Kaspersky Industrial CyberSecurity: Lösungsüberblick

kaspersky BRING ON THE FUTURE

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity: Lösungsüberblick

Einleitung

Traditionell verfolgen Industriebetriebe weltweit bei der Cybersicherheit für Ihre IT- und OT (Operational Technology)-Netzwerke unterschiedliche Ansätze. Die meisten Unternehmen haben bereits ausgereifte Maßnahmen zur Erkennung von Sicherheitsverletzungen und Zwischenfällen in ihrer Unternehmensinfrastruktur. In puncto OT-Sicherheit hingegen verlassen sie sich in der Regel auf einen klassischen „Air Gap"-Ansatz. Industriebetriebe werden zunehmend „digitaler" und investieren immer mehr in intelligente Technik, neue Automatisierungssysteme und die Einführung von Industrie 4.0. Dadurch entfällt die Lücke zwischen IT- und OT-Umgebungen, die herangezogen wird, um das Übergreifen von Cyberbedrohungen auf industrielle Steuersysteme zu verhindern. Laut Kaspersky ICS CERT hat der Prozentsatz von ICS-Computer, auf denen schädliche Objekte gefunden wurden, im ersten Halbjahr 2019 einen Wert von 41,2 % erreicht[1].

Um welche Bedrohungen handelt es sich?

Zunächst fällt darunter das Risiko der versehentlichen Infektion mit konventioneller Malware. Sie müssen nicht das eigentliche Ziel sein, um zum Opfer zu werden Ein einziger USB-Stick oder eine Phishing-E-Mail mit einem Banking-Trojaner oder mit Ransomware kann sich schwerwiegend auf das Kerngeschäft eines Unternehmens auswirken, wenn sie unabsichtlich in die ICS-Umgebung eingeschleust werden. Auch wenn solche versehentlichen Infektionen nicht häufig auftreten, ist offensichtlich, dass ein motivierter Hacker auch in OT-Netzwerke eindringen und beträchtlichen Schaden an teuren Maschinen oder Fertigungsanlagen anrichten oder wertvolle Daten stehlen kann.

Wie sehen geeignete ICS-Cybersicherheitsmaßnahmen aus?

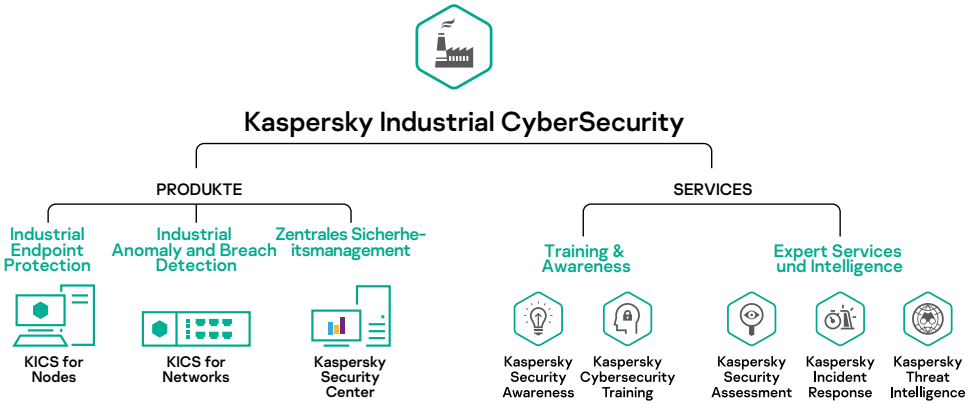
1. Schutz industrieller Endpoints, um versehentliche Infektionen zu verhindern und vorsätzliche Eindringversuche zu erschweren.
2. Überwachung des OT-Netzwerks und Erkennung von Anomalien zum Aufspüren schädlicher Vorgänge auf Ebene der speicherprogrammierbaren Steuerungen (SPS).
3. Schulungsprogramme für Mitarbeiter, um Irrtümer zu vermeiden und Risiken durch den Faktor Mensch zu minimieren.
4. Spezielle Expertenleistungen, um die Infrastruktur zu untersuchen, eine kompetente Analyse zu erstellen oder die Auswirkungen eines Zwischenfalls zu verringern.

