Cisco Digital Utility Whitepaper: OT Security

Contents

Mit der Digitalisierung der Energiebranche vergrößern sich die Angriffsflächen der Versorgungsunternehmen und ihrer Infrastruktur. Die Vernetzung und Automatisierung auf allen Ebenen nehmen zu. IT- und OT-Systeme verschmelzen (IT/OT Convergence). Gleichzeitig werden Cyberattacken gefährlicher. Schutzmaßnahmen müssen sowohl technische als auch organisatorische Faktoren umfassend berücksichtigen. Insbesondere bei der Modernisierung der Systeme sollte die Einführung entsprechender Sicherheitslösungen immer mitgedacht werden. Security muss in allen Planungen und neu eingeführten Technologien ein integraler Bestandteil sein.

Prinzipiell sind Schutzziele in der Energieversorgung und -verteilung anders priorisiert als in den meisten anderen Branchen. Die Verfügbarkeit steht hier im Vordergrund. Generell können die Schutzziele unter der Abkürzung CIA (Confidentiality, Integrity, Availability) zusammengefasst werden: Vertraulichkeit, Integrität und Verfügbarkeit. Die Verfügbarkeit steht an erster Stelle, gefolgt von der Integrität der Daten und der Vertraulichkeit. Im Weiteren gibt es noch andere Besonderheiten, vor allem im Vergleich zur IT-Branche, die Einfluss auf eine Sicherheitsarchitektur haben. Das betrifft vor allem die Lebenszeit der Geräte und Anlagen und die damit verbundenen technischen Limitierungen hinsichtlich der Implementierung von Schutzfunktionen. Dazu kommen die räumliche Ausdehnung der Anlagen sowie die Tatsache, dass viele Installationen oft ohne Personal betrieben werden und damit die physische Sicherheit auch eine große Rolle spielt. Zusätzlich müssen sich Schutzmaßnahmen gesetzlichen Regularien unterwerfen und an OT-Protokollen orientieren.

Die technischen Schutzmaßnahmen lassen sich grob in die im Folgenden ausgeführten Punkte unterteilen.

- Transparenz
- Segmentierung
- Drahtlose Kommunikation: Einsatz von Funktechnologien
- Weitverkehrsnetze
- Cloud Computing
- Ende-zu-Ende-Sicherheit
- Angriffserkennung (Intrusion Detection)
- Incident Response (Notfall-Management)
- Integrität der Geräte
- Privacy (Schutz personenbezogener Daten)
- Standards und Regularien

Transparenz

Komplexe Infrastrukturen stellen zunehmend ein Sicherheitsrisiko dar. Deshalb geht es zunächst darum, einen Überblick zu gewinnen, welche Systeme vorhanden sind und angegriffen werden können – also die Transparenz zu erhöhen. Denn die Überwachung von Geräten, Anlagen und Kommunikationssystemen ist essenziell, um eventuelle Angriffe frühzeitig zu erkennen.

Neu vernetzte Systeme müssen klar zugeordnet und ihre Sicherheit überprüft werden. Ein Grundbaustein hierfür ist eine Public Key Infrastruktur (PKI), um Systeme zu authentifizieren und zu autorisieren. Eine PKI ist ein hierarchisches System zur Ausstellung, Verteilung und Prüfung von digitalen Zertifikaten. Die digitalin Zertifikate ermöglichen eine vertrauenswürdige Zuordnung von Entitäten zu ihren öffentlichen Schlüsseln. Ein aktives Anlagenmanagement sorgt zudem dafür, dass alle Geräte und Systeme sowie deren Funktionalität bekannt und klassifiziert sind. Genauso gilt es, sie mit sicheren Wartungszugängen zu versehen. Dies ermöglicht ein vorausschauendes Patch Management und erkennt Schwachstellen in der installierten Software frühzeitig. Das Kommunikationsnetz kann so die Rolle eines Sensors spielen und notwendige Informationen für die Erkennung von kritischen Zuständen bis hin zu Angriffen liefern.

