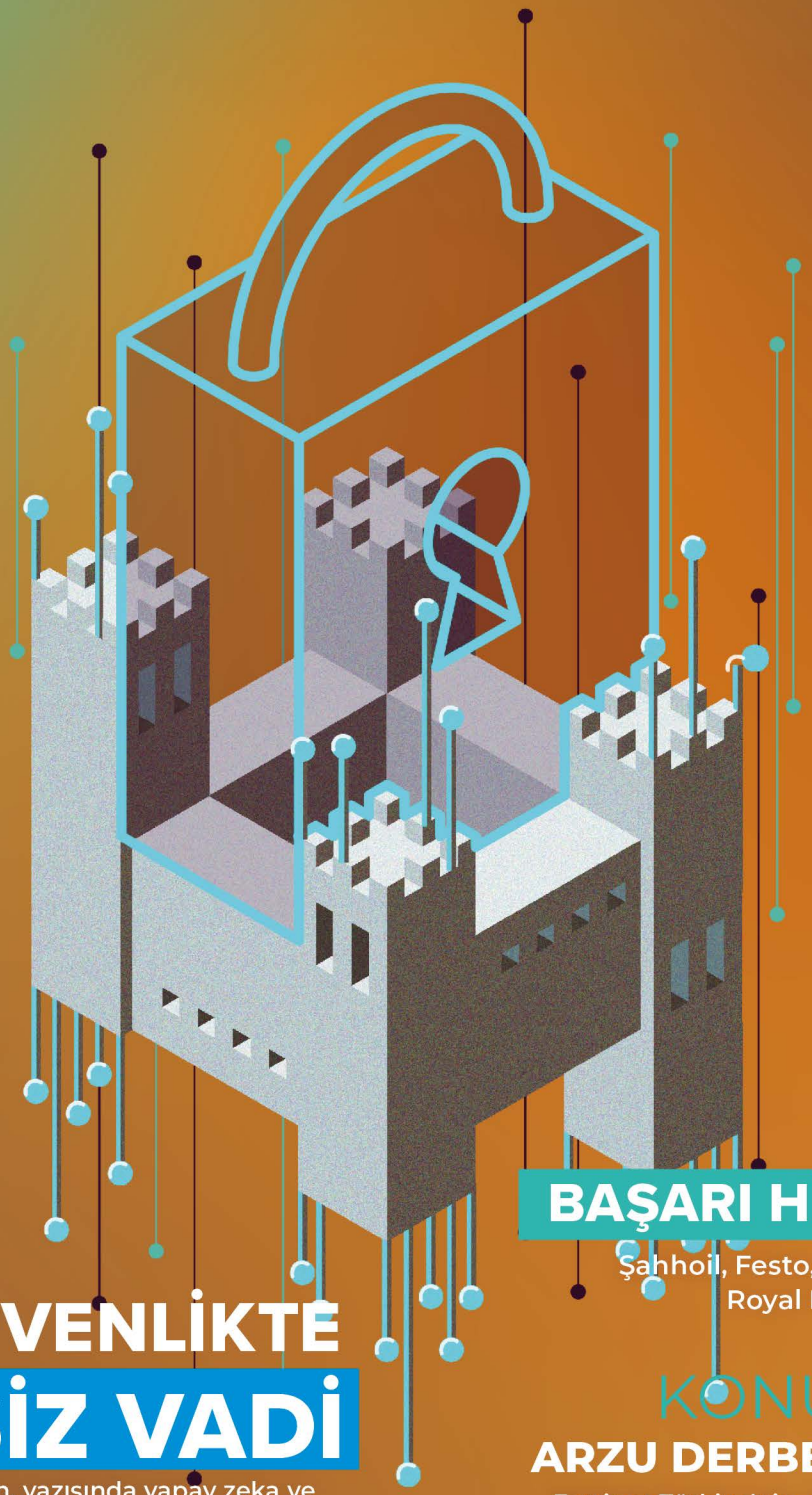
turcommunique

3 ayda bir yayınlanır

EKİM 2023



BAŞARI HİKAYELERİ

Şahhoil, Festo, Linde Opsan, Hypco Royal Diwa Tekirova Resort

SİBER GÜVENLİKTE TEKİNSİZ VADİ

Yönetici Ortak Barış Gürkan, yazısında yapay zeka ve insansı robotların kurumsal ve kişisel hayatlarımıza artan etkilerini ve bu etkilerin güvenlik boyutlarını inceliyor.

KONUĞUMUZ

ARZU DERBENT AKKAYA

Fortinet Türkiye'nin, Azerbaycan, Gürcistan, Türkmenistan, Ermenistan'dan Sorumlu Bölge Direktörü Arzu Derbent Akkaya, güncel siber tehditleri ve korunma yöntemlerini anlattı.

turcom

ISSN 1303-0744 | Maslak Mah. Saat Sok. Spine Tower No:5 Kat:14 34485 Sarıyer / İstanbul | +90 212 349 29 29 | info@turcom.com.tr

turcom | Network Operations Center

Turcom Network Operations Center (NOC) uzman ekibi, sistem ve ağ bileşenlerini 7/24 izleyerek SLA kriterlerinize uygun, bütüncül bir IT yönetimi sağlar.

Sistem ve Ağ İzleme

Topolojideki tüm sistem ve network bileşenlerinin 7/24 izlenmesi ile oluşabilecek problemlerin tespiti ve hızlı müdahalesi gerçekleştirilir.

Maliyetinizi Azaltın

Personel, tesis ve ekipman maliyetlerinden tasarruf edin. Kontratınız dahilinde operasyon maliyetiniz sabit hale gelsin.

Verimliliğinizi Arttırın

Herhangi bir sorun hızlı tespit edilip müdahale edildiğinden verimliliğiniz artar. Performans ve kapasite kayıpları minimuma iner.

İş Sürekliliğinizi Sağlayın

IT altyapınızda meydana gelebilecek problemler size engel olmaz. Bunlarla uğraşmak, görevlendirdiğiniz profesyonel iş ortağınızın görevi olur.

Tek Merkezden Yönetim

Tek bir ortam üzerinden takip ve yönetim sayesinde hızlı aksiyon alınır.

Zaman Kaybının Önüne Geçin

Çalıştığınız operatörü, üreticiyi, saha tarafını ayrı ayrı kontrol altında tutmanıza gerek kalmaz. Turcom NOC ekibi sizin yerinize yapar.

Acil Durumları Yönetebilme

Felaket durumlarında ya da sistem odalarında meydana gelebilecek her türlü sorunda bilgilendirilerek, SLA kriterlerinize uygun çözümlerle sonuca ulaşırsınız.

KATKIDA BULUNANLAR

İMTİYAZ SAHİBİ

Turcom İletişim Sistemleri San. ve Tic. A.Ş. adına Fahrettin Gürkan

SORUMLU MÜDÜR

Barış Gürkan

YAYIN DANIŞMA KURULU

Fahrettin Gürkan, Barış Gürkan, Müfit Süer, Ayça Çınarlı

KAPAK TASARIMI

Bahar Gürkan

İÇERİK VE TASARIM

Barış Gürkan, Bahar Gürkan, Ayça Çınarlı, Erenay Nişancı

KATKIDA BULUNANLAR

Hülya Tipigil, Ufuk Ersöz, Vedat Coşkun, Hasan Burçin Yenice, Abdurrakip Yıldız, Onur Köksal Akçacık, Burak Erdoğan, Turcom İdari İşler Birimi, Turcom Raporlama ve Süreç Birimi

BASKI MATBAA

Promat Basım Yayın San. ve Tic. A.Ş.
Orhan Gazi Mahallesi, 1673 Sokak, No:34
Esenyurt/İstanbul
T : (0212) 622 63 63
F : (0216) 605 07 98
E-Mail: info@promat.com.tr

www.turcom.com.tr / info@turcom.com.tr

8000 adet basılmıştır.

İÇİNDEKİLER

04 **SİBER GÜVENLİKTE TEKİNSİZ VADİ**
Yönetici Ortak Barış Gürkan, yazısında yapay zeka ve insansı robotların kurumsal ve kişisel hayatlarımıza artan etkilerini ve bu etkilerin güvenlik boyutlarını inceliyor.

10 **HPE ALLETRA PORTFÖYÜYLE YENİ FIRSATLAR**

13 **TELNET TELEKOM'DAN EŞSİZ ÇÖZÜMLER**
Telnet, telekomünikasyon sektöründe çözüm mimarisi ile fark yaratıyor.


Barış Gürkan

15 **ŞAHHOIL TURCOM İLE DİJİTALLEŞİYOR**
Turcom'un desteğini arkasına alan Şahhoil, hizmet yelpazesini genişleterek müşteri memnuniyetini arttırdı.

16 **KONUK YAZAR**
Trellix Türkiye ve Azerbaycan Bölge Satış Müdürü Tayfun Er, yapay zekânın siber güvenlikteki yerini okurlarımız için kaleme aldı.


Arzu Derbent Akkaya

18 **trcSPOT: PAYLAŞIMLI İNTERNETTE GÜVENLİ VE KÂRLI BİR DENEYİM...**

22 **FESTO, TURPRO İLE YENİ ÜRETİM DEVRİNİ BAŞLATTI**
Festo, Manisa'daki yeni üretim tesisindeki bilgi işlem altyapısının kurgulanması ve kurulumu projesinde Turpro'ya güvendi.

24 **FORTINET, ARZU DERBENT AKKAYA İLE SİBER GUVENLİK PERSPEKTİFLERİ**

27 **YÖNETİLEN HİZMETLERİN GELECEĞİ**
IT yönetiminin geleceğinde izleme ve güvenlik stratejileri...

İÇİNDEKİLER

30 HYPCO VE TURCOM'UN ORTAKLIĞI İLE TEKNOLOJİ ODAKLI YOLCULUK

34 DİJİTAL DÜNYADA GÜVENLİ GEÇİŞİN ANAHTARI

Ar-Ge Direktörü Prof. Dr. Vedat Coşkun, siber dünyada güvenliğin anahtarı kimlik doğrulama faktörlerini ve seviyelerini okurlarımız için kaleme aldı.

37 İŞLETMELER İÇİN OYUN DEĞİŞTİRİCİ...

Yazılım tanımlı ağ teknolojisi, SD-WAN ile iş ağlarının geleceği nasıl şekilleniyor, Ufuk Ersöz anlattı.

Burçin Yenice

Ufuk Ersöz

40 YAPAY ZEKÂ DESTEKLİ SİBER SUÇLARIN YÜKSELİŞİ: TEHDİTLER VE FIRSATLAR

42 LINDE OPSAN, TURNET İLE YENİ FABRİKALARINDA "TAM GAZ" İLERLİYOR!

44 TREND MICRO DİJİTAL DÜNYAYI GÜVENLİ HALE GETİRİYOR

Dünyanın önde gelen siber güvenlik şirketlerinden Trend Micro, 30 yılı aşkın süredir dijital dünyanın güvenliğini sağlıyor.

46 SİBER GÜVENLİK: ÖNEMİ, FIRSATLARI VE ZORLUKLARI

Burçin Yenice sizin için değerlendirdi.

49 TEKNOLOJİK MÜKEMMELİYETİN, TURİZM SEKTÖRÜNE DOKUNUŞU

51 MAESTRO İLE ÖLÇEKLENEBİLİR AĞ GÜVENLİĞİ

SİBER GÜVENLİKTE TEKİNSİZ VADİ

“Bir çölün ortasında yürüyorsun. Bir anda ayağının dibinde sana doğru yaklaşmakta olan kaplumbağayı fark ediyorsun. Kaplumbağaya uzanıp onu sırtüstü çeviriyorsun. Çölün yakıcı güneşine maruz kalan kaplumbağanın karnı, acı çekmesine ve kendini geri çevirmek için çırpınmasına sebep oluyor. Elbette ki, senin yardımın olmadan kendini geri çevirmesi imkânsız. Sen ise, tüm bunların farkında olduğun halde kaplumbağaya yardımcı olmuyorsun. Neden?”

YAPAY MI YOKSA GERÇEK Mİ?

Yapay zekânın gerçek zekâdan ayrılamayacağı bir gerçeklikte, ikisi arasında ayrım yapabilmek hayati önem taşır. Karşınızda birinin oturduğunu ve onun gerçek bir insan mı yoksa insanı andıran bir robot mu olduğunu beş duyunuzun ayırmaya yetmediğini düşünün.

Farz edin ki, tehlikede olup olmadığınızın tek belirteci karşınızdakinin gerçek insan olmasına bağlı. İşte tam anlamıyla bu belirteci sağlamak için, insan olan ile olmayan arasındaki en temel farkı bulmak gerekiyor. Önceki yazımda da değindiğim Phillip K. Dick’in, *Androidler Elektrikli Koyun Düşler mi?* isimli kült romanı ve onun sinema uyarlaması *Blade Runner* bu temel farkın empati olduğunu savunuyor. *Blade Runner* evreninde *Replicant* diye tanımlanan ve bir insanın sahip olduğu tüm özellikleri barındıran fakat laboratuvar üretimi olan varlıklar mevcut. Konvansiyonel robotların aksine, bizim gibi hücreler ve organlardan oluşuyorlar. İnsan gibi yiyor, içiyor, uyuyor ve yaşlanıyorlar. Bizim tanımımızda yapay zekâ, dijital dünyanın çok katmanlı sıfır, birlerini tanımlarken, burada kelimenin tam anlamıyla yapay olarak geliştirilmiş zekâya karşılık geliyor.

Bu evrende *Replicantları* ayrıştırmak için geliştirilen *Voight-Kampff* testi ile empati refleksleri sorgulayan bir mü-

lakat yapılıyor. Mülakattaki sorular kimi zaman bir hayvanı kurtarmak, kimi zaman ise anne şefkati ile ilgili olabiliyor. Cevapların barındırdığı (ya da barındırmadığı) empatik refleksler ile gerçek insanlar ve *Replicantlar* birbirlerinden ayrılıyor.

P. K. Dick, tartışmasız 1960'ların en öngörülü yazarlarından biri olarak insanlık geleceğinin yaşayacağı gerçek sorunlardan birini derin bir perspektif ile kaleme aldı. Aradan geçen 60 senede yazarın öngörülerinde yer almayan detay, yapay zekânın ne etten kemikten, ne de dişlilerle mekanik aksamlar ile geldiğiydi. Bizim gerçekliğimizde yapay zekâ veri merkezlerinin on binlerce sunucuları ve onları bağlayan milyonlarca kilometrelik kablolarından geçen kod satırları ile oluştu.

TEKİNSİZ VADİ

2018 yılında, Turcom Ar-Ge ekibi ile birlikte insansı robot projelerine başlamıştık. Türkiye'de tek yetkili temsilcisi olduğumuz Softbank Robotics'in *Pepper* isimli insansı robotunun teknik eğitimlerini almaya Paris'teki genel merkezlerine gittiğimizde, eğitime hiç de teknik olmayan bir konudan başladılar:

"Uncanny Valley tabirini duydunuz mu?"

Türkçe'ye kabaca *Tekinsiz Vadi* şeklinde çevirebileceğimiz bu tabir, insan doğasının kökünde olan konseptlerden birini kapsıyor. İnsan beyninin önemli bir özelliği, karşısındaki fiziksel tehditleri algılama konusunda nesillerdir geliştirilmiş bilinçaltı mekanizmaları barındırmasıdır. Karşımızdaki varlığın dost mu düşman mı olduğunu anlama konusunda doğuştan gelen becerilere sahibiz. Masum bir köpeğin sevecenliği ile vahşi bir kurdun tehlikesini ayırt etmek için deneyime ihtiyaç duymamamız gibi.

Bu konuda geliştirdiğimiz bir başka yetenek ise, diğer insanlara dair detaylı gözlem yapabilme ve derin farkındalığa sahip olmamız. Birçok canlının ya da objenin arasından insanları kolayca ayrıştırabiliyor, hemen her gördüğümüz insanı diğerlerinden kolaylıkla ayırt edebiliyoruz. Birçok bilimsel araştırma gösteriyor ki görsel hafızamızda en çok yer eden detaylar, insanların fiziksel özelliklerine dair olanlar...

YAPAY ZEKÂ NE ETTEN, KEMİKTEN, NE DE DİŞLİLERLE MEKANİK AKSAMLARLA GELDİ.

YAPAY ZEKÂ VERİ MERKEZLERİNİN ON BİNLERCE SUNUCULARI VE ONLARI BAĞLAYAN MİLYONLARCA KİLOMETRELİK KABLOLARINDAN GEÇEN KOD SATIRLARI İLE OLUŞTU.

BARIŞ GÜRKAN
YÖNETİCİ ORTAK

Beynimizin bu kadar çok detayı yakalayabilme yeteneği bir yan etkiye sahip. Eğer gördüğümüz kişide bir yanlışlık sezersek beynimiz bu durumu algılayarak bizi doğrudan tedirginlik ve korku gibi duygular hissetmeye itiyor. Bazen üst bilincimiz, karşılaştığımız yanlışlığın ne olduğunu bile tanımlamakta zorlanır. Muhtemelen salgın hastalıklar ve genetik deformasyonlara karşı gelişen bir savunma içgüdüsü olarak ortaya çıkan bu tepki sonucunda beynimiz, karşısındaki varlığı ne kadar zor tanımlarsa bu duyguyu o kadar şiddetli yaşıyor. *Uncanny Valley (Tekinsiz Vadi)* denilen kavram da tam olarak bunu tanımlıyor.

Softbank'in eğitimine dönecek olursak, insansı robotların hayatımıza girmeye başladığı bir dönemde bu robotlar rahatlıkla bizde bu yan etkiyi tetikleyebiliyorlar. Boston Dynamics'in de sahibi olan Softbank'ın ve birçok robot üreticisinin araştırmaları gösteriyor ki; robotlar görsel anlamda insandan ne kadar ayrıştırılamaz ise, bizde yarattığı yan etki o kadar fazla oluyor.

Eğer medyada sıkça gördüğümüz insansı robot *Sophie*'nin ilk üretildiği döneme ait videoları izlerseniz, o zamanlar peruğu ve kıyafeti ile şimdikinden çok daha fazla insana benzediğini fark edebilirsiniz. Zamanla *Sophie*'nin peruğu çıkarıldı ve robotun kafasının arkasındaki metal iç aksamı açıkça görülecek şekilde sergilenmeye başlandı.

Benzer şekilde *Pepper* da insanı neredeyse hiç andırmayan, daha çok Star Wars'taki C-3PO gibi sade ve tek renk barındıran dizaynı ile insanlarda temel refleksleri tetiklememeye dikkat ediyor.

Softbank'in vurgusu da gösteriyor ki, insanları makinelerden ayırabilmek sadece bir siber güvenlik konusu değil. İnsanlık olarak güvende hissedebilmemiz için gerekli.

YARIŞTA KİM DAHA HIZLI?

Burada biraz geriye saralım.

Dijital çağda siber güvenlik giderek artan bir öneme sahip oldu ve bu dönemin en büyük tehditlerinden biri başlangıçta çok yetenekli hackerlar ve onların yaratıcı fikirleriydi. Teknolojiye erişimin yaygınlaşmasıyla birlikte, teknolojinin maddi ve stratejik değeri de büyük ölçüde arttı. Kötü niyetli kişilerin ve giderek gençleşen, kalabalıklaşan grupların bu değerlere haksız yollarla ulaşma çabaları, her gün daha sofistike yöntemlerle sürdürülüyor, bu durum muhtemelen internetin ilk günlerinden beri beklenen bir gelişmeydi. Ancak zamanla değişiklikler yaşandı. Saldırılarda insan eliyle yapılan işlerin yerini programlar aldı ve bu durum bir süre böyle devam etti, ancak şimdi konvansiyonel metodlar, robotik süreç otomasyonlarına ve yapay zekaya yerini bırakıyor.

Orta çağda hükümdarlar, toprak kazanmak için kendileri fiziksel olarak sefere çıkıp, orduları ile birlikte hareket etmek zorundaydı. Alınabilecek aksiyonlar kısıtlı kaynaklar, kısıtlı sayıda insan ve kısıtlı zamana dayanıyordu. Tüm bu limitasyonlar, sadece belli aksiyonların alınabilmesine, dolayısıyla da başarı için en doğru stratejinin doğru uygulanmasına dayanıyordu. Fakat günümüzde, global kapsama alanına sahip güdümlü füzeler ve insansız hava araçları var. Teknolojik yatırım ve yeterli veri havuzuna sahip ülkeler

için, orta çağdaki limitasyonlar günümüzde geçerliliğini tamamen yitirmiş durumda.

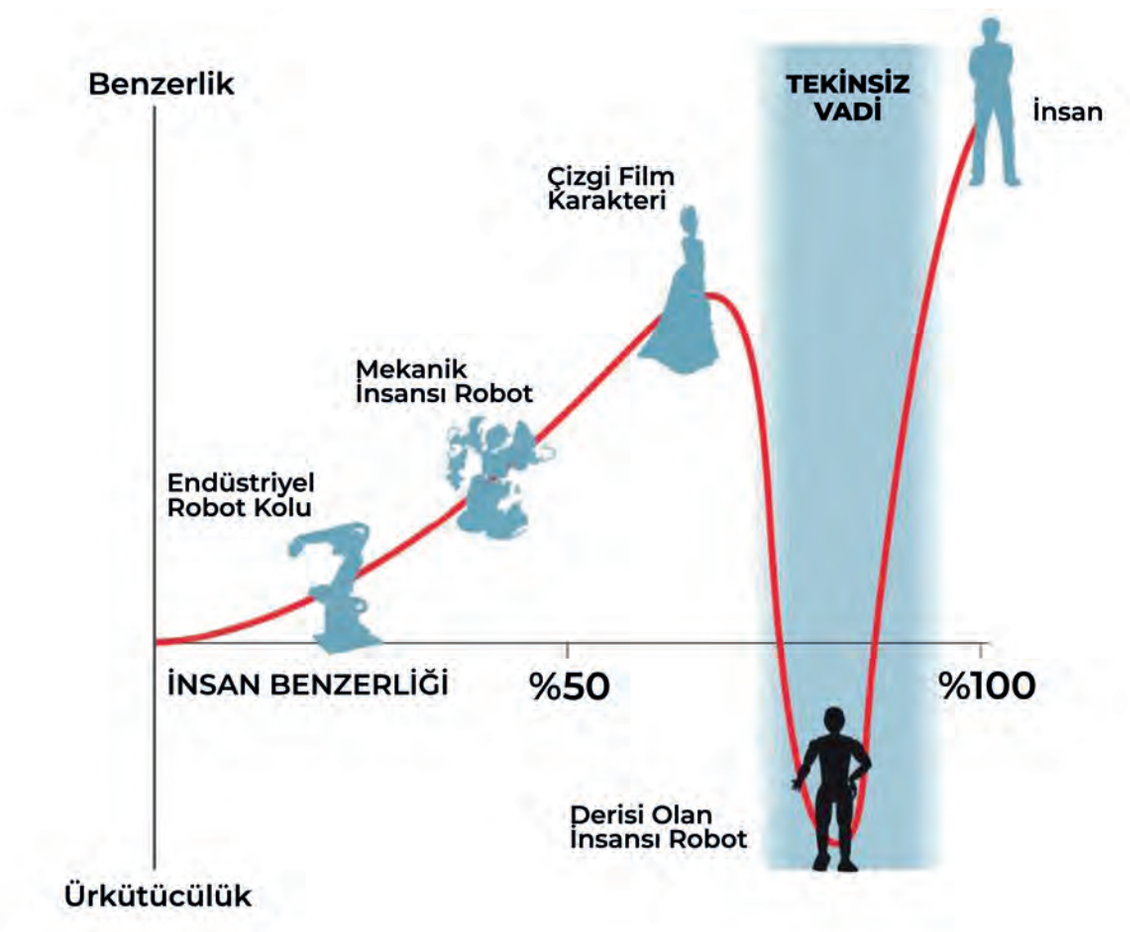
Siber saldırılar da ilk zamanlarda aynı limitasyonlara tabii olsalar da, tıpkı örnekteki gibi insan, zaman ya da kaynak limitlerinden tamamen kurtulmuş durumda. Öyle ki, ataklar için bir insana gerek olmadığı gibi, atağı ölçeklendirmek için de hiçbir kaynak ya da zamana ihtiyaç bulunmuyor. Aynı atağı milyonlarca defa tekrarlayarak da, milyon farklı atağı art arda deneyerek de başarıya ulaşmak mümkün. Bu insan gücü ile mümkün olamayacak bir ölçek.

