topsector energie

Secura
A BUREAU VERITAS COMPANY

Zonnige dagen, donkere dreigingen.

Waarom de cybersecurity van zonne-installaties ons allemaal aangaat.

Presentatie door Secura & Topsector Energie

SunChain 2 oktober 2024

L'Orient Today Subscribe

Did solar power energy systems explode during Wednesday's attack?

According to the state-run National News Agency, solar energy systems exploded in homes in several areas of Beirut and the south on Wednesday, but the reports remain unconfirmed.

L'Orient Today / Malek Jadah, 19 September 2024 21:30

L'Orient Today

Subscribe

Did solar power energy systems explode during Wednesday's attack?

According to the state-run National News Agency, solar energy systems exploded in homes in several areas of Beirut and the south on Wednesday, but the reports remain unconfirmed.

L'Orient Today / Malek Jadah, 19 September 2024 21:30

Fact check: niet waar

https://www.dw.com/en/fact-check-no-iphones-solar-panels-laptops-exploded-in-lebanon/a-70281061

Maar er is wél iets anders aan de hand…

Voorstellen…

Soe van Dijk

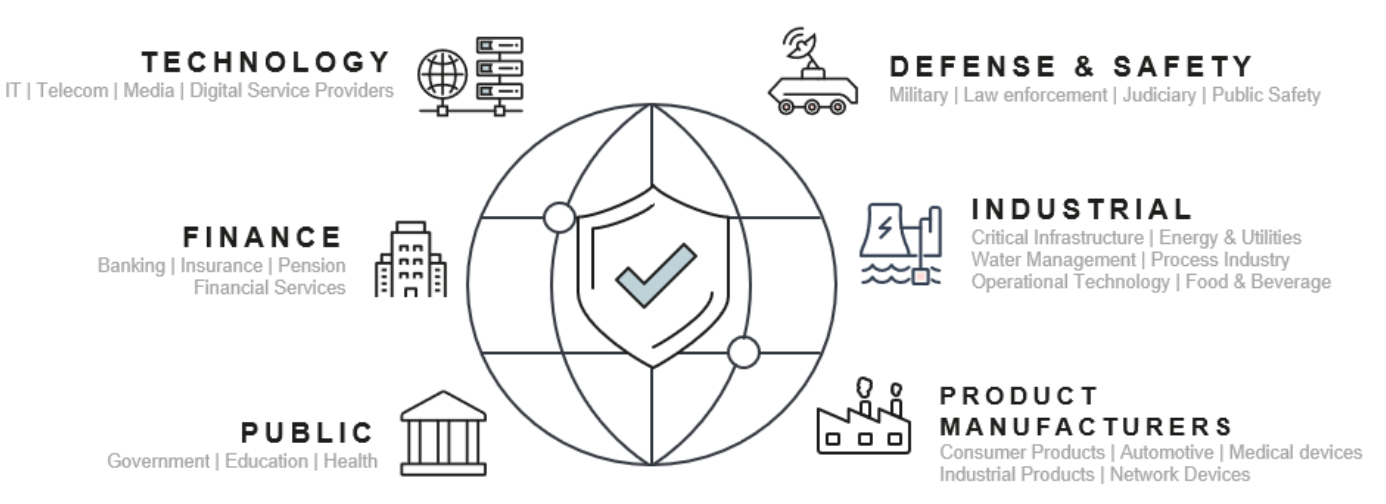
Programmacoördinator Digitalisering
Topsector Energie

Frank Ruedisueli

Principal OT Security Consultant
Secura

Wat doet Secura?

- **Onafhankelijke cybersecurity expert**
  - Gestart in 2000, sinds 2021 onderdeel van Bureau Veritas
  - Richten op mens, proces en techniek
  - Actief op verschillende markten
  - Industrial: Inclusief kritieke sectoren zoals water, olie & gas, manufacturing en (hernieuwbare) energie



Secura
A BUREAU VERITAS COMPANY

RAISING YOUR CYBER RESILIENCE

Wat doet Topsector Energie?

Innovatie voor een duurzame toekomst

- Ontwikkelen kennis & innovatie
- Stimuleren Publiek-Private Samenwerking
- Kennisdeling in de sector

Programma Digitalisering = dwarsdoorsnijdend

- Innoveren met digitale technologieën
- Reflectie op (cyber)veilige energietransitie

