Michael Paulus
Bereichsleiter Technik und Berufsbildung des VSE
michael.paulus@strom.ch

Responsable Technique et Formation professionnelle de l'AES
michael.paulus@electricite.ch

Wir stehen erst am Anfang

Ein Schlüssel zur Steigerung der Energieeffizienz, dem Schwerpunktthema dieser Ausgabe, liegt in der zunehmenden Digitalisierung. Nun bietet diese nicht nur Chancen, sondern setzt uns auch erheblichen Risiken aus: Cyber-Kriminalität, Spionage, Sabotage, Terrorismus, militärische Angriffe – keine Zukunftsvisionen, sondern bereits heute Realität. Aufgrund dieser drängenden Fragen hat der Bund die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 aktualisiert. Hauptzielgruppe der NCS sind die Betreiber kritischer Infrastrukturen, also insbesondere auch der Sektor Energie. Klar ist: Es gibt keinen vollständigen Schutz vor Cyber-Risiken. Stattdessen ist «Resilienz» das neue Zauberwort. Die Funktionsfähigkeit der kritischen Infrastrukturen soll auch bei grossen Cyber-Vorfällen gewährleistet bleiben. In den letzten Jahren sind der Strom- und der Gassektor bereits auf IKT-Verwundbarkeit untersucht worden, und es wurden Massnahmen ausgearbeitet. Diese sollen nun umgesetzt und weiterentwickelt werden.

Die Energieversorger sind dabei von zentraler Bedeutung, denn sie sind es, die effektive Schutzmassnahmen ergreifen. Eine spezielle Rolle spielen dabei die Steuerungssysteme. Diese beginnen bei den Scada-Systemen in den Leitzentralen der Anlagenbetreiber und gehen bis zum Hausmanager, der über das «Internet of Things» dezentrale Verbraucher, Speicher und Produzenten kontrolliert. Und von übergeordneter Bedeutung ist die Sorgfalt beim Umgang mit Daten jeglicher Art. Nur: Kaum ein Unternehmen ist in der Lage, die Schutzmassnahmen im Alleingang zu formulieren. Zu schnell kann sich die Bedrohungslage ändern und zu komplex sind Angriffsszenarien. Wir müssen daher prüfen, ob und wie die Energieversorger von einer verstärkten Zusammenarbeit profitieren können. Braucht es zum Beispiel eine Kommunikationsdrehscheibe, einen «Single point of contact» der Branche? Eine geeignete institutionalisierte Koordination könnte einen effektiven Nutzen bringen.

Bereits heute unterstützt der VSE seine Mitgliedsunternehmen mit Branchendokumenten und seinem breiten Ausbildungsangebot zu diesen Fragen. Doch wir stehen erst am Anfang der Arbeit. Das Thema «Cyber Security» wird uns noch lange Zeit stark beschäftigen.

Ce n'est que le début

L'une des clés de l'amélioration de l'efficacité énergétique, thème central de ce numéro, c'est la digitalisation croissante. Mais celle-ci n'offre pas que des opportunités, elle nous expose aussi à des risques considérables : cybercriminalité, espionnage, sabotage, terrorisme, attaques militaires – il ne s'agit pas de visions d'avenir, mais de la réalité, déjà aujourd'hui. Au vu de ces questions urgentes, la Confédération a mis à jour la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022. Le groupe cible principal de la SNPC, ce sont les exploitants d'infrastructures critiques, et donc en particulier le secteur de l'énergie. Une chose est sûre : il n'existe pas de protection intégrale contre les cyberrisques. Au lieu de cela, « résilience » est le nouveau mot magique. La viabilité des infrastructures critiques doit être garantie également en cas de cyberincidents de grande ampleur. Ces dernières années, on a déjà étudié la vulnérabilité des TIC dans le secteur de l'électricité et du gaz, et des mesures ont été élaborées. Celles-ci doivent maintenant être mises en œuvre et continuer d'être développées.

Dans cette démarche, les fournisseurs d'énergie sont d'importance capitale, puisque ce sont eux qui prennent les mesures de protection effectives. Les systèmes de commande jouent alors un rôle particulier : ils commencent au niveau des systèmes Scada, dans les centres de commande des exploitants d'installation, et vont jusqu'au « manager » domestique, système qui contrôle, grâce à l'« Internet des objets », la consommation, le stockage et la production dans des installations décentralisées. Sans oublier que le soin avec lequel sont manipulées les données de tous types est d'une importance primordiale. Seul hic : pratiquement aucune entreprise n'est capable de formuler des mesures de protection de manière isolée. La situation de menace peut changer trop vite et les scénarios d'attaques sont trop complexes. C'est pourquoi nous devons analyser si et comment les fournisseurs d'énergie peuvent profiter d'une collaboration renforcée. Faut-il par exemple une plate-forme de communication, un point de contact unique pour la branche ? Une coordination institutionnalisée adaptée pourrait apporter une réelle valeur ajoutée.

L'AES soutient d'ores et déjà ses entreprises membres grâce à des documents de la branche et à sa grande offre de formation touchant à ces questions. Mais ce n'est que le début de notre travail. Le thème de la « cybersécurité » va largement nous occuper, encore longtemps.