Cybersecurity
für eine sichere und zuverlässige Energieversorgung

SIEMENS

Inhalt

Netzsicherheit ist Vertrauenssache.

Cybersicherheit ist ein hochsensibler Bereich, der einen vertrauenswürdigen Partner erfordert. Einen Technologiepartner, der versteht, wie sich Produkte, Systeme und Lösungen in die Prozesse dahinter integrieren und mit den Menschen zusammenwirken.

Wir kombinieren ein branchenführendes Smart-Grid-Portfolio mit umfassender Erfahrung und Expertise bei der Bereitstellung von Cybersicherheitslösungen. Als multinationales Unternehmen mit globaler Reichweite verfügen wir über die notwendige Größe und Kompetenz, um einen zuverlässigen und nachhaltigen Support zu bieten, auf den Sie sich verlassen können.

Unser Fachwissen und unsere Integrationsfähigkeit machen unser Portfolio zum umfassendsten in der Branche. Wir bieten Produkt-, Lösungs- und Servicesicherheit, die einen einzigartigen Lebenszyklus-Support umfasst.

Wir arbeiten aktiv mit internationalen Standardisierungsorganisationen zusammen, um Sicherheitsstandards für Smart Grids zu entwickeln und zu verbessern. Zudem beraten wir Regulierungsbehörden zu technischen und prozessbezogenen Themen.

Wir beschäftigen ein Siemens-weites Computer Emergency Response Team (CERT), und unsere Aufsicht über das CERT gibt uns einen besseren Einblick in globale Cybersicherheitsbedrohungen.

KAPITEL 1

Cybersicherheit im digitalen Netz

Die Bereitstellung einer kosteneffizienten, sicheren und zuverlässigen Energieversorgung ist das Kerngeschäft von Energieversorgern, die kritische Infrastrukturen betreiben. Die Art und Weise, wie Netze betrieben und verwaltet werden, hat sich durch die Integration erneuerbarer und dezentraler Energiequellen, die Notwendigkeit der Netzoptimierung, die Interaktion mit Prosumern und Verbrauchern sowie die Beteiligung neuer Marktteilnehmer drastisch verändert.

Mit der Integration von Informations- und Kommunikationstechnologien in das Verteilnetz und sogar in die Haushalte schaffen die zunehmenden Verbindungen mehr Angriffspunkte auf kritische Infrastrukturen. Folglich steht die Cybersicherheit für Betreiber von Stromnetzen heute an erster Stelle.

Wie in **Abbildung 1** dargestellt, ist es ein wesentliches Ziel eines Stromnetzbetreibers den Betrieb zu sichern, d. h. jederzeit eine stabile Stromversorgung, sowie die Instandhaltung der Infrastruktur zu wettbewerbsfähigen Kosten und unter Berücksichtigung von Vorschriften, zu gewährleisten. Aus dieser Perspektive werden Cyberbedrohungen als Risiken wahrgenommen, die die Versorgungssicherheit gefährden. Cyber-Sicherheit umfasst alle Maßnahmen, die sich mit der Minderung solcher Risiken, der Einhaltung von Industriestandards und gegebenenfalls der Einhal-

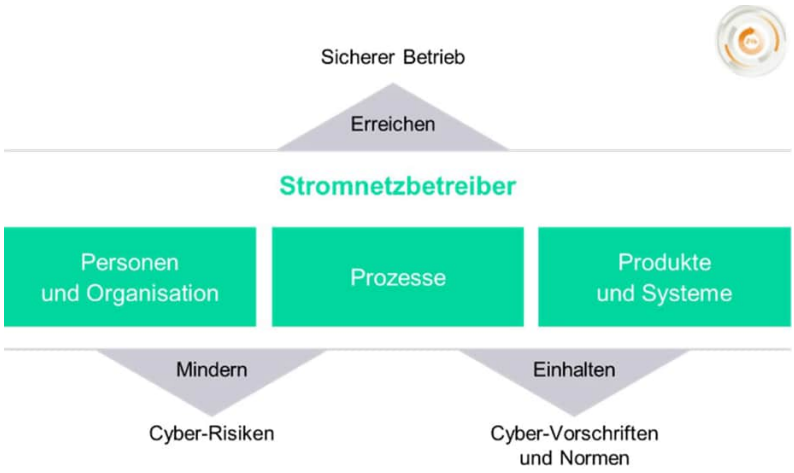


Abbildung 1: Cybersicherheitsziele für einen Stromnetzbetreiber

tung lokaler Vorschriften in Bezug auf die Cyber-Sicherheit befassen.

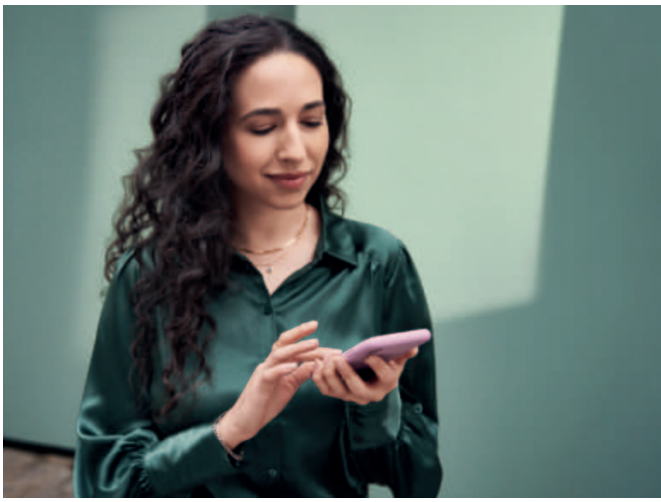
Um dieses Ziel zu erreichen, muss der Netzbetreiber:

- die für die Cyber-Sicherheit relevanten Vorschriften einhalten, welche beschreiben, was getan werden muss
- die entsprechenden Cyber-Standards einhalten, welche beschreiben, wie dabei vorzugehen ist, und
- die Cyber-Risiken minimieren.

Maßnahmen zum Cyber-Schutz können **Personen** und Organisationen, **Prozesse** sowie **Produkte** und Systeme betreffen. Dies sind die sogenannten „3 Ps“ für ein ganzheitliches Cyber-Sicherheitskonzept.

Die Produkte und Lösungen von Siemens unterstützen die Netzbetreiber dabei, die Bestimmungen für Cyber-Sicherheit einzuhalten. Darüber hinaus entsprechen die Produkte internationalen Standards, um die Interoperabilität mit Komponenten von Fremdanbietern zu ermöglichen.

Siemens berät seine Kunden zum Thema Cyber-Sicherheit. Das Ziel der Beratung ist es, die Regularien zu erfassen und einzuhalten sowie Schutzkonzepte zu entwickeln, um die Cyber-Risiken in der Energieautomatisierung zu reduzieren.



KAPITEL 2

Siemens Cybersecurity Framework

Das Cybersecurity-Framework von Siemens definiert die Art und Weise, wie Cyber-Sicherheit von den verschiedenen Akteuren in der Energiewertschöpfungskette angegangen werden muss.

1. Organisatorische Sicherheit und Prozesse

- Organisatorische Bereitschaft
- Sichere Entwicklung
- Sichere Integration und Service

2. Betriebssicherheit

- Umgang mit Schwachstellen und Vorfällen
- Sicherheitspatch Management
- Benutzerverwaltung und Zugangskontrolle
- Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM)

3. Produkte und Systeme

- Sichere Systemarchitektur
- Systemhärtung
- Zugriffskontrolle und Kontoverwaltung
- Sicherheitsprotokollierung/ -überwachung
- Sicherheits-Patches
- Schutz vor Malware
- Sicherung und Wiederherstellung
- Sicherer Fernzugriff
- Datenschutz und Integrität
- Schutz persönlicher Daten

4. Angewandte Cybersicherheit

- Produktsicherheit
- Systemsicherheit, digitales Umspannwerk
- Sicherung von Leitstellen

5. Beratung im Bereich Cybersicherheit

- Orientierung
- Zielbestimmung
- Routing
- Navigation

Siemens Cybersecurity-Framework basiert auf:

Regulierung der Cybersicherheit

Cybersicherheitsvorschriften müssen von allen Akteuren innerhalb der Energiewertschöpfungskette unterstützt werden.

Standards für Cybersicherheit

Bestehende internationale Standards beschreiben Cybersicherheit von der Verwaltung bis hin zu konkreten Realisierungsoptionen in Produkten. Die drei wichtigsten Normen in der Energieautomatisierung sind ISO/IEC 27001, IEC 62443 und IEC 62351.

Richtlinien für Cybersicherheit

Richtlinien enthalten Empfehlungen zur Umsetzung der Cybersicherheit. Die gebräuchlichsten und anerkanntesten Richtlinien für Stromnetze sind: NIST IR 7628, NERC CIP, BDEW Whitepaper.

Im Rahmen der Richtlinien definiert Siemens 14 Kategorien von Sicherheitsmaßnahmen, welche in **Abbildung 2** zu sehen sind. Diese Kategorien spiegeln einen ganzheitlichen Ansatz für die Cybersicherheit wider und umfassen die so genannten "3 P's":

Personen und Organisationen

Menschen, die im Unternehmen arbeiten

Prozesse

Prozesse, die von den Personen und Organisationen verwendet werden, um die Geschäftsanforderungen zu erfüllen

Produkte und Systeme

Die zugrunde liegende Infrastruktur zur Unterstützung der Geschäftsanforderungen

Die Kategorien für Prozesse und Organisationen sind in **Abbildung 2** in den grauen Kästen dargestellt. Die Sicherheitsmaßnahmen für Produkte und Systeme sind in den grünen Kästen kategorisiert.

1. Organisatorische Bereitschaft

Einführung von Sicherheitsmaßnahmen zur Entwicklung, Integration und Wartung sicherer Produkte und Lösungen. Dies betrifft die gesamte Organisation in Form von definierten Rollen, klaren Verantwortlichkeiten, angemessener Qualifikation, Richtlinien, Prozessen und Kommunikation. Die Informationssicherheitsrichtlinien bei Siemens entsprechen der Norm für Informationssicherheitsmanagementsysteme ISO/IEC 27001. Der Geschäftsbereich Siemens Digital Grid (SI DG) ist zertifiziert für die Konformität nach ISO/IEC 27001:2013, wobei der Geltungsbereich die Entwicklung, die Produktion, das Engineering, den Vertrieb und den Service seiner Produkte, Systeme und Lösungen umfasst.

2. Sichere Entwicklung

Die sichere Entwicklung ist ein systematischer Ansatz, um Cybersicherheit in den Produkt- und Lösungsentwicklungszyklus zu integrieren. Sie ist Teil der kompletten Prozesskette, von den Anforderungen an die Cybersicherheit bis hin zur Validierung der Cybersicherheit. Es umfasst auch die Absicherung der IT-Infrastruktur, die für die Entwicklungsorganisation benötigt wird. Bei Siemens Digital Grid entspricht der Zyklus der Sicherheitsentwicklung der Norm IEC 62443-4-1.

