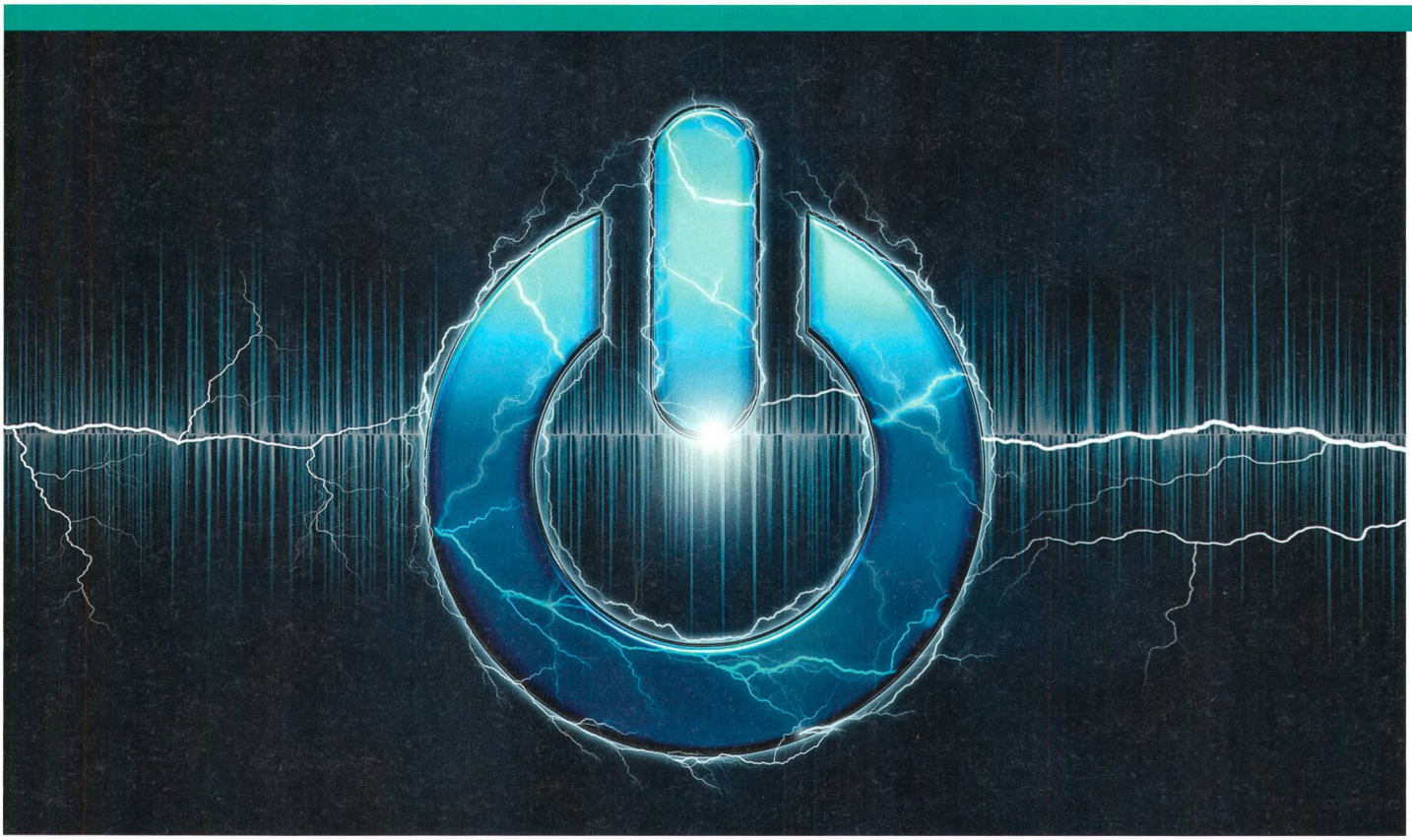
Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 110 (2019)
Heft: 12

Artikel: La cybersécurité des infrastructures électriques
Autor: Ghernaouti, Solange
DOI: https://doi.org/10.5169/seals-856025



La cybersécurité des infrastructures électriques

Enjeux stratégiques et réponses opérationnelles | Après avoir identifié les enjeux stratégiques de la cybersécurité des infrastructures de production et d'approvisionnement en électricité, des recommandations sont proposées afin de contribuer à renforcer leur sécurité et leur résilience face aux cyberrisques.

