Cybersicherheit für Stromversorger

www.kaspersky.de/enterprise-security/industrial
#truecybersecurity

Cybersicherheit für Stromversorger

Ein modernes Stromversorgungssystem ist eine komplexe technische Einrichtung, die im Hinblick auf ihren Umfang und ihre Bedeutung für unser aller Leben einmalig ist. In Anbetracht der physischen Eigenschaften des elektrischen Stroms und der hohen Geschwindigkeit elektrischer Prozesse gestaltet sich die Kontrolle über den Betrieb einer solchen Einrichtung sowohl organisatorisch als auch technisch äußerst kompliziert. Deshalb wurden schon zu Beginn der Stromindustrie Geräte entwickelt, die Stromanlagen in Notfällen schützen und Prozesse automatisieren. Die Anforderungen für diese Geräte, ihr Design und ihre Funktionalität haben sich – wie auch die Stromversorgungssysteme – seither deutlich weiterentwickelt, um auch heute einen optimalen Betrieb gewährleisten und die Verbrauchernachfrage bedienen zu können.

Bei Protection, Automation and Control Systems (PACS), also Systemen für Schutz und Automatisierung, handelt es sich um komplexe, zusammenhängende Informationssysteme, die alle Bereiche des Betriebs einer Stromversorgungsanlage abdecken. Die schnelle Entwicklung der Computer- und Kommunikationstechnologie hat auch die Schutz- und Automatisierungssysteme für elektrische Komponenten verändert. Darüber hinaus ergeben sich aus den neuen, in moderne Schutz- und Automatisierungssysteme integrierten Kontrollfunktionen ganz neue Best Practices für den Aufbau von Stromversorgungseinrichtungen.

Die Qualität dieser Kontrolle zu verbessern, ist eine der Hauptaufgaben bei der künftigen Entwicklung von Stromversorgungsanlagen und dem Weg hin zu intelligenten Stromnetzen. Kontrollsysteme spielen daher eine wichtige Rolle bei der Erzeugung, Übertragung und Verteilung von Elektrizität.

Moderne PACSs sind hoch integriert und nutzen digitale Kommunikationstechnologien, die auf offenen internationalen Standards, wie z. B. IEC 60870, IEC 61850 und IEC 61970, basieren. Die Integration separater Untersysteme hat die Leistungsfähigkeit der Schutz- und Kontrollsysteme deutlich erhöht und ermöglicht heute einen intelligenteren und effizienteren Einsatz der entsprechenden Systeme. Darüber hinaus haben gemeinsame Standards die Kosten der Integration stark reduziert und die Zuverlässigkeit der verfügbaren Funktionalität erhöht.

Ein modernes System zur Kontrolle und zum Schutz von Stromversorgungsanlagen beinhaltet verschiedene Arten von Informationsuntersystemen, wie z. B. die folgenden:

- Hardware- und Software-Appliances für automatisierte Übertragungssteuerung
- Automatisierte Steuerung der Betriebsmodi von Stromversorgungssystemen zwecks Wartung
- Schutzsysteme
- Automatische Notfallschutzsysteme
- Systeme zur Prozesssteuerung
- Automatisierte Systeme zur Strommessung
- Systeme zur Kontrolle der Stromqualität

Schwachstellen von PACSs in Stromversorgungsanlagen gegenüber IT-Bedrohungen

Das hohe Maß an Offenheit und Integration elektrischer Systeme hat in Kombination mit der Verbreitung von IT und Internettechnologien im alltäglichen Leben ganz neue Herausforderungen für den Energieversorgungssektor geschaffen. Bei modernen automatisierten Schutz- und Kontrollsystemen für Stromversorgungsanlagen handelt es sich um integrierte und verteilte Computersysteme, die über offene Protokolle miteinander kommunizieren. In solchen Systemen wird der Cybersicherheit nur wenig Bedeutung zugemessen, da elektrische Kontrollsysteme einmal als isolierte Lösungen konstruiert wurden. In modernen Kontrollsystemen, die global integriert und mit Unternehmensservices verbunden sind, ist das Risiko durch Cyberbedrohungen jedoch äußerst hoch.

Im Standard IEC 62351 zur Daten- und Kommunikationssicherheit beim Management von Stromanlagen und dem zugehörigen Informationsaustausch werden die folgenden Probleme der Informationssicherheit in Stromversorgungsanlagen und ihre Ursachen betont:

Offene Kommunikation

Offene und ungeschützte Kommunikationsverbindungen zwischen Komponenten der Schutz- und Kontrollsysteme sowie zwischen den verschiedenen Einrichtungen der Versorgungsinfrastruktur:

