La risque diffus de la cybersécurité

Autor(en): **Sénéclauze, Martin / Vizár, Damian / Alet, Pierre-Jean**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **113 (2022)**

Heft 7-8

PDF erstellt am: **27.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-1037128

Le nombre de petits producteurs, et donc de cibles potentielles, ne cesse de croître.

Le risque diffus de la cybersécurité

Numérisation et sécurisation des réseaux électriques basse tension | Les réseaux électriques sont désormais largement interconnectés par le biais de réseaux de collecte de données ou de commande, ce qui les expose à des menaces informatiques et autres attaques cybernétiques. C'est notamment le cas des réseaux basse tension, qui méritent d'être, eux aussi, protégés par des solutions appropriées.

MARTIN SÉNÉCLAUZE, DAMIAN VIZÁR, PIERRE-JEAN ALET, PHILIPPE DALLEMAGNE

La numérisation et l'interconnexion des équipements électriques constituent des éléments incontournables de l'accroissement de l'efficacité et de la souplesse des infrastructures électriques. Ceci s'applique aux domaines de la production, de la distribution ainsi que du maintien des paramètres fondamentaux des systèmes impliqués et du service offert. L'efficacité et la souplesse des infrastructures reposent sur l'accès aux ressources composant le système, sur leur gestion à distance ainsi que sur la faculté d'en orchestrer la mise en œuvre à l'aide d'arrangements informatiques complexes. Ceci permet d'observer, d'analyser et de prévoir le comportement des systèmes et, ensuite, de l'optimiser.

Cette ouverture constitue évidemment aussi une opportunité pour des parties adverses d'effectuer des opérations similaires avec des objectifs différents, voire malveillants: surcharger les équipements, immobiliser des ressources, masquer des détournements d'utilisation de ces dernières, provoquer des dysfonctionnements et des coupures, entre autres, et finalement altérer la qualité du service offert au client. Cette ouverture est donc problématique, et ce, d'autant plus si, comme le considère le rapport sur l'analyse nationale des risques [1], l'un des plus grands risques auquel la Suisse sera confrontée à l'avenir est une pénurie d'électricité.

Les réseaux de très haute, haute et moyenne tension (niveaux 1 à 5 de la **figure 1**) font l'objet d'attentions particulières tant de la part des attaquants que des exploitants. Si ces derniers ajustent les mesures de protection en permanence, ce n'est malheureusement pas toujours le cas dans le domaine de la basse tension (niveaux 6 et 7). Or,