Segmentierung

Der erste Schritt in Sachen Cybersecurity ist der Schutz der sogenannten Perimeter, also der Übergänge des Prozessnetzes zur Außenwelt sowie zwischen den verschiedenen Ebenen. IT- und OT-Systeme und -Netze verschmelzen im Zuge der Digitalisierung weiter miteinander. Darum ist die physische und logische Trennung von Teilen der Kommunikationsnetze in Zonen und sicheren Verbindungen zwischen diesen (Zones and Coduits) von hoher Bedeutung.

Energieversorger und -verteiler sollten zunächst eine Risikoanalyse durchführen. Davon ausgehend können Netzwerksegmente mit identischen Schutzzielen identifiziert und mit Schutzmaßnahmen wie Next Generation Firewalls und Access Control versehen werden. Dabei ist darauf zu achten, dass diese die OT-Protokolle interpretieren, analysieren und darauf aufbauend Maßnahmen initiieren können. Ein weit verbreitetes Protokoll der International Electrotechnical Commission (IEC) ist IEC 60850-5-104 zur Steuerung von Umspannwerken und Windkraftanlagen oder ICCP (TASE.2) für die Verbindungen zwischen den Leitstellen. Ein Zonenmodell, etwa gemäß IEC 62443, sorgt dabei für Sicherheit in der Tiefe. Die Einführung eines solchen Zonen-Konzeptes ist nur möglich, wenn die Kommunikationsnetze von Beginn an flexibel geplant werden und die Topologien eine solche Segmentierung ermöglichen.

Die zunehmende Fernwartung spielt in diesem Kontext eine besondere Rolle. Dabei muss der authentifizierte und autorisierte Zugriff auf Komponenten in unterschiedlichen Teilen des Netzes sowie ein entsprechendes Logging gewährleistet werden. Die Anforderungen hinsichtlich der Segmentierung von Netzen im Bereich Industrieller Kontroll- und Leitsysteme sind integraler Bestandteil der Normenreihe IEC/ISA 62443 (Teile 3-2 und 3-3) und der darauf aufbauenden Zertifizierungen.

Anbindungen an das Internet sollten sehr restriktiv gehandhabt werden. Oft kommen in einem solchen Szenario sogenannte Demilitarisierte Zonen (DMZ) zum Einsatz. Dabei handelt es sich um abgegrenzte und gesicherte Segmente des Netzwerks, in dem spezielle Computer (Server) mit kontrollierten Zugriffsmechanismen betrieben werden. Sie unterbinden eine direkte Verbindung vom internen Netzwerk auf Ressourcen im Internet und stellen gleichzeitig die erforderlichen Services zur Verfügung.

Drahtlose Kommunikation: Einsatz von Funktechnologien

WLAN, Bluetooth, LoRaWAN, 5G, etc. – in der OT kommen zunehmend Funktechnologien zum Einsatz, um Sensoren im Internet of Things (IoT), automatisierte Maschinen, Roboter und Monitore drahtlos remote zu steuern und zu verwalten. Doch komplexe Architekturen aus kabelgebundenen und kabellosen OT- sowie IT-Komponenten sind schwierig zu überwachen und zu sichern, zumal mit 5G die Anzahl miteinander verbundener Endgeräte enorm steigt. Daher muss drahtlose Kommunikation gerade in besonders sicherheitsrelevanten Bereichen einer intensiven Kontrolle hinsichtlich Zugriffsberechtigungen unterliegen und restriktiv gehandhabt werden. Eine Risikobetrachtung ist unbedingt erforderlich. Das betrifft vor allem die Identifizierung und Authentifizierung aller Nutzer, die mittels drahtloser Kommunikation auf die Geräte und Systeme der Schutz- und Leittechnik zugreifen. WLANs sollten nur verschlüsselt und in abgetrennten Netzwerksegmenten betrieben werden. Ein Zugriff auf kritische Funktionen der Steuerung und Überwachung ist unbedingt zu vermeiden.