1 Bedrohungslandschaft für industrielle Automatisierungssysteme, 1. HJ 2019, Kaspesky ICS CERT

Was bietet Kaspersky?

Kaspersky deckt für Industriebetriebe mit dem Portfolio von Kaspersky Industrial CyberSecurity (KICS) den gesamten Cybersicherheitsbedarf ab. KICS bietet einen ganzheitlichen Ansatz für industrielle Cybersicherheit und liefert in jeder Phase der OT Security des Kunden einen Mehrwert – vom Cybersecurity Assessment und Schulungen bis hin zu fortschrittlichen Technologien und Behandlung von Vorfällen.

Komponenten von Kaspersky Industrial CyberSecurity



2020 wurde Kaspersky im Gartner-Bericht „Competitive Landscape: Operational Technology Security“[2] als repräsentativer Anbieter in vier Produktkategorien genannt, darunter:

- OT Endpoint-Sicherheit;
- OT Netzwerküberwachung und -transparenz;
- Erkennung von Anomalien, Incident Response und Reporting;
- OT Security Services[2].

Die ARC Advisory Group betont, dass Kaspersky eine einzigartige Kombination aus Threat Intelligence, maschinellem Lernen und menschlicher Expertise bietet und so flexiblen Schutz vor jeder Art von Bedrohung ermöglicht[3].

Aus einer Forrester-Studie [4] geht ein ROI von 368 % für Unternehmen hervor, die Kaspersky Industrial CyberSecurity einsetzen – zusätzlich zu anderen Vorteilen wie Support durch Experten und Rundum-Sicherheit.

2 Gartner: Competitive Landscape: Operational Technology Security, März 2020
https://ics.kaspersky.com/KICS-cited-in-Gartnercompetitive-landscape-OTsecurity

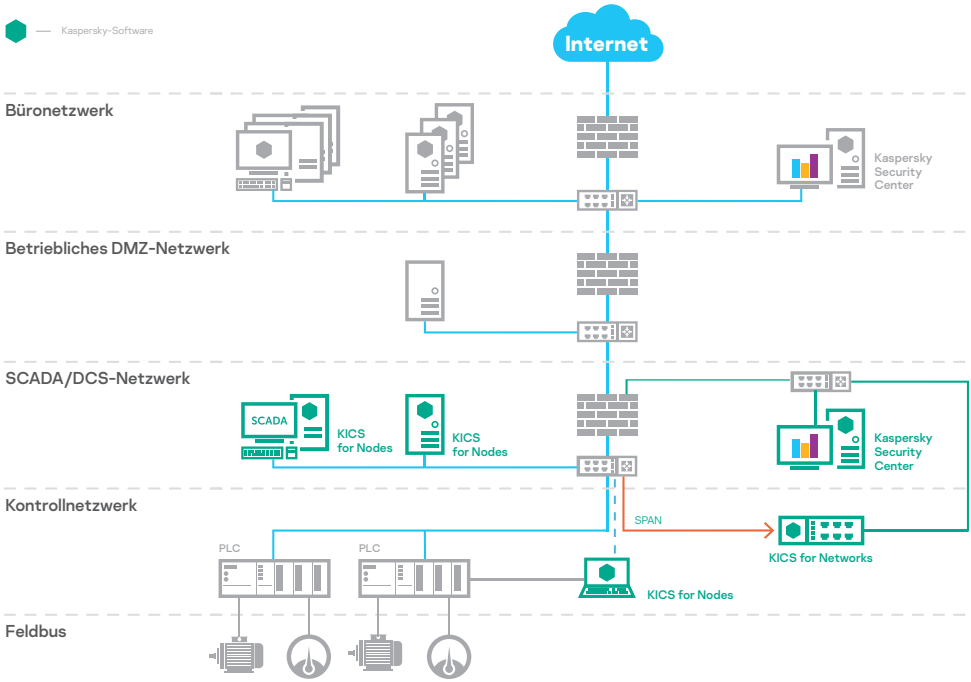
3 Arc Advisory: Kaspersky Moves Forward with Improved Cybersecurity Solutions, 2018

