



Windparken volgende doelgroep voor cyberaanvallen

23 december 2022, 16:07

Tatiana Galibus

Pieter Jan Jordaens

De voortdurende groei van windenergie is sterk afhankelijk van een steeds meer digitaal verbonden energie-infrastructuur. Maar hoe sterker verbonden de energie-infrastructuur, hoe kwetsbaarder deze wordt. Cybercriminelen anticiperen hierop wanneer ze willen toeslaan, en te vaak met succes. Hoog tijd dus om de rollen om te draaien.

Volgens een [recent artikel over Offshore WIND](#) waren er in 2022 (op het moment van schrijven) drie spraakmakende cyberaanvallen op windparken in heel Europa, waarbij OT (de computersystemen die industriële systemen beheren, monitoren, automatiseren en besturen) het risico liepen uitgebuit en gecompromitteerd te worden.

Volgens het artikel is een van de meest urgente taken waar bedrijven in de energiesector voorstaan, het vaststellen waar hun projecten en activiteiten blootgesteld worden aan bedreigingen voordat cybercriminelen ze kunnen vinden. Bedrijven hebben nood aan een duidelijk, volledig en up-to-date overzicht van hun informatie- en besturingssystemen – inclusief de aangesloten systemen van hun leveranciers en van derden. Het is niet voldoende voor bedrijven om sporadisch op zoek te gaan naar kwetsbaarheden. Het moet op zeer regelmatige basis gebeuren om weerbaar te zijn tegen nieuwe aanvalsvectoren.

Van inbreken tot hacken

Er zijn tenminste drie verschillende aanvalsmethoden (vectoren) als het gaat om windparken:

- Fysiek inbreken in de turbine en verbinding maken met de interne computer. Dit is mogelijk door een lakse beveiliging ter plaatse;
- Inbreken en op afstand bedienen van een engineering laptop of gsm om toegang te krijgen tot en misbruik te maken van een ontbrekende eindpuntverbinding of via een VPN-verbinding;
- Hacken van met internet verbonden eindpunten, zoals CCTV-camera's in het onderstation.

Alle vectoren geven uiteindelijk toegang tot de architectuur van het industriële controlesysteem SCADA (supervisory control and data acquisition). Eenmaal binnen kunnen cybercriminelen de controle over het hele windpark overnemen.

Getest en niet goed bevonden

Onderzoekers van de universiteit van Tulsa (Oklahoma, VS) toonden aan hoe makkelijk het was om een windpark te hacken, waarbij ze in minder dan een minuut een onbewaakte turbinedeur konden openbreken en rechtstreeks toegang kregen tot de onbeveiligde server erachter. Beter voorbereide criminelen zouden instabiliteit van het elektriciteitsnet kunnen veroorzaken door de stroom- en frequentieregeling naar het net te veranderen. Het worstcase scenario is verlies van mensenlevens, bv. wanneer een hacker het voltage in de turbine verhoogt terwijl een technicus aan de constructie aan het werken is of wanneer de turbine vuur vat als gevolg van dergelijke spanningsverhoging.

Cybercriminaliteit voorblijven

Het cyberbeveiligingslandschap verandert elke dag. Exploitanten van windparken worden geconfronteerd met potentieel enorme verliezen als gevolg van cyberaanvallen. Toch is het nog niet te laat voor exploitanten om actie te ondernemen. Hoe? Door voorbereid te zijn. Hackers voor te blijven. De vinger aan de pols houden is essentieel: nu aanvallen steeds beter georganiseerd zijn, moeten de beveiligingsoplossingen beter op elkaar afgestemd en wendbaarder zijn, wat betekent dat de veiligheid van de hele toeleveringsketen dient gewaarborgd te zijn.

In de komende maanden organiseert Sirris twee trajecten (masterclasses), gewijd aan [cyberbeveiliging voor zowel digitale diensten](#) als [productie](#). Beide trajecten zijn ontworpen als leerreizen, met diepgaande theoriemodules en praktijksessies op maat. We werken met andere cyberbeveiligingspartners om de beste ervaringen te leveren evenals netwerkervaring. Daarbovenop krijgt u verschillende micro-coachingsessies voor uw specifieke bezorgdheden.

Bekijk [hier](#) ons collectief en individueel aanbod!

Verder lezen: [OffshoreWIND](#)

Auteurs



Tatiana Galibus



Pieter Jan Jordaens