
James A. “Sandy” Winnefeld Jr.,
Christopher Kirchhoff ve David M. Upton

SİBER GÜVENLİKTE İNSAN FAKTÖRÜ: PENTAGON'DAN DERSLER

MICHAEL BYERS

Şirketlerin büyük çoğunluğu eskiye göre siber saldırılara çok daha açık. CEO'lar, güvenlikteki açıkları kapatmak için ABD ordusundan ilham alabilir. Bir zamanlar tehditlere açık devasa bir IT yapısı olan ordu, artık başarıyla yönetilen ağlardan oluşuyor. Bugün ordu, sızma girişimlerini dakikalar içerisinde tespit edip önlem alabiliyor.

Ordu, sadece Eylül 2014-Haziran 2015 döneminde 30 milyondan fazla saldırıya maruz kaldı. Bu saldırılar arasından çok az bir kısmı sınırları aşabildi, bunlarında sadece yüzde 0,1'i sistemlere zarar verebildi. Ordunun siber düşmanlarının ne kadar karmaşık ve becerikli olabileceği göz önüne alındığında bu çok düşük bir oran.

Ordunun deneyiminden çıkarılabilecek kilit bir ders şudur: Her ne kadar teknik güncellemeler önemli olsa da insandan kaynaklanan hataları en aza indirmek çok daha önemli. Başarılı saldırıların kaynağında ağ yöneticileri ve kullanıcılar tarafından yapılabilecek hatalar (kapalı sistemlerdeki açıklara yama uygulayamamak, hatalı konfigürasyonlar yapmak, standart prosedürlere uymamak vb.) yatıyor.

Ordunun güvenliğin bu boyutunu adreslemeye yönelik yaklaşımının kökleri "Nükleer Donanmanın Babası" olarak bilinen Amiral Hyman Rickover'a dayanıyor. Rickover'ın şekillendirilmesinde büyük pay sahibi olduğu nükleer donanma programı hayata geçeli 60 yıl oldu ve tek bir kaza meydana gelmedi. Rickover yoğun biçimde insan faktörüne odaklandı, nükleer enerjiyle çalışan gemilerdeki operatörlerin hataları önleme ve sıkıntıları sorunlara dönüşmeden önce tespit ederek ortadan kaldırma konusunda ciddi ve yoğun bir eğitim almalarını sağladı. ABD Savunma Bakanlığı da IT sistemlerine yönelik saldırılarla mücadele etmek için Rickover'ınkine benzer protokoller hayata geçiriyor. Bu makalenin yazarlarından Sandy Winnefeld ve Christopher Kirchoff, bu çalışmaların içinde etkin biçimde yer alıyor. Bu makalenin amacı, Bakanlığın yaklaşımını özetlemek ve iş dünyasından liderlerin bu yaklaşımı kendi şirketlerinde uygulamalarına fırsat vermektir.

Şirketler de aynı Savunma Bakanlığı gibi sürekli bir saldırı bombardımanı altında: Başka ülkeler, suç şebekeleri, siber vandallar, kötü niyetli rakipler tarafından tutulan saldırganlar ve memnuniyetsiz çalışanlar bu saldırıların kaynağını oluşturabilir. Hırsızlar aralarında Sony, Target, Home Depot, Neiman Marcus, JPMorgan Chase ve Anthem gibi birçok şirketin bulunduğu kurumlardan yüz milyonlarca müşterinin kredi kartı veya kişisel verilerini çaldılar. Petrol ve gaz şirketlerinin yeni bitirdikleri analizlere yönelik bilgileri çaldılar. Valilik seçimlerine hazırlanan adayların müzakere stratejilerini, savunma şirketlerinden silah sistemlerine yönelik verileri çaldılar. Geçtiğimiz üç yıl içinde ABD'deki kritik altyapı sistemlerine (kimya, elektrik, su ve ulaşım sektörlerindeki operasyonları kontrol eden sistemlere) yönelik sızma girişimleri 17 kat arttı. Tüm bunlar sonucunda ABD hükümeti hem kamuda hem de özel sektördeki siber güvenliği ülkenin önceliklerinden biri olarak tanımladı. Ancak kısa bir süre önce Başkanlık Personel Dairesi'nin hacklenmesi bunun kolay bir mücadele olmadığını gösteriyor.

Ordunun Siber Yolculuğu

ABD Savunma Bakanlığı, 2009 yılında IT sistemlerinin ve güvenlik protokollerinin birbirinden farklı olduğunun farkına vardı. Bu durum günümüzde birçok şirket için de geçerli. Ordunun üç temel biriminin her biri, dört hizmet birimi ve dokuz muharip birimi uzun bir süredir kendi kârını-zararını yöneten birimler olarak faaliyet gösteriyorlardı ve IT sistemlerine yatırım yapmaya önem veriyorlardı. Bakanlığın yapısında 7 milyon cihaz, 15 bin farklı ağ yapısı altında çalışıyordu. Bu ağların her biri farklı yöneticiler tarafından yönetiliyordu ve bu yöneticiler kendi ağlarında farklı standartlar kullanabiliyordu. Bu durum güvenlik veya etkinlik açısından pek de iyi bir tablo sergilemiyordu.

