Kusurlu **nokta**

Çoklu ağ arayüzüne sahip kontrolörler, zaman zaman SCADA ve I/O ağlarını "ayırmak" için kullanılır ancak böyle bir ayrımdan bahsetmek mümkün değil. İşte, endüstriyel ağların güvenlik mimarisinde sıklıkla gözden kaçan bir faktör; "kusurlu nokta". Siber saldırganlar bu kusuru nasıl manipüle eder? OTD Bilişim Hizmetleri şirketinden Eray ATLAS anlatıyor.

Aşağıda çeşitli yerlerde karşımıza çıkan endüstriyel ağ mimarisinin şeması yer almaktadır. Şemada, birden fazla ağ arayüzüne sahip bir PLC vardır ve bu durumda PROFINET özellikli bir Siemens S7-300 ya da S7-1500 ile bir tarafta SCADA ağı bağlanırken, diğer tarafta I/O ağı bağlanmaktadır.

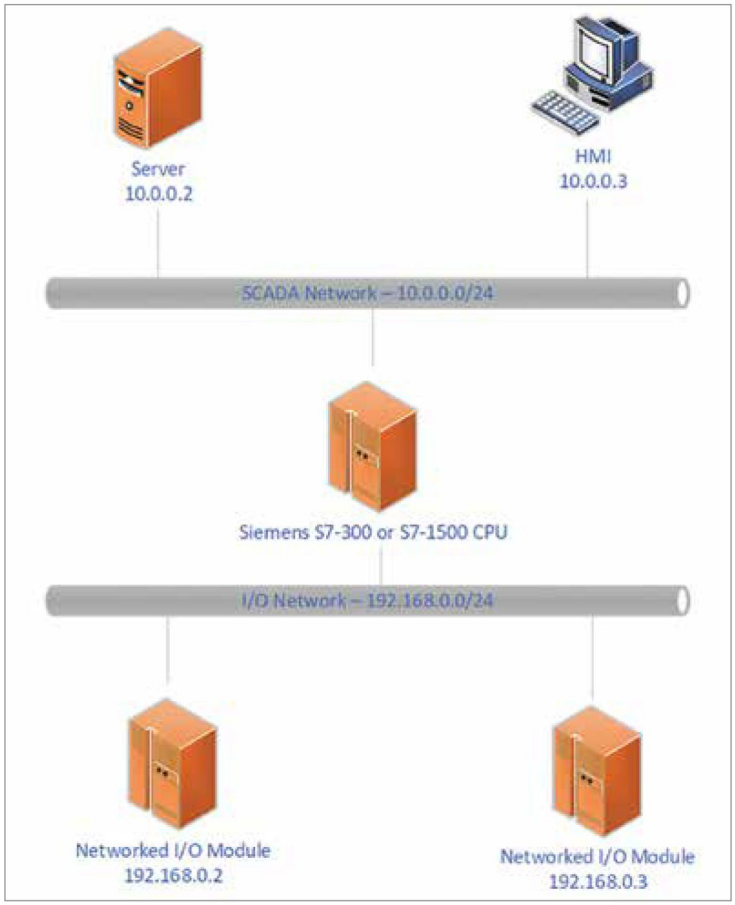
Gelin, aşağıdaki senaryoyu gözümüzde canlandıralım:
1. Diyelim ki bir saldırgan, SCADA ağı (10.0.0.x) bünyesindeki bir ana bilgisayara erişim sağladı.
2. Saldırgan, endüstriyel süreci sabote etmek amacıyla doğrudan 192.168.0.x'te bulunan I/O cihazlarına saldırmak istiyor.

SORUMUZ ŞU: I/O CİHAZLARINA ULAŞMAK İÇİN SALDIRGANIN YAPMASI GEREKENLER NELER?

Bunun üzerine biraz düşünelim ve ardından yanıtı ele alalım.

Burada da endüstriyel ağ mimarisinin şemasını görüyoruz.

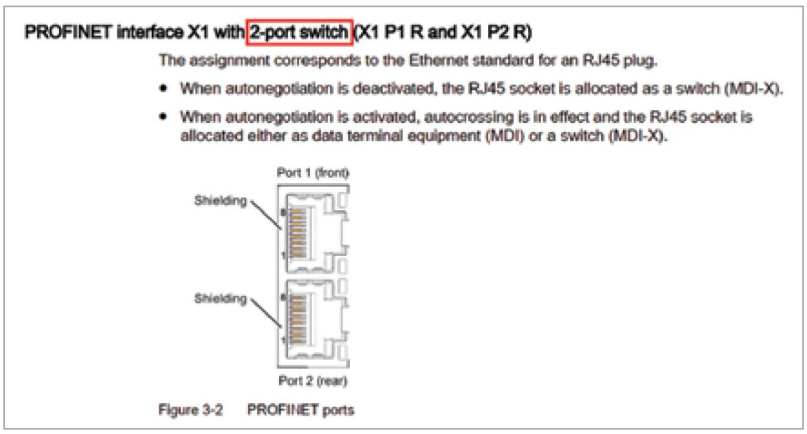
Eğer yanıtınız "Hiçbir şey" ise, doğru yanıt verdiniz.



