SIEMENS
Ingenuity for life

# Cyber Security im Energie-management

## Auszug aus dem Power Engineering Guide, Ausgabe 8.0

siemens.de/gridsecurity

# Netzsicherheit ist Vertrauenssache

Cyber Security – die Sicherheit in Kommunikations- und IT-Systemen, Stromnetzen sowie anderen digitalen Infrastrukturen – ist ein hochsensibler Bereich. Dafür benötigen Sie einen vertrauenswürdigen Partner: einen Technologiepartner, der versteht, wie die Produkte, Systeme und Lösungen sich mit den Prozessen und Personen im Hintergrund vernetzen.

Wir liefern beides: Ein in der Industrie führendes Smart-Grid-Portfolio verbunden mit umfassender Erfahrung und profundem Fachwissen im Bereich Cyber-Sicherheit. Als multinationales Unternehmen mit globaler Reichweite besitzen wir die nötige Größe und Kompetenz, um Sie zuverlässig und nachhaltig zu unterstützen.

Dank unseres Fachwissens und unserer Integrationsfähigkeiten verfügen wir über das umfassendste Portfolio der gesamten Branche. Wir bieten Ihnen Produkt-, Lösungs- und Service-Sicherheit inklusive herausragender Unterstützung über den gesamten Lebenszyklus eines Produktes hinweg.

Wir arbeiten aktiv mit internationalen Normungsorganisationen zusammen, um gemeinsam Sicherheitsnormen für intelligente Netze zu entwickeln und zu optimieren. Darüber hinaus beraten wir Regulierungsbehörden bei technischen und prozessbezogenen Themen.

Durch die Arbeit des Siemens-weiten Cyber Emergency Response-Teams (CERT) erhalten wir zudem einen sehr guten Einblick in globale Bedrohungen der Cyber-Sicherheit.

Das folgende Kapitel ist ein Auszug aus dem Power Engineering Guide zur Cyber-Sicherheit. Darin erhalten Sie einen Gesamtüberblick rund um die Cyber-Sicherheit im Energiemanagement.
Der Auszug beschreibt die Aufgaben und Rollen der Anbieter, Integratoren und Betreiber und stellt ein ganzheitliches Konzept vor, das Personen, Prozesse, Produkte und Systeme gleichermaßen berücksichtigt.

# 1 Cyber-Sicherheit

## 1.1 Cyber-Sicherheit im Energiemanagement

Das Kerngeschäft von Stromversorgern, die eine kritische Infrastruktur betreiben, ist eine wirtschaftliche, sichere und zuverlässige Energieversorgung. Die Art und Weise, wie Netze betrieben und verwaltet werden, hat sich in den vergangenen Jahren dramatisch verändert. Ursachen dafür sind die Integration erneuerbarer und dezentraler Energiequellen, die Netzoptimierung, die Interaktion mit sogenannten Prosumern – also Konsumenten, die gleichzeitig auch Strom produzieren – und Verbrauchern sowie der Eintritt neuer Marktteilnehmer.
Die Informations- und Kommunikationstechnik durchdringt zunehmend alle Bereiche bis hin zum Verteilnetz und den privaten Haushalten. Die immer stärkeren Verflechtungen bieten mehr Ansatzpunkte, die kritische Infrastruktur anzugreifen. Infolgedessen hat die Cyber-Sicherheit für die Stromnetzbetreiber heute oberste Priorität.

Wie in Abb. 1 dargestellt, gehört es zu den Hauptzielen eines Netzbetreibers, die Energieversorgung sicherzustellen – zu jeder Zeit, zu wettbewerbsfähigen Kosten und unter Einhaltung der relevanten Vorschriften. Cyber-Bedrohungen können diese Versorgungssicherheit gefährden. Zum Cyber-Schutz gehören daher alle Maßnahmen, die diese Risiken mindern, sowie die Befolgung der industriellen Standards und, wo nötig, die Berücksichtigung lokaler Vorschriften zur Cyber-Sicherheit.
Um diese Zielvorgabe zu erfüllen, sollte 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.

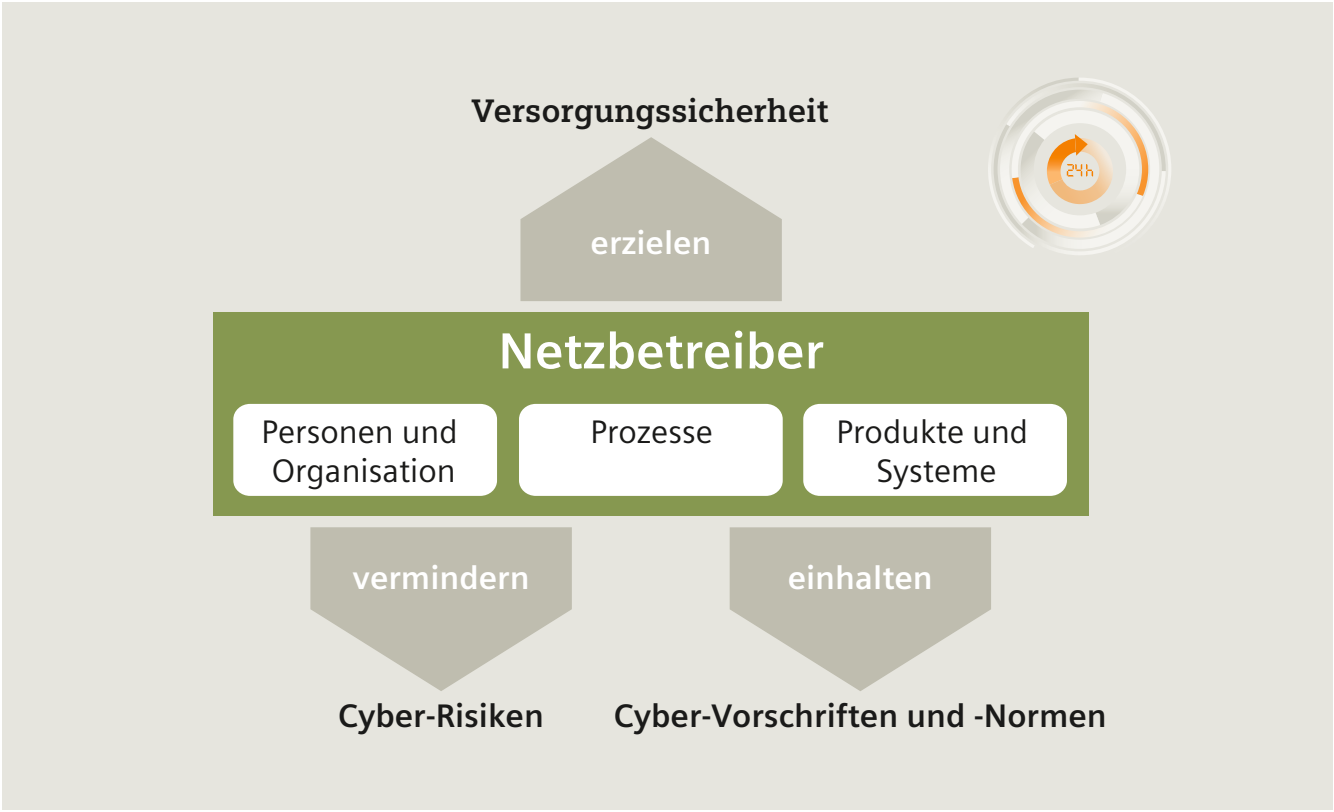


*Abb. 1:* Cyber-Sicherheitsziele eines Netzbetreibers

## 1.2 Cyber Security Framework

Das Cyber Security Framework bildet den Rahmen für den Cyber-Schutz. Es legt fest, wie die verschiedenen Akteure in der Energie-Wertschöpfungskette mit dem Thema Cyber-Sicherheit umgehen sollten. Dieser Rahmenplan basiert auf den folgenden Komponenten:

1. Cyber-Sicherheitsvorschriften
   Alle Akteure in der Energie-Wertschöpfungskette müssen die Cyber-Sicherheitsvorschriften unterstützen.
2. Cyber-Sicherheitsnormen
   Bestehende internationale Normen beschreiben Vorgaben für das gesamte Spektrum des Cyber-Schutzes – von der Steuerung bis hin zur Umsetzung in einzelnen Produkten. Die drei wichtigsten Normen für die Energieautomatisierung sind ISO/IEC 27001, IEC 62443 und IEC 62351.
3. Cyber-Sicherheitsleitfäden
   Leitfäden liefern Empfehlungen, wie Netzbetreiber Cyber-Sicherheit erreichen können. Die am häufigsten verwendeten und anerkanntesten Leitfäden sind die Empfehlungen der North Electric Reliability Corporation (NERC) zum Schutz kritischer Infrastrukturen (Critical Infrastructure Protection, CIP) und das Whitepaper des Bundesverbandes der Energie- und Wasserwirtschaft (BDEW) zu IT-Sicherheitsempfehlungen.

