Bild: Markus Spiske/unsplash

IT-Sicherheit in der Energieautomation

Tiefgreifender IT-Schutz | Sowohl die steigende Anzahl sicherheitskritischer Vorfälle als auch die aktuellen gesetzlichen Anforderungen stellen eine grosse Herausforderung für Betreiber kritischer Infrastrukturen dar. IT-Sicherheit muss in steuernden Geräten tiefgreifend verankert sein, um in Gesamtanlagen ausreichenden Schutz zu bieten.

TEXT STEPHAN HUTTERER

Regelmässig berichten Medien über sogenannte Cyberangriffe. Ziele sind dabei Regierungen, Banken oder Unternehmen mit umfangreichen Datenbeständen. Aber auch im Bereich kritischer Infrastrukturen kann eine signifikante Zunahme solcher Attacken festgestellt werden. Auf europäischer Ebene wurde bereits reagiert und im August 2016 die sogenannte NIS (Network and Information Security) Directive [1] verabschiedet, um in den kritischen Sektoren ein gemeinsames Sicherheitsniveau zu erreichen. Die EU-Mitgliedsstaaten müssen diese Richtlinie bis Mai 2018 in ihre nationalen Gesetzgebungen implementiert haben.

In der Schweiz bestehen ebenfalls Regularien mit gleichartigem Ziel. Vor über fünf Jahren war die «Nationale Strategie zum Schutz vor Cyber-Risiken (NCS)» verabschiedet und bis 2017 umgesetzt worden. Das ISB (Informatiksteuerungsorgan des Bundes) erhielt mittlerweile den Auftrag, eine Nachfolgestrategie auszuarbeiten. Diese Strategie wird zusätzliche Massnahmen beinhalten, wie beispielsweise die Umsetzung von Meldepflichten – so wie auch die NIS-Directive der EU.

Infrastrukturbetreiber – wie etwa Stromnetzbetreiber – stehen in diesem Kontext vor neuen technologischen und ökonomischen Herausforderungen, um IT-Sicherheit in ihren Anlagen

zu implementieren. Hersteller von Geräten und Anlagen sind hier gefragt, ökonomische und vor allem praktikable Lösungen anzubieten, um ihre Kunden bestmöglich zu unterstützen.

Mit Sprecon bietet Sprecher Automation eine modulare Automatisierungsplattform unter anderem zur Energieübertragung und Energieverteilung, welche für den Einsatz in kritischen Infrastrukturen entwickelt wurde. Alle Sicherheitsfunktionen, welche Betreiber bei der Umsetzung gesetzlicher Forderungen unterstützen, stehen dabei standardmässig zur Verfügung. Diese werden bereits in zahlreichen Anlagen sowohl im deutschsprachigen Raum als auch darüber hinaus eingesetzt, um zielsicher die gesetzlichen Vorgaben bezüglich IT-Sicherheit erfüllen zu können.

Tiefgreifend geschützt durch Defense-in-Depth

Ein durchgehend geschütztes System verlangt nach ausgereiften Mechanismen auf allen Ebenen. Im deutschsprachigen Raum etablierte Vorgaben wie etwa das BDEW-Whitepaper [2] fordern in diesem Kontext bezüglich einer sicheren Systemarchitektur das zentrale Defense-in-Depth-Prinzip. Dieses beschreibt die generelle Notwendigkeit, auf allen Systemebenen ineinandergreifende Sicherheitskonzepte vorzusehen, um so einen durchgehenden Schutz zu gewährleisten. Diese Herangehensweise bringt den klaren Vorteil, dass ein potenzieller Angriff – selbst wenn eine hierarchisch aussenliegende Sicherheitsmassnahme überwunden werden konnte – keine weiteren tiefgehenden Sicherheitsmechanismen ausser Kraft setzen kann.

