

Alerte rouge pour la cybersécurité dans le secteur de l’énergie

02 septembre 2025, 09:26

Tatiana Galibus

Les cybermenaces sont aussi importantes que réelles, notre défense doit l’être aussi

La menace est bien présente

11 avril 2022. Deutsche Windtechnik, un exploitant allemand d’éoliennes, est contraint de désactiver ses connexions de télésurveillance des données aux éoliennes. Ces dernières seront ensuite désactivées pour des raisons de sécurité, l’activité ne reprenant son cours normal que le 14 avril. La source confirmée de la défaillance de connexion était une attaque par rançongiciel.

14 mai 2025. Des responsables américains de l’énergie annoncent réévaluer l’utilisation d’onduleurs pour panneaux solaires de fabrication chinoise à la suite de la découverte de dispositifs de communication indésirables susceptibles d’être utilisés comme canal de communication bidirectionnel avec le fournisseur et certaines parties chinoises associées, et ainsi de constituer une véritable menace pour le réseau énergétique auquel ils sont connectés.

Ce ne sont là que deux exemples concrets de cybermenaces réelles et continues pouvant grever notre secteur énergétique. Et, alors que nous avons encore à l'esprit les mégacoupures récentes d'électricité en Espagne et au Portugal, un lien avec les cybermenaces et la criminalité pourrait encore être découvert pour des dizaines d'autres incidents. Nos systèmes énergétiques et notre réseau sont non seulement vulnérables, mais ils font l'objet d'attaques en ce moment même.

Les systèmes énergétiques sont-ils intrinsèquement vulnérables ?

Une grande majorité des systèmes énergétiques mondiaux sont confrontés à des défis de sécurité uniques, causés par une combinaison inquiétante de vulnérabilités potentielles.

La plupart des fournisseurs d'énergie dépendent encore de **l'infrastructure de technologie opérationnelle (OT) héritée**. La technologie consiste en un réseau et en des composants SCADA, datant souvent de plusieurs décennies, et n'ayant jamais été conçus pour être connectés à un réseau public comme Internet. La cybersécurité ne constituait même pas une préoccupation secondaire. Les centrales électriques et les parcs éoliens, par exemple, utilisent souvent les protocoles ICS (Industrial Control Systems) sans chiffrement ni aucune forme d'authentification moderne.

De nos jours, pourtant, ces infrastructures sont de plus en plus **accessibles à distance**, en utilisant des **interfaces** de maintenance et de surveillance souvent **mal configurées, ou dépourvues d'authentification multifacteur**. Inutile de dire qu'elles deviennent ainsi des cibles faciles pour les accès non autorisés. Vous vous souvenez du piratage Viasat, qui a attaqué et désactivé une partie de la communication ukrainienne par satellite ? Il a été permis précisément par une connectivité à distance non sécurisée de ce type pour le contrôle des interfaces.

Ajoutez à cela les différents **composants** nécessaires pour former la **chaîne d'approvisionnement** énergétique. Certains d'entre eux peuvent être fabriqués par **des fournisseurs étrangers**, comme c'était le cas des puces chinoises dans les systèmes solaires. D'autres peuvent contenir **des bibliothèques logicielles tierces**. Dans les deux scénarios, ces composants peuvent compromettre la chaîne d'approvisionnement et introduire des portes dérobées cachées. La cyberattaque SolarWinds en 2020 fut un exemple frappant de la façon dont de telles vulnérabilités peuvent être exploitées.

Par ailleurs, toutes les vulnérabilités ne sont pas numériques : l'**accès physique** à une infrastructure énergétique peut également s'avérer risqué. En particulier, il est beaucoup plus facile de s'introduire dans une infrastructure énergétique distante ou offshore et d'y causer des dommages sans être remarqué. Des chercheurs de l'Université de Tulsa ont rapporté qu'il fallait moins d'une minute pour crocheter la porte d'une éolienne non surveillée et accéder ainsi au serveur non sécurisé et, de là, accéder aux adresses IP représentant chaque éolienne du réseau.

Les systèmes énergétiques ne sont pas intrinsèquement vulnérables, mais de nombreuses vulnérabilités potentielles, pouvant mener à des violations de la sécurité, existent à divers niveaux. Une conclusion inquiétante, compte tenu des nombreuses cybermenaces qui circulent aujourd'hui.

Quelles sont les menaces les plus courantes ?

