IKARUS security software

Whitepaper

Mehr Cybersicherheit für die Energieversorgung

Monitoring, Visibilität, interaktive Visualisierung und Bedrohungserkennung in Echtzeit für Digital Substations

NOZOMI NETWORKS

powered by IKARUS

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Inhalt

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Executive Summary

Ob Effizienzsteigerung, Umweltbedingungen oder Kundenanforderungen – der Bedarf an Vernetzung und Digitalisierung in der Energieversorgung steigt stetig. Hand in Hand damit erhöhen sich die Herausforderungen zur Cybersicherheit.

Die Energieversorgung ist eines der attraktivsten Angriffsziele von Hackergruppen und staatlichen Akteuren. Bedrohungen, die auf die Energieversorgung abzielen, stellen zentrale Risiken für eine funktionierende Gesellschaft, die wirtschaftliche Stabilität und die Geschäftsfähigkeit dar. Das Weltwirtschaftsforum listet Cyberangriffe auf kritische Infrastrukturen als eines der fünf größten globalen Risiken.[1]

Mehr Cybersicherheit in der immer komplexer werdenden Automatisierung und Prozessteuerung stärkt die Abwehrkräfte und verbessert die Resilienz gegenüber Störfällen und Angriffen.

Grundlegende Best Practice ist es, Transparenz über Betriebsprozesse, Kommunikationsbeziehungen, Verwundbarkeiten und Anomalien der automatisierten Systeme zu schaffen. Der Überblick über die aktuelle Lage der Cybersicherheit und mögliche Cyberrisiken ermöglicht es, die richtigen Maßnahmen zu setzen. Entscheidend ist der Einsatz von Netzwerk Monitoring Technologie, die in Echtzeit die heterogenen und hochverfügbaren Netzwerke der Automatisierung und Prozessteuerung analysiert, überwacht und Maßnahmen für Verbesserung einleitet.

In einer eskalierenden Bedrohungslage und innerhalb staatlicher Cybersicherheitsrichtlinien sind Lösungen, die das Risiko reduzieren und zugleich die operative Leistungsfähigkeit und Zuverlässigkeit stärken, wesentlich. Dieses Paper beschreibt technische Herausforderungen in Digital Substations und wie mit Netzwerk-Monitoring und Bedrohungserkennung in Echtzeit die Verfügbarkeit des Betriebs verbessert und das angestrebte Schutzniveau für die Cybersicherheit erreicht werden kann.

[1] Vgl. “The Global Risks Report 2019”: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Referenzarchitektur für Digital Substations

Viele Energieversorgungsunternehmen haben Hunderte von digitalen Unterstationen (Digital Substations) wie z.B. Umspannwerke, die entscheidend für die Effizienz und Anpassungsfähigkeit des intelligenten Energienetzes sind. Sie leiten den Strom mit der Infrastruktur, die dem Endverbraucher am nächsten ist, aus dem Übertragungsnetz in das Verteilungsnetz. Smart Grids senden Informationen über Verbrauch und Betrieb zur Analyse durch Energiemanagement- und Automatisierungssysteme zurück. Dies erfordert eine erweiterte Kommunikation der beteiligten Systeme im Smart Grid – etwas, das in der Vergangenheit normalerweise nicht möglich bzw. notwendig war.

So werden die Kommunikationsnetzwerke von der Substation umgerüstet, um die Konnektivität mit mehreren Systemen zu ermöglichen. Die bevorzugten Netzwerktechnologien basieren auf Ethernet und TCP/IP und entsprechen den Standards der IEC 61850. Diese internationale Normenfamilie definiert die Architektur der Digital Substations und hat den Vorteil, dass Geräte verschiedener Hersteller nahtlos kommunizieren und zusammenarbeiten können. Sie deckt Bereiche wie Modellierung, Konfiguration und Low-Level Kommunikationsprotokolle ab. Primär wird IEC 61850-8-1 (GOOSE und MMS) und sekundär werden IEC 61850-9-Protokolle oder SV (Sampled Values) verwendet.

