Boru hattına siber saldırı ile **ortaya çıkan OT güvenliği ihtiyacı**

Colonial Pipeline Boru Hattı, 8 Mayıs tarihinde bir fidye yazılımı saldırısının kurbanı oldu ve bu sebeple tüm operasyonlar durdurulmak zorunda kaldı. OTD Bilişim'den Eray Atlas, "Colonial Pipeline boru hattında saldırı, yakıt boru hattının kapatılmasını ve artırılmış OT güvenliği ihtiyacını işaret ediyor." dedi.

ABD'nin en büyük yakıt boru hatlarından biri olan Colonial Pipeline Boru Hattı, 8 Mayıs tarihinde bir fidye yazılımı saldırısının kurbanı oldu ve bu sebeple tüm operasyonlar durdurulmak zorunda kaldı. Doğu Sahili'ndeki petrol ve gazın neredeyse yarısının elde edildiği Colonial Pipeline'daki saldırı siber suçluların neden petrol ve gaz sektörlerini hedef aldığını gösteren en güncel örnektir.

FİDYE YAZILIMI İLE SALDIRILAN COLONIAL PIPELINE

The Wall Street Journal'un raporuna göre ABD'nin en büyük benzin boru hattının işletmecisi Colonial Pipeline, fidye yazılımı saldırısı yüzünden 7 Mayıs gibi operasyonlarını durdurmak zorunda kaldı. Siber suçlular, enerji piyasalarını alt üst etmekle tehdit etmekle kalmıyor, Doğu Sahili'nde gaz ve dizel arzını da altüst ediyor. Colonial Pipeline, Amerika Birleşik Devletleri'nin doğu yarısı için önemli bir geçit görevi görmektedir. Boru hattı, günde 4 milyon varile yakın kapasitesi ile Doğu Kıyısı için ana benzin, dizel ve jet yakıtı kaynaklarından biridir. Cumartesi günü, kurumsal BT ağlarını da etkileyen bir fidye yazılımı saldırısının kurbanı olduklarını belirten bir bildiri yayınlandı. Bu saldırı, boru hatlarını kontrol eden ve şirket ağından ayrı olan yakıtı dağıtan operasyonel ağlar üzerinden gerçekleştirilmedi. Colonial Pipeline, saldırının yayılmasını engellemek için önlem olarak boru hatlarını kapattıklarını ilan etti.

Güvenlik endüstrisindeki birçok insanın ilk düşüncesi, bunun yabancı bir hükümet tarafından yapılan başka bir saldırı olduğu yönündeydi. Ancak Bloomberg, 8 Mayıs Cumartesi günü saldırıya DarkSide adlı fidye yazılımı grubunun öncülük ettiğine ilişkin bir rapor sundu. "Çifte gasp" planları ile bilinen DarkSide, perşembe günü Colonial ağından iki saat içerisinde neredeyse 100 gigabyte veri elde etti. Saldırganlar, talep ettikleri fidyeyi ödememeleri durumunda Colonial Pipeline boru hattını, çaldıkları tüm verileri internete sızdırmakla ve saldırganların bilgisayarına şifreleyip Colonial'in ağını tamamen kilitlemekle tehdit etti. Siber suçluların ne kadar para istediği ve ağlarını ne şekilde kullandığı belli değil. Ancak apaçık olan bir şey var ki o da bu saldırının ölçeğine ya da sektörüne bakmaksızın siber suçluların endüstriyel kuruluşlara odaklandığının somut bir örneği olduğudur.

