

Alarmbellen voor cyberbeveiliging in de energiesector

28 augustus 2025, 15:56

Tatiana Galibus

Cyberdreigingen zijn reëel en komen dagelijks voor, onze verdediging moet minstens even goed zijn

De dreiging is reëel

11 april 2022. Deutsche Windtechnik, een Duitse exploitant van windturbines, ziet zich genoodzaakt de dataverbindingen met zijn windturbines uit te schakelen om beveiligingsredenen. Pas op 14 april kan de gegevensbewaking op afstand worden hervat. Later wordt bevestigd dat de verbindingsproblemen werden veroorzaakt door een ransomware-aanval.

14 mei 2025. Amerikaanse energieambtenaren kondigen aan dat ze omvormers voor zonnepanelen van Chinese makelij opnieuw onder de loep nemen nadat er malafide communicatieapparaten zijn ontdekt. Die worden mogelijk gebruikt als een tweerichtingscommunicatiekanaal met de leverancier en aanverwante Chinese partijen en vormen zo een grote bedreiging voor het energienetwerk waarop ze zijn aangesloten.

Dit zijn slechts twee concrete voorbeelden van de reële en voortdurende cyberbedreigingen voor onze energiesector. En met de Spaans-Portugese stroomstoring nog vers in het geheugen zijn er misschien nog tientallen andere incidenten waarbij het verband met cyberdreigingen en criminaliteit nog moet worden ontdekt. Onze energiesystemen en -netwerken zijn kwetsbaar en worden voortdurend aangevallen.

Zijn energiesystemen inherent kwetsbaar?

Wereldwijd kampt het overgrote deel van de energiesystemen met unieke veiligheids-uitdagingen, veroorzaakt door een zorgwekkende combinatie van potentiële kwetsbaarheden.

De meeste energieleveranciers vertrouwen nog steeds op **hun oude OT-infrastructuur**. Die technologie bestaat uit netwerk- en SCADA-componenten die vaak tientallen jaren oud zijn en nooit ontworpen werden om met een openbaar netwerk zoals het internet te worden verbonden. Van cyberbeveiliging was toen zelfs nog geen sprake. Zo gebruiken energiecentrales en windmolenparken nog vaak ICS-protocollen (Industrial Control Systems) zonder enige vorm van encryptie of authenticatie.

Tegenwoordig worden die infrastructuren echter in toenemende mate op **afstand benaderd**, via **onderhouds- en bewakingsinterfaces** die vaak **verkeerd geconfigureerd zijn of geen multifactorauthenticatie hebben**. Het spreekt voor zich dat ze op die manier gemakkelijke doelwitten worden voor ongeoorloofde toegang. Herinnert u zich nog de Viasat-hack waarbij een deel van de Oekraïense satelliet¬communicatie werd aangevallen en uitgeschakeld? Ook die werd mogelijk gemaakt door dergelijke onbeveiligde verbindingen op afstand om interfaces te besturen.

En dan zijn er nog de verschillende **componenten** waaruit de **energieketen** is opgebouwd. Sommige daarvan zijn mogelijk door **buitenlandse leveranciers** gemaakt, zoals het geval was met de Chinese chips in zonnesystemen. Andere kunnen dan weer **softwarebibliotheken van derden** bevatten. In beide scenario's kunnen die componenten de toeleveringsketen in gevaar brengen en verborgen achterpoortjes introduceren. De cyberaanval op SolarWinds in 2020 geeft aan hoe dergelijke kwetsbaarheden kunnen worden uitgebuit.

Niet alle kwetsbaarheden zijn trouwens digitaal van aard: ook de **fysieke toegang** tot energie-infrastructuur kan riskant blijken. Vooral bij afgelegen of offshore energie-infrastructuren is het een stuk eenvoudiger om ongemerkt toegang te krijgen of te knoeien met de infrastructuur. Onderzoekers van de Universiteit van Tulsa meldden dat het minder dan een minuut duurde om een onbewaakte deur van een turbine te forceren om toegang te krijgen tot een onbeveiligde server en van daaruit de IP-adressen van elke afzonderlijke turbine in het netwerk te verkrijgen.

Energiesystemen zijn niet inherent kwetsbaar, maar ze bevatten op diverse niveaus veel potentiële kwetsbaarheden die tot beveiligingsincidenten kunnen leiden. Een zorgwekkende conclusie gezien de vele cyberdreigingen die tegenwoordig de ronde doen.

Wat zijn de meest voorkomende bedreigingen?

