Kritische Infrastrukturen, zu denen auch die Stromversorgung gehört, müssen im Besonderen vor Cyber-Angriffen geschützt werden.

Versorgungssicherheit dank OT-Security

Zertifizierte Sicherheit | Cyber-Angriffe machen auch vor Energieversorgern nicht Halt: Axpo hat einen Best-Practice-Ansatz gewählt, um die Stromnetzinfrastruktur zu schützen. Als eine der ersten Energieversorgerinnen der Schweiz hat die Axpo Grid AG die Zertifizierung ISO 27001 Informationssicherheit für ihre Prozessinformatik erhalten.

THOMAS LEIMGRUBER, TOBIAS LEDERER

Mittwoch, 9. September 2020, 23.45 Uhr: Der Chief Information Officer eines Schweizer Energieversorgungsunternehmens überprüft ein letztes Mal die Systeme, bevor er sich schlafen legt – alles «up and running». Nur wenige Stunden später verschlüsseln unbekannte Angreifer die Systeme, alle Server fallen aus. Das Unternehmen war Opfer eines Cyber-Angriffs geworden. Die Cyber-Kriminellen forderten Geld. Solche und ähnliche Vorfälle sind zu einer realen Bedrohung geworden, und die Energiebranche – wie auch Betreiber anderer kritischer Infrastrukturen – steht bei Cyber-Kriminellen im Fokus.

Cyber-Sicherheit hat viele Aspekte

Seit 2016 befasste sich Axpo im Rahmen einer VSE-Arbeitsgruppe mit dem Thema Operational Technology Security (OT-Security), also mit den Strategien und Prozessen zum Schutz von kritischen Infrastrukturen und Daten. Die Axpo Grid AG befand sich diesbezüglich schweizweit im guten Mittelfeld. Doch eine erste Analyse des Ist-Zustands und die Bewertung anhand der VSE-Branchenempfehlung [1] zeigte Handlungsbedarf auf. So können zum Beispiel ungeschützte Verbindungen, das fehlende Bewusstsein der Mitarbeitenden für Cyber-Sicherheit, Fernzugriffe durch externe Hersteller oder langlebige Komponenten ohne regelmässige Sicherheits-Updates Schwachstellen darstellen.

Mit dem Ziel, sich im Bereich OT-Security bei der Infrastruktur des eigenen überregionalen Verteilnetzes auf

Bilder: Axpo Grid AG

den neusten Stand zu bringen und eine «Best Practice» für Energieanbieter zu schaffen, rief die Axpo Grid AG ein Projekt ins Leben, um die Maturität in diesem Bereich zu erhöhen. Zuerst wurden auf der organisatorischen Ebene die Grundsätze und Kriterien für die OT-Security festgelegt, Arbeitsprozesse beschrieben und Anforderungen definiert. Anschliessend wurden die definierten Vorgaben in einem Realisierungsprojekt umgesetzt. Diese Vorgaben werden konstant weiterentwickelt.

Intensives Monitoring mit Datennetzsensoren

Obwohl sich die Sicherheit von OT und IT unterschiedlich entwickelt haben, fliessen sie durch die Standardisierung von Betriebssystemen und Internetprotokollen zunehmend ineinander. Zu den Kernthemen der OT-Security gehören die Zonierung des Datennetzwerks und das Monitoring von Aktivitäten zwischen den Geräten aller Art im Netz. Zonierungen verhindern laterale Bewegungen in einem Netzwerk, erschweren so einen Angriff auf die Infrastruktur und erlauben eine bessere Kontrolle über den Datenverkehr **(Bild 1).**

Mit einem Monitoring verschafft sich Axpo einen Überblick, ob und in welchem Ausmass die Infrastruktur der Verteilnetzbetreiberin von Angriffen oder Unregelmässigkeiten betroffen ist. Dazu wurden in den Datennetzwerken der Unterwerke IDS-Sensoren (Intrusion Detection System) installiert. Diese intelligenten Systeme überwachen den Datenverkehr und melden abnormale Aktivitäten. Tritt ein verdächtiger Vorgang auf, wird das Security Operation Center der Axpo WZ Systems AG informiert. Dieses leitet dann gegebenenfalls eine tiefergehende Untersuchung ein **(Bild 2).**

Das Monitoring ist aber erst die halbe Miete: Genauso wichtig ist, festzulegen, wie mit einem Cyber-Angriff umzugehen ist. Die Prozesse dafür wurden sorgfältig erarbeitet und in einem «Incident-Management-System» standardisiert. Neben Prozessen, die festlegen, wie organisatorisch mit einem Vorfall umgegangen wird, besteht ein Handbuch mit «Use Cases». Diese Use Cases klassifizieren und beschreiben meldepflichtige Ereignisse sowie sogenannte «Runbooks», die im Falle eines Vorfalls detaillierte Vorgehensweisen auch im Krisenmodus sicherstellen.