- **Fehlende Identitätsprüfung** Schwache oder nicht vorhandene Authentifizierung interagierender Agenten: So kann beispielsweise ein beliebiges Netzwerkgerät im technologischen Netzwerk fehlerhafte oder schädliche Steuerbefehle an ein übergeordnetes System senden, das wiederum einen Bediener in der Leitzentrale zum Ausführen falscher Aktionen veranlassen kann.
- **Offene Standards und offene Datenübertragung** Die für die Datenübertragung eingesetzten Protokolle basieren auf offenen und gut dokumentierten Standards. Die Protokolle, ihr Quellcode, die erforderlichen Werkzeuge für Analyse und Emulation – all das ist kostenlos öffentlich zugänglich. Aus diesem Grund lassen sich in solchen Netzwerken übertragene Daten leicht abfangen, lesen, modifizieren und replizieren, wodurch Cyberkriminellen der Zugang zu den entsprechenden Daten und somit auch die Durchführung kompromittierender Aktionen erleichtert wird.
- **Umfangreiche Netzwerkkommunikation** Die umfangreiche Kommunikation zwischen IEC 60807-5-10x- und IEC 61850 MMS-Protokollen ist normal für ihren Betrieb. Diese offene Kommunikation erleichtert jedoch auch einfache DoS-Angriffe auf technologische Infrastrukturgeräte (z. B. Prozesssteuerungssysteme in der Leitzentrale oder Schutzterminals) über das massenweise Versenden ungültiger Datenpakete.
- **Verbindungen zu öffentlichen Netzwerken** Die Unternehmens- und technologischen Netzwerke moderner industrieller Einrichtungen verfügen häufig über verschiedene Verbindungen zu nahezu jeder Hierarchiestufe des Kontrollsystems. Hieraus ergibt sich ein erhöhtes Risiko des nicht autorisierten Zugriffs auf technische Geräte.

Fehlendes Bewusstsein für Cybersicherheit bei den Mitarbeitern

Im Normalfall kümmern sich wenige technische Mitarbeiter um viele technische Geräte, die zusätzlich oft räumlich verteilt sind und ohne dauerhafte Überwachung auskommen müssen. Den Mitarbeitern vor Ort fehlt es oft selbst an den Grundlagen der Cybersicherheit:

- **Vergabe von Berechtigungen beim Remote-Zugriff aus nicht vertrauenswürdigen Netzwerken** Zur einfachen Wartung und aus Bequemlichkeit gewähren technische Mitarbeiter den Remote-Zugriff auf Geräte innerhalb der Einrichtung oft mit sämtlichen Berechtigungen. Ein solcher Zugriff wird oft inoffiziell und auch unsicher organisiert, beispielsweise von Unternehmens-Workstations mit Internetzugriff aus.
- **Fehlender Passwortschutz und fehlende Richtlinien zur Benutzerkontrolle** Eine große Anzahl von Geräten wird von einer kleinen Anzahl von Mitarbeitern gepflegt – ein weitverbreitetes Konzept, durch das sich die Organisation und Pflege von Richtlinien für den Gerätezugriff, einschließlich Passwortschutz und Richtlinien zur Benutzerkontrolle, schwierig gestalten. Dementsprechend werden technische Geräte häufig mit Standardpasswörtern betrieben, wodurch der unberechtigte Zugriff erleichtert wird.
- **Veraltete Software** IED-Software wird während ihrer Lebensdauer in technischen Einrichtungen nahezu nie aktualisiert. Bekannte Softwarefehler werden nicht beseitigt, sofern sie sich nicht direkt negativ auf technische Prozesse auswirken.
- **Wartung von unsicheren Workstations aus** Tragbare Workstations (Laptops), die im Rahmen der Wartung der technologischen Infrastruktur eingesetzt werden, werden häufig auch als gewöhnliche Unternehmenscomputer, für Softwaretests oder für persönliche Zwecke genutzt.
- **Fehlende regelmäßige Konfigurations- und Softwarekontrolle** Überprüfungen der Gerätekonfigurationen sowie der Software werden häufig nur manuell und unregelmäßig durchgeführt – in vielen Fällen nur einmal jährlich.

Sicherheitsbestimmungen werden nicht eingehalten

Die Anforderungen der Informationssicherheit werden beim Geräte- und Softwaredesign und bei der Entwicklung technologischer Infrastrukturen nur selten berücksichtigt.

- **Fehlender Schutz vor Hacking** Entwickler berücksichtigen für gewöhnlich nicht die Schwachstellen in ihrem Code, die für gezielte Angriffe oder nicht gestattete Aktionen in technologischen Infrastrukturen und ihren Elementen eingesetzt werden können. Das bedeutet, dass zumeist nur ein sehr schwacher Schutz vor einem Hacker-Angriff besteht.