BİRAZ DA YARATICILIK

Siber saldırı konusunda uzman olan hemen herkesin bildiği gibi, en büyük yerlere ışık hızında ve defalarca erişebilme becerilerini kullanarak çok fazla zafiyet yaratabiliyorlar. Buna rağmen, yazılımlar insanlar için yaratıldığından, insanlara o erişim hakkını yine de tanımak zorunda kalıyoruz. Dolayısıyla güvenlik önlemlerinin çoğu önce ve *Replicant* olarak tanımlananlar gezegenden atılıyorlar. Peki size de bu senaryo çok tanıdık gelmiyor mu?

Biz de web üzerinden kullanıcı adı ve şifremizi girmeden önce sık sık CAPTCHA adı verilen testleri yapıyor, "Ben robot değilim" tuşlarına basıyor, hatta bazen resimler arasında bisiklet olanları bile işaretlemek zorunda kalabiliyoruz. Biz testi geçene kadar sistem ilerlememize izin vermiyor, hatta robot olarak tespit ederse siteye zafiyet hep insanın kendisidir. Teknolojinin varoluşundaki yegane sebep insana hizmet etmek olduğu için, tüm siber saldırılar, insanı mağdur etme niyetleri konusunda aynı paydaya düşerler.

Makinelerin aksine, insanlar öngörülemez davranışlar sergileyebildiği ve rastgele hata yapabildiğinden dolayı, makinelere göre zafiyetleri daha erişilebilir durumdadır. Şifrelerini kolay hatırlamak için kısa ve basit tutanlar, ya da gelen e-postalardaki linklere masumca tıklama eğiliminde olanlar buna birkaç örnek... Yapay zekâyla ise durum daha farklı hale geliyor. Sosyal hackleme denilen, insanın hata yapmasını sağlamaya dayalı yöntemlere artık eskisi kadar ihtiyaç duyulmuyor.



Yapay zekâ, *Deepfake* denilen, kendi kendine kişilerin dijital sahte video görüntü ve seslerini yaratarak, kötü niyetlerle de kullanabiliyor. Benzer şekilde kişilerin çevrimiçi verilerinden faydalanarak daha tutarlı şifre tahminleme yapalabiliyor. Bu şifre tahminleri her gün daha çok tekrarda ve daha tutarlı tahminler haline geliyor. Görünüşe göre, sosyal medya gibi platformlarda insan gibi davranarak kişisel verileri istismar eden ve insanları mağdur eden uygulamalar ise hemen hepimizin özel hayatı için büyük bir tehdit oluşturuyor. Yapay zekânın kendisinin insan olduğuna bizi ikna edebilme becerisi aklımıza gelmeyecek sayıda siber suçun önünü açacağı gibi bize dijital evrende güvenli ortam bırakmama riskini barındırıyor.

Bu yüzden de siber güvenlikte insan ve makine arasındaki kimliksel ayrımın kutsal bir yeri var. Yazılımlar akıllandıkça, insanların erişebileceği yerlere ışık hızında ve defalarca erişebilme becerilerini kullanarak çok fazla zafiyet yaratabiliyorlar. Buna rağmen, yazılımlar insanlar için yaratıldığından, insanlara o erişim hakkını yine de tanımak zorunda kalıyoruz. Dolayısıyla güvenlik önlemlerinin çoğu önce erişim talep edenin insan olduğunu doğrulamak, kim olduğunu ise sonraki adımda sorgulama yöntemini tercih ediyor. Örneğin web üzerinden giriş yaparken banka hesabınız, ona erişenin hem bir insan olduğunu algılamak zorunda, hem de o insanın siz olduğundan emin olmak zorunda kalıyor.

KİM İNSAN KİM DEĞİL?

Şimdi *Blade Runner*'a tekrar dönecek olursak, Phillip K. Dick'in dahiyane farkındalığını bugünkü koşullarımızla ele alalım. *Blade Runner*'da *Replicant'lar*a, insanlara tanınan özgürlüklerin tamamı tanınmıyor. Kurallara uymayan *Replicant'*ları tespit edebilmek ve insanlardan ayrıştırabilmek için Voight-Kampff Testi'ni kullanıyorlar. Testi geçemeyen durum daha farklı hale geliyor. Sosyal hackleme denilen, insanın hata yapmasını sağlamaya dayalı yöntemlere artık eskisi kadar ihtiyaç duyulmuyor.

Yapay zekâ, *Deepfake* denilen, kendi kendine kişilerin dijital olarak sahte video görüntüleri ve seslerini yaratarak, çeşitli kötü niyetlerde kullanabiliyor. Benzer şekilde kişilerin çevrimiçi verilerinden faydalanarak daha tutarlı şifre tahminleme yapabiliyor. Bu şifre tahminlerini her gün daha çok tekrarda ve daha tutarlı tahminlerle becerebiliyor. Hemen hepimizin özel hayatına bile risk oluşturabilecek en büyük tehdit ise, sosyal medya gibi ortamlarda insan gibi davranarak kişilerin istismar ve mağdur edilmesi olacak gibi görünüyor. Yapay zekânın kendisinin insan olduğuna bizi ikna edebilme becerisi, aklımıza gelmeyecek sayıda siber suçun önünü açacağı gibi, bize dijital evrende güvenli ortam bırakmama riskini barındırıyor.

Bu yüzden de siber güvenlikte insan ve makine arasındaki kimliksel ayrımın kutsal bir yeri var. Yazılımlar akıllandıkça, insanların erişebileceği

tüm erişimi kapatabiliyor. *Blade Runner*'da da *Replicant'*lar ne kadar yeni sürüm ve sofistikelerse, testin süresi ve soru derinliği o kadar artıyor. Tıpkı bizim CAPTCHA testlerimizin bize daha fazla sokak lambası ya da bisiklet işaretletmesi gibi.

Biz gerçek dünyanın *Voight-Kampff* testlerini yaratıyoruz ama bir yandan da testleri alt etmekte gittikçe yeteneklenen rakipler ile mücadele ediyoruz. İnsan ve makine arasındaki satranç maçı devam ediyor.

MAKİNELER MAKİNELERE KARŞI

Yapay zekâ nasıl saldırı için kullanılabiliyorsa, aynı yetkinliklerle savunma için de kullanılabiliyor. Tehdit öngörüsü ya da olağandışı davranış tespiti gibi konularda gittikçe yaygınlaşırken, bir önemli savunma becerisi ise, kötü niyetli yazılımları yakalamak. Kötü niyetli yazılımların da yukarıda belirttiğimiz gibi yapay zekâyı kullandığını düşünürsek, artık yeni bir rekabetin doğduğunu görüyoruz.

Yapay zekâ üzerine yapılan birçok akademik araştırma, büyük veri havuzlarından beslenen sinir ağları kullanarak kendiliğinden bir yol izleyip özgün çözümler üretebiliyor. Bu çalışmaları yapmak için kullanılan en yaygın yöntem iki ya da daha fazla sinir ağını birbirleri ile etkileşime mecbur bırakılarak sonuçlarını takip etmeye dayanıyor. *Generative Adversarial Network* (GAN) denen bu mimarilerde yapay zekânın sonuçları insansal davranışlardan o kadar uzaklaşabiliyor ki, bizi yukarıda bahsettiğimiz *Uncanny Valley* noktasına çekme riski taşıyor.

PEKİ BUNDAN SONRASI?

Sonuçta yapay zekâ insanlık için kaçınılmazlığını koruyor. Siber güvenlik ile yapay zekâ birbirlerinden ayrıştırılamaz hale gelirken, insanı makineden, iyi makineyi de kötü makineden ayırmak, tıpkı *Blade Runner*'da olduğu gibi belki de güvende olup olmadığımızı belirleyen yegane katman haline gelecek.

Belki de Blockchain ve NFT gibi teknolojilerin sağladığı replike edilemez tanımlamalar yakın gelecekte bu alanda kendine yer bulabilir. Hatta insanlar olarak webde ve dijital ortamlarda aldığımız hemen her aksiyonu bir insanın aldığını doğrular nitelikte parmak izleri geliştirmemiz gerekebilir.

Phillip K. Dick, insanı yapaydan ayıran en büyük farkı empati olarak tanımlamıştı. Biz de insanlık olarak empatimizi kaybetmediğimiz sürece, kendimizi makinelerden ayrıştırabilecek ve kendimizi güvencede tutabileceğiz. Bu sebeple; çöldeki kaplumbağanın kurtulmasına yardım etmemiz gerektiğini unutmayalım.

> **İNSANLAR OLARAK WEBDE VE DİJİTAL ORTAMLARDA ALDIĞIMIZ HEMEN HER AKSİYONU BİR İNSANIN ALDIĞINI DOĞRULAR NİTELİKTE PARMAK İZLERİ GELİŞTİRMEMİZ GEREKEBİLİR.**

HPE, GENİŞLETİLMİŞ HPE ALLETRA PORTFÖYÜ İLE VERİ YAŞAM DÖNGÜSÜ YÖNETİMİNİ YENİ DOSYA, BLOK VE VERİ KORUMA HİZMETLERİYLE DÖNÜŞTÜRÜYOR

HPE Alletra Storage MP üzerine inşa edilmiş yeni veri hizmetleri, sezgisel bulut deneyimi, yüksek performanslı ölçeklenebilir depolama ve HPE GreenLake aracılığıyla sunulan hibrit veri korumasını sunmaktadır.

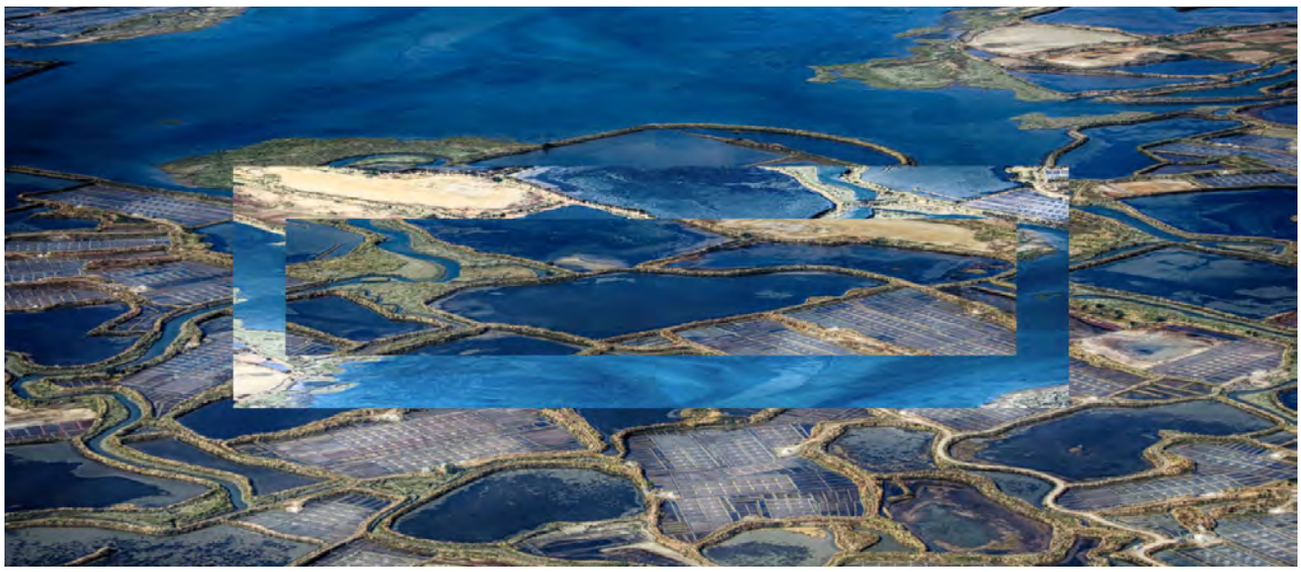
Hewlett Packard Enterprise (NYSE: HPE); veri silolarının getirdiği karmaşayı ortadan kaldırırken kurumsal maliyetlerin düşürülmesine ve sistem performansının arttırılmasına yardımcı olmak için tasarlanmış yeni veri dosyalama, bloklama, felaket önleme ve yedekleme/kurtarma hizmetlerini Nisan 2023'te sundu. HPE' nin yeni dosya depolama veri hizmetleri, veri yoğun iş yükleri için ölçeklenebilir, kurumsal düzeyde performans sunuyor. Genişletilmiş blok hizmetleri, dengeli bir fiyat performans oranıyla kritik görevler için uygun depolamanın yapılmasını mümkün kılıyor.

Yeni dosya ve blok hizmetleri HPE Alletra Storage MP aracılığıyla esnek bir mimariye dayanır ve müşterilere hibrit bulutta, birleşik tek bir platform üzerinden tüm veri türlerini depolama, yönetme ve koruma olanağı sunar. Bununla birlikte, HPE' nin sözkonusu yeni veri hizmetleri, müşterilerin veri yaşam döngüsündeki yönetim süreçlerini dönüştürerek, yaşadığımız *içgörü çağında başarılı olma imkânı tanır. Böylece sezgisel bir bulut işletim deneyimi sağlar.

**Büyük veri ve analitiğin öne çıktığı ve bunların yapay zeka çözümleri ve makine öğrenmesi ile harmanlanarak işletmeler için bilinçli ve etkili kararlar alınabilen bir dönemi anlatır.*

HPE Yönetici Başkan Yardımcısı ve Depolama Grup Genel Müdürü Tom Black; günümüzde müşterilerin verilerini yönetme konusunda eşi benzeri görülmeyen zorluklarla karşı karşıya kaldığını belirtti. Black; kompleks veri hacmindeki hızlı artış sebebiyle kuruluşların bu durumu maliyeti yüksek izole depolama kombinasyonlarıyla yönetmek zorunda kaldıklarını anlattı. Bu noktada yeni HPE GreenLake veri hizmetleri ve HPE Alletra'nın geliştirilmiş yenilikleri kuruluşların farklı veri türleri, depolama protokolleri ve iş yüklerini daha ekonomik ve daha kolay şekilde yönetmelerini sağlıyor. Bu şekilde müşterilerin inovasyon hızına katkı sağlarken onların iş sonuçlarına daha fazla odaklanmasına olanak tanıyor.

Her ölçekteki işletme, daha iyi kararlar alarak daha isabetli sonuçlar elde etmek için veriyi avantaj olarak kullanmayı amaçlar.



Bu sebeple çok önemli bir konu haline gelen kurumsal veri yönetiminin yanında veri çeşitliliğini yönetmenin maliyeti de kuruluşlar tarafından kontrol altına alınmak istenir. Bir diğer yandan 2026'ya kadar üretilen global veri miktarının da bugüne oranla iki kat artacağı öngörüleri yapılmaktadır. Bu durumda da her biri farklı destek ve yönetim sistemi gerektiren karmaşık iş yükü türleri ve veri protokolleriyle karşı karşıya olan kuruluşların işi de en az iki kat zorlaşacaktır. İşlerini yürütmek için bağımlı oldukları veriyi yedeklemekte, korumakta ve kurtarmakta daha da zorlanacaklardır.

> **"VERİ YAŞAM DÖNGÜSÜNE İLİŞKİN ZORLUKLARIN BİR KABUS HALİNE GELDİĞİNDE KURULUŞLARIN BU KABUSU AŞMALARINA YARDIMCI OLMAK İÇİN HPE, BLOK VEYA DOSYA DEPOLAMALARI KONUSUNDA YAPILANDIRILABİLİR, YENİ, MODÜLER BİR ÇÖZÜM SUNMAKTADIR."**

Kuruluşların veri yaşam döngüsü kabusunu aşmalarına yardımcı olmak üzere HPE, blok veya dosya depolamaları için yapılandırılabilir yeni, modüler bir depolama çözümü sunmaktadır. HPE Alletra Storage MP, aynı donanımda performans ve kapasite için bağımsız olarak ölçeklenebilen, çoklu depolama protokollerini destekleyen dağıtık bir altyapıyı destekler. Müşteriler, iş yüküne ve depolama protokolüne bakılmaksızın veri ve depolama hizmetlerini dağıtmak, yönetmek ve orkestrasyonunu yapmak için tek, birleşik bir bulut platformundan faydalanır. HPE Alletra Storage MP'nin esnekliği, yüksek performansına rağmen çok daha rekabetçi bir fiyat sunmanın yanı sıra gelecekte altyapının genişletilmesine ihtiyaç duyulduğunda da maliyet avantajlı şekilde buna olanak sağlar. Aynı zamanda da veri yönetim sitemine yapılan yatırımların değerinin korunarak geliştirilmesine olanak sağlar. Ayrıca, AIOps tarafından desteklenen sezgisel bulut deneyimi, özel becerilere ihtiyaç duyulmaksızın depolama alanı ayırma (provisioning) ve yönetme yeteneği sağlar.

HPE GREENLAKE, DOSYA DEPOLAMA PAZARINA GİRİYOR VE BLOK DEPOLAMAYI GENİŞLETİYOR

HPE'nin yeni dosya ve blok depolama için sundukları, HPE GreenLake aracılığıyla, HPE Alletra Storage MP'den esnek bir veri mimarisi sağlar. Birleşik tek bir platform üzerinden dosya ve blok veri hizmetlerini yönetme ve orkestrasyon yeteneği, verinin gücünden faydalanmaya odaklanan her kuruluşa rekabetçi ve inovatif olmak konusunda avantajlar elde etme imkanı sunar.

HPE GreenLake, Dosya Depolama için saniyede yüzlerce gigabayt hızında veri geçişiyle, sistem kapasitesi veya performansını daha fazla birim veya düğüm ekleyerek artırır (scale-out), veri yoğun iş yüklerini geniş ölçeklerde dahi hızlandıran kurumsal bir performansla ölçeklendirme hizmeti sunar.

Bu yeni dosya depolama hizmeti, HPE GreenLake'in bulut deneyimi ile VAST Data yazılımını birleştirerek exabyte ölçeğinde son derece dayanıklı bir dosya servisi oluşturur.

DÜNYA'NIN EN POPÜLER ONLINE KONAKLAMA PLATFORMUNUN HPE GREENLAKE DENEYİMİ

Dünya çapında bilinen, popüler bir online konaklama rezervasyon platformu ve HPE müşterisi olan Agoda' nın en değerli varlıkları müşteri bilgileri ve seyahat sağlayıcılarına ait verilerdir. (havayolları, oteller v.s.)

Agoda'nın CTO'su Idan Zalzberg, kurumun büyüyen veri yapısıyla başa çıkabilmek için performansı ve kapasiteyi kolayca ölçeklendirebilen bir veri platformuna ihtiyaç duyduklarını anlattı. Zalzberg, Agoda' nın her zaman işleri için en iyi teknolojiyi kullanmaktan kaçınmadığını ve bu amaçla, HPE GreenLake ile VAST Data teknolojisinin kombinasyonun kendileri için mükemmel bir anlam ifade ettiğini söyledi. Agoda CTO'su "Gelecek yıllarda da HPE GreenLake Dosya Depolama'nın sınıfının en iyi performansını sunmasını bekliyoruz." dedi.

Blok Depolama için orta sınıf ekonomiye sahip HPE GreenLake, görev kritik depolamanın mevcudiyetini, performansını ve ölçeklenebilirliğini genişletmeye yönelik imkanlar sunar ve yeni HPE GreenLake Blok Depolama, %100 veri mevcudiyeti garantisiyle sektörün ilk ayrıştırılmış, yatay ölçeklenebilir blok depolama sistemidir. HPE GreenLake Blok Depolama yeni haliyle daha da iyi bir fiyat/performans oranı sunarken aynı zamanda o, daima açık, hızlı bir mimariyle müşterilerin görev kritik uygulamaları ve karışık iş yükleri için SLA kriterlerine uygunluklarını sağlamalarına yardımcı olacak şekilde tasarlandı. Müşteriler, HPE Alletra Depolama MP'ye yatırım öncesi başlangıç maliyeti ile erişebilirken, HPE GreenLake Blok Depolama abonelik hizmetlerini de tercih edebilirler.

Amerikan futbolunun en tanınmış ve başarılı takımlarından biri olarak bilinen "Dallas Cowboys" un Kurumsal Sistemler Yöneticisi Evan Scates; inovasyonun, markaları için temel taşlarından biri olduğunu belirterek, bu sebeple HPE'nin hibrit bulut vizyonunda öncülüğünü ve bulut üzerindeki işletim sistemi deneyimleri konusunda da kendilerine on-premise olarak sundukları hizmetlerden memnuniyetini dile getirdi. Uzun süredir bir HPE müşterisi olduklarını belirten Evans; yeni HPE GreenLake Blok Depolama tarafından sağlanan kolay yönetimin, etkili ölçeklendirmenin ve yüksek performansın, IT operasyonlarına ve müşteri deneyimlerine daha fazla değer kattığını söyledi.

"UZUN SÜREDİR BİR HPE MÜŞTERİSİYİZ VE YENİ HPE GREENLAKE BLOK DEPOLAMA TARAFINDAN SAĞLANAN KOLAY YÖNETİMİN, ETKİLİ ÖLÇEKLENDİRMENİN VE YÜKSEK PERFORMANSIN, IT OPERASYONLARIMIZA VE MÜŞTERİ DENEYİMİMİZE DAHA FAZLA DEĞER KATACAĞINA İNANIYORUZ."

EVAN SCATES
KURUMSAL SİSTEMLER YÖNETİCİSİ / DALLAS COWBOYS

HPE, ENTEGRE VE BÜTÜNLEŞİK HİBRİT BULUTTAKİ VERİLERİN KORUNMASI İÇİN GEREKLİ EŞSİZ İMKANLAR SUNAR

HPE GreenLake şimdi felaket sonrası kurtarma ve veri yedekleme, back-up (geri yükleme) için birleştirilmiş bir yaklaşımı destekler.

HPE GreenLake Felaket Sonrası Kurtarma, HPE globalin ölçeklenebilir SaaS platformundaki esnek faturalandırma sistemi sayesinde (kurumların "subcription" ücretlerinde olası aksamalarında dahi) sürekli veri koruma (düzenlemesi) aracılığıyla (müşterilerinin yaşayabileceği) kesinti sürelerini azaltırken, veri kayıplarını azaltır. Zerto teknolojisi ile oluşturulan HPE GreenLake Felaket Sonrası Kurtarma, birden fazla sanal makine (VM) üzerinde kolay, birleşik, otomatik ve orkestrasyona uygun bir deneyim sağlayarak, müşterilerine herhangi bir kesintiden hızlı ve esnek bir şekilde kurtulma imkânı tanır.

HPE GreenLake Yedekleme ve Kurtarma, hem özel hem de kamusal bulut iş yükleri için birleşik yönetim ve tek bir veri kataloğu sayesinde on-premise ya da bulut iş yüklerini kolayca, verimli şekilde korur. Aynı zamanda politika tabanlı orkestrasyon, üstün depolama verimliliği ve %100 SaaS çözümü olarak "kullandığın kadar öde" (kullanım tabanlı) mantığındaki faturalandırmayı sunar.

HPE Pointnext Hizmetleri de organizasyonların veri-öncelikli modernizasyon stratejilerini geliştirmek ve dünya standartlarında bir müşteri deneyimi sunmak üzere oluşturulmuştur. Bu servislerin içeriğinde veri hizmetlerini ve stratejilerini tasarlamak, dağıtmak ve yönetim hizmetleriyle, katmansız (tier less), her yerden beraber çalışabilmeye (collaboration) uygun teknolojiler desteklenir.

TELNET TELEKOM: TELEKOMÜNİKASYON SEKTÖRÜNDE ÇÖZÜM MİMARİSİ İLE FARK YARATIYOR

TELNET TELEKOM'UN GENİŞ ERİŞİMİ

Ulaşılması zor, iletişim altyapısından yoksun mekânlara dahi teknolojinin dokunuşunu getiren Telnet Telekom, 21. yüzyılın iletişim çözümlerinin sınır tanımayan öncüsüdür. Dağların zirvelerinden Arabistan'ın sıcak çöllerine, uzak köylere ve metropollere kadar her yere ulaşan hizmet ağıyla müşterilerine özel en uygun, güvenilir çözüm mimarisi, ürün, ağ ve internet hizmetleri ile Telnet Telekom bölgesindeki telekomünikasyon sektörünün liderleri arasında yer alıyor. Bu geniş kapsam, sadece coğrafi erişimle sınırlı değil; aynı zamanda en son teknolojilere ve yenilikçi iletişim stratejilerine de erişim anlamına geliyor.

TEKNOLOJİK ÇEŞİTLİLİK VE ERİŞİM

Telnet'in öne çıkışının ardındaki en büyük etkenlerden biri, ülkenin dört bir yanındaki geniş servis sağlama kapasitesidir. Bakır altyapıdan fiber optiğe, Karasal xDSL'den Metro Ethernet'te mobil olarak Uydu'dan 4,5G 'ye kadar olan geniş teknoloji yelpazesi, kullanıcıların hızlı ve güvenilir internet erişimine olan ihtiyacını karşılıyor. Bu teknolojik esneklik, bölgesel farklılıkların ve özel ihtiyaçların üstesinden gelmeye olanak tanıyor.