Die meisten Digital Substations arbeiten mit verschiedenen Geräten, wovon einige IEC 61850-Kommunikation, aber auch Übertragungsprotolle nach IEC 60870-5-101 (seriell) bzw. IEC 60870-5-104 (Netzwerk basierend) nutzen.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Technische Herausforderungen für mehr Cybersicherheit

1. Implementierung der Cyber Security Appliance Guardian

Abbildung 1 zeigt die Systemarchitektur eines beispielhaften Stationsautomatisierungssystems in einer digitalen Substation sowie den typischen Einsatz von Guardian Appliances zur schnellen Asset Discovery, Netzwerkvisualisierung und Cybersicherheit Bedrohungs- und Anomalie-Erkennung, die auf verschiedenen Ebenen des Systems implementiert ist.

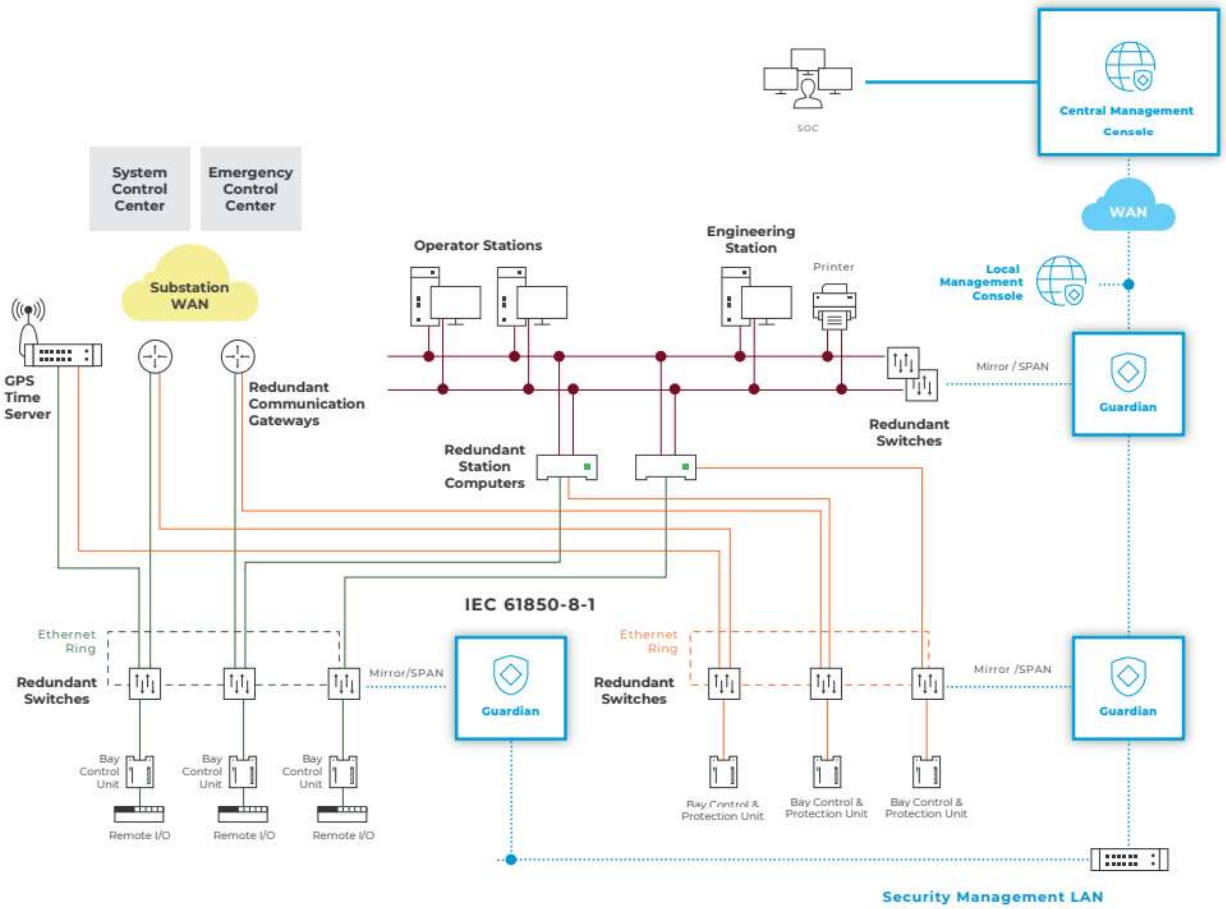

Abbildung 1 - Beispiel einer digitalen Substation-Architektur mit Einsatz Cybersicherheits-Appliances Guardian zur Erkennung und Überwachung von Bedrohungen des Stationsautomatisierungssystems und Steuerungsnetzwerks.[2]

[2] Nozomi Networks (2019): Improving ICS Cyber Security for Substations and Power Grids.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Die Stationsebene umfasst Betriebs- und Engineering-Stationen, die mit einem redundanten LAN verbunden sind, das von zwei dedizierten Switches gesteuert wird. Zwei Stationsrechner in einer HA-Konfiguration (High Availability) fungieren als IEC 61850-Kommunikationsgateways zwischen der Stations- und der Feldebene.

Der untere Teil der Abbildung zeigt zwei redundante IEC 61850-8-1-basierte Netzwerke für die Steuereinheiten sowie die Steuer- und Schutzeinheiten. Diese kritischen Netzwerke benötigen hohen Durchsatzgeschwindigkeiten und redundante dedizierte Geräte, um die Betriebs-anforderungen der Digital Substations zu erfüllen. Kommunikation, die