- **Ungültige oder nicht ausreichende Einstellungen für die Netzwerksicherheit** Ungültige Einstellungen der Netzwerksegmentierung und der Zugriffskontrolle zwischen Segmenten im technologischen Netzwerk sowie fehlende Netzwerkdesignlösungen in PACS-Implementierungsprojekten stellen ein häufiges Problem dar. Aus diesem Grund hängt die Qualität der Netzwerkinfrastruktur für gewöhnlich von den Fähigkeiten und Qualifikationen des Einrichtungsteams ab.
- **Fehlende Datensicherheit bei Übertragung über offene Kanäle** Bei der Datenübertragung über offene Kommunikationsverbindungen sind sichere Übertragungsmittel Mangelware.
- **Fehlende rollenbasierte Zugriffskontrolle** Ohne rollenbasierte Zugriffskontrolle kann es beim Gerätezugriff zur Vergabe fehlerhafter Berechtigungen kommen, mit denen Benutzer auf Bereiche zugreifen können, die über ihre Verantwortlichkeiten hinaus gehen.
- **Fehlende Lösungen zur Application Startup Control** Da es oft an kompatiblen Lösungen zum Schutz von Computersystemen vor nicht autorisierten Programmstarts mangelt, haben die Systeme der Ausführung nicht autorisierter Software in industriellen Systemen nichts entgegenzusetzen. Allgemeine Hilfsmittel für die Kontrolle von Programmstarts sind oft mit industriellen Systemen inkompatibel oder nicht effektiv (Inkompatibilität mit technologischer Software, unzureichende Ressourcen auf bestimmten technischen Systemen usw.).
- **Fehlende oder unzureichende Erkennung von Sicherheitsereignissen** Innerhalb von Prozesssteuerungssystemen stehen keine spezifischen Hilfsmittel zur Erkennung von Überwachungs- und Cybersicherheitsereignissen zur Verfügung, oder aber ihre Funktionalität ist nicht ausreichend, um entsprechende Situationen korrekt interpretieren zu können.

Komplexität der Zugriffskontrolle für Partner

Der Einsatz von Partnerunternehmen für bestimmte Arten von Wartungsarbeiten ist nichts Ungewöhnliches. Entsprechend ist es äußerst wichtig, solchen Partnern nur temporären Zugriff auf eingeschränkte Geräte zu gewähren, die keinen Einfluss auf andere Systemkomponenten haben. Auch die Entziehung des Zugriffs nach Abschluss der Arbeit ist essentiell.

Lange Lebensdauer anfälliger Komponenten

Die Lebensdauer entsprechender Geräte sowie von Schutz- und Kontrollsystemen beträgt 20 bis 30 Jahre. Unsichere Systeme bleiben also einige Jahrzehnte lang aktiv, bevor sie ersetzt werden. Oft werden auch teilweise Upgrades nicht durchgeführt, weil die Kompatibilität zu neueren und sichereren Lösungen nicht gegeben ist.

Zusätzlich zu den oben aufgeführten technischen Problemen stehen Betreiber auch vor organisatorischen Problemen. Zunächst einmal fehlt es häufig an Handbüchern, in denen geeignete Aktionen im Falle verdächtiger Aktivitäten in automatisierten Systemen definiert sind. Darüber hinaus sind auch Dokumente und Best Practices bezüglich der Untersuchung von Störungen in technischen Umgebungen, einschließlich schädlicher Auswirkungen auf Kontrollsysteme durch Informationstechnologien, oft Mangelware. Beispielsweise führen einige Referenzdokumente für die Untersuchung und Einstufung technischer Störungen aufgrund ihres Alters Cybersicherheitsvorfälle gar nicht als mögliche Fehlerquelle auf. Wenn ein solcher Vorfall eintritt, bleiben die wahren Ursachen verborgen. Entsprechend werden nicht die richtigen Gegenmaßnahmen getroffen, und der Vorfall tritt möglicherweise erneut auf.

An den oben aufgeführten Punkten lässt sich erkennen, dass einige offensichtliche systematische Probleme bestehen:

- Moderne Schutz- und Kontrollsysteme für Stromversorgungsanlagen sind keine isolierten geschlossenen Systeme mehr.
- Schutz-, Automatisierungs- und Kontrollsysteme verfügen nicht über ausreichende integrierte Cybersicherheitsfunktionen.
- Aus organisatorischer und technischer Sicht ist die Erkennung negativer Auswirkungen unter den aktuellen Bedingungen äußerst schwierig.
- Es mangelt an klaren Anweisungen für den Fall, dass ein Angriff erkannt wird.

Technische Lösungen zur Erkennung und Abwehr von Cyberbedrohungen

Im Standard IEC 62351 zur Daten- und Kommunikationssicherheit beim Management von Stromanlagen und dem zugehörigen Informationsaustausch werden die möglichen Werkzeuge für die Bereitstellung von Informationssicherheit in komplexen Stromversorgungsanlagen im Detail beschrieben. Bei den meisten vorgeschlagenen Lösungen müssen die Automatisierungsgeräte vollständig ausgetauscht werden, wenn diese einmal Prozeduränderungen bezüglich Format und Kommunikationsprotokoll erfordern.

Auch wenn es scheint, als läge eine globale Implementierung von IEC 62351 noch in ferner Zukunft, so lassen sich doch Teile der entsprechenden Anforderungen bereits jetzt umsetzen und auf moderne Systeme anwenden.

Kaspersky Industrial CyberSecurity (KICS) ist eine ganzheitliche Lösung für industrielle Infrastrukturen, die genau diese Anforderungen erfüllt.