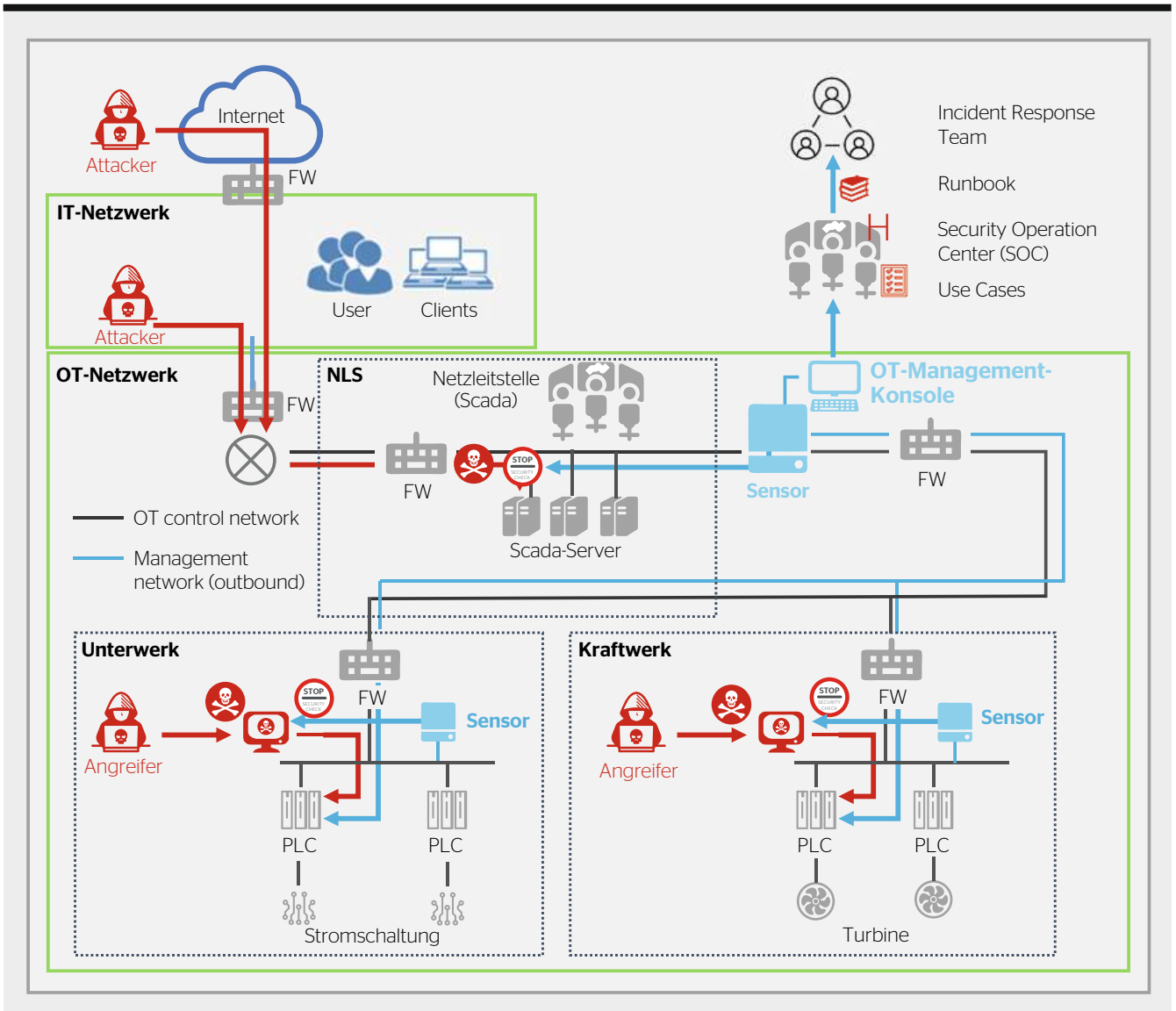

Bild 1 Die OT-Sicherheits-Landschaft ist komplex. Ein konkretes Vorgehen, wie mit einem Cyber-Angriff umzugehen ist, ist unerlässlich.

