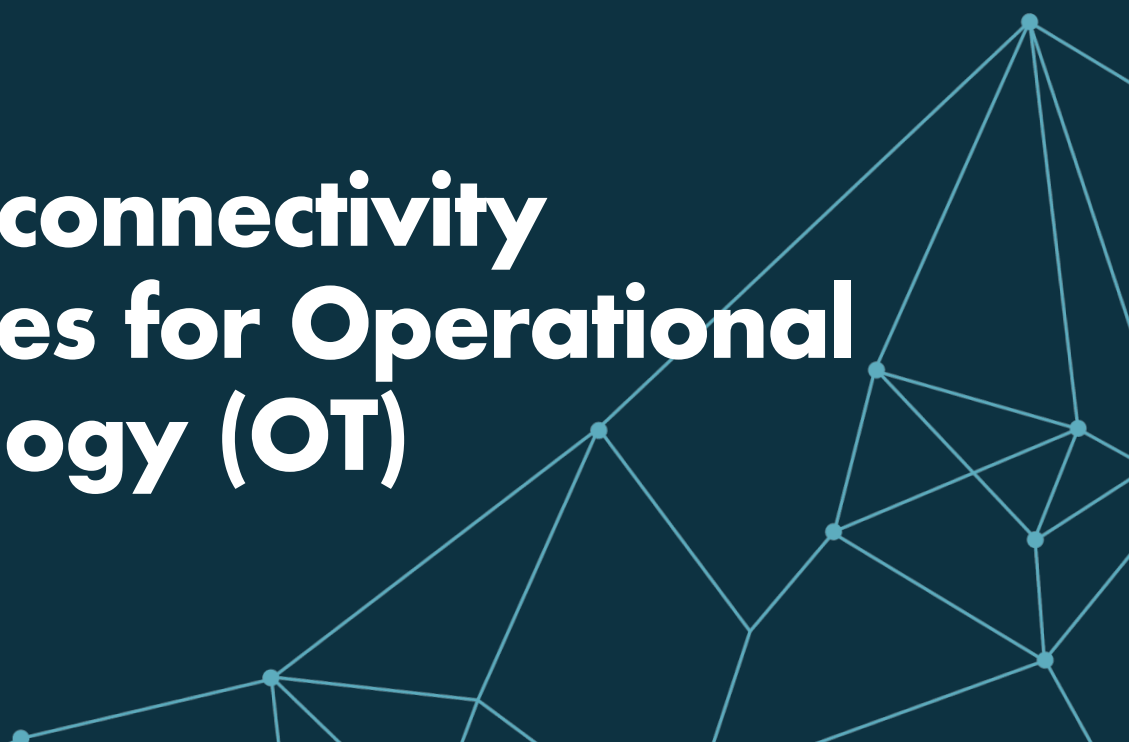


Secure connectivity principles for Operational Technology (OT)



Birleşik Krallık Ulusal Siber Güvenlik Merkezi (NCSC-UK), uluslararası iş ortaklarıyla birlikte Operasyonel Teknoloji (OT) için Sekiz Güvenli Bağlantı Prensibini yayımlamıştır. Advenica, onlarca yıldır güvenilir bir siber güvenlik sağlayıcısı olarak bu prensipleri çözümlerine uygulamaktadır. Bu prensipleri nasıl hayata geçirdiğimizi ve kurumların OT ortamlarındaki bağlantıları güvenli bir şekilde tasarlamasına, korumasına ve yönetmesine nasıl destek olduğumuzu keşfedin.

Bu Makalede Ele Alınan Prensipler

- Riskler ve Fırsatlar Arasında Denge Kurun
- Bağlantılarınızın Maruziyetini Sınırlandırın
- Ağ Bağlantılarını Merkezileştirin ve Standartlaştırın
- Standart ve Güvenli Protokoller Kullanın
- OT Ağ Sınırlarını Güçlendirin
- Güvenlik İhlallerinin Etkisini Sınırlandırın
- Tüm Bağlantıları Kaydedin ve Sürekli İzleyin
- İzolasyon Planı Oluşturun



Riskler ve Fırsatlar Arasında Denge Kurun

- Uygulamaya başlamadan önce, denetlenebilir bir iş planı oluşturmanız ve ISO/IEC 27001, IEC 62443 veya benzeri bir risk yönetimi çerçevesini uygulamanız önerilir.
- Goal Structuring Notation (GSN), Advenica'nın karmaşık sistemler için güvenlik gereksinimleri oluştururken sıklıkla kullandığı bir yaklaşımdır. Güvenlik hedeflerinizi bir GSN ağacı üzerinde tanımlayarak genel bir görünürlük elde edebilir ve hem teknik hem de teknik olmayan güvenlik önlemlerini açık ve gerekçeli şekilde belirleyebilirsiniz.
- Tedarik zincirinizi güvenli yönetmek için kullandığınız cihazların güvenli tasarım (Secure by Design) prensibine uygun olduğundan ve iş sürekliliğinizi kesintiye uğratmadan kolayca güncellenebildiğinden emin olun.

