White Paper

Güvenlik Operasyonları Merkezleri: Doğru Modelin ve İş Ortağının Seçilmesi

Sponsor: Netaş
Jonathan Tullett , Eren Eser, Yeşim Araç
Ocak 2017

IDC GÖRÜŞÜ

Türkiye'deki kuruluşlar küresel ve bölgesel trendlere paralel olarak artan seviyede siber suç ile karşı karşıyalar. Ülkenin büyük kuruluşları bir yandan devam eden dijital dönüşüm girişimlerini yürütmeye çalışıp riskleri azaltmak için etkin stratejiler geliştirmeye çalışırken, güvenlik operasyon merkezleri (SOME) hem etkin güvenlik uygulamaları hem de risk yönetimi için odak noktaları haline gelmeye başladı. Dış kaynak SOME hizmetlerinin çekiciliği Türkiye'deki büyük kuruluşlar arasında popülerlik kazanırken yönetilen hizmet sağlayıcıları güvenlik pazarının en temel parçası haline gelmeye başladı.

Dünya çapında birçok ülke siber suç olaylarının sayısında bir artış olduğunu ifade ediyor; her bir olayın finansal etkisi ise küresel çapta daha fazla hissedilir hale geldi. Bir olayın maliyeti on binlerce dolardan milyon dolarlara (büyük bir ihlal durumunda) kadar değişebilirken birçok siber suç ya sümen altı ediliyor ya da ilk sızmadan çok sonralarına kadar mağdurlar tarafından fark edilemiyor. Her yıl yüz milyonlarca kişisel kayıt çalınırken, mağdurları kimlik hırsızlığı, dolandırıcılık olayları ve diğer siber suçlarla karşı karşıya bırakıyor.

Türkiye'de siber suçların finansal etkisinin gayri safi yurtiçi hasılanın (GSYH) %0.07[1]'sine denk geldiği tahmin ediliyor. Bu seviye şu andaki dünya ortalaması ile aynı görünse de bölgedeki yüksek tansiyon nedeniyle artmakta olduğu söylenebilir.

Türkiye'deki kuruluşlar, siber tehditlere karşı hassasiyetlerini artıran bir dizi faktörün bir araya geldiği bir ortamla karşı karşıyalar:

1. **Artan Küresel Siber Suç Oranları:** Dünya çapında insanlar dolandırıcılık, şantaj, endüstriyel casusluk ve terörizm dahil olmak üzere çok sayıda suçu işlemek için çevrimiçi dünyayı kullanıyor. Saldırıların göreceli olarak daha kolay gerçekleştirilebilmesi, çalınan ve şantaj ile elde edilen verilerin değerinin gün geçtikçe daha da artması ve düşük yakalanma riski, suç teşkilatlarını, siyasi aktivistleri ve fırsat kollayan suçluları çevrimiçi suçlara yönelme konusunda cesaretlendiriyor. Siber suçlar aynı zamanda oldukça karlı. Örneğin, CryptoLocker gibi şifreli ransomware (fidye yazılımları) Truva atları saldırganlara milyonlarca dolar kazandırıyor. Çalınan kimlikler de (giriş şifreleri, kredi kartı verileri, vb.) kayıt başına birkaç kuruştan başlayarak, çalıştığı teyit edilen hesaplar için 20 dolarlara kadaralıcı bulabiliyor (2014 yılında dünya çapında bir milyardan fazla kişisel kayıt çalındı[2]). Dağıtık-hizmet-engelleme (DDoS) botnet hizmetleri, müşterileri adına hedefli sistemlere zarar vermek için günlük birkaç yüz ila binlerce dolar arasında maliyet çıkarabiliyor. Bu tarz botnet hizmetlerini işleten kişiler devam etmekte olan DDoS saldırılarını durdurmak için de

[1] Center for Strategic & International Studies, 2014
[2] Gemalto Breach Level Index 2015

