**Fortinet Operasyonel Teknoloji Altyapılarına Yönelik Saldırı Riskine Dikkat Çekiyor**

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet, genişleyen saldırı zemininde OT ortamlarının karşı karşıya kaldığı tehditlere karşı şirketleri uyarıyor.

Operasyonel Teknoloji veya OT, fiziksel süreçlere sahip olan veya üretim yapan kurumlar tarafından kullanılan kritik bir ağ bileşeni olarak tanımlanıyor. Üretim, kimyasal madde, petrol, gaz, maden, ulaşım ve lojistik sektörleri enerji şebekelerini, üretim ve montaj alanlarını çalıştırmak için özel teknolojiler kullanıyor. Bu sistemlerin kontrolü, denetimi ve yönetimi son birkaç yıl içerisinde giderek otomatik hale getiriliyor. Bu işleri yapan özel sistemler de Endüstriyel Kontrol Sistemleri (ICS), Merkezi Denetim ve Veri Toplama (SCADA) veya kısaca OT olarak adlandırılıyor.

OT sistemlerinin kullanıldığı ağlar, genellikle şirketlerdeki BT ortamlarından ve internetten yalıtık hale getiriliyor. Bu sistemler BT çalışanları yerine operasyon personelleri tarafından yönetiliyorlar. Üretim alanları şirketler için saatte milyonlarca dolarlık üretim yaparken, insanlar temiz su ve enerji gibi ihtiyaçlar için bu kritik altyapılara güveniyor. Bu sistemlerin sadece birkaç dakika durması bile yüzbinlerce liralık zarara sebep olabiliyor, aynı zamanda çalışanları ve hizmet alan insanları olumsuz etkileyebiliyor.

BT veri yönetimi ile ilgilenirken, OT ise bir şeyler üretmeye odaklanıyor. OT sistemlerinin tamamen izole edilmesi, BT dünyasının uzun süredir karşılaştığı bir güçlük olan bilgisayar korsanlığına karşı dayanıklılık algısını beraberinde getirdi.

Ancak yakın zamanda yaşanan saldırılar, aksini ispatladı.

Bu sistemleri ve OT altyapılarını hedef alan siber saldırılar giderek artıyor ve önemli zararlara neden oluyor. İlk resmi OT saldırısı olarak gösterilen on yıl önceki [Stuxnet](https://www.fortinet.com/blog/industry-trends/evolution-of-cyber-threats-in-ot-environments) saldırısında hedef alınan sistem herhangi bir dış ağ ile bağlantısı olmayan güvenli bir bağlantıydı, ama yine de dokunulmaz değildi. 2017’de [NotPetya](https://www.fortinet.com/blog/industry-trends/byline-petya-wannacry-and-mirai-is-this-the-new-normal) fidye yazılımı da üretimi aksattı ve ofislerin kapanmasına sebep oldu. Aynı yıl içerisinde [Trisis/Triton](https://www.fortinet.com/blog/industry-trends/securing-ot-networks-against-rising-attacks) kötü amaçlı yazılımı petrol ve gaz üretimi ekipmanlarının güvenlik araçlarını hedef aldı. 2020’de de ICS sistemlerini hedef alan [Ekans veya Snake](https://www.cpomagazine.com/cyber-security/new-ekans-ransomware-targets-industrial-control-systems-appears-to-originate-from-profit-motivated-cyber-criminals/) olarak bilinen fidye yazılımı ortaya çıktı.

**Fiziksel Yalıtım Yok Oluyor**

OT ortamlarını hedef alan saldırıların artmasında birkaç faktör rol oynuyor.

İzolasyon tekniği OT sistemlerine erişilmesini zorlaştırdı ancak sistemleri yalıtmak hiçbir zaman kesin güvenlik sağlamadı. Fiziksel erişim oluşturmak ise otoparkta virüslü USB belleği bırakmak veya bir personelin arkasından [binaya girmek](https://www.cmu.edu/iso/news/tailgating-dangers.html) gibi yöntemlerle her zaman mümkün.

Ayrıca endüstriyel makinelerin bakımı ve onarımı için gereken erişim, ICS araçlarının uzaktan güncellenmesi veya uzaktan yapılan aygıt yazılımı güncellemeleri, OT ortamlarının zayıf noktaları haline gelebiliyor.

Ancak BT ve OT ortamlarının birleşmeye başlamış olması ve bu yüzden OT’nin BT ortamı üzerinden gerçekleşebilecek saldırılara karşı savunmasız hale gelmesi ise en önemli faktör olarak öne çıkıyor. Veriyi ve üretim süreçlerini birleştirmek, kurumların pazarda yaşanan değişimlere daha hızlı uyum sağlayabilmesini ve sistemleri uzaktan yönetip kontrol edebilmesini sağlıyor. Ama bu avantajlar bazı riskleri beraberinde getiriyor. Özellikle OT ekipmanlarını hedef alan yeni kötü amaçlı yazılımlar, sistemlerin zayıf noktalarını bulan arama ve taşıma bileşenlerini kullanarak BT ortamını ve ağ bağlantılarını istismar edebiliyor ve endüstriyel kontrol sistemlerine erişim sağlayabiliyor.