Weitverkehrsnetze

Kommunikationsnetze müssen höchste Verfügbarkeit garantieren. Dabei kommunizieren die einzelnen Zonen oft auch über Weitverkehrsnetze (WAN). Das heißt, eine sichere Verbindung muss auch bei unterbrochenen Kommunikationsleistungen hergestellt werden können. Dazu ist zum einen Redundanz in der Topologie nötig, damit immer zwei Kommunikationspfade gegeben sind. Zum anderen erfordert dies ausreichende Echtzeitfähigkeit. Im Bereich der aktiven Komponenten erfolgt im Kommunikationsnetz derzeit ein Technologiewandel von synchronen Zeitmultiplex-basierten Systemen hin zu paketorientierten Technologien (MPLS, IP). Eine Umstellung ist ratsam, bevor die Unterstützung der Hersteller für alte Systeme ausläuft.

Die Sicherheitsmechanismen der Zonenkommunikation müssen die Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) abdecken. Dazu sind die Daten für ihre Übertragung durch die Weitverkehrsnetze entsprechend zu verschlüsseln. Die zum Einsatz kommenden Protokolle sollten die kryptographischen Anforderungen, beispielsweise auf der Grundlage der Normenreihe IEC 62351, erfüllen und die Geräte diese Standards auch implementieren. Dann können die Schutzfunktionen in einem Ende-zu-Ende-Szenario genutzt werden.

Wenn diese Voraussetzung nicht besteht, sollten VPN-Technologien implementiert und angewendet werden, um die Übertragung der Daten kryptographisch zu sichern. Diese existieren mit MACSec (IEEE.801.AE) auf Layer 2 und auch mit IPSec auf Layer 3 des OSI-Stacks. Des Weiteren sind Security Controls erforderlich, um DoS/DDoS-Angriffe zu erkennen und abzuwehren, damit die Verfügbarkeit der Systeme zu jedem Zeitpunkt gewährleistet ist.

Cloud Computing

Neue Technologien wie Virtualisierung, Cloud Computing und Industrial IoT (IIoT) stellen die Segmentierung vor neue Herausforderungen. Denn dadurch wird die IT-Infrastruktur immer komplexer. Um den Überblick auch in der Tiefe nicht zu verlieren, helfen neue Zonenkonzepte und angepasste Verantwortlichkeiten. Dabei ist die Cloud gesondert zu betrachten, da sie ein erhöhtes Sicherheitsrisiko für den externen Zugriff auf kritische Daten und Systeme darstellt, speziell im Fall einer Cyberattacke.