4 Forrester Research: The Total Economic Impact™ of Kaspersky Industrial CyberSecurity, April 2019.
https://www.kaspersky.com/ forrester-tei-for-kics

Produkte

KICS-Produkte sind auf umfassenden Schutz der industriellen Komponenten Ihrer Organisation ausgelegt: KICS for Nodes deckt industrielle Endpoints ab, während KICS for Networks die Sicherheit industrieller Netzwerke überwacht.

Einsatz von Kaspersky Industrial CyberSecurity-Produkten



KICS for Networks

KICS for Networks ist eine Überwachungs- und Transparenzlösung für OT-Netzwerke, wird als Software oder als virtuelle Appliance bereitgestellt und passiv mit dem ICS-Netzwerk verbunden.

Die Vorteile:

- ✓ **Asset Discovery**
  für passive Identifizierung und Bestandsaufnahme von OT-Ressourcen
- ✓ **Deep Packet Inspection**
  für Analyse der technischen Prozesstelemetrie beinah in Echtzeit
- ✓ **Network Integrity Control**
  zur Erkennung nicht autorisierter Netzwerk-Hosts und -ströme
- ✓ **Intrusion Detection System**
  für Benachrichtigungen über schädliche Netzwerkaktivitäten
- ✓ **Befehlsprüfung**
  Überprüfung von Befehlen über Industrieprotokolle
- ✓ **Externe Systeme**
  externe Erkennungsmöglichkeiten durch API-Integration
- ✓ **Maschinelles Lernen zur Erkennung von Anomalien (MLAD)**
  erkennt Cyber- und physische Anomalien über Telemetrie in Echtzeit und über Verlaufsdaten (rekurrentes neuronales Netz)

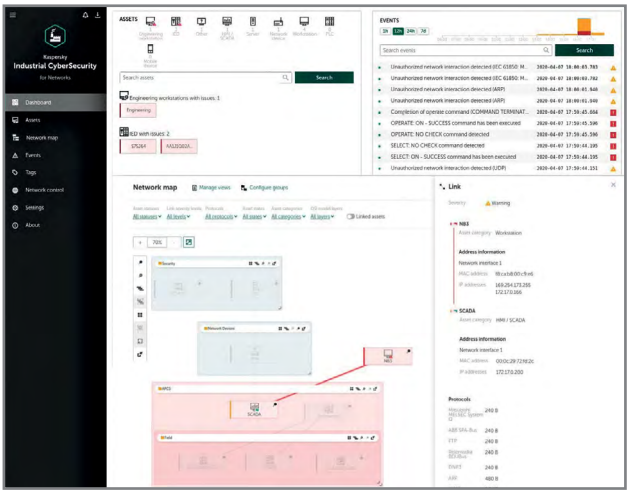
KICS for Networks erkennt Anomalien und Eindringversuche in ICS-Netzwerken in ihren frühen Phasen und sorgt für notwendige Maßnahmen, um Beeinträchtigungen der industriellen Prozesse zu verhindern.

KICS for Networks ist eine geräteneutrale Lösung, der Kunde kann also den Anbieter industrieller Rechenausrüstung wählen, dem er am meisten vertraut.

Die Benutzeroberfläche von KICS for Networks zeigt ein Live-Dashboard sowie eine Netzwerkübersicht zur Arbeit mit Ressourcen und sicherheitsrelevanten Ereignissen.