Bağlantılarınızın Maruziyetini Sınırlandırın

Maruziyet Süresini Azaltın

Ekipmanlarınız uzak bir lokasyonda bulunabilir ve otomatikleştirilemeyen bakım işlemleri gerçekleştirmeniz gerekebilir. Advenica Remote Access Device, iki faktörlü kimlik doğrulama ile geçici bağlantı imkânı sunar. Cihaz; uzaktan KVM, terminal veya IP tabanlı erişim sağlayabilir ve tüm iletişim şifrelenmiş bir uzaktan erişim tüneli üzerinden gerçekleştirilir.

Gelen Bağlantı Portlarını Ortadan Kaldırın

OT ağına yapılan tüm harici bağlantılar içeriden başlatılmalıdır. Gelen bağlantılar Data Diode ile korunduğunda, Data Diode Engine harici sistemlerle iletişimi içeriden başlatacak şekilde yapılandırılır.

Eski Sistemlerden Kaynaklanan Riskleri Yönetin

Kullanım ömrünü tamamlamış cihazlar giderek artan güvenlik riski oluşturur; ancak operasyonel nedenlerle bunların hemen değiştirilmesi her zaman mümkün olmayabilir. Advenica DD500E Data Diode, bu tür cihazları ağdan izole ederken bağlantının devam etmesini sağlayan maliyet etkin bir çözümdür.

Özel Bağlantılardan Kaynaklanan Riskleri Yönetin

Farklı üretim sahaları arasında uzaktan bağlantılar gerekli olabilir; ancak bu durum ek güvenlik riskleri de oluşturur. Genel internet bağlantıları, özel fiber hatlara kıyasla daha yüksek saldırı yüzeyi sunar. Advenica, taktik ve stratejik savunma operasyonları için tasarlanmış donanım tabanlı IP şifreleme sistemleri sağlar. Bu cihazlar, varsayılan olarak dış saldırı vektörlerini en aza indirecek şekilde tasarlanmıştır ve doğrudan internete bağlanabilir. Aynı zamanda sahalar arasında, ulusal düzeyde kritik altyapıları koruyabilecek güvenlik seviyesinde şifrelenmiş bir iç ağ oluşturur.

Ağ Bağlantılarını Merkezileştirin ve Standartlaştırın

- OT ortamına yönelik uzaktan bağlantılarınız esnek, tekrarlanabilir ve standartlaştırılmış bir yapıda sınıflandırılmalıdır. File Security Screener, tek yönlü Data Diode teknolojisini zararlı yazılım taramasıyla birleştiren, yüksek güvenli bir dosya aktarım çözümüdür.
- ZoneGuard, veri aktarımlarında kullanılan her türlü protokolü doğrulamak ve filtrelemek üzere uyarlanabilir. Çift yönlü iletişimi destekler; tek yönlü kullanım senaryolarında ise DD1000i Data Diode ile birlikte kullanılabilir.
- Bu çözümler, OT ağınıza yönelik tüm erişimler için merkezi ve güvenli tek giriş noktası olarak yapılandırılabilir.



Standart ve Güvenli Protokoller Kullanın

- Güvenlik, Gizlilik (Confidentiality), Bütünlük (Integrity) ve Erişilebilirlik (Availability) arasında bir denge kurulmasını gerektirebilir.
- ZoneGuard, TLS tabanlı iletişimi destekler. Protokol sonlandırma (protocol break) özelliği sayesinde, verilerin önceden tanımlanmış şemalara göre doğrulanmasını sağlayan esnek güvenlik servisleri sunar.
- Advenica Customised Solutions ekibi, ihtiyaç duyduğunuz iletişim protokollerini desteklemek üzere ZoneGuard veya Data Diode servislerini geliştirme ve özelleştirme konusunda destek sağlar.

Kuruluşunuz için doğru çözümü bulmak konusunda rehberliğe veya desteğe mi ihtiyacınız var? Size yardımcı olmak için buradayız.