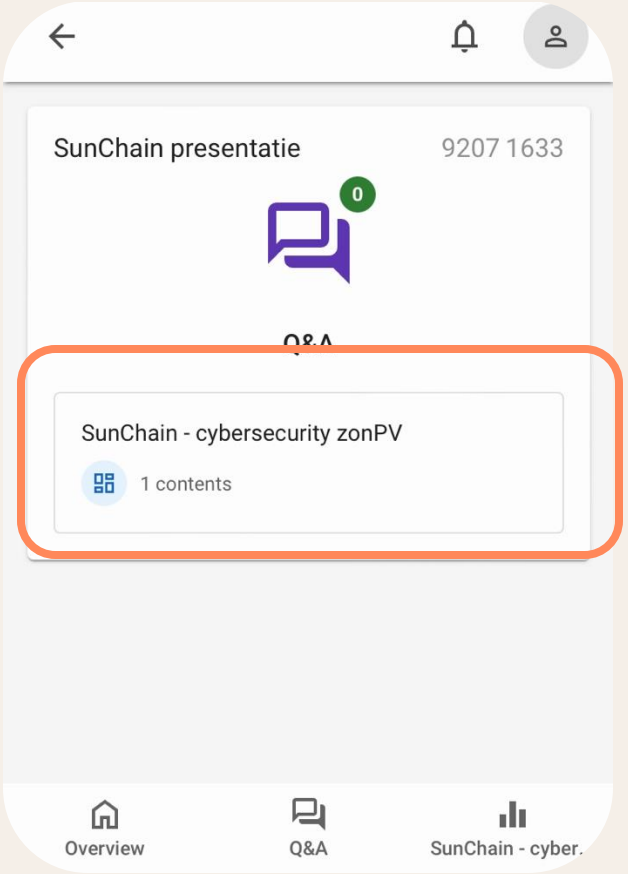
tki offshore energy
topsector energie

tki urban energy
topsector energie

tki energie & industrie
topsector energie

tki nieuw gas
topsector energie

Code 9207 1633



Of ga direct naar
www.partici.fi/92071633

Is het mogelijk dat een cyber security incident in de zonnestroom sector voor grootschalige problemen in Nederland kan leiden?

A. Ja zeker.

C. Misschien.

B. Nee.

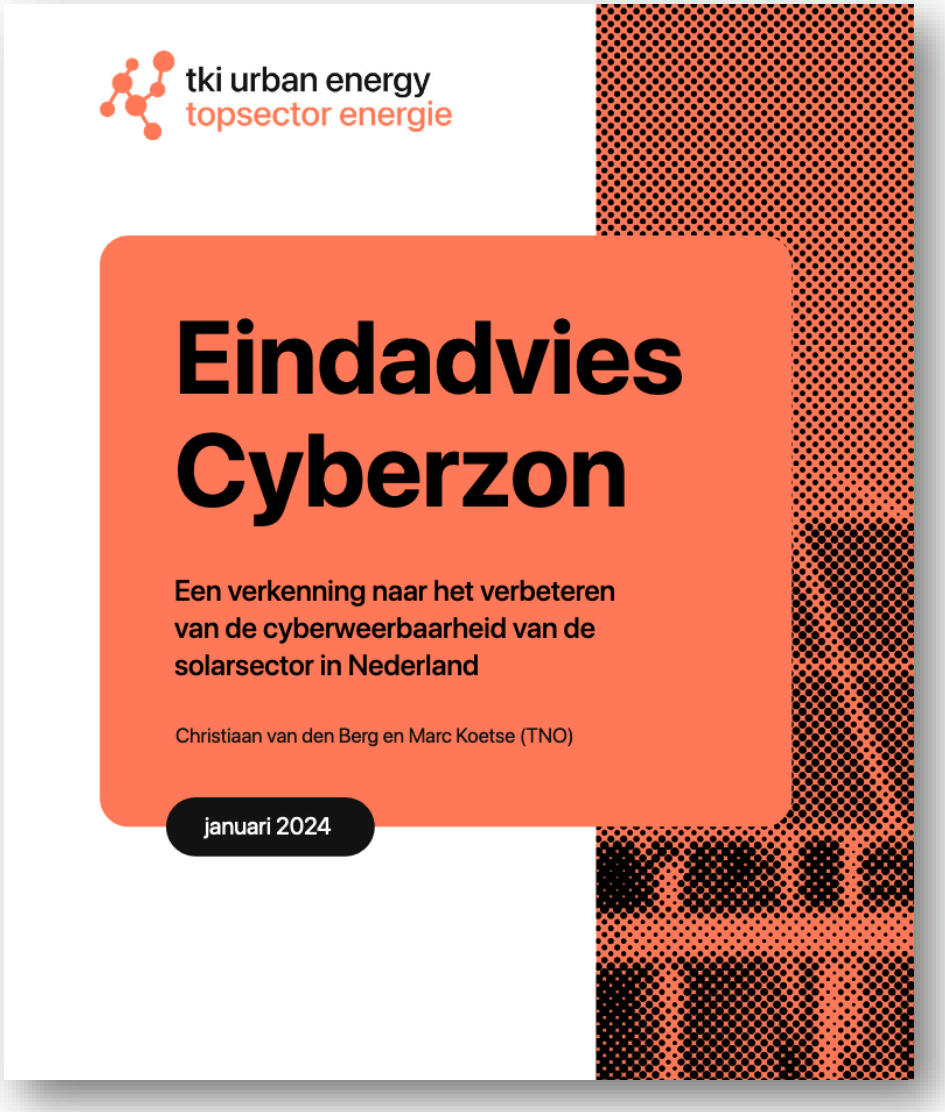
D. Geen idee?

Programma

Kwartiermakersfase (2022-2023)

Enkele bevindingen interviews:

- Het wordt aangenomen dat cyberaanvallen op zonnestroominstallaties verstoringen kunnen veroorzaken in de stroomvoorziening.
- Maar onvoldoende zicht op waar kwetsbaarheden zich precies bevinden.



Onderzoek cybersecurity dreigingen en maatregelen (2024)

- Wie zijn de potentiële aanvallers?
- Wat zijn logische aanvalspaden om de zonne-energiesector middels een cyberaanval te raken?
- Wat zou de impact kunnen zijn?
- Wat zijn mogelijke oplossingen om de kans op of de impact van zo'n aanval te verkleinen?