Bezug nehmend auf diese Leitfäden definiert Siemens 14 Kategorien von Sicherheitsmaßnahmen (siehe Abb. 2). Die Kategorien spiegeln das ganzheitliche Cyber-Security-Konzept des Unternehmens wider und umfassen die sogenannten „3 Ps“:

- **Personen und Organisationen**: Menschen, die im Unternehmen beschäftigt sind
- **Prozesse**: Abläufe, denen Personen und Organisationen folgen, um betriebliche Anforderungen zu erfüllen
- **Produkte und Systeme**: zu Grunde liegende Infrastruktur, um betrieblichen Anforderungen gerecht zu werden.

Die Kategorien für Prozesse und Organisationen sind in Abb. 2 in den grauen Kästen dargestellt.

Die Sicherheitsmaßnahmen für Produkte und Systeme sind in den grünen Kästen in Abb. 2 kategorisiert.

Die Kategorien der Sicherheitsmaßnahmen umfassen im Einzelnen:

### 1. Vorbereitetsein der Organisation

Es gilt, relevante Sicherheitsmaßnahmen für die Entwicklung, Integration und Wartung sicherer Produkte und Lösungen festzulegen. Dies betrifft die gesamte Organisation durch genau definierte Rollen, klare Verantwortlichkeiten, geeignete Qualifikationen, Richtlinien, Prozesse, Werkzeuge und Kommunikationsabläufe. Die Richtlinien zur Informationssicherheit bei Siemens entsprechen ISO/IEC 27001.

### 2. Sichere Entwicklung

Die sichere Entwicklung ist ein systematisches Konzept, um Cyber-Sicherheit in den Entwicklungs- und Lebenszyklus der Produkte und Lösungen zu integrieren. Sie ist Bestandteil der gesamten Prozesskette, vom Festlegen der Cyber-Sicherheitsanforderungen bis hin zur Überprüfung des Cyber-Schutzes. Das Konzept deckt auch den Schutz der dafür notwendigen IT-Infrastruktur ab.

### 3. Sichere Integration und sicherer Service

Cyber-Sicherheit ist ein integraler Bestandteil der Prozesse von Siemens. Die Kunden erhalten Lösungen, die Siemens unter Berücksichtigung von Best-Practice-Beispielen für die Cyber-Sicherheit entwirft, integriert und in Betrieb nimmt. Die Lösungen unterstützen den sicheren Betrieb optimal.

### 4. Umgang mit Schwachstellen und Störungen

Bei der Behandlung von Schwachstellen und Störungen handelt es sich um den Prozess, der festlegt, wie eine Organisation auf sicherheitsrelevante Schwachstellen und Störungen reagiert und mit diesen umgeht. Hierzu gehört auch die notwendige interne und externe Kommunikation. Der Prozess ist mit dem regulären Prozess zur Schwachstellenbeobachtung und „Patch“-Entwicklung aus der Produkt- oder Lösungsentwicklung verknüpft.

Siemens verfügt über ein eigenes internes Computer Emergency Response Team (CERT). Das Siemens ProductCERT-Team hat die Aufgabe, Sicherheitsprobleme zu beobachten, zu analysieren, und gemeinsam mit den entsprechenden Siemens-Organisationseinheiten produktbezogene Hinweise zu Schwachstellen sowie Empfehlungen zu deren Minimierung zu veröffentlichen. Siemens ProductCERT verfügt über anerkannte Expertise im Bereich Penetrationsprüfung. Dabei prüft das Unternehmen sowohl Siemens-Produkte als auch Fremdkomponenten im Siemens-Portfolio durch selektive Hackerangriffe auf


*Abb. 2:* Kategorien von Cyber-Sicherheitsmaßnahmen bei Siemens

Schwachstellen. Auf dieser Basis legt das Team den betreffenden Siemens-Organisationseinheiten Empfehlungen für Implementierungsrichtlinien vor.

### 5. Sichere Systemarchitektur

Eine Architektur für Cyber-Sicherheit muss nicht nur den regulatorischen Anforderungen entsprechen, sondern auch konzeptionsintegrierte Sicherheitseigenschaften aufweisen („Security by Design"). Für den Schutz des Stromnetzes ist ein fundiertes, gestaffeltes Sicherheitskonzept („Defense-in-Depth") erforderlich, das Cyber-Risiken adressiert und mit Hilfe von Personen, Prozessen und Technologien einen sicheren Betrieb unterstützt.

Abb. 3 skizziert eine typische Netzwerkarchitektur. Grundlage ist eine klare Segmentierung des Netzwerks in überschaubare Zonen. Die Zonen sind jeweils mit geeigneten Cyber-Sicherheitsmaßnahmen ausgerüstet, um einen sicheren und wirtschaftlichen Betrieb zu ermöglichen.

Die Architektur ist die sichtbarste Komponente eines umfassenden Cyber-Sicherheitskonzepts. Sie dient als Grundlage für weitere Maßnahmen im Bereich Personen, Prozesse und Produkte, die im Cyber-Sicherheitsrahmenplan festgelegt sind.