Beispiel für KICS for Networks Appliance

Benutzeroberfläche von KICS for Networks



KICS for Nodes

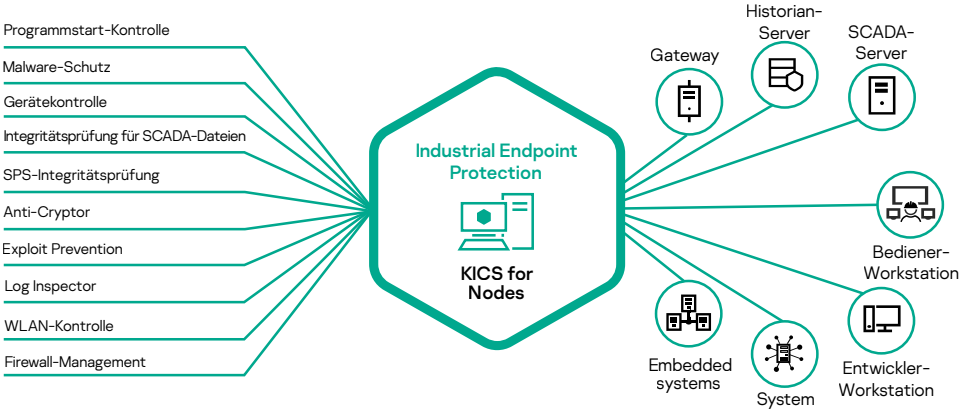
KICS for Nodes ist ein OT Endpoint Security-Produkt und wird als Software für Geräte mit Windows und Linux geliefert.

Die Vorteile:

- ✓ **Geringe Auswirkungen auf das geschützte Gerät**
- ✓ **Höchste Kompatibilität**
- ✓ **Erweiterter Schutz gegen Malware**
- ✓ **Kontrolle der Umgebung**

KICS for Nodes wurde speziell auf minimalen Ressourcenverbrauch ausgelegt. Durch die modulare, auf Sicherheits- und integrierte Systeme aufbauende Architektur brauchen Sie nur die von Ihnen benötigten Schutzkomponenten zu installieren. Die Schutzkomponenten können für die Abwehr oder nur für die Erkennung von Bedrohungen konfiguriert werden. Dieser Ansatz ist ideal für ältere Geräte, die so viel wie möglich von ihrer maximal verfügbaren Leistung brauchen.

KICS for Nodes –Funktionen und unterstützte Endpoints



„Dank der Partnerschaft mit Kaspersky konnten wir Kaspersky Industrial CyberSecurity während des laufenden Betriebs implementieren. Zudem ist die Lösung mit den Steuerungssystemen kompatibel, die wir verwenden."

Jan Houben, Werksleiter, AGC Glass Germany GmbH

KICS for Nodes bietet Schutz vor verschiedensten Cyberbedrohungen, die sich aus dem Faktor Mensch, allgemeiner Malware, gezielten Angriffen oder Sabotage ergeben können. KICS for Nodes ist mit den Software- und Hardware-Komponenten industrieller Automatisierungssysteme wie SCADA, SPS und DCS kompatibel.

Kaspersky Security Center

Kaspersky Security Center ist eine zentrale Lösung für Sicherheitsverwaltung. Sie bietet Kontrolle und Transparenz über industrielle Ebenen mehrerer Standorte sowie der umliegenden Unternehmensnetzwerke.

Die Vorteile:

✓ **Systems Management**
- Zentrale Systemdatensammlung
- Zentrale Softwarebereitstellung
- Schwachstellenerkennung und Patch Management
- Erweiterte Client-Verwaltungsfunktionen

✓ **Richtlinienverwaltung**
- Zentrale Sicherheitsrichtlinienverwaltung
- Remote-Aufgabenplanung und -ausführung

✓ **Reporting und Benachrichtigung**
- Ereignisprotokollierung
- Dashboards und Berichte
- Benachrichtigungen per SMS/E-Mail

✓ **SIEM-Integration**
- Arcsight, Splunk, Qradar
- Syslog-Server

✓ **HMI-Integration**

✓ **MES-Dashboard-Integration**
- Sicherheitsstatus- und Informationsbereitstellung an Host, KOMPATIBEL MIT IEC 104/OPC 2.0

Kaspersky Industrial CyberSecurity: services

Unser Serviceangebot ist ein wichtiger Teil des KICS-Portfolios. Wir bieten eine umfassende Palette von Sicherheitsservices, vom Cybersecurity Assessment bis hin zur Vorfallreaktion.

