KASPERSKY lab

Kaspersky Industrial CyberSecurity: Lösungsüberblick 2019

www.kaspersky.de/ics
#truecybersecurity

Kaspersky Industrial CyberSecurity: Lösungsüberblick 2019

Angriffe auf Industrieanlagen nehmen zu

Drei von vier Industrieunternehmen glauben, dass sie Opfer eines ICS-Cyberangriffs sein werden, und diesbezüglich bewerten 77 % der Unternehmen die Cybersicherheit als eine der wichtigsten Prioritäten[1]. Unterbrechungen der Geschäftsaktivitäten und der Lieferkette wurden in den letzten sechs Jahren als globales Geschäftsrisiko Nr. 1 eingestuft. Cybervorfälle befanden sich 2018 auf Platz 2[2]. Die Risiken für Unternehmen mit industriellen oder anderen kritischen Infrastruktursystemen sind heute so hoch wie nie zuvor. 40 % der Industrieunternehmen geben an, dass die Unterbrechung der Geschäftskontinuität die schwerwiegendste Folge eines Cyberangriffs sein würde[3]. Der Bereich der industriellen Sicherheit hat eine Tragweite, die weit über den Schutz von Unternehmen und geschäftlicher Reputation hinausgeht. Beim Schutz von industriellen Systemen vor Cyberbedrohungen spielen ökologische, soziale und makroökonomische Faktoren eine erhebliche Rolle.

[1] Stand der industriellen Cybersicherheit 2018, Kaspersky Lab

[2] Allianz Risk Barometer 2018

[3] PwC: The Global State of Information Security, 2018

Betriebstechnologie und Informationstechnologie (OT vs. IT)

Nach Definition der Automatisierungsnorm IEC 62443 ist ein industrielles Steuerungssystem (ICS) eine Kombination aus Mitarbeitern, Hardware und Software, die den sicheren und zuverlässigen Betrieb eines industriellen (technologischen) Prozesses beeinflussen kann.

Industrielle Steuerungssysteme sind unter anderem:

- DCS (Distributed Control Systems), PLC (Programmable Logic Controllers), RTU (Remote Terminal Units), IED (Intelligent Electronic Devices), SCADA (Supervisory Control And Data Acquisition) und Diagnosesysteme
- zugehörige interne, menschliche, Netzwerk- oder Maschinen-Schnittstellen, die Steuerungs-, Sicherheits- und Betriebsfunktionen für kontinuierliche, diskrete und andere Prozesse bieten

Allgemeiner ausgedrückt kann jede industrielle Systeminfrastruktur in zwei Bereiche unterteilt werden:

- Informationstechnologie (IT) – Systeme zur Datenverwaltung im Rahmen der Unternehmensziele
- Betriebstechnologie (Operational Technology, OT) – Systeme, die für die Verwaltung der physikalischen industriellen Prozesse der industriellen Automatisierung erforderlich sind

IT-Sicherheitsstrategien konzentrieren sich in der Regel auf den Datenschutz und verfolgen die Ziele des „C-I-A"-Modells: Datenvertraulichkeit, Integrität und Verfügbarkeit (Data Confidentiality, Integrity and Availability). Bei den meisten OT-Systemen liegt der Fokus der Cybersicherheit jedoch nicht auf Daten, sondern auf der Kontinuität industrieller Prozesse. Dem C-I-A-Modell entsprechend ist „Verfügbarkeit" daher also ein Schwerpunkt der Sicherheitsstrategien für OT. Damit unterscheiden sich die Anforderungen an industrielle Cybersicherheit von denen anderer Systeme, sodass selbst die effektivste klassische IT-Cybersicherheitslösung für den Einsatz auf OT-Systemen ungeeignet ist und die Verfügbarkeit (und in einigen Fällen auch die Integrität) von Prozessen gefährdet.

