CYBERWIZ | NETAS

Siber güvenliğe tek çatıda 360 derece yaklaşım

Pandemi ile birlikte artan dijitalleşmenin siber güvenlik alanındaki ihtiyaçları da artırdığını söyleyen Netaş Yönetilen Servisler ve Siber Güvenlik Servisleri Direktörü Baran Korukluoğlu, “55 siber güvenlik uzmanımız ve 360 derece bakış açısıyla tüm bu alanlardaki deneyim ve birikimimiz ile tek çatı altında bütünleşik bir Siber Güvenlik Hizmeti ile yanınızdayız. Finans, havacılık, enerji, perakende gibi kritik sektörlerde 33 markanın siber güvenlikteki iş ortağıyız” dedi.

Siber güvenlik ile ilgili tüm ürün ve kanalları Yönetilen Hizmetler çatısı altında tek elde toplayarak çevikliğini artıran Netaş’ın Yönetilen Servisler ve Siber Güvenlik Servisleri Direktörü Baran Korukluoğlu, “2019’da 400 milyona yakın bağlı çalışan sayısı var iken 2039’da 4.3 milyar insanın artık tamamen online çalışması, network’lere bağlı olması bekleniyor. Yapılan araştırmalara göre dünya ekonomisinin en az yüzde 60’ının 2022’ye kadar dijitalleşmesi bekleniyor. Bu kapsamda da 7.5 trilyon dolarlık bir yatırım yapılacağı öngörülüyor” dedi.

Pandemi dönemi ile birlikte dijital teknolojilerde farklı alan ve kategorilerin öne çıktığına değinen Korukluoğlu, “Örneğin sağlık, eğitim, e-ticaret ve lojistik gibi alanların önemi çok arttı. 2-3 yılda katedilecek yolları neredeyse 6 ay gibi bir sürede katetmiş olduk. Buralarda çok ciddi bir dönüşüm yaşandı. Bu dönüşüm çok hızlı olduğu için siber güvenlik biraz geri plana da itildi. Ama bundan sonra şunu görüyoruz, yapılan araştırmalarda siber güvenlik kaygıları neredeyse bütün şirketler için ilk 5’te yer alıyor. Bu yüzden de bu alanda çok ciddi aksiyonların alınacağını da bekliyoruz” diye konuştu.

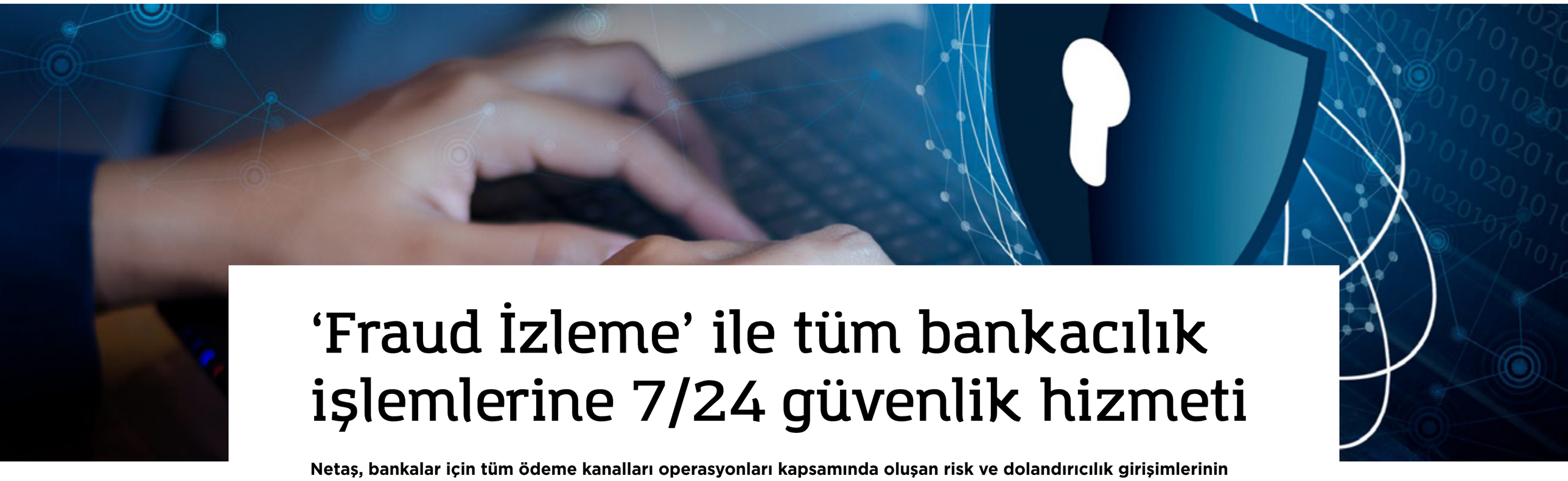
UÇTAN UCA SİBER GÜVENLİK YAPISI

Baran Korukluoğlu, şunları söyledi:
“Siber güvenlikte unutulmaması gereken bir nokta var, konu siber saldırı değil, bunun ne zaman olacağı. Bu da teknoloji ve insan kaynağının entegre olduğu bir süreç yönetimi gerektiriyor. Siber güvenlikte aslında 4 temel disiplin var: kimlik yönetimi, zaafiyet yönetimi, güven yönetimi, tehdit yönetimi. Bu 4 temel disiplinin 360 derece dediğimiz bir yaklaşımla, uçtan uca ve proaktif bir şekilde yönetilmesi gerekiyor. Siber güvenlik, insan, teknoloji ve süreç üçgenine oturtulduğunda, uçtan uca sağlıklı bir siber güvenlik yapısı kurmuş oluyorsunuz.”
Netaş olarak sahip oldukları siber güvenlik operasyon merkezinin Türkiye’nin en büyük operasyon merkezlerinden biri olduğun altını çizen Baran Korukluoğlu, “55 siber güvenlik uzmanımız ve 360 derece bakış açısıyla tüm bu alanlardaki deneyim ve birikimimiz ile tek çatı altında bütünleşik bir Siber Güvenlik Hizmeti ile yanınızdayız. Finans, havacılık, enerji, perakende gibi kritik sektörlerde 33 markanın siber güvenlikteki iş ortağıyız” dedi.

SİBER GÜVENLİKTE YENİLİKÇİ HİZMETLER

Korukluoğlu’nun verdiği bilgiye göre Netaş’ın siber güvenlik alanında, tek çatı altında 360 derece bakış açısı ve tüm katmanlardaki yetkinlik ve deneyimle bütünleşik olarak sunduğu yenilikçi hizmetler şöyle:

- Bankacılık ödeme kanallarındaki fraud risklerini izleyen ve cevap veren Fraud İzleme & Müdahale,
- Kurumların bütünsel risk yönetimi ve denetimini destekleyen Siber Güvenlik Risk İzleme ve Skorlama,
- Siber güvenlik risklerinin olası kayıp ve hasar durumuna karşı Siber Güvenlik Sigortalama,
- Para transferi kanallarında altyapı ve iletişim güvenliğini hedefleyen Swift CSP Danışmanlık Hizmetleri,
- Siber Tehdit İstihbaratı programımız sayesinde çok geniş kaynaklardan veri toplanması, analiz edilmesi, etkin ve proaktif korumanın sağlanması



‘Fraud İzleme’ ile tüm bankacılık işlemlerine 7/24 güvenlik hizmeti

Netaş, bankalar için tüm ödeme kanalları operasyonları kapsamında oluşan risk ve dolandırıcılık girişimlerinin izlenerek, en güvenli hizmet sunulması sağlayan Fraud Monitoring Hizmeti’ni kullanıma sundu.

Netaş, bankacılık ve finans sektöründe güvenliğe yönelik olarak geliştirdiği Fraud Monitoring Hizmeti’ni kullanıma açtı. FOC (Fraud Operations Center) çatısı altında verilmeye başlanan hizmet ile bankaların, fraud ve güvenlik birimi, yönetişim, analitik ve süreç iyileştirme faaliyetlerine destek verilerek, 7/24 gerçekleştirilen izleme ve müdahale süreçlerinde daha etkin olabilmeleri sağlanıyor.

