Das Sicherheitsniveau steigern

Cybersicherheit | Nebst den zahlreichen Vorteilen, die die IT den Elektrizitätsversorgern bietet, kommen auch Herausforderungen hinzu, beispielsweise die Gefahr von elektronischen Angriffen von aussen. Diese betrifft Systeme sowohl im administrativen als auch im operativen Bereich. Was man in Letzterem unternehmen kann, erläutert Yann Gosteli im Interview.

Zur Person

Yann Gosteli ist El-Ing. FH und seit 2007 bei CKW verantwortlich für Netzschutzkonzepte. Seit 2015 leitet er die Abteilung für Sekundärtechniksysteme. Für den VSE war er in verschiedenen Arbeitsgruppen (z. B. TC oder DC) tätig, ist Mitglied der Fachgruppe Netzschutz der Schweiz und unterrichtet in den Kursen für Netzschutztechnik.

→ CKW, 6015 Luzern
→ yann.gosteli@ckw.ch

Bulletin: Welche Priorität wird der Cyber Security in technischen Systemen bei CKW beigemessen?
Yann Gosteli: Der Konzern Axpo und auch CKW haben in den letzten Jahren den Fokus vermehrt auf die Cyber Security gelegt. Unsere Nachbarn in Deutschland beschäftigen sich schon länger mit diesem Thema, was an den regen Diskussionen an Fachtagungen abzulesen war. Verschiedene Audits durch interne und externe Stellen bestätigten die Notwendigkeit, sich auch in der Schweiz mit dem Thema auseinanderzusetzen. Bei CKW waren wir damals daran, einen neuen Standard für Sekundärtechniksysteme in Unterwerken zu erarbeiten und hatten die Gelegenheit, parallel am VSE-Handbuch Grundschutz für «Operational Technology» in der Stromversorgung mitzuarbeiten. Wir hatten damals schon viele Punkte aus dem Handbuch in das Design einfliessen lassen. Mittlerweile ist das Thema Cyber Security fest in unserem Arbeitsalltag verankert. Wir steigern gezielt unsere technischen und organisatorischen Fähigkeiten in diesem Bereich.

Haben die CKW bereits unerfreuliche Erfahrungen mit Cyberattacken in den Steuerungssystemen gemacht?
Aus heutiger Sicht ist uns diesbezüglich nichts bekannt. Wir hatten keine Zwischenfälle zu beklagen. Das hat sicher damit zu tun, dass das Bewusstsein für solche Themen bei unseren Mitarbeitenden schon länger sehr hoch ist, da von der klassischen IT schon länger Informationskampagnen durchgeführt wurden. Damit wir schon im Ansatz merkwürdige Vorgänge in unseren Netzen entdecken können, werden nun alle Anlagen mit Intrusion Detection Systemen (IDS) ausgerüstet und ein Security Operation Center (SOC) aufgebaut. Diese Massnahmen helfen uns, schnell festzustellen, ob wir angegriffen werden. Wir können dann zeitnah und adäquat darauf reagieren.

Bei einem Kraftwerk ist die IT sowohl für die Administration zuständig als auch für die Steuerung der Produktion (Leitsystem). Wird hier bezüglich Cyber-Strategie unterschieden?
Das ist so nicht ganz korrekt in unserem Fall. Wir haben die IT- und die OT-Systeme strikt getrennt. Konkret: Die Informatiksysteme für die Kraftwerke, Schaltanlagen oder für den zentralen Netzbetrieb sind sehr stark abgeschottet. Wir verwenden da gerne die Analogie zu einer alten Burg. Es gibt einige Hürden, die überwunden werden müssen, um zum Herz der Anlage zu gelangen. Das halten wir bei unseren technischen Systemen genau gleich. Die wichtigsten Systeme werden auch speziell geschützt. Wir legen den Fokus im Moment darauf, die neuen Standards über das ganze Verteilnetz auszubreiten, damit wir auch in älteren Anlagen ein hohes Sicherheitsniveau erreichen. Dazu sind einige Anstrengungen nötig, und der Weg ist nicht immer einfach, Eingriffe in laufenden Anlagen z. B. am Netzwerk vorzunehmen.

Wie viele Mitarbeitende sind bei der Cybersicherheit in der OT involviert?
Wir benötigen dazu aktuell für die Einführung aller technischen Systeme und Prozesse rund drei bis vier Vollzeitstellen.

Was sind die aktuellen Fragen bezüglich Cybersicherheit bei Ihnen?
Wie angedeutet, steigern wir in den älteren Anlagen das Sicherheitsniveau. Dazu bauen wir unter anderem eine neue Infrastruktur für den netzwerktechnischen Zugang zu den Systemen in den Anlagen. Die Nachrüstung der IDS und der Aufbau des SOC sind weitere wichtige Themen. Das hilft uns in Zukunft, mögliche Sicherheitslücken für die wahrscheinlichsten Angriffe zu erkennen. Ausserdem verbessern wir uns in den Bereichen der Inventarisierung, der Reaktion auf Angriffe und der Wiederherstellung von Systemen, falls ein Angriff trotz aller Massnahmen wirklich erfolgreich sein sollte. Wir gehen dabei risikobasiert vor und stimmen diese Tätigkeiten über die verschiedenen Bereiche von der Netzleitstelle über die Datenübertragung bis zu den Steuerungssystemen in den Anlagen ab.

INTERVIEW: RADOMÍR NOVOTNÝ

Bild: CKW