3. Sichere Integration und Service

Cybersicherheit ist ein integraler Bestandteil der Siemens-Prozesse zur Bereitstellung von Lösungen für den Kunden. Dieser erhält Lösungen einschließlich Design, Integration und Inbetriebnahme, die gemäß den Best Practices für Cybersicherheit ausgeführt werden und eine optimale Unterstützung für einen sicheren Betrieb gewährleisten. Bei Siemens Digital Grid ist der sichere Integrations- und Serviceprozess gemäß der Norm IEC 62443-2-4 zertifiziert.

4. Umgang mit Schwachstellen und Vorfällen

Bei der Behandlung von Schwachstellen und Störungen handelt es sich um den Prozess, der definiert, wie ein Unternehmen auf Sicherheitslücken und -vorfälle reagiert und damit umgeht, einschließlich der damit verbundenen internen und externen Kommunikation. Der Prozess bildet bei Bedarf auch eine Schnittstelle zur regelmäßigen Schwachstellenüberwachung und Patch-Entwicklung im Rahmen der Produkt- oder Lösungsentwicklung.

Abbildung 2: Kategorien von Cybersicherheitsmaßnahmen von Siemens

Siemens verfügt über ein eigenes Computer Emergency Response Team (CERT). Das Siemens ProductCERT-Team ist mit der Überwachung und Analyse von Sicherheitsproblemen beauftragt und veröffentlicht in Zusammenarbeit mit den jeweiligen Siemens-Organisationseinheiten produktbezogene Gutachten zu Schwachstellen und damit verbundene Empfehlungen zur Risikominderung. Darüber hinaus prüft das Siemens ProductCERT mit seiner anerkannten Expertise in Penetrationstests Siemens-Produkte und im Siemens-Portfolio eingesetzte Komponenten von Drittanbietern mittels gezielter Hackerangriffe auf Schwachstellen und leitet daraus Empfehlungen für Implementierungshilfen für die jeweiligen Siemens-Organisationseinheiten ab.

5. Sichere Systemarchitektur

Eine Cybersicherheitsarchitektur muss nicht nur die regulatorischen Anforderungen unterstützen, sondern sollte auch Sicherheit durch Design bieten. Der Schutz des Stromnetzes erfordert einen Defense-in-Depth-Ansatz, der sich mit Cyber-Risiken befasst und den sicheren Betrieb durch Menschen, Prozesse und Technologien unterstützt. Die Architektur ist der sichtbarste Teil eines umfassenden Cybersicherheitskonzepts. Sie bildet die Grundlage für die Anwendung weiterer Maßnahmen bei Menschen, Prozessen und Produkten, wie sie in diesem Cybersicherheitsrahmen definiert sind.

6. Systemhärtung

Systemhärtung (engl. „System Hardening“) reduziert die Angriffsfläche der Produkte und Lösungen durch eine sichere Konfiguration. Dies wird z.B. durch das Entfernen unnötiger Software, unnötiger Benutzernamen oder Logins, das Sperren ungenutzter Ports oder die Härtung des Betriebssystems erreicht. Siemens stellt Richtlinien für Produkte und Systeme zur Härtung zur Verfügung und kann Betreiber bei der Härtung ihrer Infrastruktur unterstützen.

7. Zugriffskontrolle und Kontoverwaltung

Zugriffskontrolle ist die selektive Beschränkung des Zugriffs auf Produkte, Lösungen oder Infrastrukturen durch die Authentifizierung von Benut-

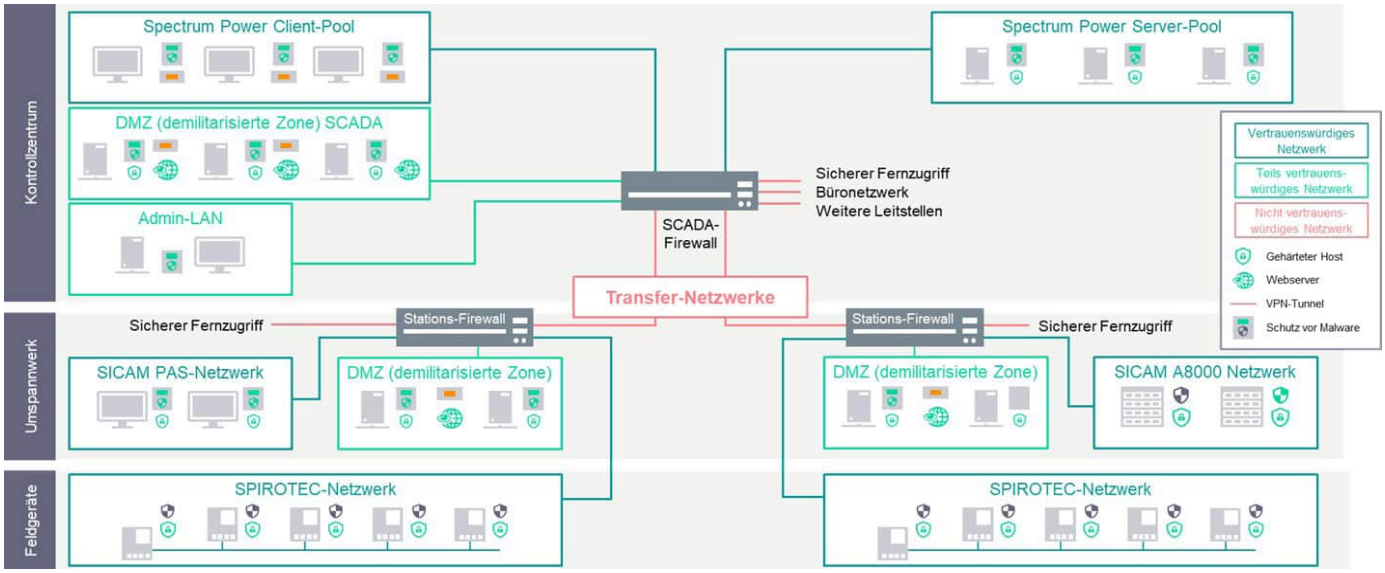


Abbildung 3: Cybersecurity-Architektur

zern (und Systemen) und deren Autorisierung durch die Gewährung entsprechender Berechtigungen. Account Management ist die Definition verschiedener Benutzerkonten mit geeigneten Privilegien, die am besten zentralisiert mit einheitlichen Sicherheitsrichtlinien durchgeführt wird. Siemens kann Anlagenbetreiber bei der Konzeption und Implementierung eines zentralen und hierarchischen Zugangskontroll- und Account-Management-Systems unterstützen. Netzbetreiber können die Produkte und Lösungen von Siemens Digital Grid neben den Produkten anderer Anbieter nahtlos in ihre zentralen User-Management-Lösungen integrieren.

8. Sicherheitsprotokollierung/-überwachung

Sicherheitsprotokollierung/-überwachung bedeutet, dass alle sicherheitsrelevanten Aktivitäten im System erfasst und überwacht werden, einschließlich der Aktivitäten von Benutzerkonten wie An- und Abmeldung oder fehlgeschlagene Anmeldeversuche. Alarme werden gemeldet und entsprechend weiterverfolgt. Siemens-Produkte und -Lösungen unterstützen die zentrale Protokollierung von Sicherheitsereignissen und Alarmen mit Hilfe des Syslog-Messaging-Standards und bilden damit die Grundlage für anspruchsvolle SIEM-Lösungen (Security Information and Event Management).

9. Sicherheits-Patches

Die Verwaltung von Sicherheitspatches umfasst die Überwachung der Schwachstellen aller in einem Produkt oder einer Lösung verwendeten Softwarekomponenten (eigene sowie von Drittanbietern), die Klassifizierung der Schwachstellen und der verfügbaren Patches, die Prüfung der Kompatibilität der Sicherheitspatches und, falls erforderlich, die Entwicklung zusätzlicher Sicherheitspatches zur Behebung von Inkompatibilitäten. Bei einer Lösung umfasst dies die Lieferung und Wartung eines Systems mit einem aktuellen Sicherheits-Patch-Level. Siemens bietet Betreibern von Energieautomatisierungssystemen umfassende Patch-Management-Dienstleistungen an.

10. Schutz vor Malware

Der Schutz eines Produkts oder einer Lösung vor Malware wird durch die Unterstützung geeigneter Malware-Schutzlösungen (z.B. klassisches Antivirus, Application Whitelisting oder Software Signing) und geeigneter Verfahren sichergestellt, die gewährleisten, dass alle Systeme vor aktueller Malware geschützt sind. Siemens verfügt über einen Malware-Schutz für Schlüsselkomponenten in der Energieautomatisierung, bietet technische Lösungen für den Malware-Schutz an und unterstützt Kunden bei der Einrichtung eines sicheren Update-Prozesses für Antiviren-Muster.

11. Sicherung und Wiederherstellung

Datensicherung ist der Prozess des Kopierens und Archivierens von Software, Konfigurationsdaten und Betriebsdaten, sodass ein Produkt oder eine Lösung wiederhergestellt werden kann, z. B. nach einem Datenverlust. Dazu gehören auch geeignete Maßnahmen und Verfahren für die Notfallwiederherstellung. Siemens verfügt über Sicherungs- und Wiederherstellungs-Konzepte und unterstützt Systembetreiber bei der Bewertung und Etablierung entsprechender Verfahren.

Sicherung und Wiederherstellung ist die Basis für einen Notfallwiederherstellungs-Prozess auf Betreiberseite.

12. Sicherer Fernzugriff

Sicherer Fernzugriff im Zusammenhang mit Energieautomatisierungssystemen ist der verschlüsselte, authentifizierte und autorisierte Zugriff auf Leitstellen- und Umspannwerksanlagen von entfernten Standorten aus über potenziell nicht vertrauenswürdige Netzwerke. Siemens bietet eine nach ISO/IEC 27001 zertifizierte Lösung für den sicheren Fernzugriff an, die auf die Bedürfnisse von Energieanlagenbetreibern zugeschnitten ist.

