

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?



Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Cette étude analyse les risques de cyberattaques sur des infrastructures énergétiques européennes, ainsi que leurs potentielles conséquences, notamment sur les réseaux électriques. Elle offre également une approche comparative des mesures prises par différents pays d'Europe afin de protéger leur industrie et collaborer à l'échelle de l'Union européenne.

La digitalisation de l'industrie énergétique permet de révolutionner les processus de production, de stockage, de transport et de consommation d'énergie. Nos infrastructures énergétiques, conçues il y a plusieurs décennies et prévues pour demeurer fonctionnelles pour de nombreuses années encore, côtoient désormais des équipements numériques avec lesquels elles interagissent au quotidien. Ces évolutions, qui sont aujourd'hui un gage de disponibilité, d'efficacité et de réactivité sur toute la chaîne de valeur énergétique, ouvrent pourtant la voie à un type de menace qui jusqu'en 2010 avait relativement épargné cette industrie : les cyberattaques.

Le nombre et la technicité des attaques ont augmenté après les dégâts causés par le virus Stuxnet au sein du complexe d'enrichissement nucléaire iranien de Natanz, bien que cette attaque demeure la plus sophistiquée observée à ce jour. Et s'il y a une réelle prise de conscience des enjeux dans le secteur énergétique, les risques persistent. Les politiques de transition énergétique et les efforts d'intégration des énergies renouvelables ne feront que renforcer cette tendance tant que la cybersécurité ne fait pas partie de la réflexion sur l'avenir du système énergétique.

La réglementation tente de s'adapter, notamment en France où les autorités collaborent étroitement avec les entreprises de l'énergie pour faire émerger un cadre réglementaire contraignant, et protéger les Opérateurs d'Importance Vitale (OIV). Cette démarche inspire également d'autres pays d'Europe, mais des mesures communes à toute l'Union européenne sont à prendre rapidement afin de garantir la sécurité de nos réseaux énergétiques, fortement interconnectés.

LIRE L'ETUDE (PDF)

Original de l'article mis en page : Cyberattaques et systèmes énergétiques: faire face au risque | IFRI – Institut français des relations internationales

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous accompagner dans vos démarches de mise en conformité avec la réglementation Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