YENİLİKÇİ ÇÖZÜMLER VE ORTAKLIKLAR

Ancak Telnet'in sunduğu hizmetler bu kadarla sınırlı değil. Şirket, ileri teknolojiyle geliştirilmiş bulut santral sistemleri, radyo link hizmetleri ve kablosuz iletişim için Point-to-Point (P2P) sistemler gibi yenilikçi çözümler sunmaktadır. Bu hizmetler, genellikle büyük veri akışları olan kurumsal firmalar için kritik öneme sahiptir.

ABDURRAKİP YILDIZ
TELEKOM ÇÖZÜMLERİ YÖNETİCİSİ

ENTEGRE TELEKOM ÇÖZÜMLERİ

Üstelik Türkiye'deki telekom devleriyle olan iş birlikleri, Telnet'in sektördeki konumunu daha da güçlendiriyor. Türk Telekom, Vodafone ve Turkcell gibi firmalarla gerçekleştirdiği iş birlikleri sayesinde, Telnet hem ulusal hem de uluslararası arenada tanınırlık kazanmıştır. Bunun yanı sıra, maliyet etkinliği ilkesiyle hareket eden şirket, yerel internet sağlayıcılarıyla da iş birliği yaparak, müşterilere daha uygun fiyatlı hizmetler sunmayı hedefliyor.

ANA OMURGADA SD-WAN VE MPLS TEKNOLOJİLERİNİN AVANTAJLARINI YAŞAMAK

Telnet'in "Tek Noktadan Toplu Telekom Teknoloji Çözümleri" yaklaşımı, telekomünikasyon sektöründe yeni bir hizmet anlayışını temsil ediyor. Hem bireysel hem de kurumsal müşterilere geniş bir hizmet yelpazesi sunarak, hizmet alım süreçlerini basitleştirmekte ve daha etkin hale getirmektedir. Özellikle SD-WAN (Software-Defined Wide Area

Network) ve MPLS (Multi-Protocol Label Switching) altyapıları üzerindeki çalışmalarıyla öne çıkan Telnet, bu teknolojileri IPsec VPN (Virtual Private Network) protokolleriyle entegre ederek, güvenli bir iletişim altyapısı oluşturuyor.
SD-WAN, geleneksel WAN mimarilerine kıyasla merkezi bir kontrol fonksiyonunu kullanarak WAN trafiğini yönetme kapasitesine sahip. Bu, çoklu şube veya uzak lokasyonlarda faaliyet gösteren kurumlar için ağ performansını ve ölçeklenebilirliği optimize eder.

Örneğin, bir şirket Asya ve Avrupa arasında veri transferini SD-WAN sayesinde daha verimli hale getirebilir. Öte yandan, MPLS, ses ve video gibi gerçek zamanlı uygulamalar için hızlı ve öngörülebilir bir performans sunar.

ÖZEL SEKTÖRLERE ÖZGÜ ÇÖZÜMLER

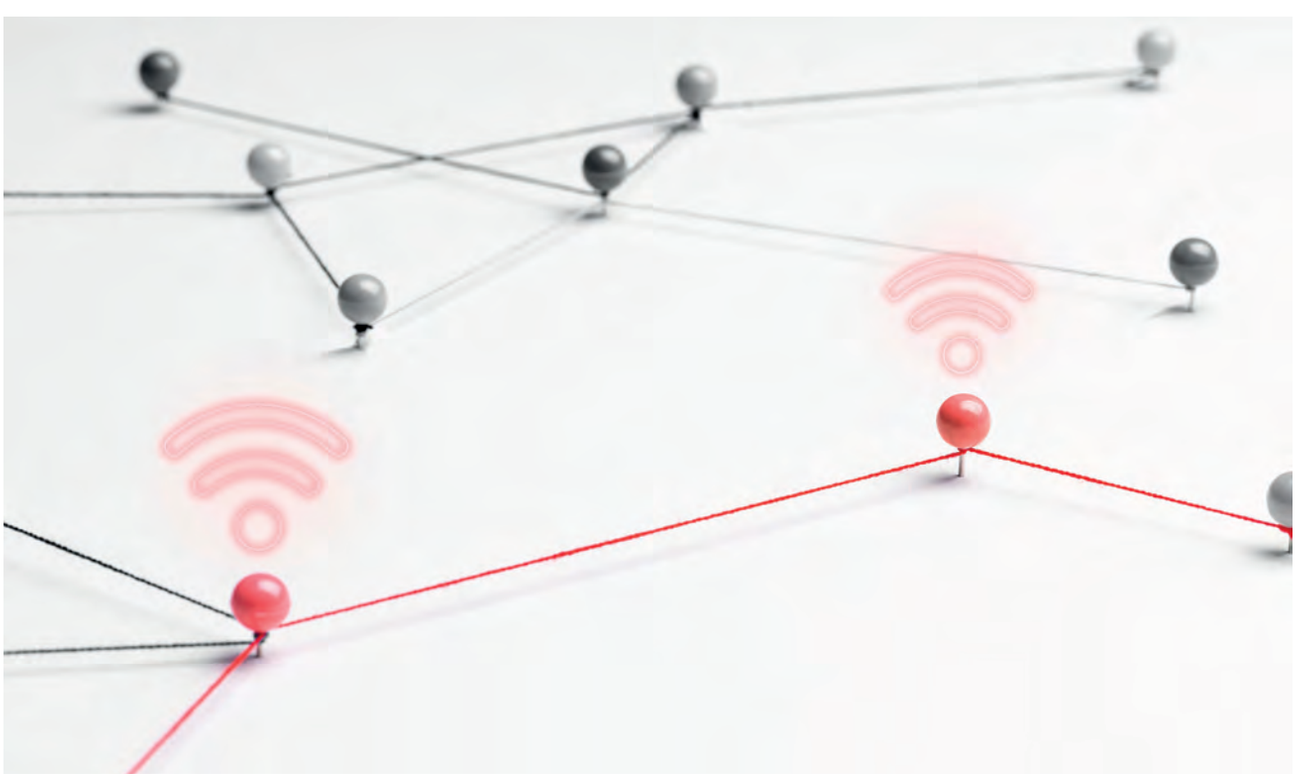
Ancak Telnet'in yenilikçi yaklaşımı sadece bu teknolojilere sınırlı değil. Enerji ve akaryakıt sektörleri gibi özelleşmiş alanlarda da faaliyet gösteriyor. Bu sektörlerin kritik, katı regülasyonlara tabi veri aktarımları için IPsec VPN ve MPLS teknolojileri büyük önem taşıyor. Özellikle regülasyonların ve yasal gerekliliklerin yoğun olduğu bu alanlarda, Telnet'in sağladığı güvenli veri aktarım hizmetleri, sektör standartlarını belirleyen bir niteliğe sahip.

IPsec VPN teknolojisinin enerji ve akaryakıt sektörlerinde sunduğu avantajlar, veri bütünlüğünün ve gizliliğinin korunmasından, ağ trafiğinin önceliklendirilmesine kadar uzanmaktadır. Bu teknoloji, şifrelenmiş tünel mekanizmasıyla veri transferini sadece yetkili kullanıcılara açık hale getirerek, potansiyel siber saldırılara karşı ekstra bir güvenlik katmanı oluşturur. Ancak, her teknolojik uygulamada olduğu gibi, IPsec VPN'nin de kendi içinde bazı dezavantajları bulunmaktadır. Özellikle kompleks yapıda olan ağ ortamlarında kurulum ve yönetim zorlukları yaşanabilir. Ayrıca, veri şifrelemenin getirdiği ekstra yük nedeniyle bazen sistem performansında düşüşler gözlemlenebilir.

Ancak bu dezavantajlar, doğru ağ yapılandırması ve optimizasyon stratejileri ile minimuma indirilebilir. Bu noktada Telnet 7/24 İzleme ve NOC servisleri ile Hat ve aktif cihaz performanslarını gözlemleyerek yönetilebilir hizmetler sunmakta, yedekli omurgası sayesinde müşterilerine kesintisiz erişimleri sağlamaktadır.

SEKTÖRDEKİ DEVRİMCİ YAKLAŞIM

Sonuç olarak, Telnet'in bu geniş ölçekli mimari yaklaşımı ve sunduğu entegre çözümler, telekom profesyonelleri tarafından sektörde öncü olarak kabul ediliyor. Modern iletişim ihtiyaçlarını karşılamak adına öne çıkan bu teknolojiler, sektördeki liderliğini pekiştiriyor.



ŞAHHOIL,
TURCOM'LA DİJİTALLEŞİYOR

Turcom'un desteğini arkasına alan Şahhoil, hizmet yelpazesini genişleterek müşteri memnuniyetini arttırdı.

Günümüzde hızla ilerleyen teknoloji ve dijitalleşme, birçok sektörden firmanın iş süreçlerini iyileştirmeye devam ediyor.

Turcom'un, çeşitli sektörlere yönelik uzmanlık alanlarından biri olan akaryakıt sektöründeki Enerji Piyasası Düzenleme Kurumu (EPDK) otomasyonu konusunda desteğini alan Şahhoil, müşterilerine sunduğu hizmet yelpazesini genişletti.

Şahhoil, Mardin/Kızıltepe'de 2013 yılında "Akaryakıt Bayilik İşletmeciliği" ile faaliyet göstermeye başlamasının ardından 2016 yılında *Europetgaz* firmasıyla birlikte LPG dağıtımına başladı. Deneyim ve bilgi birikimi sayesinde akaryakıt dağıtımına başlayarak hizmet ağını genişletti ve 107 adet istasyona ulaşarak Türkiye'nin dört bir yanında müşterilerini kalite ile buluşturmaya devam ediyor.

Akaryakıt bayiliğinin ardından dağıtımına da başlayan Şahhoil, tâbi olduğu *Enerji Piyasası Düzenleme Kurumu*'na veri aktarma yükümlülüğü için VPN bağlantısına ihtiyaç duydu. Regülasyonlara göre akaryakıt satış miktarının devlet tarafından denetlebilmesi adına kullanılan VPN bağlantısı sayesinde ilgili kuruma satış verilerinin aktarılması sağlanarak güvenlik ve kesintisizlik mümkün hale geldi.

107 istasyonun her birisinde data hattı devreye alınarak bu hatlara 4G router (M2M) kurulmasıyla VPN bağlantı tüneli üzerinden bulutta konumlandırılan sanal sunucuya veri aktarımı sağlandı. Bulut üzerinde çalışan online bir otomasyon altyapısının mümkün hale gelmesiyle Şahhoil'in iş süreci iyileştirildi.

İstasyon sayısının ve iş kolu çeşitliliğinin artmasıyla kritik iş yükleri karşısında sunucu sistemleri yetersiz kalmaya başlayan Şahhoil, yeni nesil sunucu yapısı için Turcom'u seçti. Turcom'un güçlü ekibinin yaptığı değerlendirmeler sonucunda daha önce fiziki olarak bulunan 107 istasyonun sunucularının bulut ortamına taşınmasına karar verildi. Turcom ekibinin verdiği destek ile 7/24 hizmet veren tüm istasyonlarında hızlı erişim sağlanmasıyla veriler güvenli bir şekilde yedeklenmeye başladı, bakım maliyetinden tasarruf edildi ve verimlilik arttı.

Sunucu sistemlerinin bulut ortamına taşınmasının ardından ağ güvenliğinin sağlanabilmesi için firewall konumlandırılması aşamasına geçildi. İstasyon sayısının fazla olması sebebiyle ağ trafiğinin güvence altına alınması ve yönetilebilmesi için firewall, bulut ortamında entegre edildi. 107 istasyon ve merkezin ağ trafiği, dış tehditlere ve kötü yazılımlara karşı korunaklı hale getirildi.

Şahhoil, Türkiye'nin birçok noktasında hizmet veren istasyonlarını; hizmetini kesintisiz şekilde sunabilmesi ve sistem ile network altyapılarının operasyonel işleyişini güvence altına alabilmesi için Turcom'un 7/24 hizmet veren alanında uzman teknik destek ekibine emanet etti. Turcom'un güçlü ekibi sayesinde, istasyonların herhangi birisinde olası teknik sorunlara hızlı ve etkili bir şekilde müdahale edilebilmesinin güvencesini yaşıyor.

Şahhoil'in Mersin'de bulunan merkez ofisinin internet bağlantısı ise, her sektörün telekominikasyon ihtiyaçlarına cevap veren Turcom'un internet ve network sağlayıcı firması Telnet Telekom tarafından sağlandı. Sağlanan fiber metro ethernet bağlantısı sayesinde kesintisiz hız kaybı olmayan internete kavuşmuş oldular.

SİBER GÜVENLİKTE YAPAY ZEKÂ PROBLEM DEĞİL, BİR ÇÖZÜMDÜR

AI (Yapay Zeka) / ML (Makine Öğrenimi) son zamanlarda, hayatımıza giren en kötü şeylerden biri olarak resmediliyor. Bu yazımda; yapay zekânın doğru bir amaçla kullanıldığında, geleceğe daha çok katkı ve fayda sağlayacağını ve bu sebeple iyi taraflarını ele alıp sizlerle paylaşmayı düşünüyorum.

Trellix

Yuval Noah Harari'nin yazdığı gibi, 10.000 yıl önce buğday insanları evcilleştirdi. Şimdi yeryüzünde 8 milyar insan olmamızı sağlayan buğdayın tadını çıkarıyoruz. Ancak bunun oluşması için insanoğlu olarak bir bedel ödememiz gerekti. Gelecekte de yapay zekâyı benzer şekilde, hayatımızı kolaylaştıran ama bağımlılık yaratan bir devrim olarak mı göreceğiz?

Yapay zekânın hayatımıza getirdiği risklerle başa çıkmayı kendimce üç yolda anlatmaya çalışacağım. Bunları başlıklandıracak olursak birincisi; "Teknolojiyi benimsemek", ikincisi "Karşı çıkmak" ve üçüncüsü ise "Onsuz yaşamak için bir plan oluşturmak"

TEKNOLOJİYİ BENİMSEMEK

Sahip olduğunuz teknolojiyi korumak için elinizden geleni yapmalısınız. KVKK ve GDPR kapsamında yıllardır müşterilerimizde konumlandırdığımız ve kullanıcıların hassas bilgilerinin kurum dışına çıkmasını engellemeye yardımcı olan DLP (Veri Sızıntısı Önleme) çözümü buna iyi bir örnektir. DLP çözümüne ve Google Translate ve diğer 3. parti çözümlere ek olarak; ChatGPT motorlarıyla yapılmak istenen sızıntıya karşı korunmaya da yardımcı olabilir. Siber güvenlik alanında, yapay zekâ teknolojisini tehditlere karşı korumak gittikçe daha da zorlaşıyor. Çünkü yasadışı yöntemler kullanan kötü niyetli bir düşmana karşı çalışıyoruz. Belirli örnekler için NIST (Ulusal Standartlar ve Teknoloji Enstitüsü), Microsoft, MITRE ve Trellix'in tehdit raporlarına hatta son OWASP (Açık Web Uygulaması Güvenlik Projesi) yayınlarına bakmanızı şiddetle tavsiye ederim. Herkes için çok ciddi bir uyarıda bulunmak istiyorum. Bu zamana kadar iki adet "yapay zekâ kışı" geçirdik. Eğer üçüncü bir yapay zekâ kışı daha yaşarsak, satın alıp kullanmadığınız teknolojilerinizi, korumak için yapılan tüm yatırımlar gereksiz hale gelecektir.

TEKNOLOJİYE KARŞI ÇIKIN

Günümüzde en korktuğum ve başarısız olduğum insanlar ise Luddite (otomasyona karşı çıkan kimse) gibi olan ve her yeniliğe karşı çıkanlardır. Teknolojinin getirdiği avantajları ortadan kaldıracak bir çok yeni regülasyona uyanıyoruz bu günlerde. Bu sebeple yayınlanan YAPAY ZEKÂ HAKLAR BİLDİRGESİ şöyle diyor: "Otomatik sistemler, sizin ya da toplumunuzun güvenliğini tehlikeye atma niyetiyle ya da makul ölçüde öngörülebilir bir olasılıkla tasarlanmamalıdır." Bu muhalefet sadece askeri kullanımı değil, aynı zamanda otonom sürüşü ve hatta insan ölümlerine neden olduğu bilinen otomatik asansörleri de yasaklayacaktır. Fakat siber güvenlik alanında, aşırı düzenleme ve uyumluluk kuralları, kötü aktörlerin yapay zeka teknolojisini hain amaçlar için kullanması sorununu çözmeyecektir.

ONSUZ YAŞA

Çok katı ve tutucu Hristiyan mezhebi Amişlerin yaptığı gibi, teknoloji olmadan yaşayabilmek için bir yedek plan oluşturun. Birisi elektriği kaybedebileceğimizden korkuyorsa (Nükleer savaş / EMP (Elektro Manyetik Darbe)) bu yol bir denge olabilir. O zaman manuel yedekleme prosedürlerine sahip olmak umut verici bir fikirdir. Amişlerin teknolojiyi reddetmesine katılsanız da katılmasanız da, bir anlamda bazı felaketlere karşı bir sigorta poliçesi gibidirler. Açıklığa kavuşturmak için: Amişler nükleer silahlara karşı korunmuyorlar, ancak tüm elektronik cihazları yok edecek bir EMP'nin yıkıcı etkisinden daha az etkileniyorlar.

Duyduğumda çok şaşırdığım bir bilgi de; Google'ın son çıkardığı yapay zeka robotu Bard, Avrupa'da hiç kimse tarafından kullanılmaması. Hatta dalga konusu olmuştu. Bazı AB (Avrupa Birliği) düzenlemeleri yüzünden Avrupalılardan daha fazla penguenin, Google Bard'ı kullanabilmesine olanak sağlamıştı. Bu düzenlemeler, Amiş benzeri bir ortam yaratılmasına yol açabilir. "Eski" teknolojiyi kullanmaya çalışsanız bile, ChatGPT tarafından oluşturulan kimlik avı saldırıları gibi yapay zekâ saldırganlarına karşı hala savunmasızsınız. Örneğin, teknoloji tarafından gözetlenmekten kaçınmanın yaygın bir yolu devre dışı kalmaktır. Sektörümüzden bir örnek vermek gerekirse, bazı siber güvenlik üreticilerinin; yüzde yüz güvenlik iddiaları ve hacklenme olayı gerçekleştiğinde para ödeme taahhütleri mevcut. Bunun nasıl mümkün olduğunu sorduğunuzda ise Iphone marka bir telefonu tuşlu telefon tarzında kullandığımızda ancak para iadesi yapacaklarını söylüyorlar :)

KONUK YAZAR

TAYFUN ER
TRELLIX TÜRKİYE VE AZERBAYCAN BÖLGE SATIŞ MÜDÜRÜ

> **GÜNÜMÜZDE EN KORKTUĞUM VE BAŞARISIZ OLDUĞUM İNSANLAR İSE LUDDITE (OTOMASYONA KARŞI ÇIKAN KİMSE) GİBİ OLAN VE HER YENİLİĞE KARŞI ÇIKANLARDIR.**

Yukarıdaki tüm zorluklar kendi çapında hayatımızı ve kurumlarımızı etkileyen çok önemli unsurlardır. Biz Trellix şirketi olarak şu anda hepsini tamamen çözemeyebiliriz. Ancak sektöründe lider bir siber güvenlik şirketi olarak birçok çözüm sunabilir durumdayız.

Özetlemem gerekirse; yapay zekânın kendimce bir sorun olmadığına inanıyorum. Hatta siber güvenlik sektörü için bir çözüm olduğuna inancım sonsuz. Trellix, onlarca yıldır gelişmiş yapay zekâ ve makine öğrenimi içeren araçlar kullanıyor. Bu nedenle eminim ki yukarıdaki zorlukları da yapay zekâ ve insan gücü birlikteliği ile harmanlayıp gelişmiş çözümlerle sonuçlandırabiliriz.

trcSPOT: trcSPOT

PAYLAŞIMLI İNTERNETTE GÜVENLİ VE KÂRLI BİR DENEYİM...

Kurumlar, güvenli internet erişimi sağlayarak ziyaretçi ve çalışanlarıyla kurdukları bağlantıları, avantajlı bir iş platformunda değerli bir deneyime trcSpot ile dönüştürüyor.

Turcom'un yenilenen trcSpot çözümünü tercih eden kuruluşlar, 5651 gibi yasal düzenlemelerin getirdiği internet trafiği kayıt zorunluluğunu, bir avantaj platformu olarak tasarlayabiliyor.

Bugün tüm kişisel ve iş süreçlerimizi akıllı cihazlarımız üzerinden internet vasıtasıyla gerçekleştiriyoruz. Dolayısıyla internete her yerden kesintisiz şekilde erişilir olması modern yaşamın olmazsa olmazları arasındadır.

Kablosuz internet erişim teknolojisine yönelik gelişmeler neticesinde havalimanlarından stadyumlara kadar yoğun ortamlarda halka açık Wi-Fi kullanımı yaygınlaştırmıştır. *2018'de 169 milyon olan erişim nokta sayısı, günümüzde dört katına çıkmıştır.

Örneğin; 2023 yılına kadar perakende sektörü, en çok Wi-Fi erişim noktasına sahipken, en hızlı artışı sağlık sektörünün yaşayacağı öngörülmektedir. Buna göre sağlık kampüslerindeki erişim noktalarının üç katına çıkacağı düşünülmektedir. Hastanelerdeki Wi-Fi, hem sağlık hizmetlerini ve personel verimliliğini artırmak, hem de hastalar ile ziyaretçilere internet erişimi sağlamak amacıyla kullanılmaktadır.

Kaynak: Maravedis, Cisco Yıllık İnternet Raporu, 2018–2023

İNTERNET ERİŞİMİNİZİ İŞ AVANTAJINA ÇEVİRİN

Günümüzde toplu alanlarda yönetilebilir internet erişimi sağlamak lüks değil, bir zorunluluk… Bu zorunluluğu bir adım öteye taşıyarak, interneti sağlayanlar için de bu bağlantı deneyimini güvenli, yönetilebilir ve raporlanabilir hale getirmek ve avantajlı iş sonuçları yaratmak önemlidir.

Toplu internet erişiminin oluşturulduğu alanlarda, hızlı ve güvenilir internet kullanımı, trcSpot sayesinde erişim sağlayıcılar açısından bir yük olmaktan çıkmaktadır. Böylece toplu erişim servisi, kuruluşlar için avantajlar sağlayan ve kolayca yönetilebilen bir platforma dönüşür.

trcSPOT NEDEN TASARLANDI VE NE İŞE YARAR?

trcSpot, yalnızca topluca internet erişimi mümkün kılan ve 5651 no'lu kanuna uygun olarak internet trafiğini kayıt altına almak amacıyla oluşturulmuş bir araç değil, aynı zamanda kullanıcının ihtiyaçlarına özel olarak şekillenen ve onlara benzersiz deneyimler sunan bir iş platformudur.

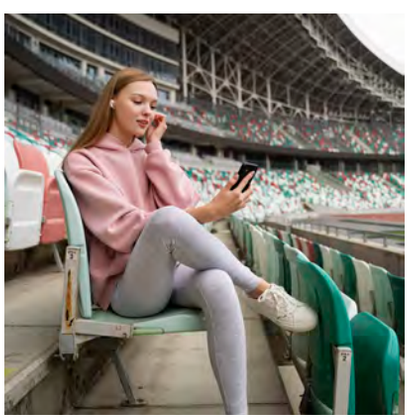
Güvenli kablosuz haberleşme ve kablosuz ağ kontrol sistemleri ile donatılan trcSpot, kimlik doğrulama ve yüksek performanslı internet erişimini birleştirerek, kablosuz bağlantı deneyimini bir adım daha öteye taşıyan öncü bir çözümdür.

İŞLETMELERE DEĞER KATAN, FARK YARATAN ÖZELLİKLER

Mevcut çözümler, kullanıcı beklentilerini tam anlamıyla karşılamakta yetersiz kalırken, trcSpot bu boşluğu doldurmak amacıyla tasarlandı. Bulut teknolojisinin gücünden faydalanarak geliştirilen trcSpot, Wi-Fi erişim noktası yönetimindeki karmaşıklıkları ortadan kaldırır ve global hotspot roaming'den özelleştirme esnekliğine kadar bir dizi özellik sunar.








Donanım Bağımsızlığı:

trcSpot, marka ve cihaz ayrımı yapmaksızın kolayca mevcut ağ yapınıza entegre olur.

Esnek Kimlik Doğrulama:

Dinamik MFA teknolojisi ile çok faktörlü kimlik doğrulama imkânı sunar.

Kullanıcı Dostu Erişim:

Farklı lokasyonlarda bile kullanıcıyı "hatırlayan" algoritması ile yeniden kimlik doğrulama işlemi gerektirmez.