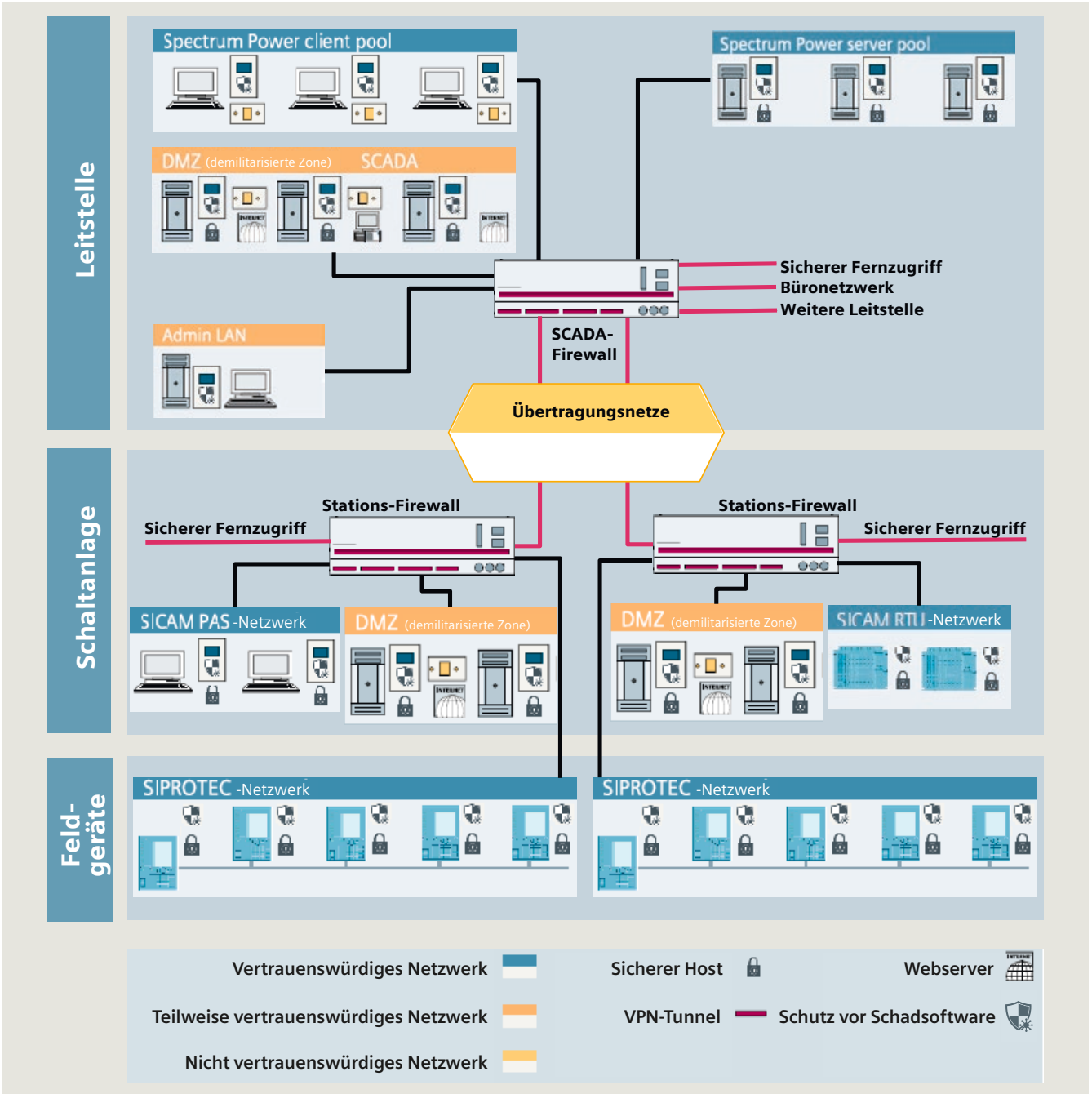


*Abb. 3:* Cyber-Sicherheitsarchitektur

### 6. Systemhärtung
Systemschutz und -härtung verkleinert die Angriffsfläche der Produkte und Lösungen durch sichere Konfiguration. Dies wird beispielsweise durch Deinstallation überflüssiger Software erzielt, durch das Löschen unnötiger Nutzernamen oder -anmeldedaten, die Deaktivierung ungenutzter Ports oder Härtung des Betriebssystems. Siemens stellt Leitfäden für die Härtung von Produkten und Systemen zur Verfügung und kann die Betreiber bei der Härtung ihrer Infrastruktur unterstützen.

### 7. Zugangskontrolle und Kontenverwaltung
Unter Zugangskontrolle versteht man die selektive Beschränkung des Zugriffs auf Produkte, Lösungen oder Infrastruktur mit Hilfe der Authentifizierung der Nutzer (und Systeme) sowie ihrer Autorisierung durch entsprechende Berechtigungen. Die Kontenverwaltung dient dazu, unterschiedliche Nutzerkonten mit jeweils entsprechenden Berechtigungen festzulegen. Dies geschieht idealerweise zentral anhand einheitlicher Sicherheitsrichtlinien. Siemens unterstützt die Netzbetreiber beim Entwurf und der Umsetzung eines Zugangskontroll- und Kontenverwaltungssystems. Netzbetreiber können die Energiemanagementsysteme von Siemens nahtlos mit Produkten anderer Anbieter in ihre zentralen Nutzermanagementlösungen integrieren.

### 8. Sicherheitsprotokollierung und -überwachung
Sicherheitsprotokollierung und -überwachung bedeutet, sämtliche im System durchgeführten sicherheitsrelevanten Aktivitäten zu erfassen und zu beobachten. Dazu gehören auch Aktivitäten in Nutzerkonten wie An-/Abmelden oder fehlgeschlagene Anmeldeversuche. Alarme werden zur weiteren Nachverfolgung aufgezeichnet. Die Produkte und Lösungen von Siemens unterstützen die zentrale Protokollierung sicherheitsrelevanter Ereignisse und Alarme anhand des Syslog-Meldungsstandards. Damit dienen sie als Grundlage für anspruchsvolle Sicherheitsinformations- und Ereignismanagementlösungen (Security Information and Event Management, SIEM).

### 9. Sicherheitspatch-Management
Zum Sicherheitspatch-Management gehört es, die Schwachstellen für alle in einem Produkt bzw. einer Lösung eingesetzten Softwarekomponenten (eigene ebenso wie die von Fremdanbietern) zu überwachen, die Schwachstellen und verfügbaren Patches zu klassifizieren, Kompatibilitätsprüfungen für die Sicherheitspatches durchzuführen sowie gegebenenfalls zusätzliche Updates zu entwickeln, um Inkompatibilitäten zu beseitigen. Dies umfasst auch die Lieferung und Wartung eines Systems inklusive Installation der neuesten Sicherheitspatches. Siemens bietet für die Betreiber von Energieautomatisierungssystemen umfassende Patch-Management-Services an.

### 10. Schutz vor Schadsoftware (Malware)
Der Schutz eines Produkts oder einer Lösung vor Schadsoftware wird durch die Unterstützung geeigneter Malware-Schutzlösungen gewährleistet (wie etwa mit klassischen Antivirus-Lösungen, dem Auflisten vertrauenswürdiger Anwendungen (Whitelisting) oder Signieren von Software) sowie durch weitere bewährte Verfahrensweisen. Siemens verfügt über Malware-Schutz für die in der Energieautomatisierung eingesetzten Hauptkomponenten, bietet technische Lösungen für den Schutz vor Schadsoftware an und unterstützt die Kunden dabei, einen sicheren Update-Prozess für Antivirus-Erkennungsmuster einzurichten.

### 11. Datensicherung und -wiederherstellung
Datensicherung beinhaltet den Prozess des Kopierens und Archivierens von Software, Konfigurations- und Betriebsdaten, damit das betreffende Produkt bzw. die Lösung bei Verlust wiedergestellt werden kann. Dazu gehören auch geeignete Maßnahmen und Verfahrensweisen für die Wiederherstellung im Notfall. Siemens bietet entsprechende Datensicherungs- und Wiederherstellungskonzepte an und unterstützt die Netzbetreiber bei der Beurteilung und Einrichtung eines geeigneten Prozesses.

### 12. Sicherer Fernzugriff
Unter sicherem Fernzugriff versteht man im Zusammenhang mit Automatisierungssystemen für Schaltanlagen einen verschlüsselten, authentifizierten und autorisierten Zugriff auf die Systeme der Schaltanlage, der von entfernten Standorten aus über potenziell nicht vertrauenswürdige Netzwerke erfolgen kann. Siemens bietet eine zertifizierte, für die Anforderungen der Netzbetreiber optimierte Lösung für den sicheren Fernzugriff.

### 13. Datenschutz und -integrität
Datenschutz gewährleistet den Schutz aller sensiblen Daten im gesamten System, und zwar sowohl in Ruhephasen als auch während des Datentransports. Diese Daten dürfen nur für autorisierte Personen oder Prozesse zugänglich sein. Darüber hinaus sollten entsprechende Verfahren auch die Integrität der Daten und der Kommunikation im gesamten System sowie die Verfügbarkeit der Daten sicherstellten. Komponenten von Siemens bieten die erforderliche Funktionalität, um den Anforderungen an Datenschutz und -integrität gerecht zu werden. Gleichzeitig stellen die bei Siemens implementierten Prozesse sicher, dass die Kundendaten in allen Phasen des Kundenprojekts mit der erforderlichen Sorgfalt verwaltet werden.

### 14. Vertraulichkeit
Durch die oben genannten Maßnahmen wird sichergestellt, dass die Nutzer bestimmen können, wie und in welchem Umfang Informationen über sie gesammelt, verwendet und mit anderen Personen geteilt werden. Ein besonders sensibles Thema ist die Vertraulichkeit der Informationen, wenn personenbezogene Daten gesammelt werden, z. B. in einer Smart-Metering-Anwendung. Das Siemens-Portfolio unterstützt die Betreiber dabei, den damit verbundenen regulatorischen Anforderungen nachzukommen.

## 1.3 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 Störungen

Der Umgang mit Schwachstellen und Störungen ist eine der zwingenden Anforderungen an den Schutz des Energienetzes.

Zur Schwachstellenbehandlung gehört es, Gegenmaßnahmen festzulegen – sofern erforderlich – sowie Kommunikationsmaßnahmen zu bestimmen, um den Betreiber angemessen über kritische Schwachstellen, Workarounds und verfügbare Patches zu informieren, siehe Abb. 4.

Andererseits müssen die Netzbetreiber in der Lage sein, die zur Verfügung gestellten Sicherheitshinweise zu analysieren sowie Gegenmaßnahmen festzulegen und effektiv anzuwenden.

