Energie : d'après le nouveau rapport de l'Agence européenne ENISA, la cybersécurité est primordiale pour lutter contre les menaces cybernétiques visant les réseaux intelligents nécessaires pour assurer la disponibilité énergétique

D'après l'Agence européenne de cybersécurité ENISA, il est primordial d'évaluer les menaces cybernétiques contre les réseaux intelligents afin d'assurer leur protection et garantir la disponibilité énergétique.

Les réseaux intelligents sont des « systèmes de systèmes » complexes, permettant le stockage, le transport et la gestion d'énergie depuis la production jusqu'au consommateur. L'énergie étant essentielle au bon fonctionnement de la société et de l'économie, un réseau intelligent devient de facto une infrastructure critique. En associant l'énergie et les infrastructures d'information, les réseaux intelligents deviennent des infrastructures critiques, qui doivent fonctionner en toute sécurité tout en respectant les données privée des utilisateurs.

Le professeur Udo Helmbrecht, directeur exécutif de l'ENISA, a commenté : « *Il est indispensable de comprendre l'éventail complet des menaces cybernétiques afin d'identifier quelles sont les mesures de protection nécessaires aux réseaux intelligents. Ce rapport répond à la question urgente des fournisseurs et des acteurs concernés par le secteur de l'énergie : il fournit des outils pour évaluer le niveau d'exposition aux risques encourus par les infrastructures des réseaux intelligents. Dans le domaine de la cybersécurité, nous devons fournir des efforts de façon collective et coordonnée afin de réduire l'impact de ces risques.*

Ce rapport fournit aussi la liste des menaces cybernétiques qui touchent les infrastructures des réseaux intelligents. Il fait l'inventaire des différentes approches et bonnes pratiques disponibles dans le domaine de la cybersécurité et de la protection. L'étude établit également la liste des menaces internes affectant les infrastructures des réseaux intelligents en matière de technologies de l'information et présente une variété de menaces provenant d'erreurs et d'attaques internes.

Principales conclusions : Les conclusions clés du rapport conseillent de :

- *Prendre en considération les menaces externes et internes* : en matière de cybersécurité, les menaces cybernétiques externes constituent la principale source d'exposition extérieure. Les responsables de menaces et attaques cybernétiques, sont à l'origine de cet environnement cybernétique à risque.
- *Décomposer et classer les éléments de réseaux intelligents exposés aux menaces* : cela comprend le matériel électrique tel que les câbles, les interrupteurs, les routeurs, les capteurs et l'information, mais aussi les logiciels tels que les systèmes d'exploitation, incluant les services, le matériel, l'infrastructure et le personnel que cela nécessite.
- *Utiliser le savoir-faire disponible* : il s'agit de réutiliser les bonnes pratiques existantes après avoir déterminé le niveau de protection désiré.
- *Etablir la **liste des menaces cybernétiques spécifiques aux réseaux intelligents**, telles que* :
    - La mise sur écoute/l'interception/le piratage : ex. la fuite d'information, l'interception de fréquences électromagnétiques/radio, les attaques contre les analyseurs de réseau (« renifleurs »), la défaillance des appareils et des systèmes, les attaques et les attaques physiques,
      et les **responsables de menaces cybernétiques** tels que les entreprises, les cybercriminels, les employés, les haktivistes, les Etats nations, les catastrophes naturelles, les terroristes ou encore les nouveaux combattants cybernétiques.
- *Evaluer les fragilités et les risques au sein même des réseaux intelligents.*
- *L'évaluation doit être faite par les propriétaires* : l'Agence conclut que seuls les propriétaires de ces infrastructures peuvent évaluer le degré d'exposition aux risques et aux menaces, car ils maîtrisent leur complexité et leurs interdépendances.

Voir le rapport complet

Contexte général :

Le rapport de l'ENISA sur les réseaux intelligents (décembre 2012) ; 10 recommandations pour rendre les réseaux intelligents européens plus sûrs (juillet 2012)
La Stratégie de l'UE en matière de cybersécurité (juillet 2012), et la Proposition de directive européenne en matière de cybersécurité.

Pour toute demande d'interview, veuillez consulter : Ulf Bergström, porte-parole, ulf.bergstrom@enisa.europa.eu, téléphone portable : + 30 6948 460 143 ; ou notre expert, Dr.

Communiqué de presse

30/01/2014

EPR/07/2014

www.enisa.europa.eu

Louis Marinos, resilience@enisa.europa.eu

Veuillez noter: traduction. La version anglaise est la seule version officielle
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu