak için kaputun altına bakmalı ve müşterilere doğru soruları sormalıdır" diyor.

> "Başta bir kuruluşun yönetim kurulu ve üst yönetimi olmak üzere paydaşlar, siber olaylara müdahale ve kurtarma kontrollerinin iyi tasarlanıp tasarlanmadığını ve etkin ve verimli bir şekilde uygulanıp uygulanmadığını doğrulamak için bağımsız, tarafsız ve yetkin güvence hizmetlerine güvenmektedir. İç denetim birimi, bu tür hizmetleri Standartlara uygun olarak ve özellikle kurumun bilgi teknolojileri ve bilgi sistemleri tarafından açıkça kullanılanlar olmak üzere yaygın olarak kabul görmüş kontrol çerçevelerine atıfta bulunarak sağladığında kuruma değer katar
>
> **Kaynak: Küresel Teknoloji Denetim Rehberi: Siber Olaylara Müdahalenin Denetlenmesi ve Kurtarma, 2. Baskı, Küresel Uygulama Kılavuzu,**

İç Denetim Yılmazlığı Artırmaya Nasıl Yardımcı Olabilir?

Echols, bu ortamda iç denetimin, yılmazlığı artırmak ve güvenlik açıklarını tespit etmek için denetimlerinin sonuçlarını, müşterilerin gevşek siber güvenliğin potansiyel sonuçlarını anlamalarına yardımcı olacak şekilde çerçevelemeye hazırlıklı olması gerektiğini söylüyor. Müşteriler en kötüsünün asla başlarına gelmeyeceğini varsayabilirken, iç denetçiler bu inancı askıya alabilmelidir, bu da onların hayal edilemeyeni hayal etmelerini daha iyi sağlayacaktır. Örneğin, Echols'un sosyal medya hesaplarında kurumsal e-posta adreslerinin kullanılmasını yasaklayan bir en iyi uygulaması olan bir müşterisi vardı, ancak bu resmi bir politika değildi. Bu yaklaşımın yanlışlığı şu durumlarda açıkça ortaya çıkmıştır, MGM önemli bir veri ihlaline maruz kaldı geçen yılın sonlarında. İhlalin araştırılması sonucunda bir çalışanın iş e-postasını bir sosyal medya platformunda kullandığı ortaya çıkmıştır. Bilgisayar korsanları çalışanın bilgilerini LinkedIn'de bulmuş ve MGM'nin BT yardım masasını arayarak çalışanın kimliğine bürünmüş ve böylece MGM'nin sistemlerine erişmek ve virüs bulaştırmak için kimlik bilgilerini elde etmiştir. Echols, "En iyi uygulamalar birçok kişinin deneyimlerinden elde edilir ve mümkün

olduğunda politika haline getirilmelidir" diyor.

İç denetçiler ayrıca denetimin uygunluk boyutunun siber yılmazlığın oluşturulmasına yardımcı olmak için yalnızca ilk adım olduğunu anlamalıdır. Echols, "Uyumluluk güvenlik değildir" diyor. İç denetçiler, bulgularını müşteri ekibinin güvenliği artırmak için kullanabileceği daha büyük içgörülere dönüştürmeye ve ekibin henüz cevaplayamadığı soruları sormaya odaklanmalıdır.

Echols'a göre, "Müşteriye bu sorunun cevabını aramamanın ve bulmamanın aslında bir güvenlik açığı yarattığını söyleyebilmelisiniz."

İç denetim, denetimler arasında, ekiplerin karşılaştıkları zorlukları öğrenmek ve kontrol etmek için zamanlar planlayarak iletişim kanallarını açık tutmalıdır. Headley, "İç denetçiler kendilerini güvenilir danışmanlar olarak konumlandırabildiklerinde, bu tamamen oyunun kurallarını değiştirir" diyor.

Şeffaflık çok önemlidir. İç denetçiler, kapsam ve planlanan test prosedürlerinin yanı sıra hangi sorunların ortaya çıktığı konusunda da net olmalıdır. "Erken ve sık iletişim kurduğunuzdan emin olun" diyor, "özellikle de BT riski söz konusu olduğunda." İç denetçilerin hemen yargıya varmaktan kaçınmalarını, bunun yerine müşteri ekibinin düşünce süreçleri hakkında açık bir konuşma yapmalarını ve iş birliğini teşvik etmelerini tavsiye ediyor.