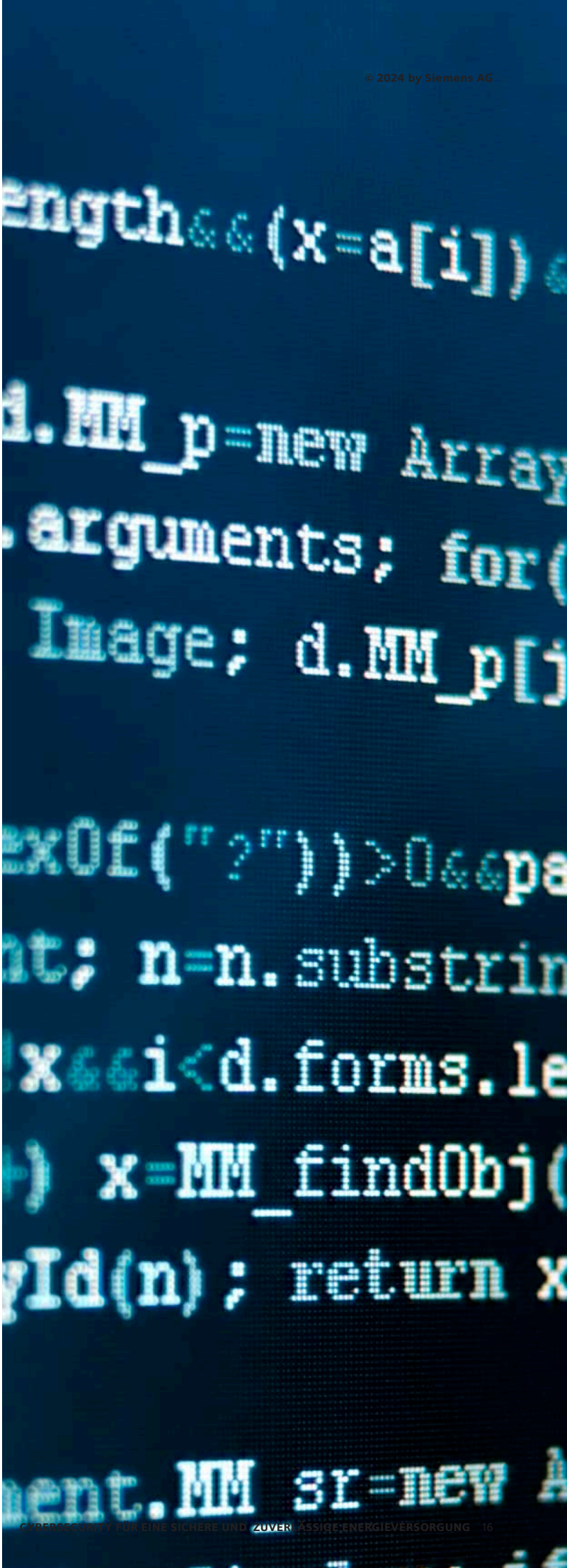
Abbildung 3: Cybersecurity-Architektur

13. Datenschutz und Integrität

Der Datenschutz gewährleistet den Schutz aller sensiblen Daten im System, sowohl im Ruhezustand als auch während der Übertragung. Diese Daten dürfen nur für befugte Personen oder Prozesse zugänglich sein. Darüber hinaus muss auch die Integrität der Daten und der Kommunikation über das System sowie die Verfügbarkeit der Daten durch geeignete Methoden sichergestellt werden. Siemens-Komponenten unterstützen die erforderliche Funktionalität, um die Anforderungen an Datenschutz und Integrität zu erfüllen, während die bei Siemens implementierten Prozesse sicherstellen, dass die Kundendaten in allen Phasen der Kundenprojekte mit der gebotenen Sorgfalt verwaltet werden.

14. Schutz persönlicher Daten

Dadurch wird sichergestellt, dass die Nutzer selbst bestimmen können, wann, wie und in welchem Umfang Informationen über sie gesammelt, verwendet und mit anderen geteilt werden. Der Datenschutz ist ein besonders sensibles Thema, wenn personenbezogene Daten erhoben werden, wie z. B. bei Smart-Metering-Anwendungen. Das Siemens-Portfolio hilft Betreibern, die damit verbundenen regulatorischen Anforderungen wie die General Data Privacy Regulation (GDPR) in der Europäischen Union zu erfüllen.



KAPITEL 3

Betriebssicherheit

Bei der Betriebssicherheit wird das Zusammenspiel der „3 Ps“ offensichtlich: Produkte und Systeme, Personen und Organisationen müssen gemäß definierter Prozesse zusammenarbeiten. Zu den wichtigsten Maßnahmen, um die Betriebssicherheit gewährleisten zu können, gehören etwa das Sicherheitspatch-Management, die Zugangskontrolle und Kontenverwaltung, die Sicherheitsprotokollierung und -überwachung sowie der Schutz vor Schadsoftware. Sie sind erforderlich, um eine Umgebung einzurichten, die Schutz bietet, Angriffe erkennt, in der alle mit dem Betrieb eines Energienetzes zusammenhängenden Aktionen zuordenbar und nachvollziehbar sind und Korrekturmaßnahmen durchgeführt werden können. Siemens unterstützt die Betriebssicherheit durch die Einhaltung internationaler Normen.

1. Umgang mit Schwachstellen und Vorfällen

Der Umgang mit Schwachstellen und Zwischenfällen ist eine der zwingenden Voraussetzungen für den Schutz des Energienetzes und umfasst die Definition von Gegenmaßnahmen, falls erforderlich, und die Kommunikation mit dem Betreiber, um ihn angemessen über relevante Schwachstellen, Umgehungsmöglichkeiten und verfügbare Patches zu informieren (siehe **Abbildung 4)**. Dies ermöglicht es den Netzbetreibern, die bereitgestellten Sicherheitshinweise zu analysieren und Gegenmaßnahmen effektiv zu definieren und anzuwenden.

Genauso wie der Umgang mit Schwachstellen den Schutz des Unternehmens unterstützt, geht es bei der Behandlung von Zwischenfällen darum, auf Cyber-Vorfälle zu reagieren und sich von diesen effektiv zu erholen. Obwohl die Sicherheitsmaßnahmen, die für die Behandlung von Zwischenfällen erforderlich sind, den Maßnahmen für die Behandlung von Schwachstellen ähneln, erfordert sie eine entsprechende organisatorische Vorbereitung für die effektive Behandlung von Zwischenfällen.

2. Sicherheitspatch-Management

Eine der wichtigsten Aktivitäten im Bereich der Cybersicherheit ist das Patchmanagement. Aufgrund der zunehmenden Vernetzung ist die

Abbildung 4: Aufgaben und Fähigkeiten, die für den Umgang mit Sicherheitsrisiken erforderlich sind

Gefahr, dass Angreifer bekannte Schwachstellen ausnutzen, enorm gestiegen.

Normen wie ISO/IEC 27002 und IEC 62443-2-3 geben Betreibern eine Anleitung, wie sie angemessene Maßnahmen für einen Patch-Management-Prozess umsetzen können. Eine Zusammenfassung der empfohlenen Prozessschritte für Betreiber sind:

- Durchführung einer kompletten Asset-Inventur
- Prüfung verfügbarer Patches
- Prüfung der Kompatibilität
- Prüfung in einer Umgebung, die der Produktionsumgebung entspricht
- Erstellung eines Zeitplans für die Patch-Installation
- Installation von Patches oder schadensmindernden Maßnahmen
- Aktualisierung der Asset-Datenbank

Ebenso sind in Normen wie IEC 62443-2-3 und IEC 62443-2-4 definierte Anforderungen an Systemhersteller zum Patch-Management festgelegt:

- Bereitstellung einer Dokumentation über die Patch-Management-Richtlinien für Komponenten und Systeme
- Verifizierung von Patches hinsichtlich Kompatibilität und Anwendbarkeit für eigene und fremde Komponenten
- Bereitstellung der Patch-Informationen und Patches für den Betreiber
- Bereitstellung von Lifecycle-Informationen für Produkte und Systeme einschließlich End-of-Life-Informationen.

Siemens begegnet diesen Anforderungen mit einem umfassenden Patch-Management-Prozess für Produkte und Systeme.

Dazu gehört ein regelmäßiger Patch-Test für eigene und Drittanbieter-Komponenten und die Bereitstellung der Testergebnisse für die Kunden. Dabei wird das Siemens-interne CERT für eine umfassende Schwachstellen-Überprüfung und die Kommunikation von Schwachstellen und Gutachten für alle Siemens-Produkte genutzt, siehe Kapitel 2 Punkt 4. Zusätzlich stellt Siemens als Voraussetzung für einen Patch-Management-Prozess eine Sicherungs- und Wiederherstellungs-Dokumentation auf Produkt- und Systemebene zur Verfügung.

Ein vereinfachter Prozess ist in **Abbildung 5** dargestellt, mit den anfänglichen Aktivitäten und den zyklischen Aktivitäten eines vollständigen Patch-Management-Prozesses aus der Sicht des Betreibers.

Zu den anfänglichen Aktivitäten gehören die Migration auf ein sicheres System, die Definition der in den Geltungsbereich aufzunehmenden Assets und die Aufbereitung der Asset-Daten, die für die Durchführung des Patch-Managements erforderlich sind (Schritte 1 und 2).

Die wiederkehrenden Aktivitäten beginnen mit dem Sammeln von Patch-Informationen auf der Grundlage des Asset-Inventars (Schritt 3) und einer Entscheidung, welche, ob und wann Patches installiert werden müssen (Schritt 4); entsprechend folgen die Patch-Validierung (Schritt 5) und die Patch-Installation (Schritt 6). Schließlich müssen die Asset-Daten aktualisiert werden (Schritt 7).

Siemens bietet umfassende Patch-Management-Services für Produkte und Systeme an, um die aus der ISO/IEC 27001 abgeleiteten regulatorischen Anforderungen auf Basis aller Prozessschritte zu erfüllen. Diese Services beinhalten optional die Meldung von Schwachstellen und die Erstellung von Berichten für OT-Systeme des Kunden, einschließlich Produkten von Drittanbietern (Router, Switches, Komponenten von Umspannwerken).

Für die Verwaltung der Patch-Management-relevanten Assetdaten bietet Siemens OT Companion als cloud-basierte IoT-Anwendung an. Diese ermöglicht die kontinuierliche OT Asset Bestandsaufnahme und unterstützt den betreiberseitigen Patch-Management-Prozess.

Der Service wird in Übereinstimmung mit den Normen IEC 62443-2-3 und IEC 62443-2-4 angeboten.

3. Benutzerverwaltung und Zugangskontrolle

Das Grundprinzip der Zugangskontrolle ist in **Abbildung 6** dargestellt. Die Zugangskontrolle stellt sicher, dass Benutzer (und Systeme) nur wie vorgesehen mit Ressourcen interagieren können. Dies ist nur möglich, wenn der Benutzer authentifiziert ist, d.h. wenn überprüft wird, dass der Benutzer derjenige ist, der er vorgibt zu sein, und wenn er autorisiert ist, d.h. wenn überprüft wird, dass der Benutzer die Operation ausführen darf, die er mit/auf den Ressourcen durchführen will.

Die Identitätsverwaltung ist die Vertrauensbasis in dieser Pyramide, da sie die zu kontrollierende Benutzer und Berechtigungsnachweise verwaltet. Der Vollständigkeit halber sei darauf hingewiesen, dass die Zugangskontrolle nicht nur die Benutzer, sondern auch alle Ressourcen wie Geräte oder Anwendungen berücksichtigt.