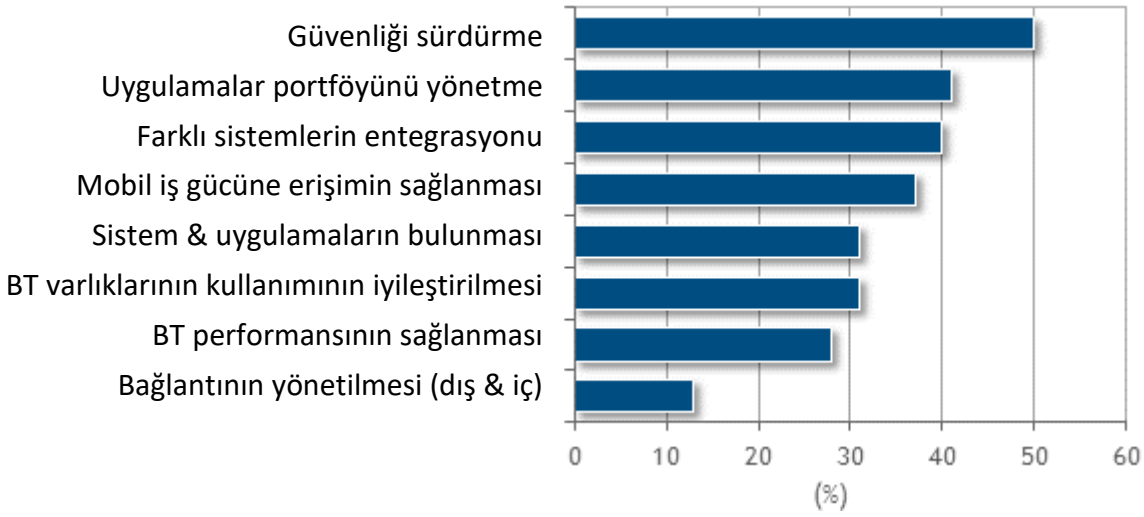
mağdurlardan büyük miktarlarda para talep edebiliyor. Bu nedenle siber suçların çok farklı şekillerde meydana geldiği ve çoğunun çok karlı ve bir o kadar da düşük riskli olduğu söylenebilir.

2. **Yurtiçi Siber Suçlar:** Türkiye, siber saldırı ve kötü amaçlı yazılımların (malware) kaynağı haline gelen bir ülke olma yolunda ilerliyor[3]. Yetenekleri dünyanın diğer kesimlerindeki siber suçlularla boy ölçüşebilecek tarzda olan yerel siber suçluların tabanı aktif bir şekilde genişlemeye devam ediyor. Bu suçlular, para ve diğer kaynaklara erişimi olan kişilere, Türkiye'de ve dünyanın diğer yerlerinde bulunan kuruluşlara karşı saldırılar düzenliyorlar.
3. **Siyasi Tansiyon:** Türkiye şu anda bir nevi siyasi huzursuzluk dönemi yaşıyor – ve elbette bunun kaçınılmaz siber suç sonuçları oluyor. Zira siber aktivistler ve yabancı güçler ülke üzerinde etki yaratmaya, devletin çeşitli organlarını işlevsiz hale getirmeye ya da her ne emelleri varsa o doğrultuda dikkat çekmeye çalışıyorlar. Bu belirsizlik de kuruluşlar ve devlet kurumları için yüksek riskli bir ortam yaratıyor.
4. **Bölgedeki İstikrarsızlık:** Ortadoğu ve Doğu Avrupa'daki çatışmalar da bölgedeki siber suç ve siber savaş faaliyetlerini teşvik ederken bu faaliyetlerden bazıları Türkiye gibi ülkelere sıçrayabiliyor.

Dolayısıyla da Türkiye'deki kuruluşlar BT operasyonlarını ve iş süreçlerini dönüştürmeye yönelik muazzam bir baskı altındalar.Genelde arka plana atılmış olan ve görece az bütçe ayrılan kurumsal BT güvenliği artık kırılma noktasına ulaştı. Daha da kötüsü, saldırganların ellerinde sofistike araçlar ve teknikler olduğu için avantajı ellerinde tutuyorlar. Saldıranlar aynı zamanda hedeflerini (ve onların hassas noktalarını) çok iyi tanıyorlar, yasadışı pazarlara erişimleri var (örneğin, çalınan veriler ve virüslü uç noktalara erişim gibi) ve uzun uzadıya keşif yapma imkânına sahipler. Buna karşın kurumları korumaya çalışan ekiplerin sürekli olarak değişen hassas noktalarla, yetenek eksikliğiyle, bütçe kesintileriyle ve kullanıcı ile yöneticiler tarafındaki farkındalık eksikliğiyle mücadele etmesi gerekiyor.

ŞEKİL 1

Güvenlik — CIO'ların Önündeki En Büyük Teknoloji Sorunu



Kaynak: IDC CIO Summit META 2016

[3] Symantec Internet Security Threat Report, 2016

Yönetilen güvenlik sağlayıcıları bu savunma eksikliklerinin büyük bir kısmını kapatıyor. İster bir projede isterse de devamlı olarak spesifik güvenlik disiplinlerinde güncel uzmanlık becerileri ile bir yandan masrafları azaltıp yetenek sorunlarının üstesinden gelme imkanı tanırken bir yandan da en iyi uygulamaları takip etmenin avantajını kullanabiliyorlar. Yönetilen güvenlik sağlayıcıları tarafından sunulan hizmetler bütün spektrumu kapsarken ağ cihazlarının yönetimini, penetrasyon testlerini, özel geliştirmeleri, operasyonel güvenlik yönetimini ve dış kaynak güvenlik operasyonları merkezlerini kapsıyor.