CAZİP HEDEF: PETROL VE GAZ ENDÜSTRİSİ

Yıllar içerisinde petrol ve gaz endüstrisi, küresel ve ulusal ekonomiler için kritik öneme sahip olduğundan en güçlü ve ekonomik olarak küresel endüstrilerden biri haline geldi. Rakipler, bu sektörleri Endüstriyel Kontrol Sistemleri (ICS) güvenlik açıklarından yararlanmak üzere değerli hedefler olarak gördüğünden büyük bir hedef olarak görülür oldu. Eskiden petrol ve

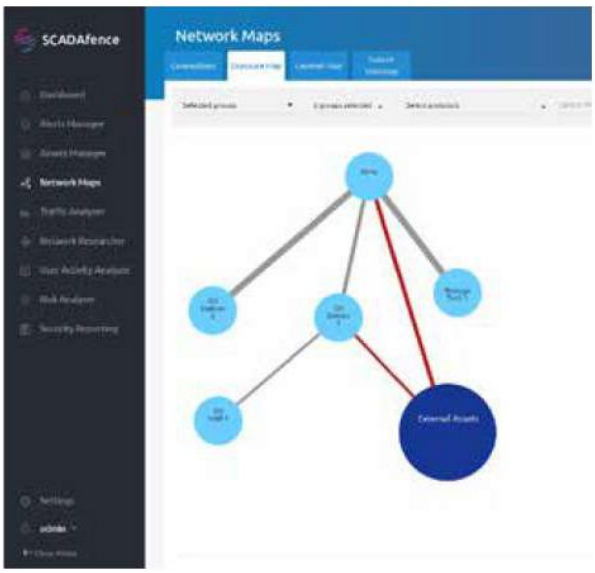
gaz operasyonlarında ihtiyaç duyulan operasyonel teknoloji (OT) izole edilmiş ve "hava boşluklu" idi ancak günümüzde operasyonel teknoloji ağları, saldırılara karşı yeni bir kapılar açan farklı BT altyapılarına ve Internete daha sık bağlantı sağlamaktadır. Petrol ve gaz operasyonlarında OT ve BT ortamlarının birleşmesi, yakınsaması, hem BT hem de OT ortamlarında sonsuz miktarda güvenlik açığının meydana gelmesine sebep oldu. Ayrıca Nesnelerin Interneti (IoT) cihazlarından kaynaklanan riskler ve uyumluluk odaklı devam eden ve büyüme gösteren öncelikler de bulunmaktadır. Pemex ve Colonial Pipeline gibi gaz ve petrol kuruluşlarına düzenlenen son saldırılardan da göründüğü üzere farklı davranışları anlamaktan kuruluşları nasıl kullanacaklarına kadar saldırganların elde ettiği pek çok avantaj bulunmaktadır. Bu sebeple küresel ekonominin ve sivil güvenliğin herhangi bir saldırıdan etkilenmemesi için petrol ve gaz kuruluşlarının her türlü siber saldırı yöntemine karşı korunması gerekli hale gelmiştir.

PETROL VE GAZ OPERASYONLARININ KORUNMASI

Colonial Pipeline saldırısında rakiplerin kurumsal ağları başarılı bir şekilde nasıl kullandığına ilişkin detaylar kamuya açıklanmamış olmasına rağmen gaz ve petrol kuruluşlarının güçlü bir OT güvenlik stratejisi uygulama zamanının çoktan geldiğini gösterdi. Geçtiğimiz ay NSA, endüstriyel kontrol sistemlerini (ICS) ve operasyonel teknolojiyi (OT) siber saldırılardan korumanın önemini açıklayan bir rapor yayınladı. Raporda NSA, "OT ağlarını ve kontrol sistemlerini BT ve iş ağı izinsiz girişleri yoluyla ortaya çıkan güvenlik açıklarına karşı dayanıklı hale getirmek için doğrudan eyleme geçilmedikçe OT sistem sahipleri ve operatörler, savunulamaz risk seviyelerinde kalacaktır." dedi. Ek olarak, NSA raporu, kuruluşların ve operatörlerin kritik operasyonları korumaları gerektiğini ifade etti.