Kullanıcıyı "Hatırlayan" Erişim ile İş Hacmini Artırmak:

Bu sistem, bağlantı alanında kalan kullanıcıları yer değiştirseler dahi unutmaz. Kuruluşlar için;

1. İnternet pazarlaması,
2. Müşteri veri tabanı oluşturmak,
3. Satış geliştirme ve lead yaratmak,
4. Anlık memnuniyet ve anket uygulamaları yapmak,
5. Hızlı bilgilendirme ve hatırlatmalar yapmak,

mümkün hale gelir. Böylece kullanıcılar ile aranızda memnuniyete dayalı bir köprü oluşur.

Örneğin; havaalanındaki son bekleme alanında hotspot noktasına bağlanan bir kullanıcı, uçağını beklerken alışveriş noktalarında ona özel kişiselleştirilmiş kampanyalarla karşılaşabilir. Sabah uçağını bekleyen bir yolcuya kahve indirimi yapmak ya da "Kahvenin yanında çöreğiniz bizden" gibi alternatifler sunmak mümkündür. Otel kompleksinizdeki bir kullanıcıya "ala carte" restoranınızda ya da SPA alanınızda o geceye özel teklifler sunabilirsiniz. Hastane internetine bağlı olan bir çalışana anlık notlar ile katılması gereken toplantıları veya uyulması gereken prosedürleri hatırlatabilirsiniz. Tüm bu örnekler, AVM'ler, kafeler ve üniversiteler için de geçerlidir.

Geçici Hotspot Oluşturma:

trcSpot, belirli bir ihtiyaç doğrultusunda geçici hotspot sistemleri kurma olanağı sunar.

Detaylı Raporlama:

Esnek raporlama algoritması ile kullanıcılar, geçmiş internet kullanım verilerine ve analizlere kolaylıkla erişebilir.

İnternet Trafiğinin Yasal Denetimi ve Kaydına Esnek Uyumlanma:

trcSpot, zararlı içeriklere ve istenmeyen erişimlere karşı önlem alarak internet trafiğini denetler. Türkiye'deki 5651 no'lu yasa gibi, farklı ülkelerin denetim yasalarına esnek şekilde uyum sağlar ve gereken kayıtları tutar.

Global Hotspot Roaming:

OpenRoaming yaklaşımı ile kullanıcılara küresel ölçekte kesintisiz ve güvenli Wi-Fi erişimi imkânı tanır.

Bulut Entegrasyonu: Bulut teknolojisinin avantajlarından yararlanarak, merkezi erişim noktası dolaşım yetenekleri ve kusursuz entegrasyon sunar.

Sürekli ve Güvenli Bağlantı: trcSpot, kullanıcılara kesintisiz internet erişiminin yanı sıra güvenli bir deneyim sunar. Yasal loglama ve imzalama yapısının yanında, gerektiğinde VPN erişim imkânı da sağlar.

Kullandığın Kadar Öde, Ödediğin Kadar Kullan: Sistem, kullanıcıların sadece kullandıkları kadar ücret ödemelerini sağlar. Bu, kuruluşlara sahip olma, bakım ve güncelleme maliyetlerinde avantaj sunar.

Özellikler	trcSpot	Diğerleri
Donanım Bağımsızlığı	✓	Hayır
API Entegrasyonu	✓	Sınırlı
Dinamik MFA	✓	Hayır
Roaming Kimlik Doğrulama	✓	Hayır
Geçici Hotspot	✓	Sınırlı/Hayır
Esnek Raporlama	✓	Sınırlı

Kolay ve Etkin Kullanım: trcSpot, kullanıcı dostu arayüzü sayesinde hızlı ve kolay bir kullanım deneyimi sunar. Farklı cihazlarda ayrı ayar gerektirmez ve sosyal medya ile e-posta entegrasyonları ile geniş bir deneyim sağlar.

Bu özellikler sayesinde trcSpot, toplu alanlarda internet erişiminin sadece bir gereklilik olmaktan çıkıp, aynı zamanda işletmelere değer katan bir hizmet haline gelmesini sağlamaktadır.

GELECEĞİN İNTERNET DENEYİMİNİ BUGÜNDEN KEŞFEDİN!

trcSpot, sizin ve işletmenizin ihtiyaçlarına mükemmel şekilde uyum sağlayarak sadece bir bağlantı noktası olmaktan çok daha fazlasını sunar. Güvenli, yüksek performanslı internet erişimi, özelleştirme esnekliği ve kolay kullanımı bir araya getirerek adeta dijital bir devrim yaratır. İster ofisinizde ister otelde, ister AVM'de, ister havaalanında olun; trcSpot ile geleceğin internet deneyimini bugünden keşfedin ve işletmenizi bir adım öne taşıyın. Beklemeyin, hemen geçiş yapın!

Demo talepleriniz veya ayrıntılı bilgi için kodu okutarak bize ulaşabilirsiniz.

FESTO, TURPRO İLE YENİ ÜRETİM DEVRİNİ BAŞLATTI

FESTO

Dünyanın sayılı otomasyon ve teknik çözümler üreticisi Festo, Manisa'daki yeni üretim tesisindeki bilgi işlem altyapısının kurgulanması ve kurulumu projesinde Turpro'ya güvendi.

Festo, 1925 yılında Almanya'da kurulmasından bugüne kadar geçen süre içerisinde fabrika otomasyon teknolojisi alanında dünya liderliğini koruyor. 176 ülkede, 300.000'den fazla endüstriyel müşterisiyle oldukça geniş bir portföye hitap eden Festo, Manisa Organize Sanayi Bölgesi'nde yeni bir üretim fabrikasını devreye almasıyla doğan teknolojik altyapı ihtiyaçları için birkez daha Turpro'nun güçlü ve deneyimli ekibine güvendi. Başarıyla tamamlanan projenin ardından fabrika, dünya çapındaki en büyük tesisler arasında yerini aldı.

FESTO, TÜRKİYE'DE ÜRETİME BAŞLADI

Üretim kapasitesi yüksek ve müşteri çeşitliliği fazla olan şirketlerin, üretimi ya da iş süreçlerini kesintiye uğratabilecek faktörlere karşı birçok önlem ve eylem planı olması hayati önem taşır.
Bu şirketlerden biri olan Festo, Ukrayna'da bulunan fabrikasını, üretim sürecini güvence altına almak adına stratejik planlamalarının bir hamlesi olarak Türkiye'ye taşımaya karar verdi.

Manisa Organize Sanayi Bölgesi'nde konumlandırılan ve %70 Türkiye kaynaklı üst düzey teknolojik sistemlerin kullanıldığı yeni fabrikada imalat, montaj, otomasyon ile proses bir arada yürütülüyor.

Böylece tek bir noktadan müşterilerin ihtiyaçlarına global düzeyde cevap verilebilen bir üretim tesisi hayata geçirilmiş oldu.

TURPRO'NUN UZMANLIĞI

Genel merkezi Almanya'da bulunan Festo, fabrikanın Türkiye'de faaliyete geçmesi kararının ardından kurulumu için gereken network ürün ve çözümlerin tedariğini yine Almanya'dan sağlanması yerine Turpro'yu tercih ederek proje çok daha hızlı ve ekonomik bir şekilde tamamlandı.

30 yılı aşkın saha tecrübesi ile Turpro ekibi, Festo'nun yeni fabrikasının tüm network altyapı projesini kurgudan kuruluma kadar titizlilikle planlayarak uygulamaya aldı.

Turpro ekibi & Festo ekibi iş birliği ile projenin aşamaları belirlendi. Öncelikli olarak fabrikanın network kablolama planı çıkarıldı. Fabrikanın üretim operasyonu sürecinde kullanılan makinelerin yerleşim planı baz alınarak network dağıtım yerleri oluşturuldu.

Dağıtım yerlerinin konumlandırılmasının ardından bilgi işlem altyapısında bakır kablo tercih edilerek düşük maliyetle birçok noktaya erişilmiş oldu. Fabrika içerisindeki kablosuz erişim ise konumlandırılan 34 adet access point ile sağlandı ve böylece üretimde hayati olan makineler arası haberleşmenin ilk fazı tamamlanmış oldu.

Personeller arası haberleşmede ise tercih edilen VoIP yazılımının aktif ve güvenli bir şekilde kullanımı için firewall konumlandırılarak iletişim ihtiyacı çözüme kavuşturuldu.

TELNET TELEKOM İLE TEK BİR NOKTADAN HİZMET FARKI

Festo'nın sektördeki en son gelişmeleri takip ederek rekabet avantajı ilkesi doğrultusunda kurulan fabrika,akıllı üretim hatları ile donatıldı. Nesnelerin İnterneti (IoT) teknolojisiyle üretim standardını en üst seviyeye çıkaran Festo, tesisin hayati faaliyetlerini sürdürebilmesi için internet olmazsa olmazdı.

Turcom'un internet servis sağlayıcısı Telnet Telekom, fabrikada network altyapısının kurulmasının ardından internet ve yedek internet erişimini sağlamasının ardından üretim için gereken ortam sağlanmış oldu.

Oldukça modern üretim teknolojilerinin kullanıldığı ve "akıllı fabrika" statüsündeki bu fabrikada, tüm makinelerin aralıksız faaliyet gösterebilmesi için internet erişiminin kesintisiz olması gerektiğinden internet erişimi karasal ve radyolink olarak iki şekilde sağlandı. Karasal yayında kesinti olması durumunda otomatik olarak radyolink yayına geçecek şekilde yedeklenerek üretim sürekliliği garanti altına alınmış oldu.

Telnet Telekom; üretim tesisinde iki türde internet erişimi sağlanan Festo'nun arka planda tüm işlemlerini takip ediyor ve oluşabilecek arıza durumunda 7/24 ulaşılabilir çağrı merkezi kadrosuya operasyonel kolaylık sağlıyor. Telnet Telekom'u tercih eden Festo, internet kesintisi sebebiyle oluşabilecek üretim aksaklıklarını minimuma indirirken, tek bir noktadan hizmet alarak çok yönlü iş süreci yönetiminde zaman kazanmış oldu.

ARZU DERBENT AKKAYA ANLATTI:
SİBER GÜVENLİĞİN GÜÇLÜ OYUNCUSU

Fortinet Türkiye, Azerbaycan, Gürcistan, Türkmenistan, Ermenistan Bölge Direktörü Arzu Derbent Akkaya konuğumuz oldu.

ARZU DERBENT AKKAYA
TÜRKİYE, AZERBAYCAN, GÜRCİSTAN, TÜRKMENİSTAN, ERMENİSTAN BÖLGE DİREKTÖRÜ

FORTINET VE GLOBAL PAZAR: FORTINET GLOBAL TEKNOLOJİ PAZARININ HANGİ ALANINDA YER ALAN BİR OYUNCU, FORTINET MARKASI TEKNOLOJİ DÜNYASINDA NASIL KONUMLANIYOR KISACA ÖZETLER MİSİNİZ?

Fortinet, 20 yılı aşkın bir süredir siber güvenliğin evriminde ve ağ ile güvenliğin yakınsamasında itici bir güç olmuştur. Güvenlik çözümlerimiz sektördeki en yaygın, patentli ve onaylanmış çözümler arasında yer alıyor. Şirketlerin satıcıları ve özel amaçlı ürünleri konsolide etme arayışları artarken biz de önde gelen bir siber güvenlik platformu ve güvenli ağ satıcısı olarak, Fortinet'i güçlü uzun vadeli büyüme için konumlandırmaya devam ediyoruz. Hem SD-WAN hem de OT'de en büyük pazar payı liderlerinden biriyiz ve 2023'te toplam 122 milyar dolarlık bir toplam adreslenebilir pazara sahip olan Güvenli Ağ, Konsolide Siber Güvenlik Dokusu, Hibrit Bulut Güvenliği ve Operasyonel Teknoloji gibi kilit uzun vadeli büyüme pazarlarımıza odaklanmaya devam edeceğiz. Fortinet, birçok sektörde her ölçekten 680.000'den fazla kuruluştan oluşan küresel bir müşteri tabanına sahip. Fortinet, 20 yılı aşkın bir süredir siber güvenliğin evriminde ve ağ ile güvenliğin yakınsamasında itici bir güç olmuştur. Güvenlik çözümlerimiz sektördeki en yaygın, patentli ve onaylanmış çözümler arasında yer alıyor. Şirketlerin satıcıları ve özel amaçlı ürünleri konsolide etme arayışları artarken biz de önde gelen bir siber güvenlik platformu ve güvenli ağ satıcısı olarak, Fortinet'i güçlü uzun vadeli büyüme için konumlandırmaya devam ediyoruz. Hem SD-WAN hem de OT'de en büyük pazar payı liderlerinden biriyiz ve 2023'te toplam 122 milyar dolarlık bir toplam adreslenebilir pazara sahip olan Güvenli Ağ, Konsolide Siber Güvenlik Dokusu, Hibrit Bulut Güvenliği ve Operasyonel Teknoloji gibi kilit uzun vadeli büyüme pazarlarımıza odaklanmaya devam edeceğiz. Fortinet, birçok sektörde her ölçekten 680.000'den fazla kuruluştan oluşan küresel bir müşteri tabanına sahip.

FortiGuard Labs, Mayıs 2023'te *Big Head* fidye yazılımının yeni varyantları olduğunu ortaya çıkardı. Big Head fidye yazılımı örneklerinin çoğu Amerika Birleşik Devletleri'nden gönderilmiş olsa da aynı saldırgan tarafından kullanılan bir başka fidye yazılımının Türkiye dahil olmak üzere birçok ülkeden yollandığı görülüyor. FortiGuard Labs, Big Head fidye yazılımının A ve B varyantları olarak adlandırılan en az iki varyantını tespit etti.

TÜRKİYE'NİN KARŞILAŞTIĞI SİBER TEHDİTLER

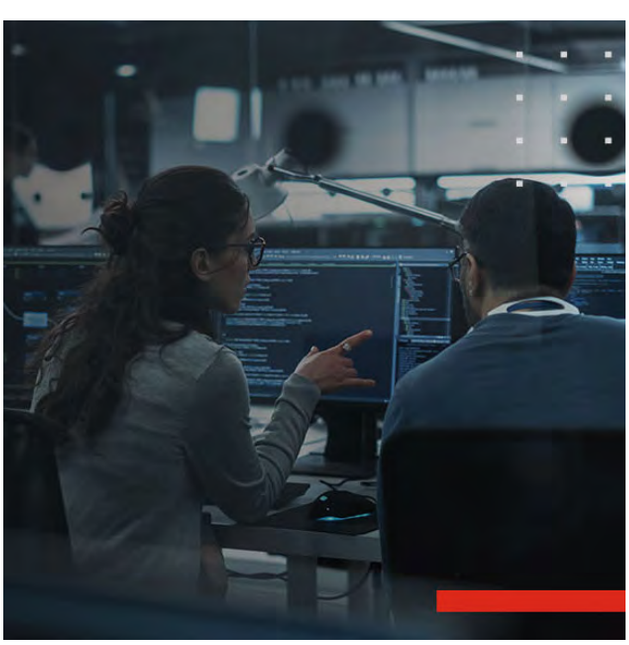
TEHDİTLERE KARŞI FORTINET ÇÖZÜMLERİ

Fidye yazılımlarının çoğu genellikle oltalama yoluyla iletiliyor. Fortinet çözümlerinden biri olan FortiPhish Kimlik Avı Simülasyon Hizmeti, kurumların kimlik avı tehditlerine karşı kullanıcı farkındalığını ve dikkatini test etmesine ve kullanıcılar hedefli kimlik avı saldırılarıyla karşılaştığında doğru uygulamaları eğitmesine ve pekiştirmesine yardımcı olmak için gerçek dünya simülasyonlarını kullanıyor.

Kurumların, gelişen ve hızla artan fidye yazılımı riskiyle etkin bir şekilde başa çıkabilmeleri için veri yedeklemelerinin sıklığı, konumu ve güvenliği konusunda temel değişiklikler de yapmaları gerek. Riski en aza indirmek ve başarılı bir fidye yazılımı saldırısının etkisini azaltmak için ağ dışı cihazları korumak için SASE gibi bulut tabanlı güvenlik çözümleri; kötü amaçlı yazılımı saldırının ortasında engelleyebilen EDR (uç nokta algılama ve yanıtlama) çözümleri gibi gelişmiş uç nokta güvenliği ve politika ve bağlama dayalı olarak uygulamalara ve kaynaklara erişimi kısıtlayan Zero Trust Access-Sıfır Güven Erişimi ve ağ segmentasyonu stratejilerinin tümünün araştırılması gerekiyor.

Fortinet olarak bu noktada şöyle yardımcı oluyoruz: Güvenlik ekosisteminizde yerel sinerji ve otomasyon sağlayan sektörün önde gelen tam entegre Security Fabric'in bir parçası olarak, geniş bir teknoloji ve insan tabanlı as-a-service teklifleri portföyü sunuyoruz. Bu hizmetlerimiz, deneyimli siber güvenlik uzmanlarından oluşan küresel FortiGuard ekibi tarafından destekleniyor.

FortiGuard AntiVirus hizmeti FortiGate, FortiMail, FortiClient ve FortiEDR tarafından destekleniyor. Güncel



AntiVirus güncellemelerini çalıştıran Fortinet EPP müşterileri de korunuyor. FortiGuard Labs'ın Acil Durum Olay Müdahale Hizmeti, bir olay tespit edildiğinde hızlı ve etkili müdahale sağlıyor. Olaya Hazırlık Abonelik Hizmeti ise hazırlık değerlendirmeleri, IR oyun kitabı geliştirme ve IR oyun kitabı testi (masa başı tatbikatları) yoluyla bir siber olaya daha iyi hazırlanmanıza yardımcı olacak araçlar ve rehberlik sağlıyor.

Benzersiz açıklar artıyor: FortiGuard Labs, 2023'ün ilk yarısında, beş yıl öncesine göre %68 artışla 10.000'den fazla benzersiz açık tespit etti. Zararlı yazılım aileleri ve türevleri sırasıyla %135 ve %175 artarak patlama yaptı.

YAPAY ZEKÂ VE FORTINET: SİZCE YAPAY ZEKÂ İLE WEB GÜVENLİĞİ SAĞLANABİLİR Mİ?

Fortinet'in yapay zekâ ile bütünleşmiş çözümleri var mı? Bu alandaki gidişat hakkında neler söylemek istersiniz?

Hızla genişleyen saldırı yüzeyini hızlanan siber tehditlere karşı güvence altına almak isteyen kurumların, entegre bir siber güvenlik platformunun merkezinde yapay zekadan [AI] yararlanan siber güvenlik çözümleri kullanması gerekiyor.

Fortinet yıllardır yapay zeka ve makine öğrenimi inovasyonunun ön saflarında yer alıyor. Ürünlerimizi ve güvenlik hizmetlerimizi güçlendirmek için tasarladığımız, eğittiğimiz ve patentini aldığımız derin öğrenme ve yapay sinir ağlarından yararlanıyoruz. Bu yaklaşım, portföyümüz genelinde tutarlı yapay zeka ile geliştirilmiş hizmetleri genişleterek daha hızlı, daha güçlü ve daha doğru müşteri savunmaları sağlıyor.

Yapay zeka destekli ilk kullanım örneklerimizden biri sanal FortiGuard tehdit analistinin tanıtılmasıydı. Gelişmiş makine öğrenimini kullanarak, koordineli koruma sağlarken tehditleri gerçek zamanlı tespit edebiliyor ve her yeni tehdit tanımlandığında savunma imzalarını otomatik olarak güncelleyen tehdit istihbaratı oluşturabiliyor.

Ayrıca platformumuz günde 100 milyardan fazla olayı alıp analiz ediyor ve Fortinet Security Fabric ve ekosistemi genelinde günde bir milyardan fazla güvenlik güncellemesi sunuyor. Rakiplerimizin çoğu güvenlik istihbaratını farklı güvenlik tedarikçilerinden alırken, yapay zeka odaklı FortiGuard Tehdit İstihbaratımız şirket içinde oluşturuldu ve yapay zekayı farklı kaynaklara tutarlı bir şekilde uygulayarak nasıl ve nerede kullanılabileceğinin kapsamını ve ölçeğini genişletmemizi sağlıyor.

YÖNETİLEN HİZMETLERİN GELECEĞİ: SİSTEM VE AĞ İZLEME SEKTÖREL ÖRNEKLER

Dijital dönüşüm, şirketlerin kurumsal teknolojilerine yönelik altyapı karmaşıklığını artırırken, bu altyapıları oluşturan sistem ve ağların yönetimi için yeni ihtiyaçlar doğurdu. Bu teknolojik altyapılar, kurumların iş süreçleri ve global kriterlere göre belirlenmiş SLA'lere uygun olarak gözlenmelidir. Sistem kesintisizliği ve performansı için uyarı ve müdahale mekanizmaları gibi bir dizi hizmetle yönetilmelidir. Peki bu evrilen manzara karşısında bizi ne tür bir yol haritası bekliyor?

Modern işletmeler, yönetilen hizmetlere ihtiyaç duyduklarında, tüm yapıyı etkin bir izleme ve müdahale yeteneği sunan yazılım araçlarıyla tarama ve görselleştirme yapmalıdır. Bilişim ya da sistem entegrasyonu konusunda uzman olmayan şirketlerin bu teknolojiye ve insan kaynağına sahip olması zor. Bu nedenle yeni nesil entegratörler, bu kaynak ve yeteneklere sahip olan firmalar tarafından desteklenmelidir.

Fiziksel Sunucu Altyapısı:

1. Fiziksel sunucuların güncel durumu
2. Temel donanım sağlık göstergeleri
3. Disk ve depolama ünitelerinin genel sağlık durumu
4. Ana kaynak kullanım bilgileri
5. Zamana bağlı trend gösteren grafikler
6. Anlık ağ trafiği analizi

Sanallaştırma Altyapısı:

1. Sanal sunucuların güncel durumu
2. Donanımın genel sağlık göstergeleri
3. Disk ve depolama ünitelerinin sağlık durumu
4. Ana kaynak kullanım bilgileri (CPU, RAM, DİSK hızları gibi)
5. Data okuma ve yazma hızlarını gösteren metrikler
6. Zaman serileri için trend grafikleri
7. Anlık ağ trafiği analizi

ONUR KÖKSAL AKÇACIK
SİSTEM VE AĞ UZMANI

Kablolu ve Kablosuz Ağlar İçin Güvenlik İzleme:

1. Ağ cihazlarının genel durumu (fiziksel ve lojistik)
2. Switch ve router cihazlarının ICMP yanıt süreleri
3. Uplink arayüz kullanımları
4. CPU ve bellek kullanım oranları
5. Port kullanım bilgisi ve yükleme/indirme durumu
6. Detaylı arayüz durumu bilgileri
7. Belirli zaman dilimleri için kaynak kullanım grafikleri
8. Olaya özgü müdahale önerileri
9. Kat planı bazında izleme yeteneği

Bu yetenekler, işletmelere altyapıları sürekli gözlem altında tutma ve potansiyel sorunlara hızla müdahale etme olanağı sunar.

YENİLİKÇİ TEKNOLOJİLER YÖNETİLEBİLİR HİZMETLERDEN NASIL FAYDA SAĞLAR?

IoT'nin (Nesnelerin İnterneti) yükselmesi, ağ trafiğini yoğunlaştırıyor. İzleme hizmetleri, fiziksel sunucu ve sanallaştırma platformlarını derinlemesine analiz ederken,

Turcom uzmanları bu analizlere dayanarak karmaşık yapıları hızla değerlendirme yeteneğine sahiptir. İşletmeler, IoT yatırımlarını kesintisiz sürdürmek istiyorlarsa, Turcom NOC'un izleme ve müdahale servisleri büyük fırsatlar sunar.

Ayrıca IoT'un bir başka yüzü olarak, akıllı şehirlerdeki trafik yönetimi, enerji tüketimi izleme, acil sağlık, güvenlik, orman yangını sistemleri (112 vb) ya da atık yönetimi gibi alanlarda kullanılıyor olması. Böylece kent yaşamları daha sürdürülebilir ve etkili hale geliyor.

Sektörel Uygulama: Sağlık

Modern hastaneler artık sadece tedavi merkezi olmanın ötesinde, teknolojik ilerlemenin merkezlerinden biri haline geldi. Tıbbi cihazların ağ üzerinden sürekli izlenmesi, hasta takip sistemlerinden tıbbi görüntüleme cihazlarına kadar geniş bir yelpazeyi kapsıyor. Turcom izleme araçları ile cihazlardan gelen veri anında analiz edilerek olası sitem arızaları veya anormallikleri saptanabiliyor ve önlemler alınabiliyor.