Expert Services

„Ihre Erfahrung im Bereich der ICS-Cybersicherheit, ihre Professionalität und die Komplexität ihrer Lösung im Vergleich zu anderen Anbietern haben uns einen hohen Stellenwert und eine gute Zukunft für die Sicherheitsstrategie unseres Unternehmens gesichert."

Ondřej Sýkora, C&A Manager, Plzeňský Prazdroj

- **Industrial Cybersecurity Assessment:** Kaspersky bietet eine minimal invasive Bewertung der industriellen Cybersicherheit mit internem und externem Penetration Testing, Bewertung der OT Security und der Sicherheit der Automatisierungslösung. Spezialisten von Kaspersky liefern wichtige Erkenntnisse über die Infrastruktur eines Unternehmens und geben Empfehlungen zur Stärkung der ICS-Cybersicherheit ab.

- **Threat Intelligence:** Aktuelle, von Kaspersky-Spezialisten ausgearbeitete Analysen helfen dabei, den Schutz des Kunden vor zielgerichteten industriellen Cyberangriffen zu optimieren. Die Bereitstellung erfolgt in Form von TI-Feeds oder maßgeschneiderten Berichten, die spezielle Kundenanforderungen gemäß regionalen, branchenspezifischen und ICS-Software-Parametern erfüllen.

„Indem wir die Übung absolviert und vom Kaspersky-Team gelernt haben, konnten wir unseren Schutz gegen Cyberbedrohungen verbessern."

Yu Tat Ming, CEO,
PacificLight

- **Incident Response:** Bei einem Cybersicherheitsvorfall erfassen und analysieren unsere Experten die Daten, rekonstruieren die Timeline des Vorfalls, bestimmen mögliche Quellen und Gründe und entwickeln einen Plan zur Problemlösung. Darüber hinaus bietet Kaspersky einen Service zur Malware-Analyse. Dabei kategorisieren die Spezialisten von Kaspersky die bereitgestellte Malware-Probe, analysieren deren Funktionen und Verhaltensweisen und stellen Empfehlungen sowie einen Plan auf, um die Malware zu entfernen und ein Rollback aller schädlichen Aktionen durchzuführen.

Training & Awareness

„Kaspersky war am besten geeignet, um unserer ICS-Gruppe professionelle Industrial Cybersecurity-Schulungen bereitzustellen."

Søren Egede Knudsen,
Chief Technical Officer,
Ezenta

- **Industrial Cybersecurity Awareness Training:** Interaktive Vor-Ort- und Online-Schulungsmodule und Spiele zum Thema Cybersicherheit für Bedienpersonal industrieller Computersysteme und für Manager. Die Teilnehmer erhalten neue Einblicke in die aktuelle Bedrohungslandschaft und Angriffsvektoren, die insbesondere auf Industrieumgebungen abzielen. Es werden praxisnahe Szenarien durchgearbeitet und Kenntnisse für cybersicheres Arbeiten erworben. Der Vor-Ort-Kurs kann auf eine Dauer von einem oder zwei Tagen angepasst werden.

- **Expert Training Programs:**Die Schulungsmodule ICS Penetration Testing und ICS Digital Forensics wurden für Cybersicherheitsprofis entwickelt. Die Teilnehmer erwerben alle erforderliche Fähigkeiten zur Durchführung umfangreicher Pentests oder digitaler Forensik in Industrieumgebungen. Diese Schulung umfasst eine Zertifizierung.

Mehr über KICS erfahren Sie unter
https://ics.kaspersky.de

#Kaspersky
#BringontheFuture

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. Weltinternet- konferenz

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