OT Ağ Sınırlarınızı Güçlendirin

- OT ortamındaki eski sistemler ve zayıf güvenlik kontrolleri, ağ sınırlarının güçlendirilmesini kritik hale getirir.
- Donanım tabanlı Data Diode ve Cross Domain Solution (CDS) çözümleriyle ağ segmentasyonu uygulamak, bu riskleri önemli ölçüde azaltır.

Güvenlik İhlalinin Etkisini Sınırlandırın

Operasyonel hijyen, ofis ağında kullanılan dizüstü bilgisayarları OT ağına bağlamamanız gerektiği anlamına gelir. SecuriRAM, zararlı yazılımları yanlışlıkla beraberinde getirmeden dosyaları OT iş istasyonunuza ve OT iş istasyonunuzdan taşımanıza olanak tanır.

Ağ Segmentasyonu

OT ağının ayrı güvenlik bölgelerine ayrılması, saldırganların ağ içinde yatay hareket (lateral movement) kabiliyetini sınırlandırır. OT ağının dış sınırlarının korunması için DDSFX-10G gibi yüksek performanslı Data Diode çözümleri gerekebilirken, DD500E gibi maliyet etkin modeller tek bir makineyi veya bir makine grubunu korumak için kullanılabilir.

Görevlerin Ayırıştırılması

OT ağına dosya veya veri aktarmak hassas bir işlemdir; buna karşılık, verilerin iş sistemlerinize aktarılması çoğu zaman tek bir Data Diode ile gerçekleştirilebilir. Data Diode Engine proxy yazılımı, çift yönlü protokolünüzü tek yönlü bir UDP veri akışına dönüştürmenizi sağlar. UDP veri akışı Data Diode üzerinden iletildikten sonra yeniden orijinal protokole dönüştürülür. Bu işlemi gerçekleştiren Data Diode Services, ihtiyaçlarınıza göre özelleştirilebilir.

Aşağı Kaydır

ZoneGuard ve Data Diode Engine yönetim arayüzleri sertifikalarla korunmaktadır. Bu arayüzlere yalnızca PAW (Privileged Access Workstation) politikanıza uygun ayrıcalıklı erişim iş istasyonları üzerinden erişilmelidir.

Sınır Kontrolleri

Data Diode Engine'in dış uç noktası, ilave güvenlik katmanları sağlamak amacıyla güvenlik duvarı ile korunan bir DMZ içerisinde konumlandırılabilir.

Tüm bağlantıların kaydedildiğinden ve izlendiğinden emin olun

- İzleme, güvenli bağlantının sağlanmasındaki son savunma hattınızdır.
- Advenica Data Diode çözümleri, logların harici bir SOC'a güvenli şekilde aktarılmasını sağlarken, SOC üzerinden gelebilecek saldırıların izlenen OT ağına geri yayılmasını fiziksel olarak engeller.

İzolasyon Planı Oluşturun

- GSN ağacı yardımıyla, ağ segmentlerinizden birinin ihlal edilmesi durumunda sistemlerinizi çalışır durumda tutmak için nelerin gerekli olduğunu analiz edebilirsiniz. Bu süreç, dayanıklılığı artırmak amacıyla fiziksel üretim süreçlerinizde iyileştirmeler yapılmasını da gerektirebilir.
- Remote Access Device, stratejik noktalara konumlandırılarak bir ağ kill switch çözümü olarak hazır bulundurulabilir.
- Yerleşik LTE bağlantısından yedek iletişim amacıyla yararlanarak, altyapınıza yönelik ciddi bir saldırı sırasında dahi sistemleriniz üzerindeki kontrolü sürdürebilirsiniz.

Kuruluşunuzun Operasyonel Teknolojiler (OT) için Güvenli Bağlantı Prensiplerine uyum sağlamasına Advenica'nın nasıl yardımcı olabileceği hakkında daha fazla bilgi almak için bizimle iletişime geçin.

Advenica provides cybersecurity solutions within encryption and network segmentation with the highest level of EU-and national approvals. We were founded in 1993 and are based in Malmö, Sweden, where most of our products are designed, developed, and manufactured. Advenica specialises in the sectors of defence, authorities, infrastructure, and industry. With decades of experience working with Sweden's national security, Advenica is known for delivering cybersecurity with exceptional service.

Read more at advenica.com

 **advenica**
Swedish cybersecurity
at your service

OTD BİLİŞİM
GLOBAL VAD