Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 109 (2018)
Heft: 4

Rubrik: VSE/AES

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 19.03.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Michael Frank
Direktor des VSE
michael.frank@strom.ch
Directeur de l'AES
michael.frank@electricite.ch

Real gerüstet für virtuelle Bedrohungen

In den 80er-Jahren dürften die Zuschauer noch über die Idee gelacht haben: Ein computerbegeisterter Teenager verursacht im Science-Fiction-Streifen «War Games» beinahe einen thermonuklearen Krieg. Doch das Lachen in Bezug auf Cyber-Risiken für kritische Infrastrukturen ist uns definitiv vergangen. Spätestens, seit die Ransomware «WannaCry» Ticket-Automaten und Anzeigetafeln der Deutschen Bahn lahmgelegt hat. Wir sprechen in der Elektrizitätswirtschaft oft von den Segnungen der Digitalisierung. Gerne wird auch die Sektorkopplung thematisiert – das Zusammenrücken von Strom, Gas, Wärme und Mobilität.

Beide Trends lösen alte Probleme und eröffnen neue Geschäftsfelder. Doch wo ist der Haken? Eine vernetzte Infrastruktur, die sich gänzlich durch Computer steuern lässt, ist zwar leistungsfähig. Sie ist aber auch ein verletzliches Gesamtsystem mit unzähligen Eintrittspforten. Der Traum jedes Hackers, der einen «FireSale» anstrebt: Eine gezielte Attacke, die mit einem Schlag den Verkehr, die Telekommunikation und die Energieversorgung ausser Gefecht setzt. Zugegeben, solch ein Szenario ist – und bleibt hoffentlich – Zukunftsmusik. Doch Attacken wie WannaCry sind mehr als nur vereinzelte Misstöne. Solche Ereignisse zeigen uns, wo wir als Branche ansetzen müssen, um für die dezentrale und digitale Energiezukunft gewappnet zu sein.

Bezüglich Hacks, das zeigt die Erfahrung, sind menschliche Makel und Indiskretionen am gefährlichsten. Jemand, der jemanden kennt, der jemandem einen Gefallen tut. Darum gilt erstens, das Bewusstsein für Cyber Security in der Elektrizitätswirtschaft zu schärfen. Zweitens, und dort setzt die Berufsbildung des VSE an, müssen wir Fachleute ausbilden, welche Hackern das Fürchten lehren. In Zusammenarbeit mit dem Verband ICT-Berufsbildung Schweiz hat der VSE darum die Weiterbildung «ICT-Security Expert mit eidg. Diplom» entwickelt. Die ersten Prüfungen finden schon im August 2018 statt. ICT Security Experts bearbeiten sicherheitsrelevante Fragen im ganzen Unternehmen. Sie erkennen und bewerten Sicherheitsrisiken, definieren und koordinieren Schutzmassnahmen – und sorgen für wirksame Abwehrmechanismen. Damit das Licht zu Hause erst dann ausgeht, wenn wir selbst den Schalter drücken.

Réellement paré contre les menaces virtuelles

Dans les années 80, les spectateurs ont certainement taxé cette idée de saugrenue : dans le film de science-fiction « Wargames », un adolescent passionné d'informatique manquait de provoquer une guerre thermonucléaire. Mais, en matière de cyberrisques pour les infrastructures critiques, nous n'avons définitivement plus envie de rire, surtout depuis que le ransomware « WannaCry » a paralysé les distributeurs de billets et les panneaux d'affichage de la Deutsche Bahn. Dans le secteur de l'électricité, nous parlons souvent des bienfaits de la digitalisation et le couplage des secteurs – à savoir le rapprochement de l'électricité, du gaz, de la chaleur et de la mobilité – est aussi régulièrement abordé.

Ces deux tendances résolvent de vieux problèmes et ouvrent de nouveaux secteurs d'activité. Mais il y a un hic ! Une infrastructure en réseau entièrement pilotable par ordinateur est certes performante, mais elle constitue aussi un ensemble vulnérable, avec d'innombrables portes d'entrée. Autrement dit, le rêve de n'importe quel hackeur qui aspire à réaliser un « fire sale » : une attaque ciblée qui met d'un seul coup à terre à la fois les transports, les télécommunications et l'approvisionnement en énergie. Je vous l'accorde, un tel scénario n'est pas pour demain – et restera du domaine de l'imagination, espérons-le. Mais les attaques comme WannaCry sont bien plus que de simples incidents sporadiques. Ce genre d'événement nous montre où notre branche doit concentrer ses efforts afin d'être parée pour l'avenir énergétique numérique et décentralisé.

Concernant les hacks, l'expérience montre que ce sont les défaillances et indiscrétions humaines qui se révèlent les plus dangereuses. Quelqu'un qui connaît quelqu'un qui rend service à quelqu'un. Voilà pourquoi la première chose à faire est d'aiguiser la prise de conscience envers la cybersécurité dans le secteur électrique. Ensuite, et c'est là qu'intervient la formation professionnelle de l'AES, nous devons former des spécialistes qui sauront faire trembler les hackeurs. C'est pourquoi l'AES a développé, en collaboration avec l'association ICT Formation professionnelle Suisse, la formation continue « ICT Security Expert avec diplôme fédéral ». Les premiers examens auront lieu dès août 2018. Les « ICT Security Experts » traitent les questions de sécurité dans toute l'entreprise. Ils identifient et évaluent les risques liés à la sécurité, définissent et coordonnent les mesures de protection – et veillent à mettre en place des mécanismes de défense efficaces. Objectif : que la lumière s'éteigne chez nous uniquement quand nous appuyons sur l'interrupteur.