De energiesector is van vitaal belang voor elk land ter wereld en vormt daarom een populair doelwit voor cyber- en andere criminelen die enorme winsten willen boeken of een land willen

destabiliseren. Het hoeft dan ook niet te verbazen dat energie-infrastructuren regelmatig ten prooi vallen aan cyberdreigingen:

- **Ransomware:** cybercriminelen vallen grote turbinefabrikanten aan om hun activiteiten te verstoren en pas weer vrij te geven nadat er een aanzienlijke som losgeld is betaald
- **Communicatiestoring:** cyberaanvallen gericht tegen satellietverbindingen of draadloze verbindingen kunnen bewakings- en controlefuncties uitschakelen, dat kan worden gebruikt bij wijze van strategische aanval in een algemene oorlogsvoering, zoals het geval was met Ka-Sat
- **Verstoring van de toeleveringsketen**: kwetsbaarheden zoals Log4j of SolarWinds stellen hele ecosystemen bloot aan ‘zero-day’-aanvallen, zelfs lang nadat ze zijn ingezet
- **Fysieke sabotage:** zoals we hierboven al aangaven, kan een zwakke fysieke beveiliging leiden tot digitale beveiligingsinbreuken. Bovendien kan de fysieke toegang worden gebruikt om fysieke schade toe te brengen aan de infrastructuur, dat gebeurt vaak in combinatie met cyberaanvallen om de impact van de aanvallen te vergroten

Let op de afwezigheid van de woorden ‘toekomstig’, ‘mogelijk’ en ‘uiteindelijk’ in bovenstaande paragrafen. De dreigingen zijn geen louter theoretische risico's, ze zijn reëel, komen steeds vaker voor en worden systematisch toegepast. Ze vereisen dan ook een onmiddellijke en krachtige reactie van alle betrokken partijen.

EU: meer aandacht voor kritieke infrastructuren

Die reactie mag zich niet beperken tot de leveranciers van energie-infrastructuur of hun verkopers. Ze mag ook niet stoppen bij de grenzen, aangezien energievoorziening een internationaal landschap van toenemend belang is geworden.

De EU erkent die realiteit en de urgentie ervan en implementeert momenteel een krachtiger regelgevend kader voor kritieke infrastructuren:

- **NIS2-richtlijn:** deze richtlijn voor essentiële diensten zoals energievoorzieningen breidt het toepassingsgebied uit naar hernieuwbare energiebronnen, netbeheerders en fabrikanten van energietechnologie, ze dwingt de spelers in de energiesector om een gedegen strategie rond risicobeheer, incidentrespons en leverancierstoezicht op te stellen
- **Cyber Resilience Act (CRA):** deze verordening introduceert basisvereisten inzake cyberbeveiliging voor alle producten met digitale onderdelen, het omvat uiteraard alle IoT- en besturingssystemen alsook industriële software voor energiesystemen

Beide bovengenoemde kaders bevorderen **de samenwerking en informatie-uitwisseling** tussen de publieke en private sector en dwingen de principes van **security by design** af in de hele toeleveringsketen.

Hoewel de termen ‘richtlijnen’ en ‘verordeningen’ anders doen vermoeden, mogen ze niet als optioneel of zorgen voor de toekomst worden beschouwd. De naleving van deze voorschriften wordt steeds meer een kernvereiste voor alle stakeholders in de energiesector. Nu handelen is dus geen keuzemogelijkheid, maar een absolute noodzaak.

Wat kunt u vandaag doen?

De overkoepelende boodschap 'grijp nu in' geldt voor iedereen die betrokken is bij de energiesector, van ontwikkelaars tot besluitvormers en integrators.

Maar wat kunt u doen? En waar ligt de prioriteit?

In de eerste plaats is het zaak om een grondig inzicht te krijgen in de hele kritieke infrastructuur en wat u kunt doen om de beveiliging op te drijven en bedreigingen te beperken.

Wij kunnen u helpen om die inzichten te verwerven en uw toekomstige inspanningen te sturen.

Hebt u voldoende inzicht gekregen en wilt u de volgende stap zetten?

Dan nodigen we u graag uit om deel te nemen aan ons **collectieve onderzoeksproject COOCK+** over ‘Betrouwbare geconnecteerde producten in de energietransitie’.

Door deel te nemen aan dit project krijgt u toegang tot:

- Eerstelijns ondersteuning door experts
- Praktijkgerichte tools en scans
- Duidelijke richtlijnen rond productbeveiliging en conformiteit met de regelgeving

Wenst u nog meer informatie over een van de bovenstaande onderwerpen, aarzel dan niet om contact met me op te nemen. Mail me via tatiana.galibus@sirris.be zodat we samen kunnen nagaan wat uw behoeften zijn en hoe we u kunnen helpen.

Samen kunnen we veilige en veerkrachtige energiesystemen bouwen vanaf de designfase.

Neem contact op

Auteurs



Tatiana Galibus