SOLANGE GHERNAOUTI

Comme pour l'ensemble des activités industrielles, la transformation numérique du secteur de l'énergie est une réalité amorcée depuis le siècle passé. Désormais, la production et la distribution d'électricité dépend des technologies du numérique et ces dernières sont dépendantes de l'électricité. L'enjeu de la cybersécurité dans le secteur de l'électricité s'exprime par le constat suivant: pas d'électricité, pas de numérique et sans numérique, pas d'électricité possible. Cette double dépendance et interdépendance témoigne de la criticité de la cybersécurité pour le secteur de l'énergie.

En devenant un « réseau intelligent », le réseau électrique s'est ouvert aux cyberrisques. De facto, leur non-maîtrise peut mettre à défaut la disponibilité, l'intégrité et la sûreté de fonctionnement des infrastructures électriques et porter atteinte aux individus, aux organisations et à l'État. La sécurité de l'approvisionnement en électricité du pays est fragilisée par l'exposition des systèmes et réseaux informatiques qui composent le système énergétique aux cyberattaques. Dès lors, bien investir dans la cybersécurité n'est pas une option. Cela nécessite de répondre aux questions suivantes: qui finance, qui est responsable et qui est imputable en cas de sinistre?

La cybersécurité ne relève pas uniquement d'une problématique technique. Elle s'inscrit également dans une démarche stratégique, politique, économique et managériale, dont la mise en œuvre opérationnelle passe par des mesures spécifiques de cybersécurité et dont la réalisation s'appuie sur des solutions informatiques.

Des risques bien réels

Dans son livre « Black-out, demain il sera trop tard » paru en 2012, l'auteur allemand Marc Elsberg met la panne électrique et les cyberattaques au cœur de son roman. S'il lui a été possible d'imaginer des scenarii de black-outs électrique et numérique affectant tout un pays et une région du monde et entraînant une chute de la civilisation, il nous est néanmoins insupportable de penser qu'un effondrement total de la société, du fait de son informatisation,

Figure: Pixabay

puisse être possible. La violence de cette idée nous la rend difficilement conceptualisable et représentable. Dès lors, impossible de penser ce risque majeur sans être taxé de catastrophiste, de collapsologue, voire de paranoïaque. Or, des tsunamis numériques se sont déjà déroulés. En voici quelques-uns à titre d'exemples non exhaustifs.

En mars 2018, la note d'alerte de l'Agence de sécurité et de cybersécurité des infrastructures du Département de sécurité nationale des États-Unis d'Amérique du Nord [1] informait que des cyberattaques affectaient des systèmes informatiques notamment d'infrastructures électriques et nucléaires du pays.

Une année auparavant, en septembre 2017, l'entreprise de sécurité Symantec révélait que le secteur de l'électricité de l'Europe et des USA subissait des attaques informatiques à des fins d'espionnage et de sabotage, du fait de hackeurs et de techniques d'attaques connus sous les noms de Dragonfly et d'Energetic Bears, qui opéraient depuis au moins 2010 [2].

Dans la nuit du 17 au 18 décembre 2016, la ville de Kiev en Ukraine a été l'objet d'un black-out électrique suite à de multiples cyberattaques et à la compromission des postes de travail et des systèmes Scada (Supervisory Control and Data Acquisition) du fournisseur d'électricité Ukrenergo. [3]

La prise de contrôle à distance des systèmes informatiques en raison de cyberattaques ou de la présence de points d'entrée dans les systèmes par l'existence de portes dérobées dans les matériels ou logiciels (backdoors), notamment des systèmes Scada, est une réalité. Le cas emblématique de l'infection par le ver informatique Stunex des centrifugeuses des centrales nucléaires iraniennes en 2010, qui a porté atteinte aux capacités d'enrichissement de l'uranium du pays, illustre la manière dont les tensions géopolitiques et économiques peuvent s'exprimer au travers de l'usage abusif et détourné de l'informatique.

Que cela soit à des fins de sabotage, d'espionnage ou de dysfonctionnement divers, s'inscrivant dans des stratégies d'attaque, de dissuasion ou de représailles, la force de frappe informatique se manifeste par des cyberattaques, du code informatique offensif ou encore par des processus d'information et de désinformation.

Partout dans le monde, les infrastructures énergétiques sont des cibles privilégiées de la guerre informatique et vulnérables aux cyberattaques. Ces dernières exploitent des failles de sécurité et des outils d'attaques de plus en plus sophistiqués, qui peuvent de surcroît être dérobés à des agences de sécurité comme la NSA (National Security Agency), comme le déclarait l'un des anciens responsables de la Federal Energy Regulatory Commission dans un interview du New York Times, en juin 2017 [4].