2009 yılında o dönemde Savunma Bakanı olan Robert Gates, sistemlerin daha tutarlı olması ve zarar verici saldırılara karşı kökten çözümler bulunması amacıyla ABD Siber Komutanlığı'nı kurdu. Bu bölüm .mil uzantılı tüm ağları dört yıldızlı bir generalin emri altında topladı. Bölüm, zaman kaybetmeden dağınık yapıdaki ağları toparlamaya başladı. 15 bin sistem Ortak Bilgi Ortamı olarak adlandırılan

Fikrin Özeti

SORUN
Siber saldırıların sayısı hızla artıyor. Sony, Target, Home Depot, Anthem ve JPMorgan Chase gibi şirketlerin yakından bildiği gibi bu saldırılar amacına ulaşabiliyor. Genelde buna neden olan hatalar güvenlik teknolojilerinden değil; yöneticiler ve kullanıcılardan kaynaklanıyor.

ÇÖZÜM
Yüksek emniyetli bir organizasyona dönüşün. ABD ordusu da bunu yapıyor. Sistemlerine yapılan saldırıları durdurma ve gerçekleşen birkaç sızmayı kontrol altına alma konusunda çok önemli yol aldılar. Kilit nokta, Amiral Hyman Rickover'ın nükleer donanma için geliştirdiği sıfır hataya dayalı kültürü oluşturmak.

PRENSİPLER
İnsandan kaynaklanan hataları önlemek ve kontrol altına almak için organizasyonun altı prensibi benimsemesi gereklidir: Dürüstlük, bilgi derinliği, prosedürlere uymak, yedekli hareket etmek, sorgulayıcı bir yaklaşım ve iletişimde resmiyet.

bir mimari altında konsolide edildi. Bu süreç sancılı oldu. Fakat kısa bir süre sonra gemiler, denizaltılar, uydular, uzay araçları, uçaklar, gemiler, silah sistemleri ve ordudaki her bir birim, tüm iletişim cihazlarını yönlendiren ortak bir komuta-kontrol yapısına bağlantılı hale geldi. Bu sayede farklı komuta kademelerine, standartlara ve protokollere sahip olan 100 binden fazla ağ operatörü, iyi yönetilen, elit bir ağ savunma gücü haline dönüştü.

ABD Siber Komutanlığı aynı zamanda ordunun teknolojisini de güncelliyordu. Sofistike sensörler, analitik uygulamalar ve bütünleştirilen güvenlik "katmanları" (büyük veri analitiği de dahil olmak üzere birçok fonksiyonu gerçekleştiren teçhizat grupları) ağ yöneticilerine daha önce sahip olmadıkları geniş bir perspektif sağlıyor. Yöneticiler artık anormallikleri hızla belirleyebiliyor, bunun bir tehdit oluşturup oluşturmadığını analiz edebiliyor ve buna cevap olarak ağın yapılandırılmasını düzenleyebiliyorlar.

Daha önce ayrık olan ağların birbiriyle bağlantılı hale gelmesi yeni riskleri de beraberinde getirdi. (Örneğin zararlı yazılımlar sistemler arasında yayılabilir veya bir sistemdeki açık, diğer sistemden veri çalmaya imkan verebilir.) Ancak avantajlar düşünüldüğünde bu riskler gölgede kalıyor. Başlıca avantajlar arasında merkezi izleme, standardize edilmiş savunmalar, kolay güncelleme ve bir saldırı durumunda anlık yapılandırma değişimleri sayılabilir. (Elbette ki gizlilik içeren ağlar açık ağlarla bağlantılı değil.)

Ancak bütünleşik mimari ve son teknoloji cevabın sadece bir kısmını oluşturuyor. .mil ağlarına yapılan tüm sızmalarda en zayıf halka insandı. IŞID, 2015 yılında ABD Merkez Karargah'ın Twitter hesabını kısa bir süreliğine ele geçirmek için bir çalışanın güncellemeyi unuttuğu bir kişisel hesabını kullanmıştı. 2013 yılında bir ülke, ABD Donanması'nın gizlilik içermeyen ağında dört ay boyunca cirit atmıştı. Bunun için de donanmanın web sitesinde bilinen ama düzeltilmeyen bir açıktan faydalanmıştı. Gizli ağlara yönelik en ciddi sızıntı 2008 yılında gerçekleşti. Ortadoğu'daki Merkezi Karargah'tan biri protokolleri ihlal ederek, güvenli masaüstü makineye içinde zararlı yazılım olan harici bir disk takmıştı.

En son sızmalardan da göreceğimiz üzere güvenlik bugün bile mükemmel değil. Bununla beraber, ordunun ağ yöneticilerinin ve kullanıcılarının insani ve teknolojik performansları 2009'daki duruma göre çok daha üst düzeyde. Bu kıyas için başvurabileceğimiz kaynaklardan biri karargahın siber güvenlik denetimleri. Bu denetimlerin sayısı 2011'de 91 adetken, 2015'te 285'e çıkmış durumda. Değerleme kriterlerinin daha da sıkılaştırılmasına rağmen geçer not alan (yani siber saldırılara hazırlıklı) bölümlerin oranı 2011'de yüzde 79 iken, bu yıl yüzde 96'ya yükseldi.

Şirketler de insandan kaynaklanacak hataları dikkate almalı. JPMorgan Chase'e sızan hackerler ikili yetkilendirmeye yönelik ayarları güncellenmeyen bir sunucunun oluşturduğu açıktan faydalandılar. Sağlık sigortası hizmeti veren Anthem'den Aralık 2014'te 80 milyon kişisel kaydın çalınması, birkaç sistem yöneticisinin, bir e-postaya kanarak tıklamalarıyla gerçekleşti. Bu olaylar hem IT çalışanlarının

ABD SAVUNMA BAKANLIĞI AYDA 41 MİLYON TEŞEBBÜS, İZLEME VE SALDIRI İLE KARŞI KARŞIYA.

