Türk Petrol Devi TÜPRAŞ, Bilgi Güvenliği Süreçlerini Forcepoint'in Yardımıyla Güvende Tutuyor

Türkiye'nin en büyük petrol rafinerisi, kullanıcı ve verilerini kötü niyetli kişi ve organizasyonlara karşı korumak için Forcepoint Web Güvenliği Karma ve DLP çözümlerine güveniyor.

TÜPRAŞ, Türkiye pazarındaki petrol ürünlerinin büyük çoğunluğunun işlenmesinden ve tedarik edilmesinden sorumlu ve şirketin işletmekte olduğu dört rafineri, Türkiye'nin kritik altyapısının omurgasını oluşturuyor. Ulus devletler de dahil olmak üzere kötü amaçlı organizasyonların bu tür tesisleri hedef aldığı bir dünyada, bu tesislerin güvende tutulması kritik önem taşıyor. TÜPRAŞ da bu korumayı sağlaması için Forcepoint'e güveniyor.

MÜŞTERİ PROFİLİ:
Türkiye'nin petrol rafineri kapasitesinin büyük kısmını ve ülkenin petrol ürünleri depolama kapasitesinin yaklaşık %60'ını kontrol eden, ülkenin en büyük petrol rafinerisi.

SEKTÖR:
Petrol ve Gaz

MERKEZ ÜLKE:
Türkiye

ÜRÜNLER:
› Forcepoint Web Security Hybrid
› Forcepoint Data Loss Prevention

Fortune 500 listesindeki üreticiler için dinamik ve rekabetçi bir dönemden geçiyoruz. Dünya çapındaki büyük ölçekli ağır sanayi şirketleri, üretim süreçlerinin otomatik hale getirilmesini sağlayan makine öğrenimi gibi yeni teknolojileri benimsiyor ve dünya çapında endüstriyel otomasyon pazarının 2018 ile 2026 arasında yaklaşık iki kat büyüyerek 296,7 milyar $ seviyesine erişmesi bekleniyor. Bu durum, diğer hiçbir sektörde petrokimya sektöründe olduğu kadar geniş kapsamlı değil. Türkiye'nin en büyük petrol rafinerisi olan ve yapay zeka tabanlı akıllı robotlar, IoT ve büyük veri analizi gibi teknolojileri benimseyen TÜPRAŞ, küresel Endüstri 4.0 hareketinin en ön saflarında yer alıyor.

Endüstri 4.0 teknolojileri, üretimi daha verimli hale getirse de endüstriyel verilerin, sistemlerin ve ağların korunmasını da her zamankinden daha önemli kılmış durumda. TÜPRAŞ'ın işletmekte olduğu dört petrol rafinerisi gibi kritik altyapı unsurlarına yapılan siber saldırılar, üreticinin bağlı kullanıcılar, uygulamalar ve ağa bağlı sistem ve cihazlardan oluşan zincirindeki en zayıf halkayı hedef alabiliyor.

TÜPRAŞ Bilgi Güvenliği Müdürü Alper Sulan, konuyla ilgili olarak, "Küresel petrol ve gaz şirketlerinin neredeyse dörtte üçü, en azından bir siber saldırıyla karşılaştı. Endüstrideki tüm kurumlar gitgide daha bağlı teknolojiler kullanmaya başladıkça, saldırıların sıklığı, karmaşıklığı ve etkisi de artmaya devam ediyor. Bu saldırılar, kırılma, patlama, yangın, tehlikeli maddelerin serbest kalması veya dökülmesi sonucunda insan sağlığı ve çevre açısından çok ciddi sonuçlar doğurabiliyor. İnsanlar ve alt yapı için felaket niteliğinde sonuçlar doğurabilecek hizmet ve dağıtım kesintilerini önlemek için ekstra dikkatli olmamız gerekiyor" ifadesini kullandı.

Doğru siber güvenlik ortağının seçilmesi, TÜPRAŞ'ın endüstri lideri ve Türkiye altyapısının temel unsurlarından biri olarak konumunu koruması açısından çok önemliydi.