Die Zugangskontrolle ist in allen Lebenszyklusphasen (von der Inbetriebnahme über den Betrieb und die Renovierung bis zur Stilllegung) von

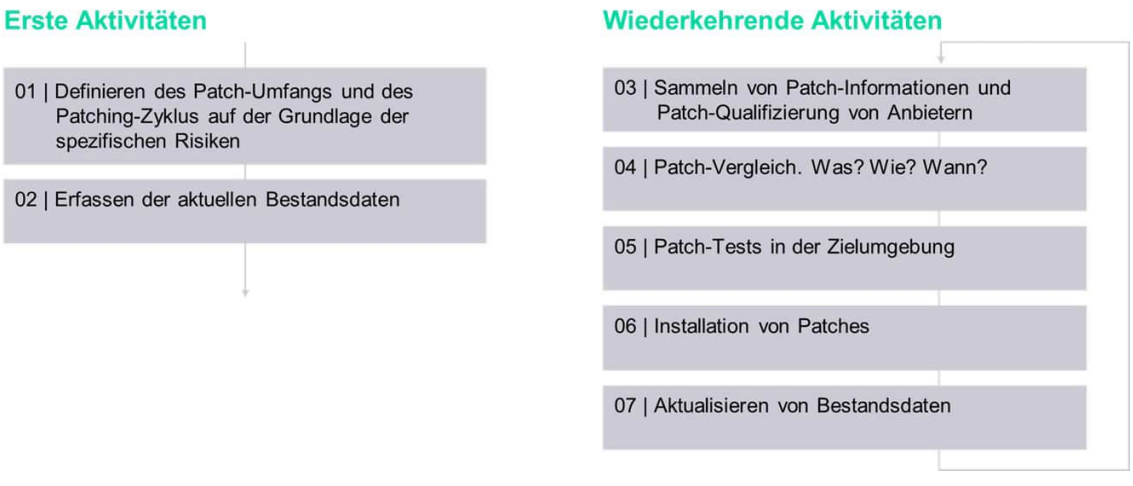


Abbildung 5: Vereinfachter Patch-Management-Prozess

Systemen und Netzen von Bedeutung. Die wichtigste Phase für die Cybersicherheit ist die des täglichen Betriebs. Typische Zugangskontrollszenarien sind physischer Zugang, HMI-Zugang, IED-Zugang, Fernzugriff usw.. Zusätzlich werden aus Sicherheitsgründen Notfallzugangswege definiert, um autorisiertem Personal in Zeiten ungeplanter Nichtverfügbarkeit der regulären Zugangskontrollmechanismen Zugang zu gewähren.

Es gibt mehrere Möglichkeiten, die Zugangskontrolle im Stromnetz mit unterschiedlichen Tiefen und Sicherheitsstufen zu realisieren. Eine typische Lösung für einen zentralisierten Ansatz ist die Verwendung von LDAP- oder RADIUS-Servern, um Identitäten zu verwalten. Die Authentifizierung und Autorisierung kann über eine Passwortverifizierung oder über eine Public Key Infrastructure (PKI) mit X.509-Zertifikaten erfolgen. Die Zugriffsrechte werden durch das System oder das Gerät definiert, da sie für diese Geräte auf der Grundlage der bereitgestellten Betriebsfunktion spezifisch sind.

Moderne Energieautomatisierungsprodukte und -systeme verwenden eine zentrale Benutzerverwaltung, um eine rollenbasierte Zugriffskontrolle auf der Grundlage von Standards wie IEC 62351-8 zu implementieren. Siehe **Abbildung 7** für eine Lösungsvariante.

Ein Benutzer beantragt über ein Gerätemanagement-Tool Zugang zu einem IED (1). Der IED

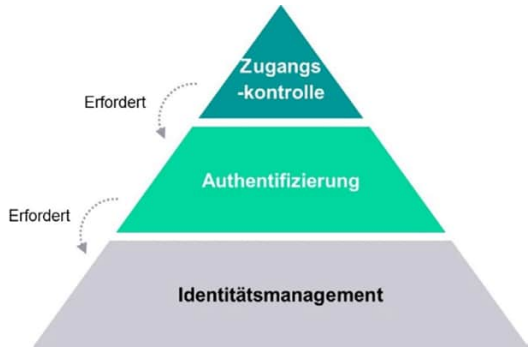


Abbildung 6: Identitäts- und Zugangs-Management – Das Grundprinzip

sendet diese Anfrage an den zentralen Benutzerverwaltungsserver zur Authentifizierung des Benutzers (2). Der Server antwortet mit dem Ergebnis der Authentifizierung, einschließlich der dem Benutzer zugewiesenen Rolle(n) im Falle einer erfolgreichen Authentifizierung (3). Wurde der Benutzer vom Server erfolgreich authentifiziert, leitet das IED die rollenbasierte Benutzersitzung ein (4).

Aufgrund der Multi-Vendor-Umgebung von Stromnetzen ist ein standardisierter Ansatz auf der Grundlage von IEC 62351 für eine effektive Implementierung der Zugangskontrolle von entscheidender Bedeutung, um die Interoperabilität zu unterstützen.

Es ist wichtig, Übergangstechnologien und -tools in Betracht zu ziehen, die die Beschränkungen der alten Sekundärtechnik berücksichtigen, die in den kommenden Jahren weiterhin den Großteil der

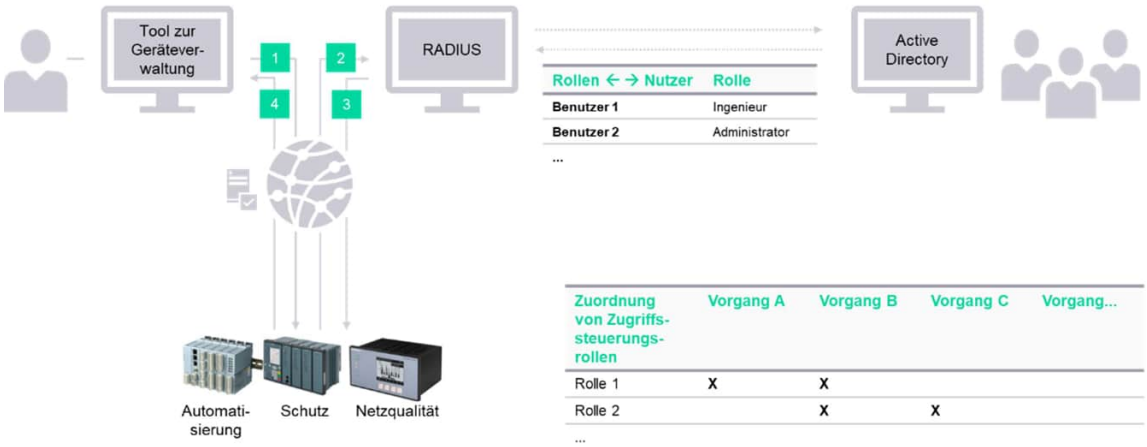
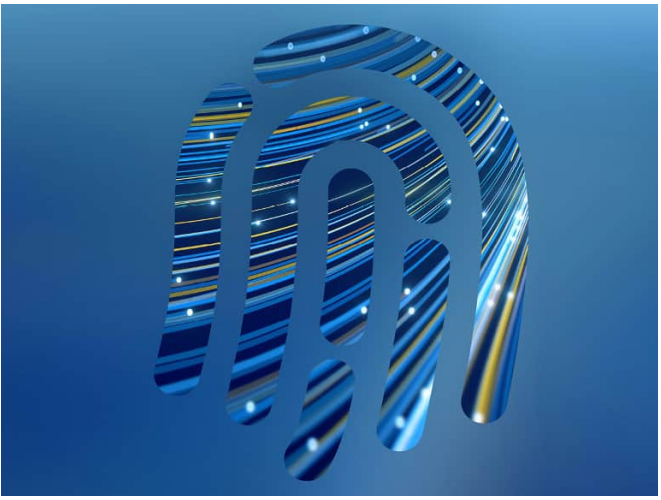


Abbildung 7: Beispiel für eine rollenbasierte Zugangskontrolle

installierten Basis ausmachen wird. Herstellerübergreifende, proprietäre Zugangsverwaltungslösungen für Sekundärgeräte der älteren Generation können neben Standard-Benutzerverwaltungssystemen eingesetzt werden, um die Lücke bei der Verwaltung von Benutzern und Rechten sowohl für Installationen der älteren als auch der neueren Generation zu schließen.

4. Verwaltung von Sicherheitsinformationen und -ereignissen

Der Schutz eines Energieautomatisierungssystems allein ist nicht ausreichend. Angriffsversuche auf die Systeme müssen frühzeitig erkannt werden, damit geeignete Maßnahmen ergriffen werden können, bevor die Funktionen der Systeme durch den Angriff beeinträchtigt werden. Internationale Normen wie IEC 27001, IEC 62443 und Branchenempfehlungen wie das BDEW-Whitepaper behandeln auch die Themen "Logging" und "Logging und Monitoring".



Seit dem Frühjahr 2021 fordert auch das deutsche IT-Sicherheitsgesetz (IT-SiG 2.0) für Betreiber kritischer Infrastrukturen den Einsatz von "Systemen zur Angriffserkennung". Als Präzisierung dieser gesetzlichen Regelung hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im September 2022 ein Dokument veröffentlicht, welches diese Anforderung näher beschreibt (BSI: "Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung", gemäß § 8a Absatz 1a BSIG bzw. § 11 Absatz 1e EnWG).

Eine manuelle Auswertung der Informationen ist in einem modernen Energieautomatisierungssystem aufgrund der schieren Menge der von den überwachten Systemen generierten Log-Events nicht möglich. Die Erfüllung dieser Überwachungsanforderungen erfordert die Implementierung einer automatischen Auswertung der Informationen. Die Lösung hierfür ist ein Security Information and Event Management System - SIEM.

Ein SIEM sammelt alle sicherheitsrelevanten Logs aus allen Komponenten des Systems und speichert sie unveränderbar in chronologischer Reihenfolge. Die sicherheitsrelevanten Ereignisprotokolle der Komponenten der Energieautomatisierung werden über das "syslog"-Protokoll an einen Syslog-Server zur standortbezogenen Persistenz und zum Schutz der Ereignisinformationen gesendet. Der Syslog-Server auf Unterstationsebene fungiert als Puffer gegenüber dem zentralen SIEM. Unter Berücksichtigung einiger Einschränkungen hinsichtlich der Verfügbarkeit ist es auch möglich, die Syslog-Informationen von den Komponenten direkt an das zentrale SIEM-System zu senden.

Die sicherheitsrelevanten Informationen unterscheiden sich je nach Art der Komponente. Im Allgemeinen werden Ereignisse wie Anmeldeversuche, Konfigurationsänderungen und die Erkennung von potenzieller Malware gemeldet. Eine Firewall zum Beispiel protokolliert zusätzlich den blockierten Datenverkehr. Alle Informationen werden im SIEM kombiniert und ausgewertet, um ein anormales Verhalten des Systems zu korrelieren und zu erkennen. Stellt das SIEM einen Angriff oder eine Anomalie fest, wird eine Alarmmeldung ausgegeben und der Betreiber informiert, zum Beispiel per E-Mail. Die Syslog-Informationen werden im SIEM gespeichert, so dass sie nach einem Cybervorfall für eine forensische Analyse verwendet werden können. Ein SIEM kann Berichte über Sicherheitsereignisse erstellen, die eine bestimmte Störung oder einen bestimmten Zeitraum abdecken.