Trisis/Triton adlı kötü amaçlı yazılım, petrokimya tesisleri tarafından kullanılan güvenlik ve denetim sistemlerini hedef alıyor. OT’ye özel olan bu siber saldırının güvenlik sistemine sızabilmek için kullandığı işlemler, prosedürler ve teknikler tamamen BT’ye ait siber saldırı, arama ve ulaşım metotlarından oluşuyor.

**BT ve OT Ortamları Birleşiyor**

BT ve OT ortamlarının birleşimi, finansal ve operasyonel anlamda faydalar sunduğu için OT ağlarına yönelik artan risklere rağmen gerçekleşmeye devam ediyor. Operasyon ekibi, BT sistemlerinde çalışan yazılım ve veri tabanlarını kullanan gelişmiş kontrol sistemlerini çalıştırıyor. Wi-Fi özelliğine sahip termostatlar ve vanalar, BT altyapısı üzerinden uzaktan gözlenebiliyor ve kontrol edilebiliyor. Ancak maliyetlerden sorumlu yöneticiler (CFO), birbirinden ayrı ağların ve ağları çalıştıran farklı ekiplerin oluşturduğu maliyetleri azaltmaya çalışıyor.

BT ve OT ortamları bir araya getirildiğinde daha gelişmiş bir süreç ve iş verimliliği oluşuyor. Dolayısıyla bu birleşim gerçekleştiği için şirketlerin siber risklerin arttığını kabul etmesi gerekiyor.

Siber saldırganların hedefleyebileceği cihaz sayısı arttığı için dijital saldırı zemini genişletiyor. Sayıları artan ağ sunucuları, şubeler, uzaktan veya evden çalışanlar ve Nesnelerin İnterneti cihazları, BT ağına bağlanan ve oradan da OT ortamına geçiş yapabilen potansiyel bir geçit görevi görebiliyor. Aynı şekilde BT sistemlerine bağlı birçok OT sistemi de güncel tehditler karşısında eskimiş olabileceği için daha savunmasız hale geliyor.

Tehlikelerin sadece sayısı değil, gelişmişlik düzeyleri de artıyor. Şirketler dijital dönüşüm yolculuklarında çeşitli yazılımlar geliştirirken, siber saldırganlar da aynı teknikleri kullanarak son derece karmaşık ve çeşitli kötü amaçlı yazılımlar üretiyor. Yaptıkları saldırılar, BT ve OT ortamlarına sızarken güvenlik aşamalarını geçmek için birçok farklı mekanizma kullanıyor.

Günümüzde güvenlik araç sayısının çok yüksek olması, tehlikelerin üstesinden gelmeyi daha da zorlaştırıyor. Anketler belli büyüklükteki birçok şirketin neredeyse her biri farklı tedarikçilerden olmak üzere 30-90 arası güvenlik aracı kullandığını gösteriyor. Birbirinden farklı yönetim konsollarına sahip güvenlik araçlarını kullanabilmek için şirketlerin eğitimli elemanlara sahip gerekiyor. Ancak çoğu zaman güvenlik elemanlarının her bir araçla ilgilenecek zamanı ve kaynağı olmuyor. Bu yüzden siber saldırılar bu karmaşa içinde tespit edilmeden sisteme sızabiliyor.

Siber saldırıları ve kişisel bilgilerin korunmasını ele alan regülasyonlar, BT ve OT yöneticileri için güvenliği daha da sıkılaştırıyor. Kurumların anlaması ve takip etmesi gereken PCI-DSS (Ödeme Kartları Sektörü Veri Güvenliği Standartları), GDPR (Genel Veri Koruma Tüzüğü), ve NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) gibi bazı genel standartlar bulunuyor. Bunlara ek olarak çeşitli kuruluşların oluşturduğu ISO (Uluslararası Standartlar Teşkilatı) ve ANSI (Amerikan Ulusal Standartlar Enstitüsü) gibi güvenliğin nerede ve nasıl uygulanması gerektiğini belirleyen sektörlere özel standartlar ve regülasyonlar da var.

**Hedef Alınan Şirketlerin Mağdur Olmamak için Yapması Gerekenler**

OT ortamları siber saldırganların ilgisini çekiyor ve bu yüzden her an bir saldırı gerçekleşebilir.