HİBRİT BULUT YAPILARI VE YÖNETİLEBİLİR SERVİSLER

Kurumlar sadece kendi iç ağlarını izlemekle kalmıyor, bulut altyapılarında da bu ihtiyacı duyuyorlar. Hibrid bulutun yükselişi, farklı yapılardaki veriyi tek bir panelde toplama gerekliliğini ortaya koyuyor. İşte tam da burada Turcom'un sistem izleme çözümleri devreye girebiliyor.

Bu yapılarda, özellikle büyük veri analitiği gibi yoğun veri işlemleri için ölçeklenebilirlik sağlamak esas olduğu için hibrid bulut yapıları, bu ölçeklenebilirliği sunarken aynı zamanda veri güvenliği ve gizlilik gereksinimleri için yapıların izlenerek yönetilmesi önemli hale geliyor.

Sektörel Uygulama:

Dünya da finans kuruluşlarının önemli bir kısmı, hibrit bulut yapısını hızla benimseyerek hem iç ağlarını hem de bulut altyapılarını izleme konusunda desteğe ihtiyaç duyar hale geldiler. Bu, özellikle finansal işlemlerin kesintisiz ve güvenli bir şekilde gerçekleşmesi için kritik bir öneme sahip.

YÖNETİLEBİLİR HİZMETLERİN SİBER GÜVENLİKLE BİRLEŞİMİ

Siber tehditlerin artışı, şirketler için ciddi bir risk oluşturuyor. Yönetilen hizmetlerin izleme kapasitesi, bu tehditleri önceden tespit ederek erken müdahalede bulunma olanağı sunar.

Sektörel Uygulama: E-Ticaret

E-ticaret platformları, kullanıcının kişisel ve finansal bilgilerini barındırır. Bu platformlar için siber güvenlik tehditleri, maddi zararın ötesinde marka itibarına da zarar verebilir. Önceden tespit edilen güvenlik tehditleri sayesinde, olası saldırılar engellenir.

Otomasyonun Gücü

Sistem ve ağ izlemenin ötesinde, çağımızda otomasyon da iş ve üretim süreçlerinde kritik bir rol oynuyor. Tespit edilen sorunlara anında müdahale, kesintilerin maliyetini minimize etmek için önemli.

Sektörel Uygulama: Sanayi

Üretim sektöründe kritik role sahip otomasyona yönelik sistemlerin izleme araçları ile gözlenerek, üretim bandındaki makinelerin durumunun anında tespit edilmesi, olası arızalara veya durmalara karşı müdahale senaryolarının oluşturulması önemlidir.

YÖNETİLEN HİZMETLERDE KİŞİSELLEŞTİRME

Her şirketin ihtiyaçları farklıdır. Bu nedenle, yönetilen hizmetlerin kişiselleştirilmesi, şirketlerin kendi stratejilerine ve ihtiyaçlarına uygun hizmet alabilmeleri için kritik bir öneme sahiptir.

Sektörel Uygulama: Eğitim

Sınıflardan laboratuvarlara kadar farklı kaynaklardan gelen verilerin izlenmesi gerekiyor. Özelleştirilebilir izleme araçları sayesinde, bu verilere erişim kontrollü bir şekilde sağlanabiliyor, böylece hem öğrenci bilgileri korunuyor hem de eğitim kalitesi artırılıyor.

Yenilikçi Eğilimler ve Uygulamalar

Endüstri 4.0'ın getirdiği dönüşümle, fabrikalar, makine öğrenimi ve yapay zeka gibi teknolojileri entegre ederek daha akıllı hale geliyor. Bu akıllı fabrikalar, üretim süreçlerini optimize etmek için sistem ve ağ izleme çözümlerini kullanıyor.

Sektörel Uygulama: Enerji ve Petrol

Akıllı şebekeler, enerji tüketimini daha verimli ve sürdürülebilir hale getirmek için gelişmiş izleme sistemlerine ihtiyaç duyuyor. Bu sistemler, enerji dağıtımını optimize ederken olası arızalara karşı da önlem alıyor.

Kritik Süreç ve Katı Regülasyona Tâbi, Dağıtık Yapılarda Yönetilebilir Bilişim Servisleri

Akaryakıt sektörü, sürekli değişen fiyat dinamikleri, karmaşık lojistik süreçleri ve yüksek rekabet ortamı nedeniyle teknolojik ilerlemelere hızla adapte olma ihtiyacı duyar. Yönetilebilir bilişim sistemleri, bu sektörde verimliliği artırmak, operasyonel riskleri azaltmak ve maliyetleri optimize etmek için kritik bir rol oynamaktadır. Özellikle ağ ve sistem izleme, akaryakıt dağıtım istasyonlarının, rafinerilerin ve depolama tesislerinin sürekli ve kesintisiz çalışmasını sağlamak için hayati öneme sahiptir. Yönetilen hizmetlerin geleceği, teknolojik ilerlemelere ve sektörel ihtiyaçlara paralel olarak sürekli değişiyor. Sadece izleme yeteneği değil, bu izlemenin nasıl stratejik bir avantaja dönüştürüleceği, modern iş dünyası için kritik bir sorundur. İşletmeler, dijital dönüşümde sadece teknolojik yatırımlara değil, aynı zamanda bu yatırımların etkin yönetimine odaklanmalıdır.

TÜRKİYE'NİN AKARYAKIT SEKTÖRÜNDE YENİLİKÇİ BİR GÜÇ: HYPCO VE TURCOM'UN ORTAKLIĞI İLE TEKNOLOJİ ODAKLI YOLCULUK

HYPCO VE TÜRKİYE OPERASYONLARI: ENERJİNİN YENİLİKÇİ YÜZÜ

HYPCO Petrolcülük; 50 senelik tarihi ile dünya çapında motorin, benzin, jet yakıtı, LNG, LPG, bitüm gibi geniş bir ürün yelpazesi sunan BB Energy grubunun bir parçası olarak Türkiye'de faaliyet göstermektedir. BB Energy Grubu, küresel pazarlarda dağıtım ağını genişletme stratejisiyle HYPCO Türkiye'nin ticari hacmini artırmaya odaklanmış bir şekilde Türkiye pazarında kalite ve hizmette fark yaratmayı hedefleyerek yoluna devam etmektedir; Hypco Green ve sosyal sorumluluk projeleriyle çevre dostu yaklaşımlarını da güçlendirmektedir.

TEKNOLOJİ VE AKARYAKIT SEKTÖRÜ: DİJİTAL DÖNÜŞÜMÜN ÖNCÜLERİ

Türkiye'nin akaryakıt sektöründe teknolojik yenilikler, operasyonel verimliliği artırmada kritik bir rol oynamaktadır. HYPCO, ERP ve otomasyon sistemlerini entegre ederek iş süreçlerini otomatize etmekte ve böylece sektörde fark yaratmaktadır. Bu teknolojik entegrasyon, EPDK ve diğer resmî kurumlara karşı yükümlülüklerini yerine getirme ve ticaret mekanizmasında doğruluk ve netlik sağlama konusunda büyük önem taşımaktadır. HYPCO, kaliteden ödün vermeyen yaklaşımı ve güvenilir iş ortaklarıyla bu alandaki liderliğini sürdürmektedir.

BAYİ AĞI YÖNETİMİNDE İNOVASYON: PROFESYONEL VE KESİNTİSİZ HİZMET

Profesyonel ve Kesintisiz Hizmet HYPCO'nun bayi ağı yönetimi, profesyonel ekipler tarafından desteklenmektedir. Bu yaklaşım, ticaretin sürekliliği ve güvenilirliğini sağlama açısından hayati önem taşımaktadır. Turcom ile iş birliği içinde yürütülen IT operasyonları, bayi ağının veri akışının güvenli bir şekilde yönetilmesini sağlayarak ticaretin sağlıklı devam etmesine katkıda bulunmaktadır.

HYPCO VE TURCOM İŞ BİRLİĞİ: NETWORK OPERASYON MERKEZİNİN KRİTİK ROLÜ

Network Operasyon Merkezinin Kritik Rolü Türkiye'nin akaryakıt sektöründeki yenilikçi liderlerinden biri olan HYPCO, Turcom ile iş birliği yaparak Network Operasyon Merkezi (NOC) hizmetlerini kullanmaktadır.

Bu kapsamlı hizmetler, sürekli izleme ve anında müdahale yeteneğiyle HYPCO'nun saha ve merkez operasyonlarında etkinliğini artırmaktadır. Küresel pazarda büyüyen NOC hizmetlerinin, artan IT altyapı karmaşıklıkları ve siber tehditlere karşı kritik bir önemi bulunmaktadır. HYPCO'nun bu adımı, sektördeki teknolojik dönüşümü ve iş sürekliliğini öne çıkarmaktadır.

Network Operasyon Merkezleri (NOC), HYPCO ve Turcom gibi iş birliklerinde olduğu gibi, IT altyapılarının güvenilirliğini ve etkinliğini artırmada kritik bir role sahiptir. NOC hizmetlerinin sağladığı temel faydalar şunlardır:

• ***24/7 İzleme ve Anında Sorun Müdahalesi:*** NOC hizmetleri, kesintisiz hizmet sunumu ve sorunlara anında mudahale imkânı sağlayarak, işletmelerin kesinti sürelerini azaltmasına ve potansiyel gelir kayıplarını en aza indirmelerine olanak tanımaktadır.

• ***Pazar Büyümesi ve Talep:*** Küresel network operasyon merkezi pazarının 2025 yılına kadar yaklaşık 21 milyar dolara ulaşması beklenmektedir. Bu büyüme, IT altyapılarının artan karmaşıklığı, siber saldırıların yükselmesi, maliyet optimizasyonu ihtiyacı ve güvenilir, ölçeklenebilir hizmetlere olan talep tarafından desteklenmektedir.

• ***Proaktif Sorun Çözümü ve Güçlendirilmiş Güvenlik:*** NOC hizmetleri, proaktif sorun çözümü ve güçlü güvenlik protokolleri sağlayarak, işletmeleri siber tehditlere karşı korur ve iş sürekliliğini, felaket kurtarma planları ve düzenli veri yedeklemeleriyle garanti eder.

• ***Azaltılmış Kesinti Süresi ve İyileştirilmiş Performans:*** Proaktif ağ izleme, potansiyel ağ sorunlarını önceden tespit ederek, kesinti sürelerini azaltır ve kesintisiz hizmet sunumu sağlar. Bu, ağ performansının iyileştirilmesi, daha hızlı yükleme süreleri ve artırılmış kullanıcı memnuniyetine yol açar.

Özetle, Turcom tarafından HYPCO'ya sunulan NOC hizmetleri, sürekli izleme, proaktif sorun çözümü, optimize performans ve güçlü güvenlik sağlayarak, günümüzün hızlı tempolu ve teknolojik olarak gelişmiş iş ortamında IT altyapılarının operasyonel verimliliğini artırmaktadır.

IT EKİPLERİNİN ÖNCELİKLERİ VE OPERASYONEL STRATEJİLER

HYPCO'nun IT ve Otomasyon ekipleri, sektörün kritik katmanları arasında yer alıyor. Otomasyon birimleriyle sıkı iş birliği yapan IT ekipleri, sistemlerin sürekli ve doğru bir şekilde çalışmasını sağlamanın yanı sıra, otomasyon tarafındaki iş ortağımız ve Turcom uzmanlarının koordineli anlık müdahaleleriyle yapımızın operasyonel verimliliği artırmaktadırlar.

TURCOM İLE İŞ BİRLİĞİ VE GELECEK HEDEFLERİ

HYPCO, Turcom ile gerçekleştirdiği iş birliği sayesinde bayi ağının yönetimi ve destek hizmetlerini et- kin bir şekilde sürdürüyor. Cisco MX100 ve Meraki Z3 sistemleri aracılığıyla oluşturulan güvenli VPN ağları, şirketin geleceğe yönelik projeleri arasında önemli bir yer tutuyor. Bu projeler arasında; tüketicilere yönelik uygulamalar, istasyonlarda Hotspot sistemleri, elektrikli araç şarj istasyonları ve güneş enerjisi sistemlerinin geliştirilmesi bulunuyor.

HAYRETTİN PARLAKTÜRK
HYPCO PETROLCÜLÜK BİLGİ İŞLEM VE OTOMASYON MÜDÜRÜ

Global bir enerji markası olan HYPCO'nun Türkiye IT ve Operasyon Direktörü Hayrettin Parlaktürk; "şirketin dijital dönüşümüne yönelik şunları söyledi:

"Türkiye'nin akaryakıt sektöründe teknolojik bir lider olma yolundayız. Bu yolculukta, kurumsal yapımızı güçlendirecek ve müşterilerimize kesintisiz hizmet sunmamıza olanak tanıyacak stratejileri benimsiyoruz. IT, otomasyon veya yiyecek-içecek servisi veren iş ortaklarımızda, her zaman en kaliteli ve kurumsal olanlarla iş birliği yapmayı tercih ediyoruz. Böylece sektörde rekabet avantajı sağlıyor ve ticari operasyonlarımızda doğruluk ve netlik yaratıyoruz. Özellikle Turcom ile iş birliğimiz, HYPCO'nun yenilikçi ruhunu yansıtan önemli bir adımdır. Bu ortaklık sayesinde, Network Operasyon Merkezi (NOC) hizmetleri aracılığıyla bayi ağımıza kesintisiz ve güvenli hizmet sunuyoruz. Mevcuttaki bayilerimiz, dolum tesisleri, merkezimiz arasındaki 500'ün üzerindeki uç nokta için Turcom NOC'unun 24/7 izleme ve anında müdahale yetenekleri sayesinde, IT altyapımızı sürekli güncel tutarak potansiyel siber tehditlere karşı proaktif bir yaklaşım sergiliyoruz. Bu iş birliği, HYPCO'nun operasyonel etkinliğini artırmanın yanı sıra, geleceğe yönelik teknolojik dönüşüm ve iş sürekliliği planlarımızın temel taşını oluşturuyor."

NETWORK İZLEME SİSTEMİNİN ETKİLERİ VE İYİLEŞTİRMELER

Network izleme sisteminde yapılan geliştirmeler, HYPCO'nun günlük iş akışını olumlu yönde etkiliyor ve iyileştiriyor. Bu sistem, EPDK tarafından belirlenen yükümlülüklerin zamanında yerine getirilmesi için kritik bir rol oynamaktadır. Ayrıca, olası arızalar ve kesintileri minimum sürede çözerek ticari kayıpları önlemektedir.

HYPCO, Türkiye'nin ilk, Dünya'nın ikinci engelli kadın ralli Pilotu Kübra Denizci'nin sponsorudur.

YEDEKLİLİK VE SÜREKLİ HİZMET ANLAYIŞI

HYPCO için yedeklilik, sürekli aktif olan bir sistem için hayati önem taşımaktadır. IT departmanı, kesintisiz hizmet sunmak ve veri kaybını önlemek amacıyla yedekli sistemlere büyük önem vermektedir. Hypco uzman firmalarla iş birliği yaparak, kaliteli cihaz ve ekipmanlarla ve yetkin ekiplerle birlikte çalışarak stratejilerine odaklanıyor.

ZORLUKLAR VE BAŞARI STRATEJİLERİ

HYPCO, zorluklarla başa çıkabilmek için uzman firmalarla iş birliği yapmak, kaliteli cihazlar kullanmak ve yetkin ekiplerle çalışmak gibi temel stratejilere odaklanıyor.

TOPLUMSAL DAYANIŞMA VE HIZLI MÜDAHALE: HYPCO'NUN DEPREM SONRASI FAALİYETLERİ

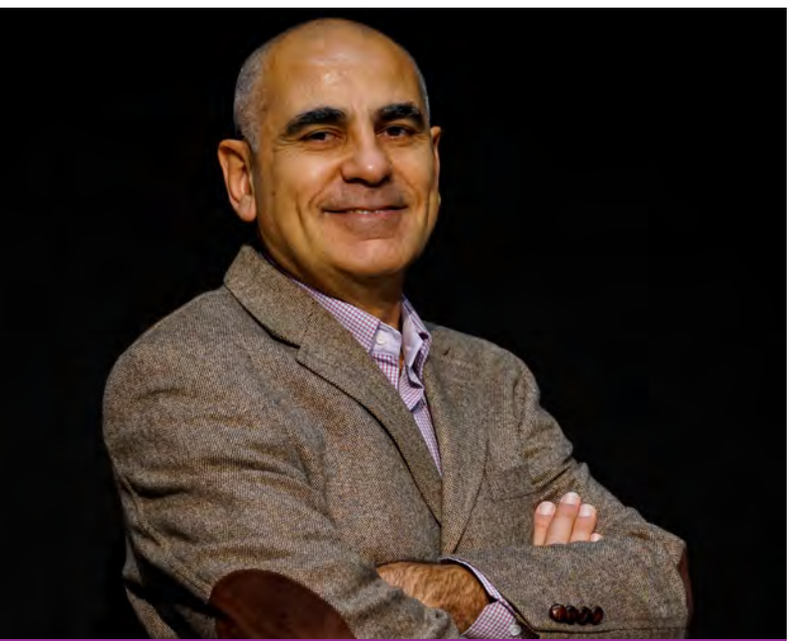
HYPCO, Kahramanmaraş'ta yaşanan 6 Şubat depremi sonrası, sadece bir enerji şirketi olmanın ötesine geçerek topluma önemli destekler sundu. Deprem sonrası karşılaşılan zorluklara hızla yanıt veren HYPCO, tarımsal amaçlı tankerlerin geçici mobil akaryakıt istasyonlarına dönüştürülmesi için gerekli girişimleri yaparak sektörde öncülük yaptı. Bu çaba, bölgede iletişim ve enerji ihtiyaçlarının karşılanmasında büyük katkı sağladı. Şirket, bölge hastanelerine karşılıksız akaryakıt sağlayarak ve mobil çözümler sunarak acil durumlara hızlı ve etkili bir şekilde müdahale etti. Bu durum, HYPCO'nun sadece bir enerji sağlayıcısı olmanın ötesinde, zor zamanlarda toplumun yanında duran sorumlu bir kurum olduğunu kanıtladı.

Bu olay, HYPCO'nun IT altyapısını yeniden gözden geçirmesi için bir fırsat oldu. Şirket, var olan ***Disaster Recovery Center (DRC)*** gerekliliklerine uygun daha da geliştirilmiş bir IT altyapısı oluşturmak için yeni projeler başlattı. Bu adımlar, HYPCO'nun sadece acil durumlarda değil, aynı zamanda uzun vadeli iş sürekliliği planlamasında da proaktif bir yaklaşım benimsediğini gösteriyor.

YENİLİKÇİ YAKLAŞIMLAR VE GELECEK VİZYONU

HYPCO, sektördeki liderler arasındaki konumunu korumak ve geliştirmek adına sosyal projelere ve teknolojik yeniliklere odaklanıyor. Güvenlik katmanını yükseltmek ve Ulusal Taşıt Tanıma Sistemleri'nin altyapısını geliştirmek de şirketin gelecek planları arasında yer alıyor. Bu makale HYPCO'nun Akaryakıt sektöründeki stratejilerini belirlerken gelecek vizyonu içerisinde teknolojiyi en verimli bir şekilde kullanmaya odaklandığını sunmaktadır.

DİJİTAL DÜNYADA GÜVENLİ GEÇİŞİN ANAHTARI: KİMLİK DOĞRULAMA



PROF. DR. VEDAT COŞKUN
AR-GE DİREKTÖRÜ

Bir kişinin, bilgiye ulaşmak ya da eylem gerçekleştirmek üzere yetkili olduğunu ispat etmek üzere beyan ettiği kimliğin, gerçekten de kendisine ait olduğunun kontrolü için yapılan işleme ***Kimlik Doğrulama (authentication)*** diyoruz. Kimlik doğrulama için kullanılan faktörler (a) bildiği (knowledge), (b) sahip olduğu (ownership) ve (c) olduğu (inherence) şeklinde sınıflandırılır.

GÜVENLİĞİN TEMEL TAŞI: ÇOKLU KİMLİK DOĞRULAMA FAKTÖRLERİ

Kişinin bildiği bir bilginin -örneğin şifrenin- beyan edilerek kimliğini ispatlaması, bu bilginin başkaları tarafından da bilinmesi, ele geçirilmesi ya da tahmin edilmesi olasılıklarının yüksekliği nedeni ile en düşük seviyede kimlik doğrulamasına neden olur, ki bu işlem ***1FA (one-factor authentication)*** olarak tanımlanır.

Kimlik ispatı için birden çok faktörün kullanılması ise ***MFA (multi-factor authentication)*** olarak sınıflandırılır, ki en yaygın MFA yöntemleri ***2FA (two-factor authentication)*** ile ***3FA (three-factor authentication)*** şeklindedir. Bilinen yanında sahip olunan (örneğin telefon, usb) bir cihazın da kullanılması (örneğin sms ya da e-imza doğrulaması) ***2FA*** olarak tanımlanır. Biyometrik verinin de kullanılması ***3FA*** seviyesinde, çok güvenli bir kimlik doğrulama olanağı sağlar. Daha yüksek güvenlik koşullarında birden çok biyometrik faktörün ek olarak kullanılması da (örneğin hem parmak izi, hem de retina doğrulaması) tercih edilebilir.

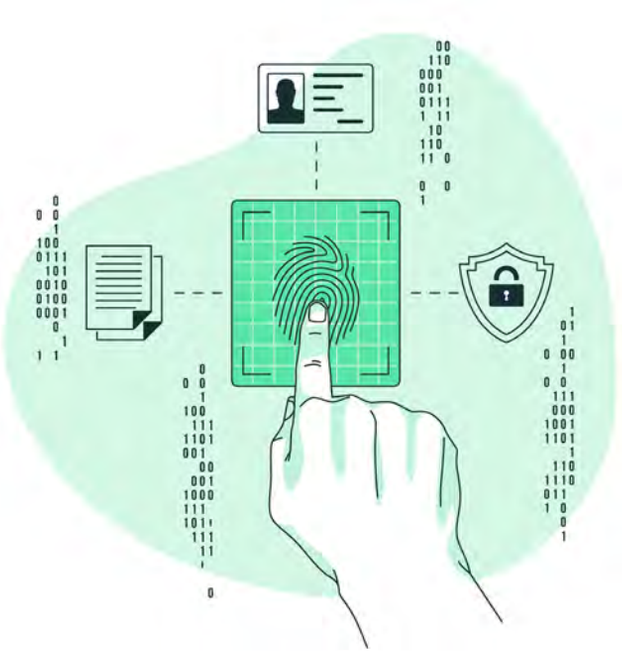
KİMLİK DOĞRULAMA SEVİYELERİ VE GÜVENLİK DENGELEMESİ

Kimlik doğrulama için kullanılan faktörlerin ve bunların kullanılma yöntemleri, kullanıcı kimliğinin doğrulanması konusundaki güven seviyesini belirler. ISO/IEC 29115 numaralı Kimlik Doğrulama Çerçevesi Standardı, dört farklı kimlik doğrulama seviyesi belirlemiştir. ***LoA1*** öne sürülen kimliğin doğruluğuna ilişkin hiç ya da çok küçük seviyeyi, ***LoA2*** normal seviyeyi, ***LoA3*** yüksek seviyeyi, ***LoA4*** ise çok yüksek seviyeyi ifade eder.

Bir veriye ulaşabilme ya da bir işlemi yapabilme konusunda hangi seviyenin seçilmesi konusu, elbette çok önemlidir. Bilinmesi gereken, yüzde yüz güvenliğin hiçbir zaman mümkün olmadığıdır; diğer bir prensip de güvenlik (security) ile işlem kolaylığının (functionality) birbirinin karşıtı olduğudur. Değerli bir bilginin ***LoA1*** seviyesinde doğrulama sonrasında erişilebilir olması ne kadar hatalı ise, değersiz bir bilginin ***LoA4*** seviyesinde doğrulama gerektirmesi de o kadar yanlış bir karar olur.

Kişilerin bilgi faktörünü, örneğin şifre girişini kullanarak kimlik doğrulama sürecinde ortaya çıkan bir sorun, bu şifrenin daha güvenli olmasını sağlamak üzere uzun ve karmaşık içerikli olmasının zorlanmasıdır. Güvenliği artıran bir husus olan bu tercih, kişilerin hatırlayamayacakları şifreleri bir yere kaydetmesi ile sonuçlanmakta, bu ise tam da başlangıçtaki riskin gerçekleşmesini kolaylaştırmaktadır. Ek olarak pek çok yerde gerekli pek çok şifrenin hatırlanması

gerektiği günümüzde bu zorluk ile baş etmenin bir yolu, şifre yönetim (password manager) sistemleri kullanmaktır. Bu sayede şifre yönetim uygulamasının şifresinin bilinmesi, diğer tüm şifrelere ulaşmanın bir yolu olarak son kullanıcının yaşamını kolaylaştırmaktadır. Bu zorluk ile başetmenin diğer bir yolu ise, erişilecek sistemin kabul edeceği bir SSO (single sign on) merkezinin şifresinin kullanılarak, söz konusu merkezin referansının, erişmek istediğimiz servis tarafından kabul edilmesi sayesinde işlemin kolaylaştırılmasıdır.