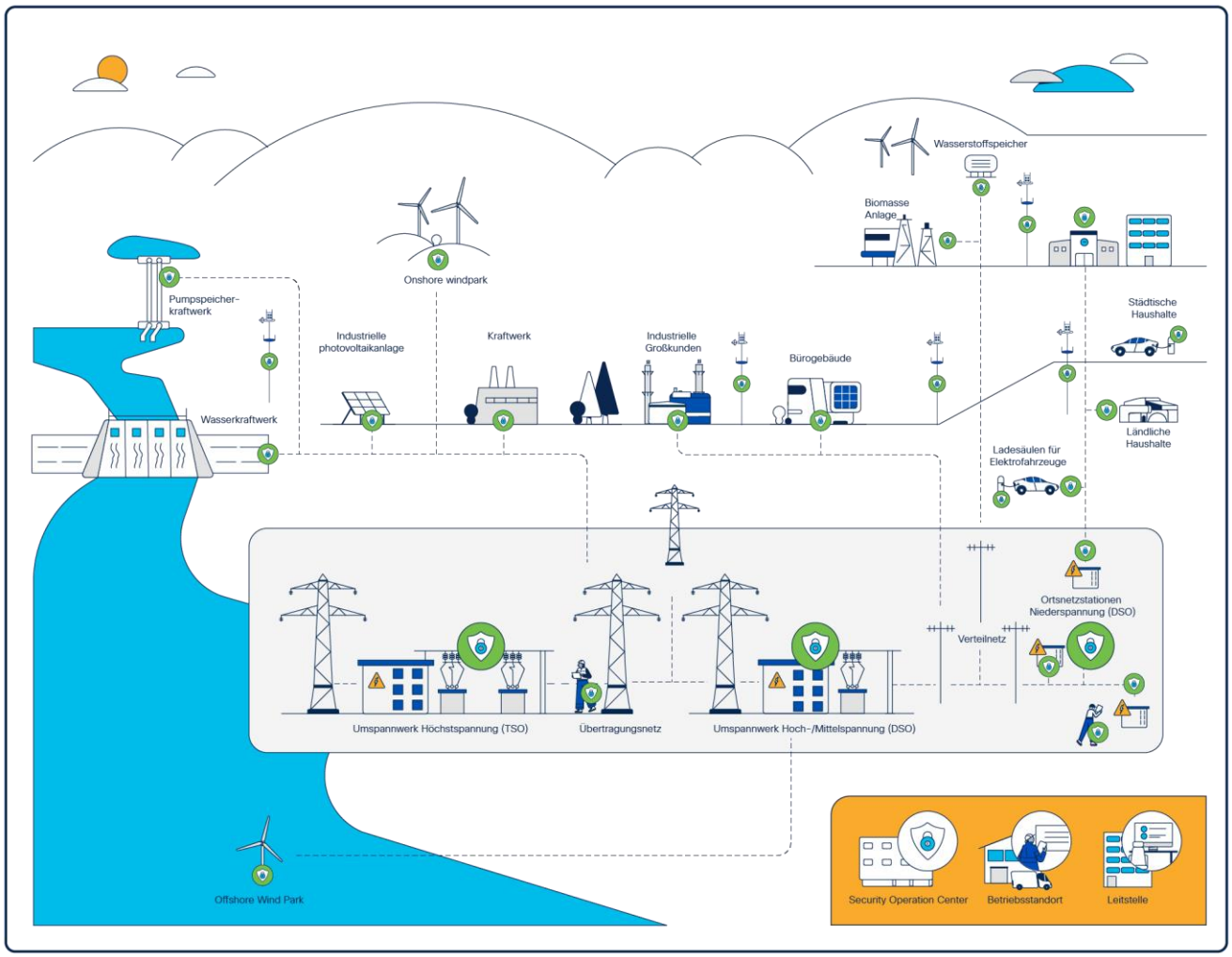
Bereits im Vorfeld sind eine sorgfältige Planung und Auswahl durch die Betreiberfirmen erforderlich. Funktionen und Systeme werden identifiziert, die für einen Betrieb in einer Cloud-Umgebung geeignet sind. Dabei ist auschlaggebend, ob diese Cloud-Systeme intern oder durch einen externen Dienstleister betrieben werden. Funktionalitäten zur Steuerung und Überwachung der kritischen Infrastruktur sind dahingehend besonders restriktiv zu handhaben und sollten nicht extern betrieben werden. Entsprechende Risikobewertungen bilden dafür die Grundlage. In jedem Fall sind entsprechende Vereinbarungen (SLAs) mit den jeweiligen Hosts zu treffen, um die erforderlichen Anforderungen hinsichtlich Verfügbarkeit, Integrität und Vertraulichkeit der Daten zu gewährleisten.

Ende-zu-Ende-Sicherheit

Visibilität, Segmentierung, Access Control und kryptographische Maßnahmen für eine sichere Datenübertragung bilden die Schutzmauer um die Kommunikationsnetze, um diese gegen Störungen, Ausfälle und Cyberkriminalität im Ernstfall abzusichern. Dabei sind die Sicherheitsmaßnahmen keineswegs nur punktuell zu ergreifen, sondern erstrecken sich von einem zu jedem anderen Ende des gesamten Kommunikationsnetzes.

Die Voraussetzung für eine kryptographisch gesicherte Ende-zu-Ende-Verbindung in einem Kommunikationsnetz ist eine Implementierung der entsprechenden Mechanismen in den Endgeräten, beispielsweise in den IEDs (Intelligent Electronic Devices). Die Normenreihe IEC 62351 stellt Spezifikationen zur Verfügung, um eine Interoperabilität zwischen den Herstellern der Geräte und Systeme zu gewährleisten. Das betrifft insbesondere die Protokolle IEC 61850 (MMS, GOOSE, SV), ICCP (TASE.2) und IEC 60870-5-104, inklusive Key-Management, sowie Festlegungen hinsichtlich RBAC.