Die Lösung besteht aus zwei Komponenten:

- KICS for Nodes, eine Komponente für den Schutz von Endpoints in industriellen Netzwerken (wie z. B. Engineering-Stations, Betreiberterminals, SCADA-Server)
- KICS for Networks, eine Komponente für die Überwachung industrieller Netzwerke, einschließlich Integritätsprüfung und tief gehenden Funktionen zur Untersuchung von Programmprotokollen (IEC 60870-5-104, IEC 61850 usw. für Stromversorgungsinfrastrukturen)

KICS for Nodes

Bei KICS for Nodes handelt es sich um ein spezielles Produkt für industrielle Systeme. Die Computersoftware wurde dazu entwickelt, Workstations in technischen Infrastrukturen – Server, Engineering-Workstations und Betreiberterminals unter Windows – vor Bedrohungen der Informationssicherheit zu schützen.

Im Folgenden finden Sie die wichtigsten Funktionen der Lösung:

- Whitelisting (Application Startup Control): Blockiert den Start aller Programme, die nicht ausdrücklich gestattet sind. Die Schutzkomponente bietet einen Testmodus, um die Einrichtung und Fehlerbehebung in der Deployment-Phase zu vereinfachen.
- Gerätekontrolle: Hierüber können Administratoren festlegen, welche Geräte mit geschützten industriellen Hosts verbunden werden können. Die Technologie bietet Möglichkeiten, industrielle Systeme vor nicht autorisierten Geräteverbindungen zu schützen, und unterstützt Masken für die einfache Administration und die Bedienung einer großen Anzahl von Geräten.

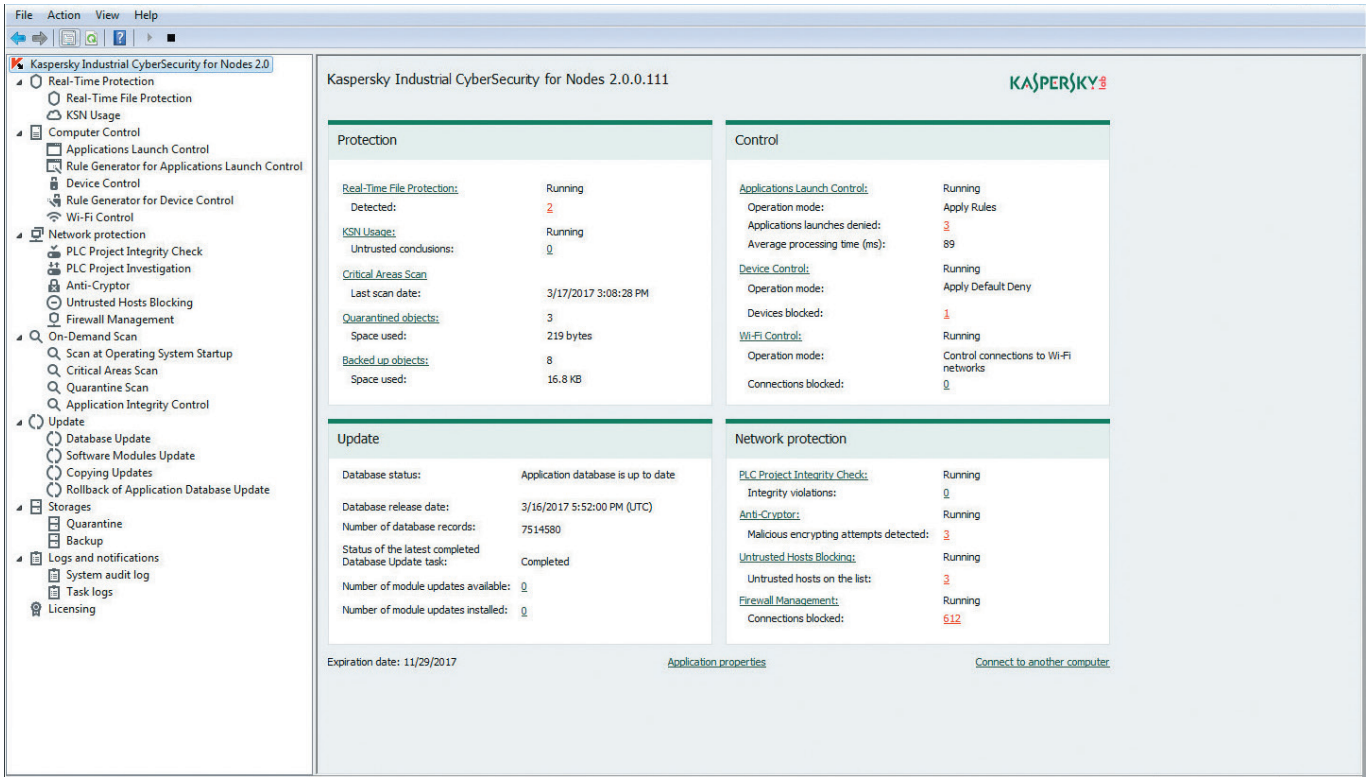

Abbildung 1: Lokale Benutzeroberfläche von KICS for Nodes

- Erkennung schädlicher Software (einschließlich Viren): Kombiniert heuristische und Signaturmethoden, um Windows-Workstations vor bekannten, unbekannten und komplexen Bedrohungen zu schützen.
- Netzwerk-Firewall: Bietet Funktionen zur Beschränkung der Netzwerkverbindungen zu industriellen Hosts. Network Attack Blocker: Ermöglicht die Überwachung und Blockierung verdächtiger Aktivitäten auf industriellen Hosts.