Onderzoek op 3 schaalniveaus:

Residentieel, Groot op dak en Zonneparken

Onderzoeken Secura en DIVD halen het nieuws (aug ’24)

Deze ethische hackers kunnen met gemak miljoenen zonnepanelen uitschakelen: 'Dan heb je een landelijke black-out'

13-08-2024 09:00 | Veiligheid en recht | Auteur: Cas de Jong

Tech & Innovatie • 20 aug 17:04 • Aangepast op 20 aug 21:55

TenneT wil regels zien voor apps voor zonnepanelen en waarschuwt voor black-outs

Fragment

Zonnepanelen zijn zeer kwetsbaar voor hacks en dat is vooral voor Nederland een probleem

Nederlandse hacker kon 4 miljoen zonnepaneelsystemen in 150 landen overnemen

GERARD JANSSEN

Meer aandacht voor bescherming zonne-installaties tegen cyberaanval noodzakelijk

Nieuw onderzoek schetst scenario’s en maatregelen voor veilige zonnestroom

| TOPSECTOR ENERGIE | 5 MIN | 12 AUGUSTUS 2024 12:22

Cyberaanval

Hoe voorkom je dat zonnepanelen worden gehackt?

Zonne-installaties niet goed beschermd tegen cyberaanval

Hans van der Lugt 12 augustus 2024

Hackers via omvormers van zonnepanelen in netwerken: ’Kans op schade bij kleinverbruikers’

28 augustus 2024

Kamervragen VVD over hacken zonnepanelen, zorgen over risico stroomuitval

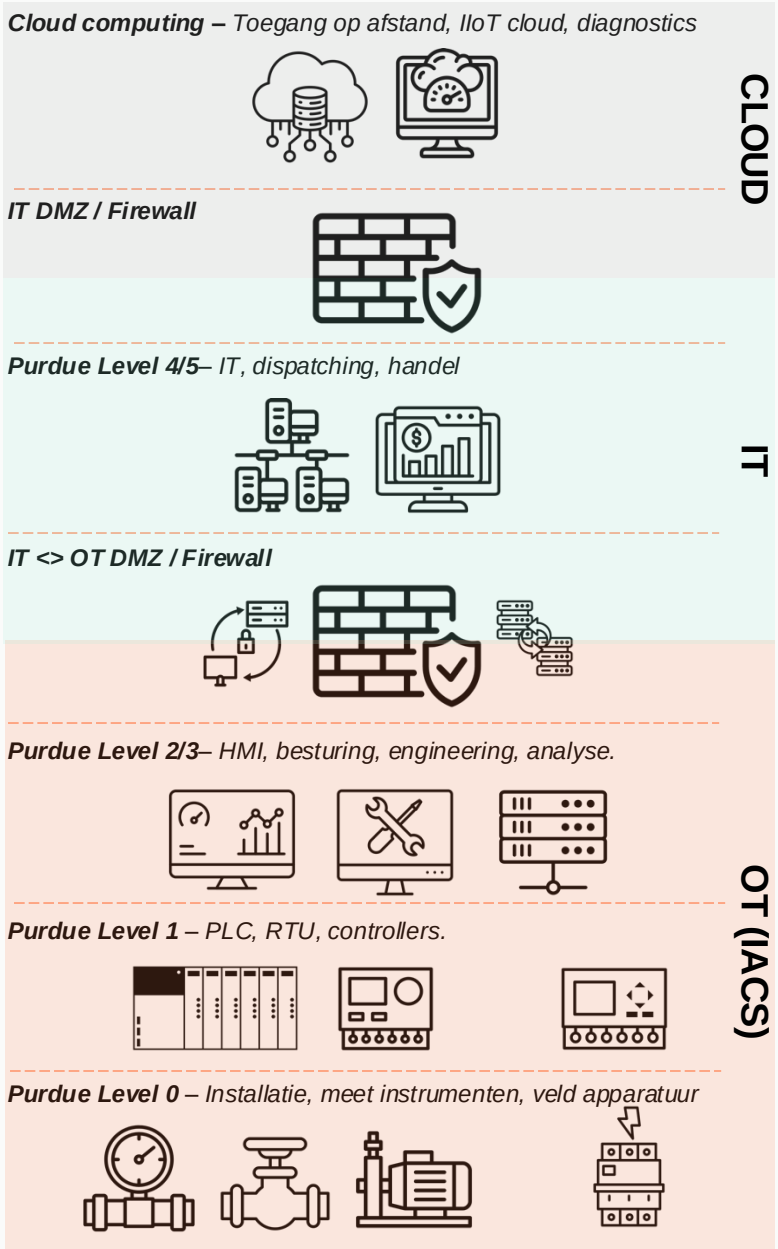
Programma

Eerst een stapje terug….

- Cyber-security ervaringen met “conventionele” bulk energie productie
  - Voornamelijk verbanden van aardgas (biomassa, afval, steenkool)
  - ~ 300 – 500 MW vermogen
  - Aangewezen als Nederlandse kritische infrastructuur (WBNI, NIS1)

- Strikte cyber-security programma’s en netwerkontwerpen.

- Conclusie:
  - Duidelijke splitsing IT en OT.
  - Netwerkscheiding, zonering, beperkte data connecties tussen zones.
  - Toegang op afstand is zeer beperkt
  - Aanpassingen via MoC / Werkvergunning, etc..

