The Institute of Internal Auditors

TONE at the TOP®

Sayı 70 | Kasım/Aralık 2014

Üst yönetim, yönetim kurulları ve denetim komitelerine yönetişim ile ilgili konularda özet bilgiler

Siber Güvenlik: İçeri Sızdılar. Şimdi Ne Yapmalı?

Hemen hemen hergün, bilgisayar korsanlarının güvenlik duvarının kırılması yoluyla hesaplara girdiğini ve belli başlı şirketlerin verilerini çaldıkları haberlerini görüyoruz. Savunmada kalan pekçok şirket bu duruma benzer şekilde cevap veriyor: Alarm halindeki kamuoyuna durumun düzeltileceğine ve müşterilerin korunacağına dair planların bildirilmesi.

Sonra bu durum tekrarlanıyor; saldırı ve önlem alma kısır döngüsü firmadan firmaya (hatta bazen dönüp dolaşıp aynı firmaya) atlayıp duruyor. Tıpkı fırsat sitelerinde en iyi fırsatı yakalayan fırsatçı gibi.

Ancak bir çok şirket için, hatta neredeyse tüm şirketler için acı gerçek şudur: Mevzu artık güvenlik ihlalinin ne zaman olacağı değildir. Büyük ihtimalle zaten ihlal olmuş durumdadır. Sadece henüz keşfedilmiş değildir. Zararlı yazılımlar ve kötü niyetli programlar bomba gibi patlamadan uzun süre bekleyebilecekleri bir fünyeye sahiptir.

"Verizon Enterprise Solutions" tarafından yapılan ve 50 küresel organizasyondan derlenen verilerden oluşan bir çalışmada araştırmacılar, siber suçluların en ileri düzeydeki veri güvenliğini bile sadece günler içinde ihlal ettiklerini ancak bunların ortaya çıkarılmasının aylar sürdüğünü ortaya koymuşlardır. Gerçekten de, "MarketWatch"'in son raporuna göre, güvenlik firması Trustware bir araştırmasında şirketlerin bir güvenlik ihlalini ortaya çıkarmaları ve yayılmasını engellemeleri ortalama olarak 114 gün sürmektedir.

Açıkçası, bu farkı kapatmak için bir şeyler yapılmalıdır.

Soru şudur: En iyi savunma -veya hücum- hattı hangisidir? "InsideCouncil Magazine" 'in yürüttüğü bir araştırmaya göre, "Fortune 1000" şirketlerinin hukuk birimlerinin yalnızca üçte biri kurumlarının önemli bir saldırıyı önlemeye hazır olduğunu hissettiklerini söylemektedir. Bu durumda geride felaket için muazzam bir boşluk kalmaktadır.

Anahtar Yönetim Kurullarındadır

Verizon'da inceleme konusundan sorumlu yönetici müdür Christopher Novak'a göre "Uzun bir zamandan bu yana, (firma yönetim kurulları ve üst yöneticileri arasında) BT güvenlik yöneticisinin herşeyi elinin altında tuttuğuna dair bir varsayım vardı." "Geçen yıl sonrasında, gördük ki içinde bulunmak istesinler veya istemesinler, üst yönetim ve yönetim kurulu üyeleri işin içine sürüklenmektedirler."

Protiviti'nin 2014 BT Güvenlik ve Bilgi Gizliliği Araştırması'na göre Yönetim Kurulu'nun işin içine girmesi, BT güvenlik profilinin güçlenmesinde fark yaratan bir anahtar olmaktadır. Hala, İç Denetçiler

Enstitüsü'nün Denetim Yöneticileri Merkezi'nin 2014 Meslek anketine cevap verenlerin %15'inden daha azı kendi Yönetim Kurullarının sibergüvenlik hazırlığında aktif olarak yeraldığını söylemiştir.

Yönetim Kurulu üyeleri işin içine girmek için nasıl hazırlanabilirler? İlk olarak, uzmanların siber riskleri yönetme tavsiyelerinin çok boyutlu yaklaşımını anlayarak. Bunlar şöyledir: içeriden gözetim ile sınırların korunması ve içeri sızmaları ortaya çıkartmak için kendini ispatlamış ve uygulanmış bir süreç ; hızlıca sistemleri kapatmak ve paydaşlarla zamanında ve dikkatli bir şekilde iletişim kurmak.

"Ön Kapı" Önlemleri

İyi bir ilk savunma hattı kontrollü bir sızma testini içerir. Böyle bir sızma testinde kurum koruma altındaki sistemlerine sızması için bir danışman tutar.

Nordstrom'da İç Denetimin başında yeralan Dominique Vincenti bu durumu "bir Fort Knox (A.B.D.'deki altın rezervlerinin bulunduğu yüksek güvenlikli önemli bir mekan Ç.N.) inşa etmek" olarak adlandırıyor.Ancak bu şekilde bir çevre sınırının korunması stratejisinin yanlış bir güvenlik hissi yaratabileceği konusunda uyarı yapıyor.