Während die Schwachstellenbehandlung das Unternehmensgeschäft schützt, soll die Störungsbehandlung die Möglichkeit bieten, wirksam auf Cyber-Störungen zu reagieren und den sicheren Betrieb wiederherzustellen. Für die Störungsbehandlung sind die gleichen Sicherheitsmaßnahmen erforderlich wie für die Schwachstellenbehandlung. Sie bedürfen jedoch zusätzlicher Maßnahmen hinsichtlich des Vorbereitetseins der Organisation, insbesondere in der Prozessabwicklung.

### 2. Sicherheitspatch-Management

Eine der wichtigsten Maßnahmen des Cyber-Schutzes ist das Patch-Management. Aufgrund der zunehmenden Vernetzung hat die Gefahr, dass Angreifer bekannte Schwachstellen ausnutzen, massiv zugenommen.

Normen wie ISO/IEC 27002 und IEC 62443-2-3 helfen den Betreibern dabei, zweckmäßige Maßnahmen für einen Patch-Managementprozess einzuführen. Zusammenfassend sind für die Betreiber folgende Prozessschritte empfehlenswert:

- 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.

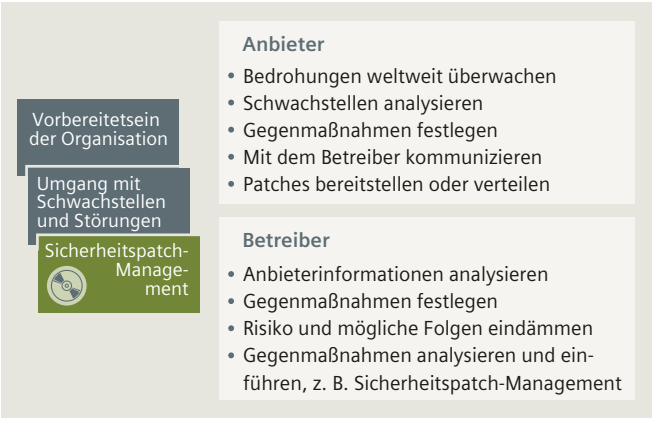


*Abb. 4:* Erforderliche Aufgaben und Sicherheitsmaßnahmen beim Umgang mit Schwachstellen

Die für Systemlieferanten vorgeschriebenen Anforderungen an das Patch-Management sind in Normen wie IEC 62443-2-3 und IEC 62443-2-4 festgelegt:

- Bereitstellung einer Dokumentation zu Patch-Management-Richtlinien für Komponenten und Systeme
- Überprüfung der Patches hinsichtlich Kompatibilität und Anwendbarkeit für Eigen- und Fremdkomponenten
- Bereitstellung der Patch-Informationen und der Patches für den Betreiber
- Bereitstellung von Lebenszyklus-Informationen für Produkte und Systeme, einschließlich Informationen zum Ende der Lebensdauer.

Um diese Anforderungen zu erfüllen, bietet Siemens einen umfassenden Patch-Managementprozess für Produkte und Systeme. Hierzu gehört ein regelmäßiger Patch-Test für Eigen- und Fremdkomponenten und die Bereitstellung der Testergebnisse für die Kunden. Dabei wird das Siemens-interne CERT hinzugezogen, um eine umfassende Schwachstellensuche durchzuführen sowie die Schwachstellen und Empfehlungen für alle Siemens-Produkte mitzuteilen; siehe Abschnitt 1.2, Punkt 4. Zusätzlich stellt Siemens die Dokumentation „Sichern und Wiederherstellen“ auf Produkt- und Systemebene zur Verfügung. Dies gilt als Voraussetzung für den Patch-Managementprozess.

Abb. 5 zeigt vereinfacht die anfänglichen und die zyklischen Maßnahmen eines vollständigen Patch-Management-Prozesses aus dem Blickwinkel des Betreibers.

Zu den anfänglichen Maßnahmen gehören die Migration zu einem sicheren System (Schritt 0 in Abb. 5), die Festlegung der zu berücksichtigenden Assets und die für die Durchführung des Patch-Managements erforderliche Vorbereitung der Asset-Daten (Schritte 1 und 2).

Die wiederkehrenden Maßnahmen beginnen mit der Zusammenstellung der Patch-Informationen anhand des Asset-Inventars (Schritt 3) und der Entscheidung, ob, wann und welche Patches installiert werden müssen (Schritt 4). Die Patch-Überprüfung (Schritt 5) und die Installation (Schritt 6) folgen entsprechend. Zum Schluss sind die Asset-Daten zu aktualisieren (Schritt 7).

Siemens bietet – sämtliche Prozessschritte aus ISO/IEC 27001 berücksichtigend – umfassende Patch-Management-Services für Produkte und Systeme an, um die abgeleiteten regulatorischen Anforderungen zu erfüllen.

### 3. Nutzerverwaltung und Zugangskontrolle

Das Grundprinzip der Zugangskontrolle ist in Abb. 6 dargestellt. Die Zugangskontrolle stellt sicher, dass die Nutzer (und Systeme) nur in der vorgesehenen Weise mit Ressourcen interagieren können. Dies ist nur dann möglich, wenn der Nutzer erstens authentifiziert ist – das heißt, wenn bestätigt wurde, dass der Nutzer die Person ist, die er zu sein vorgibt – und wenn er zweitens autorisiert ist – wenn bestätigt wurde, dass der Nutzer berechtigt ist, die beabsichtigte Operation mit/an den Ressourcen durchzuführen. Das Identitätsmanagement ist die Vertrauensbasis in dieser Pyramide. Es übernimmt die Verwaltung der zu kontrollierenden Nutzer und ihrer Anmeldedaten. Der Vollständigkeit halber berücksichtigt die Zugangskontrolle nicht nur die Nutzer, sondern auch Ressourcen wie Geräte oder Anwendungen.

Die Zugangskontrolle ist in allen Lebenszyklusphasen der Systeme und Netze relevant (von der Inbetriebnahme über den laufenden Betrieb und die Modernisierung bis hin zur Stilllegung). Die wichtigste Phase für die Cyber-Sicherheit ist der tägliche Betrieb. Typische Szenarien für die Zugangskontrolle sind physischer Zugang, HMI-Zugriff, IED-Zugriff, Fernzugriff usw. Aus Sicherheitsgründen werden zusätzlich Notfall-Zugangswege festgelegt, um den regulären Zugangskontrollmechanismus umgehen zu können.

Um den Zugang im Stromnetz zu kontrollieren, gibt es mehrere Lösungen mit unterschiedlichem Umfang und verschiedenen Sicherheitsniveaus. Ein typisches Beispiel für einen zentralisierten Ansatz sind LDAP- oder RADIUS-Server, um die Identitäten zu verwalten. Authentifizierung und Autorisierung können durch Kennwortverifizierung oder durch X.509-Zertifikate auf der Grundlage einer Public Key Infrastructure (PKI) erfolgen. Die Zugangsrechte werden vom System oder Gerät festgelegt, da sie abhängig von der Betriebsfunktion jeweils spezifisch für diese Geräte gelten.