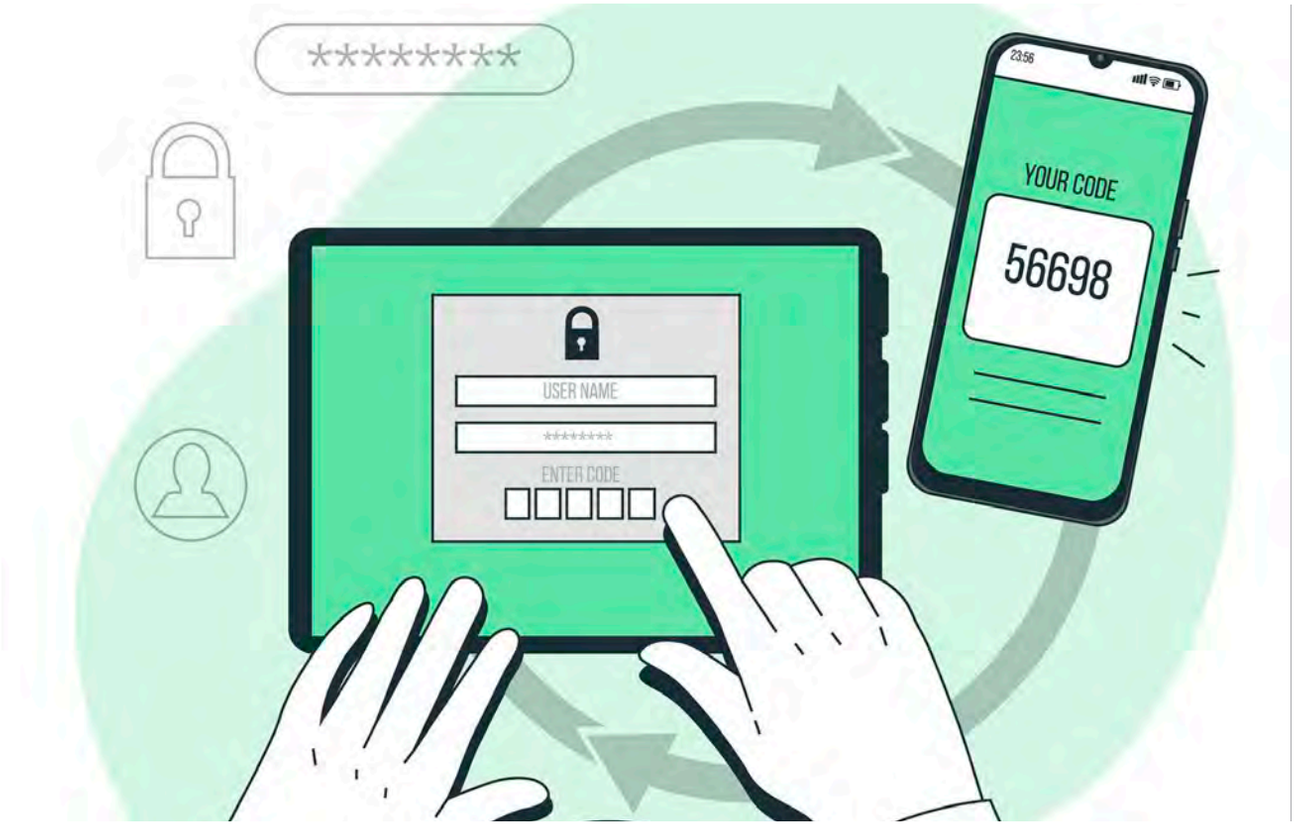
Bu kapsamda sözü edilen tüm unsurların ortak sakıncası ise, aslında her birinin kullanıcı şifresini bilmesi, dolayısı ile aslında kullanıcı kimliğinin doğrudan kullanıcı tarafından değil, fakat aracı kılınan sistem tarafından sahip olunmasıdır. Peki bu sorun nasıl aşılabilir?

WEB 3.0 VE KİMLİK DOĞRULAMA TEKNOLOJİLERİ: KULLANICI KONTROLÜ VE GÜVENLİĞİ

Daha önceki yazılarımı okuyanlar Web 3.0 teknolojisinin, kişilerin web üzerinde oluşturdukları bilgilerin teknoloji, finans, ya da diğer alanlarda faaliyet gösteren kurumlar yerine bu bilgiyi oluşturan kişilerin sahipliğinde kalarak kullanılmasını hedefleyen yeni bir teknoloji olduğunu hatırlayacaklardır. Yine beni takip eden kişiler merkezi otoriteye bir başkaldırı gibi ortaya çıkan blok zincir teknolojisinin, dağıtık yapıdaki paydaşların katılımı ile gerçekleşen bir bilgi toplama ve bilgi doğrulama platformu olarak anlatılabileceğini hatırlayacaklardır. İşte Web 3.0 yapısı ve blok zincir teknolojileri, tam da bu noktada kullanıcıların imdadına yetişmektedirler. ***FIDO (Fast IDentity Online)***, kişileri şifre belirleyerek oluşturdukları hesaplar yerine dijital cüzdan, dijital kimlik ve dijital bağlantıları kullanarak tanıyan bir model olarak ***SSI (Self-Sovereign Identity)*** modelini geliştirdi. Bu modelde bireyin kendisi hakkındaki bilgilerin kendisinde kalması, buna karşın kullanılan aracı üzerinden kimliğini ispatlaması mümkün olur.

SSI, kimlik doğrulama sürecinde kullanıcı ile servis sağlayan arasında güven oluşturmanın zorluğunun üstesinde gelmektedir. Bu yöntemde kullanıcı kimliğini doğrulaması için servis sağlayıcıya kişisel bilgilerini iletmek yerine, servis sağlayıcının güvendiği bir otoritenin referansını sunar; böylece bir yandan servis sağlayıcı kullanıcının kimliğinden emin olurken, diğer yandan kullanıcı kişisel bilgilerini servis sağlayıcıya vermek zorunda kalmayacaktır.

Kimlik Doğrulama, MFA, Blokzincir ve SSI teknolojileri konusunda bugüne değin yaptığım ve yapmakta olduğu çalışmalardan bir kısmını iletebilirim.



BİYOMETRİK VERİ KULLANAN BLOCKCHAIN TABANLI ÜÇ FAKTÖRLÜ KİMLİK DOĞRULAMA SİSTEMİ (BC-3FA)

BC-3FA projesinin amacı; biyometrik verileri kullanan ve Blockchain teknolojisi avantajlarından da faydalanarak hem kullanıcılar hem de sistemde yer alan diğer -potansiyel olarak birbirine güvenmeyen- taraflar arasında etkin, güvenli ve insan müdahalesi gerektirmeyen bir ***Üç Faktörlü Kimlik Doğrulama (3FA)*** Sistemi geliştirmek olarak belirlenmişti. Turkcell Teknoloji Ar-Ge Merkezi için geliştirilen bu proje, TÜBİTAK tarafından da desteklenerek başarı ile tamamlandı. Proje çalışmaları kapsamında ***BC-3FA*** modelinin mimarisi ve güvenlik modeli oluşturuldu, gerekli yazılımlar geliştirildi ve test edildi. ***BC-3FA*** modelinin, Turkcell Teknoloji'nin servis sağlayıcılar için aracılık edeceği bir platformda kullanılması hedeflenmektedir.

TRUSTEDID: OPEN-ID CONNECT TABANLI YENİ NESİL KİMLİK DOĞRULAMA YÖNTEMİ TASARIMI VE GELİŞTİRİLMESİ

TrustedId çalışmamızın amacı, ***MNO*** (Mobil Ağ Operatörü) müşterilerinin servislere erişimlerindeki kimlik doğrulama sürecinde kullanılmak üzere Akıllı Telefon üzerinde çalışacak yenilikçi bir Ortak Parola Sistemi geliştirilmesidir. Turkcell Teknoloji Ar-Ge Merkezi için geliştirilen ve TÜBİTAK tarafından da desteklenen bu proje, ***LoA4*** güvenlik seviyesi kriterlerine sahip olarak başarı ile tamamlanmıştır.

trcID: KURUM KAYNAKLARINA GÜVENLİ ERİŞİM YÖNETİM SİSTEMİ

Turcom Ar-Ge merkezinde çalışmakta olduğumuz projenin amacı, bir kurumun bulut ortamında ya da kendi fiziksel altyapısında yer alan bilgisayar sistemlerine erişim taleplerinin yönetilmesini sağlayacak yenilikçi bir Ar-Ge modelinin geliştirilmesidir. trcID sisteminde; kimlik doğrulama unsurları ve yetki detayı kullanılarak sisteme tanımlanacak olan bir kullanıcı, yetkili olduğu bir bilgisayar sistemlerine erişmek istediğinde, oluşturulacak olan kimlik doğrulama yöntemlerini kullanarak erişim yetkisi alacaktır. Bu kapsamda; Blockchain, ***SSI*** ve ***MFA*** teknolojileri kullanılacaktır.

İŞLETMELER İÇİN OYUN DEĞİŞTİRİCİ YAZILIM TANIMLI AĞ TEKNOLOJİSİ

SD-WAN: SOFTWARE-DEFINED WAN

Teknolojinin geldiği noktada bulut uygulamalarına geçişin kaçınılmaz olduğu, pandemi ile çalışma şekillerimizin mekân bağımsız iş modellerine evrildiği dönemde erişimlerin ve iletişimin hayatımızın ayrılmaz bir parçası olmasıyla birlikte, güvenilir ve performanslı network yapılarına ihtiyaç daha büyük zorunluluk haline geldi.

Geleneksel network çözümleri; yönetimi karmaşık, tümleşik olmayan, pahalı ve yeni teknolojilere ayak uydurmak için yeterli hız, esneklik ve kolay yönetilebilir güvenlik yapısına maalesef sahip değiller.

Uygulamaların artan bant genişliği ihtiyaçlarını kesintisiz ve yüksek kalitede erişimle karşılayabilecek, performansa dayalı akıllı yönlendirmeler yapabilecek, merkezden kurulup yönetilebilecek, güvenli erişim sağlayacak dijital dönüşümün temel başlangıç gereksinimi SD-WAN çözümüdür diyebiliriz.

SD-WAN çözümünün gündelik hayatımıza getirdiği güvenli ve kesintisiz erişimi maliyet avantajları sağlayarak, merkezi olarak yapılabilen kurulum ve yönetim ile görünürlüğü kolay bir şekilde devreye alınıp entegre edilebilmesi bu teknolojiye geçişlerin hızlanarak artmasında büyük rol oynamıştır.

SD-WAN'ın başlıca faydalarını beraberinde getirdiği kazanımları başlıklar altında kısaca özetleyelim.

SD-WAN TEKNOLOJİSİNDE GÜVENLİK

SD-WAN mimarisinin birçok avantajlarının yanı sıra birincil avantajı güvenli olmasıdır. SD-WAN mimarisinde, bir şirket veya şube, internet dahil olmak üzere diğer tüm ağlara eri-

UFUK ERSÖZ
TEKNOLOJİ DİREKTÖRÜ

> **GELENEKSEL NETWORK ÇÖZÜMLERİ;TÜMLEŞİK DEĞİLDİR VE YÖNETİMİ KARMAŞIKTIR. HIZ, ESNEKLİK VE KOLAY YÖNETİLEBİLİR GÜVENLİK YAPISINA NE YAZIK Kİ SAHİP DEĞİLLER.**

şimde bir uçtan diğer uca crypto şifrelemenin avantajlarından yararlanır. Ölçeklenebilir anahtar değişim işlevselliği ve yazılım tanımlı güvenlik sayesinde tüm aygıtlar ve uç noktaların tamamen kimliği doğrulanmıştır. Merkez birim şubeler arasındaki tüm iletişim güvenli olduğu gibi, bulut tabanlı iletişimi de ayrıca güvenli bir şekilde yapılandırır.

SD-WAN, merkezi konfigürasyon, şifreli ağ trafiği, ağ ayrımının kullanımı, WAN altyapısında görünürlük artışı ve genel olarak temiz performans ile ağ bağlantısındaki güvenilirliği artırır. Ağınızı bölümlere ayırmak, mevcut

sistemin herhangi bir bölümüne saldırı hasarını kısıtlar. Merkezi yapılandırma sistemi, geleneksel WAN kurulumundan çok farklı olarak ağınız arasında daha iyi iletişim ve bağlantı sağlayan tüm ayrı düğümleri birbirine bağlı olarak kontrol eden bir yazılım teknolojisi sağlar.

ESNEK VE YEDEKLİ HAT KULLANIMI

Sabit ve mobil telekom altyapısında birden fazla hattın tek cihazda sonlandırılıp birleştirilmesi, aynı anda hem birbirinin yedeği hem de her iki hattın aktif kullanımıyla daha yüksek band genişliği sağlayan, performanslı, verimli, kaliteli ve sürekli kesintisiz erişim sağlamasıdır.

Geleneksel WAN topolojisinde daha maliyetli MPLS, P2P vb. hatların alternatifi olarak, SD-WAN topolojisinde daha düşük maliyetli xDSL, 4,5G vb hatların kullanımı yaygınlaştı.

TAK ÇALIŞTIR (ZERO TOUCH PROVISIONING)

Bu teknolojiye sahip cihazların internet bağlantısı sağlaması sayesinde, uzak ofislerde fiziksel kurulum yapmaksızın cihazlar merkezi olarak konfigüre edilebilmektedir. Bu süreç, üreticiden üreticiye değişiklik gösterebilir. Bu noktada, çeşitli seçenekler konusunda uzman bir firmadan, ağ tasarımı ve kurulumu sürecinde başlangıçtan itibaren danışmanlık almak, işleri daha da kolaylaştıracaktır. Şube açılışlarının kolayca yapılabilmesi, zaman ve kaynak maliyetinden tasarruf sağlayacağı için bu, SD-WAN'ı geleneksel ağ teknolojilerine göre önemli ölçüde avantajlı kılar. Kurulum sırasında bireysel hataları önleyen kurulum sadeliği, SD-WAN'ı cazip hale getiren bir özelliktir. Saha yaygınlaştırmalarında fiziksel dolaşımı minimize eden merkezi yönetim yapısıyla çok tercih edilmektedir.

UYGULAMA BAZLI AKILLI TRAFİK YÖNLENDİRME

Hat kalitesine ve topolojide tercih edilen önceliklere göre performansa dayalı hat yönlendirmelerini yapabilmek SD-WAN sayesinde elde edilen önemli kazanımlardan biridir. Geçmişte klasik mimarilerde PBR, NAT, IP SLA TRACK vb. yöntemler ile karmaşık şekilde yapılmakta olan yönlendirmeler merkezi yönetim arayüzü üzerinden yapılan kolay düzenlemeler ile sıkıntısız şekilde yönetilebilmektedir.

QoS, uygulanmak istenen trafik tipleri için, IP, port, interface vb. yöntemler kullanılarak merkezi yönetim aracılığıyla sağlanabilmektedir.

OTOMATİK YÖNLENDİRME (ROUTING)

SD-WAN mimarisi ile Management ve Controller plan merkezi hale getirilmesi ile artık routing karmaşası ortadan kalkmıştır. Merkezi otomatik hale getirilen routing ile ağ mühendisleri büyük bir iş yoğunluğundan kurtulmuş ve odak noktalarını artık katma değer yaratacak servislere vermişlerdir.

NETWORK İZLEME VE RAPORLAMA AVANTAJLARI (MONITORING & ANALYTICS)

SD-WAN mimarisinde sağlanan izleme araçlarıyla, bütün uç noktalardaki şubelerin, kullanıcıların, cihazların, IP adreslerin kullandıkları uygulama, band genişliği vb. bileşenlerin durumunun anlık olarak izlenebilmektedir.
Bu sayede iletilen bir sorununun analiz ve çözüm sürecinin kolay hale gelmesi, hatta sorun size iletilmeden görülebilir olması, sorun yaşanmadan farkındalık yaratacak bir izleme akışı oluşturulması ana fikir ve hedeftir.

SD-WAN ile gelen teknolojik faydalar ile hedeflenen kolay yönetilebilirlik ve merkezileştirme özelliği, aynı zamanda bütün lokasyonların uygulama bazlı analizlerini tek ekrandan yapabilme olanağı sağlayarak network izleme ve işletim faaliyetlerini sadeleştirmektedir.

YAPAY ZEKÂ DESTEKLİ SİBER SUÇLULARIN YÜKSELİŞİ: TEHDİTLER VE FIRSATLAR

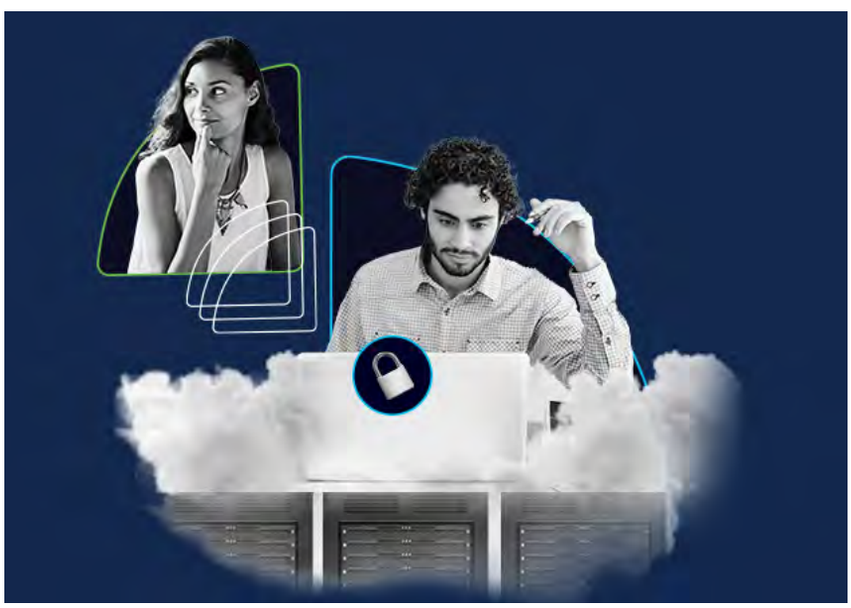
Yapay zekânın son zamanlarda benimsenmesi, suçluların yapay zekâyı yıkım için kullanabilecekleri birçok yol nedeniyle siber güvenlik açısından önemli endişelere yol açmıştır.

Yapay zekâ ile ilgili teknolojilerin etkili ve hedefe yönelik kullanımı, siber güvenlik uzmanları için çok önemli bir rol oynayacaktır.

Geçtiğimiz on yılda makine öğrenimi (MÖ) ve yapay zekâ (YZ) büyük ölçüde benimsendi ve giderek artan sayıda kuruluş, ürünlerini ve hizmetlerini daha iyi hale getirmek için operasyonlarını otomatikleştirmek üzere bu tür teknolojilerden yararlanıyor.

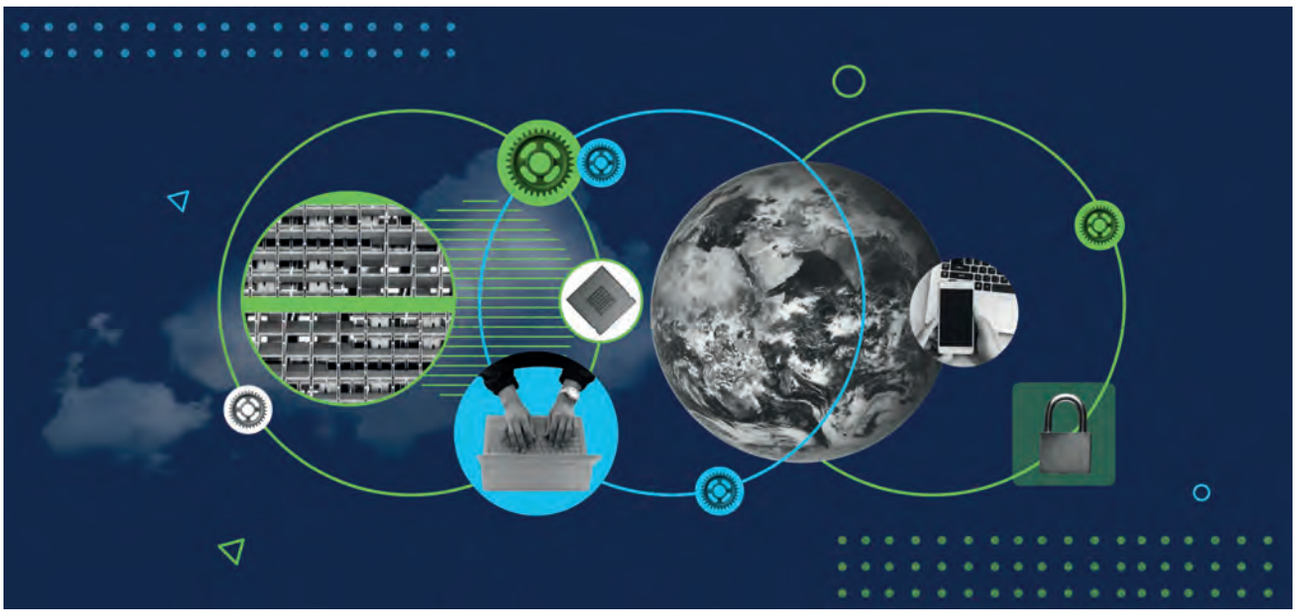
MÖ ve YZ'nin kuruluşlar tarafından bir süredir yaygın olarak kullanılmasına rağmen, birçok bireysel kullanıcı ilk etkileşimlerini yalnızca son birkaç ay içinde ve çoğunlukla YZ'yi halkın zihninin önüne getiren ve YZ geliştirme için yoğun bir yarışı körükleyen ChatGPT gibi üretken YZ biçiminde yaşadı.

Her yenilikte olduğu gibi, YZ kullanımının da küresel kültür üzerinde hem olumlu hem de olumsuz etkileri olması bekleniyor. Yine de çok azının siber suçlar kadar büyük bir fayda sağlaması bekleniyor. Siber saldırıların giderek yaygınlaştığı dijital bir çağda



yaşıyoruz ve yapay zekâ suçluların operasyonlarını kolaylaştırmaya yardımcı olabilir, onları daha verimli, sofistike ve ölçeklenebilir hale getirirken tespit ve atıflardan kaçmalarına olanak tanıyabilir.

Cisco EMEA Hizmet Sağlayıcıları ve MEA Siber Güvenlik Direktörü Fady Younes'a göre, "Günümüzün siber saldırıları her zamankinden daha sofistike ve en son teknolojileri kullanıyorlar. Buna karşı koymak için şu anda siber güvenlik alanında otomasyon, yapay zeka, makine öğrenimi, proaktif tespit ve düzeltme ve önleme tarafından yönlendirilen muazzam miktarda yenilik var. Güvenliğin amacı budur - tehditleri önlemek, ancak önleyemediğinizde, gerçek zamanlı veya neredeyse gerçek zamanlı olarak yanıt vermek, düzeltmek ve kaydetmek için onları hemen tespit etmek."



GÜÇLENEN SİBER SUÇLAR

Siber suçlarda YZ araçlarının önemli bir etki alanı, yazılım geliştirme, dolandırıcılık, gasp vb. gibi siber suç örgütlerinin insan katılımına olan ihtiyacın azalmasıdır; bu da yeni üye alma ihtiyacını azaltacak ve daha düşük personel sayısı nedeniyle operasyonel maliyetleri düşürecektir.

Yapay zekâ, sızan veriler de dahil olmak üzere muazzam miktarda bilgiyi analiz etmek için kullanılarak siber suçluların yararlanabileceği başka bir yol sunar. Bu analiz, güvenlik açıklarını veya yüksek değerli hedefleri belirlemelerini sağlayarak potansiyel olarak daha büyük mali kazançlar sağlayabilecek daha kesin ve etkili saldırılara olanak tanır.

Yapay zekâ ile gelişebilecek bir başka suç faaliyeti alanı da daha sofistike kimlik avı ve sosyal mühendislik saldırılarının geliştirilmesidir. Bu, son derece gerçekçi deepfake'lerin, aldatıcı web sitelerinin, dezenformasyon kampanyalarının, sahte sosyal medya profillerinin ve yapay zekâ destekli dolandırıcılık botlarının oluşturulmasını içerir.

SİBER SUÇLARLA MÜCADELE

Öte yandan, siber güvenlik uzmanları ve kolluk kuvvetleri, siber suçlarda kaydedilen ilerlemelere karşı koymak için yapay zekanın gücünden yararlanabilir. Kötü niyetli faaliyetlere karşı mücadelelerinde yenilikçi araçlar, taktikler ve stratejiler geliştirmek için yapay zekâyı kullanabilirler.