das GOOSE-Protokoll verwendet und die für den Schutz der Funktion von Digitalen Substations wichtig ist, muss in weniger als vier Millisekunden übertragen werden. Ebenso erfordern Vektoren zur Regelung der Spannung der Übertragungssysteme hohe Bandbreiten. Der IEC 61850-Bus, der auf Ethernet-Technologien basiert und hauptsächlich über Glasfaser läuft, ist entscheidend für den Betrieb der Digital Substations und hat analoge Leitungen ersetzt. Seine Leistung ist der Schlüssel zur Sicherstellung einer hohen digitalen Funktionalität und Verfügbarkeit.

Die Kommunikation zwischen Unterstation und Leitstelle erfolgt über dedizierte Gateways und Modems, welche die Daten über dedizierte WANs (Wide Area Networks) verschiedenen Übertragungsprotokollen zuordnen. Die WANs nutzen Mietleitungen, MPLS, leitungsgebundene Kommunikation, Satellit, Mikrowellenfunk oder Mobilfunk. Die Protokolle variieren abhängig von der Unterstation und der Kommunikationsarchitektur – verwendet werden z.B. IEC 60870-5-101, IEC 60870-5-104, DNP3, IEC 61850-80-1.

Auf der Feldebene sind zwei robuste Guardians auf DIN-Halterungsschienen montiert, während im Stations-LAN ein Rack-montierter Guardian läuft.

- Durch den passiven Ansatz ist die Installation nicht invasiv und läuft ohne Ausfallzeiten oder Netzwerkunterbrechungen.
- Für den Einsatz ist lediglich die Konfiguration des gespiegelten Netzwerksverkehrs mittels Mirroring-Ports auf Netzwerk Switches oder Einsatz von Netzwerk-TAPs notwendig.
- Die Guardians sollten mit den lokalen oder zentralen Management-Konsolen vollständig getrennt von der Produktionsumgebung über ein dediziertes Management-LAN kommunizieren. So ist sichergestellt, dass die Übertragung der IEC 61850-Kommunikation in keiner Weise gestört wird.