Bestandssysteme, die diese Funktionen nicht unterstützen, können mit Hilfe kompensierender Schutzmechanismen abgesichert werden, zum Beispiel durch die Verwendung von MACSec (Media Access Control Security, einen in der IEEE-Norm 802.1AE spezifizierten Sicherheitsstandard). Auch für OPC-UA, das gerade im Bereich der Anbindung von Windfarmen an Bedeutung gewinnt, stehen die entsprechenden Security-Spezifikationen zur Verfügung, um einen sicheren Datenaustauch zwischen den Endgeräten zu gewährleisten.



Angriffserkennung (Intrusion Detection)

Die Mehrheit der Attacken auf Energieversorger wird über IT-Systeme initiiert, beispielsweise über das Versenden von Phishing-Mails. Das ist speziell bei der Planung eines Zonenkonzeptes zu beachten. Die Übergänge von den IT-Netzen zu den OT-Systemen müssen besonders geschützt und überwacht werden. Das betrifft vor allem Zugriffsberechtigungen und eine genaue Analyse des Datenverkehrs, vor allem hinsichtlich Abweichungen (Anomalien).

Einen automatisierten Schutz bieten Next-Generation Firewalls, die in Hardware oder Software implementiert sind. Sie erkennen komplexe, domänenspezifische Angriffe und können sie blockieren, indem sie Sicherheitsrichtlinien auf Anwendungs-, Port- und Protokollebene durchsetzen. Zudem ist eine Zero-Trust-Architektur unerlässlich. Um die Versorgungssicherheit eines Landes zu gewährleisten, dürfen Netzwerke nichts und niemandem vertrauen und müssen jederzeit die geforderten Authentifizierungs- und Zugangsrechte überprüfen.

Für den Ernstfall sind automatisierte Angriffserkennungssysteme, sogenannte Intrusion Detection Systems (IDS) unerlässlich. Dabei bildet die unter Punkt 1 erwähnte Sichtbarkeit die Grundlage für eine zeitnahe Erkennung von Anomalien und Bedrohungen. Des Weiteren ist eine tiefgehende Kenntnis und Analyse der zum Einsatz kommenden Protokolle wie des Manufacturing Message Specification Protocol IEC 61850 oder des IEC 60870-5-104 notwendig, um eine Angriffserkennung auch domänenspezifisch zu gewährleisten. Methoden des Machine Learning können an dieser Stelle unterstützen und die Effektivität der Angriffserkennungssysteme verbessern. Sämtliche Protokolle wie TASE.2 (ICCP) müssen vollständig von Firewalls unterstützt werden.

Firewall-Management-Systeme prüfen sämtliche Firewall-Regeln auf Konsistenz und automatisieren die Regelverwaltung. Weitere, mehrstufige Sicherheitsmaßnahmen (RBAC, Kryptographie) helfen außerdem, die Angriffsrisiken zu minimieren. Eine Threat Intelligence kann außerdem automatisiert für mehr Sicherheit, auch in der Tiefe, sorgen, indem sie über ein Dashboard Informationen übersichtlich aufbereitet und Empfehlungen für Maßnahmen gibt.

Incident Response (Notfall-Management)

Eine schnelle und zielgerichtete Reaktion ist entscheidend, um den Schaden im Fall eines Cyber-Angriffes auf ein Minimum zu beschränken. Basis dafür ist eine zeitnahe und im besten Fall automatische Erkennung, für die vor allem die sicherheitstechnischen Maßnahmen, wie unter Topic 6 und Topic 7 beschrieben, essenziell sind. Auch ein vertrauenswürdiger Partner kann helfen, Notfälle schnell einzudämmen, sei es bei Datenschutzverletzungen oder Ransomware-Angriffen. Ein umfassendes Backup aller relevanten Daten sollte zusätzlich gesondert und damit sicher vor Angriffen abgelegt werden, damit der Betrieb nach einem Ausfall rasch wieder aufgenommen werden kann.

Zusätzlich ist eine umfassende und sichere Protokollierung (Logging) zu gewährleisten. Alle relevanten Informationen von Intrusion Detection und anderen Systemen der Threat Intelligence sowie der Protokollierung (Log-Dateien) sollten in einem dedizierten Security Information and Event Management System (SIEM) zusammengeführt werden. Davon ausgehend erfolgt eine automatisierte Analyse und eine somit verbesserte Reaktion auf eventuelle noch kommende Cyber-Angriffe. Das schließt alle weiteren Maßnahmen, die die forensischen Analysen unterstützen, ein.