Rafinerileri korumak için arka ofisleri güvenlik altına almak

Mevcut web güvenliği çözümünden memnun olmayan ve değerli ve hassas bilgilerde sızıntı yaşanması olasılığından endişe duyan TÜPRAŞ, siber güvenliğinin iyileştirilmesi gerektiğine karar verdi.

TÜPRAŞ BT Risk ve Uyum Amiri Cansu Altınışık, konuyla ilgili olarak, "Saldırı vektörlerine ve kötü niyetli kişilere baktığımızda, şirket ağlarına genellikle e-posta veya web üzerinden iletilen kötü niyetli bağlantılarla sızmaya çalıştıklarını görüyoruz. Ayrıca hatalı pozitif sonuçlar ve görünürlük konusunda da sorun yaşıyorduk, güvenliğin tam sağlandığından emin değildik ve koruma kapsamımız yalnızca ofis içi kullanımla sınırlıydı. Nihayetinde, verilerin kimin tarafından, nasıl ve ne amaçla kullanıldığını bilmiyorduk" yorumunda bulundu.

TÜPRAŞ, hem hassas kişisel verileri koruyacak hem de arka ofis operasyonlarının rafineriler ve diğer endüstriyel tesisler için birer saldırı vektörü haline gelmesini önleyecek bir siber güvenlik çözümü arıyordu. Özellikle pek çok ihtiyacı aynı anda karşılayacak bir güvenlik çözümüne ihtiyaç vardı:

- → E-postalardaki riskli fidye yazılımı bağlantılarını engellemek ve kritik altyapıları hedef alan Dragonfly 2.0 gibi bilgisayar korsanı grupları tarafından yürütülen kimlik avı veya botnet saldırıları gibi harici saldırılara karşı koruma sağlamak.
- → Kullanıcıları çalıştıkları ve bağlandıkları her yerde korumak için web güvenliğini ofis dışını da kapsayacak şekilde genişletmek.
- → AB'de GDPR ve Türkiye'de Kişisel Verilerin Korunması Kanunu gibi düzenlemelerle uyum sağlamak.
- → Verilerin kurum içerisinde ve dışında nasıl aktarıldığı konusunda daha iyi bir denetim ve kontrol sağlamak.

Zorluklar

Arka ofis BT operasyonlarını harici ve dahili tehditlerden korumak.

GDPR gibi veri koruma düzenlemelerine uyum sağlanmasına yardımcı olmak.

Yaklaşım

Tüm şirket bilgisayar ve cihazlarına yüklenen aracı tabanlı bir çözümde Forcepoint Web Güvenliği Karma çözümünü DLP ile birlikte kullanmak.

Kritik altyapılar için en iyi güvenlik çözümleri gerekir

Petrol devi, yeni bir web güvenliği ve DLP çözümü seçmek üzere Kavram Kanıtlama (PoC) çalışması için pek çok tedarikçiyi bir araya getirdi. TÜPRAŞ, web güvenliği ve DLP özelliklerini bir araya getirebilen ve kurumsal ağa bağlı tüm bilgisayar ve cihazlara yüklenebilecek bir çözüm arıyordu.

Forcepoint Web Security GW Karma ve Forcepoint DLP çözümleri, web saldırılarına engel olma ve hatalı pozitif sonuçları en aza indirme konusunda en yakın rakibinden iki kattan fazla puan alarak PoC çalışmasında açık ara en yüksek puanı aldı. TÜPRAŞ ayrıca, Forcepoint'in GDPR ve KVKK gibi düzenlemelere uymayı kolaylaştıran kişiselleştirilebilir politika kitaplıklarından ve TÜPRAŞ'ın teknoloji tabanlı kendi yol haritasına uygun olarak görülen riske uyum sağlayan koruma çözümlerinden ve siber güvenlik konusundaki insan merkezli yaklaşımından da etkilendi.

