Dieter Reichelt
Präsident Electrosuisse und Vorsitzender der Geschäftsleitung Axpo Grid AG

Cyber-Risiken begegnen

Vor zwölf Jahren beschrieb der österreichische Autor Marc Elsberg in seinem Technik-Thriller «Blackout» die katastrophalen Auswirkungen eines grossflächigen Stromausfalles. Da wurde vielen von uns zum ersten Mal bewusst, wie verletzbar unsere Gesellschaft und wie sehr sie auf eine sichere Stromversorgung angewiesen ist. Das Thema ist heute aktueller als je zuvor, denn Energieinfrastrukturen sind attraktive Ziele für Cyber-Angriffe.

Um diesen Bedrohungen zu begegnen, müssen die Energieversorger ihre IT-Systeme proaktiv schützen. Eine umfassende Strategie sowie entsprechende Massnahmen zum Schutz der IT-Systeme sind von entscheidender Bedeutung.

Ebenso wichtig ist eine enge Zusammenarbeit zwischen Behörden, Unternehmen und der Sicherheitsindustrie, um aktuellen Bedrohungen resistent zu begegnen. Nur durch eine koordinierte und umfassende Herangehensweise können wir die Sicherheit unserer Energieinfrastrukturen gewährleisten und Cyberangriffen wirksam entgegentreten.

Mit dieser Zielsetzung wurde die Verpflichtung zum angemessenen Schutz gegen Cyberbedrohungen ins Stromversorgungsgesetz (StromVG) aufgenommen und darauf basierend die Stromversorgungsverordnung (StromVV) revidiert. Die neue StromVV wird per 1. Juli 2024 in Kraft treten. Sie teilt Netzbetreiber und Stromerzeuger in drei Klassen ein und fordert basierend auf dieser Klassifizierung konkrete Sicherheitsmassnahmen. Wir hoffen, dass diese Sicherheitsvorgaben in der gesamten Elektrizitätsversorgungsbranche ein höheres Bewusstsein bezüglich IT/OT-Sicherheit schaffen. Die Kosten der Umsetzung von Massnahmen zur Erhöhung der Cybersicherheit bei Netzbetreibern sind grundsätzlich anrechenbare Netzkosten.

Die Digitalisierung bietet enorme Chancen für die Energieversorgung, aber sie bringt auch neue Risiken mit sich. Es liegt an uns, diese Risiken zu erkennen und angemessen darauf zu reagieren, um eine sichere und nachhaltige Energieversorgung für die Zukunft zu gewährleisten.

Faire face aux cyberrisques

Il y a 12 ans, l'auteur autrichien Marc Elsberg décrivait dans son thriller technique « Blackout » les conséquences catastrophiques d'une panne d'électricité à grande échelle. Cet ouvrage a entraîné une prise de conscience collective de la vulnérabilité de notre société et de sa dépendance envers un approvisionnement fiable en électricité. Cet enjeu se trouve au cœur des préoccupations actuelles, car les infrastructures énergétiques constituent des cibles de choix pour les cyberattaques.

Pour faire face à ces menaces, les fournisseurs d'énergie doivent protéger leurs systèmes informatiques de manière proactive. Pour ce faire, une stratégie globale ainsi que des mesures ajustées sont d'une importance cruciale.

Une collaboration étroite entre les autorités, les entreprises et l'industrie de la sécurité est tout aussi indispensable pour résister aux menaces actuelles. Seule une approche systémique et coordonnée nous permettra de garantir la sécurité de nos infrastructures énergétiques et de contrer efficacement les cyberattaques.

C'est dans cette optique que l'obligation d'une protection adaptée aux cybermenaces a été inscrite dans la loi sur l'approvisionnement en électricité (LApEl) et que l'ordonnance sur l'approvisionnement en électricité (OApEl) a été révisée sur cette base. La nouvelle OApEl entrera en vigueur le 1er juillet 2024. Elle répartit les gestionnaires de réseau et les producteurs d'électricité en trois catégories et exige la mise en place de mesures de sécurité concrètes sur la base de cette classification. Nous espérons que ces consignes de sécurité permettront de sensibiliser davantage l'ensemble du secteur de l'approvisionnement en électricité à la sécurité IT/OT. Les coûts d'implémentation de mesures visant à accroître la cybersécurité chez les exploitants de réseau sont en principe catégorisés comme des coûts de réseau imputables.

La digitalisation de l'industrie offre d'énormes opportunités pour l'approvisionnement en énergie, mais elle comporte également de nouveaux risques. Il nous appartient de reconnaître ces derniers et d'y réagir de manière appropriée afin de garantir un approvisionnement énergétique sûr et durable pour l'avenir.