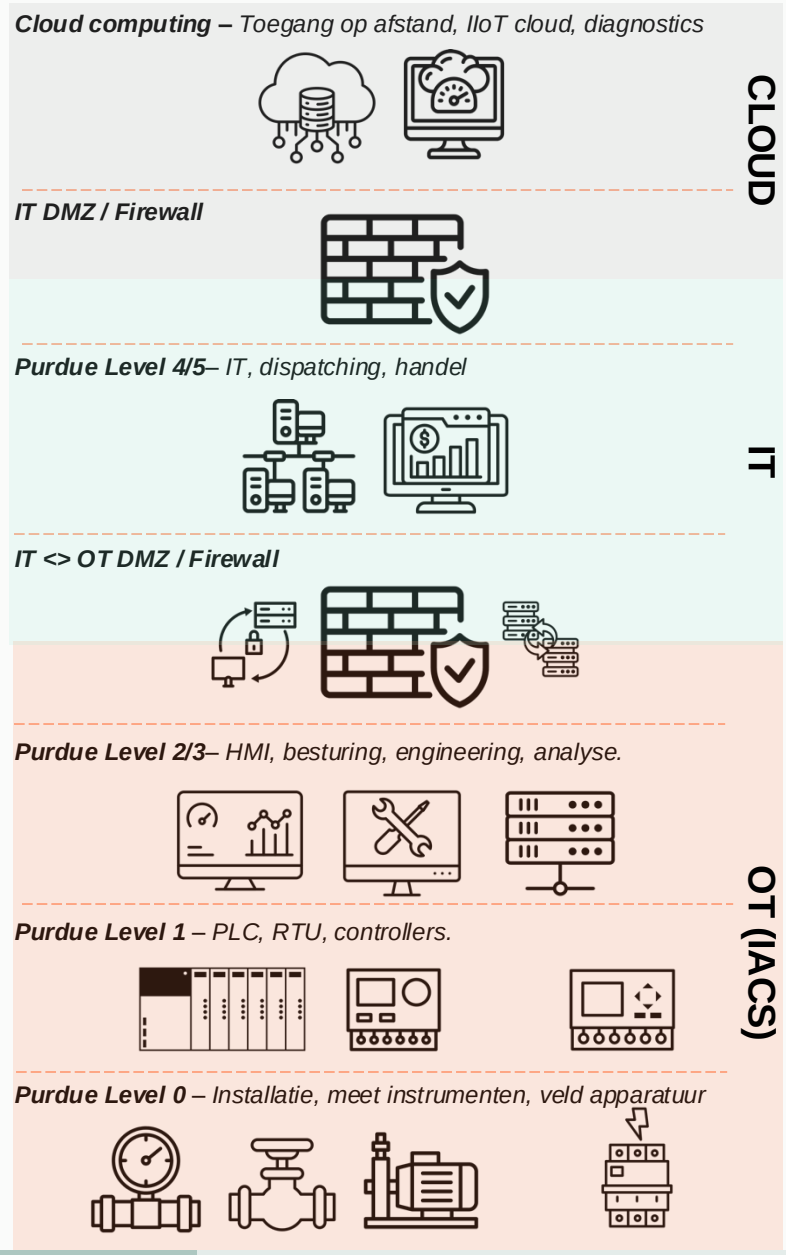


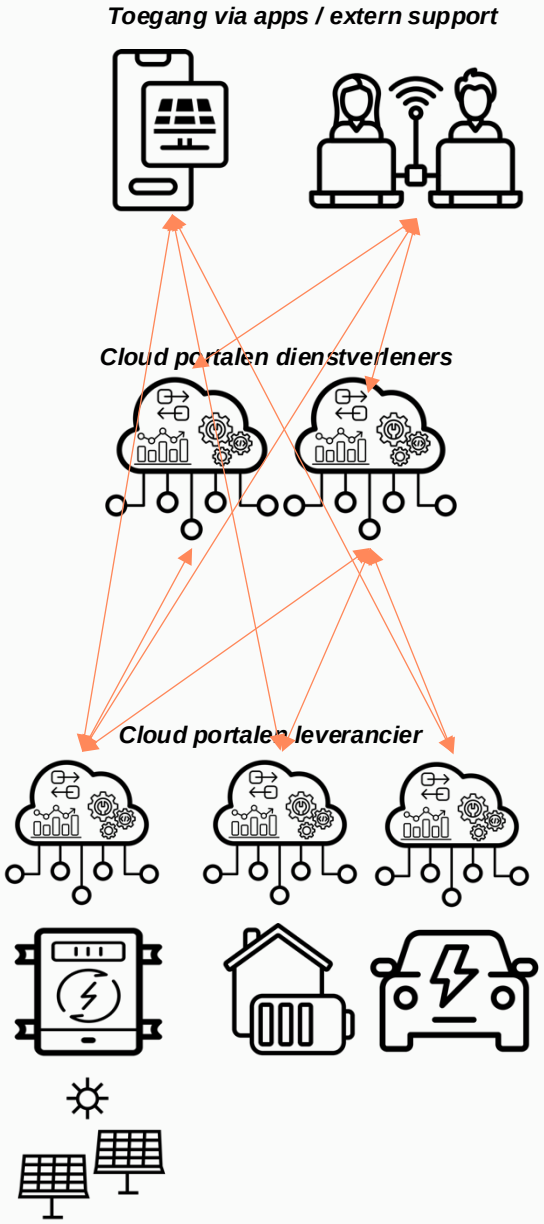
Vergelijking met zonnestroom

- Geldig voor meest particuliere en gebouw gebonden installaties
  - <5kW & 5-15kW per installatie
  - ~3 Miljoen installaties
  - Cumulatief (omvormer) vermogen > 10.000 MW

Conclusie:

- Per installatie weinig tot geen eisen.
- Afhankelijkheden van connecties en cloud portalen.
- Toegang op afstand.