Tehdit algılama ve önleme gibi alanlar, YZ güvenlik araştırmalarının ön saflarında yer alacaktır. Mevcut güvenlik araçlarının çoğu, yalnızca kötü amaçlı imzalara ve kullanıcı girdisine dayanmakta ve bu da onları gelişmiş saldırıları tespit etmek için etkisiz hale getirmektedir. Sonuç olarak, giderek artan sayıda satıcı, daha kesin ve etkili tehdit tespiti elde etmek için makine öğrenimi ve YZ teknolojilerine yöneliyor. Öne çıkan örnekler arasında Cisco Secure Endpoint ve Cisco Umbrella'nın sırasıyla son ana bilgisayarlarda ve ağlarda şüpheli davranışları otomatik bir şekilde tespit etmek ve azaltmak için gelişmiş makine öğrenimini kullanması yer almaktadır.

Cisco Talos da benzer şekilde işlenmiş web sayfalarının sınıflandırılması, logo analizi yoluyla sahtekarlık girişimlerinin belirlenmesi, metin analizine dayalı kimlik avı e-postası sınıflandırması ve ikili benzerlik analizi gibi tehdit istihbaratı işlemlerini otomatikleştirmek için birkaç yıldır yapay zekâdan yararlanmaktadır.

Yapay zekânın yükselişi, kullanıcı tabanı ve uygulamaları genişlemeye devam ettikçe yeni zorluklar ve büyük fırsatlar sunmaktadır. Yapay zekâ ile ilgili teknolojilerin etkili ve hedefe yönelik kullanımı, siber güvenlik uzmanları ve kolluk kuvvetleri için dijital suç davranışlarını tespit etme, bunlara karşı savunma ve ilişkilendirme konusunda çok önemli bir rol oynayacaktır.

Bununla birlikte, bu kuruluşlar YZ'nin gücünden bizzat yararlanarak, gelişen tehditlerle mücadele etme ve dijital ekosistemlerin güvenliğini sağlama yeteneklerini artırabilirler. Siber suç ortamı geliştikçe, yapay zekâyı benimsemek düşmanların önüne geçmek için önemli bir araç olacaktır.

LİNDE OPSAN, TURNET İLE YENİ FABRİKALARINDA "TAM GAZ" İLERLİYOR!

Otomobil parçaları üretiminde büyük pay sahibi Linde Opsan, devreye giren iki yeni fabrikasının altyapı ve network kablolama ve tesis güvenliği projesinde Turnet'e güvendi.

Kocaeli/Dilovası'nda, Linde + Wiemann ve Opsan ortak girişimi olarak faaliyete başlayan Linde Opsan, kurulduğu 2010 yılından bugüne otomobil parçaları üretiminde büyük bir pay sahibidir. Genişleyen üretim bandını karşılamak için iki yeni fabrikayı devreye alarak müşterilerinin hedeflerini gerçekleştirmedeki ana çözüm ortağı olmaya devam ediyor.

İki yeni fabrika ile üretim kapasitesini arttıran Linde Opsan, altyapı ve kablolama çalışması için sayısız zayıf akım projesine imza atan Turnet'i tercih etti. Turnet zayıf akım ekibi, daha önce başarıyla tamamladığı birçok proje gibi hızlı, güvenli ve uygun maliyetli proje hazırlayarak uygulamaya geçti.

Faaliyete geçen iki yeni fabrikanın üretim bölümüne öncelikle sistem odası kurulumu tasarlandı. Kurulacak alanın ölçüleri alınarak ve fabrikaya çekilen fiber kabloların fabrika içi dağılım güzergahı belirlenerek belirli noktalara kenar kabin konumlandırıldı. Üretim alanı büyük olduğu için veri iletiminde en son teknoloji olan fiber kablo kullanıldı.
Karadan, konumlandırılan kenar kabinlere fiber kablolama yapılmasının ardından verinin üretim cihazlarına taşınması fazına geçildi. Kenar kabinlerden üretim cihazlarına, access point'lere ve güvenlik kameralarına bağlantı kurulabilmesi için CAT6 network kablosu kullanılarak cihazlar arası iletişim sağlandı.

Güvenliği sağlamak için sistem odasına yükseltilmiş zemin yapılarak kabloların dışarıda kalmasının önüne geçildi. ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardına uyularak kurulan sistem odasının yangın güvenliği sağlandı. Yanmaz kablo kullanılarak ortaya çıkabilecek yangın riskine karşı önlem alınmış oldu. Gazla yangın söndürme sistemi devreye alınarak sistem odası içerisindeki cihazlar koruma altına alındı. Son olarak ise yangını önleyen ve 1200 dereceye kadar dayanabilen kapı takılarak sistem odası kurulumu başarıyla tamamlandı.

Tamamlanan sistem odasının bilgi işlem ekibi tarafından takip edilebilmesi için kurulan ortam izleme sistemi sayesinde Linde Opsan bilgi işlem ekibinin, uzaktan müdahale edebilmesi, yangın, su basması ya da sistem odasının kapısının açılması vb. durumlarda uyarı alması ve nem/ısı değerlerini takip edebilmesi mümkün hale geldi.

Sistem odasının kurulumunun tamamlanmasının ardından internet bağlantısının 16 bin metrekarelik alanda aktif olarak kullanılabilmesi için son teknoloji Altai access point'ler konumlandırıldı. Alanın büyüklüğüyle paralel olarak 50-60 adet kullanılması gereken access point, yalnızca 2 adet Altai model kullanılması sayesinde sistem

odası ve kullanılan cihazları arttırmaya gerek kalmadı. Turnet'in uzman ekibinin hayata geçirdiği proje sayesinde hem büyük bir maliyet avantajı hem yönetimi kolay bir network kapsama alanı oluşturularak zaman ve süreç kazanımı sağlandı.

Tüm bu uygulamalar sonrasında altyapı kablolama kısmı tamamlanarak projenin ikinci fazına yani sistemin çalışmaya başlaması için sistem odasında yer alacak cihazların konumlandırılarak kurulumlarının yapılmasına geçildi. Profesyonel takım çalışmasıyla zayıf akım ekibinden görevi devralan Turnet network ekibi, switch ve backbone cihazlarını yerleştirerek VLAN atamalarını yaptı ve sistem devreye alınmış oldu.

Projenin diğer ayağında , üretim alanının ardından ofislerin Linde Opsan çalışanları için hazır hale getirilmesi kısmına geçildi. Fabrikanın üretim kısmına uygulanan sistem odası konumlandırma ve kablolama işlemleri ofislerin bulunduğu katlara da uygulandı. Her kata kenar kabinler konumlandırılmasının ardından fiber kablolama ile sistem odası canlandırıldı. Sistem odasından çalışma masalarına ve access pointlere veri akışı sağlanması için CAT6 network kablolama yapıldı. Asansörlerin önüne güvenlik kamerası konumlandırılmasının ardından elektrik kablolama yapılarak fabrika artık üretime hazır hale getirildi.

Turnet ekibi tarafından ikinci fabrika, ilk fabrikada yapılan çalışmalar birebir tekrarlanarak üretime hazır hale getirildi. Maliyet ve zaman tasarrufu sağlanması adına farklı olarak ikinci fabrikada sistem odası kurulması yerine backbone cihaz konumlandırılarak ilk fabrikanın sistem odasından fiber kablo çekilerek kenar kabin replikasyonu tasarlandı. Turnet ekibinin ortaya koyduğu deneyim ve bilgi birikimi farkı sayesinde oluşturulan bu tasarım, Linde Opsan için tek bir yerden yönetim imkanı sağlayarak iş süreçlerinin takibi kolaylaştırıldı. İki katlı olan bu fabrikada, ilk fabrikadaki gibi her kata ikişer adet Altai access point konumlandırılarak kablosuz network erişimi, düşük maliyetle ve kolay yönetimle sunulmuş oldu.

Son olarak fabrikaların güvenliğinin sağlanması için alan girişine kollu bariyer sistemi, raylı bariyer sistemi ve X-ray cihazı ile kontrollü geçiş sistemleri kuruldu. Alanın kontrolü ve güvenliğinin sağlanmasının ardından 30 yılı aşkın proje ve saha tecrübesini konuşturan Turnet ile baştan sona maliyet avantajlı ve hızlı aksiyon alınan bu proje başarıyla tamamlanmış oldu.

TREND MICRO DİJİTAL DÜNYAYI GÜVENLİ HALE GETİRİYOR

Dünyanın önde gelen siber güvenlik şirketlerinden Trend Micro, 30 yılı aşkın süredir dijital dünyanın güvenliğini sağlıyor.

Siber güvenlik alanında 30 yılı aşkın süredir faaliyet gösteren dünyanın önde gelen siber güvenlik şirketlerinden Trend Micro, dijital bilginin dünya genelinde güvenli bir şekilde yayılmasını sağlamak için tüketicilere, işletmelere ve kamu kurumlarına yönelik katmanlı güvenlik çözümleri sunuyor. Bu çözümler, uç noktalardan sunuculara, ağ sistemlerinden endüstriyel IoT cihazlarına ve otomasyon sistemlerine kadar tüm ortamların güvende tutulmasına olanak tanıyor.

65 farklı ülkede faaliyet gösteren ve 7.000'i aşkın çalışanı bulunan Trend Micro, dünya genelinde birçok işletmeye ve kamu kuruluşuna hizmet sağlıyor. Fortune 500 listesindeki ilk 10 şirketten 9'u Trend Micro'nun çözümlerini kullanıyor. Gartner, Forrester ve IDC gibi dünyanın önde gelen araştırma şirketleri, hazırladıkları çalışmalarda Trend Micro'nun siber güvenlik sektöründeki liderliğini teyit ediyor.

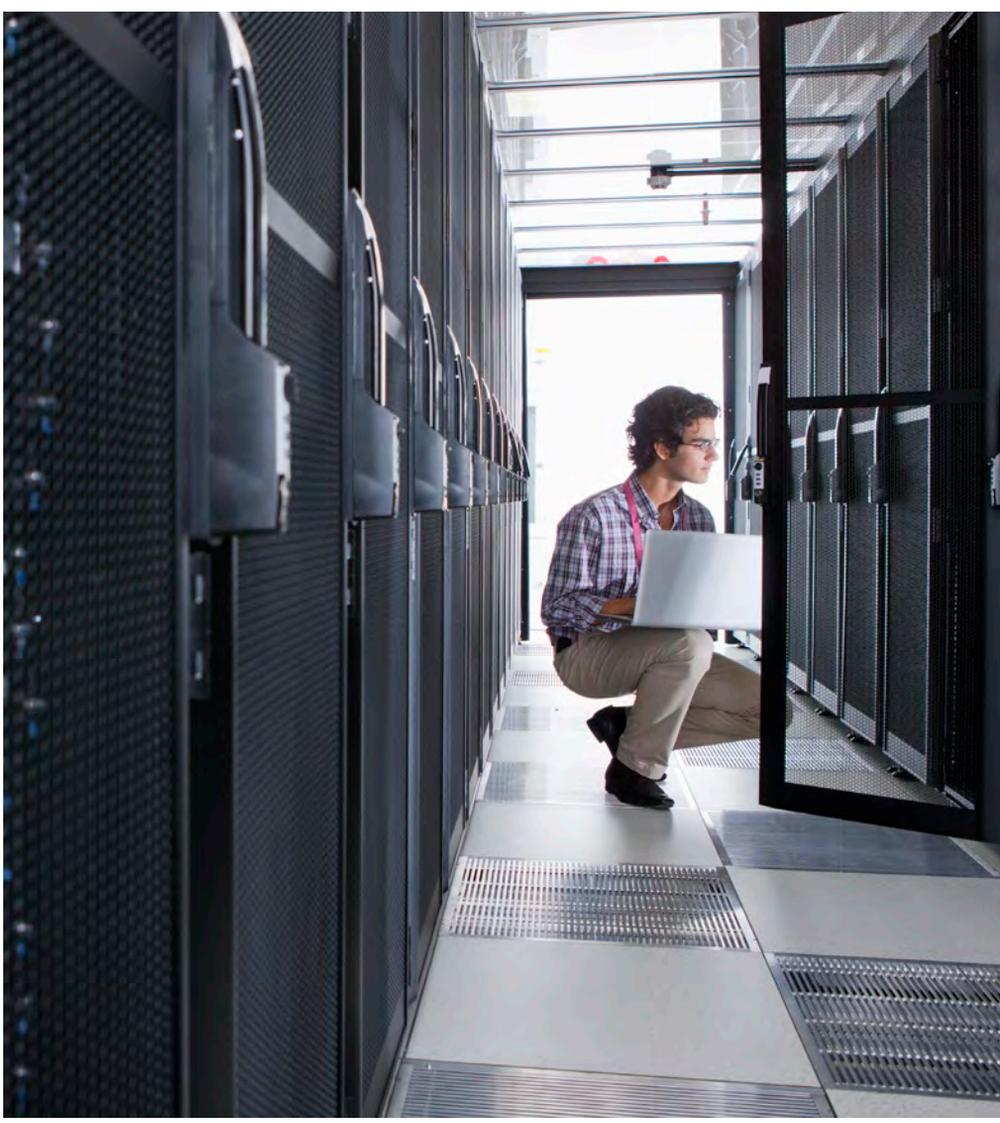
Trend Micro'nun sunduğu çözümler arasında Hibrit Bulut Güvenliği, Ağ Güvenliği, Kullanıcı Güvenliği bulunuyor ve ayrıca XDR (Genişletilmiş Tespit ve Müdahale) kapasitesi ile öne çıkıyor. XDR, güvenlik olaylarını daha geniş bir perspektiften izleme ve müdahalede bulunma yeteneği sağlıyor ve operasyonel maliyetleri azaltma, güvenlik ekiplerinin etkinliğini artırma gibi avantajlar sunuyor.

Trend Micro'nun öne çıkan ürünlerinden biri olan Trend Micro One, dijital dönüşümün getirdiği karmaşık BT süreçlerine yanıt olarak geliştirilen tümleşik bir siber güvenlik platformu olarak öne çıkıyor. Dünya genelinde 250 milyon sensörle desteklenen bu platform, tehditleri hızla tespit edebilme ve müdahale edebilme yeteneği ile işletmeleri koruyor. Ayrıca, AWS, Microsoft Azure, Google Cloud gibi önde gelen bulut servis sağlayıcıları ile entegrasyon yeteneği, işletmelerin siber güvenlik gereksinimlerini esnek bir şekilde karşılamalarını sağlıyor.

Trend Micro birçok alanda lider konumunu sürdürüyor. Dünya çapında rakiplerine göre daha fazla siber güvenlik araştırmacısı bulunuyor. Trend Micro'nun araştırmalarında ortaya koyduğu iç görüler ve tespitler siber güvenlik endüstrisinde yaygın olarak kullanılıyor ve çözümlerinin sunduğu değeri güçlendiriyor. Araştırma ekipleri, Trend Micro'nun en iyi olduğu alanlardan tehdit istihbaratının da gücüne güç katıyor. Dünya geneline yayılmış 15 küresel tehdit araştırma merkezinde çalışan yüzlerce araştırmacı ve veri bilimcisinin yanı sıra 10 binin üzerinde bağımsız araştırmacı sürekli istihbarat topluyor ve şirketlerin güvende kalmasını sağlayacak çok önemli çalışmalara imza atıyor. Bu istihbarat çalışmaları, dünya genelinde 500 bin işletmenin ve milyonlarca kullanıcının aktif olarak kullandığı çözümlerden toplanan bilgilerle destekleniyor. Bu çözümler uç noktalar (mobil, PC, Mac, Sunucular dahil), e-posta, web, ağ trafiği, IoT/IIoT, veri merkezleri ve bulut altyapıları genelinde bilgi topluyor ve dünyanın en kapsamlı tehdit istihbaratını oluşturuyor.

Trend Micro, tehdit araştırmalarıyla siber güvenliğin birçok alanında güvenlik öngörüleri sağlıyor ve aynı zamanda INTERPOL dahil olmak üzere dünya genelinde birçok kurumla iş birliği yapıyor. Bu kurumlara, siber saldırganlar, siber tehditler, kullanılan altyapılar ve araçlar dahil olmak üzere detaylı bilgiler sağlıyor. Örneğin geçtiğimiz haftalarda, Trend Micro'nun INTERPOL'e sağladığı istihbarat bilgileri sayesinde dünya genelinde 70 bin kişiyi dolandırdığı tahmin edilen *16shop* adlı siber suç grubuna büyük bir darbe indirildi. Daha önce de INTERPOL ve FBI gibi diğer kurumlarla yapılan iş birlikleri sonucunda birçok siber suç grubu faaliyet gösteremez hale getirildi. Bu, tehdit istihbaratıyla desteklenen kamu-özel sektör iş birliklerinin uluslararası siber suç soruşturmalarında önemli bir etkiye sahip olduğunu göstermesi açısından büyük önem taşıyor. Trend Micro, önümüzdeki dönemde siber tehdit araştırmalarını daha da güçlendirmeyi ve bu iş birliklerini daha da ilerletmeyi amaçlıyor.

Trend Micro, aynı zamanda sektörde fark yaratan bir diğer önemli girişimi Zero Day Initiative ile siber güvenlik açıklarını siber saldırganlardan önce bulmaya ve gerekli güvenlik düzeltmelerinin yapılmasını sağlayan çalışmalarını sürdürüyor. 2005 yılında kurulan ZDI, güvenlik açıklarının kullanıcıları ve sistemleri etkilemeden önce tespit edilmesini ve geliştiricilerin hızla yapama yayınlayabilmelerine olanak tanıyan bir oluşum. Şu ana kadar binlerce güvenlik açığını daha siber saldırganlar bulup faydalanma fırsatı elde etmeden tespit ederek üretici firmalara bildirme başarısını gösterdi.



Trend Micro'nun Trend Vision One™ çözümü, şirketlerin varlıklarını ve saldırı vektörlerini tanımlayabilmelerinin yanı sıra bunların profillerini çıkarmalarını sağlıyor. Ayrıca, saldırı yüzeyiyle ilişkili risklerin otomatik olarak değerlendirilmesine, önceliklendirilmesine ve azaltılmasına olanak tanıyor. Yerleşik sıfır güven ve eksiksiz saldırı yüzeyi risk yönetimi özellikleriyle şirketlerin riskleri kontrol altında tutmalarını sağlıyor.

SİBER GÜVENLİK: ÖNEMİ, FIRSATLARI VE ZORLUKLARI

Dijital dönüşüm yeni seviyelere ulaştığı için siber güvenlik, kurumlar için stratejik bir öncelik haline geldi. Son dönemde bazı kontrol dışı faktörlere bağlı olarak yaygınlaşan yeni çalışma ve iletişim kültürü teknolojik yenilikleri beraberinde getirdi. Bu yeniliklerle birlikte, kurumların bilgileri ve işleyişleri tehdit eden ögelerin karmaşıklığı da arttı.

Bu noktada siber güvenlik konusundaki farkındalığın kurumlardan, son kullanıcılara kadar artırılarak sağlanması ve kurumsal teknolojilerin kırılganlıklarının azaltılarak kurumsal dayanıklılık seviyelerinin yükseltilmesine bağlı olarak siber güvenlik trendleri ve stratejileri kilit bir rol oynamaktadır.

BURÇİN YENİCE
PRESALES MÜDÜRÜ

DİJİTAL ÇAĞIN ÖNCÜ KALKANLARI

Siber saldırılar arttıkça, siber güvenlikte yenilikçi adımların seslerini yapay zekadan, biyometrik kimlik doğrulamaya kadar bir dizi inovatif çözüm, kurumları tehditlere karşı korumak için kullanılmaktadır. Bulut teknolojilerinin yükselişi, IoT'nin genişlemesi ve veri gizliliğiyle ilgili düzenlemelerin sıkılaşması sonucunda şirketler siber güvenlik yaklaşımlarını yeniden değerlendiriyorlar. İşte bu yüzden, siber güvenlik trendlerini yakından takip etmek, kurumların bu hızla değişen dijital çağda bir adım önde olmalarını sağlar. İşte kısa kısa son gelişmeler…

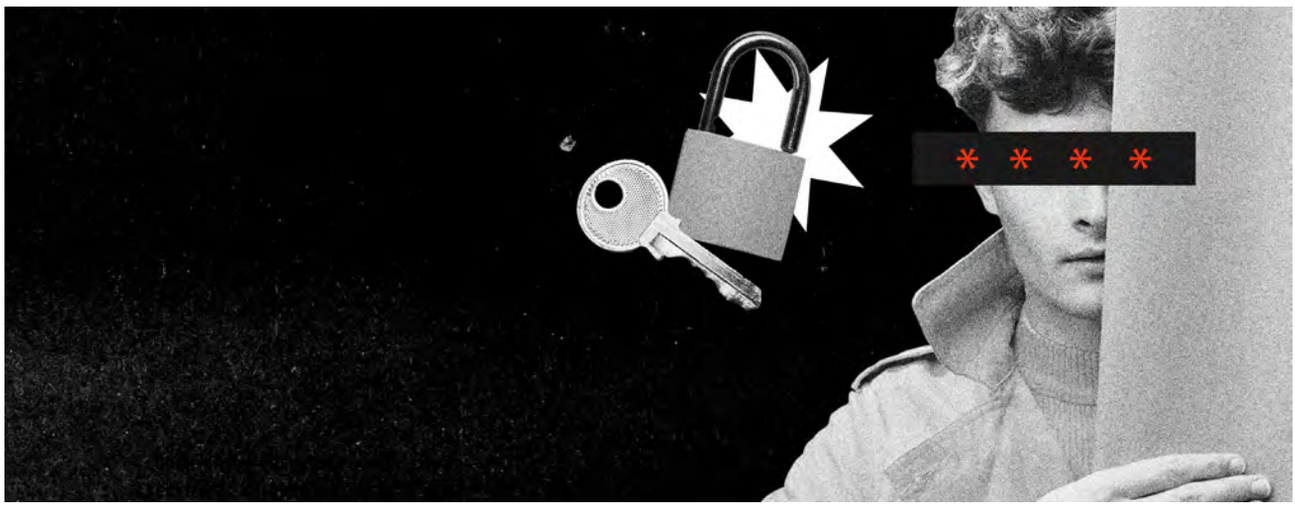
Nesnelerin İnterneti (IoT) Güvenliği: Artan sayıda cihazın internete bağlı hale gelmesiyle internete ve birbirlerine bağlanan makinalar üzerinden yapılabilecek saldırılar kurumsal sistemlerin zaafiyetini artmıştır. Bu ise OT'ye (operasyonel teknolojiler) yönelik güvenlik çözümlerine önemli oranda ihtiyaç doğurmuştur. IoT özellikli cihazların güvenliği, ağa zarar vermeden sağlanmalıdır.

Sıfır Güven İlkesi (Zero Trust): Bu yaklaşım, ağ içindeki her cihaz ve kullanıcının potansiyel bir tehdit olarak kabul edilmesini ve erişim haklarının sürekli olarak doğrulanmasını önerir. Dolayısıyla bu yaklaşımdan yola çıkan sistemler son dönemde iş gereksinimlerine uygun olarak kurumlar tarafından sıkça tercih edilmeye başlanmıştır.

Kimlik ve Erişim Yönetimi (IAM): Kimlik doğrulama ve erişim kontrolü, kurumların siber güvenlik stratejilerinde merkezi bir rol oynamaktadır. Kimlik hırsızlığını önlemek için IAM çözümleri öne çıkmaktadır.

Cloud Security (Bulut Güvenliği): Kurumlar, bulut tabanlı hizmetlere daha fazla geçtikçe, bulut güvenliği de önemli bir trend haline gelmiştir. Verilerin şifrelenmesi, güvenli erişim ve uygulama düzeyinde güvenlik önlemleri bu alanda öne çıkmaktadır.

Yapay Zekâ ve Makine Öğrenimi: Siber saldırılar giderek daha karmaşıklaşıyor. Bundan ötürü yapay zekâ ve makine öğrenimi ile kurumların iletişim, sistem ve verilerine yönelik tehditler daha hızlı tespit edilebilir. Anormal davranışların analizleri yapılarak, kurumsal savunma sistemleri daha güçlü hale getirilir.



Otonom Siber Savunma: Otomasyon ve yapay zekâ destekli savunma sistemleri, saldırılara daha hızlı yanıt verme ve manuel müdahaleyi azaltma konusunda etkili olabilir.

Biometrik Kimlik Doğrulama: Parmak izi, yüz tanıma ve iris taraması gibi biyometrik verilerin geleneksel kimlik doğrulama yöntemleriyle bütünleştirilmesiyle daha sarsılmaz bir erişim güvenliği sağlanmaktadır.