KICS for Nodes kann nach der Integration in ein auf dem Kaspersky Security Center basierendes Sicherheitsinfrastruktur-Kontrollsystem zentral verwaltet werden. Dadurch ergeben sich folgende Möglichkeiten:

- Zentrale Verwaltung und Kontrolle von Sicherheitsrichtlinien: So können Sie zentral Sicherheitseinstellungen für industrielle Geräte und Gruppen festlegen.
- Zentrale Updates der Viren-Datenbanken auf geschützten Netzwerk-Nodes (selbst, wenn das Netzwerk nicht mit dem Internet verbunden ist): Ermöglicht die Aktualisierung der Sicherheitsagenten über einen einzelnen Kontrollserver innerhalb des Netzwerks. Updates können über einen speziellen Server direkt aus dem Internet auf den Kontrollserver (im IT-Netzwerk oder der DMZ) heruntergeladen oder von einem Administrator per USB-Gerät auf den Kontrollserver übertragen werden.
- Tests neuer Updates vor der Verteilung: Ermöglicht die Überprüfung der Kompatibilität neuer Updates mit der vorhandenen industriellen Software, bevor sie auf den industriellen Hosts installiert werden.
- Rollenbasiertes Modell für separate Richtlinienverwaltung und Aktionen mit dem Sicherheitsagenten: Beseitigt die Möglichkeit nicht autorisierter Änderungen der Sicherheitsrichtlinien auf dem Kontrollserver und verhindert die Deaktivierung der Schutzmechanismen sowie Änderungen an den Einstellungen der Endpoint-Lösungen.
- Zentrale Erfassung von Daten zu Sicherheitsereignissen auf den einzelnen Endpoints: Ermöglicht die umfassende Analyse von Daten zur Informationssicherheit basierend auf registrierten Ereignissen, erkennt die genaue Ursache von Vorfällen und vereinfacht die Planung der Ursachenbehebung.

Bei der Entwicklung von KICS for Nodes haben wir verschiedene Ansätze verfolgt, um eine Lösung zu schaffen, die sich in ihrer Standardkonfiguration nicht auf technologische Prozesse auswirkt.

KICS for Networks

Bei KICS for Networks handelt es sich um eine spezielle Softwarelösung für die Überwachung industrieller Netzwerke. Die Lösung kann Anormalitäten erkennen und wichtige Informationsereignisse im Datenverkehr des industriellen Netzwerks erfassen, ohne technologische Prozesse negativ zu beeinflussen.

Im Folgenden finden Sie die wichtigsten Funktionen der Lösung:

1. Überwachung der Netzwerkintegrität:
- Ein lernfähiger Modus ermöglicht die Erkennung und Registrierung aller verfügbaren LAN-Nodes sowie der Kommunikation zwischen den Nodes. Diese Daten können als Referenz sowie zur Änderungsverfolgung verwendet werden.
- IP- und MAC-Adressen-basierte Erkennung und Registrierung neuer Netzwerkgeräte, die mit den kontrollierten Segmenten des technologischen Netzwerks verbunden werden.
- Erkennung und Registrierung neuer Netzwerkkommunikation zwischen Nodes basierend auf den folgenden Attributen: Adresse des Sender-Nodes, Adresse des Empfänger-Nodes, Netzwerkprotokoll, Port, Anzahl zulässiger Verbindungen usw.

2. Deep Packet Inspection:
- Überprüfung, Analyse und Registrierung wichtiger Nachrichten technologischer Protokolle gemäß der Konfiguration:
  - Erkennung von Befehlen zur Geräteverwaltung (z. B. Ein-/Ausschalten) über industrielle Netzwerkprotokolle (IEC 61850, IEC 60870-5-104).
  - Erkennung von Befehlen zur Änderung der Betriebsparameter des Schutz- und Kontrollsystems (z. B. Änderungen der Abschaltpunkte ganzer Gerätegruppen) über industrielle Netzwerkprotokolle (IEC 61850, IEC 60870-5-104).
  - Erkennung von Versuchen im kontrollierten Netzwerksegment, über Servicesoftware IEDs zu kontrollieren oder deren Parameter zu ändern.
- Allgemeine Fernüberwachung von Nachrichten.

3. Ereignisspeicherung:
- KICS for Networks ermöglicht die Speicherung erkannter Ereignisse in einer internen sicheren Datenbank.
- Die Speicherung hängt hierbei von der festgelegten Speicherdauer sowie der Archivgesamtgröße ab. Ein Beispiel der Lösung (siehe Abb. 3) veranschaulicht ein mögliches Deployment-Szenario für KICS for Networks und KICS for Nodes.