Figures: CSEM

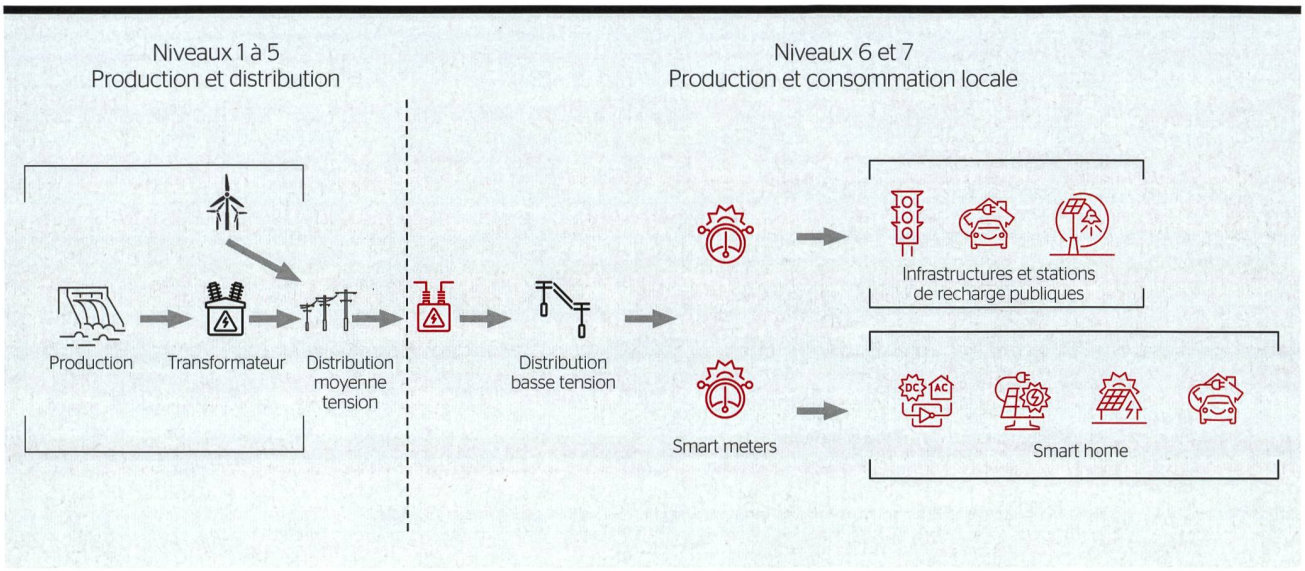

Figure 1 Les 7 niveaux du réseau électrique : en rouge, les éléments couverts dans cet article.

cette faille expose l'ensemble du système à des attaques focalisées ou globales. Il existe heureusement des solutions pour sécuriser ces systèmes connectés, qui permettent de conserver souplesse d'accès et richesse des fonctions. Cet article décrit les menaces auxquelles sont exposés les réseaux d'énergie et les mesures de protection disponibles pour y faire face.

Les systèmes centralisés constituent déjà des cibles

Plusieurs attaques perpétrées contre des infrastructures énergétiques ont fait la une des journaux ces dernières années. L'attaque dont a été victime la compagnie Colonial Pipeline a privé d'essence une bonne partie de la côte est des États-Unis en 2021; celles menées contre un système de distribution électrique de l'Ukraine ont réussi à couper l'électricité à 225 000 foyers de Kiev, et la contamination des infrastructures d'enrichissement d'uranium par le ver informatique Stuxnet a mis à mal la filière nucléaire de l'Iran. Ces attaques avaient des objectifs différents: l'attaque contre Kiev et le ver Stuxnet cherchaient à déstabiliser des États, alors que celle menée contre Colonial Pipeline semble avoir été déployée pour extorquer de l'argent à l'entreprise en question. Dans tous les cas, elles ont eu un impact majeur sur leurs cibles.

Les points communs de ces attaques: leurs portées géographiques et leurs périmètres limités à un objectif précis. Dans chacun de ces cas, la cible a été clairement identifiée en amont afin de déterminer, entre autres, ses vulnérabilités ainsi que les moyens directs ou indirects d'y accéder. L'attaque de l'infrastructure électrique de Kiev a visé les transformateurs 110 kV et 35 kV par l'intermédiaire des centres de contrôle régionaux. Sa planification a probablement duré de mars à décembre 2015, exploitant des faiblesses de la sécurité d'appareils rendus accessibles, par exemple, par des vols de mots de passe des personnes en charge de la maintenance.

De tels actes de piratage informatique vont se multiplier, car la motivation et la puissance des hackers augmentent avec l'interconnexion croissante des systèmes. Le problème est bien compris et traité par les gestionnaires de réseaux ou par leurs prestataires de services. Ainsi, bien que très exposées, ces installations sont aussi celles qui sont le plus surveillées puisqu'elles se trouvent sous la responsabilité d'exploitants qui doivent rendre des comptes aux autorités. Ceux-ci mettent dès lors en place des protections et prennent des mesures permettant de diminuer la vulnérabilité de leurs systèmes face aux attaques, jusqu'à ce que la complexité et le coût de ces dernières atteignent un niveau tel qu'elles deviennent inintéressantes pour des hackers.