Netaş’ın halihazırda SOC (Güvenlik Operasyon Merkezi) hizmetini kullanan finans kuruluşları, bankacılık operasyonlarına yönelik Netaş’ın bu yeni Fraud izleme ve cevap verme hizmetini de kullanmaya başladı. Bu sayede bankalar, hem gelecekte olası fraud güvenliği ve siber güvenlik ortak hareketi ve koordinasyonu gerektiren durumlar için, katma değerli bir hizmete sahip olurken, hem de mevcut fraud ekipleri üzerindeki yükü ve bankacılık risklerini azaltmanın önünü açmış oldu.

RİSKLERE KARŞI PROAKTİF SAVUNMA

Netaş Yönetilen Hizmetler ve Siber Güvenlik Çözümleri Kıdemli Müdürü Mehmet Fatih Yaldız, konuyla ilgili olarak şöyle konuştu:

“Netaş çatısı altında yürüttüğümüz Siber Güvenlik Operasyonları ve Hizmetleri kapsamında, müşterilerimizin atak yüzeylerini görünür hale getiriyor, sıkılaştırıyor ve 7/24 izleyerek proaktif ve reaktif yönde defans ve iyileştirmeler yaparak, çok farklı sektörlerde ve büyüklüklerde faaliyet gösteren müşterilerimizin bilgi varlıkları üzerindeki risklerin yönetilmesine önemli katkılar sağlıyoruz. Aynı zamanda bu hizmetleri müşterilerin bulundukları sektörlere, çekirdek iş uygulamalarına ve süreçlerine yönelik olarak da çeşitlendirmeye ve genişletmeye devam ediyoruz. Bu çerçevede, bankacılık ürün ve hizmetlerinin güvenli bir şekilde kullanımının gerçekleşmesini sağlamak adına, Kartlı Ödeme Sistemleri, Alternatif Dağıtım Kanalları ve finansal işlem yapılabilen diğer tüm kanallardan gerçekleştirilen işlemlerin risklerine odaklandık.”

BANKACILIKTA GÜVENLİK EN ÖNEMLİ BAŞLIK

Bankacılık ve finans sektöründe güvenliğin önemine dikkat çeken Yaldız, “Bankacılık sektöründe kullanılan Anti-Fraud izleme ürünleri, kartlı ödeme sistemleri paketi, üye işyeri fiziki ve sanal POS süreçleri, ana bankacılık sistemleri ve bankaların diğer sistemlerine sınırlı erişim yetkisi alınarak, güvenlik amaçlı kontrollerin yapılması ve buna ilişkin fraud istihbaratı ve analitiği platformlarının 7x24 izlenmesi ve tanımlanan müdahalelerin kurum prosedürlerine ve mevzuata uygun biçimde yapılmasını sağlayan bir hizmet oluşturduk” dedi.

NOVA S/COM ile güvenli olmayan ağlara ‘güvenlik’ garantisi katıyor

Günümüzde kötü niyetli saldırılar için havaalanları, alışveriş merkezleri ve kafeler gibi mekanlardaki açık internet ağları, önemli bir adres oldu. Netaş mühendisleri de güvenli olmayan açık ağlardaki iletişimin güvenliğini garanti altına almak için yüksek güvenlikli medya platformu NOVA S/COM’u geliştirdi.

Günlük hayatta mobil cihazların artan rolü ve internet altyapısına yapılan yatırımlarla birlikte, haberleşme güvenliği büyük önem kazandı. Bununla birlikte, havaalanları, kafeler ve alışveriş merkezleri gibi mekanlardaki açık internet ağları kötü niyetli saldırılara karşı büyük riskler barındırmaya devam ediyor. Bu risklere karşı Netaş, cihaz ve işletim sistemi bağımsız olarak, güvenli olmayan açık ağlarda dahi, hem istemciler arası hem de istemci-sunucu arasındaki iletişimin güvenliğini sağlayan yüksek güvenlikli medya platformu NOVA S/COM’u geliştirdi. Netaş Ar-Ge merkezinde geliştirilen Nova S/COM Sinyalleşme Sunucusu ile sesli ve görüntülü konuşma, mesajlaşma, dosya paylaşma vb. güvenli multimedya iletişimi sağlanıyor.

