Patrick Favre-Perrod
ist Vizedirektor der HTA-FR und
Electrosuisse-Vorstandsmitglied.

Cybersecurity bei EVUs

Mit der Einführung von Minimalstandards und Meldepflichten rückt Cybersecurity bei EVUs aus der IT-Nische noch stärker in den Vordergrund und betrifft nun praktisch alle Berufe im Unternehmen. Zwar ist der Fachkräftemangel im ICT-Bereich spürbar, doch die alleinige Ausbildung von IT-Spezialisten greift zu kurz: Für einen resilienten Netzbetrieb ist die Entwicklung eines unternehmensweiten Sicherheitsbewusstseins nötig.

Genau wie Helm und Sicherheitsschuhe punkto Arbeitssicherheit auf der Baustelle nicht verhandelbar sind, muss Cybersecurity als Basisverantwortung akzeptiert werden: Sicherheit ist die Basis des Betriebs. Dabei gilt es, die spezifischen Unterschiede zwischen IT und OT (Operational Technology) zu verstehen. In der OT ist die Verfügbarkeit unerlässlich. Netze sind segmentiert, und Patching-Zyklen können aufgrund langer Lebenszyklen sowie proprietärer Protokolle nicht einfach eins zu eins aus der Bürowelt übernommen werden.

Bereichsneutrale Normen mit Praxisorientierung ermöglichen eine gewisse Konvergenz, die durch spezifische Vertiefungen wie die IEC 27019 und die VSE-Richtlinien für die Stromversorgung ergänzt wird. Obwohl Tools, Technologien und Verfahren in jüngerer Zeit bemerkenswerte Fortschritte gemacht haben, bleibt der Ausgangspunkt entscheidend: der Mensch. Er wird oft als Schwachstelle genannt, ist aber auch der wichtigste Garant für Sicherheit. Durch Vernetzung, Ausbildung und Austausch wird individuelles Know-how zum kollektiven Schutzschild für unsere kritische Infrastruktur.

La cybersécurité dans les EAE

Avec l'introduction de normes minimales et d'obligations de déclaration, la cybersécurité sort de sa niche IT pour se glisser de plus en plus au premier plan dans les entreprises d'approvisionnement en énergie, où elle concerne désormais pratiquement tous les métiers. Si la pénurie de main-d'œuvre qualifiée dans le secteur des TIC est bien réelle, la seule formation de spécialistes en informatique ne suffit pas: développer une culture de la sécurité à l'échelle de l'entreprise est essentiel pour garantir la résilience des réseaux.

Tout comme le casque et les chaussures de sécurité sont indispensables pour la sécurité sur un chantier, la cybersécurité doit être acceptée en tant que responsabilité fondamentale: la sécurité constitue la base de l'exploitation. Il est essentiel de comprendre les différences spécifiques entre l'informatique (IT) et les technologies opérationnelles (OT). En OT, la disponibilité est indispensable. Les réseaux sont segmentés et les cycles de mise à jour ne peuvent pas être transposés tels quels du monde bureautique en raison des longs cycles de vie et des protocoles propriétaires.

Des normes transversales axées sur la pratique permettent une certaine convergence, complétée par des approfondissements tels que la norme CEI 27019 et les directives de l'AES pour l'approvisionnement en électricité. Même si les outils, les technologies et les procédures ont fait des progrès remarquables, le point de départ reste déterminant: l'être humain. Souvent désigné comme maillon faible, il est aussi le principal garant de la sécurité. Grâce au réseautage, à la formation et aux échanges, le savoir-faire individuel devient un bouclier collectif pour nos infrastructures critiques.