Décentralisation ne signifie pas dilution des risques

Si la protection des systèmes centralisés est en général prise en compte, ce n'est pas toujours le cas pour les systèmes des particuliers ou des petites collectivités. Bien que ces derniers puissent également être gérés à distance – que ce soit à des fins de comptabilité, de suivi de performance, de diagnostic ou de maintenance –, leur sécurité n'est, quant à elle, que peu ou pas du tout considérée. En effet, un particulier ou une petite entreprise produisant de l'électricité (installation photovoltaïque, turbinage, récupération de chaleur, etc.) manque généralement de temps, de moyens ou bien d'expertise pour assurer la sécurité de son installation. Or, le nombre de ce genre d'installations croît de manière importante et continue depuis des années: fin 2020, l'Europe comptait environ 105 GW de production photovoltaïque (PV) distribuée (cumul d'installations de puissances < 1 MW). En comparaison, il n'y avait que 59 GW de production PV centralisée [2]. De plus, même si un producteur ou consommateur d'électricité est considéré comme étant un acteur pouvant engendrer un risque pour le réseau, il n'est soumis à des obligations de sécurisation que s'il produit ou consomme plusieurs centaines de MW. En Suisse, aucune installation photovoltaïque n'est considérée comme telle, puisqu'aucune ne produit actuellement plus de 10 MW (98 % des sites ont une puissance < 1 MW). Cette situation expose les réseaux électriques (suisses et étrangers) auxquels ces installations sont connectées à des attaques relativement faciles à concevoir et peu coûteuses à mettre en œuvre.

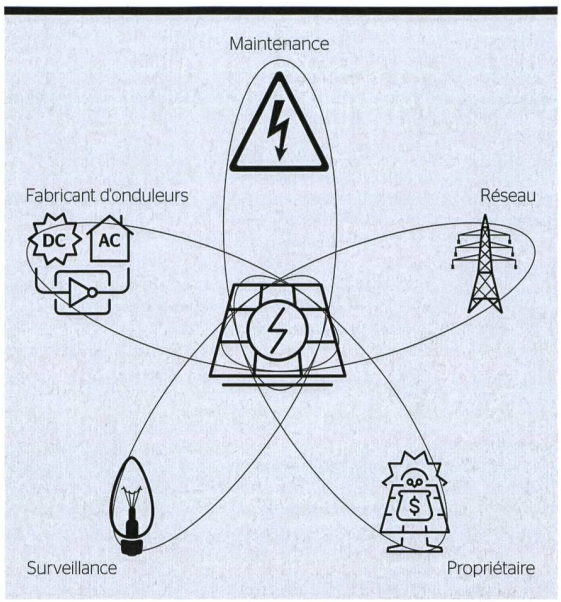

Figure 2 Les différents acteurs intervenant sur une infrastructure de panneaux solaires.

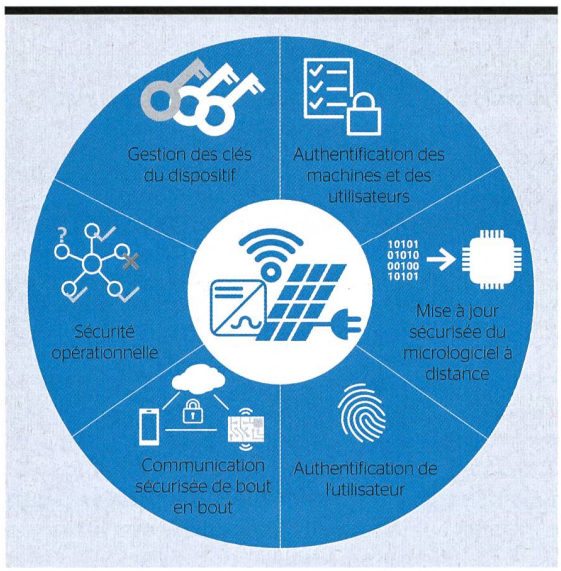

Figure 3 Les mesures les plus importantes pour augmenter la sécurité de l'infrastructure électrique « distribuée et connectée ».