Bezogen auf Automatisierungs- und Schutzgeräte würde dies etwa bedeuten, dass auf einer aussenliegenden Sicherheitsschicht beispielhaft Verschlüsselungsverfahren sowie Netzwerksegmentierung zur Netzwerksicherheit angewendet werden. Im Falle einer Überwindung dieser Mechanismen und Manipulation gesendeter Daten aber sorgen schliesslich darunterliegende Schichten für Sicherheit, wo zum Beispiel das Gerät potenzielle Manipulationen in empfangenen Nachrichten erkennen und darauf reagieren kann.

Defense-in-Depth ist somit ein grundlegendes Konzept in der Systemarchitektur von zu sichernden digitalen

Bild 1 Defense-In-Depth bei Sprecon.

Bild 2 Access Control mit zentraler Benutzerverwaltung.

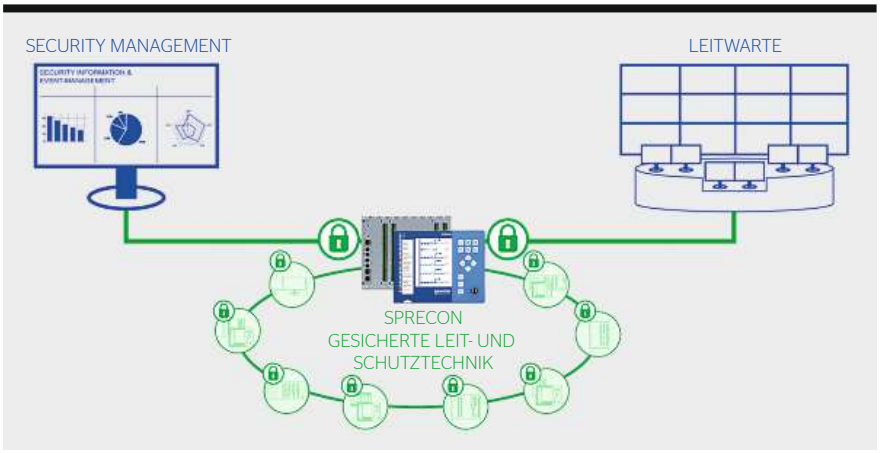

Bild 3 Einbindung der Schutz- und Leittechnik in zentrale Security-Management-Systeme.

Systemen, welches nicht nur allgemein relevant ist, sondern auch konkret von in der Energiebranche relevanten Richtlinien und Standards, wie etwa dem BDEW-Whitepaper oder aber in der IEC 62351 [3], gefordert wird und somit umzusetzen ist.

Praktische Realisierung in modernen Geräten

Bezogen auf ein Schutz- oder Automatisierungsgerät können nun prinzipielle Ebenen beziehungsweise Sicherheitsziele definiert werden, hierarchisch von innen nach aussen gegliedert, welche folgend im Detail diskutiert sowie in **Bild 1** dargestellt werden:

Systemintegrität

Das Stichwort Systemintegrität umfasst sämtliche Massnahmen, um eine Manipulationsfreiheit von Prozessen und Daten am Gerät sicherzustellen. Bezogen auf Daten bedeutet dies primär die Prüfung empfangener Daten auf Validität respektive Plausibilität sowie Korrektheit. Dies betrifft dabei sowohl empfangene Prozessda-

Bilder: Sprecher Automation GmbH

ten, also etwa Fernwirktelegramme beziehungsweise deren Inhalte, aber auch auf das Gerät übertragene Konfigurationen. Mittels kryptografischer Integritätsmechanismen müssen übergebene Daten stets prüfbar sein, wodurch eine mögliche Manipulation der Daten etwa durch Man-in-the-Middle-Attacken erkannt und vom Gerät behandelt werden kann.