Architektur

Das Protokollierungssystem sammelt die Informationen über Sicherheitsereignisse in den Umspannwerken und in den Leitstellen in lokalen Syslog-Server-Installationen. Die Informationen werden dann von den lokalen Syslog-Servern an das zentrale SIEM-System übertragen.

Die Protokolle werden auf den lokalen Syslog-Servern zwischengespeichert. Sollte das SIEM aufgrund von Kommunikationsproblemen nicht erreichbar sein, sind die Protokolle dennoch lokal an jedem überwachten Standort verfügbar.

Dies gewährleistet eine schlanke, gesicherte und verschlüsselte Schnittstelle von den Automatisierungssystemen zum SIEM für die Übertragung von Sicherheitsereignissen

Dies vereinfacht es, die Daten in Zukunft auf andere oder zusätzliche Systeme zu übertragen, ohne in die bestehende Infrastruktur einzugreifen

Randbedingungen

Die wesentlichen Komponenten des Energieautomatisierungssystems müssen die sicherheitsrelevanten Ereignisse erkennen, die zugehörigen Informationen aufzeichnen und über das Syslog-Protokoll zur Verfügung stellen. Die Siemens-Komponenten für Energieautomatisierung und Kommunikation wie SIPROTEC 5,

SICAM A8000 und Ruggedcom erfüllen diese Anforderungen.

SIEM-as-a-Service

Neben den On-Premise-SIEM-Lösungen (s. **Abbildung 8)** bietet Siemens auch SIEM-as-a-Service-Lösungen an (s. **Abbildung 9)**. Die allgemeinen Komponenten im Umspannwerk oder in der Leitstelle sind die gleichen. Der Unterschied liegt lediglich im Standort des SIEM-Systems. Anstatt das SIEM in einem Rechenzentrum des Kraftwerksbetreibers zu installieren, wird das SIEM in einer gesicherten Cloud-Umgebung installiert, die von Siemens verwaltet wird.

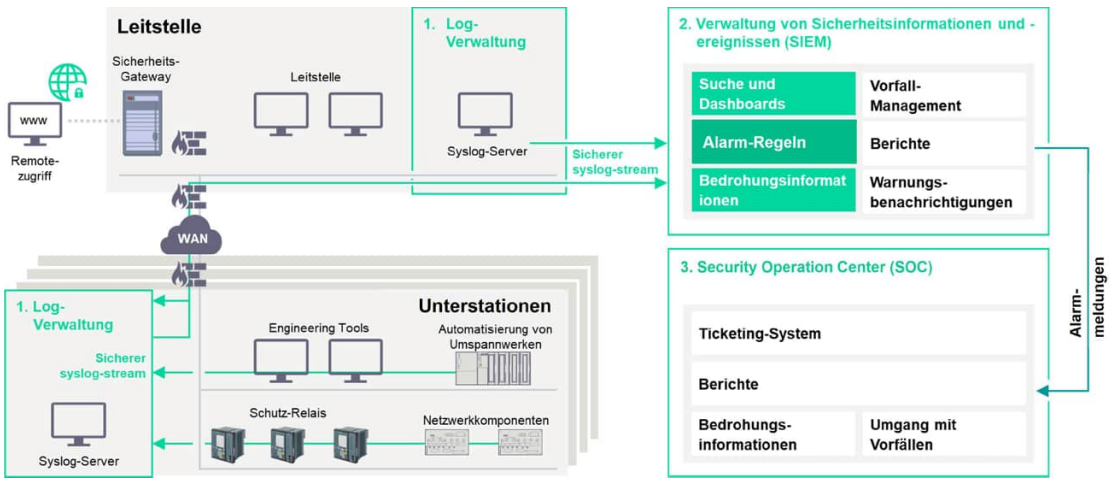


Abbildung 8: SIEM On-Premise-Lösung

Die Hauptvorteile eines SIEM-as-a-Service sind:

- Kein Aufwand für die Administration des SIEM-Hostings auf Betreiberseite
- Hohe Verfügbarkeit
- Skalierbar
- Sicherheitspatches und Software-Updates für die gehostete SIEM-Infrastruktur werden von Siemens verwaltet.

Eine gesicherte Kommunikation von den OT-Systemen zur Cloud-Infrastruktur ergänzt die Gesamtsicherheit.

SIEM-as-a-Service besteht aus:

- SIEM mit Analyse- und Alarmierungsfunktionalitäten, die als Cloud-Service auf Kundenbasis bereitgestellt werden
- SIEM-Readiness Upgrade Ihrer zu überwachenden operativen Systeme

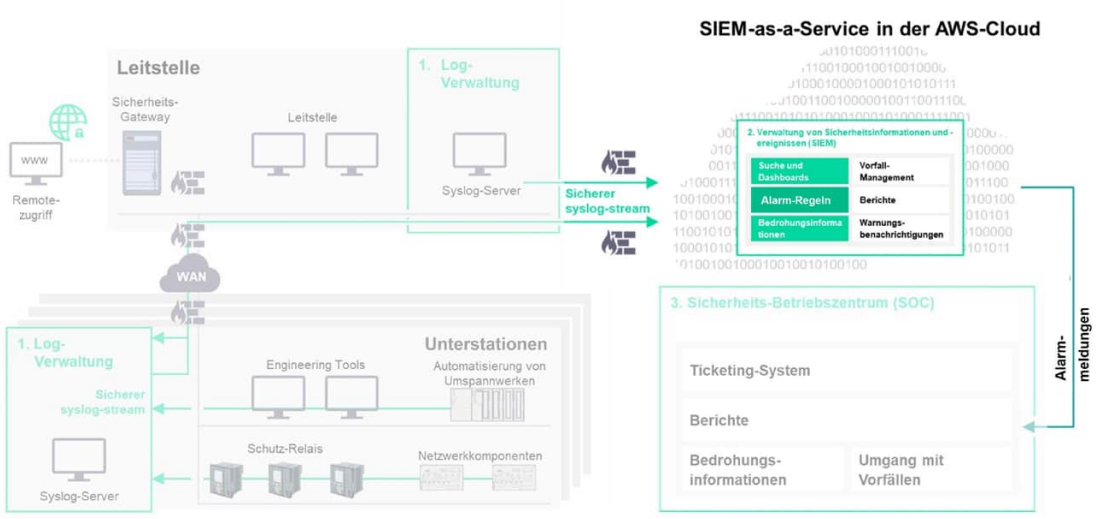


Abbildung 9: SIEM-as-a-Service-Lösung

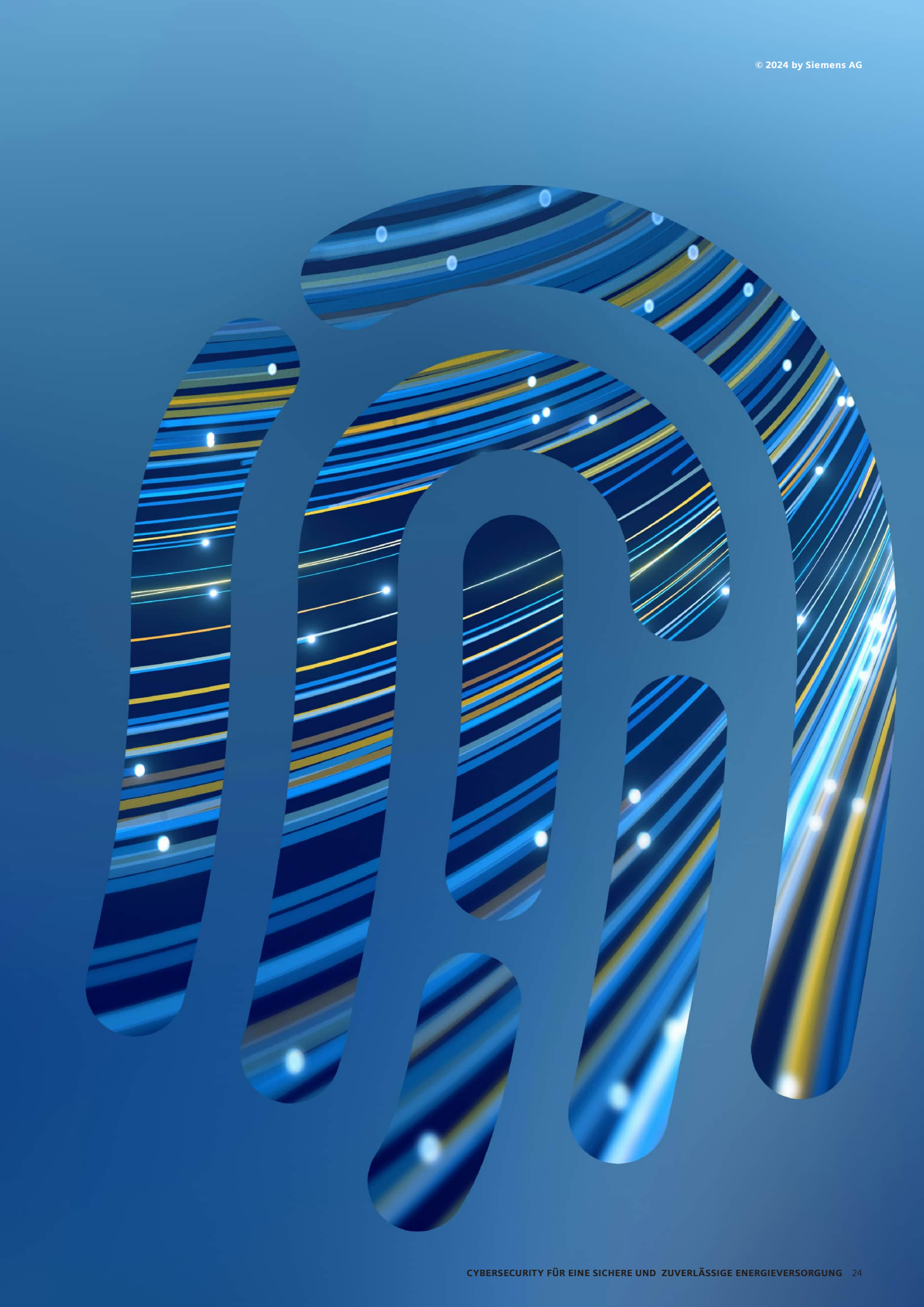
Eine Cloud-Lösung muss die gleichen Sicherheitsanforderungen erfüllen wie eine On-Premise-Lösung. Für die SIEM-as-a-Service-Lösung ist eine State-of-the-Art-Sicherheit unerlässlich. Die Grundlage bildet die Cloud-Infrastruktur von Amazon Web Services (AWS), die mit den Best Practices der Cloud Security Alliance (CSA) für die Gewährleistung der Sicherheit im Cloud Computing übereinstimmt (**Abbildung 9**).

Weiterhin sind die verwendeten AWS-Rechenzentrumsinfrastrukturen BSI-C5 testiert (BSI C5: Cloud Computing Compliance Controls Catalogue).