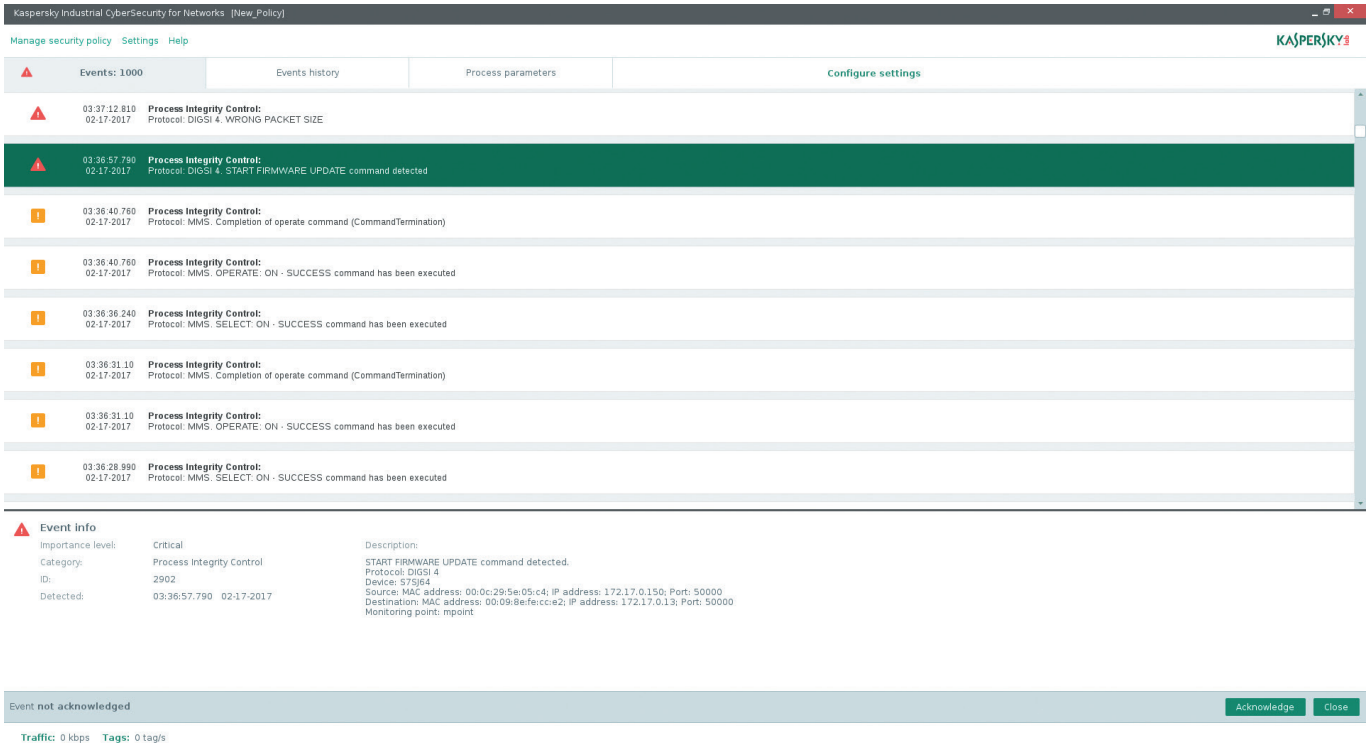

Abbildung 2: Lokale Benutzeroberfläche von KICS for Networks

KICS for Nodes und KICS for Networks: Beispiel eines Deployments in einer modernen elektrischen Schaltanlage

Ein sicheres Schutz- und Kontrollsystem umfasst zwei LAN-Segmente mit Ringtopologie. Das erste Segment der Schaltanlage ist der Stationsbus (gemäß IEC 61850), der die Kommunikation zwischen den IEDs ermöglicht. Darüber hinaus werden Schaltanlagen-Bus, -Controller und Fernüberwachungs-Gateways für den Informationsaustausch mit höheren Ebenen der Leittechnik verwendet. Das LAN-Segment bietet über Engineering-Software Zugriff auf Geräte des Schutz- und Kontrollsystems. Der Servicezugriff kann sowohl lokal als auch remote bereitgestellt werden. Der lokale Servicezugriff wird über einen direkt mit den IEDs oder dem Stationsbus-LAN verbundenen Laptop ermöglicht. Alternativ kann auch über eine Remote-Workstation auf den Service zugegriffen werden. Die direkte Kommunikation zwischen den Netzwerk-Nodes während des normalen Betriebs erfolgt gemäß IEC 61850 MMS. Servicekommunikation bezüglich der Geräteparameter des Schutz- und Kontrollsystems erfolgt im Rahmen der internen Programmprotokolle des entsprechenden Geräteherstellers.

Das physische LAN-Segment des Busses stellt ein Ringnetzwerk dar, das zwei miteinander verbundene Switches umfasst. Alle Geräte sind als DANs (Double Attached Nodes) mit den Switches verbunden. Aus diesem Grund gibt es keinen SPOF (Single Point of Failure) in diesem Segment, wodurch ein höheres Maß an Netzwerkzuverlässigkeit erzielt wird. Die IEDs sind mit integrierten Switches ausgestattet und per Linientopologie miteinander verbunden. Nur die Enden dieser Linien sind mit den Switches des Ringnetzwerks verbunden, sodass der Datenverkehr zwischen den einzelnen Geräten einer Kette nicht über die Switches des Ringnetzwerks übertragen werden. Die Steuerung des Ringnetzwerks erfolgt über das RSTP (Rapid Spanning Tree Protocol). Es ist ein Netzwerk-Switch integriert, der per VPN Remote-Servicezugriff auf das industrielle Netzwerk ermöglicht.