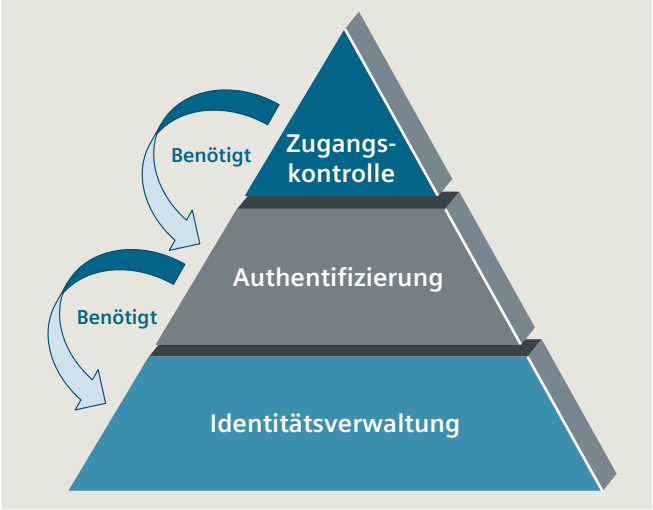


*Abb. 6:* Identitäts- und Zugangsverwaltung – das Grundprinzip

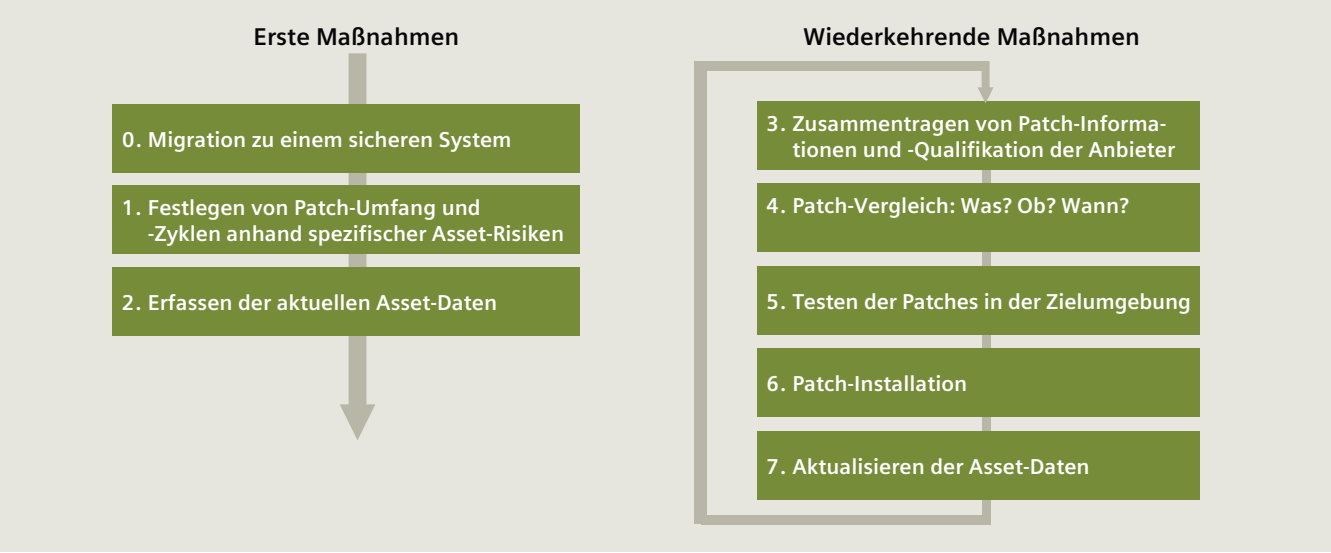


*Abb. 5:* Vereinfachter Patch-Management-Prozess

Abb. 7 zeigt ein Beispiel für rollenbasierte Zugangskontrolle (Role Based Access Control – RBAC). Ein Nutzer möchte über ein Gerätemanagement-Tool auf ein IED zugreifen (1). Das IED sendet die Anforderung zur Authentifizierung des Nutzers an einen Active Directory (AD)-Domänen-Controller (2). AD antwortet mit dem Ergebnis der Authentifizierung. Wenn der Nutzer vom IED erfolgreich authentifiziert wurde, ruft es die Rolleninformationen inklusive Autorisierungsstufe des Nutzers beim AD ab (3). Das IED startet dann die rollenabhängige Nutzersitzung (4).

Da sich ein Stromnetz aus Produkten mehrerer Anbieter zusammensetzt, ist es äußerst wichtig, standardisiert auf der Grundlage von IEC 62351 vorzugehen, um eine wirksame Zugangskontrolle herzustellen und Interoperabilität zu ermöglichen.

Wichtig ist außerdem, Übergangstechnologien und -werkzeuge zu berücksichtigen, welche die Sekundärausrüstung der zurückliegenden Generation berücksichtigen, denn diese wird auch in den kommenden Jahren noch den größten Teil der installierten Basis bilden. Zentralisierte Zugangsmanagementlösungen wie Siemens CrossBow können die Lücke schließen, indem sie die Verwaltung der Nutzer und Zugriffsrechte sowohl für ältere als auch für neuere Generationen der Sekundärausrüstung ermöglichen.

## 4. Zentrale Protokollierung

Um die Ereignisse im Stromnetz zu visualisieren, ist eine Überwachung unerlässlich. Ein Element ist die zentrale Protokollierung. Dies bedeutet, dass die Informationen über die Ereignisse und Aktivitäten im Stromnetz an einer zentralen Stelle zur weiteren Analyse zusammengetragen werden. Als Grundlage für die zentrale Protokollierung dient die sogenannte Syslog-Funktion.

Eine zentrale Protokollierung wird in Normen wie RFC 5424/5/6 definiert (syslog). Mit ihren Anwendungen im Energiesektor befassen sich Normen wie IEEE 1686 und IEC 62351. Darüber hinaus liefern Leitfäden wie das BDEW-Whitepaper oder NERC CIP Anhaltspunkte dafür, welche Aspekte überwacht werden müssen.

Siemens unterstützt eine zentrale Protokollierung und bietet den Netzbetreibern entsprechende Lösungen an.

## 5. Schutz vor Schadsoftware (Malware)

Der Malware-Schutz konzentriert sich auf Maßnahmen und Konzepte, die die Systeme vor Infektionen mit Schadsoftware schützen. Dies ist für alle Systemkomponenten erforderlich. Anders ausgedrückt: Systeme, die in Prozessnetzwerken und Steuerungen eingesetzt werden, müssen über Schutzkonzepte gegen Malware-Infektionen verfügen. Mögliche Quellen für Malware-Infektionen sind infizierte Wechseldatenträger (z. B. USB-Speichersticks, CDs usw.), Netzwerkfreigaben oder infizierte PCs (z. B. Service-PCs).

Schutz vor Schadsoftware bieten unterschiedliche technische Lösungen: klassische Antivirus-Produkte, eine „weiße Liste“ für Anwendungen (Whitelisting) PC-gestützter Systeme und Software-Signierung für eingebettete Geräte. Die Antivirus-Erkennungsmuster müssen regelmäßig aktualisiert werden, ohne sich dabei direkt mit Update-Servern in externen Netzwerken, z. B. im Internet, zu verbinden. Eine mögliche Lösung bietet ein interner Update-Server oder ein dokumentierter, sicherer manueller Prozess (z. B. durch externe, sichere Geräte). Um die Kompatibilität mit neuen Antivirus-Erkennungsmustern zu gewährleisten, prüft Siemens neue Antivirus-Muster regelmäßig auf die Fähigkeit zur Zusammenarbeit mit der Siemens-Anwendung.

In diesem Zusammenhang bietet Siemens technische Lösungen für den Malware-Schutz an und unterstützt so den Kunden dabei, einen sicheren Aktualisierungsprozess für Antivirus-Muster einzurichten.

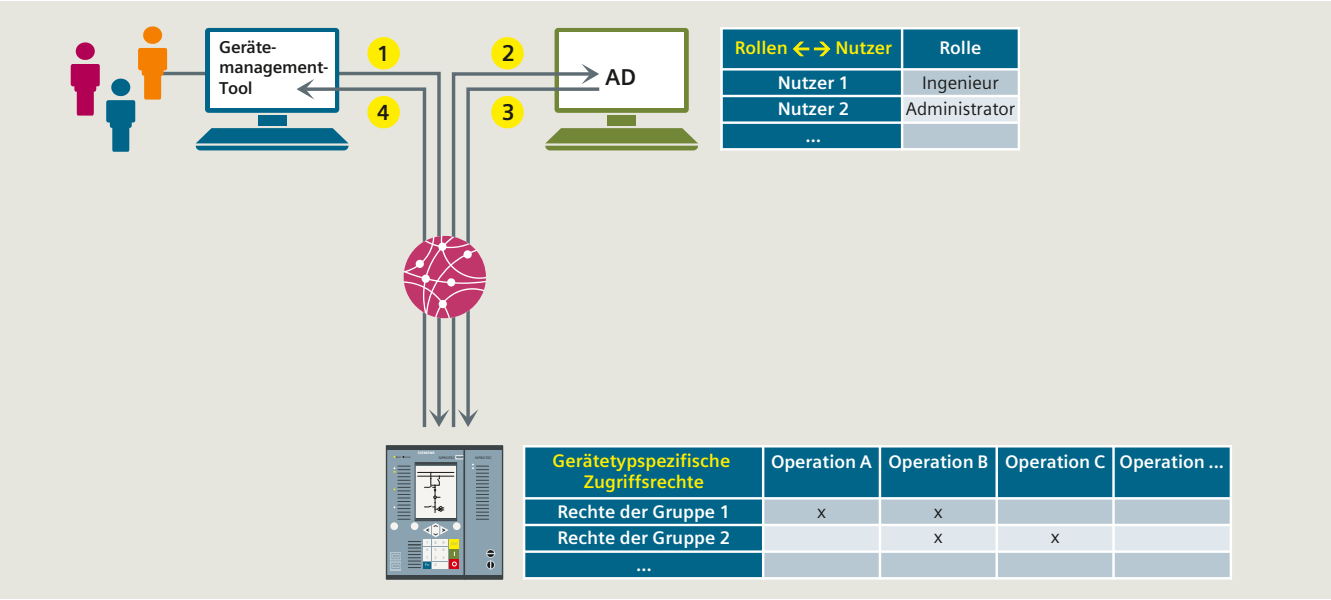


*Abb. 7:* Beispiel einer rollenbasierten Zugriffskontrolle

## 1.4 Angewandte Cyber-Sicherheit

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 1.2), und die betriebsbezogenen Voraussetzungen dafür zu erfüllen (Abschnitt 1.3).