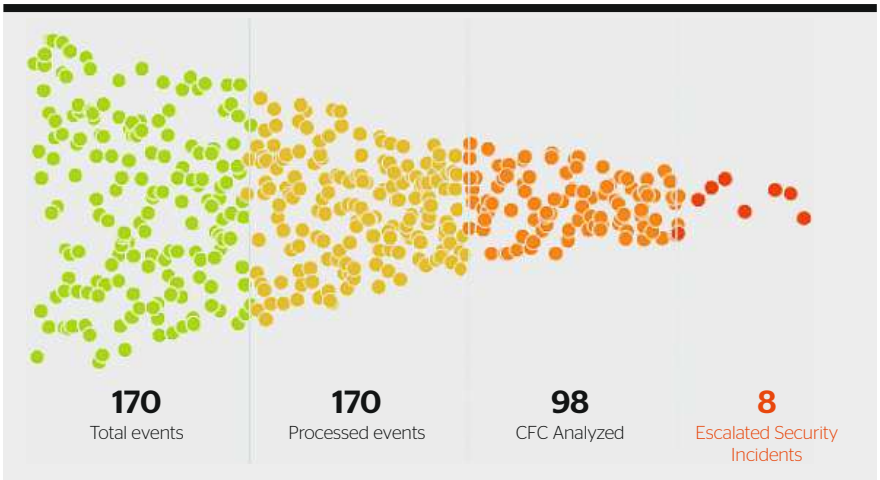

Bild 2 Cyber-Sicherheit: Monatlich werden die Überwachungsmeldungen bei Axpo kategorisiert und ausgewertet.

Alle Anlagen auf einen Nenner bringen

Während früher in Energieversorgungsanlagen oft alle Anlagenteile in einem einzigen flachen unstrukturierten Datennetzwerk zusammengefasst waren, erlauben dies die definierten Zonenkonzepte nicht mehr. So galt es, die notwendige technische Grundlage für eine durchgehende Zonierung zu schaffen. Neue redundante Switches, Router und Firewalls hielten Einzug in den Werken, bei der Netzleitstelle sowie in der übergeordneten Kommunikationsstruktur. Die Adressierungen jedes Geräts wurden einer Zone zugeordnet. Aufgrund einer anlagenspezifischen Kommunikationsmatrix wurde schliesslich genau festgelegt, welche Geräte untereinander kommunizieren dürfen.

In den Unterwerken trafen die Projektverantwortlichen dabei auf Infrastrukturen und Geräte unterschiedlicher Baujahre, denn eine Lebensdauer von über 20 Jahren ist im OT-Bereich keine Seltenheit. So galt es, die Anlagenteile aufgrund ihres Alters und ihrer Eigenschaften sinnvoll zu gruppieren und schliesslich die Modernisierungs- und Sicherheitsmassnahmen in Etappen umzusetzen – eine komplexe Aufgabe. Mit dem übergeordneten Schutzziel vor Augen, werden die Anlagen fortan kontinuierlich erneuert, um den hohen Anforderungen an die OT-Security zu entsprechen. Der Aufwand dabei ist beträchtlich. So werden unter anderem Dutzende Windows-basierte Systeme zur Steuerung und Überwachung der Unterwerke erneuert. Durch die bereits oben genannten Herausforderungen in Bezug auf Lebensdauer sowie die hohe Diversität an Herstellern, Applikationsständen und Technologiearchitektur lassen sich Konzepte nicht problemlos von Anlage zu Anlage replizieren, was teilweise die Umstellung auf einen Betrieb mit virtuellen Maschinen notwendig macht.

Ein Thema, das in der IT bereits Best Practice ist, wird künftig auch in der OT immer wichtiger: System- und Software-Updates auf den Anlagen in den Kraft- und Unterwerken. Jedes Update ist mit sehr viel Prüfaufwand verbun-

RÉSUMÉ

La sécurité d'approvisionnement grâce à la sécurité des OT

Sécurité certifiée

Depuis 2016, dans le cadre d'un groupe de travail de l'AES, Axpo s'est intéressée au thème de la sécurité des technologies opérationnelles (OT), c'est-à-dire aux stratégies et aux processus visant la protection des infrastructures et des données critiques. Dans ce domaine, Axpo Grid AG se trouvait, en comparaison à l'échelle suisse, en bonne position. Mais une première analyse de l'état actuel et l'évaluation au moyen de la recommandation de la branche de l'AES « Manuel Protection de base pour les ‹technologies opérationnelles› (OT) dans l'approvisionnement en électricité » a révélé que des interventions étaient nécessaires. Par exemple, des connexions non protégées, le manque de conscience du personnel sur la cybersécurité, des accès à distance pour des fabricants externes ou encore des composants de longue durée sans mises à jour de sécurité régulières peuvent représenter des points faibles.