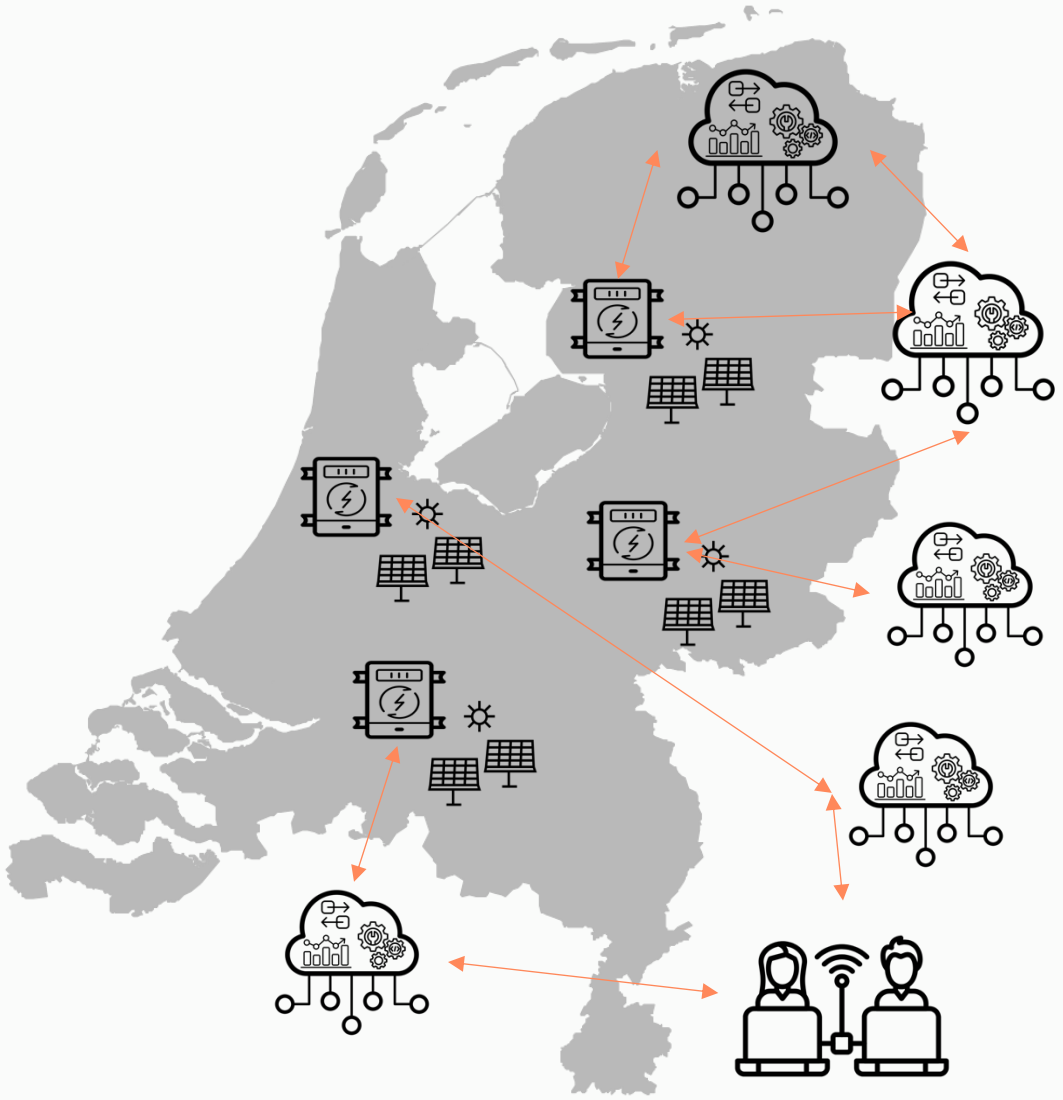


De uitdaging

- Gezamenlijk te beschouwen als “kritieke infrastructuur”
- Cloud portalen & connectiviteit zijn essentieel voor betrouwbare werking.
- Veel portalen, toegang op afstand, analyse van data buiten “eigen beheer”, zelfs buiten landsgrenzen.
- Groei in complexiteit en connectiviteit te verwachten.

Conclusie:

- Cyber-security is een cruciaal onderdeel om deze infrastructuur betrouwbaar te laten werken.
- Complexiteit van het systeem > betrouwbaarheid
- Dit geldt voor alle “lagen” en alle onderdelen van het totale systeem.
  - Van technisch ontwerp omvormer tot aan installateur en van planning tot aan inbedrijfname en onderhoud.



www.partici.fi

Code 9207 1633

Waar zitten de grootste kwetsbaarheden in zonne-installaties volgens jou?

Wat zou de impact kunnen zijn van een cyberaanval op een groot aantal zonne-installaties?

www.partici.fi

Code 9207 1633

A. Misgelopen inkomsten (financiële impact)

C. Kapotte installaties en fysieke schade

B. Regionale of landelijke stroomstoring

D. Anders, namelijk …

Programma

Greep uit het nieuws…

Woningcorporatie Domesta: beveiligingslek Hosola-omvormers, persoonsgegevens mogelijk op straat

Solar Magazine, 16 januari 2017

Onderzoekers 'hacken' 42.000 Nederlandse installaties met zonnepanelen

Solar Magazine, 10 augustus 2022

Ict-lek zonnepanelen mogelijk bedreigend voor Europese stroomvoorziening

Volkskrant, 4 augustus 2017

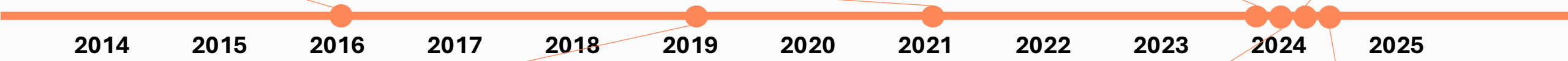
Hacker kon software van zonnepanelen met omvormers Chinese Solarman aanpassen

Hacker kon tienduizenden zonnepanelen saboteren door rondslingerend wachtwoord

RTL Nieuws, 24 juli 2022

> **China kan zijn omvormers gebruiken om aanvallen op het stroomnet uit te voeren**
>
> Paul Stockton, voormalig Amerikaans viceminister van Defensie, juli 2023

Tijdlijn diverse kwetsbaarheden en incidenten



“Horus Scenario” (Door Willem Westerhof)
21 kwetsbaarheden gevonden in omvormers waarmee een volledige aanval mogelijk was.