Headley, BT ekiplerinin genellikle çeşitli iş kollarının taleplerini karşılamakta zorlandığını, uygulamaları çalışır durumda tutmaktan günlük donanım aksaklıklarıyla başa çıkmaya kadar her şeyin sorumluluğunu üstlendiğini belirtiyor. Sonuç olarak, siber güvenlik her zaman en önemli öncelik olmayabilir. İç denetçiler bu zorluklara ilişkin farkındalığı artırabilir ve ekipleri bunları ele alma fırsatları konusunda eğitebilir, böylece denetimlerin gerçek bir katma değer uygulaması olmasını sağlayabilir.

Headley, "İç denetçiler kurumsal yılmazlığın güçlendirilmesine yardımcı olan ortaklar olabilirler" diyor. Diğer adımların yanı sıra, genellikle aynı dili konuşmayan şirket liderleri ve BT ekipleri arasındaki kopuklukları gidermeye yardımcı olabilirler. İç denetçiler hem iş riskini hem de BT riskini anladıkları için bu boşluğu doldurmaya yardımcı olabilirler.

Chang, iç denetçilerin siber risklerin anlaşılmasını ve ilgili sorunların çözümünü geçmiş uygulamalardan farklı bir şekilde şekillendirebileceğini söylüyor. Kurumlar geleneksel iş sürekliliği planlamasından veya iş felaketi kurtarmasından uzaklaştıkça, iç denetçiler daha çok yönlü ve incelikli yaklaşımlar benimsemelerine yardımcı olabilirler. Birbirinden kopuk bilgi ve veri noktalarını işleyen ve bunları daha iyi karar almaya yönlendiren ilgi çekici bir anlatıda bir araya getiren hikaye anlatıcıları olarak rol üstlenerek bu çabayı geliştirebilirler.

BT ve güvenlik operasyonları karar vericileri arasında yapılan bir ankete göre:

- Katılımcıların yalnızca %2'si bir siber saldırının ardından 24 saat içinde verilerini kurtarabileceklerini ve iş süreçlerini eski haline getirebileceklerini söylüyor.
- 69'u kurumlarının son bir yıl içinde fidye ödediğini söylerken, %77'si fidye ödemeye karşı tanımlanmış bir politikaları veya protokolleri olduğunu belirtiyor.
- 42'si kurumlarının hassas verileri belirleyebildiğini ve geçerli veri gizliliği yasa ve yönetmeliklerine uyabildiğini söylüyor. Diğerleri ise her ikisini de yapmak için yeterli BT ve güvenlik kapasitesine sahip değildir.

Kaynak: Yılmazlık Rapor 2024

Olasılıkların Eşitlenmesi

“Nihayetinde yılmazlık, saldırının kaçınılmazlığını ve kuruluşun dış duvarlarının aşılmaz olmadığını kabul etmektir” Echols'un belirttiğine göre. Bu çabanın bir parçası olarak, kuruluşlar adil olmayan bir mücadele içinde olduklarını kabul etmelidir. Chang, kuruluşlar karşılaştıkları saldırıların %100'ünü engellemeye çalışırken, bilgisayar korsanlarının tahribat yaratmak için yalnızca bir kapıyı açmaları gerektiğini belirtiyor. "Savunucu olmak fail olmaktan çok daha zor" diyor. İç denetim, şirketlerinin siber güvenlikte başarı şanslarını artırmak için ihtiyaç duydukları içgörüleri ve bilgileri sağlayabilir.

BÖLÜM 3

Yeni Bir Sıfır Güven Sınırının Oluşturulması

Uzmanlar Hakkında

Adam Kohnke

Madison, Wisconsin'de yaşayan Adam Kohnke, kimyasal üretim şirketi Charter Next Generation'ın bilgi güvenliği müdürüdür.