Risiken und Bedrohungen

Trotz des wachsenden Bewusstseins für die zunehmende Verbreitung cyber-basierter Angriffe auf industrielle Steuerungssysteme wird bei vielen Modellen zur IT-Sicherheit auch weiterhin die veraltete Ansicht vertreten, dass physisch isolierende Systeme (durch Luftschleusen, sog. „Air Gaps") und „Security by Obscurity" ausreichen. Das ist nicht der Fall: Im Zeitalter von Industry 4.0 sind die meisten nicht kritischen Industrienetzwerke über das Internet zugänglich[4], ob gewollt oder nicht. Umfassende Untersuchungen von Kaspersky Lab ICS CERT unter Verwendung von Daten aus dem Kaspersky Security Network zeigen, dass Industrie-PCs regelmäßig Opfer der gleichen generischen Malware werden, die auch Unternehmenssysteme (IT) befällt, darunter u. a. auch bekannte Täter wie Trojaner, Viren und Würmer. In der ersten Jahreshälfte 2018 blockierten die Produkte von Kaspersky Lab weltweit versuchte Malware-Angriffe auf 41,2 % aller durch Kaspersky Lab geschützten Computer, die als Bestandteil der industriellen Infrastruktur eingestuft wurden[5].

Eine weitere ICS-Bedrohung mit Aufwärtstrend ist Ransomware. Zwischen 2015 und 2017 haben sich Anzahl und Umfang der entwickelten Ransomware drastisch erhöht. Diese neu aufkommende Ransomware hat große Auswirkungen auf die Industriebranche, da derartige Infektionen zu schwerwiegenden Systemschäden führen können. ICS sind also ein besonders attraktives potentielles Angriffsziel, wie zahlreiche Vorfälle von Ransomware-Angriffen (vor allem Infektionen durch WannaCry und exPetr) auf ICS/SCADA-Systeme im Jahr 2017 belegen. Bald könnte Ransomware, die speziell für Angriffe auf industrielle Systeme entwickelt wurde, besondere Funktionen aufweisen – statt Daten zu verschlüsseln, könnte das Ziel dieser Malware darin bestehen, die betrieblichen Abläufe zu stören oder den Zugriff auf wichtige Ressourcen zu blockieren.

Neben generischen Bedrohungen muss die industrielle Sicherheit auch ICS-spezifische Malware und gezielte Angriffe abwehren: Stuxnet, Havex, BlackEnergy, Industroyer und das aktuelle Triton, das sich Safety Instrumented Systems als Ziel gesetzt haben – die Liste wird stetig länger. Wie die Stuxnet- und BlackEnergy-Angriffe gezeigt haben, kann schon ein infiziertes USB-Laufwerk oder eine einzelne Spear-Phishing-E-Mail dazu führen, dass gut vorbereitete Angreifer den so genannten „Air Gap" überwinden und in ein isoliertes Netzwerk eindringen.

Zusätzlich zu Malware und gezielten Angriffen müssen Industrieunternehmen weitere Bedrohungen und Risiken abwehren, die auf Menschen, Prozesse und Technologie abzielen. Diese Risiken zu unterschätzen, kann ernsthafte Konsequenzen haben. Kaspersky Lab entwickelt Lösungen und Services, mit denen unsere Kunden nicht nur Malware und zielgerichtete Angriffe, sondern auch viele andere Cyber-Vorfälle und Risikofaktoren bewältigen können, wie beispielsweise:

- Fehler durch SCADA-Bediener oder Auftragnehmer (Dienstanbieter)
- Betrügerische Handlungen
- Cybersabotage
- Compliance-Probleme
- Mangelndes Bewusstsein und wenig nutzbare Daten für forensische Untersuchungen

[4] ICS and their online availability 2016, Kaspersky Lab

[5] Threat Landscape for Industrial Automation Systems for H1 2018, Kaspersky Lab ICS CERT

Spezielle industrielle Cybersicherheitslösungen sind erforderlich

Lösungen, die den besonderen Anforderungen industrieller Steuerungssysteme und einer industriellen Infrastruktur gerecht werden, können nur von Cybersicherheitsanbietern bereitgestellt werden, die die Unterschiede zwischen cyberphysischen Unternehmen und datenorientierten Unternehmenssystemen verstehen. Forrester Research empfiehlt Industrieunternehmen, bei ihrem Sicherheitsanbieter auf „spezielle Branchenfachkenntnisse" zu achten. ARC Advisory betont, dass Kaspersky Lab die einzigartige Kombination aus Threat Intelligence, maschinellem Lernen und menschlicher Expertise bietet und so flexiblen Schutz vor jeder Bedrohungsart ermöglicht[6].