KAYNAK ABD SAVUNMA BAKANLIĞI

hem de geniş anlamda tüm çalışanların arasında hataların olabileceğini gösteriyor. Birçok araştırma, bilinen açıkların yamalanması ve güvenlik yapılandırma ayarlarının doğru yapıldığından emin olunması gibi basit birkaç yaklaşımla güvenlik tehditlerinin büyük bir kısmının önüne geçilebileceğini ortaya koyuyor.

Buradan alınacak net mesaj, insanların en az teknoloji kadar güvenliğe etkisi olduğu. (Aslında teknoloji sanal bir güvenlik hissi oluşturabilir.) Siber savunmacılar "yüksek emniyetli bir organizasyon" oluşturmak durumunda. Bunu yapmanın yolu da riski sürekli minimize eden benzersiz bir yüksek performans kültürü yaratmaktır. ABD Siber Komutanlığı'nın başında olan Amiral Mike Rogers, "Bu; anlayışla, kültürle ilgili. Organizasyonunuzu kimlerden oluşturduğunuzla, onları nasıl eğitip donattığınızla, yapılandırdığınızla ve uyguladığınız operasyonel konseptlerle ilgili" diyor.

Yüksek Emniyetli Organizasyon

Yüksek emniyetli organizasyon (YEO) konsepti tek bir hatanın sonuçlarının bile felakete yol açabileceği türdeki şirketlerde ortaya çıktı. Örneğin havayolları, hava kontrol sistemleri, uzay uçuşları, nükleer enerji santralleri, orman yangınlarıyla mücadele ve yüksek hızlı trenler... Bu gelişmiş teknik operasyonlarda sistemlerin etkileşimleri, alt sistemler, insan operasyonları ve dış çevre gibi faktörler hatalara zemin hazırlayabilir. Bu hataların felakete dönüşmeden önce önlenmesi gerekir. Bu organizasyonlar "yalın fabrikalar" konseptinden çok farklıdır. Bunların kullanıcılarının hatalardan ders çıkarma lüksü yoktur.

Tehlikeli ve karmaşık bir ortamda teknolojiyi güven içinde işletebilmek için en iyi mühendislik bilgisine ve malzemeye yatırım yapmaktan çok daha öte bir yaklaşım gereklidir. Yüksek emniyetli organizasyonlar kendi zayıf noktalarını çok iyi bilir, kanıtlanmış operasyonel uygulamalara ve yüksek standartlara bağlıdır, şeffaflığın net bir tanımını oluşturmuştur ve hataların gözlenebildiği bir nokta olarak konumlanır.

ABD Donanması'nın nükleer programı en uzun geçmişe sahip YEO'lardan biridir. Bir okyanusun derinliklerinde nükleer reaktörle çalışan bir denizaltıyı işletmek ve bunu yaparken uzun bir süre boyunca iletişimden ve teknik destekten yoksun kalmak basit bir iş değildir. Amiral Rickover, organizasyonun her seviyesinde bir mükemmellik kültürü oluşturmuştu. (Sadece bu kültüre ayak uydurabilecek kişilerin programa alınmasına odaklanmıştı ve programı yönettiği 30 yıl boyunca programa katılacak her bir subayla bire bir görüşme yapmıştı. Halefleri de bu uygulamayı sürdürdü.)

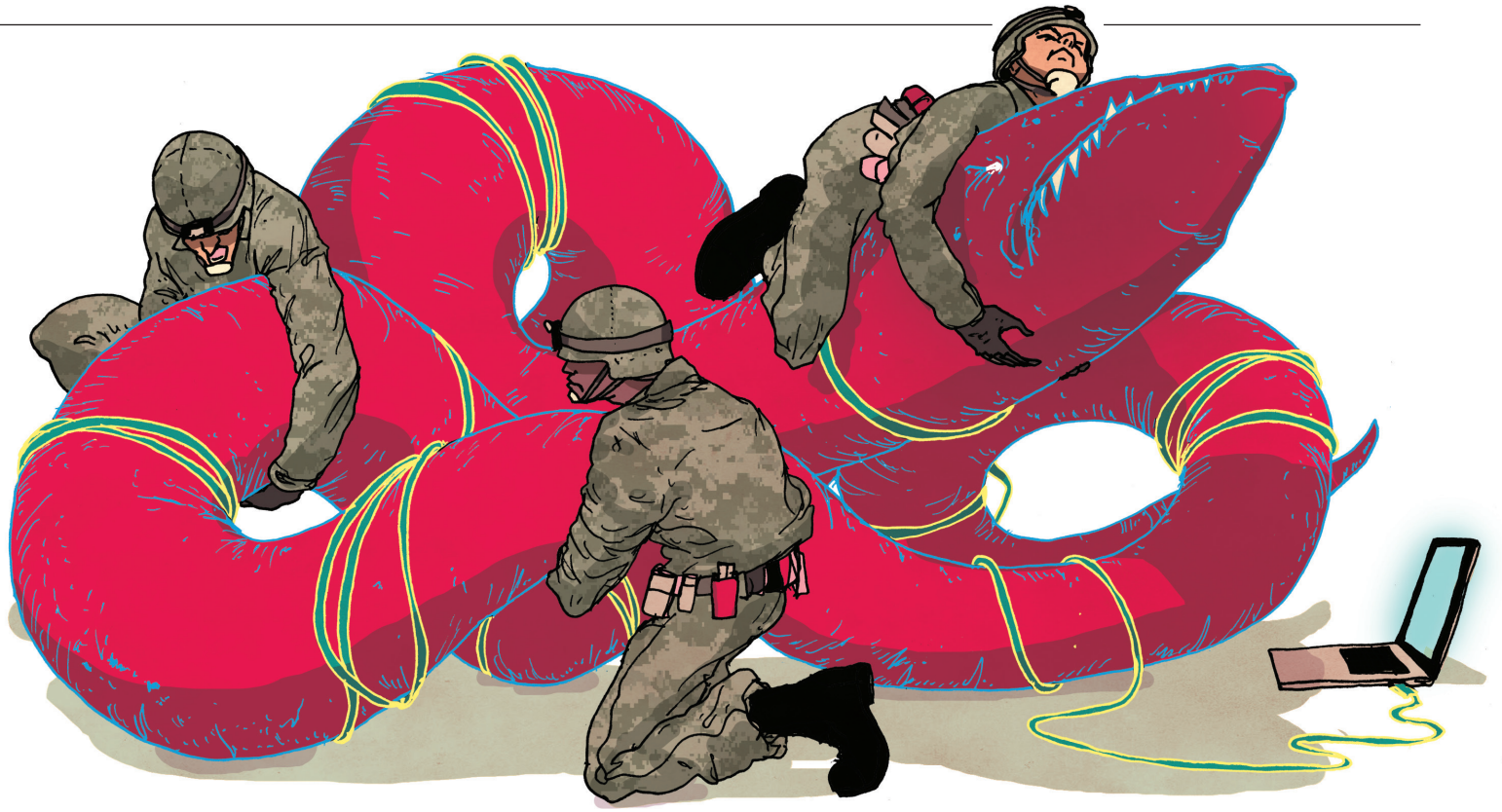
Bu kültürün temelinde donanmanın insandan kaynaklanan hataları belirlemesine ve yok etmesine yardımcı olan ve birbiriyle ilişkili altı prensip yatıyor:

1. Dürüstlük. Bu her bir kişinin, istisnasız biçimde, protokollerden uzaklaşmaması ve hatasını itiraf edip üstlenmesi idealidir. Donanma bunu daha ilk günden insanlara benimsetmeye başlar, ikinci bir şans olmadığını net olarak anlatır. Böylece sadece insanların kolay yollara sapmasının önüne geçilmiş olmaz; ayrıca insanlar olası hataları hızla belirler ve düzeltir. Böylelikle sorun çıkması durumunda gerekecek uzun soruşturma süreçlerinin de önüne geçilmiş olur. Nükleer sistemlerin operatörleri belirli bir eşiğin üzerindeki her tür anormalliği dürüst biçimde merkezi yönetim birimine iletir. Gemilerin komuta subayları kendi programlarının şeffaflığından sorumlu ve buna raporlamadaki dürüstlük de dahil.

2. Bilgi derinliği. Eğer insanlar sistemin tüm unsurlarını net biçimde anlarsa (sistemin mühendislik altyapısı, zayıf noktaları ve sistemi işletmek için gerekli prosedürler de dahil) bir şeyler ters gittiğinde bunu belirlemeye daha hazırlıklı olurlar. Herhangi bir anormalliği soruna dönüşmeden çözümleyebilirler. Nükleer teknoloji kullanan donanmada, operatörler, ellerini bir kumanda sistemine sürmeden önce çok yoğun bir eğitimden geçer ve yetkinliklerini kanıtlayana kadar gözlem altında kalırlar. Sonrasında da periyodik olarak izlenirler, yüzlerce saat ilave eğitimler alırlar ve testlerden geçerler. Gemi kaptanları eğitim süreçlerini yakından izler ve her çeyrekte mürettebatın yetkinliğini raporlar.

TÜKETİCİLERE YÖNELİK SİBER SALDIRILARIN OLUŞTURDUĞU YILLIK ZARAR 113 MİLYAR DOLAR.

KAYNAK *2013 NORTON RAPORU*, SYMANTEC



3. Prosedürlere uymak. Nükleer gemilerde çalışanların doğru operasyonel prosedürleri bilmeleri ve her kelimesine uymaları gereklidir. Ayrıca bir durumun ne zaman mevcut prosedürlerin ötesine geçtiğini ve yeni prosedürlere ne zaman başvurulması gerektiğini de fark edebilmelidirler.

Donanmanın bu uyumu maksimize etmek için başvurduğu yöntemlerden biri çok kapsamlı bir denetim sistemi kurmak. Örneğin, her bir savaş gemisi Operasyonel Reaktör Güvenlik Denetimi'nden geçer. Bu denetimde yazılı testler, görüşmeler ve günlük operasyonların izlenmesi söz konusu. Bunlara ilave olarak, Donanma Reaktörleri Bölgesel Ofisi'nden bir denetçi, önceden haber vermeden bir gemiyi ziyaret edebilir ve yürümekte olan operasyonları ve bakım durumunu denetleyebilir. Denetimcinin belirleyebileceği herhangi bir eksiklikten geminin komutanı sorumludur.

4. Yedekli çalışma. Nükleer sistemler devrede olduğunda onu kontrol eden denizciler kıdemli personel tarafından yakından takip edilir. Sistemde yüksek risk oluşturabilecek her hareket mutlaka iki kişi tarafından yapılmalıdır. Ve mürettebattan en kıdemli kişi de dahil herkes bir sorun çıktığında süreci durdurma yetkisine sahiptir.