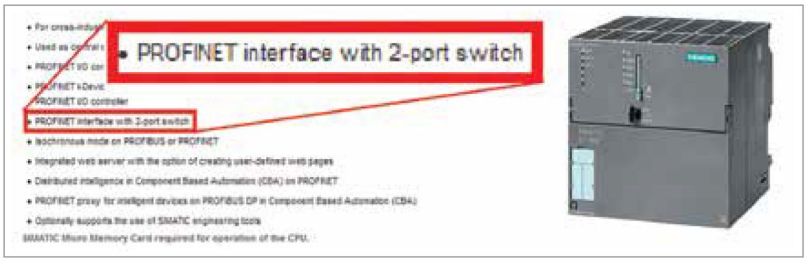
S7-300, S7-1500 ve diğer çoklu ağ arayüzüne sahip kontrolörler, zaman zaman SCADA ve I/O ağlarını "ayırmak" için kullanılır. Ancak böyle bir ayrımdan bahsetmek mümkün değil. Eğer bu özelliği kullanıyorsanız, SCADA ağ perspektifinden I / O ağına tam L2 + erişimi ya da tam tersi vardır. S7-1500 üzerindeki PROFINET arayüzü (Örn: S7-1511 PN modeli), kişinin SCADA ağından I/O ağına ya da I/O ağından SCADA ağına tam erişim sağlamasını olanaklı kılan bir ağ anahtarıdır. Saldırgan ise bu ağı tamamen düz olarak görmektedir.

S7-1500 manüel girişinde de belgelendirildiği şekilde PROFINET özellikli CPU:

S7-300 manüel girişinde de belgelendirildiği şekilde PROFINET özellikli CPU:



▲ *Kaynak: Siemens, S7-1500 CPU 1511-PN Manuel*



▲ *Kaynak: Siemens, S7-300 CPU 319-3 PN/DP Manuel*

PEKİ, SİBER SALDIRGANLAR BU KUSURU NASIL MANİPÜLE EDER?

Doğrudan I/O ağına erişim sağlamak için bir saldırganın yapması gereken tek şey SCADA ağında olan bir cihazı alıp, I/O ağında bir IP adresi eklemek ve ardından saha cihazları (I/O ağında bulunan) ile seçtiği herhangi bir protokol (Ethernet, IP, TCP, UDP, ICMP, vs) üzerinden iletişime geçmektir. Diyelim ki I/O ağında çalışan PROFINET I/O modüllerine sahipsiniz. Bu durumda hem L2 (doğrudan Ethernet) ve L3 (IP) ile SCADA ağında bulunan HER IP'ye erişim sağlanır. Eğer bu topolojiyi kullanıyor ve I/O ağının OT ağından ayrılacağını düşünüyorsanız mimarinizde çok büyük bir hata yapıyorsunuz demektir.

I/O SAHANIZIN SCADA AĞINDAN ERİŞİLEBİLİR OLUP OLMADIĞINI NASIL ANLARSINIZ?

Bakım aralıkları sırasında ya da üretim sırasında testi dikkatli bir şekilde gerçekleştirin. Yardıma ihtiyaç duymanız halinde SCADAfence destek ile iletişime geçin. I/O ağı / endüstriyel ağ sisteminiz için IP aralığının ne olduğunu öğrenin. I/O ağ aralığında, kullanımda olmayan bir IP adres seçin. Aşağıdaki komutu kullanarak SCADA ağındaki test makinasının IP'sini değiştirin: netsh int ipv4 add address "Local Area Connection" 192.168.0.253 255.255.255.0 Ardından I/O kontrolörüne, bir sensöre, bir PLC'ye veya I/O ağındaki pinglere yanıt veren başka bir IP'ye ping atın. Eğer dönüt alırsanız I/O ağınız, SCADA ağınız ile örtüşüyor demektir.

BU GÜVENLİK AÇIKLARINI OTOMATİK OLARAK NASIL SAPTARSINIZ?

Bu kusurlu tasarım SCADAfence Platformu tarafından keşfedildi: Platform, belirli bir endüstriyel tesisin hem SCADA hem de I/O ağlarını izlemek için kullanılmaktadır. Her ne kadar I/O ağının SCADA ağından segmentler halinde ayrılması gerekli olsa da SCADA ağına kurulmuş olan sensörde, SCADAfence güvenlik ekipleri, I/O ağından kaynaklı yayınlar olduğunu saptamıştır. SCADAfence güvenlik ekipleri, bu topolojiyi daha detaylı incelediklerinde sistem entegratörü ile OT ekibinin düşündüklerinin tam tersine ağların birbirleri ile bağlı ve tamamen düz olduklarını fark ettiler.

BİR AĞ ANAHTARI KULLANARAK I/O VE SCADA ARASINDA KAÇ AĞ AYRILIYOR?

Bu araştırmanın amaçları doğrultusunda bu, SCADAfence platformunun keşfedilmesine yardımcı olduğu yanlış bir ağ yapılandırmasıydı. Ancak bu soru, OT ve IoT ağ güvenliği için büyük önem arz etmektedir. Bu ağ mimarisi kusuru, ağ paketi analizinin OT ve IoT ağlarının güvenliği için son derece önemli ve temel teşkil eden bir teknoloji rolü üstlendiğinin çok açık bir örneğidir. 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. Runecast VMware Analyzer ürünlerine ilişkin daha detaylı bilgi almak ve PoC Talebiniz iletmek için https://onlineteknikdestek.com/Runecast?culture=tr web sayfamızdan iletişime geçebilirsiniz. Bu hikâye hakkında daha ayrıntılı bilgi ve ürün hakkında detaylı bilgi almak istersenız, OTD BİLİŞİM satış ekibi ile iletişime geçebilirsiniz.

SCADAfence Platformu, belirli bir endüstriyel tesisin hem SCADA hem de I/O ağlarını izlemek için kullanılmaktadır. Her ne kadar I/O ağının SCADA ağından segmentler halinde ayrılması gerekli olsa da SCADA ağına kurulmuş olan sensörde, SCADAfence güvenlik ekipleri, I/O ağından kaynaklı yayınlar olduğunu saptamıştır.