Des cyberopérations à effet systémique

Inscrites dans des contextes de conflits entre états ou de criminalité, des cyber-opérations conduites contre des infrastructures d'alimentation en électricité, eau, gaz ou pétrole par exemple, ne peuvent avoir que des effets systémiques « boule de neige » en raison de l'interconnexion des infrastructures énergétiques avec celles informationnelles. Plus elles sont connectées à l'Internet, plus grand est le nombre d'objets connectés (IIoT, Industrial Internet of Things) impliqués dans les infrastructures énergétiques, plus la surface d'exposition aux cyberrisques augmente. L'extension de la surface d'attaque et l'addition croissante de points d'entrée d'exploitation des vulnérabilités intensifient les cyberrisques et leurs impacts. Par conséquent, plus ces infrastructures sont attractives pour des hackeurs, plus les coûts de la sécurité et de l'insécurité s'aggravent.

Quelles que soient la motivation des acteurs étatiques ou non étatiques impliqués et la finalité des cyberattaques sur des infrastructures énergétiques ou industrielles, leurs conséquences sont toujours préjudiciables et le coût est toujours porté par la société. Cela peut également conduire à des risques écologiques majeurs affectant l'environnement.

Les risques et les crises environnementales et écologiques constituent, selon l'édition 2019 du Global Risk Report du World Economic Forum [5], les problèmes majeurs auxquels doit faire face le monde globalisé, hyperconnecté et dépendant des technologies de l'information. Dorénavant, nous devons faire face à des attaques sophistiquées et à des menaces persistantes sur les infrastructures énergétiques et industrielles dont l'activité est liée aux ressources naturelles: usines chimiques, de traitement des eaux, plateformes d'exploitation pétrolière, centrales nucléaires... La cybersécurité contribue à assurer la protection et la sûreté de leurs opérations.

Des exigences de sécurité et de résilience

Les cyberrisques sont des risques structurels et complexes dont les impacts sont en cascade avec des effets dominos et démultiplicateur. Pour ces raisons, il est nécessaire de penser la cybersécurité de manière holistique, de diminuer les cyberrisques et d'être en mesure de gérer des crises de grandes ampleur et intensité. La cybersécurité peut, dès lors, être considérée comme une urgence planétaire internationale.

Concrétiser une démarche de cybersécurité passe notamment par une évaluation correcte de tous les facteurs de risques, y compris de ceux liés aux mesures de cybersécurité, afin de pouvoir disposer de solutions appropriées et d'un niveau de cyberrésilience satisfaisant.

Des outils et des compétences

Pour un pays, il est impératif de disposer d'une stratégie cohérente et intégrée de cybersécurité et de cyberdéfense de ses infrastructures critiques permettant d'assurer le continuum sécurité-défense, de mettre en œuvre des mesures organisationnelles, managériales, techniques et humaines, d'évaluer périodiquement leur efficacité et efficience et de les optimiser en fonction de l'évolution des environnements, des contraintes et des besoins. Pour la gestion des risques et de la sécurité informatique, diverses normes internationales existent (normes ISO/IEC 31000, normes de la série ISO/IEC 27000 avec notamment celle spécifique au secteur de l'énergie ISO/IEC 27019 publiée en 2017) [6].

Parmi les difficultés à affronter pour sécuriser les infrastructures énergétiques, citons, entre autres, celles liées aux exigences relatives à l'efficacité des mesures de sécurité dans un contexte de travail « temps réel », qui caractérisent le secteur de l'énergie, et à l'existence de systèmes anciens (legacy systems) dont la durée de vie peut s'étendre de 30 à 60 ans et qui n'ont pas été conçus pour être interconnectés à l'Internet.

Une question de responsabilité, de coopération et de partenariat

Il devrait être de la responsabilité des fournisseurs de technologies numériques de proposer des outils qui intègrent dès leur conception des mesures de sécurité adaptées (Cybersecurity by design) et dans lesquels des failles de sécurité et des vulnérabilités n'existeraient pas afin que des acteurs malveillants ne puissent pas les exploiter pour réaliser des cyberattaques. De plus, tout un processus de remontée d'alertes et de traitement de celles-ci devrait exister, comme d'ailleurs des mesures de gestion opérationnelle qui garantiraient la maintenance des infrastructures et leur sécurité dans le temps, tout au long du cycle de vie des produits.