Master Password Cloud portaal gevonden (DIVD, Jelle Ursem)
Toegang tot beheersysteem van ~ 1M omvormers (40K in NL) met super admin rechten.
Mogelijkheid tot uitschakelen of onklaar maken.

800 Solar Monitors gekaapt
(Japan) Hiermee onderdeel geworden van het Mirai botnet. Misbruik van bekende (maar niet gepatchte) kwetsbaarheid)

Accounts webportalen beschikbaar op het “Dark web” (Secura) Accounts van individuele gebruikers en installateurs. Toegang tot diverse portalen.

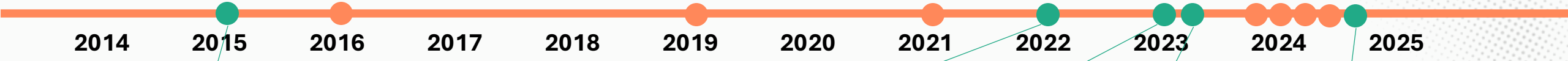
Trickle Down Vulnerabilies (Door Jos Wetzels, Secura)
Zwakheden in communicatie modules gebruikt door meerdere omvormers, hardware supply chain.

RDI, onderzoek omvormers
Belangrijkste conclusie: Geen enkele omvormer voldeed aan de cybersecurity norm.

Kwetsbaarheden in API cloud management systemen. (Bitdefender)
Kwetsbaarheden in API (gebruikt door dataloggers) te misbruiken voor volledige overname van accounts.

Kwetsbaarheden in solar gateways (DIVD, Wietse Boonstra, Hidde Smit)
Combinatie van 6 kwetsbaarheden waardoor controle op afstand mogelijk was.

Tijdlijn overige relevante gebeurtenissen



800.000 Micro omvormers op afstand ge-update.
Hawaii, update door fabrikant (in een dag), om het net te stabiliseren.

LOG4J, software supply-chain incident
Zwakheid in een veel gebruikt software component zorgt ervoor dat talloze applicaties kwetsbaar zijn.

TLStorm, zwakheid in UPS systemen kan leiden tot fysieke schade.
(Armis) Cyber aanval kan leiden tot ontbranden van de componenten in de UPS en fysieke schade van apparaten (en UPS).

600.000 netwerk routers stuk na firmware update
(US) Moedwillige cyber aanval met malafide firmware om apparaten onklaar te maken.

Foutieve software update laat systemen wereldwijd crashen
Automatische update in beveiligingssoftware gaat mis.

Aanval scenario’s

- Duidelijk en aannemelijk dat alle “ingrediënten” aanwezig zijn voor verschillende cyber scenario’s.
  - Inclusief scenario’s met grootschalige impact.

- Belangrijke nuance: **Mogelijk wil niet zeggen dat het makkelijk is!**
  - Veel verschillende factoren zijn relevant:

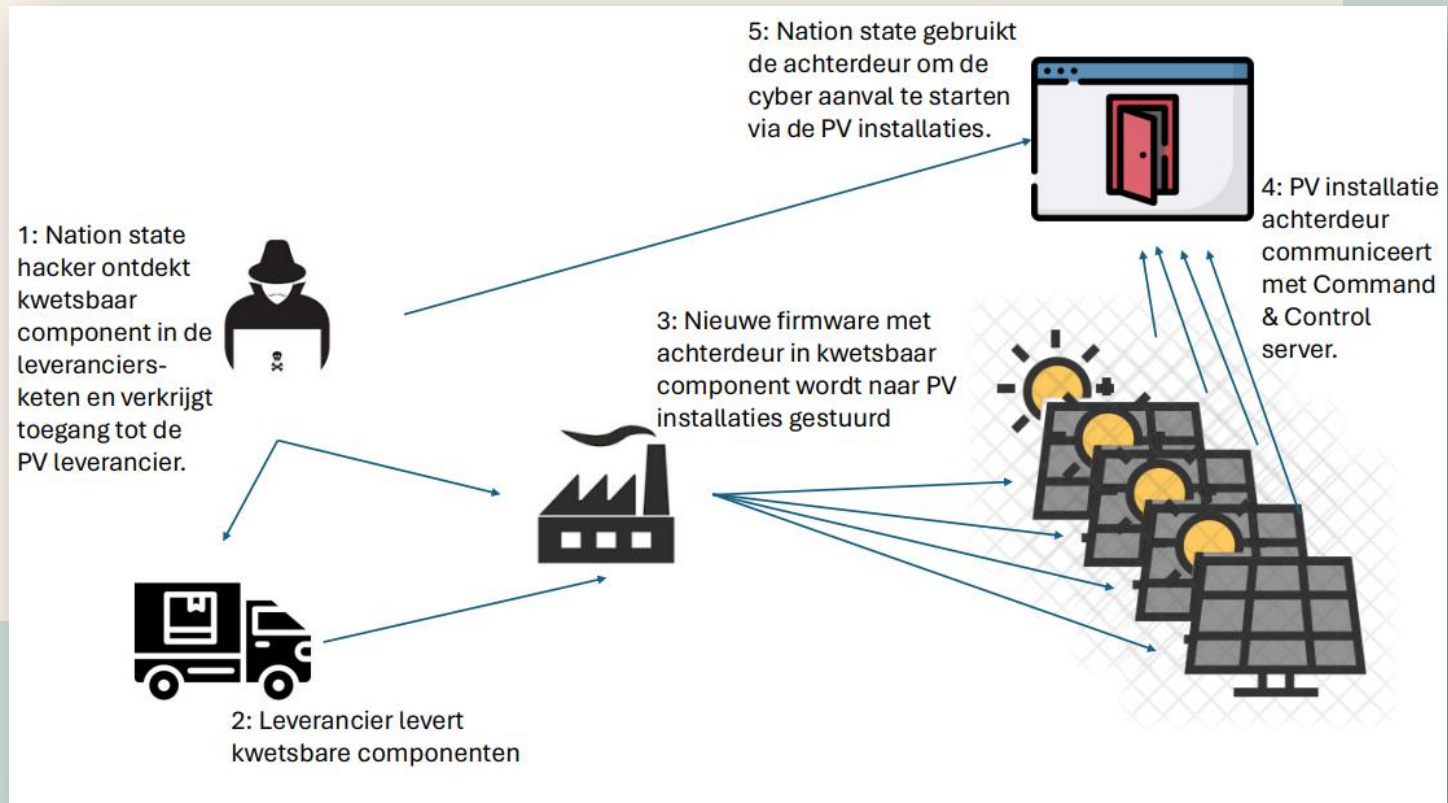
    Divers landschap, benodigde kennis & kunde, technische limieten, motivatie.
  - Tegelijkertijd: Ons belang (afhankelijkheid) wordt ook steeds groter.