ŞİFRELİ İLETİŞİM

Netaş mühendisleri tarafından NOVA Siber Güvenlik Yönetimi Ürünleri şemsiyesi altında geliştirilen bir çözüm olan NOVA S/COM ile iletişim, şifreleme ve anahtar değişim algoritmaları kullanılarak şifreli hale getiriliyor.

Cihaz ve işletim sisteminden bağımsız olarak iletişimin güvenliğinin sağlandığı çözümde, ihtiyaca göre donanım veya yazılım tabanlı veri, ses ve görüntü şifreleme seçenekleri bulunuyor.

NOVA S/COM’UN ÖZELLİKLERİ NELER?

Güvenli iletişime ihtiyaç duyan telekom firmalarına, servis sağlayıcılarına, lojistikten, eğitime birçok sektöre; tüm kamu kurum ve kuruluşlarına uçtan uca güvenlik sunan NOVA S/COM’da öne çıkan özellikler şunlar:

- Ortadaki adam (man-in-the-middle), araya girme, dinleme gibi saldırılara karşı yüksek güvenlik sunuyor.
- Sistem, cihaz ve işletim sistemi bağımsız olarak, güvenli olmayan açık ağlarda dahi, hem istemciler arası hem de istemci-sunucu arasındaki iletişimin güvenliğini sağlıyor.
- İhtiyaca göre akıllı kartlar ile donanım tabanlı veya kartsız olarak yazılım tabanlı veri, ses ve görüntü şifreleme seçenekleri sunuyor. Bunun yanında, müşteri ihtiyaçlarına göre hukuki dinleme ve hiçbir şekilde dinlenemez modları da bulunuyor.
- Çağrı başlatmak, mesaj göndermek gibi tüm sinyalleşme işlemlerini gerçekleştiriyor. İki istemci arasındaki iletişim, AES256, Blowfish, TribleDES, Diffie-Hellman gibi şifreleme ve anahtar değişim algoritmaları kullanılarak şifreli hale getiriliyor ve tüm içerik sadece istemciler tarafından görüntülenebiliyor.
- Güvenli araç takip sistemi ve güvenli beyaz tahta uygulama özellikleri ile lojistikten, eğitime birçok sektöre güvenli bir ortam sağlıyor.

‘Kuantum’ ile teknolojiye bakış açısını kökten değiştirecek

Kurumların, hükümetlerin ve hatta bireylerin büyük problemlerinin çözümüne zemin sağlayacak kuantum bilgisayar ve hesaplama teknolojisiyle köklü bir dönüşüm yaşanması bekleniyor. Geleneksel siber güvenlik, yapay zekâ veya biyoinformatik alanların da bu dönüşüme hızla ayak uydurması şart. Bu köklü dönüşüme en hızlı uyum politikası ise siber güvenlik vizyonunda geleceğe ışık tutan iş ortaklarıyla çalışmaktan geçiyor.

Avuç içlerinde, masaüstlerinde, çantalarda ve büyük verilerin tutulduğu veri merkezlerinde elde edilen muazzam bilgi işlem hızına rağmen, geleneksel bilişim teknolojisinde sınıra ulaşıldı. Kişilerin ve kurumların sürekli artan teknoloji mimarisinin beraberinde kavramsal yeni problemleri de beraberinde getirdi. Tam bu noktada teknolojinin köklü dönüşümünün önderi kuantum hesaplama teknolojisi oldu. Bu köklü dönüşümün, kurumlara ve hükümetlere fayda sağlayacak olması ile beraber bireylerin hayatında da büyük problemlerin çözümüne zemin oluşturması bekleniyor.

