Kaspersky® Industrial CyberSecurity

Kaspersky ICS Güvenlik Değerlendirmesi

Endüstriyel kontrol sistemlerinin (ICS) güvenliğini sağlamak, uzun zaman boyunca üretim kazalarını, insan kayıplarını ve çevre kirliliğini önlemek için emniyeti ve işlevsel güvenliği sağlamak anlamına gelmekteydi. Satıcılar, entegratörler ve işletme sahipleri, endüstriyel kontrol sistemlerinin tasarımı ve bakımı sırasında BT güvenliği açısından genellikle fiziksel güvenliğe ve fiziksel ağ izolasyonuna odaklanırlardı. Endüstriyel Kontrol Sistemlerini (ICS) hedef alan kötü amaçlı yazılımlarda ve saldırılarda görülen artış, ICS ekipmanlarındaki güvenlik açıklarının sayıca artması ve bu sistemlerin diğer ortamlarla (örneğin ERP) entegre edilmesine duyulan ihtiyaç, ICS güvenliğine yönelik daha titiz bir yaklaşımı gerekli kılmaktadır. Buna ek olarak ICS güvenliği, işlevsel güvenliğe sıkı sıkıya bağlıdır; başarılı bir hacker saldırısı, üretim kazalarına yol açabilir.

ICS Güvenliği Değerlendirme Sonuçları

ICS güvenliği değerlendirme hizmetinin sonucunda, kritik önem taşıyan ağ bileşenlerine yetkisiz erişim elde etmeye yol açabilecek çok çeşitli güvenli açıkları tespit edilebilir. Bu güvenlik açıklarından bazıları şunlardır:

- ICS ekipmanının fiziksel olarak yeterince korunmaması
- Tehlikeye açık ağ mimarisi, yetersiz ağ koruması (ICS ağının diğer ağlardan ayrılmasındaki kusurlar dahildir)
- Ağ trafiğinin engellenmesine ve yeniden yönlendirilmesine yol açabilecek güvenlik açıkları (endüstriyel iletişim protokollerindeki açıklar dahildir)
- SCADA, PLC'ler, akıllı sayaçlar gibi ICS bileşenlerindeki güvenlik açıkları
- Çeşitli hizmetlerde yetersiz kimlik doğrulama ve yetkilendirme
- Zayıf kullanıcı kimlik bilgileri
- Gereğinden fazla kullanıcı ayrıcalığının yanı sıra güvenlik standartlarına ve satıcı önerilerine uymama dahil yapılandırma hataları
- Analiz edilen ICS ve diğer sistemler arasında (örneğin MES aracılığıyla) yürütülen iletişimdeki güvenlik açıkları
- Uygulama kodundaki hatalardan kaynaklanan güvenlik açıkları (kod enjeksiyonu, dizin gezinimi, müşteri tarafı güvenlik açıkları vb.)
- Son güvenlik güncellemelerine sahip olmayan eski donanımların ve yazılım sürümlerinin kullanılmasından kaynaklanan güvenlik açıkları
- Bilgilerin ifşa edilmesi

ICS Güvenlik Değerlendirmesi; fiziksel güvenlik ve ağ güvenliğinden başlayıp denetimsel kontrol ve veri edinme (SCADA) sistemleri, programlanabilen mantık kontrolörleri (PLCler) ve diğer bileşenler gibi çeşitli ICS bileşenlerinde bulunan satıcıya özgü güvenlik açıklarına kadar uzanan, ICS'nizin tüm katmanlarındaki çeşitli güvenlik kusurlarını tespit etmeyi amaçlayan bir hizmettir. Bu hizmet, size ICS'nizdeki güvenlik açıkları ve bu güvenlik açıklarından yararlanılmasının sonuçları hakkında bilgi sunar; uygulanan güvenlik önlemlerinin etkililiğini değerlendirir ve tespit edilen kusurları düzeltip güvenliği geliştirmeniz için gerekli eylemleri planlamanızı sağlar.

Bunu neden yapmalısınız?

Kaspersky Lab'in ICS Güvenlik Değerlendirmesi, kuruluşların şunları yapmasına yardımcı olur:

- ICS'nin en zayıf noktalarını anlayıp bunlara karşılık gelen güvenlik süreçlerini geliştirmeye odaklanabilirsiniz
- Saldırılar için kullanılabilecek güvenlik açıklarını proaktif biçimde tespit edip onararak, kötü amaçlı kişilerin sebep olabileceği çevresel, finansal, işlemsel kayıpları, insan kayıplarını ve itibar kaybını önleyebilirsiniz
- Sistemlerinizin, örneğin NERC CIP standartları gibi bölgenize ve sektörünüze özel ICS güvenlik standartlarına uyumluluğunu analiz edebilirsiniz
- Güvenlik değerlendirmesi uygulanmasını gerektiren resmi, sektörel veya kurumsal standartlara uyum sağlayabilirsiniz

Neyi test ediyoruz?