Auch das zweite Segment, das Betreibernetzwerksegment, weist eine Ringtopologie auf, um die Interaktion zwischen Betreiber-Workstations und Servern des Prozesssteuerungssystems zu ermöglichen.

Die Interaktion mit der Netzleitstelle und dem Systembetreiber wird direkt über einen mit dem Automatisierungssystem verbundenen Unterstations-Controller bereitgestellt (siehe Abb. 3). Der Datenaustausch erfolgt über das Protokoll IEC 60870-5-104.

KICS for Networks muss in jedem der ausgewählten Netzwerksegmente installiert werden, um eine vollständige Überwachung der Infrastruktur des technologischen Netzwerks zu ermöglichen. Dementsprechend müssen für das vorliegende Schema drei KICS for Networks-Server installiert werden: einer für das Stationsbus-Segment, einer für das Betreibernetzwerksegment und einer für die Kommunikationsverbindung zu höheren Kontrollebenen. Um KICS for Networks-Server mit der Infrastruktur zu verbinden, ist eine Neukonfiguration der Switch-Geräte erforderlich, um sämtlichen SPAN-Datenverkehr eines jeden Netzwerksegments an den entsprechenden Server weiterzuleiten.

Der KICS for Networks-Server ist mit den SPAN-Ports der Netzwerk-Switches verbunden. Diese Konfiguration ermöglicht es, ausschließlich industriellen Datenverkehr zu empfangen, ohne technologische Prozesse zu beeinflussen. KICS for Networks verarbeitet industriellen Datenverkehr und erkennt verdächtige Ereignisse. Die Daten zu den registrierten Ereignissen werden verschlüsselt und sicher gespeichert. Darüber hinaus werden die Ereignisse über einen verschlüsselten Kanal an das Kaspersky Security Center übermittelt, wo Sicherheitsspezialisten eine endgültige Liste erkannter Ereignisse erhalten.

Die KICS for Nodes-Software muss auf jedem einzelnen industriellen Host installiert werden, um die Windows-Computerinfrastruktur zu schützen. KICS for Nodes sendet darüber hinaus erkannte Ereignisse an den KSC-Server (Kaspersky Security Center). Die industriellen Hosts müssen über eine zusätzliche Netzwerkschnittstelle für die Verbindung mit dem Kontrollnetzwerksegment verfügen.

Sämtliche Kommunikation des Kontrollnetzwerks wird verschlüsselt. Im Falle eines Ausfalls des Kontrollnetzwerks führen die Komponenten KICS for Networks und KICS for Nodes ihren Betrieb im eigenständigen Modus fort. Erfasste Daten werden an das Kaspersky Security Center übertragen, wenn das Netzwerksegment wieder verfügbar ist.

KICS unterstützt die Integration in SIEM-Systeme. Das Kaspersky Security Center organisiert einen verschlüsselten Kanal zu dem SIEM-System und übermittelt konfigurierte Ereignisse im Syslog-Format an entsprechende SIEM-Lösungen (HP ArcSite, IBM QRadar und andere). Benachrichtigungen können per E-Mail oder per SMS versendet werden.