KÖKLÜ DÖNÜŞÜME HIZLI AYAK UYDURMALI

Kuantum Bilgisayar & Hesaplama teknolojisi, bilgi teknolojileri alt yapısını köklü bir dönüşüme ittiği gibi, geleneksel siber güvenlik, yapay zekâ veya biyoinformatik alanların da bu dönüşümün hızına ayak uydurması gerekiyor. Bu köklü dönüşüme en hızlı uyum politikası ise siber güvenlik vizyonunda geleceğe ışık tutan iş ortaklarıyla çalışmaktan geçiyor.

Kuantum hesaplama teknolojisine, kurye ve restoran işletmesi kapsamında bir örnek veren Netaş Siber Güvenlik Hizmetleri Müdürü İsmail Orhan, kaynak kazanımı sağlamak ile beraber müşteri memnuniyetinin nasıl artırılabileceğini şu sözlerle aktardı:

“Günlük operasyonunda ürün teslimi hizmetleri veren bir firma düşünelim, hatta daha basite indirgeyelim ve bir pizza restorantını değerlendirelim. En düşük hacimli bir pizza restorantında bir kurye en az 10 teslimat yapmaktadır. 10 farklı teslimatın ulaşım kombinasyonu 3.628.800 adet farklı rota olasılığı anlamına gelmektedir. Günümüzdeki geleneksel teknolojinin düşük hacimli hesaplama yeteneği nevigasyonlarımızda 3 veya 4 rota belirleyebilir. Quantum hesaplaması 3.628.800 olasılık arasından kuryenin en hızlı teslimat rotasını çizebilecektir. Yeşil ışıklar, bekleme süreleri, hava koşulları, zemin türü vb. binlerce farklı olasılığı tek bir fonksiyon altında hesaplayıp en uygun değeri verebilecektir.”

SİBER GÜVENLİK RİSKLERİ DE ARTACAK

Bu dönüşüm ile milli güvenlik seviyesine kadar büyük risklerin de söz konusu olabileceğine dikkat çeken uzmanlar, şu değerlendirmeyi yapıyor:

“Klasik bir bilgisayarın belirli bir 56 bitlik şifrelemeyi kırması bir gün sürerse, kuantum bilgisayarları için yalnızca 0.322 milisaniye yani göz kırpma hızının binde birini alır. Peki bu anlama gelmektedir? Gizlilik dereceli hükümet verileri, silahlı kuvvetler bilgileri, milli Ar-Ge çalışmaları, milli istihbarat verileri veya kişisel hassas verilerimiz, mesajlarımız, e-postalarımız, fotoğraflarımız bizler gözümüzü kırpmayı tamamlamadan erişilebilir hale gelecektir.”

2021'in siber güvenliğine 2020'nin trendleriyle hazırlanın

Salgının gölgesinde 2020'de siber güvenlikte neler yaşandı? 2021'de neler bekleniyor?

Covid-19 salgının hayatın tüm alanlarında etkisini hissettirdiği 2020 yılında, siber güvenlik alanında yaşanan tehditler de "salgın" kimliği ile öne çıktı. Covid-19 salgınına benzer olarak, "tehdit" bir alanda başlıyor ve daha sonra her yere yayılarak birçok şirketin karşısına çıkıyor. 2021 yılına ışık tutan, 2020 yılının siber güvenlik alanında öne çıkan tehdit trendlerine toplu bir bakış attık...

Dünyanın dört bir yanında ve farklı sektörlerde görülen küresel seviyedeki tehditlerin büyük çoğunluğunun bölgesel veya benzer bir çeşidi bulunuyor. Covid-19 salgınına benzer olarak tehdit bir alanda başlıyor ve daha sonra her yere yayılarak birçok şirketin karşısına çıkıyor. Kurumsal politikalara, uygulamalara ve verilen karşılığa bağlı olarak salgın oranında bölgesel farklılıklar görülüyor.