Qu'ils soient petits ou grands, les sites de production sont de plus en plus nombreux et interconnectés afin de faciliter leur gestion à distance. La surface exposée aux attaques croît en conséquence et engendre ainsi des risques importants pour l'infrastructure globale. Par ailleurs, l'amélioration progressive de la protection des niveaux supérieurs de l'infrastructure du réseau électrique repousse les attaques vers les éléments les plus faibles des niveaux moyenne et basse tensions. Les petits sites deviennent donc des cibles de choix pour les hackers. La défaillance d'un nombre restreint de nœuds n'aura généralement qu'un impact relativement faible sur le réseau et le service fourni, mais une attaque synchronisée ciblant un nombre élevé de nœuds pourrait provoquer d'autres défaillances, voire une interruption du service ou la destruction de certains équipements.

Dans les installations de petite taille, comme dans d'autres applications de l'Internet des objets, la sécurité est très souvent négligée au profit de la simplicité d'implémentation et d'installation. Beaucoup d'appareils connectés utilisent, par exemple, encore les mots de passe par défaut [3] ou communs à toute une entreprise. Mais on peut aussi avoir affaire à des gestions de clés imparfaites compromettant les mises à jour des micrologiciels, ou à des systèmes d'exploitation obsolètes qu'il est impossible de mettre à jour.

Ces vulnérabilités des infrastructures électriques des niveaux 6 et 7 sont encore aggravées par le nombre de plus en plus élevé d'intervenants dans l'exploitation à distance **(figure 2)** et par le nombre relativement faible de fournisseurs de matériel (par exemple, 68 % du marché des éoliennes est tenu par une seule marque). Ces derniers points augmentent l'impact de la découverte d'une éventuelle vulnérabilité et rendent une mise à jour des éléments encore plus difficile, si celle-ci n'a pas été anticipée. Chacun de ces acteurs peut, volontairement ou non, devenir le vecteur d'une attaque si son système informatique est lui-même vulnérable ou compromis.

Tous les acteurs sont concernés

La sécurité informatique doit faire partie intégrante du système dès sa conception. En Europe, les professionnels de la production et du transport de l'énergie y investissent déjà entre 250 et 400 millions d'euros par an [4]. Cet effort doit être relayé par les acteurs de la moyenne et basse tension ainsi que par les fabricants de matériel et par les autorités établissant la règlementation (par exemple celle imposée par le BSI – l'Office fédéral de la sécurité des technologies de l'information allemand – ou les recommandations du Réseau européen pour la cybersécurité – l'European Network for Cybersecurity ENCS). Les compteurs connectés ont longtemps présenté des failles de sécurité importantes. Leur diffusion à grande échelle (230 millions d'unités déjà installées en Europe en 2020) justifie la part de 10 à 15 % du prix du développement consacrée à la sécurisation de ces appareils.

Même si le sujet de la cybersécurité peut sembler difficile à aborder, le nombre de recommandations **(figure 3)** que les fabricants doivent intégrer dans leurs systèmes (gestion de clés, accréditations, mise à jour sécurisée, sécurisation des échanges, etc.) est limité. Ces exigences permettent non seulement de sécuriser un appareil lors de son déploiement, mais aussi d'assurer sa maintenance durant toute sa durée de vie (20 ans et plus), par exemple en automatisant la fastidieuse tâche des mises à jour.

Dans de nombreux cas, des outils standards, existants et éprouvés tels que la sécurisation des communications en utilisant le protocole TLS (Transport Layer Security) suffiront.

De plus, de nombreuses boîtes à outils ainsi que divers frameworks et systèmes d'exploitation sont disponibles et peuvent faciliter le développement, la réalisation et la maintenance de réseaux d'objets connectés ainsi que de leurs applications.

La norme minimale pour les TIC [5] et l'IoT Security Compliance Framework [6] en sont deux exemples. Néanmoins, leur intégration ne sera pas toujours aisée : soit parce que la compétence n'est pas disponible chez le fabricant, soit car la menace n'est pas encore couverte par les outils sélectionnés. Dans ce cas, de nombreux instituts, comme le CSEM, peuvent accompagner les fabricants et leurs architectes dans l'évaluation du risque de leurs produits et dans la réalisation d'une architecture sécurisée, depuis sa spécification jusqu'à son implémentation optimisée, en adaptant les solutions proposées aux exigences et contraintes de la solution.