Kaspersky Lab: vertrauenswürdiger Anbieter von Cybersicherheit

Als renommierter Anbieter im Bereich der Cybersicherheit und Schutz von industriellen Systemen[7] ist Kaspersky Lab mit der kontinuierlichen Weiterentwicklung von Lösungen beschäftigt, die mehr leisten und mit den sich ständig weiterentwickelnden Bedrohungen für industrielle Anlagen und wichtige Infrastrukturen umgehen können. Von der Betriebsführung bis zur ICS-Ebene und darüber hinaus trägt Kaspersky Lab entscheidend dazu bei, dass Industrie, Behörden und staatliche Stellen auf der ganzen Welt rechtzeitig auf Veränderungen in der Bedrohungslandschaft vorbereitet sind und sich dagegen schützen können.

Als verlässlicher IT-Sicherheitsanbieter und Partner für führende Industrieunternehmen, die unsere Lösungen zum Malware-Schutz bereits seit vielen Jahren nutzen, arbeitet Kaspersky Lab überdies mit namhaften Anbietern aus dem Bereich der industriellen Automatisierungstechnik zusammen, darunter Emerson, SAP, Siemens, Schneider Electric, Industrial Internet Consortium etc. Unser gemeinsames Ziel ist die Entwicklung spezieller, kompatibler Verfahren und Kooperations-Frameworks zum Schutz von industriellen Systemen vor bestehenden und aufkommenden Bedrohungen, einschließlich gezielter Angriffe.

Kaspersky Lab hat ein Portfolio von Speziallösungen für bestimmte Sicherheitsanforderungen in Industrieunternehmen entwickelt: Kaspersky Industrial CyberSecurity (KICS). Kaspersky Industrial CyberSecurity verfolgt einen ganzheitlichen Ansatz für die industrielle Cybersicherheit und bietet in jeder Phase des OT-Sicherheitsprozesses des Kunden einen Mehrwert – vom Cybersecurity Assessment und Training bis hin zu fortschrittlichen Technologien und Incident Response.

Im Jahr 2018 wurde Kaspersky Lab im Gartner-Bericht „Competitive Landscape: Operational Technology Security" als renommierter Anbieter in 4 Kategorien hervorgehoben:

- OT-Endpoint Security,
- OT-Netzwerküberwachung und -transparenz,
- Erkennung von Anomalien, Incident Response und Reporting,
- OT-Security Services[8].

[6] Arc Advisory: Kaspersky Lab Moves Forward with Improved Cybersecurity Solutions, 2018

[7] Gartner Market Guide for Operational Technology Security, Juli 2018

[8] Gartner: Competitive Landscape: Operational Technology Security, Oktober 2018.

Lesen Sie den vollständigen Gartner-Bericht:

https://ics.kaspersky.com/KICS-cited-in-Gartner-competitive-landscape-OT-security

Komponenten von Kaspersky Industrial CyberSecurity

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 Vorfallsreaktion.

Schulung und Sensibilisierung

- **Schulungen:** Kaspersky Lab bietet Schulungen für Cybersicherheitsexperten und OT-Manager/ICS-Betreiber. In der Schulung „Advanced Industrial Cybersecurity in Practice" erhalten die Teilnehmer z. B. einen Einblick in die relevanten Cyberbedrohungen, deren Entwicklungstrends und die wirksamsten Vorgehensweisen, um sich gegen diese Bedrohungen zu schützen. Das Kursangebot bietet Sicherheitsexperten auch die Möglichkeit, ihre Kenntnisse in bestimmten Bereichen weiterzuentwickeln, einschließlich ICS-Penetrationstests und digitaler Forensik.

- **Awareness-Programme:** Um das Bewusstsein für Cybersicherheitsprobleme zu erhöhen und die Fähigkeiten zur Lösung dieser zu fördern, bietet Kaspersky Lab CyberSafety „Spiele" für Sicherheitsmanager und Techniker. Bei der Kaspersky Industrial Protection Simulation (KIPS) beispielsweise werden echte Cyberangriffe auf industrielle Automatisierungssysteme simuliert und die primären Probleme bei der Bereitstellung industrieller Cybersicherheit aufgezeigt.