KÜRESEL OLAYLARIN YARATTIĞI FIRSATLARI DEĞERLENDİRİYORLAR

Geçmişte de siber suçluların haberlerde yer alan konuları sosyal mühendislik tuzakları olarak kullandığına şahit olduk. Ancak 2020'de bu konu yeni bir seviyeye taşındı. Oltalama saldırısı yapanlardan kendi planlarını oluşturan devlet destekli ekiplere, siber saldırganlar küresel salgından faydalanmanın birçok yolunu buldu. Bu yöntemler arasında kurumsal e-postaları ele geçirme planları, devlet destekli kampanyalar ve fidye yazılımı saldırıları yer alıyor. Saldırganlar, dünyanın her yerinde herkesi etkileyen pandemiyi dijital saldırı zeminini genişletmek için kullandı.

SALDIRILAR DAHA KİŞİSEL HALE GELİYOR

Uzaktan çalışanların sayısının artmasıyla şirket ağları neredeyse bir gün içinde gözle görülür derecede büyüdü. Siber saldırganlar da bunu bir fırsat olarak gördü. 2020'de tüketici seviyesinde yönlendiricilere ve IoT cihazlarına yönelik istismar denemeleri, saldırı engelleme sistemlerinin (IPS) karşılaştığı tehditlerin başında geldi. IoT ürünlerindeki yeni ve mevcut zafiyetleri hedefleyen siber saldırganların kullandığı Mirai ve Gh0st da tespit edilen botnet'lerin büyük çoğunluğunu oluşturarak listede ısrarlı bir şekilde yer almaya devam ediyor.

TARAYICILAR DA HEDEF ALINIYOR

Uzaktan çalışma yöntemine geçiş, saldırganlar için herhangi bir kuşkusu olmayan bireyleri birçok yolla hedef almalarını sağlayan yeni fırsatları beraberinde getirdi. Oltalama saldırılarında ve diğer dolandırıcılıklarda kullanılan web tabanlı zararlı yazılım, önceki aylarda geleneksel e-posta saldırılarını da geride bıraktı. Ayrıca web tabanlı oltalama tuzaklarına ve dolandırıcılık araçlarına sahip olan bir zararlı yazılım ailesi ocak ve şubat aylarında ilk sırada yer alırken haziran ayında ilk 5 tehditten birisi oldu. Bu yükseliş, siber suçluların en savunmasız ve kandırılabilir olduğu an olan evinin internetini kullanarak tarayıcıda siteleri gezdiği sırada bireyleri hedef almaya çalıştığını gösteriyor olabilir.

FİDYE YAZILIMLARI HALA ETRAFIMIZDA

Fidye yazılımları gibi iyi bilinen tehditler, hala yerini koruyor. Covid-19 temalı mesajlar ve eklentiler, farklı fidye yazılımı saldırılarında tuzak olarak kullanıldı. Başka bir fidye yazılımının ise veriyi şifrelemeden önce bilgisayarın

ana önyükleme kaydını (Master Boot Record, MBT) yeniden yazdığı keşfedildi. Ek olarak, şirketin verilerini şifrelemenin yanında çalıp kullanıcıyı ifşa etmekle tehdit ederek fidye ödemesi almak isteyen fidye yazılımı saldırılarında da artış gözlendi. Bu trend, gelecekte gerçekleşebilecek fidye yazılımı saldırılarında şirketlerin paha biçilemez bilgilerini veya diğer hassas verilerini kaybetme riskini büyük ölçüde artırıyor. Tüm dünyaya bakıldığında sektörlerin tamamı fidye yazılımı saldırısına uğruyor. Ancak veriler detaylıca incelendiğinde en çok etkilenen 5 sektör telko, yönetilen güvenlik hizmeti sağlayıcılığı (MSSP), eğitim, kamu ve teknoloji olarak sıralanıyor.

STUXNET SONRASI OT TEHDİTLERİ

2020 yılında operasyonel teknolojilere yönelik tehditlerin ve güvenliğin gelişmesinde önemli rol oynayan Stuxnet'in 10. yılı geride kaldı. Yıllar sonra OT ağları hala siber saldırganlar için bir hedef olmaya devam ediyor. Bu yılın geçmiş aylarında görülen EKANS fidye yazılımı, saldırganların fidye yazılımı saldırılarının odağını OT ortamlarını da kapsayacak şekilde genişletmeye devam ettiğini gösteriyor.