Selon la recommandation de l'Union européenne (Recommandation 2019/553 de la Commission du 3 avril 2019 relative à la cybersécurité dans le secteur de l'énergie) [7], la notification des incidents de cybersécurité est obligatoire. Ainsi, être obligé de les annoncer et disposer de mesures permettant leur analyse et le partage d'information autorisent le développement d'un corpus de connaissances facilitant l'anticipation, la préparation et la planification des capacités nécessaires à la maîtrise des risques. Ce partage d'information contribue, comme le spécifie l'Académie suisse des sciences techniques dans sa fiche d'information « Le partage d'information en cybersécurité » [8], à connaître la réalité des menaces et des incidents, à développer une culture de la cybersécurité, à sensibiliser, à former et à produire de la sécurité. Le cycle du renseignement et « l'intelligence des menaces » constituent également, lorsqu'exploités correctement, des facteurs clés de succès du renforcement de la cyberrésilience des systèmes d'information et des réseaux du secteur énergétique. Cela ne peut se penser sans le développement des capacités nationales de cybersécurité, et sans une certaine coopération aux niveaux régional et international (y compris dans la coopération transfrontalière), et sans des partenariats efficients entre les secteurs privé et public.

Références

[1] Cybersecurity and Infrastructure Security Agency (CISA), US Department of Homeland Security, www.us-cert.gov/ncas/alerts/TA18-074A
[2] www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
[3] www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA
[4] www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html
[5] www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
[6] Respectivement : www.iso.org/fr/iso-31000-risk-management.html, www.iso.org/fr/standard/73906.html et www.iso.org/fr/standard/68091.html
[7] eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019H0553&from=ES
[8] www.satw.ch/fileadmin/user_upload/documents/02_Themen/03_Cyber/SATW-Le-partage-d-information-en-cybersecurite_FR.pdf

Littérature complémentaire

→ S. Ghernaouti, « Cybersécurité : analyser les risques, mettre en oeuvre les solutions ». 6e édition, Dunod 2019, www.dunod.com/sciences-techniques/cybersecurite-analyser-risques-mettre-en-oeuvre-solutions

Lien

www.scarg.org

Auteure

Prof. **Solange Ghernaouti** est directrice du Swiss Cybersecurity Advisory & Research Group (SCARG) à l'Université de Lausanne et co-fondatrice de la société genevoise Heptagone digital risk management & security.

→ Heptagone digital risk management & security Sàrl, 1202 Genève
→ solange.ghernaouti@heptagone.ch

IN KÜRZE

Cybersicherheit bei der Strominfrastruktur

Strategische Herausforderungen und Reaktionen aus dem betrieblichen Umfeld

Schon vor der Jahrtausendwende ist der digitale Wandel in der Energiebranche angelaufen. Seither hängen Produktion und Verteilung des Stroms von digitalen Technologien ab, die selbst wiederum vom Strom abhängig sind. Da sich das Stromnetz zum «Smart Grid» entwickelt hat, ist es nun auch Cyberrisiken ausgesetzt. Wenn man diese Risiken nicht in den Griff bekommt, kann dies die Verfügbarkeit, die Integrität und die Funktionssicherheit der Strominfrastruktur stören und den Menschen, den Organisationen und dem Staat schaden.

In Konflikten zwischen Staaten oder im Rahmen krimineller Handlungen können Cyberangriffe auf Versorgungsinfrastrukturen für Strom, Wasser, Gas, Öl usw. systemische «Schneeballeffekte» auslösen, weil die Energieinfrastrukturen eng mit den Informatikeinrichtungen verzahnt sind. Die Angriffsfläche für Cyberrisiken steigt mit der zunehmenden Internetkonnektivität, weil diese zu mehr vernetzten Objekten in den Energieinfrastrukturen führt (IIoT, Industrial Internet of Things). Die Ausdehnung der Angriffsfläche und die vermehrte Einbindung von Zugangspunkten, über die Schwachstellen ausgenutzt werden können, bewirken eine Intensivierung der Cyberrisiken und ihrer Auswirkungen.

Dass Cybersicherheitsvorfälle gemäss der Empfehlung der Europäischen Union zur Cybersicherheit im Energiesektor gemeldet werden müssen, erlaubt die Analyse solcher Vorfälle und den Aufbau von Kenntnissen und Kompetenzen, um die für die Risikokontrolle erforderlichen Kapazitäten vorherzusagen, zu planen und zu schaffen. Der Informationsaustausch hilft, die Bedrohungssituation und die Vorfälle zu kennen, eine Kultur der Cybersicherheit zu entwickeln, Sensibilisierungs- und Schulungsmassnahmen zu ergreifen sowie Sicherheit herzustellen. Der Austausch stellt einen Schlüsselfaktor für die Stärkung der Widerstandsfähigkeit der Informationssysteme und der Netze der Energiebranche gegenüber Cyberangriffen dar. Diese Stärkung bedingt die Schaffung von nationalen Cybersicherheitskapazitäten, eine gewisse Zusammenarbeit auf regionaler und internationaler Ebene (auch grenzüberschreitend) sowie erfolgreiche Partnerschaften zwischen dem privaten und dem öffentlichen Sektor. CR