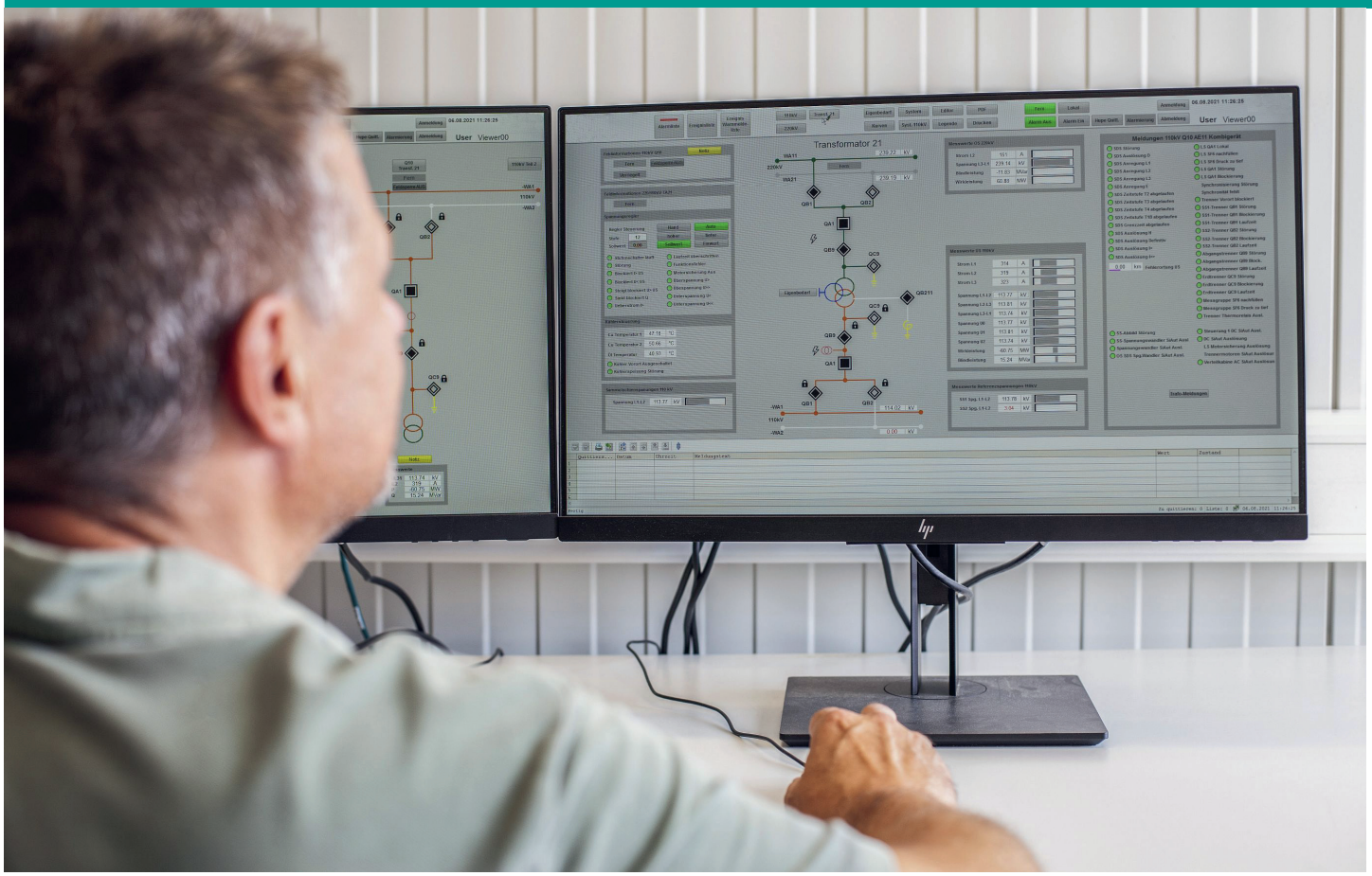

Supportprozesse müssen im Notfall einen minimalen Betrieb aufrechterhalten können.