In diesem Szenario wird eine hierarchische Managementkonsolen-Architektur verwendet. Eine lokale Management-Konsole (LMC) aggregiert die Daten und Alarme der passiven Überwachungsgeräte in einer Digital Substation. Diese Informationen werden über ein TCP/IP-WAN an das CMC weitergeleitet, das sich im Security Operation Center (SOC) befindet. Das CMC kann Informationen von mehreren, geografisch verteilten LMCs oder Appliances empfangen und aggregieren. Das CMC sollte über die Flexibilität verfügen, auf mehreren Ebenen in der Architektur zu arbeiten.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Bei Bedarf sollten die vom CMC gesammelten Alarme an ein SIEM (Security Information and Event Management) weitergeleitet und mit anderen IT-Ereignissen aus der Unternehmensinfrastruktur korreliert werden. Idealerweise integriert sich die Lösung auch in gängige Benutzerauthentifizierungssysteme und damit in die End-to-End-IT-Systeme des Unternehmens.

Moderne digitale Substations wie in diesem Beispiel müssen Interoperabilität unterstützen, eine hohe Zuverlässigkeit und Verfügbarkeit bieten und zunehmenden Anforderungen hinsichtlich Cybersicherheit gerecht werden.

Die Guardians lösen durch die automatische Identifizierung der Anlagen einen wichtigen Teil der Sicherheitsprobleme mit Überwachungssteuerung und Datenerfassung (SCADA) und bieten umfassende Echtzeit-Cybersicherheit und Sichtbarkeit von Automatisierungs- und Steuerungsnetzwerken. Sie müssen bei der Überwachung von Hunderten Digital Substations und Anlagen in Netzwerken mit geringer Bandbreite optimale Leistung bringen.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

2. Skalierbarkeit

Die Herausforderung

- Die Lösung muss bei Hunderten von Digital Substations einsatzfähig sein, von denen wiederum jede viele Anlagen hat.
- Die Bestandsüberwachung einschließlich ihres Echtzeitstatus erfordert eine Lösung, die mit hervorragender Leistung sehr große Volumina verarbeiten kann.

Die Lösung

- Die Cybersicherheits-Sensoren Guardian sollten darauf ausgerichtet sein, große digitale Substation-Implementierungen hinsichtlich Einrichtung, Konfiguration und Wartung einfach zu verwalten. Ein vereinfachter, standardisierter Einrichtungsprozess sollte verwendet werden, um jede Umgebung automatisch mit einer gemeinsamen – möglicherweise benutzerdefinierten – Konfiguration zu versorgen.
- Die Implementierung sollte eine hierarchische Architektur mit Überwachungsgeräten in den Digital Substations haben, die mit den darüber liegenden Ebenen des CMC kommunizieren. Die Gruppierung von Digital Substations und Guardians vereinfacht die Systemverwaltung und ermöglicht den Betreibern einen einfachen Überblick über die Unterstationen sowie die globale Ebene.
- Die Lernfunktionalität des Systems sollte dynamisch sein, sodass das System automatisch vom Lern- in den Schutzmodus wechselt. Zweiphasige Bedrohungserkennungssysteme, bei denen manuell für die gesamte Instanz vom Lern- in den Schutzmodus gewechselt werden muss, können problematisch und schwierig zu implementieren sein.
- Die Lösung sollte eine Asset-Management-Funktion enthalten, die automatisch die Tausenden Geräte im System sowie im Laufe der Zeit auch deren Bestandteile identifiziert. Sie sollte zum Beispiel erkennen: PLCs, RTUs, HMIs etc.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

3. Bandbreite

Die Herausforderung

- Die Netzwerkbandbreite, welche die Digital Substations mit der Netzleitstelle verbindet, ist in der Regel gering und teilweise nur auf Anforderung aktiv.
- Die kontinuierliche Überwachung von Digital Substations ist daher schwierig. Eine solide Netzwerkinfrastruktur mit Quality of Service (QoS)-Richtlinien ist ebenso erforderlich wie ein integrierter und interoperabler IEC 61850-Prozessbus nach Bedarf. Der Prozessbus muss in der Lage sein, den Verkehr unter verschiedenen Bedingungen zu optimieren, um eine angemessene Netzausfallsicherheit zu gewährleisten.

