AĞUSTOS 2021
plus
Redington

Akıllı Üretim Tesislerinde Siber Güvenlik

Trend Micro enerji sektörü gibi pek çok kritik sektördeki akıllı üretim tesislerinin omurgasını oluşturan, Endüstriyel Kontrol Sistemleri'ne (ICS) yönelik siber tehditleri, Bal Küpü (Honeypot) deneyi ile inceledi.

HASAN GÜLTEKİN
Trend Micro Türkiye Genel Müdürü

Üretim tesislerinde kurulan otomasyon sistemlerinin, standartlara uygun ve teknolojinin getirdiği avantajları müşteriye sunabilecek düzeyde olmasının yanı sıra, verimli ve kesintisiz şekilde işletilmesi de oldukça önemli. Akıllı üretim tesisleri, dijital bir tedarik zinciri oluşturmanın yanı sıra, insanların, ekipmanların ve süreçlerin üretkenliğini de artırmak için kuruluyor. Günümüzde önemi giderek artan Endüstriyel Kontrol Sistemleri (ICS), enerji tesislerinden sağlık sistemlerine, savunma sanayiinden üretim tesislerine pek çok kritik sektörün omurgasını oluşturuyor. Sektörde artan verimlilik talepleri, Endüstri 4.0 ve tüm dünyayı etkisi altına alan pandemi ile birlikte, Endüstriyel Kontrol Sistemleri alanında da dijital dönüşüm etkisini gösteriyor. Endüstriyel Kontrol Sistemlerinin zarar görmesi veya çalışamaz hale gelmesi,

ulusal ya da sektörel olarak büyük boyutlarda maddi ve manevi zarara sebep oluyor. Tam kapasite çalışan bir akıllı üretim tesisinde, üretim hattının kesintisiz bir şekilde çalışması için her bir işlemin başlangıçtan sonuna kadar dakik ve kesintisiz olarak devam etmesi gerekiyor.

TEHDİT AKTÖRLERİNE KARŞI SAVUNMADA KALMAK

Akıllı bir üretim tesisinin günlük işleyişinin sağlıklı bir şekilde sürdürülmesini sağlamak için ardındaki tehdit aktörlerini de her an göz önünde bulundurmak zorundayız. Maalesef bu tehditler, sadece ulusal düzeyde gerçekleşen ve kritik sonuçlar doğuran sofistike saldırılarda gündeme geliyor. Ancak şunu unutmamak gerekiyor ki tehdit aktörleri ulusal düzeydeki üretim tesislerinin yanı sıra daha küçük fabrika ve endüstriyel tesisler için de çok önemli riskler oluşturuyor. Bunun yanı sıra sofistike saldırılara kıyasla daha basit olan fidye ve kripto para madencilik yazılımları, diğer iş ortamlarını olduğu gibi Endüstriyel Kontrol Sistemleri ortamlarını da tehdit etme potansiyeline sahipler. Sonuç olarak Endüstriyel Kontrol Sistemleri'nde temel güvenlik çözümlerinin eksikliği, basit bir fidye veya kripto para madencilik yazılımı saldırılarına karşı bile üretim tesisini tamamen savunmasız bırakabiliyor. Bu tip saldırıların ciddi sonuçlar doğurabileceğini, üretim yapan her şirket sahibinin ve üst düzey yönetiminin bilmesi gerekiyor.

BAL KÜPÜ TUZAKLARI

Trend Micro Research, saldırı aktörlerinin bir üretim tesisini tehlikeye atmada ne denli etkili olabileceğini belirlemek ve Endüstriyel Kontrol Sistemi ortamlarını hedefleyen saldırıları daha iyi anlamak için 6 ay süren bir araştırma yürüttü. Araştırmada bal küpü (Honeypot) sistemi ile gerçek fabrika ortamı taklit edilerek, siber saldırganların tuzağa düşürülmesi sağlandı ve böylelikle saldırganların yaklaşımları incelendi. Oluşturulan bal küpünde, gerçek Endüstriyel Kontrol Sistemi donanımı, fabrikayı çalıştırmak için çeşitli programlanabilir mantık denetleyicileri (PLC), insan-makine arayüzleri (HMI), robotik ve mühendislik iş istasyonları ve bir dosya sunucusu içeren gerçek ana bilgisayar ile sanal makineler bulunuyordu. Yani saldırganları kendine çekecek gerçek bir sistem taklit edilirken, gerekli tüm bileşenler kullanıldı. Ardından bu sahte fabrika için bir kılıf şirket oluşturuldu. Gerçekçi bir şirket görünümü sağlamak için, çalışanların kapsamlı sosyal ağ profilleri yaratıldı, eksiksiz bir şirket web sitesi tasarlandı ve kritik sektörlerdeki büyük anonim kuruluşlardan oluşan bir müşteri tabanı oluşturularak, tam manasıyla bir danışmanlık şirketi yaratıldı. Böylece