Integrität der Geräte

Sichere und vertrauenswürdige Geräte sind eine weitere wichtige Voraussetzung für Aufbau und Betrieb der kritischen Infrastruktur. Das beginnt mit der Entwicklung der Geräte beim Hersteller und setzt sich über alle Lebenszyklen bis hin zum Betrieb und der Deinstallation fort. Ein aktives Patch Management ist dabei selbstverständlich eingeschlossen, wobei auch hier die bereits erwähnte Normenreihe IEC/ISA 62443 eine wichtige Rolle spielt.

Darüber hinaus sollten vertrauenswürdige Geräte über eine eindeutige Identität verfügen, die beispielsweise an eine PKI (Infrastruktur für öffentliche Schlüssel) geknüpft ist. Damit lassen sich diese Geräte eindeutig identifizieren und deren Zugriffsrechte reglementieren. Allerdings verfügen viele Geräte, die sich bereits in Betrieb befinden, nicht über solche Identitäten und auch nicht über andere kryptographische Funktionen. In diesem Fall können kompensierende Maßnahmen zum Einsatz kommen, beispielsweise Gateways oder auch Tunnel-Mechanismen (VPN). Gleichzeitig sollten solche Geräte automatisiert überwacht werden, um eventuelle Angriffe frühzeitig zu erkennen.

Zusätzlich empfiehlt sich gerade bei Geräten und Systemen aus dem Bereich der Standard-IT (PCs, Laptops) der Einsatz von Anti-Malware-Systemen zur frühzeitigen Erkennung von Schadsoftware. Eine sichere Grundkonfiguration der Geräte ist insbesondere bei Standardkomponenten unbedingt erforderlich. Schnittstellen zu Geräten (z.B. USB) müssen gesichert werden, um die Übertragung von Schadsoftware ausschließen zu können. Vertrauliche Daten müssen entsprechend der behördlichen Vorgaben verschlüsselt gespeichert und übertragen werden. Das betrifft insbesondere Passwörter, Parametrierdaten und Protokolldateien.

Privacy (Schutz personenbezogener Daten)

Wo immer personenbezogene Daten verwendet werden, müssen die entsprechenden Regularien zu deren Schutz Beachtung finden. In Deutschland ist von den nationalen Rechtsvorschriften im Rahmen der Datenschutz-Grundverordnung (DSGVO) für Energieversorger vor allem das Bundesdatenschutzgesetz (BDSG) sowie das Messstellenbetriebsgesetz (MsbG) relevant.

Es darf keine Nachvollziehbarkeit bei Kundendaten bestehen, beispielsweise bei der Beauftragung von Serviceunternehmen für die Zählerablesung oder Abrechnungen. Das betrifft neben der Datenspeicherung vor allem die Anwendungsfälle, in denen Kundendaten wie Adressen oder Zählerdaten übertragen oder verarbeitet werden. Der Datenschutz gemäß der DSGVO beginnt bereits beim ersten Mal, wenn Kundendaten erhoben und verarbeitet werden.

Er kann unter anderem durch eine Anonymisierung der Daten erreicht werden. Dabei helfen Technologien wie sichere, zertifizierte Smart Meter, also intelligente Gas-, Wasser- oder Stromzähler. Zudem sollten die Daten einem strengen Identity und Access Management (IAM) unterliegen, damit niemand unbefugt darauf zugreifen kann. Hier unterstützen integrierte Datenschutzmanagementsysteme von vertrauenswürdigen Anbietern, die hinsichtlich Sicherheit und Zuverlässigkeit geprüft und zertifiziert sind.

Standards und Regularien

Viele der unter den einzelnen Topics aufgeführten Sicherheitsmaßnahmen unterliegen klar definierten Regularien und strengen Standards bzw. referenzieren dahingehend. Das betrifft insbesondere:

- **IT-Grundschutz**

  Der IT-Grundschutz des BSI ist Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Behörden, Unternehmen und Institutionen, die sich mit der Absicherung ihrer Daten, Systeme und Informationen befassen.