DURUMA GENEL BAKIŞ

Türkiye'nin Tehdit Ortamında Artan Düşmanlık

Yerel ve uluslararası tehdit aktörlerinin sayı olarak arttığı ve kapasite anlamında olgunlaştığı bir ortamda Türkiye'deki siber suçlar artışa geçti. Büyük kuruluşların özellikle risk altında olduğu bir gerçek – çünkü bu tarz kuruluşlar finansal ya da siyasi kesintiler yaratmak için ideal hedeftir. Son zamanlarda Türkiye'de ve diğer ülkelerde bir dizi yüksek profilli siber saldırı gerçekleşti. Örneğin, enerji tedarik tesislerine karşı yapılan en son siber saldırılar Ukrayna, İsrail ve Finlandiya'da başarılı bir şekilde kesintilere neden olurken Türkiye'de neredeyse aynı dönemde benzer saldırılardan nasibini aldı ancak o dönemde altyapıya karşı bazı siber saldırılar gerçekleşse de bu kesintilerin direkt olarak siber saldırılardan kaynaklandığı düşünülmüyor. Türkiye'deki bankalar da dünyanın diğer köşelerindeki finans kuruluşlarına karşı yapılan koordine saldırılara benzer şekilde siber saldırı sayısında bir artışla karşı karşıyalar. Siyasi amacı bulunan DDoS saldırıları artık rutin bir şekilde gigabit eşiğini geçiyor (yani, DDoS saldırılarının oluşturduğu trafik saniyede bir gigabit'i rahatça geçiyor) saldırganların elinde muazzam botnet'ler bulunuyor.

Türkiye, sayıları hızla artan aktif siber suç aktörlerine ve aynı zamanda çok sayıda enfekte sisteme ev sahipliği yapıyor. 2015 yılında ülke, siber suç saldırıların kaynağı olan ülkeler sıralamasında altıncı[4] sıradayken "bot"ların(koordine saldırılara bilmeyerek katılan enfekte sistemler) kaynağı ülkeler sıralamasında ise dördüncü sıradaydı. Bu rakamlar, Türkiye'nin saldırı kaynağı olarak 20. sırada, "bot" kaynağı olarak ise 13. sırada olduğu bir önceki yıla kıyasla çok keskin artışlar gösterdi. Dolayısıyla bu rakamlar ülkedeki siber suç faaliyetlerinin nasıl hızlandığını gözler önüne seriyor. Dahası, diğer saldırı türlerinde, özellikle de DDoS'da benzer bir yukarı trend göze çarpıyor – Akamai'ye göre 2015'in 4. çeyreğindeki dünya DDoS trafiğinin %22'si Türkiye kaynaklıydı[5].

Türkiye'deki kimlik hırsızlığı da küresel trendlere benzer şekilde keskin bir artış gösteriyor; on milyonlarca Türk vatandaşı kişisel bilgilerinin siber suç vasıtasıyla çalındığını bildirdi. Hatta ülke nüfusunun yarısının kişisel verilerini barındıran tek bir veri tabanının 2016 yılında Rus hacker'lar tarafından internete verildiği iddia edildi[6].

