Contre les cyber-risques

Autor(en): **[s.n.]**

Objekttyp: **Article**

Zeitschrift: **Energeia : Newsletter de l'Office fédéral de l'énergie**

Band (Jahr): **- (2017)**

Heft 2

PDF erstellt am: **21.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-681961

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

CONTRE LES CYBER-RISQUES

Comment la Confédération conçoit-elle, avec la branche énergie, des réseaux plus intelligents et plus sûrs? L'analyse des besoins de protection de l'Office fédéral de l'énergie aide à évaluer les risques. La branche doit fixer des normes uniformes.

La Stratégie énergétique 2050 prévoit que la plupart des ménages suisses seront équipés de systèmes de mesure intelligents d'ici 2025. Ces smart meters permettront aux fournisseurs d'énergie et aux consommateurs finaux de réduire les coûts en collectant régulièrement et automatiquement des données détaillées de consommation.

Evaluer les cyber-risques

Grâce à l'utilisation de ces systèmes de mesure intelligents, le réseau devient plus intelligent, mais aussi plus vulnérable. Le défi est d'identifier au préalable les faiblesses et les risques potentiels pour la sécurité. L'étude mandatée par l'Office fédéral de l'énergie a récemment analysé les domaines nécessitant un certain degré de protection. Cette analyse pondère les menaces potentielles en fonction de la probabilité de leur apparition, afin de définir dans quelle mesure elles présentent un risque pour la sécurité.

Que se passe-t-il par exemple si mille smart meters tombent tout à coup en panne suite à un défaut technique ou à un sabotage? Quelles en seraient les conséquences? Quels en seraient les coûts? Comment faut-il protéger les smart meters contre les perturbations externes et les cyberattaques?

Analyse des scénarios de risque

L'analyse des besoins de protection traite ces questions. Elle a pris en compte des cas isolés, mais également des événements à grande échelle ainsi que des actions délibérées telles qu'une manipulation de données, l'abus de droits d'accès ou les faux décomptes sur plusieurs années. Sont considérés comme catastrophiques les cas induisant des coûts supérieurs à un million de francs. La classification du risque est basée sur un modèle de l'Unité de pilotage informatique de la Confédération.

Besoin de protection accru

14 scénarios de risque avec différentes variantes ont été conçus et analysés du point de vue du gestionnaire du réseau de distribution ou d'un prestataire tiers de mesures (gestionnaire de données) et du consommateur final. «Les scénarios plausibles ont été pris en compte», déclare Bruno Le Roy, spécialiste réseaux à l'Office fédéral de l'énergie. «L'analyse a révélé que les besoins de protection pour les infrastructures des systèmes de mesure intelligents sont de taille.» Les besoins de protection ont été définis pour chaque scénario et, sur cette base, des mesures de sécurité adéquates ont été recommandées.

Fixer des normes de branche

La balle est maintenant dans le camp de la branche: l'Association des entreprises électriques suisses (AES) doit définir et consigner par écrit des prescriptions et des normes uniformes pour la cybersécurité des systèmes de mesure. Il incombe à un organe indépendant de contrôler la mise en œuvre de ces prescriptions.

«Nous avons ainsi trouvé pour la Suisse une solution flexible et subsidiaire qui laisse aux acteurs du marché la possibilité de fixer eux-mêmes les exigences minimales», ajoute Bruno Le Roy. D'autres pays ont en revanche un système relativement plus rigide et plus onéreux. Selon l'expert, la mise en œuvre du modèle suisse doit être plus simple. *(bra)*

Répartition des tâches

La Confédération fait une analyse des besoins de protection.

La branche fixe des normes.

Un organisme de contrôle surveille la mise en œuvre.

Évaluation du risque

faible moyen haut

Ampleur des dégâts x probabilité d'apparition = niveau du risque
Il en résulte les besoins de protection et les mesures.

Source: OFEN