

Les parcs éoliens constituent le prochain groupe cible des cyberattaques

23 décembre 2022, 16:02

Tatiana Galibus
Pieter Jan Jordaens

La croissance continue de l'énergie éolienne dépend, dans une large mesure, de l'interconnexion numérique des infrastructures énergétiques. Toutefois, plus les infrastructures énergétiques sont connectées, plus elles deviennent vulnérables. Les cybercriminels ont anticipé cette évolution comme en atteste le succès par trop fréquent de leurs assauts. Il est grand temps d'inverser la tendance.

Selon un récent article consacré à l'ÉOLIEN en mer, trois cyberattaques de grande envergure portées sur des parcs éoliens situés en Europe et visant à en compromettre la TO (systèmes informatiques assurant la gestion, la surveillance, l'automatisation et le pilotage de systèmes industriels) ont été relevées en 2022 (à l'heure de la rédaction de cet texte).

D'après cet article, l'une des tâches les plus urgentes auxquelles les entreprises du secteur de l'énergie sont confrontées réside dans l'identification des maillons vulnérables de leurs projets et opérations avant que les cybercriminels puissent les déceler. Les entreprises doivent disposer d'une vue d'ensemble claire, exhaustive et actualisée de leurs systèmes d'information et de commande, fournisseurs connectés et systèmes tiers inclus. Il ne suffit pas aux entreprises de réitérer sporadiquement le processus d'identification de leurs maillons faibles. Ce processus doit

s’opérer à intervalles réguliers, afin de s’assurer de leur résistance aux nouveaux vecteurs d'attaque.

De l’effraction au piratage

S’agissant des parcs éoliens, au moins trois méthodes d’attaque distinctes (vecteurs) ont été identifiées à ce jour :

- pénétration dans une nacelle par effraction mécanique, puis raccordement à l’armoire de commande interne, en raison de la vulnérabilité du dispositif de sécurité sur site.
- compromission et commande à distance d’un ordinateur portable ou d’un téléphone d’ingénierie pour accéder à un point de terminaison manquant et tirer parti d’une connexion avec ce dernier ou bien accès par l'intermédiaire d'un RPV
- piratage de points de terminaison connectés à l’Internet tels que les caméras de vidéosurveillance installées au niveau d’une sous-station.

En définitive, ces vecteurs permettent tous d’accéder au système de surveillance et d’acquisition de données (SCADA) ainsi qu’à l’architecture du système de commande industriel. Lorsqu’ils sont dans la place, les cybercriminels peuvent prendre le contrôle de l’ensemble du parc éolien.

Parc éolien pris en défaut à l’issue de tests

Du crochetage, en moins d’une minute, de la serrure d’une porte de nacelle non surveillée à l’accès direct au serveur non sécurisé installé derrière cette porte, une équipe de chercheurs auprès de l’Université de Tulsa (Oklahoma, États-Unis) a démontré à quel point le piratage d’un parc éolien était aisé. Des criminels plus chevronnés élaborés pourraient provoquer une instabilité du réseau en agissant sur la régulation de la puissance et de la fréquence du dispositif de transmission au réseau. Scénario le plus défavorable : perte d’une ou plusieurs vies imputable, par exemple, à une augmentation, par un pirate, de la tension mesurée aux bornes d’une éolienne alors qu’un technicien travaille sur la structure ou encore à l’inflammation d’une éolienne résultant d’une telle élévation de la tension.

Maintien d’une longueur d’avance sur la cybercriminalité

Le monde de la cybersécurité évolue sans cesse. Les cyberattaques font peser un risque de pertes potentiellement considérables sur les exploitants de parcs éoliens. Mais, il n’est pas trop tard pour agir. Que faire ? Soyez prêt. Conservez une longueur d’avance sur les pirates. Il est capital de suivre de près l’évolution de la situation. Dans la mesure où les attaques sont de plus en plus organisées, la sécurité gagnerait à devenir plus leste et collaborative ; en d’autres termes, il faudrait que la sécurité soit assurée d’un bout à l’autre de la chaîne d’approvisionnement.

Dans les mois à venir, Sirris va organiser deux programmes pédagogiques (master classes), voués à la cybersécurité des services numériques ainsi qu’à celle des unités de production. Ces deux programmes sont conçus comme des parcours d'apprentissage, assortis de modules d’approfondissement théorique et des travaux pratiques personnalisés. Nous travaillons avec d’autres partenaires en cybersécurité pour dispenser les enseignements les plus pertinents en vous permettant d’acquérir une expérience déterminante en réseautage. En prime, vous bénéficierez de plusieurs séances de micro-coaching adaptées à vos préoccupations spécifiques.

Cliquez ici pour découvrir nos offres individuelles et collectives !

Pour plus d’informations : https://www.offshorewind.biz/2022/12/08/wind-firms-cannot-afford-to-ign…

Auteurs



Tatiana Galibus



Pieter Jan Jordaens