

De norm voor Cyber Security in de zonne-energiesector

Toenemende bedreigingen voor de wereldwijde energiesector

In de onderling verbonden wereld van vandaag is de energiesector bij uitstek een doelwit voor cyberaanvallen van alle kanten. Dergelijke bedreigingen variëren van cybercriminelen met financiële motieven tot politiek gemotiveerde aanvallen door natiestaten.

Alleen al in 2023 betaalden slachtoffers van cyberaanvallen wereldwijd (uit alle sectoren) 1,1 miljard dollar uit na ransomware-aanvallen - en dat is alleen nog maar de gerapporteerde schade.*

40,000

Zonne-energiesystemen op Nederlandse woningen en bedrijven zijn volgens de Nederlandse overheid kwetsbaar voor overname van afstand ([juli 2022](#))

130,000

Zonne-energiesystemen van diverse omvormerfabrikanten zijn volgens een bedrijf gespecialiseerd in cyberbeveiliging kwetsbaar voor cyberaanvallen (VS, [juli 2023](#))

\$200M

De geschatte verliezen van Target Corporation nadat in 2013 het netwerk van haar klimaatsysteemleverancier werd gehackt.

Onbeveiligde zonne-energiesystemen vormen kritieke bedrijfsrisico's

Zonne-energie is een snelgroeiend onderdeel van de mondiale energiemix en vormt inmiddels een aanzienlijk deel van de totale energieproductie in landen zoals Nederland, Duitsland en de VS. Het is voor veel bedrijven nu al een cruciale energiebron die bijdraagt aan het verlagen van de elektriciteitskosten en het garanderen van de bedrijfscontinuïteit.

Zonne-energiesystemen bieden niet alleen een duurzame energieoplossing, ze introduceren ook nieuwe cyberbedreigingen. Het hart van elk systeem wordt immers gevormd door de omvormer, een apparaat dat volgens de Internet of Things-gedachte (IoT) doorgaans verbonden is met internet om daarmee bewaking en aansturing van het systeem mogelijk te maken. Dit maakt het systeem gevoeliger voor cyberaanvallen in vergelijking met een goed afgeschermd gas- of kolencentrale.

Zonne-energie wordt ingezet voor een toenemende variatie aan energiebehoeften op locatie. Denk daarbij aan batterijen, EV-laders en klimaatsystemen. Naarmate de transitie naar energiebeheersystemen vordert, zal deze trend zich alleen maar verder doorzetten. Een onbeveiligd zonne-energiesysteem vormt daarmee niet alleen een bedreiging voor de bedrijfscontinuïteit, maar kan ook onbewust dienen als een toegangspoort voor hackers, die daarmee greep kunnen krijgen op de energieapparatuur en de bredere digitale platforms van een organisatie, met verdere materiële, financiële en reputatieschade tot gevolg.

Veelvoorkomende cyberrisico's zijn onder meer:

Datalekken en chantage

Hackers kunnen misbruik maken van kwetsbare zonne-energiesystemen om privégegevens te bemachtigen die circuleren op de interne netwerken van een organisatie. Zo'n datalek kan slachtoffers kwetsbaar maken voor chantage.

Overname van afstand en Denial-of-Service (DoS)

Als een bedrijf slachtoffer wordt van DoS-aanvallen of van afstand wordt overgenomen, loopt het risico op met aanzienlijke verstoringen van de bedrijfsvoering. Ransomware kan kritieke gegevens gijzelen, terwijl DoS-aanvallen essentiële dienstverlening volledig kunnen lamleggen.

Niet voldoen aan regelgeving

Naarmate er strengere cyberregelgeving wordt geïntroduceerd, moeten eigenaren van zonne-energielocaties proactief maatregelen nemen die ervoor zorgen dat hun systemen aan de regels blijven voldoen. Zo voorkomen ze bij mogelijke inbreuken het risico dat producten moeten worden teruggeroepen of dat ze boetes moeten betalen.

Strengere wet- en regelgeving voor online-beveiliging zijn in de maak voor zonne-energiesystemen

Zonne-energiesystemen zijn deel geworden van de kritieke energie-infrastructuur. Daarmee trekken ze de aandacht van regelgevers. Dat is te zien in een golf van nieuwe wetten en voorschriften.



UL 2941

Specifieke internationale standaard voor de online-beveiliging van slimme omvormers en gedistribueerde energiebronnen (verwacht in 2025).

Cyber Trust Mark

Amerikaans cyberbeveiligingscertificaat met bijbehorend keurmerk (verwacht in 2025).

National Association of Regulatory Utility Commissions (NARUC/ NASEO)

Online-beveiligingsnormen voor elektrische distributiesystemen en gedistribueerde energiebronnen (verwacht in 2025).

IEEE P1547.10

Werkgroep voor gateway-platforms voor gedistribueerde energiebronnen (werk in uitvoering).