Die Manipulationsfreiheit von Prozessen ist ein gleichartig wichtiges Thema. Primär müssen Möglichkeiten geschaffen werden, um sicherzustellen, dass Geräte nur mit gültiger, vom Hersteller ausgelieferter Firmware betrieben werden können, beispielsweise durch die Anwendung von Signaturen der Firmware. Aufgrund dieser Signatur kann die Hardware schliesslich prüfen, ob die eingespielte Firmware gültig und vom Hersteller signiert, und somit manipulationsfrei ist. Das notwendige Gegenstück hierfür ist ein mittels eingebautem kryptografischem Modul ermöglichter Mechanismus, welcher mit einem vom Hersteller bei der Produktion ausgestellten Zertifikat die Firmware prüfen kann. Würde eine manipulierte Firmware in das Gerät eingespielt, stimmte die Signatur nicht mehr überein, und das Gerät kann den Start blockieren beziehungsweise entsprechende Benachrichtigungen sowie eine Fehlerbehandlung einleiten.

Systemhärtung

Sämtliche Massnahmen im Bereich der Systemintegrität schützen das Steuerungssystem auf unterster Ebene. Für den Zugriff aus dem Netzwerk müssen vorgelagerte Schutzmechanismen implementiert werden, um im Vorhinein bereits Zugriffe auszuschliessen respektive diesen grundlegenden Schutz zu ergänzen. In diesem Sinne sind potenzielle Angriffsvektoren aus dem Netzwerk auf ein Minimum zu beschränken – was wiederum durch umfängliche netzwerktechnische Systemhärtung erfolgen muss.

Grundlage hierfür ist eine umfangreiche und vollständig integrierte Firewall am Schutz- beziehungsweise Leittechnikgerät. Diese ermöglicht, den Netzwerkverkehr einzuschränken, um letztlich nur mehr kommunizierte Pakete von und zu im Voraus festgelegten Geräten im Netzwerk zuzulassen. Integrierte Firewalls bieten somit einen elementaren und ebenso generischen Baustein für die Sicherheit eines Gerätes, welcher in keiner praktischen Umsetzung fehlen darf.

Neben der Firewall für die netzwerktechnische Härtung müssen ebenfalls Härtungsmassnahmen auf Betriebssystemebene ergriffen werden. Dementsprechend darf ein System nur die tatsächlich verwendeten Dienste betreiben und diese auch im Netzwerk anbieten. Wird beispielsweise eine Weboberfläche für Analyse oder Konfiguration des Gerätes angeboten, jedoch vom Betreiber nicht verwendet, so bietet diese ein signifikantes und gleichermassen unnötiges Risiko. Unbenötigte Dienste und besonders Netzwerkports müssen somit in jeder projektspezifischen Konfiguration erhoben und deaktiviert werden, um das Angriffsrisiko auf ein Minimum zu beschränken.

Ebenfalls muss auf Betriebssystemebene das (Minimal-)Need-To-Know-Prinzip angewendet werden. Demnach dürfen Benutzer und Prozesse am System nur die zur Ausführung ihrer Funktion notwendigen Rechte besitzen. Während auf Betriebssystemebene per Architekturentwurf Softwareprozesse stets nur mit minimalen Rechten ausgestattet werden, wird dieses Prinzip nach aussen hin fortgesetzt in Richtung Benutzerverwaltung für Wartungs- und Inbetriebnahmepersonal.

Access Control und Benutzerverwaltung

Ein Produkt muss generell die Authentifizierung eines Benutzers erzwingen, bevor dieser auf Konfiguration oder Funktion zugreifen kann. Zusätzlich ist eine rollenbasierte Autorisierung grundlegend, bei welcher ein Benutzer nur jene Berechtigungen erhält, die er

RÉSUMÉ

La sécurité informatique dans l'automatisation énergétique

La protection informatique doit être ancrée dans les appareils de commande

Tant le nombre croissant d'incidents critiques en matière de sécurité que les exigences légales actuelles représentent un grand défi pour les exploitants d'infrastructures critiques. La sécurité informatique doit être profondément ancrée dans les appareils de commande afin d'offrir suffisamment de protection dans les installations entières.