OT-Security im Unterwerk

Business Continuity Management | Cyberangriffe auf kritische OT-Infrastruktur in Unterwerken treten immer häufiger auf. Um den Betrieb in Notfallsituationen sicherzustellen, erarbeitete Axpo ein Konzept, das verschiedene Resilienz-Strategien vereint. Dazu gehören Redundanz und Air Gap (Isolierung) sowie die betriebliche Bereitschaft für Ausnahmesituationen.

OLIVER KINDERMANN, DANIEL SCHIRATO

Zahlreiche Cyberangriffe auf OT-Infrastrukturen (OT = Operational Technology) der vergangenen Jahre zeigen, dass die Bedrohung für die Stromversorgung weiterhin hoch ist. Beim Cyberangriff vom 10. Oktober 2022 in der Ukraine wurden 4000 Dörfer und Städte der Ukraine vorsätzlich vom Stromnetz getrennt [1,2]. Nach dem eigentlichen Angriff wurde sogar versucht, die Wiederherstellung des Betriebs zu verhindern. Neben Denial-of-Service-Angriffen wurden Konfigurationsdaten mittels «Wipern» gelöscht.

Minimalbetrieb aufrechterhalten

Ein hundertprozentiger Schutz gegen solche Angriffe ist weder technisch noch wirtschaftlich umsetzbar. Neben präventiven Schutzmassnahmen in Datennetzwerksicherheit und Systemhärtung muss deshalb auf die Resilienz geachtet werden. Widerstandsfähigkeit bedingt ein effektives Business Continuity Management (BCM) und Disaster Recovery Management (DRM), die vorgeben, wie eine Anlage trotz Ausfällen von Komponenten weiterbetrieben und rasch wieder in den Normalbetrieb geführt werden kann. Axpo hat im Rahmen des zukünftigen OT-Sekundärtechnikkonzepts einige Ansätze analysiert und auf den Weg gebracht.

Supportprozesse analysieren

Die Kernprozesse eines Unterwerks sind die sichere Verteilung und Transformation der elektrischen Energie. Diese Prozesse werden durch Supportprozesse wie dem Netzschutz sichergestellt. Fällt dieser aus, ist ein Betrieb des Unterwerks (UW) nur mit hohen Risiken für Menschen und gegebenen-

Bilder: Axpo Grid AG

falls auch für die Umwelt möglich. Die OT umfasst viele dieser Supportprozesse und stellt den Betrieb des Unterwerks sicher. Anhand einer Umfrage bei der Betriebsabteilung hat Axpo die wesentlichen Supportprozesse ermittelt:

- Netzschutz für einen sicheren Betrieb des UW
- Eigenbedarf: OT-Stromversorgung
- Zustandsüberwachung des UW
- Steuerung des UW bei eingeschränktem Netzbetrieb

Die Dringlichkeit, mit der ein Supportprozess nach einem Ausfall wiederhergestellt werden muss, hängt vom jeweiligen Prozess ab und kann sich deutlich unterscheiden. Die Fernsteuerung des Unterwerks von der zentralen Netzleitstelle aus kann über mehrere Wochen ausfallen, da im Notfall vor Ort geschaltet werden kann. Beim Netzschutz hingegen muss innerhalb von Stunden ein Minimalbetrieb wiederhergestellt sein.