Julio Tirado

Julio Tirado, Tulsa, Oklahoma'da bulunan SpiritBank'ta İç Denetim ve Uyum Direktörü olarak başkan yardımcılığı görevini yürütmektedir.

Her kuruluşun ağlarını güvende tutmak için süreçlere ve kontrollere sahip olması temel bir gereklilik olmalıdır. Ancak, teknoloji ilerledikçe ve ağlar daha büyük ve neredeyse anlaşılmaz derecede karmaşık hale geldikçe, güvenli bir ağı neyin oluşturduğuna dair standart değişti. En önemli değişikliklerden biri, konum merkezli bir güvenlik modelinden daha veri merkezli bir güvenlik modeline geçişte yatmaktadır. Biz bu modeli "sıfır güven" olarak adlandırıyoruz

Sıfır Güven Nedir?

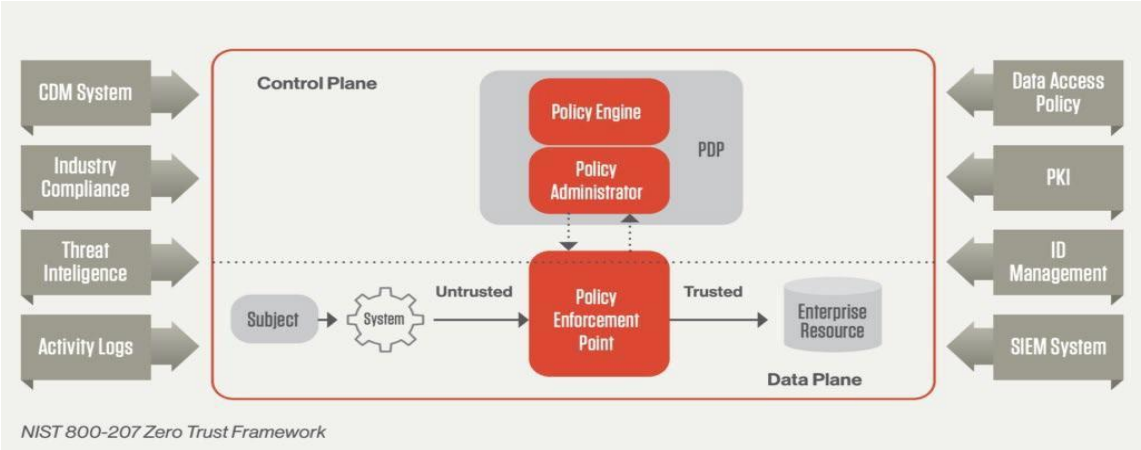
Genel olarak, sıfır güven güvenlik çerçevesi, bir ağ içinde çalışan tüm kullanıcıların - hem kurum içinde hem de dışında - uygulamalara ve verilere erişmeden önce kimliklerinin doğrulanmasını ve ardından düzenli olarak sürekli olarak doğrulanmasını gerektirir. Adından da anlaşılacağı üzere, "güven" veya daha spesifik olarak "güven ama doğrula" bu sistemde hiçbir rol oynamaz ve kurumla ilgili herhangi bir şeye erişim sürekli olarak gerekçelendirilmeli ve kurumun politikalarına göre değerlendirilmelidir.

Geleneksel olarak, siber modeller ağın konumuna göre oluşturulurdu, ancak sıfır güven sisteminde, bir kurumsal ağ yerel, bulut tabanlı veya ikisinin bir karışımı olabileceğinden, "ağ" neyin oluşturduğu daha az kesin olarak tanımlanmıştır. Özellikle yeni bir uzaktan çalışma çağını başlatan COVID-19 salgınının ardından, hibrit veya tamamen bulut tabanlı sistemler norm haline geldi ve siber güvenlik çerçevelerinin bunu hesaba katacak şekilde gelişmesi gerekti.

Mevcut birkaç resmi sıfır güven çerçevesi bulunmaktadır:

- Standart 800-207 ulusal Standartlar ve Teknoloji Enstitüsü'nden (NIST). Bu, 2021'den beri ABD federal kurumları tarafından kullanılması zorunlu olan çerçevedir (Bkz. Şekil 1).
- Google BeyondCorp.
- Microsoft Sıfır Güven Stratejisi.
- Sıfır Güven Olgunluk Modeli siber Güvenlik ve Altyapı Güvenliği Ajansı'ndan (CISA).