5. Sorgulayıcı yaklaşım. Bu bir organizasyonda oturtması kolay olmayan bir yaklaşımdır. Özellikle de belirli bir hiyerarşi içeren ve emre itaatin bir norm olduğu bir yapıda... Ancak bu tür bir bakış açısı zayıflık oluşturur. Eğer insanlar kendi içlerinden gelen tehlike sinyallerini duymak, nedenleri araştırmak ve düzeltici aksiyonları almak için eğitilirlerse problemleri önceden görme şansları büyük ölçüde artar. Sorgulayıcı yaklaşıma sahip olan subaylar işi iki hatta üç kere kontrol eder, anormalliklere karşı uyanık olur ve ortalama cevaplardan asla tatmin olmazlar. Örneğin yüzlerce teçhizat içinden bir tanesine yönelik okuma zamanının neden anormal biçimde değiştiğine veya bir ağın neden belirli bir davranış sergilediğine yönelik sorgulayıcı bir tavır göstermek tüm sisteme zarar verebilecek bir olayı önlemeye yardımcı olabilir.

6. İletişimde resmiyet. Kritik anlarda talimatların hatalı verilmesi veya anlaşılmaması ihtimalini en aza indirgemek için nükleer gemilerdeki operatörler önceden tanımlanmış biçimde iletişimde bulunurlar. Emirleri veya talimatları verenler bunları açık ve net biçimde dile getirir ve talimat alanların da bunu anında tekrarlamaları istenir. Resmiyet ayrıca yanlış anlamaya, dikkat dağılmasına, hatalı

çıkarımlara ve diğer hatalara zemin hazırlayabilecek kişiler arasındaki küçük diyalogların ve geçmişe dayanan tanışıklıkların etkilerini de ortadan kaldırır.

İnsanlardan kaynaklanan hatalar nedeniyle oluşan siber güvenlik açıkları genelde bu altı prensipten birine veya birkaçına uyulmamasından kaynaklanır. İşte Savunma Bakanlığı'nın rutin denetimler sırasında açığa çıkardığı birkaç durum:

- Karargahta çalışan nazik bir subay diğer bir subayın geçmesi için kapıyı açık tuttu. Diğer subay aslında sahte bir geçiş kartı taşıyordu. İçeri bir kez girebilen bu casus, organizasyonun ağına zararlı bir yazılım yükleyebilirdi. Burada çiğnenen kurallar: Prosedürlere uyum ve sorgulayıcı yaklaşım.
- Daha düşük güvenlik seviyesindeki kişisel hesabı üzerinden webde gezinti yapan bir sistem yöneticisi, zararlı bileşenler içeren popüler bir video klip indirdi. Burada çiğnenen kurallar: Dürüstlük ve prosedürlere uyum.
- Bir subay, kendisine indirim vaat eden bir e-postadaki linke tıkladı. Aslında bu e-posta denetimciler tarafından yapılan bir testin parçasıydı ve onun bilgisayarına bir casus yazılım yüklemeye yönelik bir hamleydi. Burada çiğnenen kurallar: Sorgulayıcı yaklaşım, bilgi derinliği ve prosedürlere uyum.
- Yeni başlayan bir ağ yöneticisi talimatları okumadan ve gözlem altında olmadan bir güncelleme yükledi. Bu hareketi sonucunda daha önce uygulanan güvenlik yamaları devre dışı kaldı. Burada çiğnenen kurallar: Bilgi derinliği, prosedürlere uyum ve yedekli çalışma.
- Ağ yardım merkezi bir ofisteki bağlantıyı resetledi ve bunu yapmadan önce bağlantının neden devre dışı kaldığını araştırmadı. Bu devre dışı kalma durumu yetkisi olmayan birinin sisteme girme girişimine karşı sistemin kendi kendini kapatması da olabilirdi. Burada çiğnenen kurallar: Prosedürlere uyum ve sorgulayıcı yaklaşım.

SON 3 YIL İÇİNDE ABD'DEKİ KRİTİK ALTYAPILARA YÖNELİK SIZMALARIN SAYISI 17' KAT ARTTI.

KAYNAK ABD SAVUNMA BAKANLIĞI

Yüksek Emniyetli Bir IT Organizasyonu Oluşturmak

Şu bir gerçek ki her organizasyon birbirinden farklı. Bu nedenle liderler, şirketlerini YEO haline dönüştürmeye yönelik zamanlamayı planlarken iki faktörü dikkate almak durumunda. Bunlardan biri işin türü ve saldırılara ne kadar açık olduğu. (Finansal hizmetler, üretim, kamu hizmetleri ve büyük perakendecilik işleri genelde risklidir.) Bir diğeri de işgücünün doğal yapısı. Y kuşağı ağırlıklı, yaratıcılığı ağır basan ve işbirliği araçlarını kullanarak dışarıdan çalışmaya meyilli bir çalışan kitlesi, birçok kuralı içeren yapısal kurgular çerçevesinde çalışan bir satış ve pazarlama ekibinden çok daha farklı sorunlara neden olabilir.

Ağ yöneticileri ve siber güvenlik personeli için kural temelli bir kültür yaratmak göreceli olarak daha kolaydır. Çalışanların geri kalanı için bunu yapmak pek kolay değildir. Buna rağmen, büyük ölçekli şirketlerde bile ekibin tamamı için böylesi bir kültür oluşturma şansı vardır. Kaliteyi, güvenliği ve fırsat eşitliğini garanti altına alan bir kültür ve operasyonel yaklaşım oluşturmayı başaran birçok şirketin var olduğuna şahit oluyoruz.

Organizasyonlarının dinamikleri ne yapıda olursa olsun liderler sözünü ettiğimiz altı prensibi çalışanlarının günlük rutin operasyonlarına entegre edebilmek için belli başlı kurallar ortaya koyabilirler.

Kontrolü ele alın. Oxford University ve İngiltere'deki Centre for the Protection of the National Infrastructure tarafında kısa bir süre önce yapılan bir çalışmada tepe yöneticilerin siber güvenlik kaygılarının diğer yöneticilere göre daha düşük olduğu belirlendi. Siber saldırıların finansal sonuçları göz önüne alındığında tepedeki bu görüş sığlığı ciddi bir sorun. Ponemon Institute tarafından 2014'te yapılan bir çalışmaya göre ABD'li şirketlerin karşı karşıya kaldığı siber suçların yıllık ortalama maliyeti 12,7 milyon dolar ki bu beş yılda yüzde 96'lık bir artışa karşılık geliyor. Bunun yanı sıra bir siber saldırıyı bertaraf etmek için gerekli süre ortalamada yüzde 33 artış gösterdi ve tek bir saldırıyı bertaraf etmenin ortalama maliyeti 1,6 milyon doları aştı.

Gerçek şu ki CEO'lar siber güvenliği ciddiye almazlarsa organizasyonları da almaz. Emin olun ki

2014 yılında siber saldırganlar tarafından müşteri verileri çalınan Target'ın kovulan CEO'su Gregg Steinhafel, bu işi daha ciddiye almış olmayı dilerdi.

Üst yöneticiler, Savunma Bakanlığı'nın yaptığı gibi birbirinden kopuk ağ sistemlerini bütünleştirmenin önemli olduğunun farkında. Ancak bu yöneticilerin birçoğu yeterince hızlı hareket edemiyor çünkü bu çalışmanın boyutu çok büyük ve maliyeti yüksek olabiliyor. Bu çabayı hızlandırmanın yanı sıra insanların, sistemlerin ve prensiplerin birlikte çalışabilmesi için tüm liderlik ekibinin koordine edilmesi de gerekiyor. Güvenliğin öneminin sürekli vurgulanması çok önemli. Ayrıca CEO'lar, hâlihazırda yüksek emniyetli uygulamalar yaptıklarını iddia eden, tüm gerekenin güvenlik bütçesinin yükseltilmesi veya en yeni güvenlik araçlarının alınması olduğunu söyleyen CIO'lardan gelebilecek direnci de kırmak durumunda.

CEO'lar, YEO oluşturmak ve bunu sürdürülebilir kılmak anlamında tüm adımları atıp atmadıklarına dair kendilerini sorgulamalı. Ağ yöneticileri, sistemlerdeki güvenlik fonksiyonlarının kullanımda ve güncel olup olmadığından emin mi? Davranışlara yönelik denetimler nasıl yapılıyor ve önemli bir eksik tespit edildiğinde ne yapılıyor? Siber güvenliğin davranışsal ve teknik unsurlarına yönelik hangi standart eğitimler veriliyor ve bu programlar ne sıklıkta yenileniyor? Önemli siber güvenlik görevleri (bir sistemde açık oluşturabilecek düzenlemeler gibi) resmi biçimde gerçekleştiriliyor mu ve doğru biçimde yedekleme yapılıyor mu? Ayrıca CEO'lar, dürüstlük, bilgi derinliği, sorgulayıcı yaklaşım, prosedürlere uyum, yedekli çalışma ve resmiyetin kurum için ne anlama geldiğini sürekli biçimde sorgulamalı. Bu arada, olaylara daha üst noktadan bakabilen yönetim kurulları da üst yönetimin siber savunmada insan faktörünü doğru biçimde ele alıp almadığını sorgulamalı. (Gerçekten de şu anda birçok kurul bunu yapıyor.)

Herkesi sorumlu kılın. Ordudaki subaylar artık bilgi teknolojilerinin doğru uygulanmasından da sorumlu ve bu sorumluluk hiyerarşinin bütününde tepeden en alt noktaya kadar yayılıyor. Savunma Bakanlığı ve ABD Siber Komutanlığı, birimlerin güvenlik sıkıntılarını ve anormalliklerini izledikleri basit bir sistem kuruyor. Bu sistemden önce kimin hata yaptığına yönelik bilgiler sadece sistem yöneticilerine iletiliyordu. Kısa süre içinde kıdemli komutanlar birimlerin performansını neredeyse gerçek zamanlı izleme şansına sahip olacak ve bu performans hiyerarşinin daha üst noktalarından da gözlemlenebilecek.

Buradaki temel amaç askeri personel için ağ güvenliğini en az tüfeklerini temiz ve çalışır tutmak kadar rutin bir öncelik haline getirmek. Silahlı kuvvetlerin her bir mensubu ağlarla ilgili temel kuralları bilmek ve bunlara uymak durumunda. Bu kurallar arasında kullanıcıların potansiyel zararlı programları sisteme yüklemelerini önlemek, onaylanmamış yazılımları indirmemek, ağlarda açık oluşturacak web sitelerine girmemek veya kandırmacalı e-postalara karşı uyanık olmak sayılabilir. Bir kural ihlal edilirse ve bu ihlal dürüstlükle ilgili sıkıntıdan kaynaklanıyorsa, komutanların bu hatayı yapan kişiye disiplin cezası uygulaması gerekir. Ve birimde genel bir sıkıntı varsa komutan da yargılanabilir.

Şirketler de benzer bir yol izlemeli. Her ne kadar ordudaki bazı kurallar şirketlerde olmasa da CEO'dan birim yöneticisine tüm yönetim ekibi astlarının siber güvenlik uygulamalarının takipçisi olmalarını sağlamalılar. Yöneticiler, soruna neden olan çalışanların yanı sıra kendilerinin de sorumlu tutulacağının farkında olmalı. Organizasyonun tüm üyeleri, kontrolleri altındaki durumlardan sorumlu tutulacaklarını bilmeli. Şu anda birçok şirkette böyle bir norm yok.