Veri Gizliliği ve Uyum: Verilerin işlenmesi ve gizliliğine yönelik regülasyonların artmasıyla, kurumlar GDPR, CCPA ya da ülkemizdeki 6698 KVKK gibi düzenlemelere uyum sağlamalı ve gerektiğinde rapor verebilir, kanıt sunabilir noktada olmalıdır. Bu durumda da çeşitli güvenlik teknolojilerinin kullanılmasının "şart" hale getirmektedir.

DİJİTAL DÖNÜŞÜMÜ SORUNSUZ KILACAK SİBER KALKANIN ÜÇ BOYUTU

Dijital çağda siber güvenlik kritik bir öneme sahip, 30 yılın üzerinde farklı sektörlerde başarılı kurumsal teknolojilere yönelik uygulamalar yapan bir topluluğun üyesi olarak, firmaların dijital dönüşüm süreçlerinde sorunsuz ilerlemesi için 3 adımda bir yaklaşım öneriyoruz.
İşte bu yaklaşımlar…

Öncü Strateji: Proaktif yaklaşım, geleneksel reaktif metotların ötesine geçerek, tehditleri önseziler yoluyla da algılamak için proaktif güvenlik stratejilerini benimsiyoruz.

Bilgi ve Farkındalık: Kullanıcılara yönelik siber tehdit eğitimleriyle, sosyal mühendislik saldırılarını önlemek için bilinç seviyesini yükseltiyoruz.

Derinlemesine Savunma: Çok katmanlı güvenlik olarak da adlandırılabilecek bu yaklaşım tekil güvenlik önlemlerinin sınırlılıklarını aşmak adına çok önemlidir. Böylelikle farklı seviyelerde tehditlere karşı birbirini bütünleyen ama katmanlı hale getirilmiş bir yaklaşımı benimsiyoruz. Bu noktada her organizasyonun siber güvenlik ihtiyaçlarının ve risk profilinin benzersiz olduğunun farkındayız. Genelde, çok katmanlı yaklaşımın, tehditlere çok yönlü bir perspektiften yaklaşarak en üst düzeyde savunma imkânı sunduğunu görüyoruz.

Siber güvenlik yaklaşımları organizasyonların ihtiyaçlarına ve risk profilimize bağlı olarak değişebilir. Genellikle çok katmanlı bir yaklaşım en etkili olanıdır, çünkü bu, tehditleri çok farklı açılardan ele almayı ve daha etkili bir savunma sağlamayı mümkün kılmaktadır.

TÜRKİYE'DE SİBER GÜVENLİK: MEVZUAT, İLERLEMELER VE STRATEJİK YAKLAŞIMLAR

Türkiye'de siber güvenlik konusunda mevzuatın yanı sıra sektörel ilerlemeler de göz önüne alınarak kurumsal güvenlik teknolojilerinin projelendirilmesine ilişkin çalışmalarımız devam etmektedir. Bu sebeple hem kurumsal düzeyde hem de kullanıcı seviyesinde dijital dünyanın güvende olmasını sağlamak adına yasal düzenlemeleri de dikkate alan bir teknoloji partneriyle çalışmanın kritik bir öneme sahip olduğunu belirtmek istiyorum.

Çok kısaca ülkemiz koşullarına ve ülke koşullarındaki yasal düzenlemelere değinmek gerekirse;
Bilgi Teknolojileri ve İletişim Kurumu (BTK) Kanunu: BTK, Türkiye'de bilgi teknolojileri ve iletişim hizmetlerini

düzenleyip denetleyen ana kurumdur. BTK Kanunu, siber güvenlik konusunda çeşitli yönergeler barındırır ve BTK'nın bu alandaki görevlerini belirtir.

Kişisel Verilerin Korunması Kanunu (KVKK): KVKK, kişisel verilerin işlenmesi, saklanması ve korunması konularında belirleyici kuralları kapsar. Aynı zamanda, kişisel verilerin siber tehditlere karşı korunmasını da hedefler.

Siber Suçlarla Mücadele Kanunu: Bu kanun, siber suçların tanımını yapar, siber saldırılar için hukuki yaptırımları ortaya koyar ve siber suçların önlenmesini hedefler.

Bilgi Güvenliği Rehberleri: BTK başta olmak üzere ilgili diğer kurumlar, siber güvenlik önlemlerini almak isteyen kurum ve bireyler için bilgi güvenliği rehberleri yayınlamaktadırlar. Bu rehberler, en iyi uygulamaları ve güvenlik standartlarını tanımlar.

Kamu Kurumları Siber Güvenlik Tedbirleri Yönetmeliği: Bu yönetmelik, kamu kurumlarına özgü siber güvenlik tedbirlerini ortaya koyar ve kamu hizmetlerinin siber tehditlere karşı nasıl korunması gerektiğine dair yönlendirmelerde bulunur.

Görüleceği üzere Türkiye, siber güvenlik altyapısını güçlendirmede konusunda kayda değer çalışmalara imza atmaktadır. Elbette tüm bunlar sürekliliği olan konulardır ve çalışmalar süregelecektir.

Tedbirler kamu ve özel sektör iş birliği ile alınmaya çalışılmaktadır. Özellikle son dönemde siber güvenlik alanında artan istihdam ihtiyaçlarının yine kamu ve özel sektör iş birliğiyle sağlanan eğitim olanaklarıyla genişletilmeye çalışıldığını gözlemliyoruz.

Ancak buna rağmen son iki yıldaki veri ihlallerine göz attığımızda ihalelerden doğan zararların maliyetlerinde artışlar gözlemlemekteyiz. Örneğin; IBM'in hazırladığı 2022 raporunda bir veri ihlali vakasının toplam maliyeti ortalama 4,35 milyon dolar olarak bildirilerek tarihin en yüksek seviyesine ulaşırken bu maliyet ortalaması 2021'e göre %2,6'lık, 2020'ye göre ise %12,7'lik bir artış anlamına gelmişti.

Tüm yasal ve reel önlemlere rağmen bu tip bir artışın ise şu şekilde açıklamak mümkün olabilir. Artık kurumlar işlerini ve işleri için değer olan ve değer yaratan öğelerinin çok daha büyük bir kısmı için teknolojik imkanları kullanarak işliyorlar. Kurumsal dijitalleşmenin boyutları artıyor. Dolayısıyla kurumların artan oranda dijital ortama akan verileri ve bu verilerin değerleri de giderek artış göstermektedir. O halde giderek değerlenen bu varlıkların da daha iyi korunması gerekmektedir.

Bu durumda da uluslararası iş birlikleri ve siber güvenlik standartlarına uyumu hızlandırmak adına gerçekleştirilen çalışmalara ek olarak kurumlar tarafından alınacak önlemlere gerekli özenin gösterilmesi ayrıca önem taşımaktadır.

Sonuç olarak; siber güvenlik, modern dünyanın kaçınılmaz bir gerçeğidir. Türkiye, bu alanda gösterdiği başarılı performansıyla siber tehditlere karşı daha dirençli bir yapıya sahip olmuştur. Ancak, siber dünyanın dinamik yapısı gereği, güncel tehditlere karşı daima hazırlıklı olmalı ve savunma stratejilerimizi sürekli yenilemeliyiz.

TEKNOLOJİK MÜKEMMELİYETİN, TURİZM SEKTÖRÜNE DOKUNUŞU

Antalya/Tekirova'nın elit tesislerinden Royal Diwa Resort, dijital dönüşümü benimseyerek konuk deneyimini yenilikçi bir sanat formuna dönüştürdü.

Turizm sektörü, dünyanın dört bir yanından gelen farklı kültürlerin, değerlerin ve beklentilerin bir araya geldiği benzersiz bir kavşaktır. Bu çeşitlilik, hizmet sağlayıcılarına her bir müşterinin ihtiyaçlarını ve arzularını anlama ve karşılama zorunluluğu getirir. Bu özgün ve karmaşık talepleri karşılamak için sektör, alanında uzmanlaşmış ve deneyimli profesyonellere ihtiyaç duyar. Bu profesyoneller, iş süreçlerinin mükemmel bir şekilde işlemesini sağlar, hizmet kalitesini artırır ve organizasyonun tüm potansiyelini ortaya çıkarır. Dolayısıyla, turizm sektöründeki başarının anahtarı, doğru çalışma partnerleriyle iş birliği yapmaktır. Bu sebeplerden dolayı turizmin Türkiye'deki merkezlerinden biri olan Antalya/Kemer'de hizmet veren Royal Diwa Resort, kusursuz hizmet anlayışını sürdürmek için 30 yılı aşkın süredir diğer sektörlere olduğu gibi turizm sektörüne de daima üstün hizmet ve yeni nesil teknoloji çözümleri sunan Turcom'la iş birliğine imza attı.

Bölgedeki ev sahibi otellerden biri olan Royal Diwa Resort, Antalya'nın tüm güzelliğini misafirleriyle buluşturuyor. Müşteri memnuniyetinden taviz vermeme ilkesiyle konuklarını ağırlayan Royal Diwa Resort, misafirlerine her türlü rahatlığı sağlamak ve sunduğu konforu arttırmak için başlattığı renovasyon süreci kapsamında doğan altyapı ihtiyaçlarını kısa sürede ve kusursuz şekilde karşılamak, ayrıca kaliteli hizmet almak için Turcom topluluğunun çözümlerinden faydalandı.

Misafirlerinin rahatı için her türlü ayrıntının düşünüldüğü ferah, rahat ve konforlu odaların bulunduğu lüks bloklar için planlanan yenilenme kapsamında internet erişimiyle ilgili yenilikler de unutulmadı. Kusursuz internet erişimi, misafirlerin teknolojik ihtiyaçlarını karşılamakla kalmaz, işletmenin güvenlikten satışa kadar tüm iş süreçlerinin kesintisiz ilerlemesinin de anahtarıdır. Hızlı ve kesintisiz internet erişim altyapısının gereksinimleri nedeniyle Royal Diwa ve Turcom bir araya geldi. Projenin ilk etabında, otelin zayıf akım servisleri alanında iş birliği yapıldı. Turcom zayıf akım ekibi tarafından proje sonrasında sahada yapılan analizlerle işletmenin elektrik altyapısına müdahalede bulunuldu. Tüm elektrik altyapısı, internet erişiminin kusursuzluğu için projenin iletişim altyapısı A'dan Z'ye, detaylı bir uzmanlıkla yeniden tasarlandı.

Royal Diwa, mimarisinde doğayla uyum içinde olan ve her biri dört kattan oluşan çok sayıda bloğa sahiptir. Bu turistik mimari, Royal Diwa'ya eşsiz bir özellik katmasına rağmen, teknolojik altyapı açısından bazı zorlukları da beraberinde getiriyordu. Dağıtık yapılı bu yerleşkede, elektriksel altyapının yanlış planlanması otelin tüm teknolojik yapısını olumsuz yönde etkileyebilirdi. Royal Diwa'nın benzersiz mimarisine uyum sağlayacak şekilde planlanan kenar kabin yerleşimleri, ana binadaki teknolojik altyapının merkezi olan sistem odasıyla hızlı fiber bağlantılarla entegre edildi. Turcom'un uzmanları tarafından tasarlanan bu merkezi ve detaylı elektriksel mimari, mükemmel bir uygulama ile projenin bu bölümünü başarıyla tamamladı.

Sonraki aşamada, dağıtık yapıdaki konuk adalarında aktif internet erişimi amacıyla harekete geçildi. Kenar kabinlerden başlayarak odalarda kritik iletişim ihtiyaçları için AP (access point) ve telefonlara CAT6 standardında erişim sağlandı. Yeni sezona hazırlık yapan Royal Diwa, doğa ile teknolojinin mükemmel uyumu konusunda gösterdiği hassasiyetle elektriksel altyapının kusursuz olmasını hedefledi. Bu sistem, sonlandırma ve testlerin ardından etiketleme ile tamamlandı ve işletmenin titiz IT ve Teknik yönetim ekibine teslim edildi.

KESİNTİSİZ OLMAK ŞART İSE...

Elektriksel altyapının mükemmeliyetini garantileyen kampüste, kenar kabinlere enerji sağlayan şebeke elektriğine yönelik olası kesintilere karşılık önlemler alındı. Bu doğrultuda, sürdürülebilirlik amacıyla 15 ve 10 kVA'lık kesintisiz güç kaynakları devreye sokuldu.

TEKNOLOJİNİN TESİS ÜZERİNDEKİ SON DOKUNUŞU, KONUK AĞIRLAMANIN DİJİTAL DÖNÜŞÜMLE YENİ BİR SANAT FORMUNA DÖNÜŞMESİNİ SAĞLADI

Bu prestijli tesis, misafirlerine benzersiz bir dijital deneyim sunmak amacıyla altyapıda büyük bir dönüşüme gitmekle kalmayıp son katmandaki erişim mimarileri için de Turcom' un seçkin ağ hizmetlerinden yararlandı. Otelin özgün oda dağılımı dikkate alınarak, her katta ideal internet erişimi sağlanması için detaylı bir ağ planlaması gerçekleştirildi.

Switchler, AP'ler ve diğer gerekli donanımların hızla teslimi ve konfigürasyonuyla müşteri memnuniyeti en üst seviyeye taşındı.

Böylece, Royal Diwa Resort'ta konaklayan misafirler kesintisiz iletişimin keyfini sürerken, işletmenin iş süreçleri de akıcı bir şekilde ilerlemekte. Bu, dijital dönüşümün modern konuk ağırlama anlayışında sadece bir gereklilik olmadığını, aynı zamanda bir sanat formu haline geldiğini gözler önüne seriyor.

MAESTRO İLE ÖLÇEKLENEBİLİR AĞ GÜVENLİĞİ

CHECK POINT™

Günümüzde hiper ölçekli sistemler yüksek talep görüyor ve BT departmanları arasında giderek daha fazla benimseniyor. BT ve ağ endüstrisi, özel bulutların (private cloud) güvenliğinin sağlanmasına ve aynı zamanda genel bulut (public cloud) hizmetlerinin operasyonel esnekliğine ve çevikliğine öykünülmesine büyük ilgi duyuyor.

Hiper ölçekli ağ güvenliği çözümleri esneklik sağlar ve aynı zamanda finansman açıdan tasarruf etmenizi sağlarken performansı da önemli ölçüde artırır. Üstelik inanılmaz derecede hızlı devreye alınır ve bulut düzeyinde esnekliğe sahip olursunuz.

HİPER ÖLÇEKLİ AĞ GÜVENLİĞİNİN TEMEL AVANTAJLARI

Hiper Ölçeklenebilirlik

Gereksinim oldukça her ölçekteki mevcut ağ güvenlik sistemini birkaç dakika içinde tekil kapasitesinin 50 katına kadar artış imkanı sağlar. Yataydaki genişleme sorunsuzdur ve kurumun mevcut yatırımlarını korur.

Operasyonel Basitlik

Bir kurumun tüm güvenlik duvarları, tek bir birleşik güvenlik sistemi olarak merkezi olarak yönetilir ve yönetim yükü en aza indirilir. Çözümün basitliği, ağ geçitlerini hızlı bir şekilde devreye alma yeteneğinde ve tek bir ekran aracılığıyla otomatikleştirilmiş yönetim yeteneklerine sahip olmasıdır. Ölçeklendirme, birkaç dakikada otomatik olarak tamamlanır.

Bulut Seviyesinde Dayanıklılık ve Maliyet Verimliliği

Tek bir birleşik sistem altında verimli bir N+1 kümeleme dağıtımı elde edersiniz. Tek bir sisteme dayalı birden çok mantıksal ağ geçidini yönetirken, maksimum maliyet verimliliği için tüm donanım kaynaklarından tam olarak yararlanabilirsiniz.

TÜM KURUMLAR İÇİN TEK GÜVENLİK ÇÖZÜMÜ

İster küçük ölçekli bir kurum olun ister kurumunuz hali hazırda yüksek kapasiteli bir güvenlik altyapısına sahip olsun, Hiper Ölçekli Ağ Güvenliği çözümü mevcut ve gelecekteki yatırımlarınızı güvence altına almanın ve korumanın en iyi yoludur.

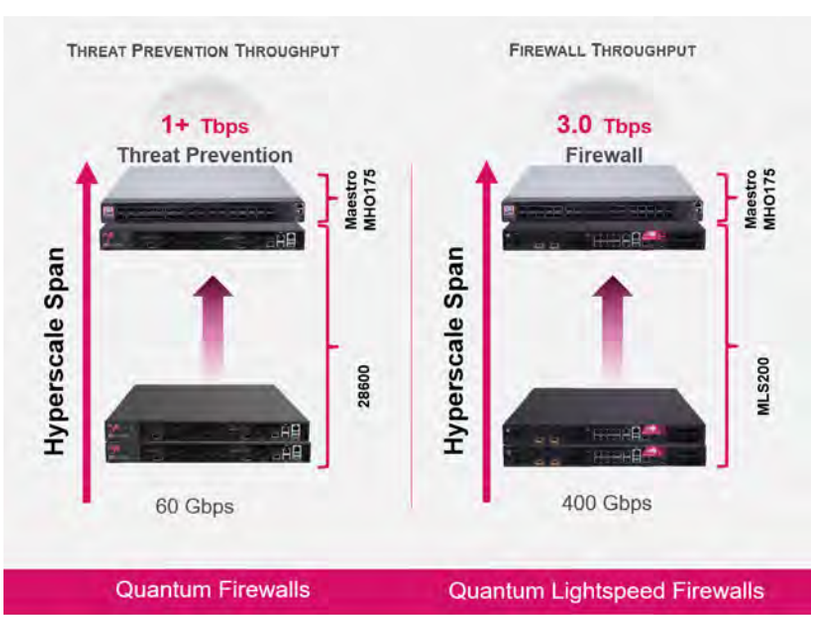
Güvenlik dünyasının ilk gerçek Hiper Ölçekli ağ güvenliği çözümü Check Point Maestro, her büyüklükteki kurumun esnek bulut düzeyindeki güvenlik platformlarının gücünden yararlanmasını sağlayan devrim niteliğinde bir özel bulut mimarisidir. Güvenlik talepleri değiştikçe, mevcut güvenlik kümesi performansını saniyede 100 Gigabit'ten saniye başına Terabit'e kadar sorunsuz bir şekilde genişleyebilir.

Check Point Maestro, Check Point HyperSync teknolojisine dayalı verimli N+1 çalışma yöntemiyle bulutun ölçeklenebilirliğini, çevikliğini ve esnekliğini şirket içinde bir araya getirerek mevcut güvenlik ağ geçitlerinizin yeteneklerini en üst düzeye çıkarır. Birden fazla Check Point güvenlik ağ geçidini, ihtiyaca göre ölçeklenen ve iş yüklerini sistem arasında paylaşan akıllı, çevik bir sistemde bir araya getirerek kendi sanallaştırılmış özel bulut sisteminizi oluşturabilirsiniz.

Check Point Maestro, Check Point HyperSync teknolojisine dayalı verimli N+1 çalışma yöntemiyle bulutun ölçeklenebilirliğini, çevikliğini ve esnekliğini şirket içinde bir araya getirerek mevcut güvenlik ağ geçitlerinizin yeteneklerini en üst düzeye çıkarır. Birden fazla Check Point güvenlik ağ geçidini, ihtiyaca göre ölçeklenen ve iş yüklerini sistem arasında paylaşan akıllı, çevik bir sistemde bir araya getirerek kendi sanallaştırılmış özel bulut sisteminizi oluşturabilirsiniz.

YETERİNCE AL GEREKİNCE ÖLÇEKLENDİR

Check Point Maestro ile kurumlar, tıpkı genel bulut ortamında yeni bir sunucu oluşturur gibi, ihtiyaç halinde mevcut Check Point güvenlik ağ geçitlerinin ölçeğini kolaylıkla büyütebilirler. Maestro, tek bir ağ geçidinin dakikalar içinde 52 ağ geçidinin kapasitesine ve performansına genişletilmesini sağlayarak şirketlere esneklik kazandırır ve devasa Terabit/saniye güvenlik duvarı verimi sağlar. Bu benzeri görülmemiş ölçeklenebilirlik, kuruluşların 5G ağlarının yüksek veri hızlarını ultra düşük gecikmeyle desteklemesine ve en büyük, en çok kaynak tüketen ortamları güvence altına almasına olanak tanıyarak hiper ölçekli ağ güvenliğinde yeni standartlar belirliyor. Check Point Maestro, küçük ortamlardan en zorlu veri merkezi, e-ticaret ve servis sağlayıcı ağlarına kadar ölçeklenen gelişmiş güvenlik yeteneklerini genişletir.

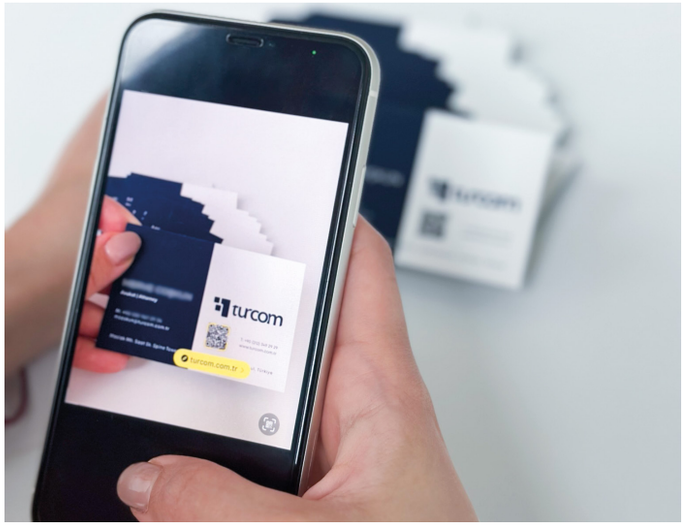


Check Point Maestro Hiper Ölçekli Ağ Güvenliği

trcVCard

turcom

Güncel Kartvizit Bilgilerinizi Dijital Olarak Paylaşmanın En Hızlı Yolu!



DİJİTALLEŞEN ÇAĞA ADIM ATIN!

trcVCard, geleneksel kartvizitleri dijital ortama taşıyarak, iletişim bilgilerini anında güncel ve erişilebilir kılar. QR kodun MS 365 entegrasyonu ile kullanıma sunulan bu pratik uygulamayla çalışanlarınız için sürekli kartvizit bastırmak zorunda kalmazsınız.
Güvenli ve sürekli güncel bilgi paylaşımı çevre dostu bir yaklaşımla mümkün olur.
trcVCard ile modern ve etkin bir iletişim deneyimi yaşarsınız.

- Etkin İletişim ve Zaman Tasarrufu
- Geniş Uyumluluk
- Güvenli
- MS 365 ile Entegrasyon
- Çevre Dostu Bir Seçim

Demo talepleriniz veya ayrıntılı bilgi için kodu okutarak bize ulaşabilirsiniz.

turcom

Gelecek 100 Yıla

Cumhuriyetimizin 100. yılında, Turcom olarak, 30 yılı aşkın tecrübemizle teknolojinin işletmeler için vazgeçilmez önemini vurguluyoruz. Teknoloji yatırımı, işletmelerin rekabet gücünü ve yenilikçiliklerini artıran temel bir unsurdur. Teknolojiyi, işletmelerin varoluş ve gelişiminin temeli olarak görüyoruz.

Türk teknoloji sektöründe öncü bir topluluk olarak, lisans optimizasyonundan kurumsal iletişim ve sistem altyapısına kadar yeni nesil bir anlayışla hizmet sunuyoruz. Ayrıca, Turcom Ar-Ge'nin yoğun çalışmaları ile sürekli gelişen Generative AI, Blockchain ve siber güvenlik gibi güncel teknolojileri temel alan yenilikçi kurumsal teknoloji çözümlerimizle hem yerli hem de yabancı pazarları hedefliyoruz.

Uzman ekiplerimiz, binlerce referansımızın da teyit ettiği üzere, müşterilerimizin iş süreçlerini güvenli ve verimli hale getirmede büyük rol oynamaktadır. Bu bağlamda, Cumhuriyetimizin yeni yüzyılında, sektörel ihtiyaçlara özel çözümlerimizle ayrışarak inovatif teknolojilerle alanımızda liderliği sürdüreceğiz.

Yenilikçi ve sürdürülebilir çözümlerle sektördeki konumumuzu güçlendireceğiz. Geçmişten aldığımız güçle, teknoloji alanında yenilikler sunarak toplumun gelişimine katkıda bulunacağız.

Cumhuriyetimizin ikinci yüzyılında, yenilik, kalite ve güvenin simgesi olarak anılacağız.

Geleceğe yönelik vizyonumuz, daha parlak bir gelecek inşa etmek üzerine kurulu. Bu vizyonu gerçekleştirmek için var gücümüzle çalışacağız.

100

Maslak Mah. Saat Sok. Spine Tower No:5 Kat:14 34485 Sarıyer / İstanbul | +90 212 349 29 29 | info@turcom.com.tr