Les cyberattaques augmentent de manière significative, notamment dans le domaine des infrastructures critiques. À l'échelle européenne, on a déjà réagi en adoptant, en août 2016, la directive sur la sécurité des réseaux et des systèmes d'information (« directive NIS » pour « Network and Information Security ») afin d'atteindre un niveau de sécurité commun dans les secteurs critiques.

En Suisse aussi, il existe des réglementations qui poursuivent un objectif similaire. La « Stratégie nationale de protection contre les cyberrisques (SNPC) », adoptée il y a plus de cinq ans déjà, a été mise en œuvre jusqu'en 2017. L'Upic (Unité de pilotage informatique de la Confédération) a depuis reçu le mandat d'élaborer une stratégie pour y faire suite. Celle-ci contiendra des mesures supplémentaires, telles que la mise en œuvre d'obligations de déclarer – comme le prévoit aussi la directive NIS de l'UE.

Dans ce contexte, les exploitants d'infrastructures – tels que les gestionnaires de réseau électrique – se trouvent face à de nouveaux défis technologiques et économiques pour implémenter la sécurité informatique dans leurs installations. Les fabricants d'appareils et d'installations sont donc appelés à proposer des solutions économiques et surtout applicables pour soutenir au mieux leurs clients.

De nombreux clients de Sprecher Automation utilisent d'ores et déjà des systèmes de technique de conduite et de technique de protection intégrant des fonctions de sécurité. Cela permet aux gestionnaires de réseau de distribution et de transport, aux entreprises de transports publics et aux entreprises communales comme les services industriels d'exploiter sans souci leurs installations énergétiques. MR

zur Ausführung seiner Tätigkeit benötigt. Dabei kann beispielsweise zwischen Berechtigungen für Schutz- und Leittechnik unterschieden werden, oder etwa eine sicherheitskritische Konfiguration für ausgewählte Personen erlaubt sein. Um Benutzer, deren Berechtigungen und Passwörter praktikabel unternehmensweit verwalten zu können, hat sich in der Anlagentechnik ebenfalls die Einbindung in zentralisierte Systeme zur Benutzerverwaltung etabliert.

Sprecon unterstützt hierfür das standardisierte Radius-Protokoll, mit welchem zentrale Dienste wie etwa Windows Active Directory für die Benutzerverwaltung einfach eingebunden werden können. Dies ist exemplarisch in **Bild 2** dargestellt. Es erlaubt die zentrale Verwaltung aller Benutzer und deren Berechtigungen. Dabei unterstützt das System standardmässig eine Vielzahl an Rollen zur Zuordnung auf Benutzer, um ein rollenbasiertes Rechtemanagement nach IEC 62351-8 zu ermöglichen. In aktuellen Projekten wurden bereits Hunderte Geräte über Radius in eine zentrale Benutzerverwaltung eingebunden.

Netzwerk-Monitoring und -Management

Für die allgemeine Sicherheit von Anlagen ist die Überwachbarkeit und auch zentrale Erfassung aller im Netzwerk befindlichen Komponenten eine grundlegende Anforderung. Alle potenziell sicherheitsrelevanten Vorgänge müssen erfasst und mit Zeitstempel versehen werden. Beispielsweise müssen alle Benutzerlogin-Versuche geloggt und somit auditierbar sein. Derartige Loggings sind nicht nur auf den jeweiligen Geräten gesichert abzulegen, sondern sollten normkonform auch über ein standardisiertes Protokoll (Syslog) zu zentralen Netzwerk-Monitoringsystemen übertragen werden.