Şekil 1



Kaynak: Sıfır Güven Ağları | NIST

Hepsinin kendine özgü nitelikleri olsa da, her biri aynı temel ilkeleri paylaşmaktadır:

- Tüm kaynaklara erişimi sürekli olarak doğrulayın.
- Harici veya dahili bir ihlal durumunda etki alanını en aza indirin.
- BT altyapısından bağlam toplamak için davranışsal verileri kullanın.

Böyle bir sisteme geçiş önemli gibi görünse de, bunun mevcut sistemlerin yerini alması anlamına gelmediğinin unutulmaması önemlidir. Kimyasal üretim şirketi Charter Next Generation'da bilgi güvenliği müdürü olan Adam Kohnke, "Sıfır güven, mevcut ağ koruma modellerini ve hatta altyapı değişikliklerini tamamen değiştirmeyi amaçlamıyor" diyor ve ekliyor: "Daha ziyade, gelişmiş ağ koruması için bunları artırmayı amaçlıyor. Bunun bir uzantı olması gerekiyordu çünkü güvenlik duvarları, web proxy'leri ve sınır izolasyon mekanizmaları gibi geleneksel sistemler çalışmıyordu."

IBM' e göre, 2024 yılında tek bir veri ihlalinin ortalama maliyeti 4,88 milyon dolardı. Ayrıca, bir ihlalin ortalama yaşam döngüsü, tespit edilmesinden kontrol altına alınmasına kadar tam 292 gün sürmüştür. Geleneksel ağ korumasının yeterli olmadığı ve ciddi bir dikkat gerektirdiği açıktır.

İç Denetimin Rolü

Ayrıntılar farklılık gösterse de, iç denetçiler sıfır güven sisteminin uygulanması ve sürdürülmesiyle ilgili çeşitli sorumluluklara sahip olabilirler. Örnek olarak, bir iç denetim değerlendirmesinin en fazla değere sahip olabileceği alanlar aşağıda belirtilmiştir.

Korunan Yüzeylerin Tanımlanması

Geleneksel olarak, bir siber güvenlik sistemi çabalarını bir kurumsal ağın etrafındaki güvenlik parametrelerinin ne olduğunu tanımlamaya yoğunlaştırmıştır. Güvenlik duvarları ve VPN sistemleri bu konsept etrafında tasarlanmıştır, hassas verileri ve savunmasız bilgiyi
ağ çevresinden mümkün olduğunca uzakta tutarak. Ancak bir sıfır güven sisteminde parametreler yerine, toplu olarak "koruma yüzeyleri" olarak bilinen veri, uygulama, varlık ve hizmet gruplarına (DAAS) odaklanılır.

Bu yüzeylerin uygun şekilde tanımlanmasını sağlamak, kapsamlı bir iç denetim değerlendirmesinin merkezinde yer almalıdır.

SpiritBank İç Denetim ve Uyum Direktörü, Başkan Yardımcısı Julio Tirado'ya göre, "Değerlendirme, sistemlerin ve verilerin uygun şekilde sınıflandırılıp sınıflandırılmadığını ve her biri için yürürlükte olan koruma politikalarının uygun olup olmadığını belirlemek için kurumun veri sınıflandırma politikalarını incelemeye odaklanmalıdır."

Tirado, korumalı hizmetlerin sadece verilerle sınırlı olmadığını da söylüyor. Hassas verilere erişimde rolü olan fiziksel varlıkların da envanterinin çıkarılmasını ve periyodik olarak değerlendirilmesini sağlayacak süreç ve prosedürlere sahip olması gerekir.

> Değerlendirme, sistemlerin ve verilerin uygun şekilde sınıflandırılıp sınıflandırılmadığını ve her biri için yürürlükte olan koruma politikalarının uygun olup olmadığını belirlemek için kuruluşun veri sınıflandırma politikalarını incelemeye odaklanmalıdır.

