Le secteur des énergies renouvelables particulièrement vulnérable aux cyberattaques selon le FBI

Le FBI alerte l'industrie privée sur les vulnérabilités du secteur américain des énergies renouvelables face aux cyberattaques, rapporte Cybersecurity Insiders. Ces attaques, qui visent à voler la propriété intellectuelle, à perturber les opérations, à déployer des ransomwares ou à déstabiliser des pays, présentent des risques importants.

L'alerte vise en particulier les logiciels qui contrôlent les systèmes matériels et logiciels indispensables au bon fonctionnement des technologies des énergies renouvelables.

Les pirates informatiques ciblent de plus en plus les systèmes de panneaux solaires, qu'ils soient personnels ou commerciaux. Ils se concentrent sur les logiciels qui relient les panneaux solaires aux onduleurs, qui convertissent le courant continu en courant alternatif. La plupart de ces onduleurs ne disposent pas de mesures de cybersécurité suffisantes pour surveiller les changements lorsqu'ils sont connectés à l'internet, ce qui les rend vulnérables aux cyberattaques.

Sources : US Renewable Energy Sector vulnerable to cyber threats says FBI - Cybersecurity Insiders (cybersecurity-insiders.com)

https://france3-regions.francetvinfo.fr/grand-est/marne/cyberattaque-des-pirates-s-attaquent-a-une-centrale-hydroelectrique-ils-s-en-prennent-en-fait-a-un-moulin-2957297.html

https://www.welivesecurity.com/2022/06/13/industroyer-cyber-weapon-brought-down-power-grid/

NOTE : ESET ne porte aucune responsabilité quant à l'exactitude des informations provenant de sources tierces.

Benoit Grunemwald - Expert en Cybersécurité chez ESET France réagit

« Les beaux jours arrivent (enfin), il est temps pour bon nombre de particuliers et d'entreprises d'envisager des alternatives à leurs sources d'énergies fossiles ; les plus répandues sont les panneaux solaires. Pour autant, ceux-ci sont contrôlés par des systèmes informatiques qu'il est possible de pirater. Le sabotage est une éventualité, une modification malveillante pourrait endommager l'installation, voir sa destruction.

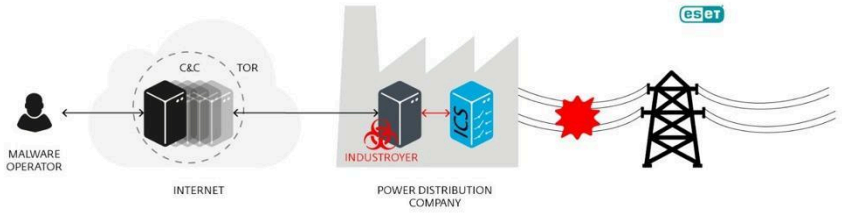
Ces cas rares sont possibles et seront de plus en fréquents à mesure de l'adoption massive des installations personnelles et professionnelles. Ceci s'est produit en mars 2024 sur une centrale de production hydroélectrique, comme le rapporte FranceInfo. Cette attaque sans graves conséquences n'est pas sans rappeler les attaques menées contre les fournisseurs d'énergie en Ukraine, créant un blackout.

Nos conseils si vous souhaitez installer une production d'énergie alternative :

- *Considérez la sécurité informatique de votre installation, faites appel à un professionnel si besoin.*

- *Pour tout accès depuis l'extérieur, utilisez un VPN pour vous connecter à votre installation. N'ouvrez pas l'accès à votre installation sans protection.*
- *Surveillez les logs de vos installations pour détecter les comportements malveillants.*

Gardez vos systèmes à jour, appliquez les correctifs dès que possible. »



N'hésitez pas à revenir vers nous pour toute mise en relation.

NOTE : ESET ne porte aucune responsabilité quant à l'exactitude des informations provenant de sources tierces.

A propos d'ESET

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour protéger les entreprises, les infrastructures critiques et les consommateurs du monde entier contre des menaces digitales de plus en plus sophistiquées. Protection des terminaux et des mobiles, détection et traitement des incidents, chiffrement et authentification multifacteur... les solutions performantes et faciles à utiliser d'ESET protègent et supervisent discrètement 24 heures sur 24, 7 jours sur 7, en mettant à jour les défenses en temps réel pour assurer sans aucune interruption la sécurité des utilisateurs et le bon fonctionnement des entreprises. L'évolution des menaces exige d'une entreprise de sécurité informatique qu'elle évolue également. C'est le cas d'ESET grâce à ses centres de R&D dans le monde entier travaillant à la protection de notre avenir commun. Pour plus d'informations, consultez www.eset.com/fr/ ou suivez-nous sur LinkedIn, Facebook et Twitter.