- Onderzoeksrapport
  - 27 scenario’s geïdentificeerd, 3 in detail uitgewerkt.
  - (Aanval via webportalen, via firmware of via supply chain)

Voorbeeld scenario – Supply chain aanval (1/2)

1. Aanvaller ontdekt (of introduceert) een kwetsbaarheid in een (software) component.
2. Software modules worden direct of indirect gebruikt in cloud software of omvormer firmware.
3. Uiteindelijk vindt deze aangepaste software (via legitieme updates) zijn weg naar omvormers.
4. Via een achterdeurtje kunnen aanvallers de controle overnemen.
5. Aanvallers kunnen nu op grote schaal omvormers manipuleren (uitzetten, configuratie aanpassen).

IMPACT: Afhankelijk van de schaalgrootte kan dit leiden tot een grootschalige black-out !



Voorbeeld scenario – Supply chain aanval (2/2)

- Benodigde kennis & kunde: APT’s
  - Landen met een offensief cyber-programma. Meerdere mogelijkheden (inclusief omkoping en afpersen insiders
  - Motivatie: Geopolitiek, disruptief van landelijke kritieke infrastructuur. (of verkrijgen van mogelijkheden om hiermee te dreigen)
  - Minder waarschijnlijk voor criminele groeperingen of andere actoren.

- Hoofdoorzaken:
  - Gebrek aan bewustwording van (software) supply chain risico’s.
  - Leverancier: Softwareontwikkeling niet op orde
  - Gebruiker: Geen aandacht voor inkoopeisen, certificering, eigen installatie ontwerp.

Programma

Hoe gaan we de zonnesector meer cyberweerbaar maken?