Die Lösung

- Die Kommunikation zwischen den Guardians in den Digital Substations und den CMCs sollte stark auf Bandbreite optimiert sein. Außerdem sollte sie für ein höheres Maß an QoS auf die Bandbreitenrichtlinien im Digital Substation-Bus abgestimmt sein.
- Die Kommunikation sollte auch auf Basis von festen Bandbreitenbeschränkungen reguliert werden, sodass sie zum Beispiel nur nachts stattfindet oder nur mit Teilen des Systems synchronisiert wird – je nach den allgemeinen Anforderungen und den spezifischen Bedürfnissen der Digital Substation.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

4. Zeitsynchronisation

Die Herausforderung

- Geräte im Steuernetz wie IEDs (intelligente elektronische Geräte), Merging Units, Steuereinheiten und Ethernet-Geräte müssen zeitlich mit hoher Genauigkeit synchronisiert werden, oft auf weniger als eine Mikrosekunde. Das bevorzugte schnelle und sichere Timingsystem verwendet das IEEE 1588-Protokoll und eine Hauptuhr oder das Global Positioning System (GPS). Aber auch SNTP (Simple Network Time Protocol) ist sehr verbreitet, wenngleich es weniger genau ist und für IT-Umgebungen entwickelt wurde.
- Die Zeitsynchronisation ermöglicht die Wiedergabe von Ereignissen wie z. B. Fehlern mit detaillierter Beschreibung, was während des gesamten Ereignisses wann und an welcher Ausrüstung passiert ist.
- Cyberattacken, die die IEEE 1588- / SNTP-Kommunikation oder die Hauptuhr bzw. GPS beeinträchtigen, können den Betrieb stören oder für böswillige Zwecke missbraucht werden.

Die Lösung

- Die Lösung zur Überwachung der Netzwerksicherheit sollte schnell Änderungen der Kommunikations-Basislinien oder des Gerätestatus erkennen, um eine präventive oder schnelle Korrektur von Bedrohungen im Zusammenhang mit der Zeitsynchronisation zu ermöglichen.
- Das System sollte auch leicht spezifische Angriffe auf SNTP-Quellen erkennen.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

5. Komplexität

Die Herausforderung

- Hauptsächlich werden IEC 60870-5-104, DNP3 und Modbus als Protokolle für die Kommunikation der Digital Substations verwendet. Mit diesen Protokollen gesendete Pakete sind einfach zu verstehen. Zum Beispiel kann ein mäßig erfahrener Techniker mit Wireshark die Daten entschlüsseln, die von den Endpunkten gesendet werden. Alle Bits und Bytes des Protokolls werden deutlich angezeigt und dargestellt.
- Heutzutage verwenden digitale Substations IEC 61850 und die ihr zugrundeliegenden Protokolle für die Kommunikation. Dieser Ansatz ist viel komplexer.
- Um die IEC 61850-8-Kommunikation zu analysieren, ist eine fortschrittliche Deep Packet Inspection (DPI)-Implementierung erforderlich. Die DPI-Technologie muss mit komplexen Nutzlasten mit mehreren Schichten (wie ACSI über MMS) umgehen können und erfordert eine zustandsorientierte Analyse sowie umfassende Fähigkeiten zur Kontexterkennung. Außerdem muss das System einen kohärenten Zustand jedes IEDs behalten und aufrechterhalten, auch während es durch Befehle von mehreren Protokollen wie z.B. GOOSE und ACSI gesteuert wird.

Die Lösung

- Cybersicherheit erfordert ein leistungsfähiges DPI-Datenmodell mit tiefgreifenden Kenntnissen der IEC 61850, das die IED-Interaktionen sowohl auf Netzwerk- als auch auf Prozessebene auswerten kann. Dies beinhaltet:
    - Untersuchung von Paketen in allen sieben Ebenen des OSI-Modells
    - Kenntnis der offiziellen Syntax und Grammatik für jedes Protokoll
    - Verstehen der Anpassungen in spezifischen Industriesektoren, einschließlich Stromübertragung und Verteilungssysteme
    - Bereitstellung eines leistungsstarken Analyse-Algorithmus zur Bewertung komplexer Möglichkeiten in Echtzeit
    - Möglichkeit zur Handhabung verschlüsselter Kommunikation
    - Schnelle und klare Alarmierung von OT- und IT-Mitarbeitenden bei problematischen Situationen