Axpo Grid AG s'est fixé pour objectif de se mettre à jour dans le domaine de la sécurité des OT au niveau de l'infrastructure de son réseau de distribution suprarégional et de créer une « meilleure pratique » pour les fournisseurs d'énergie. Pour ce faire, l'entreprise a mis sur pied un projet visant à améliorer la maturité dans ce domaine. D'abord, les principes et les critères de la sécurité des OT ont été fixés au niveau organisationnel, les processus de travail, décrits et les exigences, définies. Ensuite, on a mis en œuvre les prescriptions définies dans un projet de réalisation.

La mise en œuvre des projets à large portée ainsi que la construction d'un système global de gestion de la sécurité de l'information ont permis à Axpo d'atteindre un haut degré de maturité pour sa cybersécurité des OT, ce qui lui a valu la certification selon la norme ISO 27001 pour la sécurité de l'information et des mesures complémentaires spécifiques aux secteurs issues de la norme ISO 27019 pour les fournisseurs d'énergie. Non seulement cette certification, obtenue en avril 2022, renforce la confiance en Axpo, mais elle oblige aussi l'entreprise à maintenir la cybersécurité de ses installations à l'état le plus avancé de la technique grâce au système de gestion de la sécurité des OT et à poursuivre son développement en continu. Surtout, le certificat garantit le bénéfice durable des investissements considérables effectués par Axpo. MR

OT oder IT?

Im Bereich Operational Technology (OT) sind Geräte und Anlagen angesiedelt, die direkt an physischen Produktionsprozessen beteiligt sind – zum Beispiel in einem Kraftwerk die Schutz-, Steuer- und Regelungseinrichtungen einer Turbine oder in Unterwerken Systeme der Leitungsfelder oder Transformatoren sowie die dafür benötigten Kommunikationsinfrastrukturen. Im Gegensatz dazu beschäftigt sich die Information Technology (IT) mit der kommerziellen Datenverarbeitung, die nicht direkt mit physischen Prozessen verknüpft ist.

Mit der OT-Security lassen sich industrielle Systeme überwachen und schützen, insbesondere vor kriminellen Angriffen beispielsweise via Internet. Ein umfassendes OT-Security-System besteht dabei sowohl aus einem organisatorischen Konzept als auch aus technischen Massnahmen an den Anlagen.

den, um den hochverfügbaren und sicheren Betrieb der Hochspannungsanlagen zu garantieren. In verschiedenen Projekten ist Axpo seit zwei Jahren in der Planung und Vorbereitung der Umsetzung, um solche Updates auch in der OT-Umgebung künftig möglichst automatisiert durchzuführen.

ISO-zertifiziert und hochmotiviert

Mit der Umsetzung der weitreichenden Projekte sowie dem Aufbau eines umfangreichen Informationssicherheits-Managementsystems erreichte die Cyber-Sicherheit für die OT von Axpo einen hohen Reifegrad. Sie resultierte in der Zertifizierung gemäss ISO-Norm 27001 (Axpo Grid AG und Axpo WZ Systems AG) für Informationssicherheit und ergänzenden sektorspezifischen Massnahmen aus ISO 27019 (Axpo Grid AG) für die Energieversorger. Die vor Kurzem erfolgte Zertifizierung stärkt nicht nur das Vertrauen in Axpo, sondern verpflichtet das Unternehmen auch, mit dem OT-Security-Managementsystem die Cyber-Sicherheit seiner Anlagen auf dem Stand der Technik zu halten und kontinuierlich weiterzuentwickeln. Nicht zuletzt sichert das Zertifikat zudem den nachhaltigen Nutzen der seitens Axpo getätigten, erheblichen Investitionen.

Die Axpo Grid AG zählt zu den ersten Energieversorgerinnen der Schweiz, die für ihre OT-Security diese Zertifizierung erhalten hat. Damit sollen auch andere Energieversorger motiviert werden. Denn es ist davon auszugehen, dass eine Zertifizierung für Schweizer Energieversorger in Zukunft Pflicht wird, wie es im umliegenden Ausland bereits der Fall ist, denn das Schweizer Stromnetz ist nur so stark und zuverlässig, wie jeder einzelne Akteur in diesem Bereich.

Referenz

[1] «Handbuch Grundschutz für ‹Operational Technology› in der Stromversorgung», VSE, 2018.

Autoren

Thomas Leimgruber ist Leiter Verkauf und Projektmanagement bei Axpo Grid AG.
→ Axpo Grid AG, 5401 Baden
→ thomas.leimgruber@axpo.com

Tobias Lederer ist Leiter OT-Unterwerke & Leittechnik bei Axpo Grid AG.
→ tobias.lederer@axpo.com