bugüne kadarki en gerçekçi bal küpü kullanılarak, siber suçluları saldırılara sürükleyebilecek ve eylemlerinin direkt olarak incelenebileceği bir ortam oluşturulmuş oldu. Trend Micro Research ekibi bu sayede, siber saldırganları bal küpüne çekmeyi başardı. Zayıf güvenlik önlemleri, siber saldırganların sahte üretim tesisini potansiyel bir kazanç kapısı olarak görmesini sağladı. Böylece, günden güne daha fazla tehdit aktörü sisteme girdi. Yaratılan sahte üretim tesisinde, gerçek bir şirkette olabilecek pek çok güvenlik açığı bulunması nedeniyle saldırılar çoğunlukla başarılı oldu.

Bal küpü deneyi ile akıllı üretim tesislerini işleten kuruluşların ve Endüstriyel Kontrol Sistemi sorumlularının yeterli güvenlik önlemlerini almaları için neler yapmaları gerektiğini gösteren çok önemli bulgular elde edilmiş oldu. Araştırmanın sonucunda; açık bırakılan bağlantı noktası sayısının en aza indirilmesi ve erişim kontrol politikalarının sıkılaştırılması gerektiği net bir şekilde görüldü.

TREND MICRO YAKLAŞIMI

Trend Micro olarak olası tehditlere karşı "önleme", "tespit etme" ve "süreklilik" adımlarından oluşan bir yaklaşım öneriyoruz.

Üretim tesisindeki operasyonların kesintisiz devam edebilmesi için Endüstriyel Kontrol Sistemi'nin teknik ve operasyonel kısıtlamalarını karşılayan bir çözümün yanı sıra çok katmanlı bir BT güvenlik çözümünün de hayata geçirilmesi gerekiyor.

Onlarca yıldır faaliyet gösteren fabrikalarda, mevcut ağ yapısının veya varlıkların korunarak, dijitalleştirilmiş üretim sürecini güvenlik altına almaya yönelik araçların sağlanması da oldukça önemli.

Ayrıca, akıllı üretim tesislerinde uç noktalar ve bulut iş yükleri için, "Hizmet olarak Güvenlik (Security as a Service)" türü bulut çözümlerinin devreye alınması, fabrikaların sürekli değişen ortamına uyum sağlayacak, verimli ve güncel güvenlik yatırımlarının yapılması da gerekiyor.

Güvenlik operasyonlarının artan karmaşıklığına yardımcı olmak için tasarlanan Trend Micro çözümlerinin her biri, ağlar ve diğer ortamlardaki güvenlik olaylarını tespit etmek, analiz etmek ve müdahale etmek için tasarlanmış bir platform olan Trend Micro™ XDR ile bir sensör görevi de görüyor. Tüm bunlarla birlikte, saldırıların üretim tesisine zarar vermeden anında ortadan kaldırılması için tasarlanmış gelişmiş bir tespit analitiği kullanan Trend Micro™ Smart Protection Network™, dünyanın her yerinden tehdit verilerini sürekli olarak izliyor ve topluyor.

“Güvenlik Çözümlerimiz Tüm Kategorilerde Talep Görüyor”

Trend Micro Kanal Yöneticisi Mehmet Dağdevirentürk, pandemi sürecinde siber güvenliğe yönelik ihtiyaçlardaki değişimi değerlendirdi.

MEHMET DAĞDEVİRENTÜRK
Kanal Yöneticisi
Trend Micro

Trend Micro’nun her yıl siber güvenlik kapsamında önemli raporlar yayınladığını biliyoruz. Pandemi sürecinde de saldırılara dair raporlar yayınladınız. Sizin bu konudaki değerlendirmelerinizi alabilir miyiz?

MEHMET DAĞDEVİRENTÜRK: Pandemi süresince şirketlere en önemli saldırı kanallarından biri e-posta oldu. Üstelik çok farklı tekniklerle çok ciddi saldırılar gerçekleşti. Dört tane yeni hacker gurubu tespit ettik. Bunlar, son derece organize, arkalarında yüzlerce çalışanı olan, pazarlama müdürleri filan olan şirketleşmiş yapılar aslında.