Türkiye'de Dijital Dönüşüme Başlayan Kuruluşlar

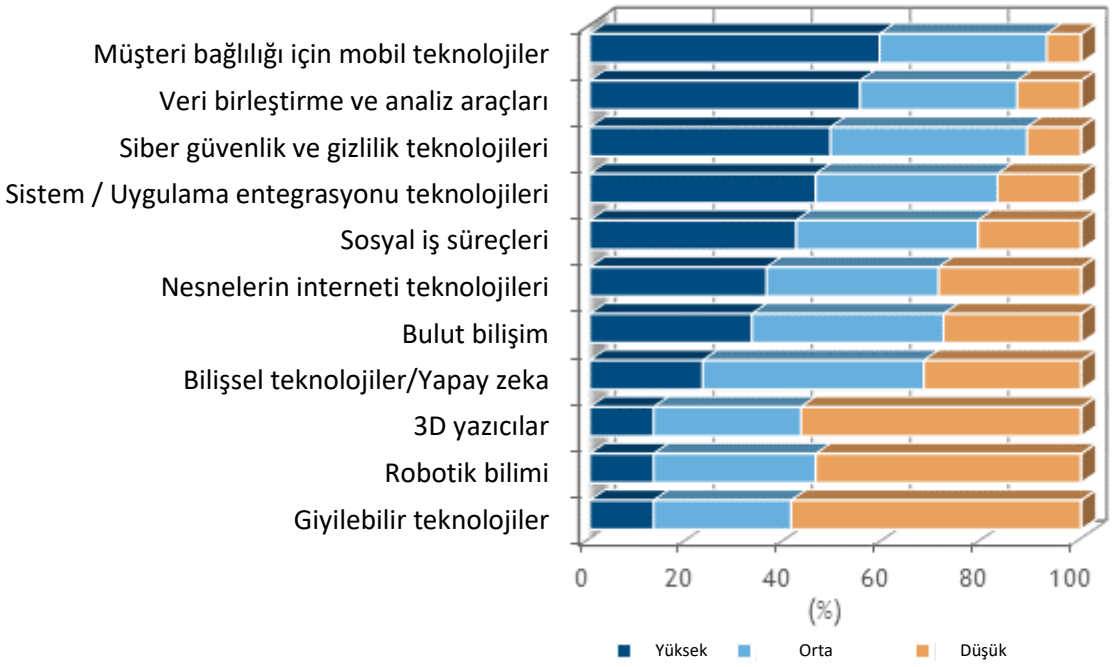
Türkiye'deki CIO'ların yaklaşık %69'u aktif bir şekilde resmi dijital dönüşüm girişimlerine başlamışlardır [7]. Silolar halinde yapılandırılmış dijital dönüşüm projelerinin başarısız olması büyük bir ihtimal olduğundan dolayı güvenliğin mutlaka bu sürecin bir parçası olması gerekiyor. Kuruluş içerisinde ya da dış kaynaktan alındıktan sonra SOME mutlaka iş operasyonlarına daha fazla değer

[4] Kaynak: Symantec Internet Security Threat Report 2016
[5] Akamai State of the Internet/Security Report, Q3 2016
[6] Kaynak: The Guardian, April 2016
[7] Kaynak: IDC CIO Summit META 2016

katmak üzere yapılandırılmalıdır. Aslında ülkedeki CIO'ların %89'u güvenliği yüksek ya da orta seviyeli öncelik olarak görüyor.

ŞEKİL 2

Dijital Dönüşümü Destekleyen Kilit Teknolojiler



Kaynak: IDC CIO Summit META 2016

Türkiye'deki siber tehditler, büyük kuruluşların artan karmaşıklığı ve tesadüfen de olsa BT operasyonlarının ortaya koyması beklenen ölçek ve hızı artıran dijital dönüşüme yönelik trend tarafından engelleniyor.

Maalesef Türkiye'deki siber suçlar da olgunlaştı ve dönüşüme uğradı. Artık büyük bir yer altı ekonomisi bu organize hackleme, dolandırıcılık ve çevrimiçi suçları destekliyor. Bunun sonucunda da en sofistike araçlar ve teknikler suçluların eline geçmiş bulunuyor. Bütün bunların karşılığında da kuruluşlar güvenlik kaynaklarını zamanında tespit edip hayata geçirerek fark yaratmaya çalışıyorlar.

Güvenlik yönetimi Türkiye'deki kuruluşların karşılaştığı en büyük zorluklar arasında yer almaktadır. TL/USD kurunu etkileyen ekonomik ve siyasi belirsizlikle birlikte BT bütçeleri genelde kısıtlı kalıyor. Güvenlik becerileri de kritik seviyede eksik. Uzmanlık ise bulut, mobil uygulamalar ve büyük veri gibi 3. Platform teknolojileri alanlarında ya çok pahalı ya da istense de bulunamıyor.

ŞEKİL 3

Kurum Güvenliğinde CIO Zorlukları

Kaynak: IDC CIO Summit META 2016

Etkin Bir Güvenlik Operasyonları Merkezinin Fonksiyonları

SOME, bütün kuruluş çapında bütüncül ve entegre bir sistem kurmalı ve politikalar, prosedürler ve uyumluluk için mükemmeliyet merkezi olarak hareket etmelidir. Bir SOME, aynı zamanda güvenlik operasyonları, yönetim ve tepki alanlarında birinci sınıf yeteneklere sahip kişilerce yönetilmelidir.

Dış kaynak SOME hizmetleri (bazen çok uluslu kuruluşlarda küresel SOME (KSOME) olarak da adlandırılır) büyük kuruluşların yüksek bilgi güvenliği standartlarını çok daha düşük maliyetle yakalamaları için etkili bir yöntem olabilir.