Link: https://aws.amazon.com/de/compliance/bsi-c5/

- Implementierung von Alarmregeln im SIEM-System
- Regelmäßige Aktualisierung und Anpassung der Alarmregeln an sich entwickelnde Cyberbedrohungen
- Schulungen zur SIEM-Nutzung für Kundenmitarbeiter

Wenden Sie sich für weitere Informationen an Ihren lokalen Siemens-Partner.



KAPITEL 4

Angewandte Cybersicherheit

Für einen wirksamen Cyber-Schutz sollte auf verschiedenen Ebenen auf Cyber¬Sicherheit hingearbeitet werden. Dieser Abschnitt stellt Best-Practice-Beispiele vor, bei denen die weiter oben beschriebenen Methoden und Sicherheitsmaßnahmen zum Schutz von Produkten und Systemen angewandt wurden. Um Cyber-Sicherheit herzustellen, ist es erforderlich, die Anforderungen zu berücksichtigen, die im Cyber Security Framework festgelegt sind (Abschnitt II), und die betriebsbezogenen Voraussetzungen dafür zu erfüllen (Abschnitt III).

1. Produktsicherheit

Siemens hat für das Portfolio der Energieautomatisierung einen ganzheitlichen Ansatz gewählt, der Prozesse, Kommunikation, Mitarbeiter und Technologien umfasst. Erstens ist die Cybersicherheit in der Organisation durch definierte Rollen, Regeln und Prozesse verankert; eine Governance-Struktur wurde gemäß ISO/IEC 27001 implementiert. Zweitens ist die sichere Produktentwicklung, die sich an einen sicheren Entwicklungslebenszyklusprozess wie IEC 62443-4-1 hält, Teil des Produktlebenszyklusmanagements, das die strengen Anforderungen an die Cybersicherheit erfüllt und eine sichere Produktarchitektur beinhaltet.

Die Produktentwicklung umfasst das sichere Design, beginnend mit Sicherheitsanforderungen, der Implementierung von Software, und die Durchführung systematischer Cybersicherheitstests. Auch die Cybersicherheit der eigenen Infrastruktur spielt eine große Rolle. Die interne

Designdokumentation und der Quellcode müssen vor unbefugtem Zugriff und Manipulation geschützt werden um die Integritätsanforderungen durch die Anwendung von ISO/IEC 27001-Kontrollen zu gewährleisten.

Sicherheitsfähige Energieautomatisierungsprodukte bilden die Grundlage für ein sicheres Energieautomatisierungssystem. Die Anforderungen an die Cybersicherheit der Produkte hängen von verschiedenen Faktoren ab, unter anderem von der beabsichtigten Funktion (Schutz, Steuerung, Bedienung oder Überwachung) und der räumlichen Anordnung der Produkte. Die Sicherheitsfunktionen in modernen Energieautomatisierungsprodukten folgen den allgemeinen Zielen der Cybersicherheit:

Verfügbarkeit, Integrität und Vertraulichkeit und erfüllen die branchenspezifischen Standards. Schutzgeräte der aktuellen Generation können diese Anforderungen erfüllen, siehe **Abbildung 10.** Eine sichere Kommunikation zwischen der Engineering-Software und dem Gerät ist für den sicheren Betrieb entscheidend. Die verschlüsselte Verbindung wird erst nach gegenseitiger Authentifizierung der X.509-Zertifikate des jeweils anderen hergestellt. Kunden können ihre Zertifikate für die Engineering-Software-Installationen aus ihrer eigenen Public-Key-Infrastruktur (PKI) ausstellen, um die Betriebssicherheit zu erhöhen. Siemens bietet hierfür das Produkt SICAM GridPass als Zertifiaktemanagementsoftware an, mit welcher auf einfacher Weise standardkonforme X.509-Zertifikate erstellt und verwaltet werden können. Für die Benutzerauthentifizierung und -autorisierung wird eine rollenbasierte Zugriffskontrolle (RBAC) eingesetzt, die u.a. dem RBAC-Standard IEC 62351-8, dem Standard IEC 62443-4-2, dem BDEW-Whitepaper und den NERC CIP-Empfehlungen entspricht.

Alle sicherheitsrelevanten Ereignisse werden in einem nicht löschbaren Sicherheitsprotokoll und optional über das Syslog-Protokoll an einen zentralen Logging-Server protokolliert. Das Schutzgerät ist mit einem Krypto-Chip ausgestattet, der die kryptographischen Funktionen, einschließlich einer kryptographischen Integritätsprüfung der digital signierten Gerätefirmware in einer geschützten Umgebung, sicherstellt.

Während der Softwareproduktion wird die Firmware mit einer digitalen Signatur versehen, die das Gerät authentifizieren kann, um sicherzustellen, dass die Firmware auf ihrem Weg von den Produktionsanlagen zum Gerät selbst nicht manipuliert wurde. Darüber hinaus ermöglicht das Gerät eine physikalische und logische (V-LAN) Trennung von IP- und Ethernet-basierter Prozess- und Managementkommunikation.

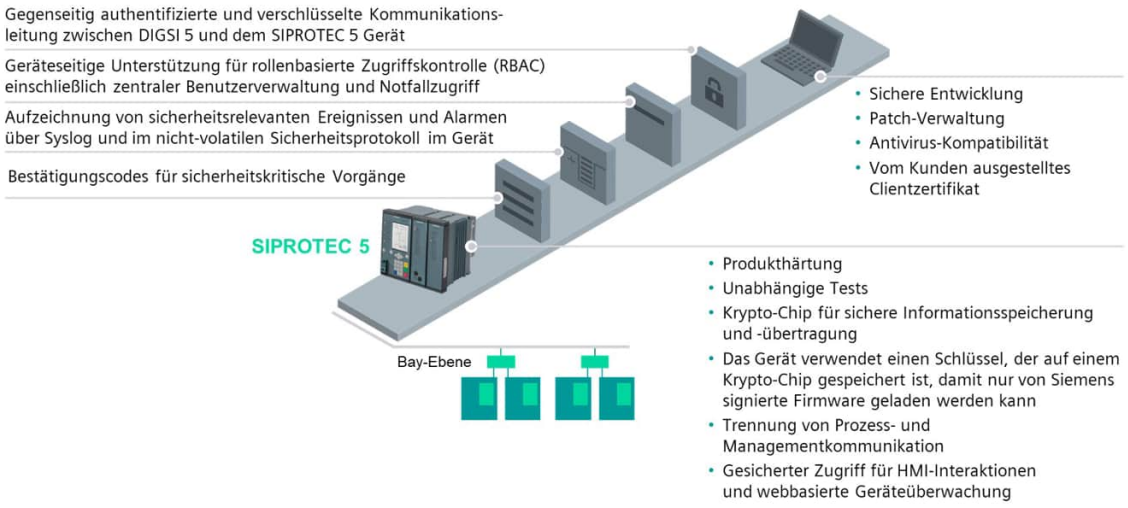


Abbildung 10: Sicherheitsmerkmale eines Schutzgeräts der aktuellen Generation

Geräte, die außerhalb einer physikalisch geschützten Zone kommunizieren, müssen höhere Anforderungen an die Kommunikationssicherheit erfüllen als Geräte, die innerhalb eines physikalisch geschützten Bereichs kommunizieren.

Siemens testet regelmäßig Sicherheitspatches und Virenmuster auf einem Referenzsystem, um zu verifizieren, dass regelmäßige Installationen des Betriebssystems die Verfügbarkeit der Energieautomatisierungsfunktionen nicht beeinträchtigen.

Für Verteilungsautomatisierungsszenarien, in denen es nicht immer möglich ist, adäquate physische Sicherheitsmaßnahmen zum Schutz der Automatisierungsgeräte vor Manipulationen der Prozesskommunikation einzurichten, unterstützen die A8000-RTU-Produkte von Siemens eine Ende-zu-Ende-Verschlüsselung mit TLS und eine Ende-zu-Standort-Verschlüsselung mit IPSec. Die SICAM A8000 RTUs kommunizieren sicher über IEC 61850 MMS/IEC 104/DNP3i-Protokolle mit den Leitstellen und anderen Standorten in Übereinstimmung mit den relevanten Sicherheitsstandards der Prozesskommunikation IEC 62351-3/-4/-5, wie in der **Abbildung 11** dargestellt.

Das RTU/Gateway kann automatisch die erforderlichen Zertifikate von einem normenkonformen CA-Server beziehen, um seine IEC 60870-5-104-, DNP3i- und IEC 61850-MMS-Kommunikation in der Master/Slave- und Client/Server-Rolle abzusichern.

2. Systemsicherheit – Beispiel für ein digitales Umspannwerk

Als Systemintegrator ist Siemens für die sichere Integration von Produkten verantwortlich. Auch diese Aufgabe erfordert dedizierte Prozessbeschreibungen, Richtlinien und technische Beschreibungen, um eine sichere Integration zu gewährleisten. Die Systemkonfiguration erfolgt anschließend gemäß den technischen Beschrei-

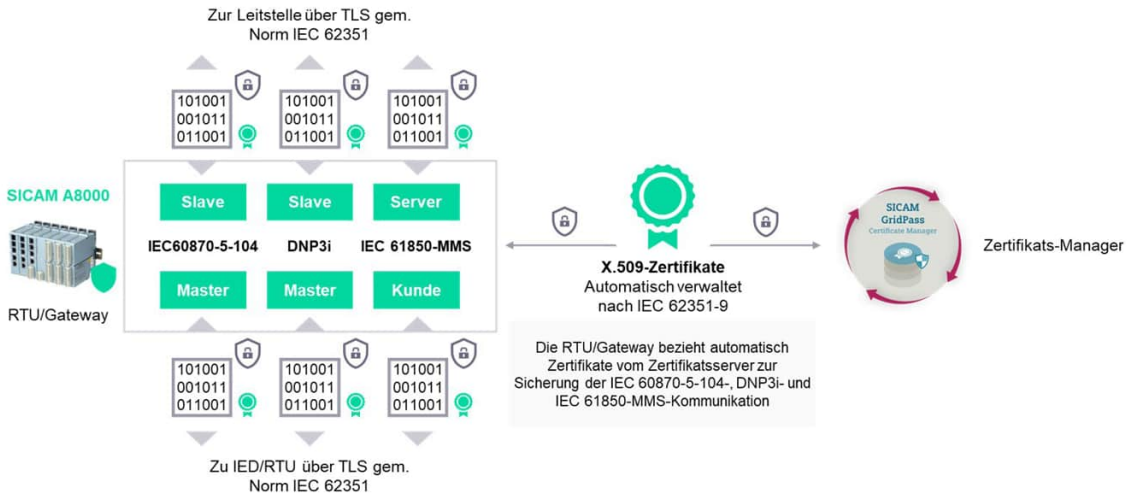


Abbildung 11: Kommunikationssicherheitsfunktionen in einer RTU der aktuellen Generation

bungen. Die Sicherheitsmaßnahmen werden im Rahmen des Factory Acceptance Tests (FAT) und des Site Acceptance Tests (SAT) anhand definierter Testfälle validiert. Der Sicherheitsplan und das Sicherheitsprogramm für sichere Umspannwerke von Siemens Digital Grid (SI DG) sind nach IEC 62443-3-3 bzw. 62443-2-4 zertifiziert.

und unterschiedlicher Technologiegenerationen zusammen. Viele der etablierten Office-IT-Maßnahmen priorisieren die Schutzziele unterschiedlich oder berücksichtigen die speziellen Randbedingungen nur unzureichend. Dies erfordert die Umsetzung von Strategien, die auf die Bedürfnisse der Energieautomatisierung zugeschnitten sind.