Neben Logging ist für ein funktionierendes Patchmanagement zudem die Inventarisierung sämtlicher Geräte im Netzwerk notwendig (Asset-Management), dies kann standardisiert mit SNMPv3 gesichert realisiert werden. Somit ergibt sich eine in **Bild 3** beispielhaft dargestellte Situation: Während die klassische Leitwarte der funktionellen Überwachung von Anlagen dient, werden parallel dazu zentrale Security-Management-Systeme betrieben, welche zum Beispiel dieses Monitoring ermöglichen, oder auch in Bezug auf die vorhin genannte «Access Control» die zentralisierte Benutzerverwaltung zur Verfügung stellen.

Netzwerksicherheit und kryptografische Funktionen

Gerade bei der Übertragung von Daten über Weitbereichsnetzwerke (WAN) müssen Integrität, Authentizität, und gegebenenfalls auch Vertraulichkeit von Daten sichergestellt werden. Über entsprechende Verschlüsselungsmechanismen, welche direkt von den Geräten umgesetzt werden – so etwa VPN-Technologien – kann hierbei standardisiert eine sichere Verschlüsselung aufgebaut werden. Neben Verschlüsselung ist ebenfalls Netzwerksegmentierung eine wichtige Methodik, wobei etwa die Abschottung des Stationsnetzwerkes vom WAN über integrierte Firewalls in den Leittechnikgeräten oder auch die logische Separierung von Daten über virtuelle LANs (VLANs) als beispielhafte Massnahmen anzuführen sind.

Patching und Patch-Management

Alle eingesetzten Produkte müssen patch-fähig sein. Dies bedeutet insbesondere, dass der Hersteller bei kritischen Sicherheitslücken wie etwa in Betriebssystemen oder in Firmware aktualisierte Versionen zur Verfügung stellt und diese anschliessend in den betriebenen Geräten eingespielt werden. Dies erfordert einerseits vom Hersteller ein aktives Schwachstellenmanagement, aber besonders auch, dass praktikable Kommunikationswege zwischen Hersteller und Betreiber implementiert werden. Geräteherstellen haben hierfür auch zielführende Massnahmen zu setzen in Richtung ISMS-Einführung und ISO-27001-Zertifizierung, welche die Produktentwicklung umfasst. Schwachstellenmanagement wird dabei als Massnahme in das interne ISMS integriert und gelebt. Gemäss den genannten Richtlinien sollten ebenfalls skalierbare Wartungsverträge abschliessbar sein, welche die konkreten Dienstleistungen zu Patch-Information, Test und Installation definieren.

Umsetzung in der Praxis

Die in diesem Artikel genannten Sicherheitsfunktionen sollen die wichtigsten Eckpfeiler zur Herstellung sicherer Automatisierungssysteme umreissen. Diese Eckpfeiler werden ebenfalls in aktuellen facheinschlägigen Standards und Regularien gefordert, und bilden somit die Grundlage für eine moderne Sekundärtechnik.

Aktuelle Lösungen für Schutz- und Leittechnik sollten derartige Funktionen bereits heute bieten, da diese den Stand der Technik bilden werden. Somit können zukünftige gesetzliche Forderungen bereits bei aktuellen Neuanschaffungen berücksichtigt werden. Viele Kunden von Sprecher Automation setzen bereits Leit- und Schutztechniksysteme mit integrierten Security-Funktionen für den unbesorgten Betrieb ihrer Energieanlagen ein – von Übertragungs- und Verteilnetzbetreibern über Transportunternehmen bis zu kommunalen Betrieben wie beispielsweise Stadtwerke.

Referenzen

[1] ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[2] «Anforderungen an sichere Steuerungs- und Telekommunikationssysteme», Whitepaper, Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW), überarbeitete Version 1.1, März 2015, www.bdew.de.

[3] International Electrotechnical Commission: IEC 62351 – Power systems management and associated information exchange – Data and communications security.

Autor

Dr. **Stephan Hutterer** arbeitet im Produktmanagement Schutz- und Leittechnik bei Sprecher Automation GmbH in Linz.
→ Sprecher Automation GmbH, A-4018 Linz
→ stephan.hutterer@sprecher-automation.com