Bunlardan bazılarının isimlerini verebilir misiniz?

MEHMET DAĞDEVİRENTÜRK: Lazarus, Tropic Trooper bunlardan ikisi örneğin. Başlarında bir CEO olan son derece profesyonel yönetilen şirketler. Pandemi süresinde hastanelere saldırıda bulunacak kadar da kötü niyetli olabiliyorlar. Tehditlerini yaparken istedikleri fidye üzerinden indirim teklif edebiliyorlar. Pazarlama stratejileri geliştirebiliyorlar. Komik gelebilir ama gerçek bunlar. Kişiye, kuruma özel kampanya yapabiliyorlar yani. Bunların özellikle bireysel olanları blöf yani spam oluyor ama insanları korkutabiliyor.

“Pandemi süresince, ağırlıklı olarak lojistik şirketleri, teknoloji şirketleri ve hükümetler hedef alındı. Özellikle buluta doğmuş online alışveriş ve lojistik şirketleri daha fazla siber saldırıya açık hale geliyorlar. Böyle saldırılar sonucu bir şirketin tahmini ortalama zararı 1.3 milyon doları buluyor.”

Bu şekilde paralarını kaptıran insanların hikayelerini duyabiliyoruz. Teknoloji okuryazarlığı arttıkça bu tip tehditler işe yaramıyor tabi. Kurumsal tarafta ise zaten işimiz çok kolay. Amaca uygun güvenlik araçları ile bu tip saldırılar engellenebiliyorlar.

Daha çok hangi kuruluşlar hedef alındı bu süreçte?

MEHMET DAĞDEVİRENTÜRK: Pandemi süresince, ağırlıklı olarak lojistik şirketleri, teknoloji şirketleri ve hükümetler hedef alındı. Bunun niye olduğu zaten çok açık. Bu sektörler kontrolü daha fazla eline almış olan, çok daha fazla işlem yapan sektörler. Ortada dönen finansal rakamlar da bu sektörlerde büyük bir artış gösterdi. Özellikle buluta doğmuş online alışveriş ve lojistik şirketleri daha fazla siber saldırıya açık hale geliyorlar. Böyle saldırılar sonucu bir şirketin tahmini ortalama zararı 1.3 milyon doları bulmuş durumda.

Sadece pandemi döneminde, büyük işletim sistemi ve altyapı üreticileri, bugüne kadar hiç yayınlamadıkları sayıda güvenlik açığı ve yaması yayınladılar.

Bireysel tarafta neler yapılabilir?

MEHMET DAĞDEVİRENTÜRK: Aslında son derece düşük maliyetlerle yapabileceğiniz çok şey var. Uluslararası siber güvenlik organizasyonları ve siber güvenlik üretici raporlarının çıktılarını takip ederek yüksek oranda kurumların güvenliğini artırması mümkün. Siber saldırı camiası iki kola ayrılıyor: Hacker’lar ve Lamer’lar. Hacker’lar, zararlı yazılımı tasarlayan kişilerden oluşuyor. Lamer’lar ise onların tasarladıklarını kullanarak saldırı yapan kişiler. Saldırı yapmak için hacker olmanıza falan gerek yok. Şu anda 50 dolar yatırım yaparak dünyanın en büyük siber saldırılarından bir tanesini gerçekleştirebilirsiniz. Bunun için hiçbir teknik bilgiye ihtiyacınız yok. Ransomware as a Service diye bir bulut hizmeti açıldı pandemi döneminde. Lamer’lar bu servisi fütursuzca kullandılar. Ransomeware as a Service, üç-dört yıllık bir hikâye. Siber saldırı yapıp karşılığında fidye isteyen Lamer’lar için özel bir servisin internetten para karşılığında satıldığını biz Trend Micro olarak, 3-4 yıl önce duyurmuştuk. Ransomware as a Service yazdığınızda karşılığını göreceksiniz. Üstelik bunun için “deep web” filan da gerekmiyor. Bildiğimiz yüzeydeki web ortamında veriliyor bu hizmet. Bir tane tuşa basıyorsunuz, “Saldırı nasıl olsun?” diye soruyor. İkinci tuşa basıyorsunuz, “Hangi ülke?” diyor. Üçüncü tuşa basıyorsunuz, “Sizin saldırı yapmak istediğiniz bir e-posta adresi listesi varsa ya da herhangi bir bilgi varsa