### 1. Produktsicherheit

Siemens verfolgt bei seinem Portfolio für die Energieautomatisierung ein ganzheitliches Konzept. Es berücksichtigt Prozesse, Kommunikation, Mitarbeiter und Technologien. Zunächst hat Siemens in der Organisation selbst Cyber-Sicherheit durch definierte Rollen, Regeln und Prozesse aufgebaut sowie eine Governance-Struktur gemäß ISO/IEC 27001 etabliert. Zweitens ist die Entwicklung sicherer Produkte Bestandteil des Produktlebenszyklus-Managements von Siemens. So entspricht das Unternehmen den strengen Anforderungen des Cyber-Schutzes und verwendet eine sichere Produktarchitektur.

Bestandteil dieser Produktentwicklung sind ein sicherer Entwurfsprozess, die Implementierung der Software und systematische Cyber-Sicherheitstests.
Die Cyber-Sicherheit der Siemens-eigenen Infrastruktur spielt ebenfalls eine wichtige Rolle. Die interne Entwurfsdokumentation und der Quellcode müssen vor unbefugtem Zugriff und vor Manipulationen geschützt werden, um die Integrität sicherzustellen.

Sichere Automatisierungsprodukte sind die Basis für ein sicheres Energieautomatisierungssystem. Die an die Produkte gestellten Sicherheitsanforderungen sind von verschiedenen Faktoren abhängig, wie z. B. von der vorgesehenen Funktion (Schutz, Kontrolle, Betrieb oder Überwachung) und von der räumlichen Anordnung der Produkte. Die Sicherheitsfunktionen in modernen Energieautomatisierungsprodukten folgen den allgemeinen Zielvorgaben der Cyber-Sicherheit: Verfügbarkeit, Integrität und Vertraulichkeit sowie Einhaltung der branchenspezifischen Standards. Modernste Schutzgeräte können diese Anforderungen erfüllen, siehe Abb. 8. Die sichere Kommunikation zwischen der Projektierungssoftware und dem Gerät ist für einen sicheren Betrieb unerlässlich. Eine verschlüsselte Verbindung wird erst nach gegenseitiger Authentifizierung aufgebaut. Bei diesem Prozess muss ein Verbindungskennwort verwendet und verwaltet werden, das den Empfehlungen im BDEW-Whitepaper und in NERC CIP entspricht. Alle sicherheitsrelevanten Ereignisse werden in einem löschgeschützten Sicherheitsprotokoll aufgezeichnet.

**Weitere Informationen zu Schwachstellen und zu Updates von Produkten und Lösungen finden Sie im Siemens-Internet:**

*siemens.com/cert/advisories*

**Oder beim ICS-CERT:**

*https://ics-cert.us-cert.gov/advisories*

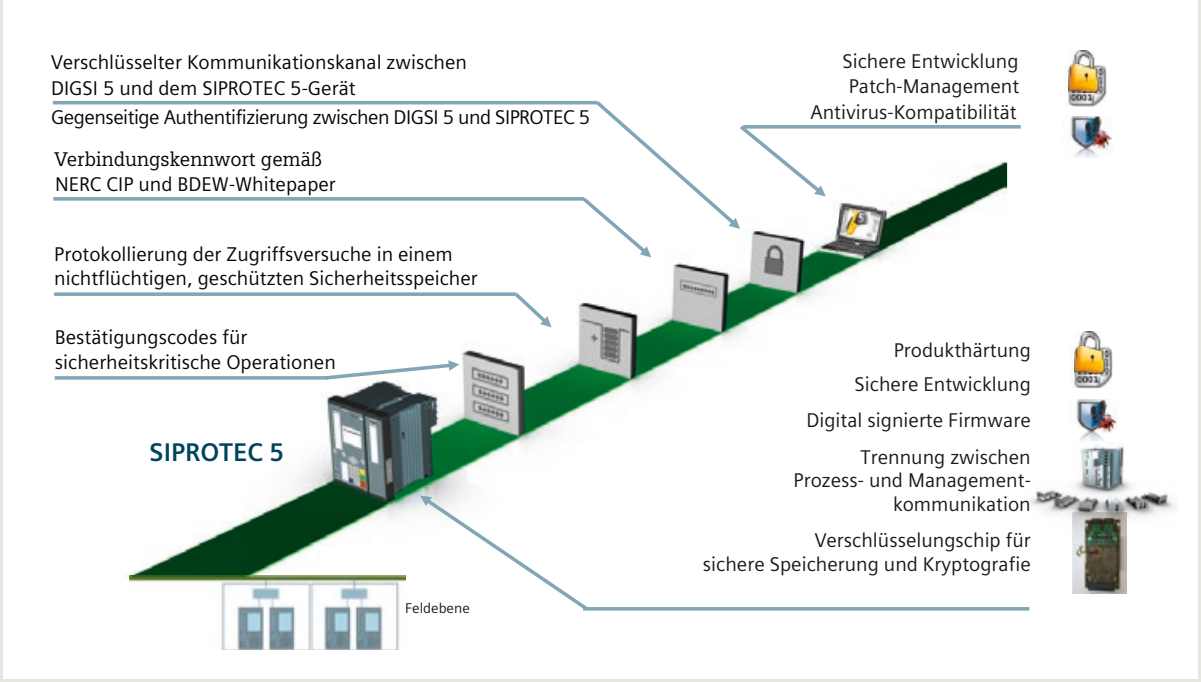


*Abb. 8:* Sicherheitseigenschaften eines modernen Schutzgeräts

Das Schutzgerät ist mit einem Verschlüsselungs-Chip ausgestattet, der auch eine Integritätsprüfung der Geräte-Firmware in einer geschützten Umgebung durchführt.

Während der Erstellung der Software wird die Firmware mit einer digitalen Signatur versehen. Mit deren Hilfe kann das Gerät eine Authentifizierung durchführen, um zu bestätigen, dass die Firmware auf dem Weg von der Erstellung zum Gerät nicht manipuliert wurde. Darüber hinaus ermöglicht das Gerät eine physische Trennung zwischen Prozess- und Managementkommunikation. Geräte, die außerhalb einer physisch geschützten Zone kommunizieren, müssen höhere Anforderungen an die Kommunikationssicherheit erfüllen als solche, die innerhalb eines physisch geschützten Bereichs kommunizieren.

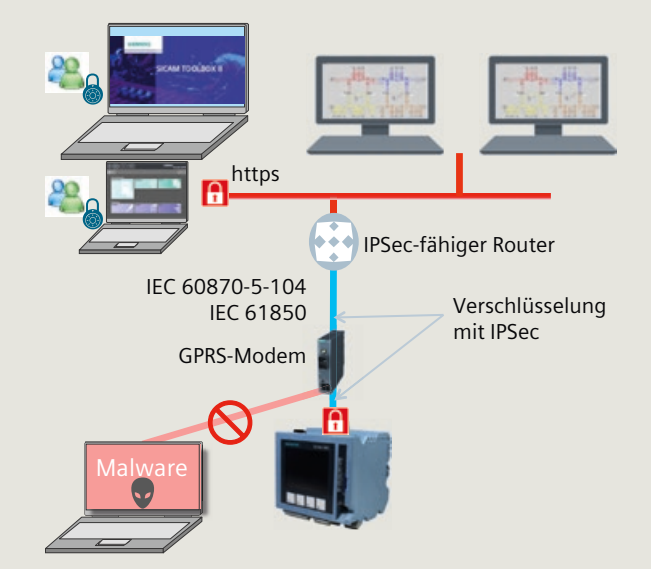


*Abb. 9:* Beispiel einer sicheren Telekommunikation

In einigen Szenarien der Verteilnetzautomatisierung ist es nicht immer möglich, die Prozesskommunikation mit geeigneten physischen Sicherheitsmaßnahmen vor Manipulation zu schützen. Hier unterstützen RTU-Produkte von Siemens eine durchgängige Verschlüsselung der Prozesskommunikation mit den Leitstellen, siehe Abb. 9.