"OT sistemleri, düzgün çalışmak için nadiren harici bağlantıya ihtiyaç duyar. Ancak gerçek risk ve potansiyel olumsuz iş ve görev sonuçları göz önünde bulundurulmadan kolaylık sağlamak için sıklıkla bağlantı sağlarlar. Vakit kaybetmeden harekete geçmek, siber güvenliği geliştirmeye ve göreve hazır hale gelmeye yardımcı olabilir." NSA, tavsiyelerini kapsayan bu raporu yayınlamadan önce, birçok petrol ve gaz kuruluşu, OT sistemlerini ve ağlarını korumak için gerekli önlemleri aldı. Son yedi yıldır SCADAfence, OT ağlarının güvenliğini sağlamak ve uygun siber güvenlik altyapısının uygulanmasını sağlamak için petrol ve gaz opertörleri de dahil olmak üzere birçok kritik altyapı kuruluşuyla çalışmaktadır. Bunu da tam ağ görünürlüğü sunarak yapıyor ve fidye yazılımı saldırı kaynaklı anormallikler de dahil olmak üzere her türlü anormal hareketi ve kötü niyetli davranışı doğru bir şekilde tespit ediyor.

> SCADAfence, OT ağlarının güvenliğini sağlamak ve uygun siber güvenlik altyapısının uygulanmasını sağlamak için petrol ve gaz operatörleri de dahil olmak üzere birçok kritik altyapı kuruluşuyla çalışıyor.



UYGULAMADA YAĞ ÖRNEĞİ ŞEMASI

Yukarıdaki şema, SCADAfence'in Petrol ve Gaz ve boru hattı endüstrilerindeki kuruluşların BT ve OT ağları arasında tam görünürlüğe sahip olmalarına ne şekilde yardımcı olduğunu göstermektedir. Bu sayede saldırı vektörlerinin lokasyonu saptanır ve ağlar arasındaki tüm bağlantıları kesin doğrulukla tanımlanabilir. Bu yaklaşım sayesinde yüzlerce kuruluşun operasyonel ağlarında daha sonra bir siber saldırıya dönüşebilecek anormal faaliyetleri başarıyla azaltılması sağlanmıştır.

OPERASYONEL TEKNOLOJİ DÜNYASINDA, PLAN YAPAMAMAK = BAŞARISIZLIĞI PLANLAMAK

Temel siber güvenlik uygulamaları, bu saldırıların ilerlemesini önlemeye yardımcı olabilir. Bu da göremediklerimizi korumak da zor olduğundan tüm ağın görünür hale getirilmesini de içerir. Ek güvenlik uygulamaları, mümkünse ağ segmentasyonu ve hatta mikro segmentasyonu da kapsar ve sürekli ağ izleme faaliyeti, benzer saldırıların ilerlemesini önlemek için büyük öneme sahiptir. Pek çok petrol ve gaz operatörü, OT ağlarına görünürlük sağlamak ve kritik altyapı ağlarını güvende tutmak amacıyla halihazırda kesintisiz ağ izleme ve tehdit algılama teknolojilerini kullanıyor. Ağ izleme, anormallik tespiti, uzaktan erişim görünürlüğü ve uyumluluğa ilişkin bu bütüncül yaklaşım ile pek çok petrol ve gaz kuruluşu gelecek saldırılara karşı risk düzeyini %95 oranında azaltmıştır. Bunun en iyi yanı ise bu çözümlerin aracı gerektirmemesi, müdahaleci nitelik taşımaması ve bir çalışanın maliyetinin çok altında söz konusu görevleri yerine getirebilmesi. Eğer sizin de kuruluşunuzun endüstriyel ağlarını güvence altına almanız gerekiyorsa, SCADAfence'in OT ağlarında ne şekilde tam görünürlük sağladığını ve kötü amaçlı bir faaliyetin gerçek zamanlı tehdit algılamasını nasıl gerçekleştirdiğini öğrenmek için ihtiyacınız olan tek şey 100 Petrol ve Gaz Endüstri Lideri ile gerçekleştirdiğimiz vaka çalışmasını indirmek. SCADAfence Platformunu denemek ve OT ağınızdaki tüm güvenlik açıklarını bulmak istiyorsanız size yardımcı olmaktan memnuniyet duyarız. Ürünlere ilişkin daha detaylı bilgi almak ve PoC Talebiniz için"https://onlineteknikdestek.com/Pocrequest?culture=tr" adresini ziyaret edin.Bu hikâye hakkında daha ayrıntılı bilgi ve ürün hakkında detaylı bilgi almak isterseniz, OTD BİLİŞİM satış ekibi ile iletişime geçebilirsiniz.