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

6. Risiken für Automatisierungs- und Steuerungssysteme

Die Herausforderung

- Vor der Einführung von Standard-IT-Technologien wie Ethernet-, TCP/IP-basierte Kommunikation oder Verbindungen zu externen Systemen waren Automatisierungs- und Prozessnetzwerke durch undurchsichtige Kommunikationsprotokolle und Isolierung geschützt.
- Automatisierung und Steuerungssysteme sind nun anfällig für dieselben Cybersicherheitsrisiken wie IT-Systeme, nur mit dem Potenzial für noch schwerwiegendere Folgen.
- In der Ukraine verursachten Cyberattacken sowohl 2015 als auch 2016 Stromausfälle. Glücklicherweise wurden die Ausfälle innerhalb weniger Stunden behoben. Die Reparaturen am Steuerungsnetzwerk und den Systemen dauerten weitaus länger.

Die Lösung

- Ein umfassendes Verständnis der IEC 61850-Netzwerke ist erforderlich, um eine umfangreiche Ausgangsbasis an Verhaltensweisen zu erfassen und Alarme zu generieren, wenn Anomalien auftreten.
    - Zum Beispiel sollten ein einfaches defektes Netzwerkgerät, das sich an das Netzwerk anschließt, oder unsichtbare unregelmäßige Kommunikation zwischen bekannten Netzwerkgeräten problemlos erkannt und gemeldet werden.
    - Auch komplexe Zustandsänderungen innerhalb von IEDs sollten leicht erkannt und ausgewertet werden. Die Cyberbedrohungserkennung sollte in der Lage sein, Objekte sowohl auf Netzwerk- als auch Prozessebene mit hoher Leistung zu lernen und zu analysieren.
    - Die Architektur der IEC 61850 wird weiterentwickelt, um bessere Cybersicherheit zu gewährleisten. Zum Beispiel definiert das IEC Technical Komitee 57, Arbeitsgruppe 15 (WG15), Wege zur Stärkung globaler Standards, um die Sicherheit weltweiter Energiesysteme zu verbessern. Anbieter von passiven Überwachungslösungen sollten fundierte Kenntnisse über die Weiterentwicklung der IEC 61850-Normen und führende Architekturen für sichere Schaltanlagen haben.[3]

[3] Vgl. Nozomi Networks (2017): Advancing IEC Standards for Power Grid Cyber Security.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Zusammenfassung

Aufgrund von zunehmenden staatlichen Richtlinien, Cybersicherheits-Vorfällen und Sorgfaltspflichten des Managements steigt der Bedarf der Energieversorger an Cybersicherheitsprogrammen. Innovative Lösungen schützen die Ausfallsicherheit Ihrer Systeme und schaffen die notwendige Transparenz über Betriebsprozesse, Kommunikationsbeziehungen, Verwundbarkeiten und Anomalien.

Sicherheitslücken können großen Einfluss auf die betriebliche Ausfallsicherheit haben. Die traditionelle Trennung zwischen IT und OT, während die Stromnetze zunehmend mit den Unternehmensnetzwerken verbunden werden, kann zu blinden Flecken in der Cybersicherheit führen. Ohne Transparenz über die Automatisierung- und Steuerungssysteme ist es schwierig, den Überblick über die Netz- oder Digital Substation-Ebene zu behalten. Selbst kleine Veränderungen oder Netzwerkprobleme können sich auf Zuverlässigkeit, Sicherheit und Umsatz auswirken. Schnelle Reaktionen sind entscheidend. Die Problemerkennung erfordert Echtzeit-Transparenz über Anlagen, Verbindungen, Kommunikation und mehr. Noch fehlen diese Fähigkeiten vielen Stromübertragungs- und Verteilungssystemen.