Siemens testet Sicherheits-Patches und Virenmuster auf Referenzsystemen, um sicherzustellen, dass normale Installationen des Betriebssystems die Verfügbarkeit der Energieautomatisierungsfunktionen nicht beeinträchtigen.

## 2. Systemsicherheit – Beispiel digitale Schaltanlage

Als Systemintegrator ist Siemens dafür verantwortlich, die Produkte sicher zu integrieren. Dazu gehören ausführliche Prozessbeschreibungen, Leitfäden und technische Beschreibungen. Anschließend wird die Systemkonfiguration gemäß der technischen Beschreibungen durchgeführt. Die Sicherheitsmaßnahmen werden bei den Abnahmeprüfungen wie der Werksabnahme (Factory Acceptance Test, FAT) und der Baustellenabnahme (Site Acceptance Test, SAT) anhand festgelegter Testfälle überprüft.

In Automatisierungssystemen für Schaltanlagen unterliegen die Sicherheitsfunktionen besonderen Randbedingungen. Zum Beispiel müssen die Anlagen ständig verfügbar sein und möglichst unterbrechungsfrei laufen. Eine Schaltanlage enthält in der Regel eine Kombination aus PC-basierten und eingebetteten Systemen verschiedener Hersteller mit einer Lebensdauer von bis zu 40 Jahren. Daher besteht ein Energieautomatisierungssystem häufig aus vielfältigen Komponenten diverser Hersteller, mit unterschiedlichen Technologien aus verschiedenen Technologiegenerationen. Viele der in der Büro-IT etablierten Maßnahmen setzen die Prioritäten der Schutzziele anders oder berücksichtigen die Randbedingungen nicht adäquat. Dies erfordert speziell auf die Anforderungen der Energieautomatisierung zugeschnittene Strategien.

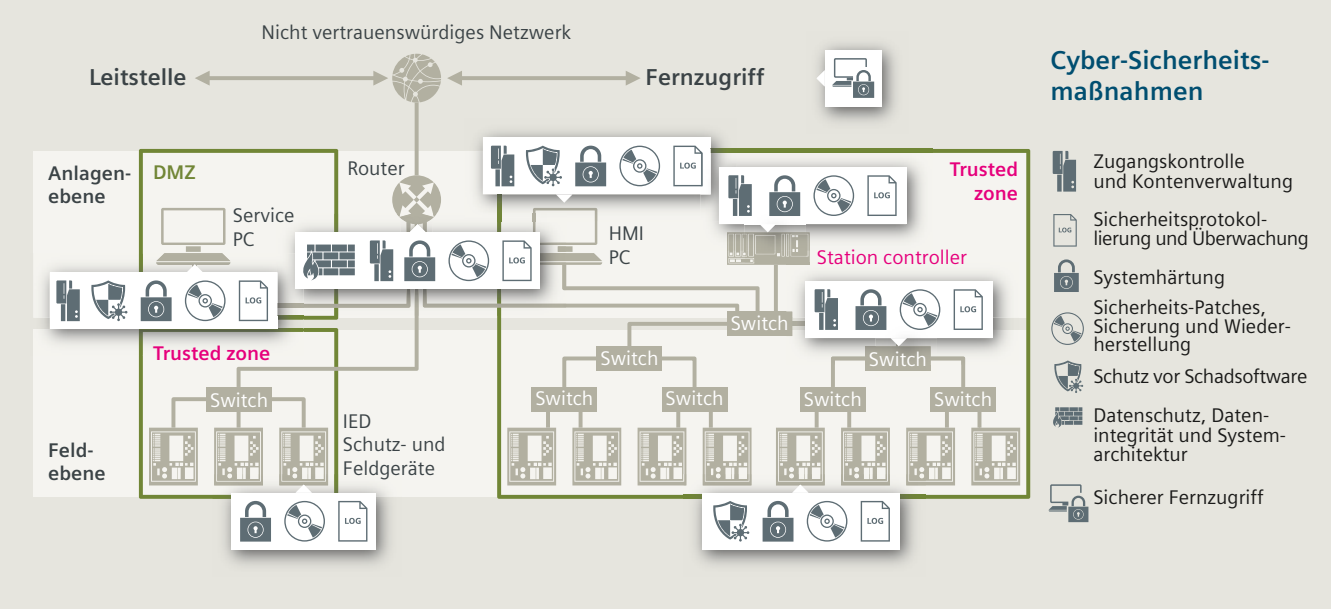


*Abb. 10:* Digitale Schaltanlage

In Abb. 10 sind die Sicherheitsmaßnahmen für eine digitale Schaltanlage dargestellt. Alle Cyber-Sicherheitsmaßnahmen folgen im Wesentlichen zumindest den Sicherheits-Entwurfsprinzipien „Defense in Depth", „Least Privilege" und „Network Segmentation".

Ein Netzwerk zu segmentieren ist ein wirkungsvoller Schutzmechanismus. Die Grundidee: Netzwerkelemente mit sensiblen Kommunikationsanforderungen und ähnlicher Schutzstufe werden demselben Teilnetz zugeordnet. Firewalls filtern den ein- und ausgehenden Datenverkehr. Diese Zonen werden auch als „vertrauenswürdige Zonen" bezeichnet. Eine Umgehung der Firewalls ist nicht zulässig. Die vertrauenswürdige Zone ist von außen, aus nicht vertrauenswürdigen Netzwerken, nicht zu erreichen. Um von außen Zugang zu der vertrauenswürdigen Zone zu erhalten, verwendet Siemens eine „Puffer"-Zone, die „demilitarisierte Zone" (Demilitarized Zone, DMZ).
Damit lassen sich häufig die Sicherheitsanforderungen für die interne Kommunikation in einer „vertrauenswürdigen Zone" im Vergleich zu einem größeren Netzwerk, das keine Sicherheitszonen einsetzt, auf ein für typische Industriekomponenten praktikables Maß begrenzen.

Unter dem Prinzip der geringsten Rechte („Least Privilege") versteht man die Praxis, den Zugang auf ein minimales Maß zu begrenzen, mit dem die gewünschte Funktionalität ermöglicht wird. Auf menschliche Nutzer angewandt bedeutet das Prinzip, dass dem Nutzer die niedrigste Stufe der Nutzerrechte zugewiesen wird, mit der die erforderlichen Aufgaben ausgeführt werden können. Das Prinzip wird auch auf alle anderen Teilnehmer eines Systems wie Geräte, Softwareanwendungen, Dienste und Prozesse angewandt. Es soll die potenziellen Schäden durch eine Sicherheitsverletzung – ob vorsätzlich oder unbeabsichtigt – begrenzen.

„Defense in Depth", also eine mehrstufige Verteidigung, ist der koordinierte Einsatz mehrerer Sicherheitseinrichtungen zum Schutz eines Systems. Das Ziel besteht darin, Redundanz für den Fall zu gewährleisten, dass eine der Sicherheitseinrichtungen ausfällt oder eine Schwachstelle in einer Sicherheitseinrichtung ausgenutzt wird. Bestandteile von „Defense in Depth" sind beispielsweise Sicherheitseinrichtungen/-maßnahmen wie Firewalls, Kontenverwaltung, Malware-Schutz und Systemhärtung.

Bei der Implementierung aller Sicherheitsmaßnahmen werden die allgemeinen Einschränkungen für Automatisierungssysteme in Schaltanlagen und die Leitfäden für Sicherheitskonzepte berücksichtigt. Die auf Cyber-Sicherheit abzielenden Maßnahmen sind (vgl. Abb. 2 und Abschnitt 1.2 zu den Sicherheitskategorien):
- Zugangskontrolle und Kontenverwaltung
- Sicherheitsprotokollierung und Überwachung
- Systemhärtung
- Sicherheits-Patches, Sicherung und Wiederherstellung
- Malware-Schutz
- Datenschutz, Datenintegrität und Systemarchitektur
- sicherer Fernzugriff.