- Julio Tirado, SpiritBank

Harita İşlem Akışlarının Doğrulanması

Koruma yüzeylerinin belirlendiğinden emin olunduktan sonra, değerlendirme sürecindeki bir sonraki adım, tüm bu DAAS sistemlerinin birbirleriyle nasıl etkileşime girdiğinin paydaşlar tarafından anlaşılmasını sağlamaktır. BT ekipleri, bu sistemlerin birbirlerine nasıl eriştiğini ve kullanımlarının nereye varabileceğini toplu olarak özetleyen karmaşık bağlantı noktaları ağını, ağ trafiği taban çizgilerini ve protokolleri haritalamaya adanmış ayrıntılı dokümantasyon şemalarına sahip olmalıdır.

Çoğu kurumda iç denetim birimi bu diyagramların doğruluğunu kendi başına doğrulayacak yeterli bilgi veya deneyime sahip olmasa da, Kohnke iç denetim biriminin paydaşlarla veya güvenilir üçüncü taraflarla birlikte çalışarak tasvir edilenlerin yeterli olduğundan emin olmak için doğrulama testleri yapabileceğini söylemektedir. "Önemli olan" diyor, "ilgili DAAS'ın her bir diyagramda hesaba katılması ve yeterli ayrıntıların mevcut olup olmadığı... ve önceki adımlarda tanımlanan ilk güvenlik politikalarının değiştirilip değiştirilmediği veya ek kontroller gerektirip gerektirmediğidir."

Sıfır Güven Politikalarının Oluşturulmasının ve Sürekli İyileştirilmesinin Doğrulanması

Sıfır güven politikaları her bir koruyucu yüzey için detaylandırılmalı ve aşağıdaki gibi kritik sorulara cevap vermelidir:

- Kurumsal DAAS sistemlerine kimlerin erişmesine izin verilmelidir?
- Hangi uygulamaların kurumsal DAAS sistemlerine erişmesine izin verilecek?
- Kurumsal DAAS sistemlerine erişim ne zaman gerçekleşmeli veya gerçekleşiyor olmalıdır?
- Kurumsal DAAS sistemleri nerede bulunur?
- Kurumsal DAAS sistemlerine neden erişilmesi gerekiyor?
- Kurumsal DAAS sistemlerine erişim nasıl sağlanmalıdır?

Oluşturulan sıfır güven politikalarının uygunluğunu ve geçerliliğini değerlendirmek için, kurumsal ağ genişlemeye ve gelişmeye devam ettikçe BT paydaşlarıyla sürekli etkileşim kritik önem taşır. "Sıfır güven bir hedef değildir" diyor Tirado, "bu nedenle güvenlik politikası ve DAAS koruma gereksinimleri süreç ilerledikçe gelişmelidir."

Tirado'ya göre amaç, bir ağa girebilecek, ağdan çıkabilecek ve ağdan geçebilecek her tür trafiği ele almaya adanmış, sürekli gelişen bir politikaya sahip olmak olmalıdır. "Bir ağ içinde kaynağı veya amacı belirlenemeyen hiçbir şey olmamalıdır" diyor. "İç denetçi değerlendirmesinde, incelemelerin yapılıp yapılmadığını, yeterli ölçüde yapılıp yapılmadığını ve yürürlükteki politikaların bulguları doğru bir şekilde ele alıp almadığını belirlemelidir."

Sıfır Güven Mimarisi İzleme

Önceki örneklerin de gösterdiği gibi, sürekli izleme sıfır güven çerçevesinin başarısı için kritik öneme sahiptir. İzlemenin güvenlik parametrelerine odaklanacağı geleneksel bir sistemin aksine, sıfır güven sisteminin izleme sistemleri kullanıcılar, cihazlar ve hizmetler etrafında yoğunlaşacaktır. "Performansı ölçmek, ağınıza bağlı tüm cihazları tanımlamak ve hileli cihazları ve kötü niyetli faaliyetleri tespit etmek için ağlarınızda izleme yapılmalıdır." Ulusal Siber Güvenlik Merkezi sıfır güven kılavuzunda. Bu özellikle şirket içi hizmetleri barındırıyorsanız geçerlidir, ancak daha yaygın hale geldikçe, mobil cihaz yönetimi de aynı ölçüde dikkate alınmalıdır.