- **KRITIS**

  Kritische Infrastrukturen (KRITIS) unterliegen dem Gesetz des Bundesamtes für Sicherheit in der Informationstechnik (BSIG). Dieses bestimmt Rechtsgrundlagen sowie Pflichten für KRITIS-Betreiber wie Energieversorger.

- **IT-Sicherheitsgesetz 2.0**

  Das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme stärkt das BSI bei Detektion und Abwehr, Cyber-Sicherheit in den Mobilfunknetzen, Verbraucherschutz und Sicherheit für Unternehmen, um Energieversorgern bei Informationssicherheit und Digitalisierung zur Seite zu stehen.

- **BDEW Whitepaper**

  Der Bundesverband der Energie- und Wasserwirtschaft vertritt rund 1.900 Unternehmen, darunter Energieversorger. Whitepaper zu aktuellen Anforderungen für Sicherheit oder Steuerung dienen als kostenlose Anwendungshilfen.

- **IEC/ISA 62443**

  Die internationale Normenreihe IEC 62443 beschäftigt sich mit industriellen Kommunikationsnetzen und IT-Sicherheit für Netze und Systeme. Die Norm ist in verschiedene Abschnitte unterteilt und beschreibt sowohl technische als auch prozessbezogene Aspekte der industriellen Cybersecurity.

- **IEC 62351**

  Die Norm IEC 62351 beschreibt den Standard für Sicherheit im Energiemanagement und zugehörigem Datenaustausch. Sie beschreibt Maßnahmen, um vier Grundforderungen (Vertraulichkeit, Datenintegrität, Authentifizierung, Unleugbarkeit) für sichere Datenkommunikation bzw. -verarbeitung zu erfüllen.

- **NERC CIP**

  Die NERC-CIP-Standards (North American Electric Reliability Corporation Critical Infrastructure Protection) zielen darauf ab, die Zuverlässigkeit des Bulk Electric System (BES) aufrechtzuerhalten und zu verbessern. Sie bieten elektrischen Infrastrukturen Schutz vor Bedrohungen der OT-Sicherheit.

Zusammenfassung

Die aufgeführten Schutzfunktionen sind Bausteine für eine umfassende Security-Architektur. Diese richtet sich an den Schutzzielen Verfügbarkeit, Vertraulichkeit und Integrität aus und unterliegt Regeln, Normen und Standards. Das Ziel ist, komplexe Strukturen zu trennen und zu vereinfachen, sämtliche Komponenten der IT- sowie OT-Infrastruktur sichtbar und beobachtbar zu gestalten und diese vollständig und möglichst automatisiert vor Fehlfunktionen, Datenschutzvorfällen und vor allem Cyberangriffen abzusichern. Denn Energieversorger und -verteiler zählen zur kritischen Infrastruktur Deutschlands und müssen auch im Notfall voll einsatzfähig bleiben.

Die Implementierung von Sicherheitsmaßnahmen muss natürlich von den notwendigen administrativen und prozeduralen Maßnahmen im Betrieb begleitet werden. Das ganze Personal ist einzubeziehen und zu schulen, um Cyberangriffe zu erkennen und gegebenenfalls Gegenmaßnahmen einzuleiten. Eine modern Sicherheitsarchitektur muss ständig überarbeitet und angepasst werden. Nur so können Unternehmen mit neuen Angriffsszenarien und Bedrohungslagen Schritt halten.

Dabei werden automatisierte Prozesse wie Intrusion Detection, Incident Response, Security-Managementsysteme oder auch Smart Meter eine immer größere Rolle spielen. Denn neben Weitverkehrsnetzen verlagert sich die Administration und Datenspeicherung auch im Energiesektor zunehmend in die Cloud. Dies hilft dabei, die heute geforderte Agilität zu unterstützen und die steigende Komplexität zu beherrschen. Insgesamt zeigt sich: Die Digitalisierung durchdringt auch kritische Infrastrukturen immer mehr – Energieversorger sollten jetzt handeln und sich mit den richtigen Maßnahmen und Hilfestellungen gegen heutige sowie zukünftige IT-Bedrohungen und Cyberkriminalität wirksam absichern.

Sie wollen mehr erfahren? Nähere Infos finden Sie auf unsere Website für den Energiesektor: www.cisco.de/Energiesektor

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-3504752-00 03/23