Grundschutz für Operational Technology

Cyber Security | Die durch Cyberangriffe Ende 2015 und 2016 beeinträchtigte Energieversorgung der Ukraine hat die Auswirkungen eines Hackerangriffs verdeutlicht. Die Prävention gegen Cyber-Risiken hat daher auch politisch an Präsenz gewonnen. Für Schweizer EVUs bedeutet dies, dass künftig Sicherheitskonzepte zu implementieren sind, die auch gesetzlichen Mindestanforderungen genügen müssen.

ANDREAS KLIEN, MARKUS LENZIN, RETO AMSLER

Auf dem politischen Parkett wird das Thema Cybersicherheit seit einigen Jahren immer wieder aufgegriffen. Das Resultat sind mehrere Initiativen und Motionen. Im Rahmen der nationalen SKI-Strategie (Schutz kritischer Infrastrukturen) wurde 2015 beispielsweise ein Leitfaden erarbeitet und die zweite Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) wurde im April 2018 verabschiedet. Mit dem 1. Januar 2018 ist zudem das revidierte Energiegesetz in Kraft getreten. Nach dem Stromversorgungsgesetz sind die Netzbetreiber schon seit 2007 für ein sicheres Netz verantwortlich. Allerdings gehen weder der Gesetzestext noch die Initiativen darauf ein, wie diese Mindestanforderungen in Bezug auf die Cybersicherheit konkret aussehen.

Dies wird sich höchstwahrscheinlich ändern. Die letzte diesbezügliche Motion «Verpflichtender Grundschutz für kritische Strominfrastruktur» wurde zwar 2019 abgelehnt, im Rahmen der Revision des Energiegesetzes jedoch inhaltlich berücksichtigt, und in der Leitlinie für die sichere Energieversorgung soll auch der Schutz von kritischen Infrastrukturen (einschliesslich Informations- und Kommunikationstechnik) erwähnt werden.

Branchenempfehlung

Als Massnahme aus der NCS hat der Verband Schweizerischer Elektrizitätsunternehmen (VSE) im Juli 2018 eine Branchenempfehlung herausgegeben. Das Dokument «Handbuch Grundschutz für Operational Technology in der Stromversorgung» wurde in einer Arbeitsgruppe mit Vertretern des Bundes sowie grösserer EVUs erarbeitet. Dieses Handbuch ergänzt die Branchenempfehlung «ICT Continuity» des VSE und orientiert sich mit seinen 21 empfohlenen Massnahmen an international etablierten Standards für die Sicherheit von OT-Systemen. Als Kernelement wird darin auf das vom NIST (National Institute of Standards and Technology) entwickelte Cyber Security Framework **(Bild 1)** referenziert. Die darin enthaltenen Aktivitäten und Massnahmen müssen vom Unterneh-

Bild: iStock.com/Ziga Plahutar

men in einem wiederkehrenden Prozess laufend überarbeitet und an die aktuelle Bedrohungslage angepasst werden.

Dieses Framework basiert auf dem «Defense-in-Depth»-Prinzip und arbeitet mit fünf Schritten: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Eine Voraussetzung ist, dass man akzeptiert, dass es keinen vollständigen Schutz gegen jegliche Art von Cyber-Bedrohungen geben kann. Auf Basis dieses Bewusstseins über die eigene Verwundbarkeit können dann entsprechende Strategien und Massnahmen entwickelt werden. Am Beginn steht daher die Identifikation von Angriffsvektoren (Identifizieren), um sich in einem weiteren Schritt bestmöglich gegen diese absichern zu können (Schützen). Durchbricht ein Angreifer diese Barrieren, muss der Angriff erkannt (Erkennen) und bestenfalls sofort richtig gehandelt werden (Reagieren), damit sich der Normalzustand so schnell wie möglich wiederherstellen lässt (Wiederherstellen).

Nach diesem Prinzip werden die Anlagen also nicht nur durch einzelne Massnahmen nach dem Motto «Harte Schale, weicher Kern» geschützt, sondern es wird auf mehrere «Schalen» gesetzt, die kontinuierlich überwacht werden. Als Überwachungskomponenten dienen beispielsweise Virenscanner und Intrusion Detection Systeme (IDS). Beide Systeme sollten auch innerhalb von Schaltanlagen eingesetzt werden. Wird eine Schale durchdrungen, beispielsweise durch eine Schadsoftware auf einem Wartungscomputer, kann dies durch einen Virenscanner bzw. das IDS erkannt und sofort darauf reagiert werden. Mit Fokus auf die Schadensminimierung gilt es dann zu analysieren, wie die Schadsoftware überhaupt auf den Rechner gelangen konnte. Die Identifizierung dieses neuen Angriffsvektors ist essenziell, um ihn in Zukunft vermeiden zu können und die Resilienz des gesamten Systems kontinuierlich zu verbessern (Schützen).