> Performansı ölçmek, ağınıza bağlı tüm cihazları tanımlamak ve hileli cihazları ve kötü amaçlı etkinlikleri tespit etmek için ağlarınızda izleme yapılmalıdır.
>
> **- Ulusal Siber Güvenlik Merkezi**

Tirado, "Benimki gibi şirketler, kullanıcı kabul ettiği sürece söz konusu cihaz için bir ölçüde kontrol sağlayacak mobil cihaz yönetimi yazılımı kullanacak" diyor. "İzleyecek

faaliyeti, tehlikeli sitelerin kısıtlanmasına yardımcı olmak, cihaza yüklenebilecek belirli yazılımları kısıtlamak ve söz konusu sisteme güncellemelerin dağıtılması için bir kontrol sağlamak."

Ayrıca, izleme sadece sistemlerin fiili kullanımını değil, aynı zamanda ne kadar süreyle kullanıldıklarını da içermelidir. Ulusal Siber Güvenlik Merkezi tarafından belirtildiği üzere, "Kullanıcı davranışı, normal çalışma saatleri veya normal çalışma yeri gibi, izlenmesi gereken önemli bir ölçüttür."

Söz konusu ağın özel ihtiyaçlarını karşılamak üzere tasarlanmış çeşitli izleme sistemleri mevcuttur, ancak genellikle bu sistemler toplanan verileri daha sonra analiz edilebilecekleri merkezi bir konuma aktarır. Bu bilgi, zaman içinde, işlem hacmi, varlık iletişimleri ve kullanıcı etkinliği gibi değişkenlere ilişkin normal davranışı neyin oluşturduğuna dair bir "temel" oluşturacaktır.

İç denetçiler yaptıkları değerlendirmelerle bu verilerin düzenli olarak gözden geçirilmesini - ve yönetimin bu görevi uygun şekilde sahiplenmesini - ve bulgularının ağın gerçekliğini doğru şekilde yansıtan bir temel oluşturmasını sağlayabilirler.

Tirado, "İç denetçiler için bunun büyük bir kısmı yönetişimle ilgili" diyor. "Yönetim, sistemin güvence altına alınmasında oynadıkları rol konusunda bilgilendirilmelidir, çünkü sistem kendi başına uzun süre ayakta kalamaz. Güvenlik politikalarındaki değişiklikler, temel çizginin 'normal' ve 'anormal' olarak belirlediği şeylere göre belirlenir. Yönetim incelemeleri bu temel çizgiyi belirler."

Bir Referans Noktası Oluşturma

Siber güvenliğin veya aslında risk yönetiminin birçok unsuru gibi, "herkese uyan tek bir model" yoktur ve bu nedenle, iç denetim biriminin buna nasıl katkıda bulunacağı önemli ölçüde değişecektir. Tirado, "Bu kaynaklara bağlı" diyor. "Bu, kuruluşun büyüklüğüne bağlıdır. Bu, iç denetim ekibinin görev alanına bağlıdır."

Bir temel oluşturmak için iyi bir yer, diğer denetim sistemlerine benzemeyen bir güvence sağlama sürecinin haritasını çıkarmaktır diyor. "Örnek olarak Sarbanes-Oxley'i düşünün" diyor. "Her halka açık şirket, bu matrisi geliştirerek mali tablolarla ilgili iç kontrollerin haritasını çıkarmalıdır. Ve bu eşleştirmenin bir parçası olarak, belirli bir dönem boyunca test prosedürleri oluşturacaksınız - belirli bir yıl gibi. Aynı yaklaşımı sıfır güven için de uygular, şirketin büyüklüğünü, kaynaklarını vs. göz önünde bulundurarak güvenceyi yıl boyunca parçalara ayırırsınız.