Dominique Martin
Bereichsleiter Public Affairs des VSE
dominique.martin@strom.ch
Responsable Affaires publiques de l'AES
dominique.martin@electricite.ch

Entwarnung? Keineswegs!

Die Versorgungssicherheit der Schweiz ist bis 2035 gesichert. Das bekräftigt der Bundesrat hauptsächlich gestützt auf zwei Annahmen: 1. Die Schweiz ist stärker in den europäischen Strommarkt integriert; 2. Der Produktionspark (längerfristig ohne Kernenergie) bleibt erhalten und entwickelt sich gemäss den Zielen der Energiestrategie 2050.

Gemäss Bundesrat braucht es für extreme Situationen höchstens eine strategische Reserve. Entwarnung also für alle jene, die sich um unsere Versorgungssicherheit sorgen? Keineswegs! Eine strategische Reserve zielt einzig auf die kurzfristige Versorgungssicherheit, um zum Beispiel punktuelle Knappheitssituationen im Winter zu überbrücken. Sie hat jedoch keinen Einfluss auf Bestand und Ausbau der Produktionskapazität. Sie gibt somit keine Antwort auf die zentrale Frage nach der langfristigen Versorgungssicherheit und damit einer ausreichenden einheimischen Produktion.

Hier liegt der Kern des Problems. Der Bundesrat selber rechnet nämlich mit einem Investitionsbedarf in Erneuerung und Instandhaltung der Schweizer Wasserkraft von 30 Milliarden Franken von 2010 bis 2050. Diese (Re-)Investitionen sind indes im vorderhand weiterbestehenden Tiefpreisumfeld schwer finanzierbar. Auch eine strategische Reserve im Umfang von 100 bis 200 Millionen Franken pro Jahr wird daran nichts ändern. Der nachhaltige Weiterbestand der Schweizer Wasserkraft kann somit nicht als gegeben angenommen werden.

Der Ständerat ist sich dieser Lage voll bewusst: In der letzten Frühjahrssession hat er mit deutlicher Mehrheit eine Motion angenommen, welche den Bundesrat beauftragt, Investitions- oder Reinvestitionsanreize für den langfristigen Erhalt der Schweizer Stromproduktionsanlagen zu schaffen.

Die vom Ständerat ohne Zwischentöne eingeschlagene Richtung stimmt. Eine strategische Reserve als alleinige Massnahme kann unsere Versorgungssicherheit nicht garantieren. Legen wir also nicht die Hände in den Schoss, sondern gehen wir die wirklichen Herausforderungen an.

Ne restons pas les bras croisés!

La sécurité d'approvisionnement de la Suisse est garantie jusqu'en 2035. C'est ce qu'affirme le Conseil fédéral en se basant principalement sur deux hypothèses: 1) La Suisse sera plus fortement intégrée dans le marché de l'électricité européen; 2) Le parc de production suisse (à terme sans nucléaire) sera maintenu et se développera conformément aux objectifs de la Stratégie énergétique 2050.

Selon le Conseil fédéral, il conviendrait uniquement d'introduire une réserve stratégique pour des situations extrêmes. Fin de l'alerte donc, pour tous ceux qui se soucient de notre sécurité d'approvisonnement? Non! Une réserve stratégique ne vise que la sécurité d'approvisionnement à court terme, par exemple pour couvrir des situations ponctuelles de pénurie en hiver. En revanche, elle n'a aucun impact sur le maintien et le développement de la capacité de production. Elle ne répond donc pas à la question centrale de la sécurité d'approvisionnement à long terme et du maintien d'un niveau de production indigène suffisant.

C'est ici qu'on touche au cœur du problème. En effet, le Conseil fédéral estime lui-même à 30 milliards de francs le besoin d'investissement pour rénover et entretenir la force hydraulique suisse entre 2010 et 2050. Or, ces (ré)investissements pourront difficilement être financés dans un environnement de prix bas. Une réserve stratégique de 100 à 200 millions de francs par an n'y changera rien. La pérennité de notre force hydraulique ne peut donc pas être considérée comme un acquis.

Le Conseil des États est parfaitement conscient de cette situation: lors de la dernière session de printemps, il a accepté à une très nette majorité une motion qui charge le Conseil fédéral de proposer des mesures visant à stimuler les investissements et à maintenir ainsi les installations suisses de production électrique à long terme.

L'approche adoptée sans équivoque par le Conseil des États montre la bonne voie. Une réserve stratégique ne saurait constituer l'unique mesure pour garantir notre sécurité d'approvisionnement. Ne restons donc pas les bras croisés et attaquons-nous aux vrais défis.