SOME'nin rolü kuruluşun olgunluğuna ve karmaşıklığına göre kuruluşlar arasında farklılık gösterebilir. Ancak, çoğu SOME aşağıdaki olanaklardan en az birkaçını sunmaktadır:

- **Güvenlik Olayı ve Olay Yönetimi (SIEM) ve Logların ve Alarm Verilerinin Merkezi olarak İzlenmesi:** SOME, ihlalleri tespit etmek ve, daha gelişmiş ortamlarda, davranışsal güvenlik analizleri için verileri analiz etmek ve ihlalleri bulmak için verileri birbirleriyle bağdaştırma kabiliyetine sahip olmalıdır.
- **Olaya Cevap Verme:** SOME, herhangi bir olay anında güvenlik kaynaklarının koordinasyonunda kilit rol oynar ve olay sonrasındaki incelemelere yardımcı olur.

- **Tehdit İstihbaratı:** SOME, riskleri daha etkin yönetebilmek için dışarıdaki istihbarat kaynaklarını entegre etme ve bunları kuruluşun altyapısına eşleştirme becerisine sahip olmalıdır.
- **Zaafiyet Yaşam Döngüsünün Yönetimi:** Bu özellik, penetrasyon testleri ve yazılım uygulama testlerini içeren sürekli test ve değerlendirme süreçleriyle birlikte kuruluş çapında zaafiyetlere dair bütüncül bir bakış açısı sunar.
- **Hizmet Dışı Bırakmanın Engellenmesi:** DDoS hiçbir zaman kaybolmayan bir tehdit olduğu için kesintilerden ve gelir kaybından kaçınabilmek için SOME'nin bu tarz saldırılara anında cevap verebilmesi gerekir.
- **Uç Nokta ve Cihaz Yönetimi ve Güvenliği:** Her geçen gün daha fazla şirket kendi-cihazını-getir (BYOD) modellerini uygulamaya koyduğu için şirket politikasının uygulanması da gittikçe zorlaşıyor. Uç noktasındaki cihazlarda güvenlik politikalarının durumsal farkındalığı ve tanımlanmış yüksek riskli davranışlar üzerinde harekete geçmek çok büyük bir önem taşıyor.
- **Ağ ve Çevre Güvenliği Politikası**: SOME, özellikle de büyük ve geniş coğrafyalara yayılan ağlara sahip kuruluşlarda güvenlik politikalarını entegre edebilmelidir. Bu politikalar aynı zamanda iş ortağı hizmetleri ve bulut platformları ile entegre edilmelidir.
- **Birleşik Kimlik ve Erişim Yönetimi:** Bu bütün kurum sistemlerini kapsamalıdır.
- **Uyumluluk ve Yönetişim Göstergelerinin İzlenmesi ve Raporlanması:** SOME, uyumluluk gözlemcisine dönüştü.
- **Felaket Kurtarma ve İş Devamlılığı Uygulamaları ile Yakın İşbirliği:** SOME'nin bu yönü test ve sürekli tekrar değerlendirmeyi kapsar.

Dış Kaynak SOME'nin Rolü

SOME işletmek genellikle kuruluşlar açısından maliyetli ve kaynak harcayıcıdır. İlk baştaki sermaye harcamaları arasında altyapı, yedek tesisler ve insan kaynakları (güvenlik uzmanları, vardiyalı çalışanlar ve yöneticiler dahil) harcamaları bulunur. Operasyonel masraflar da oldukça yüksektir – BT'nin bütün alanlarındaki eğitimi ve personel değişiklikleri gibi konular özellikle de güvenlik alanında çok zorludur. Danışmanlık ve entegrasyon, ek ve tekrar edici masraflar anlamına gelir; bir SOME'nin kabiliyetleri hem tehdit ortamı hem de şirketin değişen altyapısı ve stratejileri ile aynı doğrultuda olmalıdır.

SOME'nin dış kaynak hizmet olarak alınması yukarıdaki zorlukların büyük bir kısmını hafifletir. Eğer SOME şirket içerisinde kurulursa, belirtilen CAPEX harcamaları aynen kalacaktır; ancak operasyonel masraflar büyük oranda artacaktır. Tamamen dışarıdan alınan bir SOME ise bütün maliyet yapısını OPEX'e kaydıracaktır ve en belirgin masraflar danışmanlık ile mevcut altyapıya entegre olacaktır.

Ancak, dış kaynak bir SOME hizmetinin de kendine has zorlukları vardır ve bu nedenle kurumun SOME/KSOME'sini yönetmesi ve/veya sağlaması için iş ortağı seçerken dikkatlice düşünmesi gerekir. Güvenlik karmaşık bir alan olduğundan dolayı birçok kuruluş izleme, olaya tepki, penetrasyon testi gibi farklı yeteneklerinden dolayı birden fazla dış kaynak iş ortağı kullanmaktadır –. En üst seviyede çok iyi yönetilen bir güvenlik hizmetleri sağlayıcısı, kuruluşun stratejik ihtiyaçlarıyla birlikte alt yüklenicilerin faaliyetlerini çok iyi koordine edebilmelidir.