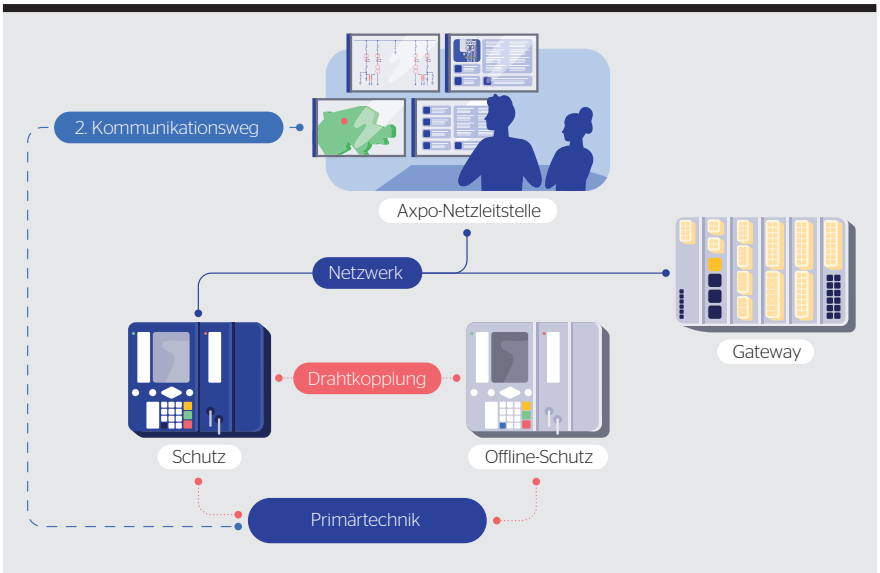

Bild 1 Ein zusätzliches Schutzgerät, das nicht über das OT-Netzwerk kommuniziert, stellt den Netzschutz im Unterwerk bei einem Cyberangriff sicher.

Hintergrund

Business Continuity Management

Das Business Continuity und Disaster Recovery Management hat das Ziel, den Betrieb in Notfallsituationen sicherzustellen. Es ist auch ausserhalb der Welt der Cybersicherheit weit verbreitet.

Die klassischen Frameworks der Informations- und Cybersicherheit, wie ISO/IEC 27001 und 22301 sowie das Cyber Security Framework des National Institute of Standards and Technology (NIST), enthalten Massnahmen zur Reaktion auf Störungen im Betrieb. Wesentliche Kernaufgaben des BCM und DRM sind:

- **Die Identifikation der Kernprozesse, die durch Cyberangriffe oder technische Störungen bedroht sind.**
- **Die Zusammenstellung und Gap-Analyse der technischen, organisatorischen und regulatorischen Anforderungen.**
- **Die Ermittlung der eigenen Bereitschaft im BCM/DRM im Vergleich zu einem Zielbild.**
- **Die Entwicklung von praxisnahen, wirtschaftlichen und einfach betreibbaren Lösungskonzepten.**
- **Die Integration der Lösungskonzepte in vorhandene Prozesse, wie zum Beispiel Incident Response.**
- **Die kontinuierliche Feststellung der Wirksamkeit in Bezug auf die Bedrohungen der Kernprozesse.**

Netzschutz sicherstellen

Beim erarbeiteten Konzept für das BCM im Unterwerk wurde der Schwerpunkt auf den Netzschutz gelegt. Die anderen Supportprozesse sind bereits besser auf das BCM ausgelegt: Der Eigenbedarf ist batteriegepuffert und die Steuerung sowie die Überwachung des Unterwerks sind vor Ort möglich.

Beim Netzschutz wurde das Szenario eines kompletten Ausfalls in einem Feld oder dem Unterwerk betrachtet. Auch bei segmentierten Netzwerken sind oft alle Geräte im gleichen Segment eines Unterwerks untergebracht. Bei Befall mit Ransomware wäre der gesamte Netzschutz des Unterwerks betroffen. Daher besteht hier der grösste Handlungsbedarf.

Geräte diversifizieren

Die klassischen Ansätze der Literatur geben einen Überblick über Lösungen. Dies beginnt bei gängigen Konzepten zur Ersatzteilhaltung und setzt sich bei der technischen Redundanz von Komponenten fort. Die zusätzlichen Komponenten halten den Betrieb bei einem Ausfall aufrecht – zumindest einen Minimalbetrieb. Die eingesetzten Geräte und Systeme können zudem mit unterschiedlichen Komponenten diversifiziert werden, beispielsweise durch Geräte unterschiedlicher Hersteller, Gerätefamilien mit signifikanten Unterschieden sowie Kommunikationsvarianten. Eine einzelne Schwachstelle kann somit nie die Funktion des Gesamtsystems gefährden. Die Diversität stellt eine Hürde dar, die ein Angreifer überwinden muss. Allerdings muss auch beachtet und akzeptiert werden, dass durch eine grössere Diversität ein Mehraufwand für den Betrieb und somit zusätzliche Kosten entstehen.