Dabei misst der Ansatz dem Zusammenspiel zwischen Menschen, Prozessen und Technik eine hohe Bedeutung bei. Denn die kontinuierliche Überwachung ist nur sinnvoll, wenn auf eine Alarmmeldung eine angemessene und präzise Reaktion folgt.

Ein ganzheitlicher Zugang für mehr Sicherheit

Die Anwendung des Frameworks in der Operational Technology (OT) ist komplex und erfordert eine intensive Auseinandersetzung mit dessen Inhalten sowie spezifisches Fach- und Branchenwissen, um den gewünschten Sicherheitslevel zu erreichen.

Ausgangspunkt für die Umsetzung sollte eine klare Definition der Cyber-Security-Strategie des eigenen Unternehmens sein. Diese ist nicht nur erforderlich für die Entwicklung einer Security-Architektur, sondern stellt auch das Commitment seitens des Managements sicher, das für die kritische Auseinandersetzung mit den bestehenden Prozessen und deren Erweiterung benötigt wird. Ein Aspekt, der nicht zu unterschätzen ist – gilt es doch, in dieser Phase Schwachstellen offen anzusprechen und neue Lösungen zu finden, die unter Umständen auf Widerstand stossen. Mitunter bietet sich für diesen Prozessschritt daher die Inanspruchnahme einer externen Beratung an, die Cyber-Security-Know-how und Erfahrung bereitstellen und das Vorhaben methodisch begleiten kann. Denn am Ende sollten die definierten Massnahmen perfekt ineinandergreifen. Diese umfassen die eingesetzten Technologien, organisatorische und prozessuale Anpassungen sowie notwendige Ausbildungen bezüglich Sensibilität, Verhalten und Arbeitshilfen, wie Checklisten, Anweisungen und Richtlinien. Dies gilt besonders für die kritischen Systemumgebungen der Schutz- und Leittechnik, in welche Überwachungssysteme der Cyber Security eingebettet sind.

Bild 1 Cyber Security Framework Version 1.1.

Umsetzung in Schaltanlagen

Ein Intrusion Detection System (IDS) als Umsetzung des Schritts «Erkennen» stellt damit ein wesentliches Element des Grundschutzes dar. Als letztes Element überwacht es das Netzwerk und schlägt Alarm, wenn es Unregelmässigkeiten in der Kommunikation entdeckt. Nur wenn ein Angriff erkannt wird, können auch entsprechende Handlungen folgen, um Schäden zu minimieren. IDS müssen daher auch neuartige Angriffe erkennen können. Zugleich sollten sie schon nach kurzer Zeit eine möglichst geringe Zahl an Fehlalarmen melden, damit Meldungen nicht irgendwann ignoriert werden. Wenn ein Energieversorger Dutzende Schaltanlagen betreibt und jede Anlage nur ein paar Fehlalarme pro Monat erzeugt, summieren sich diese schnell zu einer beträchtlichen Zahl pro Tag. Weil jeder Alarm von Spezialisten so schnell wie möglich analysiert werden muss, sind IDS gefragt, die schon nach kurzer Konfigurationsphase möglichst wenige Fehlalarme liefern.

Bild 2 Klare IDS-Alarmmeldungen sparen Zeit bei der Analyse.

Bilder: NIST / Omicron

Um dies zu erreichen, muss das IDS die Vorgänge in Schaltanlagen und das Verhalten der Schutz- und Leittechnik kennen, um zwischen erlaubtem und gefährlichem Verhalten unterscheiden zu können. Gerade bei IEC-61850-Anlagen hat sich deshalb der Whitelist-Ansatz bewährt, denn in solchen Anlagen gibt es eine maschinenlesbare Dokumentation der Geräte und deren Kommunikation im SCL (Substation Configuration Language) Format. Mittels der SCL kann die Whitelist für das IDS automatisch generiert werden. Danach sind nur noch wenige Eingaben nötig, um auch das Verhalten der restlichen Geräte zu deklarieren.

Wird ein echter Angriff erkannt, zählt jede Minute. Eine effektive Reaktion setzt voraus, dass alle involvierten Mitarbeiter entsprechend sensibilisiert sind und die kritischen Prozesse und Systeme genau kennen. Dazu sind eine mit Cyber-Security-Kompetenzen ergänzte Organisation sowie Trainings für die Fachspezialisten ebenso notwendig wie die Übung des Ernstfalls. Bei einem IDS-Alarm werden meist zuerst die Cyber-Security-Spezialisten informiert. Diese müssen den Alarm analysieren und entscheiden, ob es sich um eine echte Bedrohung oder um einen Fehlalarm handelt. Für die weitere Einschätzung der Auswirkungen auf den Netzbetrieb und die folgenden Entscheidungen müssen auch die Fachspezialisten der Schutz- und Leittechnik hinzugezogen werden. Welcher Kategorie bezüglich der Kritikalität sind die Geräte zugeordnet? War jemand zu dieser Zeit in der Anlage? Ist der Netzwerkverkehr in der Anlage plausibel, bezogen auf die aufgetretenen Ereignisse?