L'industrie de l'énergie est vitale pour tout pays dans le monde, et constitue donc une cible populaire pour la cybercriminalité et d'autres criminels cherchant à réaliser des profits considérables ou à déstabiliser une nation. Sans surprise, une variété de menaces visent les infrastructures énergétiques :

- **Rançongiciels:** les cybercriminels attaquent les grands fabricants d'éoliennes pour perturber les activités et ne les libérer qu'après le paiement d'une rançon importante
- **Perturbation de la communication:** les cyberattaques ciblant les liaisons par satellite ou sans fil peuvent désactiver les fonctions de surveillance et de contrôle, ce moyen peut être utilisé comme attaque stratégique dans une guerre générale, comme ce fut le cas avec Ka-Sat
- **Compromission de la chaîne d'approvisionnement**: les vulnérabilités telles que Log4j ou SolarWinds exposent des écosystèmes entiers à des attaques jour zéro, même longtemps après leur déploiement
    - **Sabotage physique**: comme nous l'avons vu ci-dessus, une sécurité physique faible peut entraîner une violation numérique. Mais l'accès physique peut également être utilisé pour endommager physiquement l'infrastructure, la méthode est souvent utilisée en combinaison avec les cyberattaques, pour renforcer l'impact des attaques

Notez l'absence des mots « futur », « possibilité » et « potentiellement » dans les paragraphes ci-dessus. Les menaces ne sont pas seulement des risques théoriques : elles sont réelles, en augmentation et systémiques. Et elles requièrent une réaction ferme et immédiate de toutes les parties impliquées.

UE : une attention accrue aux infrastructures critiques

La réaction requise ne doit pas se limiter aux fournisseurs d'infrastructures énergétiques ou à leurs propres fournisseurs. Elle ne doit pas non plus s'arrêter à la frontière, car l'approvisionnement énergétique s'inscrit toujours plus dans un contexte international.

Consciente de cette réalité et de l'urgence de la situation, l'UE met en place un cadre réglementaire renforcé axé sur les infrastructures critiques :

- **Directive NIS2:** cette directive visant les services essentiels, comme la fourniture d'énergie, élargit son champ d'application pour inclure les énergies renouvelables, les gestionnaires de réseau et les fabricants de technologies énergétiques, elle oblige les acteurs de ce secteur à élaborer une stratégie solide autour de la gestion des risques, de la réponse aux incidents et de la supervision des fournisseurs
- **Cyber Resilience Act (CRA, règlement sur la cyberrésilience):** ce règlement introduit des exigences de base en matière de cybersécurité pour tous les produits comportant des éléments numériques. Cela inclut bien évidemment tout l'IoT énergétique, les systèmes de contrôle et les logiciels industriels

Les deux cadres susmentionnés favorisent **la collaboration et le partage d'informations** entre les secteurs public et privé, et appliquent des principes de **sécurité dès le stade de la conception** dans l'ensemble de la chaîne d'approvisionnement.

Même s'il s'agit de « lignes directrices » et de « réglementations », vous ne devez pas les considérer comme facultatives ou comme des préoccupations futures. La conformité à ces

réglementations devient de plus en plus une exigence métier fondamentale pour toute partie prenante du secteur de l'énergie. Agir maintenant est donc non seulement souhaitable, mais tout simplement essentiel.

Que pouvez-vous faire aujourd'hui ?

Le message général « il est temps d'agir » s'applique à toutes les parties impliquées, que vous soyez développeur, intégrateur ou décideur dans le secteur de l'énergie.

Mais comment pouvez-vous agir ? Et que convient-il de faire en premier ?

Pour commencer, vous devez avoir une compréhension globale du domaine de la sécurité des infrastructures critiques et des moyens de renforcer la sécurité et de réduire les menaces.

Nous pouvons vous aider à acquérir ces connaissances et à guider vos travaux futurs.

Vous pensez avoir atteint un niveau de connaissance suffisant et voulez maintenant passer à l'étape suivante ?

Nous vous invitons à intégrer notre projet de recherche COOCK+ collective sur les « produits connectés de confiance dans la transition énergétique ».
En participant à ce projet, vous aurez accès à :

- Un soutien d'experts de première ligne
- Des outils pratiques et des analyses
- Des directives claires concernant la sécurité des produits et leur préparation réglementaire

Si vous souhaitez en savoir davantage au sujet d'un des thèmes abordés, n'hésitez pas à me contacter. Pour discuter de vos besoins et de la manière dont nous pouvons vous aider, n'hésitez pas à me contacter à l'adresse tatiana.galibus@sirris.be.

Contactez-nous

Auteurs



Tatiana Galibus