Ancak tüm vakalar arasındaki ortak nokta, iç denetimin sıfır güven sisteminin uygulanmasını ve sürekli iyileştirilmesini sürekli olarak destekleme yükümlülüğüdür. Piyasada, sıfır güven modelinin odaklandığı unsura bağlı olarak bu göreve yardımcı olan çeşitli kaynaklar bulunmaktadır. Örneğin, Tirado fidye yazılımı riskleriyle ilgili olarak, FBI ve özel sektör üyeleriyle ortaklık yoluyla geliştirilen ücretsiz bir bilgi paylaşım aracı olan InfraGard'ı kullanıyor. Tirado, her günün başında sadece birkaç dakika içinde bu aracı kullanarak hem kendi sektöründeki hem de sektör dışındaki en son fidye yazılımı saldırıları ve veri ihlalleri hakkında güncel bilgilere ulaşabiliyor. "Bu saldırıların ölçeği, çevre tabanlı bir güvenlik modelinin ötesinde bir yaklaşım için yalvarıyor" diye açıklıyor. "Paydaşları risk ortamının neye benzediği ve nelerin tehlikede olduğu konusunda bilgilendirmek iç denetimin bir numaralı önceliğidir."Ayrıca, bunun bir anda gerçekleşmesi gereken bir geçiş olmadığını da unutmamak gerekir. Tirado, "Kısmi formda bile olsa, sıfır güven modelinin muazzam bir değeri var" diyor. "Günün sonunda, sıfır güven modeli bir elektronik tablo kontrol sütununa indirgeniyor. Belki 20, belki de sadece 10 ya da 12. Bu beşten iyidir."

- theiia.org

Sıfır güven modelinin ilk aşamalarında dikkate alınması gereken basit kontrol örnekleri şunlardır:

- Veri Şifreleme.
- Güvenlik Farkındalığı Eğitimi.
- Olay Müdahale Planları.
- Uç Nokta Tespit ve Müdahale
- Mikro
- Uyumluluk İzleme.
- Davranışsal Analitik ve Kullanıcı Varlığı

Temel Zaten Var

Ağdaki temel felsefi değişikliğe rağmen, iç denetçiler sıfır güven bir kez anlaşıldığında, fonksiyonun sorumluluklarının daha önce kendilerinden beklenenden tamamen farklı olmaması gerektiğini fark etmelidirler. Sıfır güven uygulamasının kendisi, belirli ticari araçların olası benimsenmesi dışında hiçbir mimari veya altyapı değişikliği gerektirmez, dolayısıyla bunun için güvence sağlayan sistemler de gerektirmez.

Aslında, herhangi bir denetim çalışmasının temel ilkeleri tanımlama, iletişim ve güvenceyi içerir ve bu sorumlulukların her biri değişmeden kalır. Sağlam bir el, Global İç Denetim Standartları™'na bağlılık ve öğrenme isteği ile sıfır güven ağ mimarisine geçiş, bir kurumun korkması gereken bir şey değildir.

Önceki Sayılar

Global Perspectives and Insights'ın önceki sayılarına erişmek için şu adresi ziyaret edin theiia.org/GPI.

Okuyucu Geri Bildirimi

Sorularınızı veya yorumlarınızı şu adrese gönderin globalperspectives@theiia.org.

IIA Hakkında

İç Denetçiler Enstitüsü (IIA) 255.000'den fazla küresel üyeye hizmet veren ve dünya çapında 200.000 Sertifikalı İç Denetçi® (CIA®) sertifikası veren uluslararası bir meslek birliğidir. 1941 yılında kurulan IIA, iç denetim mesleğinin standartlar, sertifikasyon, eğitim, araştırma ve teknik rehberlik alanlarında dünya çapında lider kuruluşu olarak tanınmaktadır. Daha fazla bilgi için şu adresi ziyaret edin theiia.org.

Sorumluluk Reddi

IIA bu belgeyi bilgilendirme ve eğitim amacıyla yayınlamaktadır. Bu materyalin belirli bireysel durumlara kesin cevaplar sağlaması amaçlanmamıştır ve bu nedenle sadece bir rehber olarak kullanılması amaçlanmıştır. IIA, herhangi bir özel durumla doğrudan ilgili bağımsız uzman tavsiyesi alınmasını tavsiye eder. IIA, bu materyale tek başına güvenen hiç kimse için sorumluluk kabul etmez.

Telif Hakkı

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