SOME uygulaması ya da yönetmesi için yönetilen bir güvenlik hizmetleri sağlayıcısı (MSSP) seçilirken aşağıdaki hususlar çok önemli olacaktır:

- **Kabiliyet**: Hizmet sağlayıcının becerileri ne kadar kapsamlı? Sağlayıcının personeli hangi profesyonel sertifikalara sahip? Kaç çalışanı var? Özellikle de mesai saatleri dışında kıdemli mühendislerin müşterilere oranı nedir? YGHS'deki personel havuzu şeffaf olmalıdır ki kapsam anlamında herhangi bir sıkıntı yaşanmasın.

- **Yerel Ofis ve Hizmet**: Bazı SOME özellikleri, uluslararası sınırların da ötesinde etkin bir şekilde yönetilebilir ancak bazı fonksiyonlar yerel kabiliyetler(örneğin entegrasyon, olaylara tepki, ve eğitim) gerektirir. Dolayısıyla da coğrafi erişim alanları ve felaket senaryoları düşünüldüğünde kuruluşların ihtiyaçlarının tam olarak tespit edilmesi büyük önem taşır. Bu ihtiyaçlar YGHS'nin kaynaklarına göre belirlenmelidir.
- **İlişkiler**: Hangi fonksiyonlar alt yükleniciye verilmelidir? Teknoloji sağlayıcılarının elindeki profesyonel sertifikalar ağ donanımları, işletim sistemleri ve uygumalar gibi alanlarda önemli olabilir.
- **Sertifikasyon ve Standartlar**: YGHS'ler hangi endüstri standartlarını sunar? ISO 27001 genellikle minimum standart olarak mutlaka bulunur ancak veri merkezi operasyonları, müşteri desteği ve finansal sistemlere uygunluk gibi diğer sertifikalar da faydalı olacaktır.
- **Esneklik**: Kurumsal BT hızla değişirken,güvenlik operasyonları inovasyonu engellemekten ziyade mümkün kılmalıdır. YGHS'ler bir kuruluşun dijital dönüşüm hedefleri ile stratejik bir şekilde hizalanmalı ve o kuruluşun sahip olduğu teknolojiyi kapsayabiliyor olmalıdır.

Yetenekli bir stratejik iş ortağının yardımıyla doğru bir şekilde hayata geçirilen yönetilen ya da dış kaynak SOME, ilgili kuruma şirket içi bir SOME'nin bütün faydalarını çok daha düşük bir risk ve maliyetle sahip olma imkanı verecektir.

Türkiye'deki kurumsal müşteriler, YGHS ve dış kaynak SOME fikrine yavaş yavaş ısınıyor ancak pazardaki hizmet olanaklarının derinliği hakkında hala şüpheler var. Uluslararası sağlayıcılar genelde çok uzak görülürken, yerel sağlayıcılar pazar farkındalığı eksikliği çekiyorlar. Ancak, referans alanları ve vaka çalışmaları ortaya çıktıkça benimsenme oranının hızlanması bekleniyor.

NETAŞ HAKKINDA

Netaş, bilgi ve iletişim teknolojilerinin (ICT) çeşitli alanlarında yenilikçi uçtan uca katma değerli sistemlerin entegrasyonu ve teknoloji hizmetlerini sunmaktadır. Şirket, 50 yıllık başarılı bir geçmişe sahiptir ve deneyimli 1. Kademe AR&GE merkeziyle BT alanında inovasyonlarına devam etmektedir. Netaş, Türkiye, Kuzey Afrika, CIS ve Asya-Pasifik'te Telekom operatörleri dahil olmak üzere kamu ve özel sektör için ICT danışmanlığından satış sonrası desteğe kadar geniş bir yelpazede mobil geniş bant, siber güvenlik, bulut bilişim, yönetilen ve stratejik hizmetler, GSM-R, ICT entegrasyonu ve yazılım geliştirme gibi alanlarda kapsamlı ve hedefe odaklı çözümler sunmaktadır.

Netaş: Türkiye'de Birinci Sınıf MSS Kabiliyetleri İnşa Etme

Netaş, Türkiye ve bölgedeki lider sistem entegratörlerinden bir tanesidir. Şirketin 2.000'den fazla çalışanı bulunmaktadır ve 50 yıllık başarılı bir geçmişe sahiptir. Netaş son dört yıldır güvenlik kabiliyetlerini artırmaya yatırım yapmaktadır. Çok sayıda tedarikçi ortaklığının yanı sıra Netaş, şirket içerisinde bir araştırma ve geliştirme tesisi kurarak VoIP iletişimlerini güvenceye alacak teknolojiyi geliştirdi.