Niçin? Çünkü, risk yöneticileri ön kapıyı izleyedursun, siber suçlular bir çalışanı hatta bir üst yöneticiyi kandırarak kapının anahtarını doğrudan elde ediyorlar- örneğin e-posta ekinde yer alan zararlı yazılımdaki potansiyel tehlikelerinin farkedilememesi ve zararlı yazılımın çalıştırılması ile.,

Çevreleyen surlara hücum etmek yerine içeri sessizce sızarak giren bilgisayar korsanları işlerini sıklıkla ifşa olmadan yapmakta, ticari sırları, savunma Istihbarat bilgilerini veya müşteri hesap bilgilerini çalmakta, bazen yakalanmadan çıkıp gitmelerinden veya unutularak gözden kaybolmalarından önce aylar veya yıllar geçmektedir.

Hızlı Karşılık Verme Planları

Sabre Holding'in İç Denetim Yöneticisi Glyn Smith'e göre, kamunun gözünde itibarını kaybeden şirketler bir ihlale neden olabilecek güvenlik açıklarından ziyade, ,siber suçlular içeri sızdığında buna gereken cevabı veremeyen şirketler oluyor. ". Uzmanlara göre, her kurumun bütünsel kriz yönetimi stratejisinin bir parçası olacak şekilde dokümante edilmiş bir karşılık verme planına ve bunun düzenli provalarını yapmaya ihtiyacı vardır.

Yönetim Kurulu'nun endişelerini gidermek için, yönetim tarafından direktörlerin rollerini içeren genel bir plan sunması gerekir.

Smith'e göre, bu durum herhangi bir antrenörün takımını bir oyuna çıkmadan önce antremanlarla mükemmel hale getirdiği bir futbol oyunu gibidir. "Eğer oyunu hiç oynamamışlarsa; eğer oyun kurucu topu doğru yere atmamışsa, işler iyi gitmeyecektir" diyor Smith.

İletişim ve İşbirliği

Bir kurumdaki yukarıdan aşağıya ve aşağıdan yukarıya olan iletişime ek olarak, Novak, aynı sektördeki kurumların bilgi paylaşmak ve birbirlerinin açık yanlarını korumak için birlikte çalışmalarını tavsiye ediyor.

Novak'a göre "Eğer bir grup sizin sektörünüzdeki bir şirketi hedefliyorsa, sizi de hedeflemesi yüksek bir ihtimaldir". Bilgisayar korsanları birlikte çalışırlar. Kurumlar da güvenlik ihlali ve bunun ortaya çıkarılması arasındaki boşluğu doldurmak için birlikte çalışmalıdırlar.

Şimdi Ne Yapmalı?

IIA Araştırma Vakfı ve ISACA tarafından son dönemde yapılan "Siber güvenlik: Yönetim Kurulu Üyeleri Ne Sormalı" adlı araştırmada, American International Group (AIG) ve İnternet Güvenlik Birliği (Internet Security Alliance (ISA) ile birlikte Ulusal Kurum Direktörleri Derneği'nin (National Association of Corporate Directors – NACD) yayınladığı siber riskler hakkındaki bir rapora dikkat çekmektedir. NACD kurumların yönetim kurulu üyelerinin siber güvenlik endişelerinin giderilmesi ve daha koruyucu bir savunma planı yapmalarını sağlamaya yönelik yönetim için beş gözetim ilkesi öneriyor. Bu beş ilke şunlardır:

1 Siber güveliğe sadece bir BT konusu olarak değil, kurumun tamamını ilgilendiren bir risk yönetimi konusu olarak yaklaşın.

2 Şirketin potansiyel zayıf noktaları ile ilgili olması nedeniyle siber risklerin yasal etkilerini anlayın.

3 Kurumun siber güvenlik uzmanlığını kullanın ve siber risklerin yönetimi konularına yönetim Kurulu toplantılarında yeterli ve düzenli bir şekilde yer verin.

4 Yönetimin uygun bir personel ve bütçe ile kurumun tamamında risk yönetimi çerçevesi oluşturmasını talep edin.

5 Hangi risklerden kaçınılması, hangi risklerin kabul edilmesi, azaltılması ve sigortalanma yoluyla transfer edilmesi gerektiğini tanımlayın ve her bir yaklaşımla ilgili olarak yönetimle somut planlar hakkında tartışma yapılmasını sağlayın.

Direktörler için bir Soru Listesi

- En son siber saldırı zaafiyet değerlendirmeniz ne zaman yapıldı?
- Bu değerlendirmeden ne öğrendik?
- Eğer saldırıya uğruyorsak, nasıl bileceğiz?
- Nasıl tepki vereceğiz?
- Yazılı bir saldırıya karşılık verme planımız var mı?
- Saldırıya karşılık verme planımız bir iletişim stratejisi içeriyor mu?
- Kriz yönetimi ve saldırıya karşılık verme faaliyetlerimizin bir parçası olarak bu planın provasını yaptık mı?