İSTİSMAR TRENDLERİNİ HARİTALAMAK

CVE List'in yaptığı bir özet, yayınlanmış zafiyetlerin sayısının geçmiş birkaç yılda arttığını gösteriyor ve yamaların önceliği hakkında önemli tartışmaları da beraberinde getiriyor. Her ne kadar 2020'de yayınlanan zafiyet sayısı artacak gibi görünse de bu yıl bulunan açıklar aynı zamanda CVE List'in son 20 yılda kaydettiği tüm zafiyetler arasında istismar edilme derecesi en düşük olanlar arasında yer alıyor. 2018'de bulunan zafiyetler de yüzde 65 ile en çok istismar edilen zafiyetler olarak yer alıyor. Aynı zamanda şirketlerin yüzde 25'inden fazlası 15 yıllık CVE'lerin istismar edilmeye çalışıldığını kaydetti.

Servis sağlayıcılar uçtan uca güvenlik için tetikte

Dijital dünyada siber saldırılar hız kesmeden devam ediyor. Dünyadaki şirketlerin yüzde 31'i günde en az 1 kez saldırıya uğruyor. Peki servis sağlayıcılar müşterilerini güvende tutmak için ne yapıyor?

Birçok güvenlik şirketi ve servis sağlayıcı salgın döneminde müşterilerine daha üstün bir koruma sağlamak için yoğun bir şekilde çalışıyor. Şirketler özellikle; yedekleme, felaket kurtarma, yeni nesil kötü amaçlı yazılım önleme, siber güvenlik ve uç nokta yönetimi araçlarını tek bir çözümde birleştirmeye gayret gösteriyor. Buradaki tek amaç ise müşterilerin ya da kullanıcıların siber güvenliğini sağlama karmaşıklığını ortadan kaldırmak ve veri kurtarma altyapısını iyileştirerek daha fazla üretkenlik sağlamak olarak özetleniyor.

Salgın döneminde işletmelerin verilerini ve altyapılarını yeni uzaktan çalışma ortamının risklerine karşı korumakta zorlandıkları yadsınamaz bir gerçek. Devam eden Covid-19 salgınının ardından 3.400 küresel şirketi ve uzaktan çalışanı üzerine yapılan bir araştırmaya katılan şirketlerin yüzde 92'sinin işyeri dahil uzaktan çalışmayı mümkün kılmak için işbirliği araçları, gizlilik çözümleri ve uç nokta siber güvenlik gibi yeni teknolojileri benimsediklerini ortaya koyuyor.

KURULUŞLAR İÇİN ZORLU ALANLAR

Kuruluşlar için zorluk, şirket ağı ve tüm bu yeni cihazlarda farklı çözümlerden oluşan bir yığın kullanarak verilerin korunmasını yönetmenin pahalı, zaman alıcı ve karmaşık olması olarak öne çıkıyor. Entegrasyon eksikliği de işletmelerin siber suçluların istismar ettiği savunma sistemlerinde boşluklar yaratıyor. Araştırma, bilgisayar korsanlarının uzaktaki çalışanları hedef aldığından, kimlik avı, dağıtılmış hizmet reddi (DDoS) ve video konferans saldırılarının en yaygın kullanılan taktikler olduğunu ortaya koyuyor.

3 ÖNEMLİ TREND

Servis sağlayıcıların odaklanması gerekenleri şu şekilde özetlemek mümkün:

- Çalışanlar Zoom, Cisco Webex ve Microsoft Teams gibi uygulamalara güvenirken, şirketlerin yüzde 39'u son üç ayda bir video konferans saldırısı yaşadı. Cisco kısa süre önce Webex uygulamasında, saldırganların potansiyel olarak değerli veya zarar verici içeriği açmasına, okumasına ve çalmasına izin verebilecek bir güvenlik açığını ortaya çıkardı.
- Fidye yazılımı gibi kötü amaçlı yazılım saldırıları, salgın sırasında da artış gösterdi. Şirketlerin yüzde 31'i günlük siber saldırıları bildirirken yarısı da (yüzde 50), haftada en az bir kez hedef alınıyor. Temmuz ayında önde gelen bir GPS teknolojisi üreticisinin WastedLocker fidye yazılımı saldırısında 10 milyon dolar ödediği iddia edildi.
- Kimlik avı saldırıları tarihi düzeylerde gerçekleşiyor ve bu şaşırtıcı değil. Çünkü şirketlerin yalnızca yüzde 2'sinin bir siber güvenlik çözümünü değerlendirirken URL filtrelemeyi düşündüğü de görülüyor. Bu denetim, uzaktaki çalışanları kimlik avı sitelerine karşı savunmasız bırakıyor.

