7 Gründe für Kaspersky Industrial CyberSecurity Assessment

„Primum Non Nocere“ – Zuerst einmal nicht schaden!

Das ist unsere Leitlinie. Als erfahrene Anbieter von industrieller Cybersicherheit und Automatisierungstechniker verstehen wir nur zu gut die Risiken im Zusammenhang mit der Durchführung von Sicherheitstests in einer Betriebsumgebung. Wir arbeiten in jeder Stufe des CSA (Cybersecurity Assessment) eng mit Ihren Technikern zusammen und halten negative Auswirkungen von Ihnen fern.

Wir setzen uns mit Ihrem System auseinander

Wir führen eine umfangreiche technische Prüfung und Auswertung Ihrer ICS-Betriebsarchitektur und -komponenten durch. Das umfasst eine detaillierte Analyse betrieblicher Prozesse, einschließlich der zugrunde liegenden Netzwerkarchitektur, der IT- und OT-Teamintegration, der Unterstützung durch den Hersteller, der Kontrolle der Cybersicherheit, der Überwachung und aller Ihrer internen und externen Verbindungen.

Unser Ansatz für die Bewertung von Risikofaktoren ist ganzheitlich

Unser Hauptziel ist es, für Ihre industriellen Systeme, Netzwerke und industriellen Prozesse spezifische Angriffsvektoren zu erkennen. Diese Vektoren (von menschlichen Faktoren bis zur erweiterten Ausbeutung von Zero-Day-Schwachstellen) können ihren Ursprung an jedem beliebigen Punkt in Ihren IT/OT-Domänen und sogar auf mobilen Geräten haben. Wir analysieren also Ihre industrielle Organisation ganzheitlich als ein komplexes cyberphysisches System.

Wir machen unsere Hausaufgaben

Wir bei Kaspersky Lab demonstrieren unsere Expertise im Bereich industrielle Cybersicherheit nicht nur während des Bewertungsprojekts selbst, sondern auch durch die Sorgfältigkeit unserer Vorbereitung. Dies umfasst die Durchführung vorbereitender Schwachstellenanalysen der eingesetzten industriellen Ausstattung, sowohl Software als auch Hardware. Allein im Jahr 2016 entdeckten Forscher von Kaspersky Lab offiziell 14 ICS-Schwachstellen und 50 weitere, die noch von den betroffenen IAVs (Industrial Automation Vendors, Anbieter industrieller Automatisierung) berücksichtigt werden.

Wir definieren die Normalität, damit wir Anomalien erkennen können

Wir können eine nicht intrusive Analyse der Netzwerkdaten aus dem in Ihrem ICS-Netzwerk auftretenden Verkehr durchführen und eine visuelle Karte der Kommunikation von Gerät zu Gerät erstellen. Wenn eine Benchmark für „normale“ Kommunikationsmuster erstellt ist, werden Anomalien nach und nach deutlich.

Wir bleiben am Ball

Support in der Nachprojektphase ist uns wichtig. Wir lassen unsere Kunden nicht mit nicht gepatchten Schwachstellen und vagen Empfehlungen wie „Implementieren Sie Netzwerksegmentierung" zurück. Wir tun alles, um Ihnen eine möglichst umfassende Cybersicherheit zu bieten, auch ohne zusätzliche Lösungen zu nutzen - wir finden beispielsweise Problemumgehungen zur Vermeidung von Schwachstellen oder setzen IAVs unter Druck, zeitnah Updates anzubieten.

Jeder Kunde ist einzigartig

Bei all unseren CSA-Projekten wird auf die spezifischen Belange unserer Kunden eingegangen - es werden nicht einfach nur Schwachstellen-Scans durchgeführt. Jeder kundenspezifische und technische Prozess ist einmalig, daher haben wir Forscher mit spezifischem Fachwissen in verschiedenen Branchen – Öl und Gas, Energieversorgungsnetze, Fertigung usw. Unsere Experten suchen manuell nach Schwachstellen, unser ICS Cyber Emergency Response Team bereitet eine Analyse Ihrer spezifischen regionalen/industriellen Bedrohungslandschaft vor, und wir bleiben mit Ihren IAVs bezüglich des Status Ihrer Geräte in Kontakt.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity ist ein Portfolio bestehend aus Technologien und Services, das umfassenden Schutz für jede einzelne Ebene von Betriebstechnologie und sämtliche Elemente Ihres Unternehmens bietet, darunter auch für SCADA-Server, HMIs, Engineering-Workstations, SPS, Netzwerkverbindungen und Mitarbeiter, ohne dabei die Geschäftskontinuität und Konsistenz der technologischen Prozesse zu beeinträchtigen.

Weitere Informationen zu Kaspersky Lab finden Sie unter
https://www.kaspersky.de/enterprise-security/industrial

Informationen über ICS-Cybersicherheit:
https://ics-cert.kaspersky.com
Neues über Cyberbedrohungen: **de.securelist.com**

#truecybersecurity

www.kaspersky.de

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* Auszeichnung für weltweit führende Leistungen in den Bereichen Internetwissenschaft und Internettechnologie auf der 3. Weltinternetkonferenz (Wuzhen-Gipfel)

** Sonderpreis der Industriemesse China International Industry Fair (CIIF) 2016