Hızlı Anket Soruları

1. Bir siber saldırı kapıdadır. Buna karşılık vermek için kurumunuz ne kadar hazır durumdadır? (1-5 arası ölçek, 1 "son derece hazır" ve 5 "hiç hazır değil"
2. Zararın tespiti ve düzeltmelerin yapılması için kurumunuzda acil müdahale ekibi var mı?

Cevaplamak için aşağıdaki sayfayı ziyaret ediniz ve diğerlerinin cevaplarını görünüz.
www.theiia.org/goto/quickpoll

Kötü Amaçlı Yazılımlardan Uzak Durun

Eğer bir anahtarınız varsa veya arka kapıdan veya açık bir pencereden içeri girme imkanınız varsa neden kapıyı kırarak giresiniz? Bilgisayar korsanları bir nevi yetenekli elektronik yankesicilerdir.

Büyük ihtimalle oltalama e postalarını duymuşsunuzdur; uydurma bir email ile çalışanların bilgisayarlarına onların klavye vuruşlarını kayıt eden bir zararlı yazılım bulaştıranları.

Duymamış olabileceğiniz iki kavram ise aşağıda bulunmaktadır:

Zıpkınla oltalama: Hedefe yöneltilmiş, üst yöneticilerin şifrelerini almak üzere kişiselleştirilmiş oltalama e-postalarıdır. Üst yöneticilerin daha yüksek yetkilere sahip oldukları varsayımına dayanarak, bilgisayar korsanları bir kurumdan veya bir ilgili bir konu hakkında meşru bir iletişim mesajı olarak görünen bir e-postayı hedefe doğru ustalıkla hazırlamak amacıyla sosyal medyada yer alan bilgileri, haberleri ve diğer halka açık kaynaklardan temin ettikleri bilgileri kullanarak e-postalarını hazırlarlar. E-posta bir kere açıldımı, ondan sonrası diğer herhangi bir oltalama epostası gibidir.

Su birikintisi (watering hole) saldırısı: Kamu kurumları, sosyal kulüpler veya kiliseler gibi düşük güvenlikli web sitelerine yerleştirilen zararlı yazılımlar ile bu sitelere sıklıkla giren yüksek güvenlikli kurumların yöneticilerini hedef alan dolaylı saldırılardır. Tekrar edersek, amaç bir üst yöneticinin bilgisayarını ele geçirmektir. – bu senaryoya göre tehdit yöneticinin ziyaretine kadar daha az güvenlikli bir Sunucu üzerinde sessizce beklenecektir. üst yönetici sayfayı ziyaret edip bilmeden klavye vuruşlarını kaydeden zararlı yazılımı indirecek ve böylelikle korsan yöneticinin şifresini ele geçirecek ve yüksek güvenlikli bilgiye kolaylıkla ulaşacaktır.

Kaynak: Christopher Novak, Verizon Enterprise Solutions

IIA Hakkında

Institute of Internal Auditors (Uluslararası İç Denetçiler Enstitüsü) 190 ülkede 180.000 üyesi bulunan küresel bir mesleki birliktir. IIA, iç denetim mesleğinin savunucusu, uluslar arası standartların düzenleyicisi, baş araştırmacı ve eğiticisidir. www.globaliia.org

Ücretsiz Abonelik

Ücretsiz abonelik için;

www.globaliia.org/Tone-at-the-Top sitesini ziyaret ediniz ya da +1-407-937-1111 numarasını arayınız.

Okuyucu Görüşleri

tone@theiia.org adresine görüş ve yorumlarınızı gönderiniz.

İçerik Danışma Kurulu

Üst yönetim ve yönetim kurullarındaki deneyimleriyle birlikte, aşağıda belirtiler saygıdeğer uzmanlar, bu yayının içeriğine doğrudan katkı sağlamaktadırlar.

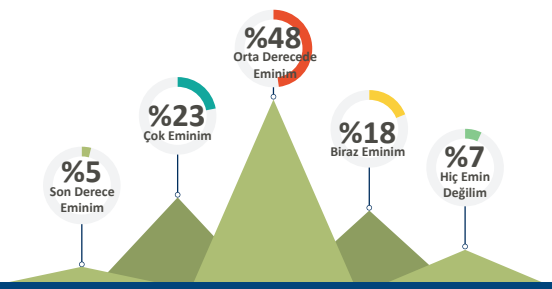
The Institute of Internal Auditors | TONE at the TOP®

NONPROFIT ORGANIZATION
U.S. POSTAGE
PAID
THE INSTITUTE OF
INTERNAL AUDITORS

247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA

Hızlı Anket Cevapları:

Kurumunuzun uyum talepleriyle diğer stratejik riskleri etkili bir şekilde dengelediğinden ne kadar eminsiniz?



Gelecek 3 yılda, iç denetimin uyum taleplerine cevap vermek için ihtiyaç duyacağı kaynakların artacağını mı, azalacağını mı yoksa aynı seviyede kalacağını mı bekliyorsunuz?

*352 cevap verene göredir. Kaynak: İç Denetçiler Enstitüsü Tone at the Top Ağustos/Eylül 2014 anketi