Netaş, Dijital Dönüşüm ve Siber Güvenlik Panelinde

ETKİNLİK

Netaş; Cisco Türkiye, UN Women, BinYaprak, Habitat ve TOG'un katkılarıyla genç kadınları siber güvenlik ile tanıştırmak amacıyla düzenlenen "Dijital Dönüşüm ve Siber Güvenlik" paneline katıldı.

Genç kadınları siber güvenlik ile tanıştırmak, temel eğitimler vermek ve onların bu alandaki işgücüne katılımına yardımcı olmak için başlatılan "Siber Güvenlik K-Atılımı" bir parçası olarak düzenlenen panelde, Netaş Yönetilen Servisler ve Siber Güvenlik Servisleri Direktörü Baran Korukluoğlu Netaş'ın siber güvenlik alanındaki tecrübelerini gençlerle paylaştı. Siber güvenlikteki yetkin insan kaynağı ihtiyacına değinen Korukluoğlu, "Yetkin insan kaynağı sektör için kanayan bir yara. Bu açığı yüksek teknoloji eğitim merkezimiz n-telligent institute ile kapatıyoruz. Burada uzmanlığımızla şirketler için siber güvenlik uzmanları yetiştiriyoruz" dedi.

'Yönetilen hizmetlere olan talep artıyor'

Netaş Yönetilen Hizmetler ve Siber Güvenlik Hizmetleri Çözüm Direktörü İsmail Kar, A Para'da "Teknoloji Çağı" programı Şafak Tükle Uysal'ın konuğu oldu. İsmail Kar, "Yönetilen hizmetlere olan talebin önümüzdeki dönemde yükseleceğini düşünüyoruz. Markets and Markets'ın çalışmasına göre de dünyada yönetilen servisler pazarı 2025 yılı itibarıyla 329.1 milyar dolarlık bir hacme ulaşacak. Bu hacim Covid-19 sonrası dünyada daha da hızlı artma potansiyeline sahip. Benzer dinamikler ülkemizde de görülüyor." dedi.
https://www.youtube.com/watch?v=D7cYKlbFjZY

Bilişim Zirvesi'nin gündemi 'Kuantum'

Bilişim Zirvesi'20, bilim çevrelerinde derin tartışmalara yol açan, ülkelerin rekabette yeni bir güç olarak hazırlıklarını sürdürdükleri, gelecek 30 yıla şekil verecek olan "Kuantum Teknolojisi"ni gündeme taşındı. İş, kamu, bilişim ve akademik dünya "Kuantum Yolculuğu" ana temasıyla etkinlikte bir araya geldi. Bilişim Zirvesi'nin Tema Sponsoru olan Netaş, zirvede 3 farklı konu ile yer aldı. Yönetilen Hizmetler Platformu oturumunda Yönetilen Servisler ve Siber Güvenlik Servisleri Direktörü Baran Korukluoğlu "Şirketlerin Dijital Dönüşüm Sürecinde Yönetilen Hizmetler" konusunda sunum gerçekleştirdi.

İşletmeler siber güvenlikte nelere dikkat etmeli?

Netaş Yönetilen Hizmetler ve Siber Güvenlik Hizmetleri Çözüm Direktörü İsmail Kar, Hürriyet Teknoloji Kutusu programında Selim Öztürk'ün konuğu oldu. Kar, ''İşletmeler siber güvenliği sağlamak için nelere dikkat etmeli?'' konusunda bilgilerini izleyicilerle paylaştı. **https://www.youtube.com/watch?v=Jiy5iYyWuWU**