Son zamanlarda şirket, yönetilen güvenlik alanında bazı kabiliyetler geliştirerek ağ operasyonları merkezi ile uzaktan ve yerinde güvenlik yönetim hizmetleri sunmaya başladı. Netaş, kapsamlı portföyünün parçası olarak büyük kuruluşlara güvenlik danışmanlığı ve SOME yönetim hizmetleri sunmaktadır. Netaş aynı zamanda güçlü hizmet-seviyesi anlaşmaları (SLA) ile desteklenen mevcut teknolojilerin karışımını içeren kuruma özel çözümlerle teknik uzmanlık sunmaktadır. Ayrıca, Türkiye'nin bütün şehirlerindeki varlığı ile Netaş ne kadar uzakta olursa olsun bütün müşterilerine saatler içerisinde ulaşabilmektedir.

Her geçen gün daha fazla siber tehditle karşılaşan Türk şirketler ve kuruluşlar ICT alt yapılarını ve veriyle bağlantılı güvenlik yatırımlarını artırmaktadır. Bugün, birçok kuruluş farklı güvenlik teknolojilerini entegre etse de güvenlik olaylarını izlemek ve tespit etmek hala büyük bir zorluk olarak karşılarında durmaktadır. Bütün kuruluşlar özellikle de günümüzün hızlı teknolojik değişimleri göz önünde bulundurulduğunda, güvenliğin etkin şekilde izlenmesi ve olaylara tepki verilmesi, pazardaki yetenek eksikliği, personelleri sürekli olarak eğitme ve elde tutma ve bütçe sıkıntılarıyla karşı karşıyadır.

Netaş Siber Operasyon Merkezi bütün bu ihtiyaçları karşılayacak ve müşterilerin güvenlikle ilgili personel yatırımlarını azaltacak şekilde yapılandırılmıştır. Netaş Siber Operasyon Merkezi 7 gün 24 saat çalışarak SOME gibi yerel düzenlemelere uygunluk göstermekte ve dünya çapındaki teknoloji liderlerinin ön plana çıkardığı bütünleşmiş deneyimle uluslararası en iyi uygulamalara uygun şekilde faaliyetlerini sürdürmektedir. Siber Operasyon Merkezi, yürürlükteki yasalara, regulasyonlara ve endüstri standartlarına uyumluluğundan emin olunması için denetlenmeye açıktır; Netaş Yönetilen Güvenlik Hizmetleri platformu gerekli bütün sertifikalara sahiptir.

Netaş Siber Operasyon Merkezi, milyonlarca tehdit alarmını analiz etmekte ve riskleri ve potansiyel zararları azaltmak için müdahalede bulunmaktadır.

.

TEMEL KILAVUZ

Türkiye'de artan siber suç riski düşünüldüğünde IDC, ülkede faaliyet gösteren büyük kuruluşlara aşağıdaki temel rehberliği sunmaktadır:

- **Tehdit Ortamına Öncülük Eden Kilit Trendler Hakkında Sürekli Bilgilendirme**: Siberle bağlantılı tehditlerin, özellikle de kurum içi tehditler, veri hırsızlığı, sosyal mühendislik dolandırıcılıkları (özellikle yönetim kurulu/üst yönetim seviyesinde) ve ilgili suçlar kurum güvenlik operasyonları tarafından yeterince ele alınmamaya devam ettiği sürece Türkiye'de ve dünyada artmaya devam etmesi bekleniyor. Bu nedenle büyük kuruluşların pazar kuvvetlerine tepki olarak güvenlik stratejilerini evrimleştirmesi gerekiyor.
- **SOME Kapasitelerinin Geliştirilmesi:** Büyük kuruluşlar öncelikle modern bir SOME kurmalı ve sürdürmelidir. SOME, güvenlikle ilgili en iyi uygulamaları kurmalı ve sürdürmeli ve ayrıca ne kadar karmaşık olursa olsun ICT altyapısı boyunca tehditler, olay tepkileri, kimlik, erişim yönetimi ve yönetişim üzerinde tek tip bir bakış açısı sunmalıdır. SOME kapasitesi de bütün ve düzenli olarak test edilmelidir. Tehditlerin başarılı bir şekilde tespiti ve azaltılması için SOME'nin her bir temel yetkinliği test edilmeli ve gözden geçirilmelidir. Kuruluş çapında operasyonların/farkındalığın test edilmesinde dışarıdan penetrasyon testleri ve kırmızı/mavi takım tatbikatları yapılmalıdır. SOME, test sonuçlarının koordine edilmesi ve harekete geçilmesinde kilit rol oynayacaktır.
- **SOME'nin Dijital Dönüşümün Temeli Olarak Ön Plana Çıkarılması:** Büyük kuruluşlar, SOME'nin kabiliyetlerine yeni sistemlerin ya da her türlü altyapı değişikliğinin yansıtılmasını sağlamalıdır. Yeni teknoloji yatırımlarının değerlendirilmesi ve entegrasyonu (örneğin Nesnelerin İnterneti) önceliklendirilerek güvenlik uygulamaları güncel tutulmalı ve tehditlerin önlenmesine yönelik olarak bütün ilgili taraflar ellerinden gelenin en iyisini yapmalıdır. Buna ek olarak, yeni teknolojileri edinme kriterleri de güvenlik uygulamaları seviyesinde değerlendirilmelidir. SOME'nin belgelendirilmiş en iyi uygulamalarıyla kolayca entegre olabilme kabiliyetinden yoksun sistemler yüksek riskli olarak tanımlanmalıdır. Ayrıca, SOME'nin bileşenleri proaktif şekilde kurumun bütün BT altyapısında yeni teknolojilere entegre edilmelidir. Güvenlik uygunluğunun yeni teknolojilerin kullanımını engellememesi için de SOME'nin operasyonel fonksiyonları proaktif şekilde güncellenmelidir.
- **Stratejik Ortaklıkların Kurulması**: Güçlü ve olgunlaşmış şirket içi bilgi güvenliği olanakları bulunmayan kuruluşlar, SOME'nin işletilmesi dahil olmak üzere bazı kilit fonksiyonları tamamen ya da kısmen dışarıya vermeyi düşünmelidir. Ortakların seçimi, sektör sertifikasyonları ve standartlarına uygunluk, stratejik iş ayarlamaları ve yerel kaynakların, altyapının ve yeteneklerin mevcut olması konularına dayandırılması gerekir. Beklentilerin net bir şekilde anlaşılması için sağlam Hizmet Seviyesi Anlaşmaları (SLA) yapılmalı ve takip edilmelidir. SLA başarısızlıkları risk profilinin parçası olarak görülmeli ve güvenlik opeasyonlarının güvenlik ihlallerine karşı hazırlandıkları ve planlama yaptıkları gibi özenle dikkate alınmalıdır.

IDC Hakkında

International Data Corporation (IDC), bilgi teknolojileri, telekomünikasyon ve tüketici teknolojisi pazarlarına yönelik pazar istihbaratı, danışmanlık hizmetleri ve etkinliklerinde üst düzey bir küresel tedarikçi konumundadır. IDC, BT profesyonellerinin, yöneticilerin ve yatırım topluluklarının teknoloji satın alımlarını ve iş stratejilerini kanıtlara dayalı bir şekilde yapabilmelerini sağlamaktadır. 1.100'den fazla IDC analisti 110'dan fazla ülkede teknoloji ve endüstri fırsatları hakkında küresel, bölgesel ve yerel uzmanlık hizmetleri sunmaktadır. Son 50 yıldır IDC, müşterilerinin kilit iş hedeflerine ulaşabilmelerine yardımcı olmak için stratejik iç görüler sunmaktadır. IDC, dünyanın lider teknoloji medyası, araştırma ve etkinlik şirketi olan IDG'nin bağlı şirketidir.

IDC Türkiye

Nispetiye Mahallesi, Cahit Bayar Sokak
Zincirlikuyu Harp Akademileri Sitesi, D Blok Kat: 4 Daire: 74
34340 Beşiktaş – İstanbul, Türkiye
+90 212 356-0282
Twitter: @IDC
idc-community.com
www.idc.com

Telif Hakkı Bildirisi

Bu IDC araştırma dokümanı, yazılı araştırmalar, analist etkileşimleri, tele-brifingler ve konferanslar sunan IDC sürekli istihbarat hizmetinin bir parçası olarak yayınlanmıştır. IDC abonelik ve danışmanlık hizmetleri hakkında daha fazla bilgi için www.idc.com adresini ziyaret ediniz. IDC'nin dünya çapındaki ofislerinin listesine ulaşabilmek için www.idc.com/offices adresini ziyaret ediniz. IDC hizmeti satın almak ya da ek suret veya web hakları hakkında daha fazla bilgi için lütfen 800.343.4952 (dahili 7988) telefon numarası üzerinden IDC Yardım Hattı ile iletişime geçiniz ya da sales@idc.com adresine e-mail gönderiniz.

Copyright 2017 IDC. İzinsiz çoğaltılması yasaktır. Tüm hakları saklıdır.