onu yükleyebilirsin ya da 10 dolar daha ver, Türkiye'ye ait 50 milyon e-posta adresi bende var, istersen onu da benden satın alabilirsin" diyor. Hatta belli bir şirket adı verip filtreleyebiliyorsun, o şirketten 1000 tane e-posta adresine saldırı yapabiliyorsun. Bu kadar detaylı ve odaklı bir mekanizma geliştirilmiş durumda. Ne yazık ki pandemi süresince de hacker olmaya gerek kalmadı, Lamer'lar çok kontrolsüz bir şekilde bu sistemleri kullanıp saldırılar yaptılar. Bu nedenle uzaktan çalışmayla da birlikte ev cihazlarının güvenliği çok önemli bir hale geldi.

Şirketlerde çalışırken bir güvenlik şemsiyesinin altındayız ama evlerde çalışırken korumamız kalmıyor, değil mi?

MEHMET DAĞDEVİRENTÜRK: Evet, çünkü şirketlerde bir firewall var, bir takım güvenlik sistemleri ve politikaları var. Evde kullandığınız bilgisayarı, telefonu şirketiniz verdiyse ve doğru politikaları kullanan bir şirketse, yine güvenlik altındasınız. Ancak işin içine kişisel internetinizi, kişisel bilgisayarınız ve telefonunuzu dahil ediyorsanız güvenlik açıkları ile baş başasınız demektir. Oysa artık, özellikle yeni çalışma şartları altında, evde de o koruma şemsiyesinin altında olmak durumundasınız.

Güvenlik çözümleriniz hakkında da biraz bilgi alabilir miyiz? Ve özellikle hangi alanlarda daha çok talep geldi çözümlerinize?

MEHMET DAĞDEVİRENTÜRK: Trend Micro'nun kurumsal olarak, "kullanıcı güvenliği", "ağ güvenliği" ve "sunucu güvenliği" olmak üzere üç farklı kategoride siber güvenlik çözümleri var. Bu kategoriler altında yaklaşık 55 farklı siber güvenlik çözümümüz mevcut. Pandemi süresinde bu üç kategoride de ve özellikle bulut güvenliği tarafında büyük bir talep artışı yaşadık. Çünkü pandemi, buluta geçişi de hızlandırdı.

"Önümüzdeki süreçte hibrit modele geçeceğimiz öngörülüyor. Bu çerçevede, şirketlerin çok net bir şekilde otomazisyona, yapay zekâya ve buluta yöneleceği net bir şekilde görülüyor. Trend Micro'nun çok güçlü bir yapay zekâ entegrasyonu ve bulut çözümleri var. Bu durum, pazarda önemli bir büyümeyi de vaat ediyor bizim için."

Şirketlerin genel taleplerini gördüğümüzde şunu da fark ettik: Özellikle regülasyona tabi olmayan, kamu kurumları ya da Cumhurbaşkanlığı regülasyonunun dışındaki kurumların genel maliyetlerini ve BT yatırım maliyetlerini düşürme çalışmaları hızlandı. Güvenlikle beraber her şeyi otomatize etmeye çalıştıklarını fark ettik.

Dolayısıyla 2021 yılı stratejilerimizi bu gerçeği de görerek belirledik. Önümüzdeki süreçte hibrit modele geçeceğimiz öngörülüyor. Bu çerçevede, şirketlerin çok net bir şekilde otomasyona, yapay zekâya ve buluta yöneleceği net bir şekilde görülüyor. Trend Micro'nun çok güçlü bir yapay zekâ entegrasyonu ve bulut çözümleri var. Bu durum, pazarda önemli bir büyümeyi de vaat ediyor bizim için.

Trend Micro'dan En Kapsamlı XDR Platformu

Trend Micro, XDR çözümüyle "Forrester Wave: Kurumsal Tespit ve Müdahale Araştırması" kapsamında şirket tespit ve müdahale alanında lider olarak tanımlanmış ve MITRE ATT&CK çerçevesinde "en yüksek ilk tespit" sonucunu alarak başarısını belgelemişti.

Trend Micro XDR ile geleneksel tespit ve müdahalenin (EDR) kalıplarını kırarak, BT ekiplerinin karmaşık tehditlerle mücadelelerinde ellerini güçlendiriyor.

Bulut güvenliğinin küresel lider şirketlerinden Trend Micro, XDR ile uç nokta tespit ve müdahalenin ötesine geçerek, siber güvenlik sektöründe en kapsamlı tespit imkanı sunan ilk şirket oldu.

