

Siber Gvenlięe Btnzel Yaklařım:

Sektrlere zg Zorluklarla Bařa ıkmak iin
İnsanlar, Sreler ve Teknoloji arasında
Nasıl bir Denge Kurmalı?



İçindekiler

IDC'nin Görüşü.....	6
1. Kimlik.....	6
2. Analitik.....	6
3. Uygulamalar.....	6
Küresel ve Yerel Siber Güvenlik Ortamı.....	8
1. Küresel Siber Güvenlik Ortamı.....	8
2. Türkiye'nin Siber Güvenlik Ortamı.....	8
3. Yaygın Saldırı Türleri.....	10
Risk Yönetiminin Siber Güvenlik Stratejilerindeki Yeri.....	11
1. RiskDeğerlendirmeProtokolleri.....	12
Siber Güvenliğin Çeşitli Sektörlerdeki Evrimi.....	14
1. Finans.....	14
2. Perakende.....	14
3. Enerji.....	14
4. Sağlık Hizmetleri.....	14
5. Üretim.....	15
Siber Güvenlik Ekosistemini Bozan Yeni Teknolojiler.....	17
360° Siber Güvenlik Yaklaşımı.....	19
Kurumların Önündeki Başlıca Zorluklar.....	22
Temel Tavsiyeler.....	24
1. SiberGüvenlikStratejileriniziDXPlatformuGenelindeUygulayın.....	24
2. Esaslı bir “Olaylara Müdahale Planı” Yapın.....	24
3. Proaktif bir Güvenlik Yaklaşımı Benimseyin.....	24
4. Güvenlik Uzmanlarınızı Sürekli Olarak Eğitin.....	24
5. Tehdit Avcılığı Becerilerinizi Geliştirin.....	24
6. Yönetilen Güvenlik Hizmeti AR&GE Yol Haritanızı Değerlendirin.....	24
Geleceğe Bakış.....	25

Nevin Çizmecioğulları

Ülke Direktörü

IDC Türkiye

IDC Türkiye olarak gerek güvenlik alanında yayınladığımız raporlar ve pazar araştırmalarıyla, gerekse belirli aralıklarla gerçekleştirdiğimiz CISO Danışma Kurulu toplantılarımız ve güvenlik özelindeki odaklı etkinliklerimizle güvenlik pazarının nabzını tutmaya devam ediyoruz.

Günümüzün siber tehditleri siber güvenlikten daha hızlı büyüyor ve kurumlarımız maalesef hiç olmadığı kadar yüksek güvenlik riskleriyle karşı karşıyalar. Bu süreçte, artan tehdit sayısı ve yeni teknoloji yatırımlarıyla genişleyen tehdit yüzeyi ile birlikte kurumlar güvenlik riskini nasıl daha iyi yöneteceklerine odaklanıyorlar.

Güvenlik artık yönetim kurulu seviyesinde değerlendirilen bir alan ve dijital dönüşüm stratejilerinin ayrılmaz bir parçası haline geldi. Dijital dönüşüm stratejileri doğrultusunda yeni teknolojilere hızla yatırımlarını gerçekleştiren kurumlar, değişen ve karmaşıklaşan BT altyapılarının güvenliğini sağlamak için güvenlik yaklaşımlarını değiştiriyor. “Güvenliğin Sürdürülebilirliği” CIO’ların en büyük endişesi olarak IDC Türkiye araştırmalarında da yer alıyor. Nitekim, global risklerin haritasının çıkarıldığı “World Economic Forum”’un raporunda normal olmayan hava olayları, iklim değişikliği ve doğal afetlerden sonra 4. sırada veri dolandırıcılığı yer alırken, 5. sırada ise siber saldırılar geliyor.

Türkiye güvenlik sektörünün karşılaştığı zorluklardan bir diğeri ise uzman insan kaynağı eksikliği. Bu zorluğu aşmak için şirketler, güvenlik uzmanı yetiştirme programları oluştururken, bir yandan da üniversitelerle çeşitli iş birliklikleri yapmaya başlasalarda, bu çalışmaların ve yatırımların güvenlik pazarının ihtiyacını karşılayacak sayıya ve seviyeye ulaşması oldukça



uzun zaman alacak görünüyor. Bu nedenle kurumlar bu ihtiyacı yönetilen güvenlik hizmetleri, güvenlik operasyon merkezi hizmetlerine yatırım gerçekleştirerek karşılamaya devam edecekler.

Dijital dönüşümle hızlanan güvenlik dönüşümü, güvenlik pazarının karşılaştığı zorluklar, güvenlik yaklaşımları ve yeni teknolojilerin güvenliğe olan etkisine yer verdiğimiz raporumuzun, güvenlik dönüşümü yolculuğundaki karar vericiler için bir rehber olacağına inanıyoruz. Çalışmamıza katılarak raporumuza ve sektörümüzün gelişmesine katkıda bulundukları için değerli yöneticilerimize ve kurumlarımıza teşekkür ederiz.

Selda Parın

Kurumsal Pazarlar Genel Müdürü Netaş

Günümüzde dijitalleşmenin artışı her alanda hayatımıza etki ediyor. Ülkeler ve şirketler en büyük sınavını Dijital Dönüşüm Liginde veriyor.

IDC rakamlarına göre, 2022 yılına kadar dünya ekonomisinin en az yüzde 60'ının dijitalleşmesi bekleniyor. 2022 yılına kadar, dijital dönüşüm için dünyada bilişim sektörü alanına toplam 7,5 trilyon dolar yatırım yapılacağı da öngörüler arasında. Türkiye'de ise bilişim harcamaları bugün 8,6 milyar dolar civarında.

Dijital dönüşüm sürecinde belki de en hızlı değişen alanlardan biri de siber güvenlik. Siber saldırıları ve savunma yöntemlerini incelediğimizde, dünyadaki gelişmelerle birlikte iki taraf da her seferinde bir üst seviyeye taşıyor. Dijital dönüşümle birlikte gelişen yapay zekâ, nesnelerin interneti (IoT) ve otomasyon gibi teknolojiler de, iş dünyasının risk toleransını değiştiriyor. Bu nedenle riskin yapısı değişerek, ataklar daha organize hale gelirken, bu da firmaların siber güvenlik risklerine ciddi bir şekilde maruz kalmalarına neden oluyor.

IDC öngörülerine göre siber güvenlik açısından 2022 yılına kadar güvenlik harcamalarının yüzde 60'ı ölçeklendirilebilir sınır güvenliği korumasına kayacak. Ölçeklenebilir paketler halinde çözümler sunan MSSP'ler yüzde 15 daha hızlı büyüyecek. Dijitalleşme bir yandan hızlı şekilde ilerlerken; regülasyonlar, standartlar, kişisel veri mahremiyeti gibi olgular ve bunlara uyum süreçleri de beraberinde gündeme geliyor. Dolayısıyla inovasyon beraberinde güvenlik ve risk yönetimi için yeni düşünme biçimlerini getiriyor. Yeni regülasyonlar ve kanunlarla uygulanmaya başlanan cezalar da, kurumları risk toleranslarını düşürmeye zorlayıp yeni düşünce yapılarını hayata geçirmelerini; güvenlik risk faktörlerini önceliklendirmelerini beraberinde getiriyor. Bu anlamda; siber güvenlik hizmetlerinde geleneksel önlemlerinin ötesine geçmek artık bir zorunluluk haline gelmiş durumda.

Tüm bu gelişmelerin ışığında, Netaş olarak siber tehditlere yönelik planlama yerine risk bazlı planlamaya geçerek;



“teknoloji-süreç-iş” bağlantısını kuran analitik ve “makine öğrenmesi” ile verimli sonuçlar ortaya koyan güvenlik çözümleri ile sektörde ilerliyoruz. Siber güvenlik alanındaki yatırımlarımızı doğru insan kaynağı ve otomasyonla beraber, sürdürülebilir ve güvenilir siber güvenlik hizmetleri odağında şekillendiriyoruz.

Bu yıl kuruluşunun 47. yılını kutladığımız Netaş ArGe olarak da ayrıca geliştirdiğimiz yazılımlarla Türkiye'deki bilişim pazarına önemli katkılar sağladığımızı düşünüyoruz. Geliştirdiğimiz ürünler küresel pazarda birçok ülkede kullanılıyor. Bunun yanında, ülkemizde imza attığımız bilgi teknolojileri alanındaki büyük projelerde kazandığımız bilgi birikimimizi; teknolojinin gelişimini ve kullanılmasını güvenli olarak sağlayan siber güvenlik alanında, Türkiye'de yüzde 100 yerli ve yüksek teknoloji belgeli ArGe ürünleri geliştirmede kullanıyoruz. Yeni nesil telefon sistemlerinde güvenlik duvarı, operasyonel yönetim ve detaylı analiz, zafiyet tarama aracı, büyük veri analitiği ve makine öğrenmesi ile kullanıcı davranış modelleme, aykırılık tespiti ve akıllı telefonlarda güvenli iletişim ürünleri geliştirmeye devam ediyoruz.

İnovasyonun beraberinde getirdiği yeni siber güvenlik bakış açısına ışık tutması adına IDC Türkiye ile beraber bu araştırma raporunun hazırlanmasına katkıda bulunmaktan memnuniyet duyuyoruz. Umuyoruz ki bu doküman kurumların, üretici ve hizmet sağlayıcıların kendi güvenlik serüvenlerinde onlara ilham veren bakış açıları kazanmalarına destek sağlasın.

IDC'nin Görüşü

Dijital dönüşüm (DX) vizyonu kurumların, siber güvenlikle baş etme biçimleri de dahil olmak üzere çalışma yöntemlerini değiştirmeye zorluyor. BT altyapısının giderek artan karmaşıklığı, cihazların yaygınlaşması, Kişisel Verileri Koruma Kanunu (KVKK) gibi yeni yönetmeliklerin yürürlüğe girmesi ve hızla değişen tüketici talepleri de kurumların işleyiş biçimlerini değiştiren diğer unsurlar arasında yer almaktadır.

Ayrıca, Nesnelerin İnterneti (IoT) ve Yapay Zeka (AI) gibi dönüşümü hızlandıran etkenlerin yanı sıra Büyük Veri Analitiği, bulut bilişim, sosyal iş ve mobilite gibi 3. Platform teknolojileri de tehditlerin kapsamını genişleterek kurumları yeni zorluklarla baş başa bırakıyor. Türkiye'deki kurumlar 2017'den itibaren aşağıdaki üç husus sebebiyle güvenlik stratejilerini değiştirmek zorunda kaldı:

1. Kimlik

Kimlik artık güvenlik stratejilerinde çok önemli bir yere sahip. Bir kavram olarak kimlik, kişisel olarak tanımlanabilen bilgileri ifade eder ancak kullanıcı davranışını ve kullanıcının anonimliğini de içerir. Kişisel olarak tanımlanabilen bilgileri açığa çıkaran bütün ihlaller, güvenlik ekipleri açısından mağdur tarafın tazmin edilmesini de içeren yasal sonuçlar barındırmaktadır.

2022'ye gelindiğinde “anonimlik” sadece “karanlık ağa” özgü olacak; ticari veya sosyal faaliyetler yürütenlerin tamamı ya takma adlı (yani isimlerin koruma altında olup ancak mahkeme kararıyla açıklanabilmesi) ya da tanımlı olacak.

(IDC FutureScape: Dünyadaki Güvenlik Ürünleri ve Hizmetleri 2019 Tahminleri)

2. Analitik

Analitiğin giderek artan kullanımı 2017'den bu yana ortaya çıkmış eğilimlerin bir diğeridir. Kullanıcı davranışı analitiği (UEBA) artık uç noktalarda, güvenlik ürünlerinde ve yönetilen güvenlik hizmeti platformlarında yaygın şekilde kullanılıyor. UEBA'dan bir aşdaki çeşitli oyuncuların davranış modellerini izlemek amacıyla da yararlanılıyor. Analitik yardımıyla, ajanların kullanılamayacağı durumlarda cihazlardaki veri depolaması ve iletimi ile ilgili fikir sahibi olmak da mümkün. (Bu beceri IoT çağında giderek önem kazanmaktadır.) Güvenlik

analitiği ayrıca alarmları iyileştirmede, “yanlış alarmların” sayısını düşürmede ve gereksiz alarmları bastırmada da kullanılıyor. Bunun dışında, analitik yardımıyla ağlara yapılan farklı türlerdeki saldırılar tahmin edilebiliyor ve yeni savunma stratejileri veya mimarileri geliştirilebiliyor (örneğin, toplanan analitik bilgileri kullanarak alışılmışın dışında güvenlik çözümleri geliştirme gibi).

2021'e gelindiğinde, güvenlik alarmlarının %50'si analistlerin müdahalesi olmadan otomatik olarak cevaplanabilecek.

(IDC FutureScape: Dünyadaki Güvenlik Ürünleri ve Hizmetleri 2019 Tahminleri)

3. Uygulamalar

“Yazılım konteynerleri” en yeni güvenlik endişelerinin başında geliyor. “Geliştirme, güvenlik ve operasyonlar” (DevSecOps) terimi güvenlik ve BT ekiplerinin isteğe özel uygulamalar yazmada kullandığı yazılım konteynerlerini ve uygulama ortamlarını tanımlamada kullanılır. Yazılımcılar çoğu zaman çevikliği güvenliğe tercih eder. Ancak, açıkları olan bir uygulamayı düzeltmek güvenli ancak savunmasız bir uygulamayı düzeltmekten 10 kat daha zor olabilir. Eğer bellekte bir sorun varsa, yanlış alarmlar ortaya çıkabilir. Sonuç olarak, uygulama geliştirmeye başlamadan önce güvenlik ve operasyonlar (SecOps) kümesinin dikkate alınması gerekir.

2024'e kadar, DevSecOps, yeni uygulamaların % 60'ını dağıtım hattında kapsamlı güvenlik ve uyumluluk değerlendirmelerine otomatik olarak tabi tutacak.

(IDC FutureScape: Dünyadaki Güvenlik Ürünleri ve Hizmetleri 2019 Tahminleri)

BT güvenliği bu nedenle Türkiye'deki üst düzey yöneticilerin en önemli sorunu olarak öne çıkıyor. Ancak, son zamanlardaki yüksek maliyetli ve yüksek profilli saldırılara rağmen, ülkedeki üst seviye yöneticiler ve şirket direktörleri genellikle BT güvenliğine pek dikkat etmiyor ve birçoğu siber güvenlik konusunda sorumluluğu tamamen BT departmanlarına yüklerken bunu yapınca da güvenliğin artık bir endişe konusu olmaktan çıktığına inanıyor. CIO ve CISO'ların önündeki en önemli sorun da işte bu aşırı güven tuzağıdır.

BT yöneticileri temel sorunun bir ihlalin meydana gelme olasılığı olmadığını; saldırı sıklığının ve oluşturduğu etkinin daha büyük bir tehlike olduğunun farkına varmalıdır. Dolayısıyla, BT yöneticileri kendi organizasyonları içinde aşağıdakilere hazırlıklı olmalıdır:

- Küresel ve yerel tehdit istihbaratından yararlanarak her tür saldırıyı tespit etme
- İhlallerin niteliğini hızla anlama
- Saldırlara etkin biçimde cevap verme
- Gerekli önlemleri en kısa sürede alma
- Her türlü hasarı tespit etme ve inceleme
- Meydana gelen güvenlik ihlallerini açıkça duyurma

Bazı kuruluşlar siber saldırılardan payını fazlasıyla alır. Bu kuruluşlar kendi güvenlik açıklarının daha çok bilincinde olmalı ve emsallerine göre daha gelişmiş siber güvenlik yöntemleri kullanmalıdır. Ayrıca, finans, devlet, sağlık ve enerji gibi sıkı kontrol altındaki sektörlerde iş yapan firmalar en iyi güvenlik uygulamalarını hayata geçirerek yönetmeliklere uyum sağlamalı ve olası güvenlik risklerini en aza indirmelidir.

IDC Türkiye CIO Zirvesi Anketi 2019'a göre Türkiye'de şirketlerin iş alanındaki en önemli öncelikleri değişiyor. 2019'da müşterilerin ve maliyet etkinliğinin yanında siber güvenlik de en önemli önceliklerden biri oldu. Buna göre, ülkedeki kuruluşların iş alanındaki değişen öncelikleri ve farklılaşan olgunluk düzeyleri paralelinde yenilikten de ödün vermeksizin farklı güvenlik stratejileri benimsemesi gerekiyor. Ancak, kuruluşların fiyat konusundaki hassasiyeti arttıkça CISO'lar ve güvenlik yöneticileri de bütçeden pay almada veya yönetim kurulu üyelerini yeni güvenlik yatırımlarına ikna etmede zorluk yaşayabilir.

Bu güçlüklerin üstesinden gelmek için, yönetim kurulu üyeleri ve üst seviye yöneticiler siber güvenliğe doğru yaklaşımla bakmalıdır. Bu yaklaşımda bir ihlalin gerçek maliyetinin yanında bir siber saldırı sonrası şirket itibarının maruz kalacağı olumsuz sonuçlar dikkate alınmalıdır.

Araştırma Hakkında

Netaş sponsorluğunda hazırlanan bu IDC araştırma raporunda Türkiye'deki mevcut siber güvenlik pazarının dinamikleri incelenmektedir. Ayrıca dijital dönüşümün beraberinde getirdiği güvenlik sorunlarına değinilmekte, güvenlik devriminin gerekliliğine ışık tutulmakta ve güvenlik alanında kesin tavır almanın önemi vurgulanmaktadır.

IDC, kendi güvenlik stratejilerini pekiştirmek isteyen kurumlara uygulamalı rehberlik hizmeti vermektedir. IDC bu araştırma raporunu hazırlarken siber güvenlik alanında yaptığı kesintisiz araştırmalardan ve Türkiye'de yürütmüş olduğu incelemelerden yararlanmıştır.

Küresel ve Yerel Siber Güvenlik Ortamı

1. Küresel Siber Güvenlik Ortamı

Saldırganlar giderek daha gelişmiş tekniklerle saldırılarına devam ediyor. Saldırı kodları katlanarak artıyor ve daha karmaşık siber saldırılar için kolayca birleştirilebiliyor. IDC'ye göre saldırırganlar dört farklı kategoriye ayrılıyor:

- Haktivistler (siyasi amaçlı saldırırganlar)
- Endüstriyel casuslar
- Organize siber suçlular
- Ulus-devlet oyuncuları

Bu saldırırganların gelişme yolunda çok akıllı olmaları gerekmez. Örneğin, aşağıdaki öğeler karanlık ağdan uygun fiyatlarla kolayca temin edilebilir:

- İstismar setleri (exploit kits)
- Hizmet-olarak dağıtık hizmet aksatma (DDoS) araçları
- Kimlik bilgileri
- Kişileri tanımlayıcı bilgiler

Türkiye'deki ve tüm dünyadaki iş ve BT yöneticileri DX'in sunduğu fırsatlarla kuşatıldıkça daha karmaşık ve daha dağıtık BT ortamları oluşturmada ve bunlardan yararlanmada zorluklarla karşılaşılıyor.

Bunun sonucunda, işletmeler karmaşık iş süreçlerini desteklemek, veri toplamak ve önemli bilgileri ve değerli verileri belirlemek için yeni teknolojileri kullanmaktadır. Kurumlar aynı zamanda yeni teknolojilerle beraber gelen yeni zorlukları ve ihtiyaçları karşılamak için siber güvenlik uygulamalarını iyileştirmekte ve bütünleştirmektedir. IDC'nin yaptığı araştırmalara göre siber güvenlik son birkaç yıldır CIO'ların ve BT yöneticilerinin en önemli meselesi haline gelmiştir.

Örneğin, 30 Kasım 2018'de, Marriott International'ın yan kuruluşu Starwood'un misafir rezervasyon sistemlerinin hacker'lar tarafından ele geçirildiği duyuruldu. Marriott International, saldırırganların 2014 yılından bu yana 500 milyon müşterinin verilerine eriştiğini tespit etti. Bu saldırı tarihinde görülmüş en büyüklerden birisiydi ve Facebook, Dunkin', Under Armor, Yahoo, ve Equifax gibi kuruluşlara yapılan uzun bir saldırı dizisinin ardından geldi.

Bir veri ihlalinin ortalama maliyeti 2017'de \$3.62 milyon iken 2018'de bu rakam \$3.86 milyona yükseldi (kaynak: IBM, Bir Veri İhlali Maliyetinin İncelenmesi 2018). Dolayısıyla veri ihlali raporlama planları geliştiren CIO ve CISO'lar kendilerine aşağıdaki soruları sormalı:

- Benim sektörüm ve sistemlerim hangi veri ihlali yasa ve yönetmeliklerine tabi?
- Veri ihlali kimlere bildirmem gerekiyor ve onlarla nasıl irtibat kurabilirim?
- Veri ihlallerinin etkisini en aza indirmek için hangi teknoloji kontrollerini uygulayabilirim?
- Bir veri ihlali raporlama çalışmasının maliyetini azaltmak için siber güvenlik sigortası yaptırmalı mıyım?
- Bildirilmesi gereken bir veri ihlali yaşanması halinde işimi kolaylaştırmak için hangi araç ve prosedürleri geliştirebilirim?

2. Türkiye'nin Siber Güvenlik Ortamı

Türkiye'de Nisan 2018'de yürürlüğe giren KVKK yönetmeliği uyarınca kuruluşlar tüketici verilerini korumak zorundadır ve uygunsuzluk durumunda yüksek cezalarla karşılaşılır. (KVKK kişisel verilerin yönetilme ve korunma biçimlerine değişiklikler getirmiştir.) IDC'ye göre bu yasa ile yerel kurumların veri denetimini ve güvenlik stratejilerini de içeren veri politikalarına yaklaşma yolları değişecektir. Bu yasa ayrıca kurumları veri güvenliği politikalarını tekrar tasarlamaya ve böylece kişisel verilerin izinsiz analiz edilmesi veya kullanılması gibi farklı türdeki kötü niyetli faaliyetlerden korunmaya da itebilir.

Tüm dünyada, işletmelerin %40'ı Avrupa Birliği Genel Veri Koruma Yönetmeliğine (GDPR) uygunluk için gereken denetim prosedür ve araçlarını yönetmeliğin Mayıs 2018'deki geçerlilik tarihine kadar yürürlüğe koymayı başaramayarak yönetmeliğin her ihlali için gelirin %4'üne varan oranda ceza ödemek zorunda kaldığı tahmin ediliyor.

(Kaynak: IDC FutureScape: Dünyadaki Analiz ve Bilgi Yönetimi 2018 Tahminleri)

IDC'nin 2019 Türkiye Güvenlik Roadshow Anketine göre, CISO'ların üçte birinden fazlası şirket olarak KVKK'da belirtilen güvenlik şartlarını ve değerlendirmelerini kapsadıklarını düşünüyor. Ancak, CISO'lar KVKK'daki zorunlulukların ötesinde sürekli iyileştirmeler getirmeye ve en iyi uygulamaları hayata geçirmeye pek hazırlıklı olmadıklarını

da belirtiyor. Bununla beraber, IDC'nin tahminlerine göre KVKK Türkiye'deki güvenlik harcamalarına yön vermeye devam ederek hem güvenlik yazılımlarını hem de hizmet piyasasını önemli oranda etkileyecek.

Veri güvenliğine dair endişelerin ve AB'nin GDPR'si dahil düzenleyici hükümlerin artması nedeniyle, 2020'ye kadar, perakendecilerin veri gizliliğini korumak için yaptığı yıllık harcama %25 oranında artmış olacak.

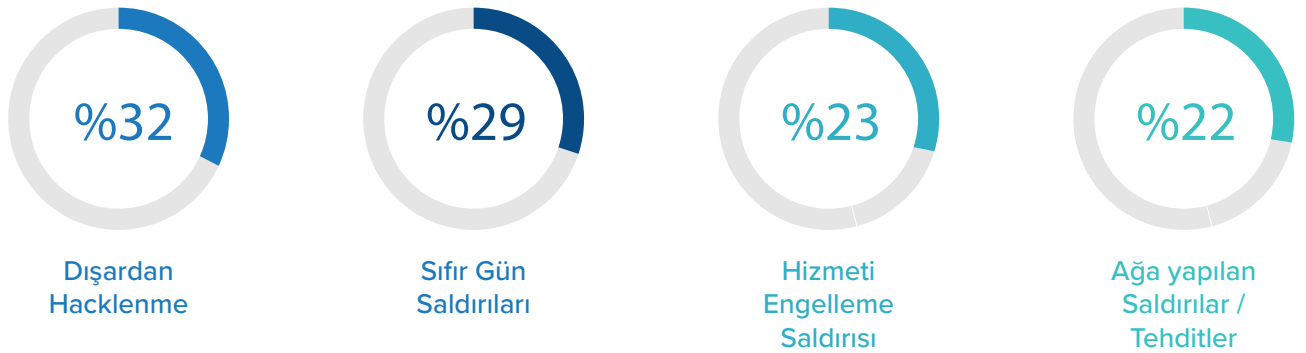
kaygı konusu olup kuruluşları sıfır güven modeli olarak da bilinen dağıtık-bütünlük modelini dikkate almaya itiyor.

Türkiye'deki kuruluşlar siber güvenlik alanında uzmanlaşmış insan kaynakları bulmada güçlük çekiyor. Siber güvenlik becerisine sahip olanlar mevcut personel havuzlarından bulunamadığı için, yeni kaynakların eğitilmesi gerekiyor. Dolayısıyla, işletmeler siber güvenlik personeli boşluğunu doldurmak için yönetilen güvenlik hizmetlerine yatırım yapmaya yöneliyor. Yukarıda belirtilen ankete göre, Türkiye'deki kuruluşlar özellikle yönetilen güvenlik hizmeti sağlayıcılarıyla çalışmayı tercih ederek daha yetenekli güvenlik personeline erişim sağlıyor ve kendi güvenlik duruşlarını da önemli oranda iyileştirebiliyor. Ankete katılanlar ayrıca yönetilen güvenlik hizmetlerinin görünürlüğü ve BT

Şekil 1

Türkiye'deki En Önemli Güvenlik Tehditleri

S. İşletmenizin ağına, verilerine ve internet güvenliğine yönelik aşağıdaki tehditleri ne derece ciddi buluyorsunuz?



Note: n = 216

Kaynak: IDC Türkiye, Türkiye Güvenlik Roadshow 2019, Şubat 2019

(Kaynak: IDC FutureScape: Dünya'daki Perakende 2019 Tahminleri)

Birçok kurumda güvenlik yazılımları ve hizmet uygulamalarında yer alan dahili ekiplerin eğitime ve veri değerlendirme ve keşfetme faaliyetine yatırım yapılıyor. Bunun da ötesinde, gelecekteki operasyonlarında KVKK'nın oynayacağı kritik rolün farkında olan sınırlı sayıda işletme de bu nedenle yeni güvenlik mimarileri için yol haritaları çiziyor.

IDC'nin 2019 Türkiye Güvenlik Roadshow Anketine göre, harici korsanlık ve sıfır gün saldırıları kuruluşların son derece ciddiye aldığı en önemli iki tehdit olarak karşımıza çıkıyor. Bu olası tehditler Türkiye'deki büyük ve çok büyük ölçekli kuruluşların güvenlik harcamalarına yön veriyor. Ayrıca, CIO'ların üçte birinden fazlası çalışanların istemeden yol açtığı veri sızıntısının/kaybının özellikle de KVKK'nın yürürlüğe girmesinin ardından çok ciddi bir tehdit olarak öne çıktığına değindi. Çalışanların sabotajı gibi dahili tehditler de başka bir

altyapısı üzerindeki kontrolü arttırdığına işaret etti. Bu artmış bilinç sayesinde, yönetilen hizmetler eğilimi Türkiye'de güvenlik operasyonları merkezine (SOC) yapılan yatırımları da çoğaltacak.

Güvenlik süreçlerini uygulama, yapılandırma ve yönetmeye uygun güvenlik becerilerine sahip uzmanlar çok az sayıda olduğu için yönetilen güvenlik hizmetleri ve SOC kullanımı giderek daha çok kabul görmektedir. IDC'nin Güvenlik Roadshow anketine katılanların %46'sı kendi SOC'larının orta düzeyde güvenlik sunduğuna işaret etti, başka bir deyişle SOC'lar ağlara, host'lara ve kullanıcılara görünürlük sağlıyordu. Katılımcıların %41'i de SOC'ların ileri düzeyde güvenlik sunduğunu ve ağlara, host'lara ve kullanıcılara tam görünürlük; bütünsel tehdit istihbaratı; gelişmiş analiz imkanı; ve otomatik iş akışı hizmetleri sağladığını belirtti. İleride, SOC sağlayıcılar son kullanıcı taleplerindeki artış ve üstün nitelikli tehdit istihbaratına, olay tespitine ve müdahaleye duyulan

İhtiyaç paralelinde güvenlik açısından daha olgunlaşacaktır. Yönetilen güvenlik hizmeti sağlayıcıları müşterilerin herhangi bir yönlendirmesi olmadan güvenlik olayları için alarm oluşturma ve ötesine geçmeleri gerektiğinin farkındalar. “Yönetilen tespit ve müdahale” (MDR) terimi de böylece son yıllarda moda oldu. Kısaca, MDR güvenlik olaylarının anında tespit edilmesi ve düzeltici tedbir alınması için bağlamanın genişletilmesini ifade ediyor. Ayrıca müşterilere tehdit uyarıları hakkında rehberlik hizmeti vermeyi de içeriyor. Yönetilen güvenlik hizmeti sağlayıcıları şimdi gelişmiş analiz, telemetri, tehdit istihbaratı ve diğer ileri seviyeli teknolojiler sunarak tespit ve müdahale sürelerini kısaltmaya odaklanmaktadır. MDR metodu güvenlik operasyonu uzmanlarına yön vererek, güvenliği düzenleyerek, yönetilen hizmetler sunarak ve olaylara müdahale ederek güvenlik iş akışlarını otomatikleştirmekte ve olayları bağlama yerleştirmektedir.

Şekil 2

Türkiye’de Güvenlik Operasyonları Merkezi Kullanım
S. Lütfen siber güvenlik/güvenlik operasyonları merkezini (CSOC/SOC) olgunluk düzeyini aşağıdaki ölçeği kullanarak değerlendirin.



Note: n = 216

Kaynak: IDC Türkiye, Türkiye Güvenlik Roadshow 2019, Şubat 2019

Dinamik tehdit ortamına ayak uydurma ihtiyacına ve kurumların BT güvenlik ortamlarının giderek artan karmaşıklığına bağlı olarak, güvenlik bilincini artırma ve eğitim verme çözümleri de daha fazla talep görmektedir. Ayrıca, şifre avcılığı ve sosyal mühendislik teşebbüsleri kurumlara meydana okumaya devam etmekte ve güvenlik bilincinin önemini çalışanların gözleri önüne sermektedir. Dolayısıyla, işletmeler güvenlik bilinci konusuna daha fazla odaklanmakta ve siber güvenlik bilinciyle

ilgili olarak çalışanların ikramiyelerini doğrudan etkileyen temel performans göstergeleri (KPI) belirlemektedir. IDC’nin 2019 Türkiye Güvenlik Roadshow Anketinin sonuçlarına göre güvenlik bilinci gelecekte kuruluşlar için en önemli ikinci güvenlik konusu olacaktır.

IDC Dünya Çapında Güvenlik Ürünleri ve Hizmetleri Tahminleri raporunda siber güvenlik alanında hizmetler ve ürünler sunan firma sayısının da 2019’daki 1400 firma seviyesinden düşerek 2023’e kadar yaklaşık %40 azalacağını altı çizilmektedir. Türkiye’de işletmeler için birden fazla güvenlik sağlayıcısının ürün ve hizmetlerinden faydalanmak oldukça yaygın bir uygulama olup bazı firmalar 50’ye varan sayıda sağlayıcı ile çalışmaktadır. Bu kuruluşlar iş yaptıkları güvenlik sağlayıcılarının sayısını azaltacak ve uçtan uca güvenlik çözümlerine veya yönetilen güvenlik hizmetlerine yatırım yaparak yönetim becerilerini iyileştirecektir. Ayrıca, siber güvenlik uzmanlarının az sayıda olması ülkedeki siber güvenlik firmalarının sayıca azalmasını hızlandıracaktır.

3. Yaygın Saldırı Türleri

İşletmelerin her biri kendine özgü bir yapıya, işletim modeline ve altyapıya sahip olsa da hepsi saldırı tehdidi ile karşı karşıya. Dolayısıyla kurumlar güvenlik hizmeti firmalarının uzmanlığından yararlanarak kendi ihtiyaçlarına özel hazırlanmış kapsamlı çerçeveler geliştirebilir.

Dünyanın en büyük alüminyum üreticilerinden biri olan Norsk Hydro’ya yakın geçmişte yapılan saldırı, kuruluşların giderek artan sayıda tehditlerle karşı karşıya olduğunu tam zamanında hatırlatmıştır. ABD’deki bazı fabrikalarda ve Norveç’teki bazı izabe tesislerinde üretimin durmasına sebep olan bu saldırı sonucunda 2019’un ilk çeyreğinde toplamda \$35–41 milyonu bulan zarar meydana gelmiştir. Şirket bu saldırının mali etkisinin 2019’un ikinci çeyreğinde daha da büyüyeceğini tahmin etmektedir. IDC, 2016’da hazırladığı bir raporda, “2019’a gelindiğinde, kökleri ABD ve Avrupa’da bulunan başlıca çok uluslu kuruluşların %70’i malların dağıtımını engellemeye yönelik önemli siber güvenlik saldırılarıyla karşılaşacak.” ifadesiyle bu riske dikkat çekmişti (IDC FutureScape: Dünya Çapındaki Güvenlik Ürünleri ve Hizmetleri 2017 Tahminleri, IDC #US41866116, Kasım 2016).

Bu tahmin doğrultusunda, madencilik endüstrisinin liderleri, kuruluşun işletme tarafındakiler başta olmak üzere yürürlükteki güvenlik süreçlerini ve uygulamalarını tekrar değerlendirmelidir. Cihazların, varlıkların ve operasyonların arasındaki bağlantılar arttıkça bütün endüstri dallarındaki kuruluşların saldırı yüzeyleri de genişlemeye devam etmektedir.

Risk Yönetiminin Siber Güvenlik Stratejilerindeki Yeri

En etkili güvenlik stratejisi asgari BT ve insan kaynakları ile riski en aza indirmektir. Dolayısıyla, firmalar güvenlik risklerinin olasılığını ölçmek zorundadır. Bazı risk ölçme metotlarıyla kötü amaçlı programların, şifre avcısı e-postaların ve web saldırılarının sıklığı azaltılabilir.

Güvenlik programlarının kontrol mekanizmaları bazı işlemlere ya izin verir ya da bunları reddeder. Güvenlik duvarları bazı bağlantılara izin verirken diğerlerini keser, kötü amaçlı yazılım karşıtı çözümler ise hangi dosya ve nesnelerin açılmasına izin verileceğini belirler. Bu kontroller olası saldırıları önleyerek riski azaltır. Ancak, bu güvenlik kontrollerinin tespitleri her zaman doğru olmaz. Örneğin, bazen zararlı yazılım içeren nesnelerin çalışmasına izin verilirken, bazen de meşru eylemler engellenebilir. Bu nedenle risk yönetimi zor bir iştir. Güvenlik kontrollerinin dört olası sonucu vardır: gerçek pozitif, gerçek negatif, yanlış pozitif ve yanlış negatif. Hatalı sonuçların doğru değerlendirilerek ortadan kaldırılması ve kötü amaçlı nesnelerin ve eylemlerin hızla engellenmesi ya da caydırılması bu nedenle önemlidir.

Yanlış pozitiflerin veya negatiflerin doğrulanması zor olabileceğinden, bir güvenlik olayından sonra mutlaka kök neden analizleri yapılmalıdır. Bu analizlerde toplanan bilgiler güvenlik kontrollerinin etkinliğini değerlendirmede kullanılabilir.

Bu kontroller başarılı risk yönetiminin belirleyici unsurlarıdır. Risk analizi, doğası gereği, güvenlik olaylarının olasılığını ve sonuçlarını tahmin etme girişimidir. Risk analizinin özünde

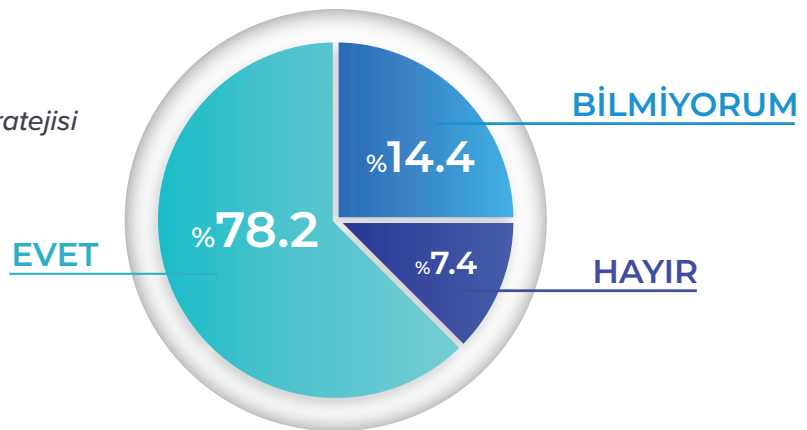
herhangi bir kesinlik derecesi yoktur. Ayrıca, güvenlik uzmanlarının yetkinlikleri ve eylemleri riski doğrudan etkileyen faktörlerdir. Bu nedenle, güvenlik uzmanları elde bulunan bilgileri – örneğin güncel ve geçmiş faaliyet kayıtları ve mevcut varlıklar – yapacakları olasılık tahminleri için girdi olarak kullanmalıdır. Ancak, güvenlik uzmanlarının çoğu girdilerin uygulanması ve analiz edilmesinde fazla deneyim sahibi değildir. Dolayısıyla, siber güvenlik sektöründe risk yönetimi ile güvenlik uzmanlarının yetkinlikleri arasında doğrudan ilişki vardır.

2019 IDC Türkiye Güvenlik Roadshow sırasında yapılan ankete göre, katılımcıların %78.2'si kendi kuruluşlarında risk yönetiminin güvenlik stratejisi planlama süreçlerine dahil edildiğini belirtti. Türkiye'deki işletmeler ayrıca risk bazlı bir yaklaşım benimsiyor ve kendi siber güvenlik stratejisi planlarında risk yönetimini ele alıyor. Bu metodun birkaç bileşeni var:

- **Stratejik:** Stratejik risk yönetimi unsuru sadece olaylara ya da mevzuat parçalarına tepki vermekten ibaret olmamalı. Yönetmelikler genellikle dar odaklıdır ve çoğu zaman kişisel veriler gibi belirli bilgilerin korunması için çıkarılır. Stratejik yaklaşım ise daha geniş açılı ve proaktif.

Şekil 3

Siber Güvenlik Risk Yönetimi
S. Kuruluşunuzda siber güvenlik stratejisi risk yönetimini kapsıyor mu?



Note: n = 99

Kaynak: IDC Türkiye Güvenlik Roadshow Anketi, 2019

- **Bütüncül:** Bütüncül bir risk yönetimi tutumunda kuruluşun karşı karşıya olduğu tehditler, varlıklarının değeri, ve kuruluşun ortamı, altyapısı, sistemleri ve süreçlerindeki hassas noktalar değerlendirilir.
- **Nüans:** İyi bir risk modeli sadece yüksek ve düşük riskleri sınıflandırmakla kalmaz; aynı zamanda riskleri bir spektruma oturtarak önceliklendirmeyi ve uygun şekilde hafifletmeyi sağlar.
- **İşbirlikçi:** BT/Güvenlik yöneticileri kurumsal öncelikler, bağlam ya da deneyim konusunda her zaman çok geniş görüşlü olamaz. Bu nedenle risk komiteleri de risk yaklaşımına katılır; ayrıca tartışmalar yaratıp sonuçlara vararak bunları genel kurumsal hedeflerle hizalar. Dolayısıyla, şirketler farklı iş birimlerinden daha çok sayıda çalışanı buna dahil etmelidir.

Risk yönetiminde, daha önce tespit edilmiş olan istenmeyen sonuçların olasılığı ve etkisi değerlendirilir. Buna göre, ilk adım istenmeyen sonuçların belirlenmesidir çünkü bu aşama risk değerlendirme sürecinin tamamına yön verir. İkinci adım ise riskin tahmin edilmesidir. Bu adım muhtemelen değerlendirme sürecinin en zor bölümüdür çünkü uygun koruyucu mekanizmaların analiz edilerek değerlendirilmesini içerir. Böyle olunca da, sadece riskleri ele almanın ötesinde, kararlar için fikir veren daha sıkı bir süreçle kuruluşlar da daha iyi bir duruma gelir. Riskin tahmin edilmesi aşamasında yürütülmesi gereken başlıca iki eylem olasılığın tahmin edilmesi ve etkinin tahmin edilmesidir.

Risk değerlendirildiğinde ve istenmeyen sonuçlar tespit edildiğinde, güvenlik ekibi bu riskleri hafifletme amaçlı kontrolleri hayata geçirebilir. Bu da belirleme-koruma-seçenekler safhasıdır. Bunu kontrollerin uygulanması ve ortamın izlenmesi safhası izler. Güvenlik tahminlerindeki olası sapma bilinmediği için bu aşama çok karmaşık olabilir. Bu nedenle risk değerlendirmelerinin ardından geri bildirim döngülerinin oluşturulması çok önemlidir. Periyodik değerlendirmeler yapılarak değerlendirme ile ilişkili girdilerin ve değişkenlerin mantıklı olup olmadığı belirlenmelidir. Bu değerlendirme döngüsü kontrol yapılarındaki değişiklikleri etkileyebilir ve gelecekteki tahminleri iyileştirebilir. Ayrıca, ortamın sürekli izlenmesi de kuruluşları tahmin edilemeyen

güvenlik tehditlerine hazırlar. Kuruluşlar güvenlik risklerinin olasılığını düşürmek için güvenlik işlem merkezlerinden, özellikle de onların sunduğu MDR hizmetlerinden de yararlanır.

Güvenlik son yıllarda piyasayı farklılaştıran bir etken ve bir rekabet aracı olmuştur. Firmaların ihaleleri kazanması ya da kaybetmesi artık siber güvenlik becerilerine bağlı. Buna bağlı olarak, siber güvenlik riski yönetimi hakkındaki görüşmelerde üst düzey yöneticiler ve yönetim kurulu üyeleri de yer almalıdır. Aslında, bir kuruluşun koyduğu hedeflere başarıyla ve emin bir şekilde ilerlemesi ancak yönetim kurulu seviyesinde katılım ve destekle mümkün olur. IDC Türkiye Güvenlik Roadshow anketine göre, ülkede yönetim kurulu toplantılarına düzenli olarak katılan CISO'lar çok az sayıdadır. Güvenlik müdürlerinin yönetim kurulu seviyesindeki toplantılarda güvenlik konusunda giderek daha fazla güncel bilgi vermesiyle birlikte bu sayı da gelecek yıllarda artacaktır.

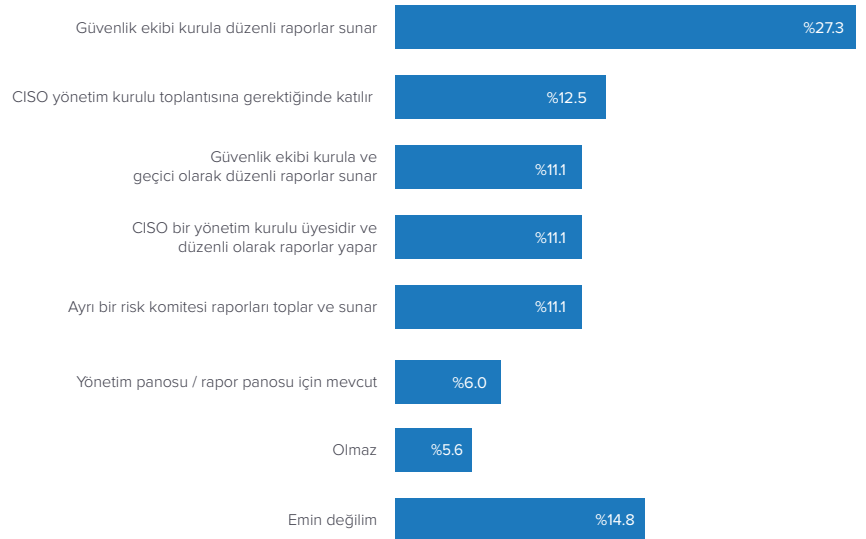
Risk Değerlendirme Protokolleri

Risk değerlendirme protokolleri, tehdit modelleme egzersizleri ve güvenlik prosedürleri yardımıyla yeni güvenlik mimarileri oluşturulabilir. Burada işin zor tarafı eski metotların gelişen bir ortama ne derece uyacağını (ya da uymayacağını) tespit etmektir.

Kapsamlı güvenlik metotları oluşturan ve DX'in beraberinde getirdiği yeni güvenlik güçlüklerinin üzerine eğilen girişimler aşağıdaki etkenleri göz önünde bulundurmalıdır:

Şekil 4

Güvenlik Risklerinin Etkisini Duyurma
S. Güvenlik risklerinin etkileri yönetim kuruluna nasıl duyuruluyor?



Note: n = 99
Kaynak: IDC Türkiye, IDC CIO Zirvesi Türkiye 2019

- **BT güvenliğinin genişleyen sınırları:** Yeni teknolojilerin gelmesi, yazılım geliştirme mimarilerinin evrimi ve giderek artan uygulama çeşitleri sadece girişim altyapısının sınırlarını genişletmekle kalmaz, aynı zamanda hizmet olarak yazılım (SaaS), hizmet olarak platform (PaaS), hizmet olarak altyapı (IaaS) gibi yeni konuşlandırma modellerini kullanmanın yolunu açar.
- **Risk spektrumunun önemi:** Varlıklar ve yazılım/hizmet kaynakları farklı düzeylerde risk içerir. Bu nedenle iyi bir risk modeli sadece varlıkları ve kaynakları yüksek ve düşük riskli olarak sınıflandırmakla kalmamalı, aynı zamanda riskleri hafifletmek için uygun tedbirlerin alınmasını sağlamalıdır.
- **Dağıtık bütünlük modeli:** Son siber saldırılar çevre

güvenliği kavramının geçerliliğini yitirdiğini ortaya koydu; böylece, korunmaya artık bir güvenli bölgenin “içinde” ya da “dışında” olarak bakılamaz. Yeni güvenlik yöntemleri daha çok bölgelerin içi ya da dışı kavramlarını ortadan kaldıran dağıtık-bütünlük/sıfır güven modelinin çevresinde oluşturulmalıdır.

- **Sanallaştırma yoluyla bozulmanın hızlanması:** Geçmişte fiziksel kısıtlar altyapının geçirdiği evrimi yavaşlatmıştı. Ancak, kuruluşlar artık sanal ve yazılım tanımlı kaynaklar sayesinde mevcut altyapıları fazla çaba harcamadan değiştirebiliyor.

IDC'ye göre bu değişen manzara karşısında aşağıdaki dört temel disiplin önem taşıyor:

Şekil 5

Siber Güvenlikteki Dört Temel Disiplin



Kaynak: IDC, 2019

Siber Güvenliğin Çeşitli Sektörlerdeki Evrimi

Her sektörün siber güvenlik dinamikleri ve sorunlu noktaları farklıdır. Dolayısıyla, sektöre özgü bilgiler ve endüstriyi temel alan güvenlik yaklaşımları özellikle de yeni teknolojilerin ve değişen müşteri taleplerinin işteki öncelikleri değiştirdiği ve güvenliğin evrimini endüstri dalından bağımsız olarak hızlandırdığı bir dönemde kuruluşlar için elzemdir.

AI, IoT ve otomasyon gibi teknolojilerin tümü kuruluşları güvenlik risklerine daha da açık hale getirir; ancak, dijital teknolojilere yapılan yatırımlar ve özellikle de bu dijital çözümlerin güvenliğiyle ilgili yatırımlar artarak sayısız seçeneği önümüze sermektedir.

1. Finans

Yeni gelişen teknolojiler ve giderek artan sayıdaki dijital ürün ve hizmetler finans endüstrisindeki kuruluşların risk toleranslarını önemli ölçüde değiştirmiş ve kurumların siber güvenlik risklerine maruziyetini artırmıştır. Kimlik hırsızlığı, dolandırıcılık, fidye yazılımlar ve sosyal mühendislik finans sektöründeki siber tehditlere örnek olarak verilebilir. Bu nedenle finansal hizmet sağlayıcılar bir taraftan veri güvenliğine öncelik verirken diğer taraftan siber güvenlik risklerini azaltabilen teknolojilere odaklanmaktadır. Örneğin, biyometrik ve veri şifreleme teknolojileri kullanılarak hileli işlem riski azaltılır ve veri güvenliği artırılır. Sahtekarlık tespitinde veri analizini zaten kullanmakta olan finansal hizmet sağlayıcılar ise blok zincir teknolojisini uygulayarak işletme maliyetlerini daha da azaltabilir ve şeffaflığı artırabilir.

2. Perakende

Veri tabanlarında gizli nitelikte ve hassas bilgilerin yer alması ve müşterilerle sıkça işlem yapılması nedeniyle perakendeciler siber güvenlik saldırılarından en fazla mağdur olanlar arasındadır. Perakendecilerin çoğu saldırı başına \$250,000'dan daha az dolaylı mali hasar bildirmektedir; ancak, yaklaşık %2'sinin bildirdiği hasar \$5 milyon ile \$10 milyon arasındadır (2017 Veri İhlali Maliyeti Çalışması, IBM Security ve Ponemon Institute, Haziran 2017 verilerine göre). Siber olaylarla ilişkili maliyetler nedeniyle, perakende sektöründeki kuruluşlar şimdi siber güvenliğe yatırım yaparak durumu dengelemeyi düşünmektedir (riske karşı maliyet açısından). Dünya çapındaki perakendeci kuruluşların bu değerlendirmeler paralelinde gelecek üç yıl boyunca yönetilen güvenlik hizmetlerine ve hassasiyet değerlendirmelerine daha fazla yatırım yapması beklenmektedir.

3. Enerji

Yeni teknolojiler ve değişen tüketici talepleri nedeniyle enerji hizmeti sunan kurumlar kendi işlerinde köklü değişikliklere gidiyor. Bu kurumlar müşterilerin kişisel verilerini korumada ve operasyon teknolojisini (OT) fiziksel altyapıya yönelik olası tehditlerden uzak tutmada güçlük çekiyor. Yönetmelik değişiklikleri ve OT/BT'ye siber saldırı riskinin giderek artması da bu sektördeki güvenlik yatırımlarını hızlandırıyor. OT/BT güvenliği ve veri gizliliği gelecek üç yıl boyunca enerji hizmeti kuruluşlarının odaklandığı alanlar olacak.

2020'de, enerji hizmeti kurumları yıllık cirolarının ortalama %1'ini OT/BT siber saldırı riskinin ve veri gizliliğine uygunluğun yönetimine ayıracak.

(Kaynak: IDC FutureScape: Dünyadaki Enerji Hizmeti Endüstrisi 2019 Tahminleri)

4. Sağlık hizmetleri

Elektronik sağlık kayıtları (EHR), çevrimiçi hasta portalları ve hastalara daha iyi hizmet verilmesini sağlayan bağlantılı cihazlar gibi teknolojik gelişmeler nedeniyle sağlık hizmetleri sektörüne yönelik siber tehditler giderek artıyor. Tıbbi ekipmanların dijitalleşmesi ve IoT temelli sensörlerin kullanılması sonucunda, sağlık hizmetlerindeki saldırı yüzeyi genişliyor, sınırlar kayboluyor ve dijital altyapının karmaşıklığı artıyor. Sağlık hizmeti kuruluşları da ihlalleri gerçek zamanlı olarak izleyebilen, rapor edebilen ve tahmin edebilen gelişmiş ve otonom tehdit tespit araçlarına yatırım yapıyor.

Otomatikleşmiş siber savunma sistemleri ve yeni nesil siber güvenlik çözümlerinde yapay zekaya ve makine öğrenimine giderek daha fazla yer verildiği için sağlık hizmeti alanındaki BT personeli güvenlikle ilgili anormalliklerden gerçek zamanlı olarak haberdar olabiliyor. Ayrıca, KVKK'ya uygunluk sağlık kuruluşlarının stratejik gündemlerinde ön sırada yer alıyor.

2022'ye gelindiğinde, sağlık kuruluşlarının %40'ı makine öğreniminden ve yapay zeka algoritmasındaki gelişmelerden yararlanarak kendi siber güvenlik becerilerini geliştirecek ve tehditleri otomatik tespit ederek fidye yazılımlarının önünü alacak.

Kaynak: IDC FutureScape: Dünya Sağlık Endüstrisi 2019 Tahminleri

5. Üretim

“Endüstriyel Nesnelerin İnterneti” (IIoT) girişimleri her geçen gün artıyor ve üretim sektöründeki başarılı iş ekosistemlerinin temelini oluşturuyor. Örneğin, değer zincirlerinin sensörlere bağlanmasıyla daha önce hiç olmadığı kadar işbirliği ve yenilik yapılabiliyor. Sensörler ve IIoT cihazları analiz edilebilecek çok miktarda veri üretiyor. Böylece, üreticiler de üstün özellikli cihazlar ve bolca veri yardımıyla güçlü güvenlik tedbirleri alabiliyor. Ayrıca, üreticiler proaktif güvenlik yöntemleri kullanarak kendi sistemlerini sürekli değerlendiriyor ve güvenlik programlarını güncelliyor.

Her sektörde farklı seviyede siber güvenlik riski vardır. Bu nedenle, firmalar kendi sektörlerindeki başlıca güvenlik

risklerine bağlı olarak siber güvenlikte farklı öncelikler belirler. Örneğin, siber saldırganlar finans sektörünü hedef almaya son derece heveslidir. Dolayısıyla, finans kurumlarının güvenlik risklerini detaylı olarak inceleyip önceliklendirmesi ve uygun siber güvenlik stratejileri belirlemesi önemlidir. Yüksek güvenlik riski barındıran diğer iki sektör ise üretim ve enerji hizmetleridir. Enerji hizmeti kurumlarının çoğu kendi operasyonel ağlarını (örneğin elektrik dağıtım ve iletim ağlarını) izlemek için merkezi kontrol ve veri toplama (SCADA) sistemlerini kullanır. Bu sistemler mevcut hassasiyetleri sebebiyle güvenlik açısından büyük risk barındırır. Üretim tesisleri ve bağlantılı araçlar da siber güvenlik açısından yüksek risk altındadır.

Siber güvenlik riski yönetimi karmaşık bir süreçtir. Ancak, yöneticiler cesaretlerini kaybetmemeli ya da siber güvenlik sorumluluğunu tamamen BT personeline devretmemelidir. Siber güvenlik kurumun tamamını etkiler ve siber riskleri azaltmak için çok sayıda departman ve sorumlu kişi el ele vermelidir. Bu nedenle, ağdaki ihlalleri, kötücül yazılımları ve kötü amaçlı faaliyetleri tespit eden ve bu tehditlerin yok edilmesine ve azaltılmasına yardımcı olan MDR hizmetleri siber güvenlik riskleri yönetiminin özünü oluşturur.



Erkan Sertoğlu

Bilgi Güvenliği Direktörü
Sahibinden.com

GDPR, KVKK ve PCI-DSS gibi düzenlemelerle birlikte bilgi güvenliği alanındaki gereksinimler her geçen gün artarken, yaşanan olaylar güvenlik sorunları da yeni ekleniyor.

Söz konusu düzenlemelerde ve uyumu denetleyen kurumların aldıkları kararlarda teknik bilgi güvenliği önlemlerine yönelik istekler giderek daha fazla yer alıyor. İş gereksinimlerini karşılamak için oluşturulan çözümlerin yalınlıktan uzaklaşması ve çözümlerin birbirleriyle etkileşimlerinin artması da bilgi güvenliği olaylarının sayısında ve etkisinde artışa yol açıyor. Bununla birlikte halen bilgi güvenliği -genellikle- lüks bir ihtiyaç olarak değerlendiriliyor ve bilgi güvenliği bütçeleri varsayılan tasarruf alanı olarak görülüyor. Bilgi güvenliği alanında yetişmiş insan kaynağının sınırlı oluşu da göz önüne alındığında günümüzün ihtiyacı olan odaklanmış bilgi güvenliği uzmanlarının şirket içinde bulundurulması ihtiyacına yanıt verilemez hale gelmektedir. Bu durum beraberinde şirketler, giderek her geçen gün bilgi güvenliğiyle ilgili daha büyük riskleri daha az kaynakla yanıtlamak zorunda kalmalarına yol açmaktadır.

Bu kaynak yönetim sorununu gidermek için yönetilen güvenlik hizmetleri gerek dünya genelinde ve gerekse Türkiye’de giderek daha fazla tercih etmeye başlanmıştır. Yönetilen güvenlik hizmetleri kullanımı doğru tedarikçinin seçilmesini kritik bir öneme getirmektedir.

Sahibinden.com olarak yönetilen güvenlik hizmetlerini seçim kriterlerimiz ise sırayla kaliteli hizmet; uygun fiyat ve tedarikçinin verdiği hizmetin sürekliliğini hedeflediğini gösterebildiği bir yönetim ve yatırım modeli olarak öne çıkmaktadır. Aynı zamanda güvenlik hizmetleri sağlayıcısı şirketin, kendi iş önceliklerimizi destekleyecek bilgi güvenliği çerçevesini tanımlamış olması da değerlendirmemiz de önemli bir kriter olarak yer almaktadır. Bununla beraber her şirket kendi iş ihtiyaçlarına göre tedarikçi seçim kriterlerini oluşturması gerekmektedir.

Bilgi güvenliğinde önemli hale gelen bir diğer odak noktası ise siber istihbarat verisidir. Doğru kararların alınabilmesi için



doğru ve yeterli istihbarat verisine zamanında erişebilmenin kritik başarı faktörü haline gelmiştir. Risklerin azaltılması veya veri kaybının önlenmesi gibi bilinen faydalarının yanı sıra bu veri, eğer doğru kullanılırsa, bilgi güvenliği ekibinin etkinliğinin ve verimliliğinin artırılmasıyla, eğitilmesi gibi kritik faydalar sağlanacaktır. Ancak burada önemli olan nokta bir değil binlerce samanlık içindeki altın iğne olarak ifade edilebilecek yeterlilikte ve odaklanmış veriye ulaşabilmektir. Global siber istihbarat otomasyon çözümleri yapılan analizleri hızlandırırsa da; yerel siber tehdit kaynaklarına (örn: Türkçe deep/darkweb portalleri) erişimlerinin sınırlı olması, potansiyel siber saldırganların motivasyon faktörleri ve riskin gerçekleşme olasılığı konusunda “empati” kuramamaları gibi nedenlerden dolayı eksik kalmaktadır. Bu nedenle insanlar tarafından yürütülen siber istihbaratın önemi gittikçe artacaktır.

Özetlemek gerekirse; önümüzdeki günlerde yerel siber istihbarat sağlayıcıların önemi giderek artacak ve doğru veriyi, doğru zamanda ve yeterli içerikte sunabilen güvenlik hizmeti sağlayıcıları öne geçecektir. Bununla beraber sınırsız bütçeler ile çalışmamamız doğru siber istihbarat sağlayıcının seçimi ise daha kritik hale gelecektir.

Sonuç olarak yukarıda bahsedilen ve bahsedilmeyen riskler ve gelişmelerin ortak bir noktası bulunmaktadır. Eskiden bilgi güvenliği teknik çözümleri yöneten bir fonksiyon iken gelecek bizim düşünce tarzımızı değiştirmesini ve artık bir iş insanı bakış açısı ile güvenliğe yaklaşmamızı gerektirmektedir. Edinmemiz gereken bakış açısı kıt bütçe kaynaklarını kullanarak organizasyonumuzun iş hedeflerine ulaşmasını destekleyecek güvenlik çözümleri seçebilir hale gelmemizi gerektirmektedir.

Siber Güvenlik Ekosistemini Bozan Yeni Teknolojiler

Sektörler arası dijitalleşme çağında işletmelerin en önemli önceliklerinden biri yenilik yaparak üretkenliği artırmak ve değişen müşteri ihtiyaçlarına cevap vermektir. Bu nedenle, daha verimli, konsolide ve yönetilebilir kurumsal BT çözümlerine yatırım yapan kuruluşların sayısı giderek artmaktadır.

Bulut, mobilite, sosyal iş ve Büyük Veri analizi gibi Üçüncü Platform teknolojileri ve AI, makine öğrenimi ve robot bilimi gibi yeniliği hızlandıran etkenler bu yatırımları ilerletiyor ve işletmelerin çalışma biçimini yeniden şekillendiriyor. Hizmet sağlayıcılar da çözüm sunma yöntemlerinde değişikliğe gidiyor.

Yeni teknolojilerin hızla benimsenmesine bağlı olarak siber güvenlik alanı da benzer şekilde değişiyor. Bazı kuruluşlar yeni teknolojilerin getirdiği tehditlerin hala farkında olmasa da, ya da (güvenlik ürünlerine yaptıkları yatırımlar nedeniyle) olası tehditlerden zarar görmeyeceklerine inansa da, bu bakış açıları her yeni siber saldırı türüyle beraber yavaş yavaş değişiyor.

Bulut: Küresel firmalar bulut bilişim alanın yatırım yapmaya devam ettikçe bulut bazlı ya da bulut kökenli yeni uygulamalar hızla geliştiriliyor. Ancak, çoklu bulut, hibrit bulut ve uça hesaplama çözümlerinin önem kazanmasına rağmen bulut teknolojisi Türkiye’de diğer yerlere kıyasla daha yavaş benimseniyor. Aslında, yeni bulut yaklaşımları güvenlikle ilgili potansiyel sonuçlar doğurur ve çoğu kurum da güvenli ağlardan mahrum olduğu ve tehditlere karşı yeterli tedbir almadığı için bunlardan kaçınmaz. Bu nedenle işletmeler artık kendi bulut yolculuklarına dahili güvenlik politikalarını gözden geçirerek başlamaktadır. Buluta geçiş aşamasında mutlaka güvenlikle ilgili endişelerin detaylı bir listesi çıkarılmalı ve bunların üzerine gidilmelidir. .

İki yıl içinde, işletmeler temel güvenlik eylemlerinin %50’sini halka açık başlıca bulut platformlarının tümü üzerinden tutarlı iş akışlarıyla yürütebilecek

(Kaynak: IDC FutureScape: Dünyadaki Bulut 2018 Tahminleri)

Bulutun güvenlikle desteklenmesi başarılı bulut uygulamalarında önem taşır. Yönetmeliklere uygunluk, veri

gizliliği ve genel BT riski yönetimi bulut güvenliğinin temel özellikleridir. Yazılım Tanımlı Çevre (Siyah Bulut olarak da bilinir) ve uygulama seviyesindeki bulut güvenliği teknolojileri giderek daha gerekli olacaktır.

Yapay Zeka ve Makine Öğrenimi: Yapay zeka ağlar, cihazlar ve sistemlerdeki yapıları öğrenmede ve bir olay olmadan önce sorunları tahmin etmede büyük potansiyel taşıyor. Yapay zeka ile çalışan sistemler süreçlerdeki sapmaların kodlarını çözerek devam eden siber saldırıları da tespit edebilir. Yapay zeka ayrıca akıllı güvenlik özelliklerinden yararlanarak iletim sırasındaki veri ve paket kaybını da tespit eder. Güvenliğin iyileştirilmesi ve uygunluk riskinin azaltılması Yapay zeka /makine öğrenimi temelinde oluşturulan güvenlik çözümlerinin başlıca avantajlarıdır.

Güvenlik alarmlarının %50’den fazlası AI ile çalışan otomasyonla işlenecek.

(Kaynak: IDC’nin dünyadaki ilk on BT endüstrisi tahminleri)

Bununla beraber, saldırganlar da bu teknolojilerden yararlanıyor ve bunları kullanarak bir işletmenin hassas noktalarını eskiye göre çok daha hızlı şekilde tarıyor. BT ve güvenlik operasyonları grupları şimdi bu teknolojiler ve ince ayar tespit metotları yardımıyla tam otomatik müdahale becerisi geliştirmek ve farklı saldırı çeşitlerinin önünü almak için el ele veriyor.

Nesnelerin İnterneti (IoT): Bulutun benimsenmesi ve OT ortamlarında bağlanabilirliğin artmasıyla beraber saldırı yüzeyi de genişliyor. Yeterli koruyucu tedbirler alınmazsa, eskiden kalan OT cihazlarının hassasiyeti özellikle de OT altyapısına paralel olarak yeni cihazların eklenmesi halinde artabilir. Ayrıca, firmalar artık hem buluttan hem de IoT cihazlarından çok daha büyük hacimli hassas veriler topluyor. IoT cihazları çoğu zaman geleneksel uç noktalar kadar yetenekli olmasalar da saldırganların kendi saldırı

planları kapsamında bu cihazlar da hedef alınıyor. IoT ortamlarının karşı karşıya olduğu tehditlere örnek olarak fidiye yazılımları, fikri sırları çalmakta kararlı olan ulus devlet tehdit aktörleri ve hatta rakiplerin kurumsal casusluk ve sabotaj faaliyetleri verilebilir. Bu nedenle, işletmeler şimdi gerekli tedbirleri hayata geçirerek IoT cihazlarını güvenceye almanın yollarını belirliyor. Öte yandan, IoT cihazı satıcıları da yeni IoT cihazlarının daha yüksek güvenlik standartlarında üretilmesi için güvenlik firmalarıyla işbirliğine gidiyor.

2021 yılında G2000 firmalarının %50'den fazlası siber güvenlik veya kamu güvenliği endişelerine değinmeksizin kendi endüstriyel kontrol sistemleri içinde IoT'yi modernleştirip devreye alarak düzenleyicileri yasa çıkarmaya teşvik edecek.

(Kaynak: IDC FutureScape: Dünyadaki IoT 2019 Tahminleri)

Robotik Süreç Otomasyonu (RPA): Otomasyon alanında, robotlar insanların aksine hata yapmadığı ve iyi tanımlanmış kurallar çerçevesinde çalıştığı için faaliyetler daha hatasız ve daha tutarlı şekilde yürütülür. Otomatik iş süreçleri kötü iç ve dış aktörlerden de zarar görmez; sadece programlandıkları şekilde görevlerini yerine getirirler. Dolayısıyla otomasyon güvenlik riskinin azaltılmasında hayati bir unsurdur. Diğer taraftan, hassas verilerin sohbet robotu gibi otomatik araçlar yardımıyla toplanması başka güvenlik riskleri doğurabilir. Bu nedenle güvenlik risklerinin yönetimine RPA açısından öncelik verilmesi şarttır. Görev bazlı merkezileştirilmiş yönetim ve şifreleme başlıca güvenlik tedbirleri olarak öne çıkar.

Mobilite: Mobilite hızla örgütsel ortamların parçası haline gelmiş bir özellik olmakla beraber hala güvenlik

departmanlarının tam olarak kontrolü altında değildir; şirketlerin mobil güvenliğe veya mobil uygulamalara yatırım yapma hızı mobil cihazların buralardaki teknoloji ortamlarına yayılma hızının gerisinde kalmıştır. Bu nedenle mobilite, IDC'nin Türkiye CIO Zirveleri sırasında yapılan anketlerde son beş yıl içindeki yatırım öncelikleri arasında ilk sıraya yerleşmiştir. Kuruluşlar uygulama mobilizasyonunun yanı sıra mobil cihaz yönetimi ve güvenliğine yatırım yapmaya devam edecektir. Mobil uygulamaların güvenliği de önümüzdeki yıllar boyunca şirketlerin gündemindeki yerini koruyacaktır. Bazı kuruluşlar salt mobiliteye özgü güvenlik çözümlerine yatırım yapmaktan çok, güvenli mobil uygulamalar hazırlayacak yazılımcı personel yetiştirmektedir.

Büyük Veri Analizi: IDC 2019 Türkiye CIO Zirvesi Anketine göre, Büyük Veri Analitiği teknolojisi kurumsal DX stratejileri açısından en önemli dijital teknolojiler arasında üçüncü sırada yer alıyor. Ayrıca, Büyük Veri ve Analitik teknolojilerin CIO'ların yatırım planlarındaki yeri her geçen yıl artıyor. Kuruluşlar Büyük Veri ve Analitik stratejilerini siber güvenlik planlarına paralel götürüyor. Güvenlik uzmanları bir Büyük Veri ve Analitik çözüm yaşam döngüsünün her noktasında kontroller yapıyor ve güvenlik risklerinin azaltılması için geçerli yönetmelikler uyarınca gereken tedbirleri alıyor. KVKK ile bilgi keşfi, sınıflandırma, şifreleme ve diğer veri yönetimi ürünlerine talep tetiklendi; ayrıca veri göçü ve bilgi keşfetme ve silme çözümlerine yönelik danışmanlık hizmetlerinin Türkiye'de daha fazla kabul görmesi sağlandı.

Blok Zincir: Blok zincir teknolojisi müşteri işlemlerini güvence altına alır ve paydaşlar arasındaki güveni artırır. Blok zincir teknolojisi ayrıca işlemlerin gizliliğini ve bütünlüğünü pekiştiren ve koruyan, DX faaliyetlerini güvenceye alan ve nihai olarak işinize değer katan yetenekler de sunar. Ancak, dağıtık defter teknolojisi (DLT) yeni tehditleri beraberinde getirir. Örneğin, cryptojacking blok zincir ve kripto para madenciliğin giderek daha revaçta olmasıyla ortaya çıkmış nispeten yeni bir tehdittir.

360° Siber Güvenlik Yaklaşımı

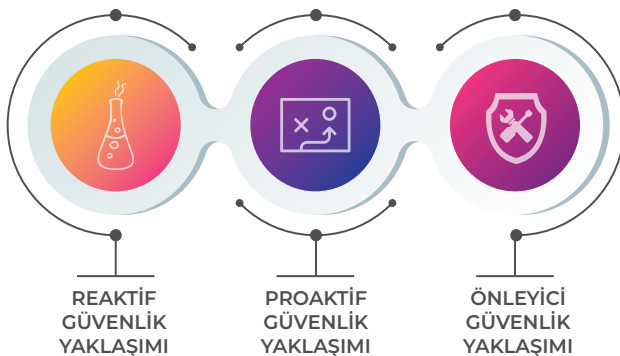
Yeni teknolojiler benimsendikçe tehdit yüzeyi de genişlemeye devam etmektedir. Bunun sonucunda, şirketlerin siber tehditlere maruziyeti de artmaktadır.

Bir şirketin çevresini korumaya ve bilinen tehditleri belirlemeye dayalı pasif güvenlik stratejileri artık yeterli değildir. Ağa ve çevreye odaklı güvenlik tedbirleri yaygınlaştıkça, şirketler de siber güvenlik konusunda 360° bir yaklaşım benimsemelidir. Bu gelecekçi siber güvenlik yaklaşımı aşağıdaki dört hususu içermelidir:

- **Uç Noktalar:** Verilerin şifrelenmiş olmadığı bitiş noktalarında kötü amaçlı yazılım tespiti yapılmalıdır. Uç noktalar en çok verinin üretildiği yer olduğundan bir saldırının da ilk hedef noktalarıdır. Uç noktalar bu nedenle analiz ve tespit için önemli telemetri verileri sağlar.
- **Kimlik:** Kimlik yeni “çevre” olarak tanımlanabilir. Ancak, kimlik sadece bir defa doğrulanmayla sınırlandırılmamalıdır. Bunun yerine, göreve ve ihtiyaca bağlı olarak sürekli şekilde doğrulanmalı ve teyit edilmelidir.
- **Uygulama:** Görece etkisiz güvenlik tedbirlerini dengelemek için uygulama seviyesinde güvenlik benimsenmelidir.
- **Veri:** Veri en değerli kurumsal varlıktır ve kurum savunmasının yeni paradigmasıdır. Veri uygun şekilde korunmalıdır çünkü üretkenliği artırır ve rekabet avantajları sağlar.

Şekil 6

Güvenlik Yaklaşımında Reaktiften Proaktif Geçiş



Kaynak: IDC Türkiye, Türkiye Güvenlik Roadshow 2019, Şubat 2019, n:216

Artık işletmelerin düşmanları proaktif şekilde avlayan, ciddi bir hasar ya da bozulma meydana gelmeden önce tehditleri tespit eden ve güvenlik olaylarına ve veri ihlallerine hızla müdahale eden güvenlik çözümlerine ihtiyacı var. Güvenlik yöntemleri de bu nedenle yeni teknolojileri ve çözümleri de barındıracak ve şirketin bütün varlıklarını kapsayacak şekilde yeniden tasarlanmalıdır. Buna bağlı olarak, şirket varlıklarının düzenli aralıklarla keşfedilip sınıflandırılması elzem bir süreç olacaktır. Bütüncül bir güvenlik yaklaşımı belli aralıklarla yerine getirilmesi gereken tüm süreçleri ve kontrolleri kapsar; buna göre, firmalar ya kendi güvenlik yaklaşımlarını genişletmeli ya da önleyici güvenlik modellerinden yararlanmalıdır.

- **Reaktif:** Reaktif güvenlik yaklaşımı uygulayan firmalarda güvenliğe hazırlık seviyesi ortalamanın altındadır. Bu firmalarda güvenlik uygulamalarından genellikle, eğer varsa, güvenlik uzmanları ve müdürleri sorumlu olur. Güvenlik personelinin olmadığı firmalarda ise günlük güvenlik yönetimi BT departmanlarına devredilmiştir. Üst seviye yöneticiler de güvenliğe orta derecede özen gösterir. Reaktif firmalar ihlal riski altında olduklarını bilmekle beraber, güvenlik tehditlerine vaka bazında tepki verir ve üç ayda bir risk değerlendirmeleri yaparlar. IDC'nin 2019 Türkiye Güvenlik Roadshow Anketine göre, bu kuruluşlar kendi güvenlik deneyimindeki boşlukları doldurmak için üçüncü şahıslardan yararlanır.

- **Proaktif:** Proaktif firmaların güvenliğe hazırlık seviyesi ortalamanın üzerindedir. Proaktif güvenlik yaklaşımı uygulayan firmalar güvenlik ihlallerinin doğuracağı maliyetlerin ve itibar kayıplarının farkındadır. Dolayısıyla, ihlallerden korunmak için temel güvenlik yatırımlarını yapmışlardır ancak sistemlerindeki açıkların siber suçlular tarafından sürekli izleniyor olmasına rağmen gelişmiş güvenlik çözümlerinden veya önleyici güvenlik hizmetlerinden faydalanma olasılıkları düşüktür. Bununla beraber bu şirketlerdeki üst seviye yöneticiler güvenliğin üzerinde önemle durur. Proaktif firmalar genellikle ayda bir kez risk değerlendirmeleri yapar ve dahili güvenlik personelini desteklemek ve kendi güvenlik tutumlarını pekiştirmek için üçüncü şahıslardan yararlanır.

- **Önleyici:** Önleyici bir yaklaşım uygulayan kuruluşlar güvenlik yatırımlarına öncelik verir ve buradaki üst seviye yöneticiler de güvenlik tutumlarını belirleme, yönetme ve gözden geçirmede önemli rol oynar. Bu yöneticiler çalıştıkları şirketin çoğu zaman siber saldırıların hedefinde olduğunu ve bunun sonucunda da zaman zaman ihlallerin yaşandığını bilir. Bu nedenle proaktif biçimde gelişmiş güvenlik teknolojilerini kullanarak veri sızıntılarını ve ihlalleri azaltırlar. Ayrıca, güvenlik zafiyetlerini bulmaya ve tespit edilen boşlukları kapatmaya çalışırlar. Sürekli risk değerlendirmeleri de yaparak güvenlik hizmetlerinden yararlanıp kendi güvenlik personelinin yükünü azaltır ve daha güçlü tehdit istihbaratı becerilerinden faydalanırlar.

IDC'nin araştırmasına göre üçüncü şahısların kullanılması güvenlikte olgunluğun diğer bir ölçütüdür. Güvenlik olgunluğunun düşük seviyelerde olduğu firmalar daha çok iç kaynaklarını kullanmaya odaklanır ve bunun sonucunda da yönetilen güvenlik hizmeti sağlayıcıların sunduğu güvenlik uzmanlığından yararlanmaz. Öte yandan, proaktif bir güvenlik yaklaşımı benimseyen firmalar ise bir taraftan üçüncü şahıslar kanalıyla dış kaynak kullanırken diğer taraftan kendi dahili becerilerini de en kritik görevlere odaklar. Her iki durumda, güvenlik hazırlığı işteki başarıda hayati önem taşır.

Türkiye'de ve dünyada, artan güvenlik uzmanı açığı nedeniyle akademik çevreyi temel alan eğitim programları giderek önem kazanıyor. Güvenlik teknolojileri hızla evrimleştiğinden, mevcut güvenlik uzmanlarının sürekli eğitilmesi gerekiyor. Güvenlik sertifikalarının önemi bir yana, güvenlik uzmanları aynı zamanda modern savunma metodlarını da öğrenmek ve kendi kuruluşlarına daha iyi koruma sağlamak zorunda.

Sektöre özgü güvenlik çözümü eksikliği ve son kullanıcı ihtiyaçlarının hızla değişmesi nedeniyle güvenlik alanındaki araştırma ve geliştirme (AR&GE) faaliyetleri önem kazanıyor. Şirketler güvenlik protokollerini yükseltmek için kendi güvenlik mimarilerine ve altyapılarına paralel çözümler geliştirmek zorunda. Uzman seviyesinde insan kaynağının olmaması ve sektöre özgü çözümlerin bulunmaması nedeniyle, hassasiyetleri tespit etmek, izlemek ve yönetmek ve tehdit istihbaratını ve tespitini sağlamak için (tehdit avcılığı için müdahale hizmetleri dahil) yönetilen güvenlik hizmetlerini kullanmak gerekiyor.



Bülent Kemal Mutlu

ArGe Genel Müdür Vekili
Netaş

Türkiye'nin ilk özel telekomünikasyon ArGe merkezi olarak, bundan 45 yıl önce kurulduğumuz günden bu yana öncü teknolojiler sunuyor ve teknolojiyi sadece kullanan değil, aynı zamanda üreten nesiller yetiştirme vizyonuyla hareket ediyoruz.

Netaş ArGe merkezinde Siber Güvenlik ArGe birimimizde, yerli ve milli kaynaklarımızla geliştirdiğimiz siber güvenlik ürün ve yazılımlarını ülkemize kazandırmanın gururunu yaşıyoruz. Siber güvenlik alanında çok fazla sayıda ürün kategorisi bulunuyor. Bu kategorilerden tespit ettiğimiz üç alanda öncelikli olarak geniş kapsamlı geliştirmeler yapıyoruz. Bunlar, uygulama seviyesi protokol ve uygulamalar için güvenlik çözümleri, güvenli iletişim platformları ve büyük veride güvenli analitik çözümleridir.

Geliştirdiğimiz yerli ve milli ürünlerimizin, ülkemiz açısından önemli bir atılım olduğuna inanıyoruz. Şirketimizin güvenlik ürünlerini destekleyici ve tamamlayıcı bir alt yapı sağlamasının da ayrı bir kritik öneme sahip olduğunun altını çizmemiz gerekir. Yurtiçinde yeni mühendislerin istihdamı ile ulusal siber güvenlik bilgi birikimi artırılıyor. Bu ürünlerin uluslararası pazarlarda başarı elde etmesiyle elde edilen gelirler, toplam yazılım ihracatımıza ve ülke ekonomimize de katkı sağlayacaktır.

4.5G/LTE telekom altyapısının hayatımıza girmesiyle birlikte, VoIP sistemlerde karşılaştığımız güvenlik riskleri ve siber saldırılar giderek arttı. Yeni yöntemlerle verilen zararın kritik seviyelere ulaştığını görüyoruz. Özellikle birçok hizmet ve servisten oluşan VoIP ortamlarında, dolandırıcılık faaliyetlerinin şirketlerin ciddi maddi zararlara uğramasına ve itibar kaybetmesine neden olduğunu gözlemliyoruz.

Bu alandaki güvenlik ihtiyacına yönelik olarak geliştirmiş olduğumuz NOVA V-SPY aracımız ile yeni nesil



telekomünikasyon sistemlerinin açıklarını tespit ediyoruz. NOVA V-GATE uygulama seviyesi güvenlik duvarımız ile ise VoIP protokol ataklarını ve dolandırıcılık faaliyetlerini oluşmadan önleme, operasyonel yönetim ve sistemi izleme özellikleri sunuyoruz. NOVA FMS adlı büyük veri güvenlik analitik platformumuz, VoIP ve 4.5G yeni nesil iletişim ortamlarında gerçekleşen dolandırıcılık faaliyetlerini, makine öğrenme destekli davranış analizi yöntemleriyle gerçek zamana yakın sürelerde tespit ediyor ve aksiyon alması için bütünlüklü çalışan NOVA V-GATE uygulamasına anlık olarak şüpheli durumları bildiriyor.

Netaş ArGe'sinde geliştirdiğimiz NOVA S/COM ürünü, akıllı telefonlarda sesli ve görüntülü konuşmayı, mesajlaşmayı, dosya transferini ve beyaz tahta ile karşılıklı çizimi yüksek güvenli bir ortamda gerçekleşmesini sağlayan Android ve iPhone için geliştirilmiş mobil güvenli bir iletişim uygulaması. Ayrıca Avrupa Birliği projeleri ile yurt dışı konsorsiyumlarda nesnelerin interneti güvenliği ve finans alanında blok zincir, güvenlik konularında işbirliği çalışmalarımızla siber güvenlik alanındaki ArGe faaliyetlerimizi genişletiyoruz.

Kurumların Önündeki Başlıca Zorluklar

Türkiye’de yöneticiler geçerli güvenlik sorunlarını çözmek ve gelecekte olabilecek tehditler için planlama yapmak arasında hassas bir denge kurmak zorundadır. Sadece güvenlik riskleri için mantıklı düşünmekle kalmayıp aynı zamanda yüksek öncelikli girişimler için de bütçe tahsis etmeleri gerekir.

Şekil 7

2019’da Türkiye’nin İş Öncelikleri

S: Aşağıdakilerden hangisi 2019’da kuruluşunuz için çok önemli iş öncelikleri arasındadır?



Note: n = 619

Kaynak: IDC Türkiye CIO anketleri, 2018–2019 (n = 619)

Türkiye’de güvenlik yöneticileri siber güvenlik olayları ile ilgili bilgilere erişmede zorluk yaşamaktadır. KVKK uyarınca yerel işletmeler siber saldırılar hakkında bilgi yayınlamak zorunda olmakla beraber bugüne kadar paylaşılmış olan raporlar detaydan ve derinlikten uzaktır. Bilginin siber güvenlik alanında ne kadar değerli olduğu düşünülürse, saldırıların ve alınan karşı tedbirlerin detayları ulusal güvenlik için hayati önem taşıyan ve risk altında olan kurumların korunması için çok önemlidir.

Üstel olarak artan miktarlardaki verinin yönetilmesi orta vadede karmaşık bir sorun haline gelecektir. Örneğin, IoT sensörlerden (örneğin akıllı sayaçlar, hava istasyonu sensörleri, bağlantılı arabalar, ambar okuyucular ve üretim hattı vericileri) gelen ve giderek artan miktardaki veriler artık gerçek zamanlı olarak üretilebiliyor; ancak, bu verilere erişmek ve bunları analiz etmek için yeni platformlar ve yeni veri koruma teknikleri gerekiyor. Dolayısıyla güvenlik yöneticilerinin KVKK

hükümlerini sağlayabilmek ve kendi kuruluşlarına ait gelişen strateji ve planları barındırabilmek için veri güvenliği ve gizlilik platformlarına yatırım yapması gerek.

Türkiye’deki 2019 IDC Güvenlik Roadshow sırasında yapılan bir ankete göre, güvenlik müdürlerinin %60’ı bütçe kesintilerinin güvenlik yatırımları önündeki en büyük engel olduğunu belirtti. Aynı ankette, güvenlik personelinin %42’si rutin işlerle çok meşgul oldukları için kırılganlıkları yeterince analiz edemediklerine veya gerekli düzeltici tedbirleri alamadıklarına değindiler. Güvenlik becerilerine sahip personelin kıtlığı sebebiyle siber güvenlik uzmanlarının maaşları da artmakta ve kalifiye adaylara yüksek ücret ödemek istemeyen firmaların bünyesinde bir yetenek boşluğu doğmaktadır. Güvenlik uzmanlarının bu yetersizliği aynı zamanda işletmeleri yönetilen güvenlik hizmeti sağlayıcılara doğru itmektedir.

Araştırmalar şifre avcılığı, “spearphishing” ve “whaling” saldırılarının kurumsal sistemlere erişim sağlamada ve siber saldırı atılımlarını gerçekleştirmede en çok kullanılan yöntemler arasında olduğunu gösterdi. Aslında, güvenlik savunması çalıntı kimlik bilgileriyle büyük oranda etkisizleştirilebilir; bu anlamda, işgücü ilk savunma hattıdır. Ancak, güvenliğe duyarlı bir kültürü yukarıdan aşağı tüm şirket çapında uygulayıp sürdürmekte firmalar hala güçlük çekmektedir.

Yönetim güvenlik eğitimiyle ve en iyi uygulamaların yerleştirilmesiyle ilgilenmeli ve eğitimde etkinliği en üst düzeye çıkarma amaçlı, role dayalı bir faaliyet olmalıdır. Satıcılardan ve ortaklardan gelen uzman girdisi bu süreçte kritik önem

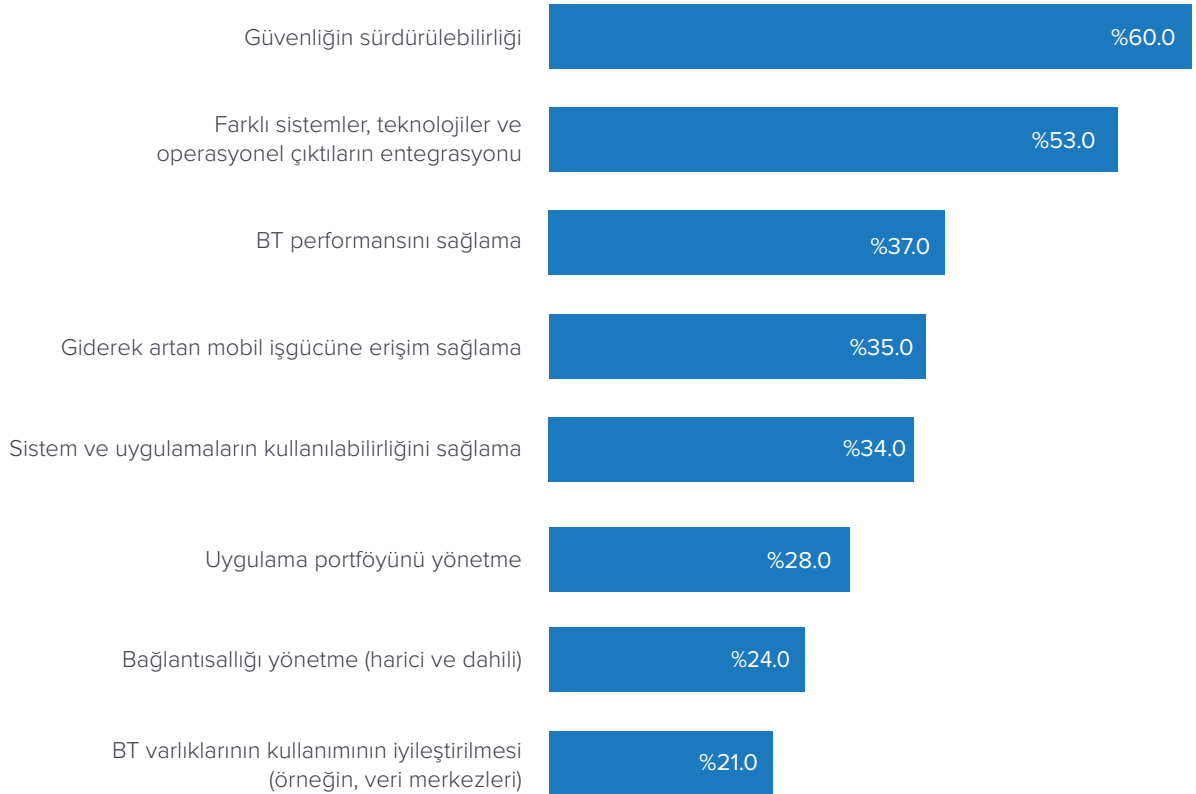
taşıyabilir, hatta bazı sağlayıcılar şifre avcılığı bilincini test eden ve iyileştiren araç ve hizmetler de sunabilir. Güvenlik personeline ihlallerin sonuçlarını çalışanlara gösterme fırsatı tanıyan uygulamalı alıştırmalar da salt PowerPoint ile verilen eğitimlerden daha kalıcı ve yararlı bir etki oluşturabilir.

2019 IDC Türkiye CIO Zirvesinde ankete katılan CIO'ların yaklaşık %60'ı teknoloji konusunda yaşadıkları en büyük güçlüklerden birinin güvenliği sürdürmek olduğunu belirtti. Bu nedenle güvenlik yöneticileri ve CIO'lar farklı seviyelerde (BT sistemi seviyesi, çalışanların seviyesi, vs.) güvenliğin sürdürülebilirliğini değerlendirmeli ve her seviyede gerekli tedbirlerin alındığından emin olmalı.

Şekil 8

Teknoloji ile ilgili Zorluklar

S. Teknoloji ile ilgili en büyük üç zorluk/öncelik sizce hangileridir?



Note: n = 99

Kaynak: IDC Türkiye, IDC CIO Zirvesi Türkiye 2019

Temel Tavsiyeler

IDC yönetilen güvenlik hizmetlerini “uzaktaki güvenlik işlemleri merkezleri (SOC) tarafından yerine getirilen BT güvenlik işlevlerinin gün boyunca saha personeli kanalıyla değil, uzaktan yönetimi ve izlenmesi” olarak tanımlar. IDC pazarı müşterinin yerinde yönetilen güvenlik hizmetleri (CPE MSS), yönetilen konakçı güvenlik hizmetleri (MSS’de yerleşik), ve bulutta yerleşik şirket güvenliği hizmetleri (bu IDC’nin bir hizmet olarak güvenliğe verdiği isimdir) olarak segmentlere ayırır.

Siber Güvenlik Stratejilerinizi DX Platformu Genelinde Uygulayın

İşletmeler alışılmış güvenlik stratejilerini kuruluşun DX ihtiyaçlarını karşılayacak şekilde genişletmelidir. Kurumlar riski yönetmek ve operasyonlarını korumak için ayrıca DX girişimleri paralelinde yeni siber güvenlik stratejileri de belirlemelidir. Şirketler güvenlik stratejilerinde ölçeklendirilebilirlik, hız, gizlilik ve güven ihtiyacı gibi konuları da dikkate almalıdır. Aslında, DX girişimlerinin benimsenmesi ve geliştirilmesi sırasında mevcut güvenlik programlarının güncellenip hizalanması şarttır.

Esaslı bir “Olaylara Müdahale Planı” Yapın

Kurumlar olaylara müdahale planlarında bir yaşam döngüsü yönetimi yaklaşımına yer vermeli ve gerektiğinde modası geçmiş prosedürleri iptal etmelidir. Tehdidin izlenmesi, sınırlandırılması, düzeltilmesi ve adli bilişim kuruluşların kendi olay ve müdahale stratejilerine dahil ederek düzenli olarak güncellemesi gereken alanlardır. İşletmelerde ayrıca açıkça tanımlanmış ve belgelenmiş bir iletişim ve yönetime taşıma planı olmalı ve bu da düzenli olarak test edilip gözden geçirilmelidir. Bu yeni güvenlik mimarileri ve değişen güvenlik modelleri (örneğin dağıtık bütünlük modeli) paralelinde gelişmelidir.

Proaktif bir Güvenlik Yaklaşımı Benimseyin

Tehditlerin değişken niteliğinin üzerine gidebilmek için güvenlik kontrolleri yapılmalıdır. Bu değişiklikleri kolaylaştırmak için, kuruluşlar alışılmış, reaktif güvenlik modellerinden daha proaktif yaklaşımlara geçiş yapmalıdır. Günümüzde, saldırı metotlarının hızla evrimleşmesi nedeniyle şirketler derinlemesine savunma metotları benimsemek ve olası alışılmadık siber saldırılara karşı koruma sağlayan sıkı kontroller uygulamak zorunda kalmaktadır.

Güvenlik Uzmanlarınızı Sürekli Olarak Eğitin

Siber güvenlik alanı geliştikçe bilgi güvenliği uzmanları da bilgi ve becerilerini sürekli güncelleyebilmelidir. Bu nedenle

siber güvenlik uzmanlarının yeni mimarilerden, güvenlik yaklaşımlarından ve AI, makine öğrenimi ve otomasyon gibi teknolojilerden haberdar olmasını sağlayan esaslı geliştirme programları hayata geçirilmelidir. Örneğin, siber güvenlik personeli tehdit istihbaratı hizmet sağlayıcılarının ve satıcılarının hazırladığı raporları okumalıdır çünkü bu raporlarda modern saldırganların kullandığı araçlar ve tekniklerin yanı sıra, onları güdüleyen şeyler hakkında da derinlemesine bilgi verilmektedir.

Tehdit Avcılığı Becerilerinizi Geliştirin

Kuruluşlar sistemlerinin tehlike altında olup olmadığını anlamak için organize ve sistematik bir tehdit avcılığı metodu uygulamalıdır. Örneğin, analitik teknolojileri kullanılarak şüpheli faaliyet işaretleri takip edilebilir ve tehdit avcılığı süreçleri kapsamında araştırmalar yapılabilir. Kuruluşlar tehdit istihbaratı faaliyetlerini desteklerken aynı zamanda kendi tehdit avlama becerilerini de geliştirmelidir.

Yönetilen Güvenlik Hizmeti AR&GE Yol Haritanızı Değerlendirin

İleriye dönük yönetilen güvenlik hizmeti sağlayıcıları gelişmiş tespit teknikleri, tehdit istihbaratı, AI, ML, ve Büyük Veri Analitiği gibi şeyleri içeren hizmetler sunmalıdır; ayrıca bulut evrimini ve olaylara müdahaleyi de hizmete dahil etmelidir. Ancak, son kullanıcı şirketler hizmet sağlayıcıların yol haritalarını değerlendirerek DX için gereken güvenliği sağlayıp sağlayamayacaklarını belirlemelidir. İlave olarak, son kullanıcı şirketler yönetilen güvenlik hizmetlerinin sunduğu düşük işletme maliyetleri ve dağıtık konumların merkezden daha iyi yönetilmesi gibi avantajlardan da yararlanmalıdır. Örneğin, kuruluşlar bulut hizmetlerini, yani kolayca konuşlandırılabilen ve kullanıcı dostu güvenlik yönetimiyle işletmenin maliyet verimliliğini arttıran hizmetleri benimsedikçe bulut izleme hizmetlerinin önemi de giderek artıyor. Uygulamalar buluta taşındıkça kimlik erişimi yönetimi de daha hayati önem kazanacak.

Geleceğe Bakış

DX'in temposu ve güvenlik ekosistemlerinin evrimi tahminlerden daha hızlı ilerliyor. DX'in en zorlu yönleri risk seviyelerinin belirlenmesi ve yeni girişimler için gerekli kontrollerin uygulanması. Çok fazla güvenlik tedbiri alınırsa genel masraflar ağır yük haline gelebilir ve yetersiz güvenlik de felaketle sonuçlanan güvenlik ihlallerine yol açabilir.

Siber saldırganlar yeni teknolojilere bayılır çünkü yenilikler çoğu zaman öngörülemeyen hassasiyetler barındırır. Örneğin, eskiden kalan ödeme sistemlerinde (işlemler anında gerçekleşmediği için) güvenlik personelinin saldırıyı fark etmek ve suçluları yakalamak için daha fazla zamanı vardır. Gerçek zamanlı ödeme sistemlerinde ise tersine siber suçlular parayı anında çalabilir; yeni sistemlerde finans kuruluşlarının da işlemleri tersine çevirmek için çok sınırlı süresi vardır. Bu nedenle yeni siber güvenlik metotları ve yaklaşımları gelişecektir. Biyometrik kimlik doğrulama metotları da giderek yaygınlaşacaktır, üstelik bu durum gerçek zamanlı ödeme sistemlerine bağlı olarak sadece finans sektöründe değil, aynı zamanda IoT hizmetlerinin yaygınlığı sayesinde üreticiler arasında da görülecektir.

Başka bir örnek olarak, uygulama programlama arayüzleri (API'ler) de kendilerine özgü güvenlik sorunları barındırır. API'ler üçüncü şahısların kurumsal ağlara girmesine ve hassas arka uç veri tabanlarına ve sunuculara erişmesine izin verir. API'ler uygun şekilde korunmazsa çeşitli saldırı türlerinde kullanılabilir. Blok zincirin merkezden dağıtılmış yapısı dijital işlemlerde artırılmış güvenlik ve şeffaflık sağlasa da, cryptojacking gibi yeni tehdit türleri DLT ile ilişkilidir. IDC'nin araştırmasına göre, Türkiye'deki kuruluşlar dijital alanda "yıkıcı" olarak tanımlanabilecek firmaların siber güvenlik alışkanlıklarını giderek daha çok benimsiyor. Dijital yıkıcı firmalar aşağıdaki özellikleri taşır:

İtici Güçtürler

Bu firmalar güvenlik stratejileri açısından öncüdür ve son derece karmaşık BT ortamlarının güvenliğini başarıyla temin ederler. Siber güvenlik risklerini ölçerler ve kayıpları tahmin ederler.

Sadedirler

Bu şirketlerin güvenlik yatırımları en uygun düzeydedir. Genellikle güvenlik çözümleri ve hizmetlerine duyulan ihtiyacın farkında olmakla beraber harcamalarda dikkatli davranırlar. Güvenlik stratejilerini optimize ederek kendi güvenlik harcamalarını da kolayca yönetirler.

En Az "Olay" Sayısına Sahiptirler

Bu şirketler kendi hassasiyetlerinin farkındadır ve bu boşlukları kapatacak şekilde hareket ederler. Bu lider kuruluşlar verimliliği ve etkinliği de göz önünde tutarak güvenlik programlarını düzenli aralıklarla gözden geçirip riski azaltırlar.

Güvenlikte Yeniliğe Açıkırlar

Bu tarz firmalar siber güvenlik alanında yenilik getirmenin ve otomasyon teknolojileri kullanmanın önemini farkındadır. Yeni teknolojilerin BT ortamlarında hızla yayılması nedeniyle bu şirketler de yeni teknikleri güvenlik programı yazılımcılarından daha hızlı şekilde kucaklar.

IDC Hakkında

International Data Corporation (IDC), bilgi teknolojileri, telekomünikasyon ve tüketici teknolojisi pazarları için pazar istihbaratı, danışmanlık hizmetleri ve etkinlikleri alanında küresel çapta bir hizmet sağlayıcıdır. IDC, BT profesyonellerinin, yöneticilerin ve yatırım topluluğunun teknoloji satın alımları ve iş stratejisi ile ilgili olarak gerçek veriler bazında karar almalarına yardımcı olur. 1100'den fazla IDC analisti 110'dan fazla ülkede teknoloji ve endüstri fırsatları ve trendleri hakkında küresel, bölgesel ve yerel uzmanlık sunmaktadır. 50 yılı aşkın bir süredir IDC, müşterilerinin kilit iş hedeflerini yakalamalarına yardımcı olacak stratejik içgörüler sunmaktadır. IDC, dünyanın önde gelen teknoloji, medya, araştırma ve etkinlik şirketi olan IDG'nin bağlı şirkettir.

IDC Türkiye

Zincirlikuyu Akademiler Sitesi, D Blok
34340 Beşiktaş – İstanbul, Turkey
+90 212 356-0282
<https://idc-community.com/>
www.idc.com



IDC Türkiye



IDC_Türkiye

Telif Hakkı Bilgilendirmesi

IDC Bilgi ve Verilerinin Şirket Dışında Yayınlanması - Herhangi bir reklam, basın bülteni ya da tanıtım materyalinde kullanılacak olan IDC'ye ait bilgiler için ilgili IDC başkan yardımcısından ya da ülke yöneticisinden yazılı izin alınmalıdır. Bu tarz bir talepte bulunulması durumunda bilginin kullanılacağı dokümanın taslak kopyası da sunulmalıdır. IDC, bu tarz bir kullanımı herhangi bir nedenle reddetme hakkını saklı tutmaktadır. Telif Hakkı 2018 IDC. İzinsiz çoğaltılması kesinlikle yasaktır.

Global Headquarters:

5 Speen Street Framingham, MA 01701 USA
P.508.872.8200
F.508.935.4015
WWW.IDC.COM