UK PSTI

Britse eisen aan productbeveiligings- en telecommunicatie-infrastructuur (2023).



RED 2014/53/EU

Europese richtlijn voor radio-apparatuur.

Cyberweerbaarheidswet

EU-brede wetgeving voor de online-beveiliging van IoT-apparatuur en aangesloten apparaten (verwacht in 2026-2027).

Richtlijn NIS 2

EU-brede richtlijn voor het bereiken van een hoog niveau van cyberbeveiliging in de hele EU (ingangsdatum oktober 2024).

SolarEdge - Toonaangevend in de cyberbeveiliging van zonne-energiesystemen

Als marktleider in de zonne-energiesector, met een wereldwijde voetafdruk van miljoenen IoT-apparaten, verkeert SolarEdge als geen ander in de positie om de cyberbeveiligingsrisico's te herkennen waaraan eigenaren van zonne-energiesystemen worden blootgesteld. Dat geldt evenzeer voor de bedreigingen voor onze energienetwerken.

We hebben een uitgebreide staat van dienst op het gebied van veiligheid voor zonne-energiesystemen. Zo hebben we geholpen bij het opstellen van cruciale veiligheidsnormen in de VS en daarbuiten. We zijn hetzelfde van plan als het gaat om de online-beveiliging van zonne-energiesystemen.



Uw veiligheid is de kern van ons bedrijf

We hebben aanzienlijk geïnvesteerd in het werven van cyberexperts.



We helpen bij het formuleren van internationale regelgeving op het gebied van cyberbeveiliging

SolarEdge neemt actief deel aan diverse technische commissies, zodat onze producten afgestemd blijven op toekomstige regelgeving. Onze apparaten voldoen aan de nieuwste cyberbeveiligingsnormen voor gedistribueerde energiebronnen.



SolarEdge-producten zijn ontwikkeld met cyberbeveiliging als kernprioriteit

We streven ernaar onze klanten voortdurend te beschermen tegen cyberbedreigingen door maatregelen te nemen tijdens elke stap van ons productontwerp, in alle software en hardware van SolarEdge.



Neem een cybervoorsprong

Samenwerken met SolarEdge betekent profiteren van extra bescherming tijdens de gehele levensduur van het systeem. Onze gelaagde beveiligingsaanpak is gericht op databescherming, communicatie en de bedrijfsvoering van inbedrijfstelling tot productie.

Om verbindingen, functionaliteit en klantgegevens veilig te stellen, volgt SolarEdge het principe van Cyber Informed Engineering (CIE). Dat betekent dat onze informatiebeveiliging al in de ontwerpfase wordt ingebouwd. Bovendien passen we onze oplossingen voortdurend aan om zo te blijven voldoen aan steeds strengere eisen en regelgeving.

We geven prioriteit aan de behoeften van de beveiligingsteams van onze klanten door onze producten niet alleen veilig te maken, maar ook om onze gebruikers maximale zichtbaarheid en controle te geven.

Het subnetwerk voor energie is zo gestructureerd dat het veilig kan worden geïntegreerd met de IT- en OT-netwerken in uw organisatie.

Gebruikersgegevens en gegevens over het energieverbruik worden veilig overgedragen en opgeslagen, waardoor maximale gegevensprivacy en bescherming tegen cyberbedreigingen verzekerd zijn.

SolarEdge-omvormers zijn het hart van het zonne-energiesysteem. Net zoals alle andere SolarEdge-apparatuur zijn ze ontworpen om systeembrede cyberaanvallen te voorkomen en te detecteren.



Zichtbaarheid & controle



Netwerk beveiliging



Gegevens beveiliging



Hardware beveiliging

Online-beveiliging is net als veiligheid geen onderhandelbaar thema

Minimaliseer elk cyberrisico door te kiezen voor een samenwerking met SolarEdge. Zo blijft uw organisatie veilig en veerkrachtig tegen steeds veranderende bedreigingen.

About SolarEdge

SolarEdge Technologies is een wereldleider in duurzame energietechnologie. Door techniek van wereldklasse en een focus op innovatie creëert SolarEdge zonne-energieoplossingen voor de consumentenmarkt, zakelijke markt en de nutssector. SolarEdge biedt daarvoor een geoptimaliseerde aanpak voor het opwekken, opslaan, beheren en verbruiken van energie. Het bedrijf ontwikkelt en produceert omvormers en Power Optimizers en biedt daarnaast oplossingen voor energiebeheer, energieoptimalisatie, energieopslag en netwerkdiensten. De DC-geoptimaliseerde technologie van SolarEdge is inmiddels geïnstalleerd in miljoenen woningen in meer dan 140 landen. Meer dan 50% van de Fortune 100-bedrijven hebben SolarEdge-technologie op hun dak. SolarEdge versnelt daarmee de transitie naar duurzame decentrale energienetwerken die overal de productie en het verbruik van energie gaan optimaliseren.