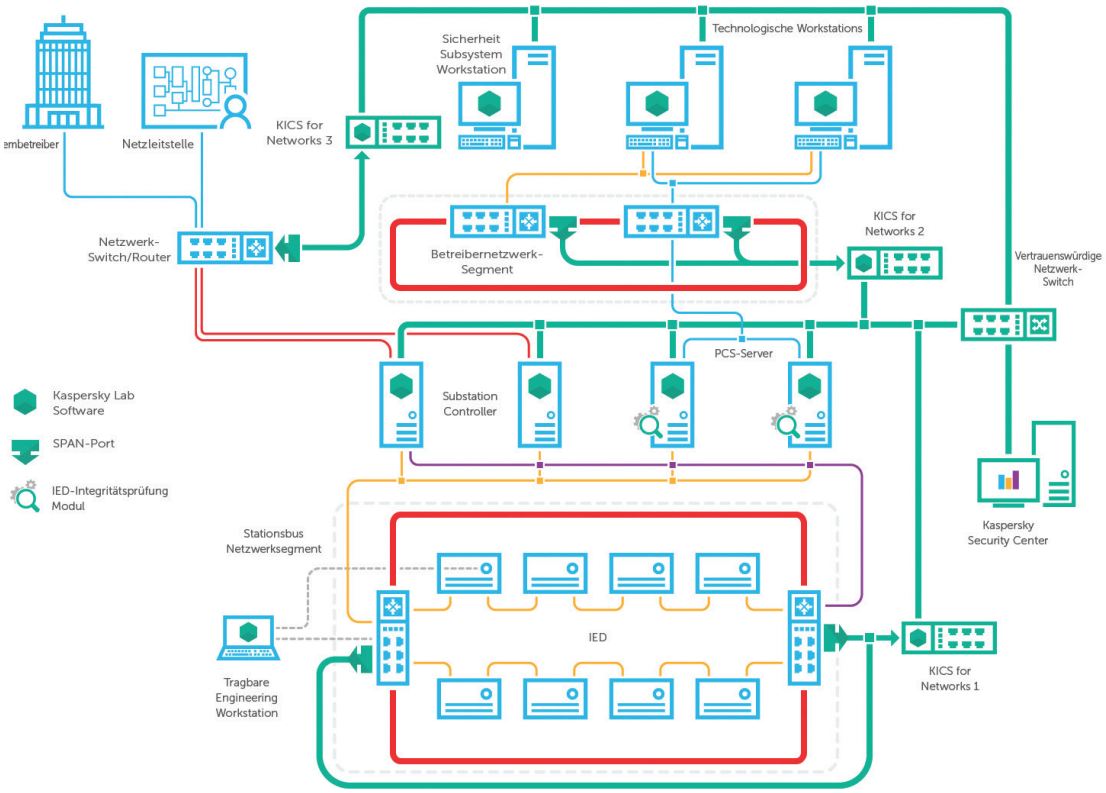

Abbildung 3: Deployment der KICS-Komponenten (Kaspersky Industrial CyberSecurity)

Begriffe und Definitionen

CD (Computing Device)**:** ein technisches Gerät, das gemäß vordefinierten Programmlogiken Daten verarbeiten kann.

CSPS (CyberSecurity Protection System): ein automatisiertes System, das die Cybersicherheit der geschützten Einrichtung gewährleisten soll.

IED (Intelligent Electronic Device): ein spezielles mikroprozessorbasiertes Mehrzweck-Computergerät mit umfassenden digitalen Kommunikationsfunktionen.

ICS (Industrial CyberSecurity): eine Lösung zum Schutz industrieller Anlagen, die Verfügbarkeit, Integrität und Vertraulichkeit technischer Prozesse auf IT-/OT-Ebene bietet.

LAN (Local Area Network): ein Computernetzwerk, das eine feste Anzahl von Netzwerkeinheiten enthält, die über logisch verwaltete Medien miteinander verbunden sind und nach dem Prinzip eines abgegrenzten Bereichs funktionieren.

PACS (Protection, Automation and Control System): ein zusammenfassender Begriff, der für den gesamten Bereich am Standort installierter automatischer und automatisierter Kontrollsysteme für verschiedene Zwecke steht.

PCS (Protection Control System): ein Mensch-Maschine-System, das auf industrieller Automatisierung und Telekommunikationseinrichtungen basiert, am Standort die umfassende automatische und automatisierte Prozesssteuerung der entsprechenden Einrichtung ermöglicht und sich per Fernzugriff von einem externen Standort aus kontrollieren lässt.

Schutzsystem: eine Kombination von IEDs, die dafür verantwortlich ist, beschädigte Segmente kontrollierter Stromversorgungssysteme umgehend zu erkennen und die Verbindung zu ihnen zu trennen, um eine stabile Systemleistung zu gewährleisten.

SCL (Substation Configuration Language): Sprache und Darstellungsformat gemäß IEC 61850-6 für die Konfiguration elektrischer Schaltanlagen. Die XML-basierte Sprache enthält Ressourcen für die Darstellung eines Geräteinformationsmodells, von Datensätzen und Kommunikationsservices. Basierend auf XML-Sprache.

Intelligentes Stromnetz: eine neue Generation von Stromversorgungssystemen, die bei Organisation und Kontrolle über Betrieb und Entwicklung einen Ansatz mit mehreren Agenten verfolgt, um alle Ressourcen (natürliche, soziale und Produktionsressourcen sowie Mitarbeiter) effektiv zu nutzen. Diese Systeme bieten Verbrauchern dank der flexiblen Interaktion mit allen enthaltenen Einheiten (alle Arten von Stromerzeugung, -netzwerken und -verbrauchern) eine sichere, hochwertige und effiziente Stromversorgung, die auf modernen Technologien und einer einheitlichen intelligenten Steuerhierarchie basiert.

SPAN (Switched Port Analyzer): ein Netzwerk-Switch-Port, der dafür verwendet wird, den gespiegelten Netzwerkdatenverkehr von ausgewählten Ports des verwalteten Switches zwecks Analyse zu erfassen.

Stationsbus: schnelles und äußerst zuverlässiges Computernetzwerk, das die Datenübertragung über intelligente Geräte ermöglicht, die Prozessfunktionen implementieren (Zellenebene), sowie über Geräte-, Hardware- und Softwarekomplexe, die allgemeine Schaltfunktionen (Schaltanlagenebene), wie z. B. SCADA, Telemecanique-Gateways usw., implementieren. In einigen Fällen ermöglicht ein Stationsbus die horizontale Kommunikation zwischen den Geräten auf Zellenebene. Um elektromagnetische Kommunikationsstörungen zu vermeiden, wird bei Stationsbussen oft auf optische Glasfasermedien zur Datenübertragung zurückgegriffen.

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