Abläufe trainieren

Die organisatorische Bereitschaft ist neben der eingesetzten Hard- und Software ein wesentlicher Erfolgsfaktor. Die Business Continuity und Disaster Recovery muss über geschulte Mitarbeitende und klare Prozesse gestärkt werden. Die Incident Response Fähigkeit wird regelmässig geübt, damit die Wiederherstellungsdauer massgeblich reduziert werden kann.

Sicherstellung der Integrität

Wichtig ist auch das Wissen um den Zustand der Anlage. So kann die Integrität eines OT-Systems automatisiert überprüft werden, beispielsweise mithilfe eines Message Authentication Codes (MAC). Nicht integre Systeme werden so leichter erkannt und können

Bild 2 Das redundante, nicht vernetzte Schutzgerät wird bei Bedarf vor Ort bedient.

schneller aus dem produktiven Betrieb entfernt werden. Letztgenannte Lösung ist jedoch nicht ohne Weiteres auf Unterwerke adaptierbar, da entsprechende Systeme von Herstellern kaum angeboten werden.

Schutzgerät ohne Kommunikation

Axpo hat sich für eine Kombination der Lösungen entschieden. Die Verfügbarkeit des Netzschutzes soll durch eine technische Redundanz erhöht werden, jedoch nicht durch eine reine Verdopplung der Geräte. Ein zusätzliches Gerät für den Rückfallbetrieb soll dieselben Netzschutzfunktionen erhalten, lediglich ohne Netzwerkschnittstellen **(Bild 1)**. Auf diese Weise wird sichergestellt, dass ein Befall des OT-Netzwerks mit Schadsoftware nicht den gesamten Schutz beeinträchtigen kann. Aus demselben Grund werden zudem separate Engineering-Systeme für die Konfiguration der redundanten Schutzsysteme verwendet. Die Informationen über den Zustand des zusätzlichen, redundanten Geräts wird per Drahtkopplung abgeholt. Eine Fernsteuerung ist nicht vorgesehen. Weitere Massnahmen verhindern, dass ein kompromittiertes Gerät auf die Primärtechnik wirken kann.

Normal- und Rückfallbetrieb

Das Lösungskonzept von Axpo hat zwei Betriebsmodi: Im Normalbetrieb sind beide Schutzgeräte aktiv und können auf die Primärtechnik wirken. Fernschaltungen sind nur mit dem Gerät für den Normalbetrieb möglich, da nur dieses Gerät kommunikativ ist. In dieser Situation stehen alle Funktionen des Unterwerks zur Verfügung, und ein effizienter Betrieb über die Netzleitstelle ist sichergestellt.

Im Rückfallbetrieb bleiben beide Geräte eingeschaltet. Das Gerät für den Normalbetrieb wird hingegen in einen Read-Only-Modus versetzt und vom Netzwerk getrennt. Das Gerät für die Rückfallebene stellt hingegen weiterhin den Netzschutz sicher. Sein Zustand kann nur drahtgebunden oder vor Ort am Gerätedisplay ausgelesen werden. Im Notfall kann das Bedienpersonal das Gerät vor Ort steuern **(Bild 2)**.

Der Anlagenzustand im Rückfallbetrieb kann Tage oder Wochen aufrechterhalten werden, da das Unterwerk den Kernprozess «sichere Verteilung und Transformation der elektrischen Energie» erfüllt. Limitierende Faktoren können das Personal oder die Häufigkeit von Schaltungen vor Ort sein, was eine personelle oder finanzielle Herausforderung darstellen kann.

Use Cases definieren

Die Umschaltung zwischen Normal- und Rückfallbetrieb wird in den bestehenden Incident-Response-Prozess von Axpo integriert. Dazu werden Use

RÉSUMÉ

Sécurité OT dans les sous-stations

Gestion de la continuité des activités

Les cyberattaques visant les infrastructures OT critiques dans les sous-stations sont de plus en plus fréquentes. Une protection à 100 % contre ce type d'attaques n'est toutefois ni techniquement ni économiquement réalisable. Outre les mesures préventives en matière de sécurité des réseaux de données et de renforcement des systèmes, il est aussi essentiel de porter une attention particulière à la résilience. Pour garantir la continuité des opérations en situation d'urgence, Axpo a donc élaboré un concept réunissant différentes stratégies de résilience. Cette dernière repose sur une gestion efficace de la continuité des activités (Business Continuity Management, BCM) et de leur reprise après sinistre (Disaster Recovery Management, DRM), ou comment maintenir une installation en fonctionnement malgré des défaillances de composants et la ramener rapidement à un état normal.