Références

[1] Office fédéral de la protection de la population (OFPP), « Catastrophes et situations d'urgence en Suisse 2020 : rapport sur l'analyse nationale des risques », p. 33, 2020.

[2] G. Masson, I. Kaizuka, « Trends in Photovoltaic Applications 2021 », IEA Photovoltaic Power Systems Programme, 2021. iea-pvps.org/wp-content/uploads/2022/01/IEA-PVPS-Trends-report-2021-4.pdf

[3] ispyconnect.com/userguide-default-passwords.aspx

[4] D. Ferrara, L. Marinos, S. Portesi, E. Tsekmezoglou, Gartner Team, « EU Cybersecurity Market Analysis : IoT in Distribution Grids », European Union Agency for Cybersecurity ENISA, 2022. doi:10.2824/519005

[5] Norme minimale pour les TIC, Office fédéral pour l'approvisionnement économique du pays OFAE. bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

[6] iotsecurityfoundation.org/tag/iot-security-compliance-framework

Auteurs

Martin Sénéclauze est senior project manager au sein du groupe Firmware & Security for connected devices du CSEM.
→ CSEM, 2000 Neuchâtel
→ martin.seneclauze@csem.ch

Damian Vizár est data security expert au sein du groupe Firmware & Security for connected devices du CSEM.
→ damian.vizar@csem.ch

Pierre-Jean Alet est responsable du groupe Digital Energy Solutions du CSEM.
→ pierre-jean.alet@csem.ch

Philippe Dallemagne est senior expert et coordinateur des activités IoT & Vision au sein de la Business Unit Integrated & wireless systems du CSEM.
→ philippe.dallemagne@csem.ch

RÉSUMÉ

Das diffuse Risiko der Cybersicherheit

Digitalisierung und Sicherung von Niederspannungsnetzen

Um die Fernverwaltung zu vereinfachen, werden grosse und kleine Stromerzeugungsanlagen immer öfter miteinander verbunden. Die Angriffsfläche für Cyberattacken wächst entsprechend und stellt ein erhebliches Risiko für die gesamte Infrastruktur dar. Während der Schutz zentralisierter Systeme auf den Netzebenen 1 bis 5 in der Regel berücksichtigt wird, ist dies bei Systemen von Privatpersonen oder kleinen Gemeinschaften, die an das Niederspannungsnetz angeschlossen sind, oft nicht der Fall. Die Zahl dieser Systeme, die aufgrund ihrer geringen Leistung keinen Sicherungspflichten unterliegen, steigt jedoch schnell an.

Kleine Standorte werden daher zu beliebten Zielen für Hacker, zumal die zunehmende Intensivierung des Schutzes bei höheren Netzebenen die Angriffe auf Elemente der niedrigeren Netzebenen zurückdrängt. Ein gleichzeitiger Angriff auf viele Knoten kann zu Ausfällen, Unterbrechungen des Dienstes oder der Beschädigung von Geräten führen.

Die IT-Sicherheit muss daher von Anfang an ein integraler Bestandteil der Systeme sein. Glücklicherweise gibt es Lösungen, um diese besonders anfälligen Geräte zu sichern. Es ist auch positiv, dass die Anzahl der Empfehlungen, die Hersteller bei ihren Systemen berücksichtigen müssen (Schlüsselverwaltung, Akkreditierungen, sichere Updates, sicherer Datenaustausch usw.), begrenzt ist. Oft reichen bereits vorhandene und bewährte Standardwerkzeuge aus, wie z. B. die Sicherung der Kommunikation mithilfe des TLS-Protokolls (Transport Layer Security). Zudem gibt es zahlreiche Toolkits sowie verschiedene Frameworks und Betriebssysteme – der IKT-Minimalstandard und das IoT Security Compliance Framework sind zwei Beispiele –, die die Entwicklung, Implementierung und Wartung besser gesicherter Netzwerke vernetzter «Dinge» erleichtern. CHE