Kaspersky Industrial CyberSecurity Expert Services: Cybersecurity Assessment

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

Unternehmen, die sich um die potentiellen betrieblichen Auswirkungen der IT-/OT-Sicherheit sorgen, bietet Industrial CyberSecurity Assessment von Kaspersky Lab vor der Installation ein minimal invasives Cybersecurity Assessment an. Dies ist ein maßgeblicher erster Schritt bei der Bestimmung der Sicherheitsanforderungen im Rahmen der betrieblichen Anforderungen und bietet darüber hinaus wichtige Erkenntnisse zur derzeitigen Cybersicherheit, ohne dass weitere Schutztechnologien bereitgestellt werden müssen.

Warum industrielle Systeme besonders anfällig sind

Neuartige industrielle Steuerungssysteme Industrial Control Systems, ICS sind aus bestimmten Gründen anfällig für Cyberangriffe. Diese Systeme kombinieren häufig Netzwerktechnologien mit älteren Systemen, und es ist nicht ungewöhnlich, dass Unternehmen, anstatt einen Prozess zu unterbrechen, kritische Schwachstellen ungepatcht lassen – das ist Cyberkriminellen durchaus bewusst.

Schwache Zugriffskontrollen, Standardeinstellungen, Nutzungsregeln und Richtlinien – wenn auch zugunsten der Betriebskontinuität – können schwerwiegende Folgen haben. Sicherheitslücken, die speziell bei branchenspezifischer Software auftreten, wie z. B. durch hartcodierte Passwörter und unsichere Protokolle, sind ein Relikt der Vergangenheit, in der ICS nicht mit dem Netzwerk verbunden und „Software-Schwachstellen" als solche kaum vorhanden waren.

Kaspersky Lab nutzt einen konsistenten und strukturierten Ansatz, um relevante Schwachstellen und Bedrohungen zu identifizieren – und so die kosteneffizienteste Methode zur Erhöhung der Cybersicherheit zu ermitteln.

Serviceumfang von Cybersecurity Assessment

Phase 1: Identifizierung von Objekten, die Schutz benötigen („Objects of Protection", OoP), und Folgenabschätzung basierend auf[1]:

- Potenziellem Schaden durch einen Cybervorfall für bestimmte industrielle Objekte, einschließlich direkter finanzieller Verluste durch physische Schäden, Nachwirkungen infolge von Ausfallzeiten, Kosten im Zusammenhang mit Rufschädigung usw.
- Rolle und Einfluss des Informationssystems, das die OoP unterstützt

Auf Grundlage dieser Kriterien ermitteln KICS-Experten die wichtigsten OoPs der Infrastruktur und bieten den Kunden folgende Vorteile:

- Vollständige Liste der Informationssysteme hinter den OoPs, die untersucht werden sollten
- Priorisierte Liste der für die Cybersicherheit kritischen Informationssysteme

Phase 2: Untersuchung und Risikoanalyse, einschließlich:

- Gesprächen mit Führungskräften, Technikern, Anlagenbedienern und Systemadministratoren
- Abschätzung des derzeitigen Schutzstatus durch Analyse der aktuellen Konfigurationen, des Netzwerkverkehrs, der Speicherauszüge, Protokolle usw.
- Penetrationstests von industriellen Systemen über alle möglichen Vektoren – Internetverbindungen, Verbindungen zu interagierenden Netzwerken und Objekten
- Emulation bestimmter Angriffsvektoren – Tests spezifischer Komponenten industrieller Systeme –, Controller und Software
- Untersuchungen von Zero-Day-Schwachstellen in ausgewählten ICS-Komponenten (SCADA, HMI, Engineering-Workstations, SPS, IED, Terminals usw.) werden in einer isolierten ICS-Infrastruktur durchgeführt, um den tatsächlichen Schutzgrad besser nachzuvollziehen
- KICS-Experten können zusätzlich nach schädlichen Aktivitäten innerhalb der Infrastruktur des Kunden suchen

[1] Für die Zwecke dieses Dokuments haben wir die wichtigsten Kriterien aufgeführt. Bei jeder Bewertung werden auch unternehmensspezifische, individuelle Kriterien berücksichtigt.

Warum Kaspersky Lab?

Kaspersky Lab ist im Bereich der industriellen Cybersicherheit ein renommierter führender Anbieter von maßgeschneiderten Lösungen für die speziellen Anforderungen industrieller Infrastrukturen. Wir sind einer der wenigen Anbieter mit einem reichen Erfahrungsschatz und Expertise in diesem Marktsegment:

- Über 10 Jahre Erfahrung bzgl. der Erkennung und Analyse hoch entwickelter, hartnäckiger Bedrohungen und gezielter Angriffe, einschließlich Angriffen auf kritische und industrielle Infrastrukturen
- Einzigartige Scanmethodik zur Erkennung von industriellen Angriffsvektoren, die zu Ausfallzeiten führen können
- Engagiertes Team von Experten für industrielle Cybersicherheit, die das Zusammenspiel von Automatisierung und Sicherheit im Detail kennen
- Kaspersky Industrial CyberSecurity ist ein ganzheitliches Portfolio bestehend aus Services und Technologien, einschließlich Malware-Analyse, Schulungs- und Sensibilisierungsprogrammen, Überwachung industrieller Netzwerke, Vorfallsreaktion und vielem mehr. Ein Anbieter stellt alle Bausteine bereit, die Sie für Ihr Sicherheitssystem benötigen.

In Phase 2 erhalten Kunden:

- Eine vollständige Liste erkannter Schwachstellen und vorhandener Sicherheitslücken mit detaillierten Analysen darüber, wie sie ausgenutzt werden können
- Eine Beschreibung der erkannten und bestätigten Angriffsvektoren, die die Kontinuität oder Integrität des technologischen Prozesses beeinträchtigen können

Phase 3: Bedrohungsmodell und Empfehlungen zur Cybersicherheit

Basierend auf den Daten der Phasen 1 und 2 entwickeln KICS-Experten ein Bedrohungsmodell, das als Grundlage für die Erstellung spezifischer Empfehlungen dient. In Phase 3 erhalten Kunden:

- Eine Liste der Sicherheitsempfehlungen für bestimmte Komponenten wie SCADA, Controller usw., einschließlich Eindämmungsverfahren für Schwachstellen, die nicht auf direktem Wege behoben werden können

Phase 4: Planung von Maßnahmen für erweiterte OoP-Sicherheit

Sehr häufig wird die Umsetzung von Sicherheitsempfehlungen aufgrund der Besonderheiten technischer Prozesse, schmaler Wartungsfenster oder der Notwendigkeit zusätzlicher Analysearbeiten aufgeschoben. Um den Erfolg sicherzustellen, arbeiten die Experten von Kaspersky Lab in dieser zusätzlichen Phase mit dem Kunden zusammen, um einen umsetzbaren Sicherheitsplan zu entwickeln, der die Anforderungen von Phase 3 auf die Besonderheiten der Infrastruktur des Kunden, etwaige Einschränkungen und alles Weitere abstimmt.

In Phase 4 erhalten Kunden für jedes OoP einen umsetzbaren „To-do"-Maßnahmenplan, der von Kaspersky Lab-Experten zusammen mit den Kundenvertretern entwickelt wird.

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 ★ FINALIST ★ 2017

* 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