ICS veya SCADA sistemlerinin yer aldığı örneklerde yatırımların önemli derecede eksik olduğu gözlemleniyor. Bunun birçok nedeni var ama önce bu durumun düzeltilmesi gerekiyor. Kurumların BT ve OT ortamlarını birleştirmese bile aşağıdaki bazı yüksek seviyeli güvenlik önlemiyle Operasyonel Teknolojilerini koruması gerekiyor.

1. **Giderek artan riskleri tanımlamak ve buna karşı önlem almak için harekete geçmek.**
2. **OT ve BT ağlarına kapsamlı görünürlük sağlayacak güvenlik araçlarını yerleştirmek.** Bu araçların cihazları tanıyabilmesi ve envantere dahil edebilmesi gerekiyor. Aynı zamanda erişim izni olan çalışanlara kontrol erişimi sağlaması ve uygulamalar ve trafik üzerinde görünürlük sağlaması da önemli.
3. **Bir bölümleme stratejisi geliştirmek.** BT ve OT alanları arasına sıkı ilkelere sahip geçitler entegre ederek bu tekniğin OT ağının farklı seviyeleri arasında uygulanması sağlanabilir. Bu işlemle her sistemin ve altsistemin sadece yapmaları gereken işleri yapması hedeflenmeli. Çünkü bölümleme işlemi, bir noktadan başlayıp her yere yayılan saldırıların önüne geçebiliyor.
4. **Açık ve güven temelli erişim sistemi yerine sıfır güven stratejisini kullanmak.** Kullanıcıyı doğrulayacak erişim kontrolleri sayesinde çalışanların sadece işlerini yapmaları için gereken sistemlere bağlanması sağlanabilir ve bağlıyken de denetlenebilir. Bu yöntemin herkese uygulanması gerekiyor ama özellikle tedarikçiler gibi üçüncü taraf şirketlerin buna dahil edilmesi hayati öneme sahip.
5. **Olayların analizinde destek ve reaksiyon hızınızı arttırmak için otomasyondan faydalanmak.** Aktiviteleri kaydeden araçlar, bu kayıtlarda anormal davranışlar arayan analitik sistemler ve bu tespit edilen tehditlere karşılık verebilen güvenlik sistemleri kurulmalı. Otomasyon ve orkestrasyon, günümüzdeki saldırıların hızı göz önünde bulundurulduğunda birkaç saniye içerisinde tehditleri saptayabilmek ve harekete geçebilmek için çok önemli.
6. **Bir sızıntı durumunda denetleme için bir işlem sürecine ek olarak yedekleme, kurtarma ve onarım için kural ve strateji dokümanı oluşturmak.**

Hiç kimse ve hiçbir şey sizi saldırılardan korumayı tamamen garantileyemez. Ama ektili bir savunma stratejisi olmadan saldırıya uğrayacağınız ve zarar göreceğiniz kesindir.

BT ve OT’leri farklı tip saldırılardan ve bir istilanın farklı aşamalarından korumak için tasarlanmış birçok güvenlik aracı bulunuyor. Şirketlerin birbiriyle entegre edilmiş birçok yazılım veya donanım gibi alet bulması mümkün. Hatta seçenekler arasından özellikle OT ortamına özel güçlüklerle baş etmek için tasarlanmış aletler de tercih edilebilir. Bu yaklaşım, şirketlere en iyi güvenliği sunuyor.

Kendi içinde tehdit ile ilgili bilgi paylaşabilen, verilecek karşılığı belirleyebilen ve birbiriyle uyumlu bir şekilde durumu idare edilen güvenlik araçları, güvenlik yapısını herhangi bir ödün vermeden basitleştiriyor. Bütüncül bir güvenliğin faydalarını sunacak şekilde tasarlanmış açık ve birçok sağlayıcının yer aldığı bir ekosistem olan [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-security), bunun en iyi örneklerinden birisi.

**Fortinet Hakkında**

Fortinet dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün büyüyen saldırı zemininde müşterilerine eksiksiz görünürlük ve kontrol sağlar, günümüzde artan ve gelecekte de artacak olan performans ihtiyaçlarını karşılamak için onları güçlendirir. Ağlardaki uygulamaların, çoklu bulut sistemlerinin ve sınır ortamlarının karşılaştığı en kritik güvenlik sorunlarına karşı tek çözüm olan Fortinet'in Security Fabric platformu, tüm dijital altyapıda veriyi korur. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 465 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Hem bir teknoloji şirketi hem de öğrenen bir şirket olan [Fortinet Network Security Expert (NSE)](https://training.fortinet.com/?utm_source=blog&utm_campaign=2019-q3-nse-institute) Eğitim Enstitüsü, sektördeki en büyük ve kapsamlı siber güvenlik eğitim programlarından birini sunmaktadır. Daha fazla bilgi için: <http://www.fortinet.com>, [Fortinet Blog](https://blog.fortinet.com/) sayfası veya [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=FortiGuardLabs).