Kaspersky Lab uzmanları, tüm satıcıların ve sektörlerin endüstriyel kontrol sistemlerini analiz edebilir: **enerji üretimi ve aktarımı, ulaşım sistemleri, petrol ve doğal gaz üretimi, madencilik faaliyetleri ve çok daha fazlası.**

Altyapınıza ve gereksinimlerinize bağlı olarak farklı güvenlik değerlendirmesi yaklaşımları ve kombinasyonları kullanılabilir:

- **Sızma Testi**: Seçiminize bağlı olarak, amaçları mevcut ayrıcalıklarını yükselterek ICS ortamınıza erişmek olan çeşitli davetsiz misafirleri taklit eden bir güvenlik değerlendirmesi.
- **ICS Altyapı Güvenliği Değerlendirmesi**: Uzmanlarımızın teknik ICS belgelerini analiz edeceği, ICS personeliyle görüşmeler yapacağı, kullanılan endüstriyel sistemleri ve protokolleri analiz edeceği ve üretim ortamındaki ICS bileşenlerinin kapsamlı teknolojik denetimlerini yapacağı yapısal güvenlik değerlendirmesi.
- **ICS Çözümleri Güvenlik Değerlendirmesi**: Yeni güvenlik açıkları bulmak üzere test ortamında yürütülecek ICS çözümü yazılım ve donanımlarına yönelik güvenlik araştırması ve ardından gerçek sistemde tatbik edilecek olan önceden onaylanmış testler.

Proje ekibi üyeleri, güvenlik uygulamaları alanında derin bilgi sahibi, becerilerini sürekli geliştiren ve ICS güvenliği araştırmalarıyla tanınan deneyimli uzmanlardır.

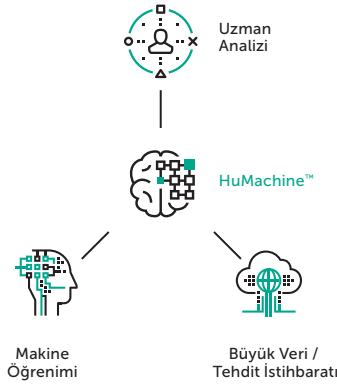
Hizmet tamamlandıktan sonra müşterilerimize, test süreçleri, güvenlik kusurları ve öneriler hakkında detaylı teknik bilgiler ile test sonuçlarından elde edilen kanıları açıklayan ve sektöre özgü saldırı senaryolarını anlatan kapsamlı yönetici özetini içeren bir rapor sunulur. Gerektiği takdirde teknik ekibiniz veya üst düzey yöneticileriniz için saldırı tatbikatlarıyla ilgili videolar ve sunumlar da hazırlanabilir.

Bunu nasıl yapıyoruz?

Bu hizmet, uluslararası kanunlara ve örnek uygulamalara bağlı, sistemlerinizin gizliliğine, bütünlüğüne ve kullanılabilirliğine saygılı, deneyimli Kaspersky Lab güvenlik uzmanları tarafından gerçekleştirilir.

Kaspersky Lab, ICS güvenlik değerlendirmesi hizmetlerini aşağıdaki uluslararası standartlara ve örnek uygulamalara uygun biçimde gerçekleştirir:

- Sızma Testi Uygulama Standardı (PTES)
- NIST Özel Yayınları 800-115 Bilgi Güvenliği Testi ve Değerlendirmesi İçin Teknik Kılavuz
- Açık Kaynak Güvenlik Testi Metodolojisi El Kitabı (OSSTMM)
- Bilgi Sistemleri Güvenlik Değerlendirmesi Çerçevesi (ISSAF)
- North American Electric Reliability Corporation Kritik Altyapı Koruma (NERC CIP) standartları
- Web Uygulama Güvenliği Konsorsiyumu (WASC) Tehdit Sınıflandırması
- Açık Web Uygulamaları Güvenlik Projesi (OWASP) Test Kılavuzu
- İnternet Güvenliği Merkezi (CIS) standartları
- Genel Güvenlik Açığı Puanlama Sistemi (CVSS) ve diğer standartlar (kuruluşunuzun yaptığı işe ve konumuna bağlı olarak).



Kaspersky Lab
Kurumsal Siber Güvenlik: **www.kaspersky.com.tr/fraudprevention**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliği Haberleri: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr

© 2019 AO Kaspersky Lab. Tüm hakları saklıdır. Tescilli ticari markalar ve hizmet markaları, ilgili sahiplerinin mülkiyetindedir.