XDR, e-posta, uç noktalar, sunucular, bulut iş yükleri ve ağlardan verileri topluyor ve analiz ederek, SOC ekiplerinin söz konusu

tehditleri tespit etmesini, incelemesini ve müdahale etmesini sağlıyor. Günümüzde en gelişmiş korumaları atlatmak üzere tasarlanmış sofistike tehditlerle mücadele eden SOC analistleri, günlük olarak sınıflandırmaları gereken binlerce uyarı alıyor.

SOC'ların en sık karşılaştığı diğer zorluk ise düşük iş memnuniyeti ve siber güvenlik alanındaki yetenek eksikliği. Tam bu noktada Trend Micro, bu sorunlara çözüm getirmek üzere SOC'lara yüksek doğrulukta uyarılar gönderen XDR'ı tasarladı.

XDR kullanıcılara, şimdiye kadar eşi görülmemiş üç önemli avantaj sağlıyor:

>> Uyarı yükünü azaltıyor: XDR, birden çok güvenlik vektöründen gelen verileri birbiriyle ilişkilendirerek analiz ediyor. Böylece büyük resmi ortaya çıkarıyor. XDR sayesinde, birinci seviye SOC analistleri, potansiyel bir saldırıyı tanımlamak için artık birçok analiz ve sistem günlüğünü derinlemesine incelemek zorunda kalmıyor. XDR bunu onlar için otomatik olarak yapıyor. Çok güvenilir olmayan binlerce uyarı yerine birkaç doğruluk payı yüksek uyarı oluşturarak, SOC analistleri için uyarı hacmini düşürüyor.

>> Uyarılar için daha net görünürlük sağlayarak güçlü bir çalışma alanı yaratıyor: XDR kontrol paneli, saldırıları görselleştirilmiş bir şekilde sunarak SOC analistlerinin tehditlerin farklı aşamalarını, saldırı vektörlerini, durma süresini, yayılma ve etkisini görmesine olanak tanıyor. XDR ayrıca bağlamsal olarak duyarlı müdahale seçenekleri sunuyor, böylece SOC analistleri platform içinde daha hızlı harekete geçebiliyor.

>> Güvenlik Bilgi ve Etkinlik Yönetimi'ni (SIEM) artırıyor ve zahmetsiz API entegrasyonu sağlıyor: Trend Micro XDR, normalleştirilmiş verilerin merkezileştirmesi ve olay müdahale yeteneği ile operasyonel verimliliği ve üretkenliği iyileştirerek SOC ekipleri için SIEM'in verimliliğini artırıyor. SIEM çözümünü tercih eden kullanıcılar, entegrasyon için genel bir API kullanabiliyor.

Trend Micro XDR aynı zamanda; şirket içi ekiplerin üzerindeki baskıyı azaltmak için, 7/24 tam tehdit analizi, tehdit avcılığı, müdahale planları ve iyileştirme öneri hizmeti veren "Yönetilen Tespit ve Yanıtlama (Managed Detection & Respond - MDR)" ile sunuluyor.

Uzaktan Çalışmanın Riskleri

Trend Micro yayınladığı bir araştırmada uzaktan çalışanların davranışlarını mercek altına aldı ve işletmeler için güvenlik tehdidi oluşturan pek çok davranış tespit etti.

Bağımsız araştırma şirketi Sapio Research, çalışanların yüzde 78'inin evden çalışmaya geçtiği bu dönemde, çalışanların siber güvenlik yaklaşımlarını ve davranışlarını yakından incelemek için 27 ülkeden 13 binden fazla uzaktan çalışanın katıldığı bir araştırma gerçekleştirildi. Trend Micro adına gerçekleştiren ve siber güvenlik stratejisinin önemli bir parçası olan insan davranışlarının incelendiği araştırmada, Siber Psikoloji Uzmanı **Dr. Linda K. Kaye** ile çalışıldı.

TEMEL TEHDİTLER

Araştırma sonucunda ortaya konulan belli başlı siber güvenlik tehditleri şu şekilde:

>> WiFi'dan kaynaklanan sorunlar: Ankete katılanların yaklaşık beşte ikisi çoğunlukla kurumsal VPN kullanmaksızın halka açık WiFi kullandıklarını belirtti. Ayrıca çalışanların üçte birinin herhangi bir ekran gizlilik filtresi kullanmaksızın halka açık mekanlarda hassas iş belgeleri üzerinde çalıştığı ortaya çıktı.