Altınışık, "Forcepoint Web Security Hybrid çözümü sayesinde ofis içinde veya dışında tam koruma sağlayabiliyoruz ve çalışanlarımız web veya e-posta üzerinden gelebilecek her türlü tehdide karşı koruma altında. Forcepoint DLP ile de verilerimizin kullanılma şekli, gönderildiği yerler, hangi verilerin kritik olup, hangilerinin olmadığı konusunda tam bir kontrol sağlıyoruz, kullanıcı ve veri etkileşimi konusunda da tam görünürlüğe sahibiz. Forcepoint bize tam kapsamlı bir raporlama fırsatı sağlıyor" diyor.

TÜPRAŞ, özellikle DLP'nin kolayca devreye alınmasından memnun kaldı. Altınışık, bu konuyla ilgili olarak, "Özellikle Forcepoint'in sunduğu ön tanımlı binlerce DLP kuralını kullanarak veri güvenliği politikalarımızı çok hızlı bir şekilde uygulayabildik. Ayrıca, iyi niyetle kötü amaçlı davranışlar arasında ayrım yapabilmek için bazı özel politikalar da ekledik" ifadesini kullanıyor. "Hukuk veya denetim ekibimizin tanımladığı şekliyle kişisel verileri filtreler aracılığıyla tanımlayabiliyor ve kurum içinde veya dışında aktarılmalarına izin veren veya aktarımı kısıtlayan politikalar uygulayabiliyoruz. Bu sayede, kullanıcılar artık kişisel verileri yükleyemiyor, kopyalayıp yapıştıramıyor veya yazdıramıyor."

Küresel durumda radikal bir değişiklik olduğunda, Forcepoint ile ortaklığın önemi daha da arttı. Altınışık, "COVID-19 salgını yüzünden tüm çalışanlarımız siber risklere karşı korunmalı bir şekilde evden çalışmak zorunda kaldı. "Forcepoint Web Güvenliği Karma çözümünün sağladığı 7-24 koruma sayesinde ne yapacağımız konusunda hiçbir endişe yaşamadık. Forcepoint, bulut güvenliğine geçiş ve web'de gezinmede daha yüksek performans için çok hızlı bir destek sundu" diyor.

İç ve dış tehditlere karşı koruma

Forcepoint çözümleri sayesinde TÜPRAŞ artık iç ve dış tehditlere karşı sistem çapında koruma sağlama hedefine ulaşmış durumda. Şirket, Web Güvenliği çözümü, siber tehdit oluşturabilecek URL'leri engelleyerek, şirketin İnternet'ten gelen botnet saldırılarına ve kimlik avı veya fidye yazılım bağlantıları içeren e-posta saldırılarına karşı korunmakta. Forcepoint aracısı, Web Güvenliği ACE Motorunun da yardımıyla, gelen e-posta saldırılarını doğrudan durdururken, hassas verilerin de e-posta, web ve taşınabilir diskler, yazıcılar ve üçüncü taraf uygulamaları gibi popüler uç nokta kanalları üzerinden sızdırılmasını engelliyor.

TÜPRAŞ artık güçlü ve risklere uyum sağlayan Forcepoint Web Security ve DLP çözümleri sayesinde şirket fikri mülkiyeti, kritik sistemlerdeki veriler, çalışan verileri ve finansal veriler gibi kritik verileri koruma konusunda kendi standartlarını ve yasal düzenlemeleri karşılayabiliyor.

TÜPRAŞ CISO'su Alper Sulan, "Forcepoint, bizim için güvenilir bir danışman ve bilgi güvenliği çözüm ortağı" ifadesini kullanıyor. "KVKK ve benzer düzenlemelere uyum sağlama konusunda bizim için çok önemli bir yardımcı. Tam korumalı Web Security ve DLP çözümleri sağlamanın yanı sıra, buluttaki operasyonlarımızı geliştirdikçe kullanmayı düşündüğümüz CASB ve Dynamic Edge Protection gibi çözümlerle bugün ve gelecekteki dijital dönüşümümüzde Forcepoint ile birlikte büyüyebileceğimizi biliyoruz."

Sonuçlar

Botnet'lere, kimlik avı saldırılarına, fidye yazılımlarına ve iç tehditlere karşı daha iyi koruma.

Veri koruma kanun ve standartlarına uyumun kolaylaştırılması.