Axpo a également examiné, entre autres cas, comment l'opérateur ukrainien victime d'une cyberattaque à grande échelle le 10 octobre 2022 aurait pu bénéficier de la solution BCM présentée dans cet article pour protéger le réseau. Il s'avère que l'attaque aurait tout de même pu perturber l'approvisionnement en électricité, mais que le délai de rétablissement aurait été considérablement réduit. Grâce à une protection du réseau redondante, séparée du réseau OT et donc idéalement non compromise, le fonctionnement normal du réseau aurait pu être rétabli beaucoup plus rapidement, améliorant ainsi la résilience.

Cases und Situationen definiert, die festlegen, wann die Umschaltung auf den Rückfallbetrieb erfolgt – entweder als Sofortmassnahme oder als vorbehaltener Entschluss.

Es braucht eine klare Dokumentation dieser Fälle mittels Runbooks und Festlegung der Entscheidungswege. Wichtig ist auch die Zusammenstellung von Bedingungen für die Rückkehr zum Normalbetrieb. Schliesslich müssen Übungen durchgeführt werden, an denen sämtliche Stakeholder (CSIRT, Fachabteilungen, Netzleitstelle, Betrieb) beteiligt sind. Durch diese Massnahmen wird die Organisation auf echte Notfälle vorbereitet und kann bei Bedarf schneller und wirksamer reagieren.

Wirksamkeit testen

Im Anschluss an das ausgearbeitete BCM-Konzept hat Axpo – neben anderen Fällen – untersucht, wie der ukrainische Betreiber beim eingangs erwähnten Cyberangriff von der vorgestellten BCM-Lösung für den Netzschutz profitiert hätte. Es zeigt sich, dass der Angriff die Stromversorgung weiterhin hätte stören können, die Zeit bis zur Wiederherstellung jedoch erheblich kürzer gewesen wäre. Über den redundanten, vom OT-Netzwerk getrennten und dadurch idealerweise nicht kompromittierten Netzschutz hätte ein normaler Netzbetrieb wesentlich schneller wieder aufgenommen, wodurch sich die Resilienz verbessert hätte.

Präventive Massnahmen bleiben weiterhin unverzichtbar, um die Eintrittswahrscheinlichkeit von technischen Störungen und Cyberangriffen im Normalbetrieb zu senken. Aber das Beispiel aus der Ukraine verdeutlicht, dass das Business Continuity und das Disaster Recovery Management notwendig sind, um bei einem Vorfall zumindest einen minimalen Betrieb aufrechtzuerhalten und die primären Aufgaben eines Unterwerks zu erfüllen – die elektrische Energie zu verteilen und zu transformieren.

Axpo stellt ihr Wissen im Bereich OT-Security aus Projekten, Betrieb und Unterhalt der eigenen Systeme sowie Business Continuity und Disaster Recovery Management als Dienstleisterin gerne auch anderen Betreibern im Bereich kritische Infrastrukturen zur Verfügung [3].

Referenzen

[1] www.nzz.ch/technologie/russischer-cyberangriff-loest-in-ukraine-einen-stromausfall-aus-dieser-neu-artige-angriff-erhoeht-die-gefahr-fuer-kritische-infra-strukturen-auch-im-westen-ld.1764650

[2] cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/?hl=en

[3] www.axpo.com/ch/de/energie/digitale-loesungen/cyber-security-connectivity.html

Autoren

Oliver Kindermann ist Projektingenieur Leittechnik & OT-Security bei Axpo Grid AG.
→ Axpo Grid AG, 5400 Baden
→ oliver.kindermann@axpo.com

Daniel Schirato ist IT/OT Security-Officer bei Axpo Grid AG.
→ daniel.schirato@axpo.com