Expert Services

- **Cybersecurity Assessment:** Unternehmen, die sich um die potentiellen betrieblichen Auswirkungen der IT-/OT-Sicherheit sorgen, bietet Kaspersky Lab vor der Installation ein minimal invasives industrielles 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 bestehenden Cybersicherheit, selbst wenn keine weiteren Schutztechnologien bereitgestellt werden.
- **Informationen zur Bedrohungslandschaft:** Aktuelle Analysen, die von Experten von Kaspersky Lab zusammengestellt wurden, tragen dazu bei, den Cyberschutz von Kunden vor zielgerichteten Cyberangriffen zu verbessern. Diese werden als TI-Feeds (Threat Intelligence) oder Berichte bereitgestellt und decken individuelle Kundenanforderungen nach regionalen, branchenspezifischen und ICS-Softwareparametern ab.
- **Vorfallsreaktion:** 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 Lab einen Service zur Malware-Analyse. Dabei kategorisieren die Spezialisten von Kaspersky Lab 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.

Kaspersky Industrial CyberSecurity: zentrale Sicherheitsverwaltung

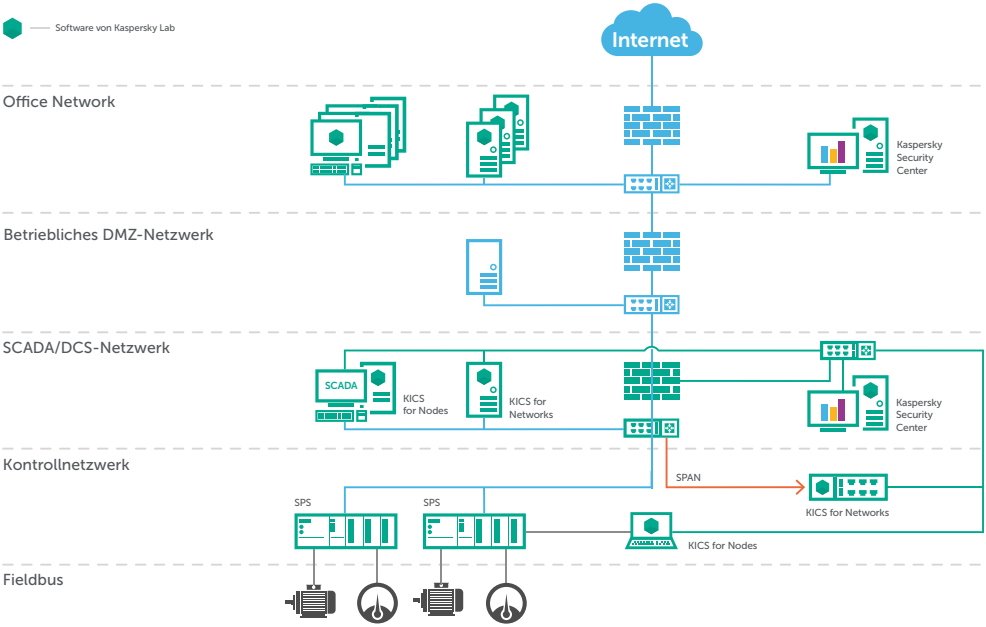
Kaspersky Security Center

Für den bestmöglichen Schutz vor allen Angriffsvektoren muss die Sicherheit für Industrieanlagen sowohl am Node, als auch auf Netzwerkebene ansetzen. KICS ist für optimale Kontrolle, einfache Verwaltung und hohe Transparenz ausgelegt und wird, wie alle Schutztechnologien von Kaspersky Lab, über eine einzige Management-Konsole gesteuert – das Kaspersky Security Center. Dies hat folgende Vorteile:

- Zentrale Verwaltung von Sicherheitsrichtlinien, Festlegen unterschiedlicher Schutzeinstellungen für verschiedene Nodes und Gruppen
- Vereinfachtes Testen von Updates vor der Einführung im Netzwerk, somit umfassende Prozessintegrität
- Rollenbasierter Zugriff im Rahmen der Sicherheitsrichtlinien und dringenden Maßnahmen

Das Kaspersky Security Center gewährleistet eine einfache Steuerung und hohe Transparenz nicht nur auf industrieller Ebene an mehreren Standorten, sondern auch auf den zugehörigen geschäftlichen Ebenen, wie im Folgenden dargestellt.