Tatsächlich sind Transparenz und Cybersicherheit für Automatisierungssysteme mit der intelligenten und lernenden Technologie von Nozomi Networks leicht zu erreichen. Sie verbessert mit dem automatisch generierten dynamischen Inventar die Sichtbarkeit Ihrer Assets. Sie erstellt prozess- und sicherheitsspezifische Systemprofile, überwacht das Verhalten der Anlagen und des Netzwerkverkehrs und warnt bei Änderungen, die auf potenzielle Probleme hinweisen könnten. Das Ergebnis sind schnelle Identifizierung, Priorisierung und Alarmierung bei Cyberangriffen, Sicherheitsvorfällen, Schwachstellen und kritischen Prozessanomalien. Diese Informationen können Cyberbedrohungen oder Prozessvorfälle verhindern, einzudämmen oder entschärfen, bevor signifikanter Schaden entsteht. Die Datenanalyse ist auch von unschätzbarem Wert für die Aufwandsreduzierung bei der Fehlerdiagnose und Wiederherstellung.

Guardian powered by IKARUS deckt verschiedene Use Cases in den Branchen Energieversorgung, industrielle Produktion, Gebäudeautomation, Transportation etc. ab, arbeitet trotz der Größe und Komplexität, die Energieversorgungssysteme mit sich bringen, extrem effizient und verbessert damit die Cybersicherheit, Transparenz und Ausfallsicherheit.

Haben Sie Fragen?

Energieversorgungsunternehmen können von der Investition in Transparenz und Sicherheit ihrer Automatisierung- und Steuerungssysteme stark profitieren.

Vereinbaren Sie einen Präsentations- oder Demo-Termin!

IKARUS Security Software GmbH
A-1050 Wien, Blechturmgasse 11

Telefon: +43 1 58995-500
E-Mail: sales@ikarus.at

Abkürzungsverzeichnis

CMC	Central Management Console
DPI	Deep Packet Inspection
GPS	Global Positioning System
IED	Intelligent Electronic Device
IP	Internet Protocol
LMC	Local Management Console
PLC	Programmable Logic Controller
QoS	Quality of Service
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SNTP	Simple Network Time Protocol
SOC	Security Operation Center
SV	Sampled Values
TCP	Transmission Control Protocol
TAP	Test Access Point
WAN	Wide Area Networks

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Worauf Sie bei Lösungen zu OT/IoT-Cyber Security achten sollten?

Obwohl zunehmende Cybersicherheits-Bedrohungen die Nachrichten dominieren, gibt es Grund, optimistisch zu sein. Neue Technologien wie die Lösung von Nozomi Networks powered by IKARUS sind einfach und sicher zu implementieren, verbessern die OT/IoT-Cybersicherheit drastisch und lassen sich nahtlos in Ihre bestehende IT-Infrastruktur integrieren.

Wenn Sie sich für eine OT/IoT Cyber Security-Lösung und einen IT/OT/IoT Cyber Security-Anbieter für Ihr Unternehmen entscheiden wollen, achten Sie auf folgende Vorteile:

- ✓ Detaillierte Transparenz über die OT/IoT-Betriebsabläufe
- ✓ Fortschrittliche Bedrohungserkennung für Automatisierungs- und Steuerungssysteme
- ✓ Bewährte, groß angelegte globale Installationen
- ✓ Schneller Einsatz über viele Standorte hinweg
- ✓ Einfache IT/OT/IoT-Integration
- ✓ Globales Partner-Ökosystem
- ✓ Leidenschaft für Kundenerfolg

Über IKARUS Security Software

Der österreichische Cyber Security-Spezialist IKARUS Security Software entwickelt und betreibt seit 1986 führende Sicherheitstechnologien: von der eigenen Scan Engine über leistungsstarke Cloud-Services für Endpoints, mobile Endgeräte und E-Mail-Gateways bis hin zur Threat Intelligence Platform (TIP).

Durch Partnerschaften mit FireEye/Mandiant, Marktführer im Bereich Threat Intelligence, und Nozomi Networks, Technologieführer bei OT/IoT-Security, erweitert IKARUS das eigene Portfolio und positioniert sich als der lokale Ansprechpartner und Systemintegrator für professionelle IT, OT- und IoT-Security.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com