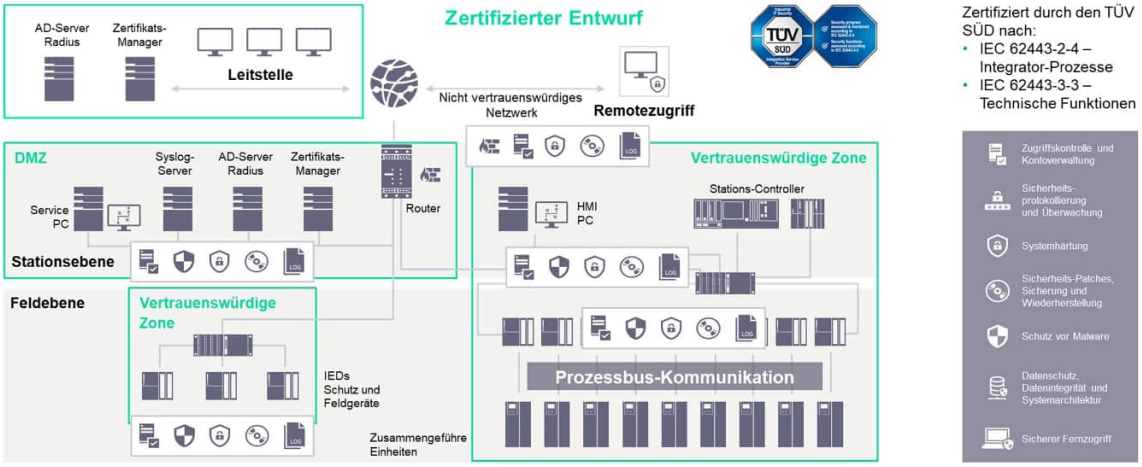


Abbildung 12: Gesichertes digitales Umspannwerk gemäß IEC 62443-3-3 und IEC 62443-2-4

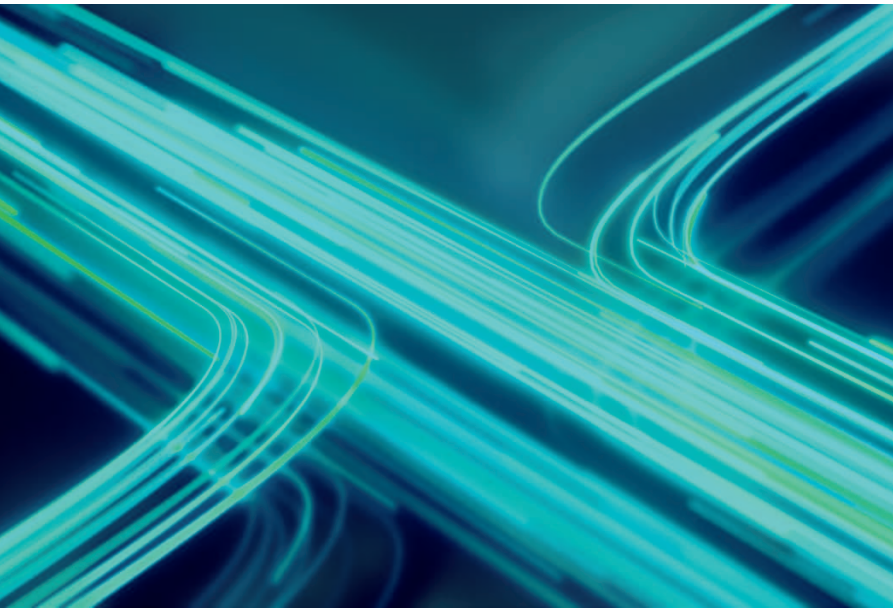
Der zertifizierte Plan für sichere Umspannwerke umfasst ein komplettes digitales Umspannwerk, einschließlich Schutzrelais, RTUs, Kommunikationsgateways, Laufzeit- und Service-PCs, Engineering-Software, Routern, Switches, GPS-Uhren, Logging-Server, Firewall und Intrusion-Detection-System.

Bei Automatisierungssystemen für Umspannwerke unterliegt die Realisierung von Sicherheitsfunktionen einer Reihe von Einschränkungen, wie z. B. der Anforderung der Verfügbarkeit, die einen unterbrechungsfreien 24/7-Betrieb erwarten lässt. Ein Umspannwerk besteht typischerweise aus einer Mischung von PC-basierten und eingebetteten Systemen verschiedener Hersteller mit einer Lebensdauer von bis zu 40 Jahren. Ein Energieautomatisierungssystem setzt sich daher häufig aus verschiedenen Komponenten unterschiedlicher Hersteller, unterschiedlicher Technologien

In **Abbildung 12** sind die Sicherheitsmaßnahmen für ein digitales Umspannwerk dargestellt. Alle Cybersicherheits-Maßnahmen folgen grundsätzlich mindestens den Sicherheitsdesignprinzipien "Defense-in-Depth-Prinzip", "Least-Privilege-Prinzip" und "Netzwerksegmentierung".

Die Netzwerksegmentierung ist ein leistungsfähiger Schutzmechanismus. Der Grundgedanke besteht darin, Netzwerkelemente mit sensiblen Kommunikationsbedürfnissen und ähnlichem Schutzniveau in ein und demselben Subnetz zusammenzufassen. Firewalls filtern den ein- und ausgehenden Verkehr. Diese Zonen werden auch "vertrauenswürdige Zonen" genannt. Es ist nicht erlaubt, die Firewalls zu umgehen. Die vertrauenswürdige Zone ist von außen, von nicht vertrauenswürdigen Netzwerken, nicht zugänglich. Um von außen auf die vertrauenswürdige Zone zugreifen zu können, verwendet Siemens eine "Pufferzone",

die Demilitarisierte Zone (DMZ). Mit diesem Ansatz können die Sicherheitsanforderungen für die interne Kommunikation in der "vertrauenswürdigen Zone" oft auf ein für typische Industriekomponenten praktikables Niveau reduziert werden, verglichen



mit einem größeren Netzwerk, das nicht auf Sicherheitszonen setzt.

Das Prinzip der geringsten Rechte ist die Praxis, den Zugriff auf die minimale Ebene zu beschränken, die die gewünschte Funktionalität ermöglicht. Angewandt auf menschliche Benutzer bedeutet das Prinzip der geringsten Rechte, dass der Benutzer die niedrigste Stufe an Benutzerrechten hat, um in der Lage zu sein, um die gewünschten Aufgaben auszuführen. Das Prinzip wird auch auf alle anderen "Mitglieder" eines Systems wie Geräte, Softwareanwendungen, Dienste und Prozesse angewendet. Das Prinzip wurde entwickelt, um den potenziellen Schaden einer Sicherheitsverletzung zu begrenzen, unabhängig davon, ob sie beabsichtigt oder unbeabsichtigt ist.

Defense in Depth ist der koordinierte Einsatz mehrerer Sicherheitskontrollen zum Schutz eines Systems. Ziel ist es, Redundanz für den Fall bereitzustellen, dass eine Sicherheitskontrolle ausfällt oder eine Schwachstelle in einer Sicherheitskontrolle ausgenutzt wird. Zu den Komponenten der Defence in Depth gehören beispielsweise Sicherheitskontrollen wie Firewalls, Kontoverwaltung, Malware-Schutz und Secure Hardening. Alle Sicherheitsmaßnahmen werden unter Berücksichtigung der allgemeinen Beschränkungen von Automatisierungssystemen für Umspannwerke und der Richtlinien für das Sicherheitsdesign umgesetzt. Die Cybersicherheitsmaßnahmen sind (vgl. Abbildung 2 und Abschnitt II über Sicherheitskategorien):

- Zugangskontrolle und Kontoverwaltung
- Sicherheitsprotokollierung und -überwachung
- Systemhärtung
- Sicherheits-Patches, Backup und Wiederherstellung
- Schutz vor Malware
- Datenschutz, Datenintegrität und Systemarchitektur
- Gesicherter Fernzugriff

Betrachtet man den Malware-Schutz als ein Beispiel für Cybersicherheitsmaßnahmen, so bietet die Implementierung verschiedene Optionen.

Blacklisting/Antivirus

Klassische Antivirenlösungen, die den Inhalt des PC-Dateisystems mit Mustern bekannter Viren vergleichen.

Im Falle einer positiven Übereinstimmung warnt die Antivirensoftware den Benutzer.

Whitelisting von Anwendungen

Eine Whitelisting-Lösung für Anwendungen ist ein Schutzmechanismus, der es nur vertrauenswürdigen Programmen und Anwendungen zulässt, auf einem System ausgeführt werden. Nach der Installation der Systemsoftware und der Anwendungen wird zusätzliche Whitelisting-Software auf dem virenfreien System installiert. Nach Abschluss der Installation wird von der Whitelisting-Lösung eine Whitelist mit Programmen, Anwendungen

und Diensten erstellt. Alle Anwendungen/ Programme/Dienste auf der Liste werden signiert oder durch eine Prüfsumme gesichert. Dadurch wird sichergestellt, dass nur genehmigte Software ausgeführt wird. Heruntergeladene Software oder Viren, die das System nach der Aktivierung des Whitelisting-Schutzes möglicherweise infiziert haben, werden an der Ausführung gehindert.

leistungsstarkes End-to-End-Angebot von Produkten und Lösungen integriert, in welchem Cybersicherheit ein integraler Bestandteil ist.

Bei der Gestaltung der Sicherheitsmaßnahmen in der Leitstellenumgebung werden die Sicherheitsdesignprinzipien "Defense-in-Depth", "Least-Privilege" und "Netzwerksegmentierung" befolgt, wie

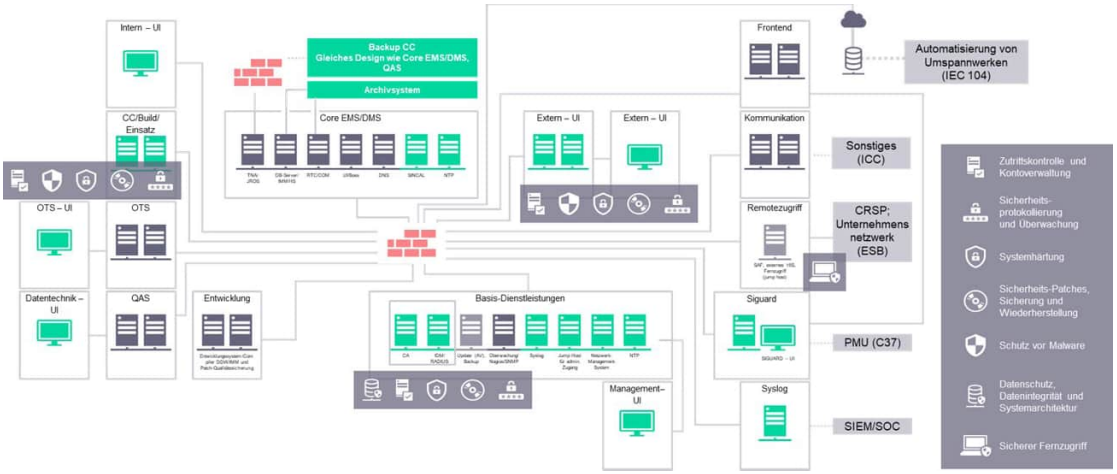


Abbildung 13: Zonierungsstruktur und Kategorisierung der Zonen nach ihrem Schutzbedarf

Alle Windows-basierten PC-Systeme sind mit einem entsprechenden Malware-Schutz ausgestattet. Der Vorteil des Anwendungs-Whitelisting besteht darin, dass es nicht notwendig ist, regelmäßige Pattern-Updates für neu entwickelte Malware sofort zu installieren.