Deployment der KICS-Komponenten (Kaspersky Industrial CyberSecurity)



Kaspersky Security Gateway

KICS kann auch ereignisbezogene Daten an andere Systeme wie z. B. SIEMs, MESs und Business-Intelligence-Lösungen senden. Alle erkannten Vorfälle und Anomalien werden über CEF-2.0-, LEEF- und Syslog-Protokolle an Drittanbietersysteme wie SIEM, Mail, Syslog-Server und Netzwerkmanagement-Systeme gesendet. Neben dem Aufspüren, Bekämpfen und Untersuchen von Cyberangriffen unterstützt die gründliche Überwachung industrieller Netzwerke die vorausschauende Wartung.

Integration mit HMIs (Human-Machine Interfaces)

Die Lösung kann Sicherheitsbenachrichtigungen direkt an HMIs senden und liefert Mitarbeitern in der Produktion spezielle Informationen zur sofortigen Reaktion und Eskalation des Cybervorfalls.

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes wurde speziell für die Abwehr von Bedrohungen auf Betreiberebene in ICS-Umgebungen entwickelt. Es schützt ICS/SCADA-Server, HMIs und Engineering-Workstations vor den unterschiedlichen Cyberbedrohungen, die durch menschliche Faktoren, generische Malware, zielgerichtete Angriffe oder Sabotage entstehen können. KICS for Nodes ist mit den Software- und Hardware-Komponenten industrieller Automatisierungssysteme wie SCADA, SPS und DCS kompatibel.

Bedrohungen und Risikofaktoren	Technologien von Kaspersky Lab
Nicht autorisierte Ausführung von Software	Whitelisting; Präventions- oder ausschließlicher Erkennungsmodus (Registrierung statt Blockierung)
Malware	Fortschrittliche signaturbasierte Erkennungs-Engines für Malware-Schutz: Cloud-basierte Erkennungs-Engine, die Kaspersky Lab Public Cloud (KSN) oder Private Cloud (KPSN) nutzt NEU: **Dateiintegritätsüberwachung**
Crypto-Malware einschließlich Ransomware	Anti-Cryptor
Netzwerkangriffe	Host-basierte Firewall NEU: **Memory-Schutz (Exploit Prevention), Log Inspector**
Nicht autorisierte Geräteverbindungen	Gerätekontrolle
Nicht autorisierte WLAN-Verbindungen	WLAN-Netzwerkkontrolle
Gefälschte SPS-Programme	SPS-Integritätsprüfung
ICS-spezifische Funktionen: Air Gaps, Fehlalarme (False Positives) für ICS-Software und -Prozesse usw.	Vertrauenswürdige Updates, die mit Software von führenden Industrieanbietern getestet wurden, Zertifizierung der Produkte durch führende Anbieter von Lösungen zur industriellen Automatisierung

Anwendungs-Whitelists

Die relativ statische Beschaffenheit von ICS-Endpoint-Konfigurationen bedeutet, dass Integritätskontrollmaßnahmen sehr viel effektiver sind als in dynamischen Unternehmensnetzwerken. KICS for Nodes umfasst u. a. die folgenden Technologien zur Integritätskontrolle:

- Steuerung von Programminstallation und Programmstart anhand von Whitelist- (Best Practice für industrielle Kontrollnetzwerke) oder Blacklist-Richtlinien
- Steuerung des Programmzugriffs auf Betriebssystemressourcen: Dateien, Ordner, Systemregistrierung usw.