Net standartlar, tek merkezden yönetilen eğitimler ve sertifika programları oluşturun. ABD Siber Komutanlığı ordu ağlarını işleten veya kullanan herkesin sertifika sahibi olmasına, belirli kriterleri karşılamasına ve belirli zamanlarda eğitimler almalasına yönelik standartlar geliştirdi. Ağları savunmaktan sorumlu özel ekiplerdeki personel yoğun bir resmi eğitimden geçiriliyor. Savunma Bakanlığı'ndaki siber güvenlik profesyonelleri donanmadakine benzer bir modelin içinde bulunuyor. Onların eğitiminde sınıflarda dersler, kişisel çalışmalar ve bu sürecin sonunda da resmi bir sınav söz konusu. Ordu akademileri, geniş ve derinlemesine bir savunma ekibi kurabilmek için tüm katılımcıların siber güvenlik dersleri almasını zorunlu kılıyor. İki akademide siber güvenlik operasyonlarına yönelik üst programlar varken iki akademide alt programlar bulunuyor. Tüm birimlerde ileri seviye eğitimler için okullar var ve siber güvenlik uzmanlarınınkine benzer bir kariyer yolu oluşturuluyor. Ayrıca ordu, siber güveliği tüm personelinin devamlı eğitim programına da dahil ediyor.

Buna karşın görece olarak az sayıda şirkette her seviyeden çalışan için siber güvenlik eğitimleri verilir ve yeni tehlikeler ortaya çıktıkça bu program

güncellenir. Çalışanlara riskleri anlatan e-postalar atmak yeterli olmaz. Tüm çalışanların yılda bir kez kurs almaları, dijital politikaları gözden geçirmek için birkaç saatlerini ayırmaları ve her bir dönemin ardından bir teste tabi tutulmaları da yeterli olmaz.

Yoğun biçimde kurgulanmış kurallar zaman gerektirir ve dikkatlerin günlük işlerden bu alana kaymasına neden olur. Ancak her boyutta şirket için bu bir gerekliliktir. Bunlar etik kuralları ve güvenlik uygulamalarını düzenleyen programlar kadar güçlü olmalı ve şirketler kimin katılıp kimin katılmadığını izlemelidir. Sonuçta bir güvenlik açığının oluşması için tek bir eğitimsiz çalışan bile yeterlidir.

Resmiyeti yedekli çalışmayla birleştirin. ABD ordusu 2014 yılında siber komuta ve kontrol yapısını detaylarıyla açıklayan bir yönerge oluşturdu. Bu yönerge kimin neden sorumlu olduğunu, güvenlik yapılandırmalarının hangi seviyelerde yönetildiğini ve güvenlikle ilgili olaylar çerçevesinde nasıl değiştirildiğini netleştiriyordu. Raporlama ve sorumluluklar hakkındaki bu net çerçeve ilave bir koruma işlemiyle de desteklenmişti: Savunma Bakanlığı'nın ağındaki ana bölümlerle ilgili güvenlik güncellemeleri yapıldığında veya sistem yöneticileri hassas verilerin depolandığı yerlere eriştiklerinde "iki kişi" kuralı devreye giriyordu. İki kişinin de yapılan işlemi izlemesi ve doğru olduğuna onay vermesi gerekli. Bu, ilave bir güvenirlik sağlıyor ve şirketin içinden gelecek saldırıları da önemli ölçüde azaltıyor.

Şirketlerin de bunları yapmaması için bir neden yok. Birçok şirket kendileri için kritik kişilerden oluşan "özel kullanıcılar" listelerini oluşturmuş, bir projeyi sonlandıran ya da işten ayrılan çalışanların erişim haklarını kısıtlamaya yönelik süreçler kurgulamıştır. Orta ve küçük ölçekli şirketler de benzer biçimde davranmalı.

Güvenlik konusunda atılabilecek adımlardan biri de ucuz ve kurulumu kolay bazı uyarı yazılımlarını kullanmak. Bu yazılımlar, hassas bilgileri indirirken veya iletirken çalışanları uyarır veya bunu yapmalarına engel olur ve sonrasında onların hareketlerini izler. Çalışanlara, güvenlik kurallarına ne kadar uyduklarının izlendiği bilgisinin verilmesi daha yüksek güvenlikli bir kültürün oluşmasına destek olacaktır.

Savunmanızı kontrol edin. Haziran 2015'de ABD Siber Komutanlığı ve Savunma Bakanlığı hem ağ operatörlerine hem de kullanıcılara yönelik operasyonel testler uygulayacaklarını açıkladılar. Ordu, ayrıca siber güvenlik denetimleri için katı standartlar belirliyor ve bu denetimleri yapacak ekipleri yakından koordine ediyor.

Şirketler de bu yöntemi izlemeli. Her ne kadar birçok büyük ölçekli şirket güvenlik denetimleri gerçekleştiriyor olsa da daha çok ağların dış saldırılara yönelik güçlendirilmesine odaklanıyorlar ve çalışanlardan gelebilecek tehditlere yeterince önem vermiyorlar. CEO'lar operasyonel IT uygulamalarının test edilmesini ve kurumsal denetim fonksiyonunun sorumluluk alanının siber güvenlik teknolojilerini, uygulamalarını ve kültürünü de kapsamasını sağlamalı. (Bu denetim hizmeti kurum dışından da alınabilir.)

Bu düzenli denetimlerin yanı sıra şirketlerde ani, önceden bilgi verilmeyen denetimler de yapılmalı. Bu tür denetimler, çalışanlarda alışkanlık yaratabilecek kısa yolları kullanmanın ve olaylara yeterince özen göstermeme refleksinin önüne geçmek için iyi bir araç. Çalışanlar evde çalışmak için özel bilgileri güvenli olmayan bilgisayarlara yüklemek, hassas bilgileri göndermek için herkese açık bulut sistemlerini kullanmak ve şifrelerini diğer çalışanlarla paylaşmak gibi davranışlarda bulunabilir. Bu davranışları, ciddi bir sorun oluşturmadan belirlemek ve düzeltmek önemli.