Die Entscheidung, welche Lösung am besten zu den Anforderungen und der Betriebsführung des Anlagenbetreibers passt, muss projekt- oder anlagenspezifisch getroffen werden.

Siemens bietet umfassende Dienstleistungen und Technologien, um Betreiber bei der Definition von Schutzkonzepten für digitale Umspannwerke und der Migration zu einer modernen Architektur und einem Defense-in-Depth-Ansatz zu unterstützen.

3. Sicherung von Leitstellen

Mit Spectrum Power bietet Siemens eine zukunftsweisende Lösung für zentrales und dezentrales Energiemanagement. Spectrum Power ist in ein

bereits im vorherigen Kapitel über Umspannwerke beschrieben.

Siemens stellt einen Systementwurf und die dazugehörige Dokumentation für Spectrum Power zur Verfügung. Um eine tiefgreifende Verteidigung zu gewährleisten, wird empfohlen, das Netzwerklayout in verschiedene Sicherheitszonen aufzuteilen. Teile des Systems, die außerhalb des Kontrollzentrums kommunizieren, befinden sich in separaten DMZs. Im Allgemeinen ist das Spectrum Power-System durch Firewalls in Sicherheitszonen unterteilt, d.h. die Server sind durch Firewalls von anderen Netzwerkzonen oder DMZs getrennt. Dieser Ansatz erhöht nicht nur die effektive Verteidigung, sondern bietet auch Trennungspunkte, um kompromittierte Systemkomponenten oder Zonen zu isolieren. Wenn beispielsweise ein UI-Client oder ein Webserver, der sich in einer DMZ befindet, kompromittiert wird, kann die Firewall zwischen der DMZ und dem Kernsystem

verwendet werden, um Interaktionen und Zugriffe zu blockieren.

Die Zonenstruktur und die Kategorisierung der Zonen nach ihrem Schutzbedarf ist in der **Abbildung 13** dargestellt. Im Allgemeinen definiert die

Komponente mit dem höchsten Sicherheitsanspruch die Sicherheitsstufe aller Komponenten in einer Zone. Das Kernsystem wird als systembetriebskritische Zone mit dem höchsten Schutzbedarf eingestuft.

Das Inter-Control Center Communications Protocol (ICCP) ist ein standardisiertes und weit verbreitetes Protokoll für den Informationsaustausch zwischen Leitzentren. Die ausgetauschten Daten bestehen in der Regel aus Echtzeit-Überwachungs- und Steuerungsdaten des Stromnetzes, einschließlich Messwerten, Fahrplandaten, Energieabrechnungsdaten und Betreibermeldungen. Die ICCP-Anwendung bietet Sicherheit, wie sie von der Internationalen Elektrotechnischen Kommission (IEC Technical Committee 57, Working Group 15 – IEC 60870-6 TASE.2) empfohlen wird. Die sichere ICCP-Funktion umfasst TLS (Transport Layer Security) für die Authentifizierung und Verschlüsselung. Die sichere Version von ICCP von Spectrum Power entspricht dem TASE.2-Standard für sichere Kommunikation.

Sie integriert die Sicherheit der Public Key Infrastructure (PKI) und bietet Unterstützung für eine starke Verschlüsselung und Knotenauthentifizierung.

Die Siemens-Kategorien von Cybersicherheitsmaßnahmen werden in Spectrum Power wie folgt implementiert:

Zugriffskontrolle und Kontoverwaltung

Spectrum Power enthält Funktionen für einen sicheren Benutzerzugriff. Benutzerkonten werden mit Kennworteinschränkungen und Kontosperrung bei wiederholten fehlgeschlagenen Anmeldungen erstellt. Das System ist mit minimierter Verwendung privilegierter Konten aufgebaut. Darüber hinaus definiert das System Berechtigungen nach bestimmten Funktionen.

Sicherheitsprotokollierung/-überwachung

Spectrum Power bietet verschiedene Sicherheits- und Alarmprotokolle zur Erkennung, Meldung und Analyse von elektronischen Sicherheitsvorfällen. Signifikante Sicherheitsereignisse generieren Alarme, die in der Anzeige der Alarm- und Ereigniszusammenfassung angezeigt werden.

Sicherheitsrelevante Alarme und Verbindungsanfragen werden auf der Festplatte in lesbaren, durchsuchbaren Dateien protokolliert.

Datenschutz und Integrität

Siemens-Komponenten unterstützen die erforderliche Funktionalität, um die Anforderungen an Datenschutz und Integrität zu erfüllen, während die bei Siemens implementierten Prozesse sicherstellen, dass Kundendaten in allen Phasen von Kundenprojekten mit der gebotenen Sorgfalt verwaltet werden.

In Spectrum Power wird eine kryptografische Integritätsprüfung eingesetzt. Die Integritätsprüfung umfasst Systemdateien, Anwendungen und Konfigurationsdateien.

Schutz vor Malware

Das empfohlene Antivirenprodukt maximiert den Schutz vor Daten- und Anwendungsbeschädi-

gungen und umfasst eine zentralisierte Verwaltung, Richtliniendurchsetzung, Aktualisierung und Berichterstellung.

Systemhärtung

Härtung reduziert die Angriffsfläche der Produkte und Lösungen durch sichere Konfiguration. Dies wird z.B. durch das Entfernen unnötiger Software, unnötiger Benutzernamen oder Logins, Deaktivieren ungenutzter Ports oder Härtung des Betriebssystems erreicht. Das Design von Spectrum Power 7 folgt dem Prinzip "Security by Default".

Patch-Verwaltung

Siemens bietet umfassende Patch-Management-Services an. Updates werden über eine zentrale Update-Instanz bereitgestellt, die sich in der Zone der Basisdienste befindet und Zugriff auf jede vorhandene Zone hat.

Sicherung und Wiederherstellung

Siemens verfügt über Sicherungs- und Wiederherstellungs-Funktionen und unterstützt Anlagenbetreiber bei der Bewertung und Etablierung entsprechender Prozesse. Spectrum Power verfügt über integrierte Funktionen, wie z. B. Redundanz- und Back-System-Konzepte, um Notfall- und Krisenszenarien auf definierte und getestete Weise zu bewältigen. Dazu gehören Redundanzkonzepte für Komponentenund Back-up-Leitstellen.

Sicherer Fernzugriff

Siemens bietet eine zertifizierte sichere Fernzugriffslösung an, die auf einer zentralen Fernzugriffsplattform namens Siemens cRSP (Common Remote Service Platform) basiert. Das Siemens cRSP ist eine Online-Plattform, die eine starke Authentifizierung und Autorisierung für den Fernzugriff durch Siemens oder den Kunden (unter Verwendung des CWP – Customer Web Portal) auf der Basis von Benutzer-ID/Passwort oder Smartcard-Token (Multi-Faktor-Authentifizierung) durchsetzt.

Privatsphäre

Der Datenschutz ist ein besonders sensibles Thema, wenn personenbezogene Daten erhoben werden, z. B. Protokolldateien. Das Spectrum Power-System bietet Zugangskontrollmechanismen, um „Security by Design“ und das Prinzip des „minimalen need-to-know“ zu befolgen.

KAPITEL 5

Beratung im Bereich Cybersicherheit

Die Cyber-Sicherheit im Energiesektor ist ein weites Thema, bei dem viel bereichsspezifisches Know-how und Erfahrung erforderlich sind, um die geeigneten Maßnahmen festlegen zu können. Siemens unterstützt die Betreiber beim Überprüfen, Festlegen und Umsetzen des Cyber-Schutzes ihrer Systeme, Services und Prozess.

Das Siemens-Beratungskonzept zur Cyber-Sicherheit basiert auf dem bewährten Modell Smart Grid Compass®, das von führenden Siemens-Experten entwickelt wurde und seitdem viele Netzbetreiber weltweit erfolgreich dabei unterstützt hat, sich zu einem „Versorgungsunternehmen der Zukunft“ zu entwickeln.

Wie in **Abbildung 14** dargestellt, gliedert sich die von Siemens angebotene Cybersicherheitsberatung in 4 Phasen:

Orientierung

Umfassende und objektive Analyse des aktuellen Cybersicherheits-Status im Technologie-, Prozess- und Organisationsumfeld

Zielbestimmung

Definition des angestrebten Sicherheitsniveaus auch im Hinblick auf die relevanten regula-

Abbildung 14: Phasen der Cybersicherheitsberatung

torischen Anforderungen und Standards und Ableitung konkreter Sicherheitsmaßnahmen

Routing

Entwicklung einer ganzheitlichen Cybersicherheits-Implementierungs-Roadmap auf Basis der abgeleiteten Maßnahmen und mit Empfehlungen zur Umsetzung

Navigation

Kontinuierliche Unterstützung des Kunden bei der Umsetzung von Sicherheitsmaßnahmen

Systeme mit einem hohen Maß an Schutz vor Cybersicherheits-Angriffen sind realisierbar, wenn Cybersicherheits-Methoden und -Funktionalitäten konsequent implementiert werden.

Siemens kann Betreiber von Energienetzen bei der Bewertung, Definition und Implementierung von Cybersicherheit unterstützen und hat Kunden bei der Implementierung von ISO/IEC 27001 begleitet und Cybersicherheitsbewertungen im Zusammenhang mit dem BDEW-Whitepaper, NERC CIP und anderen Sicherheitsstandards und -richtlinien im Zusammenhang mit Energiesystemen durchgeführt.

Sie haben **Fragen?** Dann wenden Sie sich an unser **Expertenteam**!

Georg Artmeier
Senior Promotor IT/OT-Security

+49 (176) 11728143
georg.artmeier@siemens.com

Sebastian Adelfinger
Promotor IT/OT-Security

+49 (152) 22775114
sebastian.adelfinger@siemens.com

Mark Werbik
Promotor IT/OT-Security

+49 (162) 7162549
mark.werbik@siemens.com

Herausgeber
Siemens AG

Smart Infrastructure
Electrification & Automation
Siemenspromenade 2
91058 Erlangen, Germany