- Kontrolle aller in Windows-Umgebungen ausgeführten Installationsdateien wie exe, dll, ocx, Treiber, ActiveX, Skripte, Kommandozeileninterpreter und Kernel-Modus-Treiber
- Aktualisierung der Reputationsdaten von Programmen
- Vordefinierte und kundendefinierte Programmkategorien zur Verwaltung von Listen kontrollierter Programme
- Feinabstimmung der Programmkontrollen für unterschiedliche Benutzer
- Modi für Überwachung oder Erkennung: Blockieren aller Programme, die nicht in der Whitelist aufgeführt sind oder sich nicht im Beobachtungsmodus befinden; Zulassen der Ausführung von Programmen, die nicht in der Whitelist aufgeführt sind, wobei diese Aktivität aber zur Überprüfung im Kaspersky Security Center registriert wird

Gerätekontrolle

Zugriffsverwaltung für Wechseldatenträger, Peripheriegeräte und System Busses je nach Gerätekategorie, Gerätefamilie und bestimmter Geräte-ID

- Unterstützung für Whitelists und Blacklists
- Detaillierte Richtlinienzuweisung pro Computer und Benutzer für einzelne Benutzer/Computer oder eine Gruppe von Benutzern/Computern
- Modi nur für Überwachung oder nur für Erkennung

Host-basierte Firewall

Einrichten und Durchführen von Netzwerkzugriffsrichtlinien für geschützte Nodes wie Server, HMIs oder Workstations. Wichtige Funktionen:

- Zugriffssteuerung für eingeschränkte Ports und Netzwerke
- Erkennen und Blockieren von Netzwerkangriffen aus internen Quellen, z. B. Laptops von Dienstleistern, über die Malware eingeschleust werden kann, die den Host sofort nach Verbindung mit dem industriellen Netzwerk scannt und infiziert

WLAN-Netzwerkkontrolle

Dies ermöglicht die Überwachung aller Versuche, eine Verbindung zu nicht autorisierten WLAN-Netzwerken herzustellen. Die Aufgabe der WLAN-Kontrolle basiert auf der Default-Deny-Technologie, die automatisch Verbindungen zu einem WLAN-Netzwerk blockiert, das in den Aufgabeneinstellungen nicht erlaubt ist.

SPS-Integritätsprüfung

Dies ermöglicht zusätzliche Kontrolle über SPS-Konfigurationen anhand regelmäßiger Überprüfungen eines bestimmten, durch Kaspersky Lab geschützten Servers. Die Prüfsummen-Ergebnisse werden mit gespeicherten „Etalon"-Werten verglichen und alle Abweichungen gemeldet.

Dateiintegritätsüberwachung

Diese Funktion dient der Überwachung von Aktivitäten in bestimmten Dateien und Ordnern im überwachten Bereich, der in den Aufgabeneinstellungen angegeben ist. Sie können diese Funktion zur Feststellung von Dateiänderungen verwenden, die möglicherweise auf eine Sicherheitsverletzung auf dem geschützten Server hindeuten – wie Änderungen an SCADA-Projekten, die auf einem SCADA-Server gespeichert sind.

Moderner Malware-Schutz

Die Technologien zur Malware-Erkennung und zum Malware-Schutz von Kaspersky Lab wurden angepasst und verbessert, um dem intensiven Ressourcenverbrauch und den hohen Anforderungen an die Systemverfügbarkeit gerecht zu werden. Unser fortschrittlicher Malware-Schutz funktioniert sogar in statischen oder nur selten aktualisierten Umgebungen. Die Anti-Malware-Lösung von Kaspersky Lab umfasst die gesamte Palette an Technologien; dazu gehören:

- Signaturbasierte Malware-Erkennung
- Zugriffs- und bedarfsabhängige Erkennung
- Speicherinterne (speicherresidente) Erkennung
- Ransomware-Erkennung durch spezielle Anti-Cryptor-Technologie
- Erstklassiger Malware-Erkennungsservice mit dem Kaspersky Security Network (KSN) und dem Kaspersky Private Security Network (KPSN)

Vertrauenswürdige Updates

Um sicherzustellen, dass die Sicherheits-Updates von Kaspersky Lab keine Auswirkungen auf die Verfügbarkeit des geschützten Systems haben, werden sowohl vor Datenbank-/Komponentenfreigaben als auch vor PCS-Software-/Konfigurations-Updates Kompatibilitätsüberprüfungen durchgeführt. Potentielle Probleme bei der Ressourcenbelastung können anhand unterschiedlicher Szenarien gelöst werden:

- Kaspersky Lab führt Kompatibilitätstests für Datenbank-Updates mit industrieller Anbietersoftware zur Automatisierung in unserer unternehmenseigenen Testumgebung durch
- Ihr IAV führt Kompatibilitätsüberprüfungen durch
- Kaspersky Lab überprüft die Updates der Sicherheitsdatenbank für Sie: SCADA-Server, Workstation und HMI-Images werden in die Testumgebung von Kaspersky Lab integriert
- Die Sicherheits-Updates von Kaspersky Lab werden an Ihrem Standort getestet und über das Kaspersky Security Center automatisiert

Kaspersky Industrial CyberSecurity for Networks

Die Sicherheitslösung auf Netzwerkebene von Kaspersky Lab arbeitet auf der Ebene des industriellen Kommunikationsprotokolls (Modbus, IEC-Stack, ISO usw.) und untersucht den Datenverkehr von Industrieunternehmen mithilfe fortschrittlicher DPI-Technologie (Deep Packet Inspection) auf Anomalien. Netzwerkintegritätskontrolle und IDS-Fähigkeiten werden ebenfalls bereitgestellt.

Bedrohungen und Risikofaktoren	Technologien von Kaspersky Lab
Nicht autorisierte Netzwerkgeräte im industriellen Netzwerk	Network Integrity Control entdeckt neue/unbekannte Geräte **NEU: Ressourcenerkennung, Netzwerkübersicht**
Nicht autorisierte Kommunikation im industriellen Netzwerk	Network Integrity Control überwacht die Kommunikation zwischen bekannten/unbekannten Geräten **NEU: Ressourcenerkennung, Netzwerkübersicht**
Schädliche SPS-Befehle durch: • Anlagenbediener oder Drittanbieter (beispielsweise Auftragnehmer), versehentlich • Insider (betrügerische Handlungen) • Angreifer/Malware	Technologische DPI analysiert Kommunikationen zu und von den SPS und kontrolliert alle Befehls- und Parameterwerte der Technologieprozesse.
Netzwerkangriffe	Fortschrittliches Intrusion Detection System: Erkennt alle bekannten Netzwerkangriffsmuster, einschließlich der Ausnutzung von Schwachstellen in industrieller Software und Hardware **NEU: Ereigniskorrelationen**
Keine Daten für Untersuchungen und Forensik	Forensik-Tools: Überwachung und sichere Protokollierung von verdächtigen Ereignissen in industriellen Netzwerken und erkannten Angriffen

Nicht-invasive Kontrolle des industriellen Netzwerkverkehrs

KICS for Networks ermöglicht eine passive Überwachung von Anomalien und Netzwerksicherheit und bleibt doch für potentielle Angreifer unsichtbar. Für die Installation muss lediglich die Port-Spiegelung aktiviert/konfiguriert werden, und eine einfache Integration der Software-/Virtual oder Hardware-Appliance in vorhandene industrielle Netzwerkgeräte wird über den SPAN-Port des vorhandenen Switches oder TAP-Geräts erzielt. KICS for Networks ist modular aufgebaut – Sensoren können einzeln von einer zentralen Steuereinheit eingesetzt werden.

Industrielle DPI zur Erkennung anormalen Verhaltens

KICS for Networks bietet Industrieunternehmen eine vertrauenswürdige Plattform zur Überwachung des Befehlsflusses und der Telemetriedaten bei der Prozesskontrolle. Dies hat u. a. die folgenden Vorteile:

- Erkennung aller Befehle, durch die eine SPS neu konfiguriert oder der SPS-Status geändert würde
- Steuerung von Parameteränderungen in Technologieprozessen
- Schutz vor externen Bedrohungen unter gleichzeitiger Risikosenkung von „erweiterten" Insider-Störungen durch Ingenieure, SCADA-Bediener oder andere interne Mitarbeiter mit direktem Systemzugriff

Lernfähige Systeme

Unsere industrielle DPI kann nicht nur nach einem regelbasierten Standardansatz konfiguriert werden, sondern kann auch Anomalien innerhalb industrieller Prozesse über ein leistungsfähiges LSTM-basiertes Prognosemodell erkennen. Durch Maschinenlernfunktionen erreicht die Erkennung industrieller Anomalien ein neues Niveau, was die Erkennung von Vorfällen in den komplexesten und oft neu konfigurierten industriellen Netzwerken ermöglicht.