Dürüstlük korkusunu ortadan kaldırın ve dürüst olmamanın bedelini ağırlaştırın. Liderler; bilinçli yapılmayan durumsal hataları, bu hataların oluşmasına zemin hazırlayan süreçleri düzeltmek için bir fırsat olarak görmeli. Ancak bu hatalar, söz konusu eksiklikleri bilinçli biçimde kullanıp zarar vermeye niyetli olan kişilere de açık vermemeli. Edward Snowden, sivil bir memuru, kendisinin bilgisayarına şifresini girmeye ikna etmek suretiyle gizli bilgilere erişebilmişti. Bu protokolün ciddi biçimde ihlal edilmesiydi ve sivil çalışan işinden oldu. Tüm bunlar askeri yetkililerin; dürüstlüğü, sorgulayıcı yaklaşımı, yedeklemeyi, prosedürlere uyumu öne çıkaran bir kültür yaratılması durumunda Snowden gibilerin durdurulabileceğini

SAVUNMA BAKANLIĞI, 15,000 AĞI TEK BİR MİMARİ ALTINDA KONSOLİDE EDİYOR.

KAYNAK ABD SAVUNMA BAKANLIĞI

anlamasına imkân verdi. Bu tür kural ihlalleri nükleer reaktörlerin işletildiği donanma gemilerinde söz konusu bile olamaz.

Bu arada, kullanıcılar da masum hatalarını bildirmeleri konusunda cesaretlendirilmeli. Nükleer sistemleri yöneten operatörler bir hata bulduklarında bunu anında yöneticilerine iletmekle yükümlü. Benzer şekilde, şüpheli bir e-postayı açan veya bir siteye giren bir ağ kullanıcısı da herhangi bir kaygı duymadan bunu bildirebilmeli.

Ve son olarak, organizasyondaki herkesin kolaylıkla soru sorabilmesi gerekli. Nükleer sistem yöneticileri, nasıl başa çıkacaklarını bilemedikleri bir durumla karşılaştıklarında anında üstlerine danışıp fikir almak üzere eğitilirler. Şirketlerde de çalışanlar bir bilgi hattından veya yöneticilerinden bilgi alabilmeli. Böylelikle kullanıcıların hangi davranışın doğru ve güvenli olduğuna dair tahmin yürütmesine gerek kalmayacaktır.

Şu bir gerçek ki birçok şirketin uygulamakta olduğundan çok daha resmi ve katı bir yapı kurmaktan bahsediyoruz. Ancak siber tehditler şirketlere ve ülkelere net ve açık bir tehlike oluşturduğu müddetçe başka bir alternatifimiz de yok. Amerika'nın siber savunmasındaki delikleri doldurmak için kurallar ve prensipler kaçınılmaz.

Peki, şirketler sadece en önemli değerlerini korumaya odaklanamazlar mı? Bunun cevabı: Hayır. Öncelikle, bu siber güvenlikte çoklu standart anlamına gelir ki bu ortamı yönetmek zordur ve tehlikelere açıktır. İkincisi, şirketin en değerli unsurları sizin düşündüğünüz şeyler olmayabilir. (Bazıları Kuzey Kore'nin Sony'yi hacklemesi sonucunda oluşan en büyük zararın ahlaksızca yazılan e-postaların açığa çıkması olduğunu sanabilir.) Son olarak, hackerlar genelde hassas verilerin saklandığı sistemlere, e-postalar gibi daha alt seviye sistemler üzerinden giriş yapar. Bir şirket, tüm verilerini korumak için ortak bir yaklaşım geliştirmeli.

Teknik Yetkinlik, İnsani Mükemmellik

Geçen 10 yılda ağ teknolojisi ciddi bir evrim geçirdi ve önemli olduğu kadar açıklar da barındıran bir operasyonun çok daha ötesinde algılanmaya başladı. Bu yapının güvenliği, en önemli kurumsal önceliklerden biri olarak belirlendi. Siber saldırıların sayısındaki inanılmaz artış bunun doğru bir yaklaşım olduğunun bir kanıtı. Teknoloji tek başına bir ağı korumak için yeterli değil. İnsandan kaynaklanan hataları azaltmak en az teknoloji kadar önemli. Bunu yapmanın yolu kararlı bir amiralin nükleer teknoloji kullanan donanma için 60 yıl önce oluşturduğu prensipleri benimsemekten geçiyor.

Yüksek emniyetli bir kültür oluşturmak ve bu kültürü sürekli beslemek için CEO'ların ve yönetim kurullarının özel desteği kadar önemli yatırım ve eğitimleri de gerektirir. Siber güvenlik ucuz bir konu değil. Ancak bu yatırımlar yapılmak zorunda Şirketlerin ve bu şirketlerin faaliyet gösterdiği ekonomilerin sahibi olan ülkelerin güvenliği ve bekâsı buna bağlı.

James A. "Sandy" Winnefeld Jr., ABD Genel Kurmay Başkanlığı'nın sözcüsü ve ABD Donanması'nda amiraldi. Geçen ağustosta emekli oldu. **Christopher Kirchoff,** ABD Genel Kurmay Başkanı'nın özel yardımcısıdır. **David M. Upton,** Oxford University Said Business School'da Operasyon Yönetimi alanında American Standard profesörüdür.