>> Çevrimiçi tehditler: Uzaktan çalışanların üçte birinden fazlası kurumsal dizüstü bilgisayarlarını kişisel amaçlar için kullanıyor. Bu durum kurumsal verilerin, torrent siteleri, onaylanmamış uygulamalar gibi güvenli olmayan platformlardan bulaşan kötü amaçlı yazılımlara maruz kalması anlamına geliyor. Ayrıca

araştırmaya katılan uzaktan çalışanların beşte ikisi (yüzde 39) çoğunlukla iş için kişisel cihazlarını kullandıklarını kabul etti.

>> Gölge BT (Shadow IT): Uzaktan çalışanlar iş veya kişisel cihazlarına çeşitli uygulamaları yükleyerek profesyonel işleri için kullanabiliyor. Bu da gölge BT'nin katlanarak büyümesine neden oluyor. BT departmanlarının kontrolü olmadan, çalışanların iş verilerini kişisel cihazlar, çevrimiçi hesaplar gibi şirket veri merkezinin dışında depolamak ve bunlara erişmek için kendi seçtikleri uygulamaları, yazılımları ya da hizmetleri kullanmaları Gölge BT'yi (Shadow IT) BT departmanları için ciddi bir zorluk haline getiriyor.

ZAYIF HALKA

Uzaktan çalışanların kurumsal siber güvenlik zincirinin en zayıf halkası olduğu gerçeği, pandemi döneminde şirketlerin görmezden gelemeyeceği bir zafiyet halini aldı. Şirketlerin esnek çalışma modelini kalıcı hale getirmeye doğru ilerlediği bu dönemde, BT departmanlarının ve yöneticilerin güvenlik konusunda çalışanlarının davranışlarını belirlemesi ve buna göre de en uygun güvenlik uygulamalarıyla birlikte güvenlik stratejilerini yeniden planlamaya odaklanması önem kazanıyor.

Farkındalar, ama ciddiye almıyorlar

Sosyal izolasyon önlemleri siber güvenlik bilincini artırdı.

Ancak Trend Micro'nun "Head in the Clouds" araştırmasına göre çalışanlar hala risk alıyor ve risk alma motivasyonları değişiklik gösteriyor.

13,000
uzaktan çalışan
27
ülke

Siber Güvenlik farkındalığı var

%85
Uzaktan çalışanların yüzde 85'i **BT ekiplerinin talimatlarını ciddiye alıyor**

%72
Uzaktan çalışanların yüzde 72'si, kuruluşlarının **siber güvenlik politikalarının** daha fazla **farkında**

Ama çalışanlar hala kuralları esnetiyor

%64
Uzaktan çalışanların **yüzde 64'ü kurumsal bir cihazda iş dışı uygulamaları kullanmanın bir güvenlik riski olduğunu biliyor**

Ancak yüzde 56'sı yine de bunu yaptığını kabul ediyor

%39
Uzaktan çalışanların **yüzde 39'unun kişisel bir cihazdan iş verilerine erişerek kurumsal güvenlik politikasını ihlal etme olasılığı çok yüksek**

Çalışanların ihmalkarlıkları riskleri artırıyor

%34
Çalışanların yüzde 34'ü, **kullandıkları uygulamaların BT departmanı tarafından onaylanıp onaylanmadığını** pek düşünmediklerini, sadece işlerini tamamlamak istediklerini belirtti

%29
Çalışanların yüzde 29'u, şirketlerinin sunduğu çözümlerin beklentilerini karşılamaması nedeniyle **farklı uygulamalara yöneldiklerini** belirtti

%80
Uzaktan çalışanların% 80'i **iş cihazlarını kişisel işleri için kullanıyor**

- **%38** sosyal medya sitelerine giriyor
- **%34** çevrimiçi alışveriş yapıyor
- **%24** İnternet üzerinden film ve dizi izliyor
- **%19** çevrimiçi oyun oynuyor
- **%8** uygunsuz içeriğe ulaşıyor
- **%7** karanlık web'e erişiyor

Uzaktan çalışanlar artık güvenlik konusunda daha bilinçli olsalar da hala kuralları çiğneyebiliyor. Kuruluşların genel eğitim ve öğretiminden ziyade BT güvenlik stratejilerine daha uygun kişileri önde tutan eğitim stratejilerine geçmeleri gerekiyor.

Ayrıntılı bilgi için: www.trendmicro.com