Netzwerkintegritätskontrolle für Sicherheit und Bestandsverwaltung

Mit KICS for Networks können Sie alle mit dem Ethernet verbundenen Netzwerkressourcen identifizieren, darunter SCADA-Server, HMIs, Engineering-Workstations, SPS, IEDs und RTUs. Alle neuen oder unbekannten Geräte und die zugehörige Kommunikation werden automatisch erkannt. Dadurch erhalten Sicherheitsteams die Möglichkeit, ihre eigenen, zuverlässigen und sicheren Netzwerkbestände zur Ressourcenverwaltung zu entwickeln, statt potentiell anfällige OT/IT-Verwaltungstools zu verwenden, auf die es Angreifer besonders abgesehen haben.

Forensiktools

Die Lösung von Kaspersky Lab stellt industriellen Benutzern ein sicheres Protokollsystem mit Tools für Datenanalyse und digitale Forensik bereit. Darüber hinaus lässt das System Änderungen an ICS-Protokollen nicht zu.

Weitere Services für Kaspersky Industrial Cybersecurity

Kaspersky Security Network

Das Kaspersky Security Network (KSN) ist eine Cloud-basierte, komplexe verteilte Infrastruktur für die intelligente Verarbeitung sicherheitsrelevanter Datenströme von Millionen freiwilliger Teilnehmer weltweit. Das KSN ermittelt und blockiert nicht nur aktuelle Bedrohungen und Zero-Day-Angriffe, sondern unterstützt Kunden auch beim Ermitteln von Online-Angriffsquellen und deren Aufnahme in eine Blacklist. So werden Reputationsdaten für Webseiten und Programme bereitgestellt.

Alle Unternehmenslösungen von Kaspersky Lab, einschließlich denen für industrielle Anwendungen, können auf Wunsch mit dem KSN verbunden werden. Wichtige Funktionen:

- Hohe Erkennungsraten
- Kürzere Reaktionszeiten: Herkömmliche, signaturbasierte Antworten dauern Stunden, das KSN reagiert in etwa 40 Sekunden
- Weniger Fehlalarme (False Positives)
- Reduzierter Ressourcenverbrauch für standortgebundene Sicherheitslösungen

Kaspersky Private Security Network (KPSN)

Für Unternehmen mit speziellen Datenschutzanforderungen hat Kaspersky Lab das Kaspersky Private Security Network entwickelt. Es bietet so gut wie alle Vorteile des KSN, es werden aber keine Informationen an Ziele außerhalb des eigenen Netzwerks übertragen.

Das KPSN kann im Rechenzentrum eines Unternehmens installiert werden. Die eigenen IT-Spezialisten behalten so die vollständige Kontrolle. Lokale KPSN-Installationen können zur Erfüllung landesspezifischer Compliance-Anforderungen oder anderer branchenspezifischer gesetzlicher Auflagen nützlich sein.

Wichtigste Funktionen des KPSN:

- Datei- und URL-Reputationsservices: MD5-Hashes für Dateien, reguläre Ausdrücke für URLs und Malware-Verhaltensmuster werden zentral gespeichert, kategorisiert und schnell auf dem Client bereitgestellt
- Record Management System (RMS): Bisweilen treten Fehler in der Sicherheitssoftware auf, und Dateien oder URLs werden fälschlicherweise als vertrauenswürdig/nicht vertrauenswürdig eingestuft; RMS verhindert Fehlalarme (False Positives), korrigiert Fehler und führt kontinuierliche Analysen zur Qualitätsverbesserung durch
- Cloud-basierte Informationen

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 industriellen Prozesse zu beeinträchtigen.

Weitere Informationen finden Sie unter
www.kaspersky.de/ics

Informationen über ICS-Cybersicherheit:
https://ics-cert.kaspersky.com

Neues über Cyberbedrohungen:
https://de.securelist.com

#truecybersecurity

www.kaspersky.de

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

* Auszeichnung „World Leading Internet Scientific and Technological Achievement Award" auf der 3. World Internet Conference (Wuzhen-Gipfel)

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