Wenn man als ein Beispiel für eine Cyber-Sicherheitsmaßnahme den Schutz vor Schadsoftware betrachtet, so stehen für die Implementierung unterschiedliche Optionen zur Verfügung (siehe auch Abschnitt 1.3 Teil 5):

**Blacklisting / Antivirus**
Klassische Antivirus-Lösungen, die den Inhalt des PC-Dateisystems mit Erkennungsmustern bekannter Viren vergleichen. Im Falle einer Übereinstimmung wird der Nutzer von der Antivirus-Software gewarnt.

**Whitelisting von Anwendungen**
Eine Lösung, die mit dem Whitelisting von Anwendungen arbeitet, verwendet eine „weiße Liste". Dabei handelt es sich um einen Schutzmechanismus, der nur die Ausführung vertrauenswürdiger Programme und Anwendungen auf dem System zulässt. Nach der Installation von Systemsoftware und Anwendungen wird auf dem virenfreien System eine zusätzliche Whitelisting-Software installiert. Nach Abschluss der Installation wird von der Whitelisting-Lösung eine Liste vertrauenswürdiger Programme, Anwendungen und Dienste erzeugt. Alle in der Liste enthaltenen Anwendungen/Programme/Dienste werden signiert oder mit einer Prüfsumme gesichert. Dies gewährleistet, dass nur zugelassene Software ausgeführt werden kann. Heruntergeladene Software oder Viren, die das System nach der Aktivierung des Whitelisting-Schutzes möglicherweise infiziert haben könnten, werden an der Programmausführung gehindert.

Alle Windows-basierten PC-Systeme sind mit einem geeigneten Malware-Schutz ausgestattet. Der Vorteil des Whitelisting von Anwendungen besteht darin, dass regelmäßige Aktualisierungen der Erkennungsmuster für neu entwickelte Malware nicht sofort installiert werden müssen.

Welche Lösung zu den Anforderungen des Netzbetreibers und des Betriebsmanagements am besten passt, muss auf einer projekt- oder systemspezifischen Basis entschieden werden.

Siemens bietet umfassende Serviceleistungen und Technologien, um die Betreiber dabei zu unterstützen, Schutzkonzepte für digitale Schaltanlagen zu entwickeln sowie eine moderne Architektur und eine „Defense-in-Depth"-Strategie zu etablieren.

## 1.5 Beratungsleistungen zur Cyber-Sicherheit

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 Prozesse.

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 Abb. 11 dargestellt, sind die von Siemens angebotenen Beratungsleistungen zur Cyber-Sicherheit in vier Phasen gegliedert:

- **Orientierung:** Umfassende und objektive Analyse des aktuellen Cyber-Schutzstatus der Technologien, Prozesse und Organisationen.
- **Zielsetzung:** Definition der angestrebten Sicherheitsstufen auch in Bezug auf die relevanten regulatorischen Anforderungen und Standards sowie Ableitung konkreter Sicherheitsmaßnahmen
- **Roadmap:** Entwicklung eines ganzheitlichen Cyber-Schutzes. Implementierung einer Roadmap basierend auf den abgeleiteten Maßnahmen und Empfehlungen für die Umsetzung.
- **Navigation:** Kontinuierliche Unterstützung der Kunden während der Umsetzung der Sicherheitsmaßnahmen.

Netze lassen sich sehr wirksam vor Cyber-Angriffen schützen, wenn die Methoden und Funktionalitäten des Cyber-Schutzes konsequent umgesetzt werden. Siemens kann die Stromnetzbetreiber bei der Beurteilung, Festlegung und Umsetzung der Maßnahmen für Cyber-Sicherheit unterstützen.

Siemens empfiehlt Beratungen und führt selbst Risikobewertungen für Organisationen oder Infrastrukturen durch. So kann sich das Unternehmen ein umfassendes Bild von den bestehenden Risiken machen, entsprechende Maßnahmen ableiten und die ermittelten Risiken minimieren.

## 1.6 Schlussbemerkungen

Ein wirksamer Cyber-Schutz setzt ein ganzheitliches Sicherheitskonzept voraus. Cyber-Sicherheit erfordert kontinuierlichen Einsatz für den Schutz vor bestehenden und zukünftigen Bedrohungen und Risiken.

Dies gilt für Prozesse, Technologien und Personen. Wichtig sind beispielsweise ein kontinuierliches Kompetenzmanagement, um stets auf dem Laufenden zu bleiben, Prozessverbesserungen, die mit internationalen Normen wie ISO/IEC 27001 übereinstimmen, sowie technische Wartung, um das Sicherheitsniveau auf dem neuesten Stand zu halten. Dies gilt für alle Akteure in der Energie-Wertschöpfungskette: Betreiber, Anbieter, Systemintegratoren und Berater.

Daher setzt sich Siemens während des kompletten Lebenszyklus seiner Produkte und Lösungen systematisch für einen auf internationalen Normen basierenden Cyber-Schutz ein. Darüber hinaus arbeitet Siemens gemäß ISO/IEC 27001.

Mit unserem Portfolio und Service, verbunden mit dem Siemens CERT, ist Siemens als starker, vertrauenswürdiger Partner für seine Kunden optimal aufgestellt.

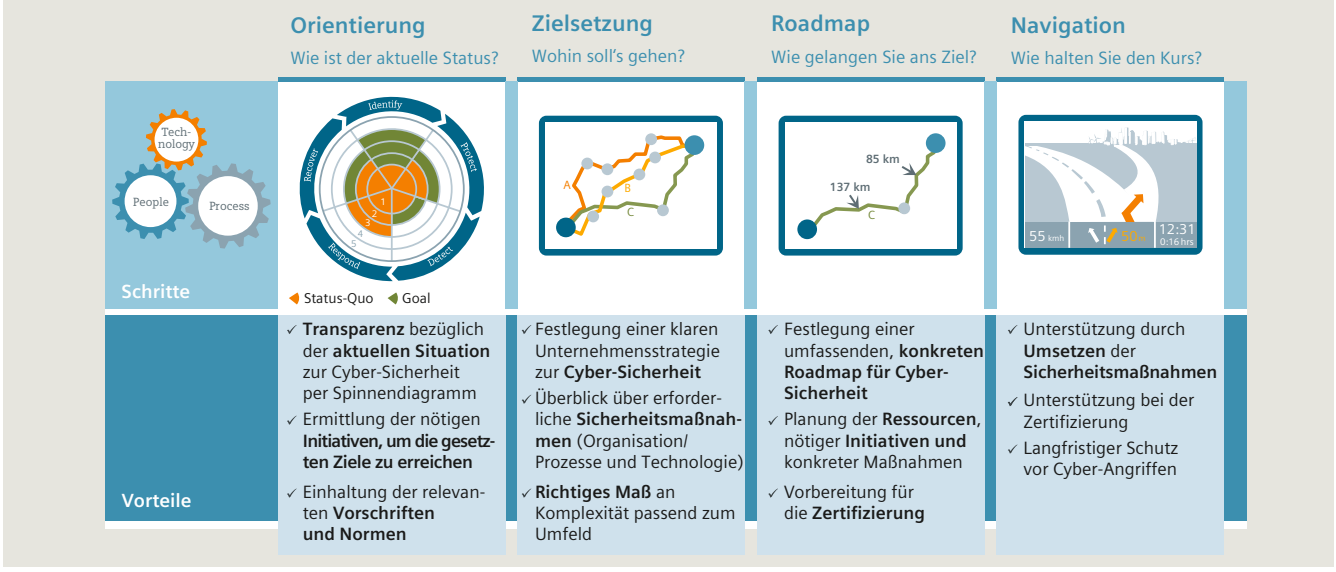


*Abb. 11:* Phasen bei der Beratung zur Cyber-Sicherheit

**Herausgeber**
**Siemens AG 2017**

Energy Management Division
Freyeslebenstrasse 1
91058 Erlangen, Deutschland

Wünschen Sie mehr Informationen,
wenden Sie sich bitte an unser
Customer Support Center für Power & Energy:
Telefon:+49 180 524 70 00
Fax: +49 180 524 24 71
E-Mail: support.energy@siemens.com
siemens.com/csc

Artikel-Nr. EMDG-T10100-00-00DE
Gedruckt in Deutschland
Dispo 06200
BG184-000595-00 | 08170.5