Für die zügige Interpretation der Informationen sind die Benutzerfreundlichkeit und grafische Darstellung des IDS wichtig. Im Beispiel in **Bild 2** sind typische Alarme dargestellt, bei denen erst noch ermittelt werden muss, ob diese Aktionen von einem Techniker durchgeführt oder von einer Schadsoftware ausgeführt wurden. Stationguard orientiert sich bei der Darstellung von Alarmen beispielsweise an den Anlageplänen und nutzt für Meldungen die Schaltanlagen-Terminologie. Dies ermöglicht bei der Analyse eine effiziente Zusammenarbeit von Schutz- und Leittechnikern mit Cyber-Security-Spezialisten. Hinderlich können hier kryptische Fehlermeldungen sein. Denn Cyber-Security-Experten haben hier meist Schwierigkeiten, weil ihnen das Fachwissen in Bezug auf IEC-61850-Protokolldetails und der Zuordnung zu Schutzereignissen fehlt.

Auch in anderen Bereichen der Umsetzung des VSE-Grundschutzes kann ein IDS Unterstützung bieten. Im ersten Schritt (Identifizieren) müssen, noch vor den möglichen Angriffsvektoren, die zu schützenden Geräte in der Anlage identifiziert werden. Welche Geräte kommunizieren im Anlagennetzwerk? Welche Protokolle benutzen sie dabei? Welche Firmware-Versionen sind im Einsatz? Ein IDS kann hierfür passiv ermittelte Informationen aus dem Netzwerkverkehr mit Informationen aus den SCL-Dateien der Anlage kombinieren, um so einen umfassenden Datenauszug über das Gerät bereitzustellen.

Ein weiterer Vorteil des Whitelist-Ansatzes ist, dass sich damit die Whitelist einsehen und auditieren lässt. Anschliessend stellt das IDS auch deren Einhaltung sicher. Alle Verstösse gegen die Whitelist lösen Alarme aus und werden in einem manipulationssicheren Logbuch aufgezeichnet. Die Alarmmeldungen können zudem über verschiedene Kanäle weitergeleitet werden, beispielsweise an ein zentrales Siem (Security Information and Event Management) System.

Agieren statt reagieren

Das Thema Cyber Security, speziell im Bereich der Operational Technology, ist komplex. Genau wie für andere kritische Infrastrukturen existieren auch für die Energieversorgung Branchenempfehlungen, wie diejenige des VSE, in Form von Vorgaben und Standards. Dazu kommt, dass sich in naher Zukunft weitere gesetzliche Vorgaben abzeichnen. Um den Maturitätslevel einer Organisation in Bezug auf Cybersicherheit zu erhöhen, müssen daher die Domänen «Technologie – Prozesse – Menschen» gleichermassen behandelt werden. So lassen sich kommende gesetzliche Vorgaben weitgehend erfüllen und die Operational Technology vor Cyberangriffen schützen.

Autoren
Andreas Klien leitet den Geschäftsbereich Power Utility Communication bei Omicron.
→ Omicron electronics GmbH, AT-6833 Klaus
→ andreas.klien@omicronenergy.com

Markus Lenzin und **Reto Amsler** sind Inhaber der Alsec Cyber Security Consulting AG.
→ Alsec Cyber Security Consulting AG, 5082 Kaisten
→ info@alsec.ch

RÉSUMÉ

Protection de base pour les technologies opérationnelles

Cybersécurité pour les EAE

Les perturbations de l'approvisionnement énergétique de l'Ukraine engendrées par des cyberattaques en 2015 et 2016 ont permis de se faire une idée plus concrète des conséquences d'une attaque de hackers. La prévention contre les cyberrisques a, de ce fait, aussi gagné en importance au niveau politique. Pour les entreprises suisses d'approvisionnement en énergie, cela signifie qu'à l'avenir, il faudra mettre en œuvre des concepts de sécurité qui devront aussi répondre à des exigences légales minimales.

Pour prévenir les cyberrisques, l'AES a publié en 2018 la recommandation de la branche « Manuel Protection de base pour les technologies opérationnelles (OT) dans l'approvisionnement en électricité », qui repose sur un concept de sécurité global et mise sur l'interaction des personnes, des processus et des technologies. Un système de détection des intrusions (IDS) fait office d'élément-clé dans cette approche. Celui-ci est nécessaire pour détecter les attaques à temps et constitue également la base de l'amélioration continue de la résilience des appareillages électriques. Toutefois, un IDS ne remplit cette tâche que s'il est intégré dans un concept global bien pensé, dont la définition exige des connaissances techniques spécifiques à la branche. NO