www.partici.fi

Code 9207 1633

A. Implementatie van cybersecurity wetgeving

C. Samenwerking tussen ketenpartijen

B. Strenger toezicht en handhaving op de sector

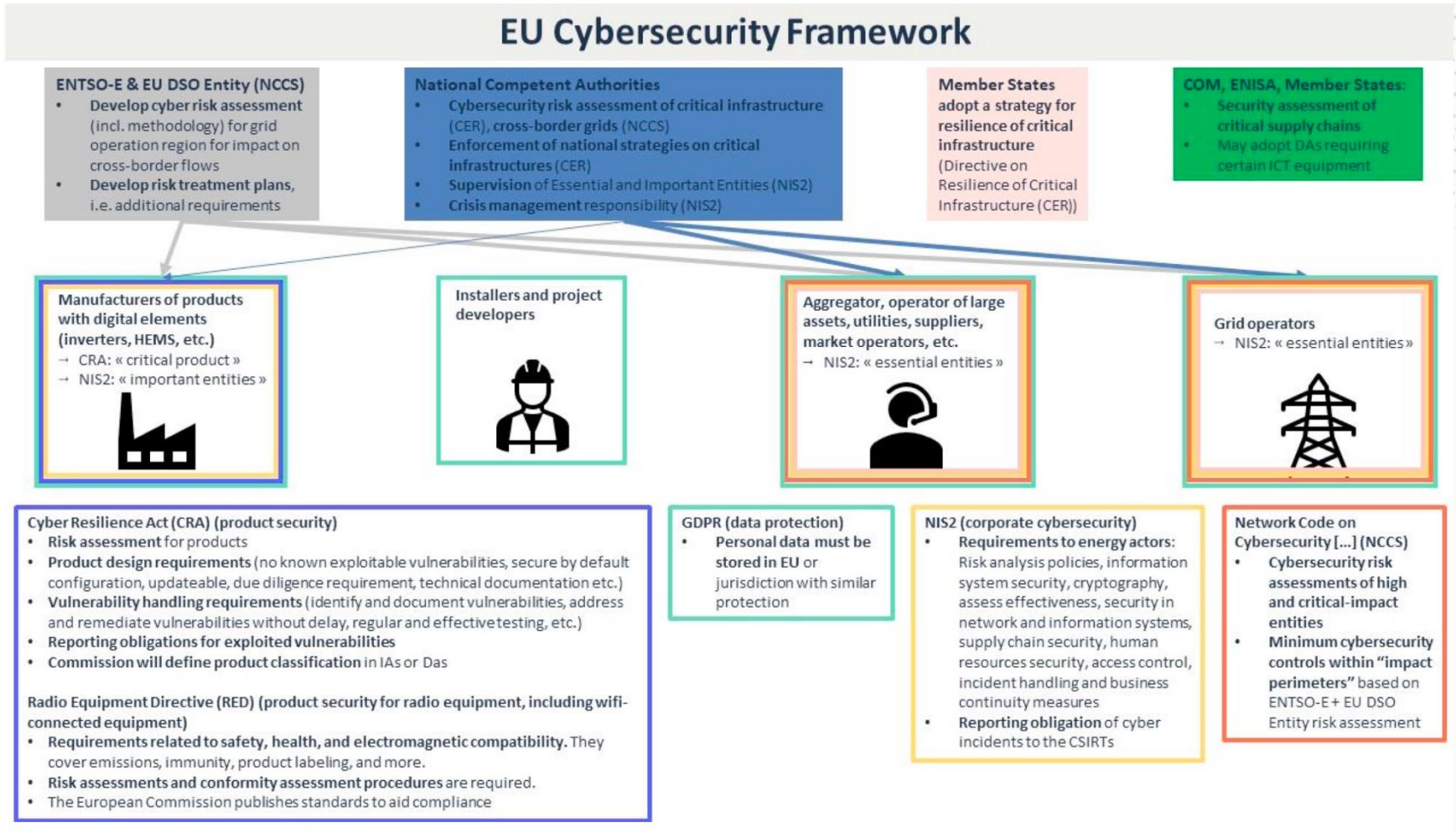
D. Anders, namelijk …

EU werkt aan inhaalslag op cybersecurity wetgeving…

Cyberbeveiligingswet (NIS2)

Securityeisen productniveau:

- **RED 3.3**
- **Cyber Resilience Act**



Maar met wetgeving ben je er niet…

- Toezicht op naleving & handhaving
  - Bedrijven in de energiesector
  - Apparatuur met digitale componenten

- Verplicht certificeringsproces voor producten, diensten en processen
  - Bijv. ETSI EN 303 645 voor consumenten IoT

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

TÜV NORD

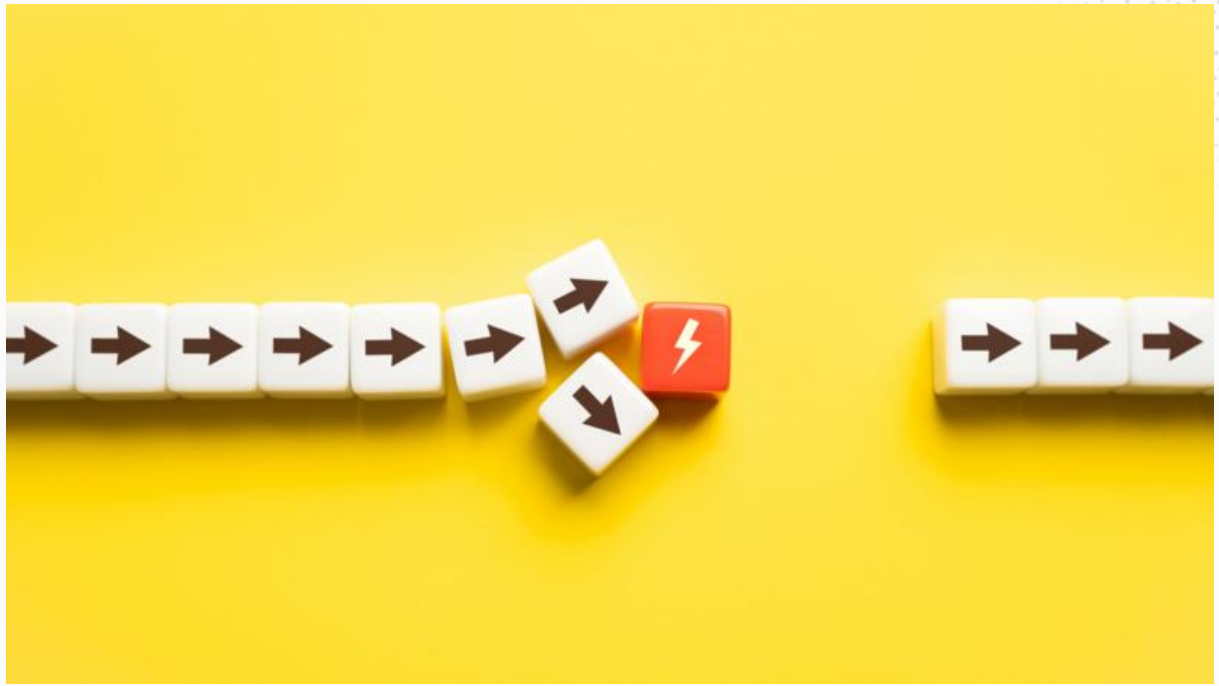
kiwa

Officiële certificeringsorganisaties

& **Securitybedrijven die pentesten uitvoeren**

Bewustwording en samenwerking in de hele keten!

- Projectontwikkelaars en installateurs
- Opdrachtgevers en inkopers (PvE)
- Eigenaren van installaties



Tot slot… geopolitiek kan veranderen

Hoe bereiden we ons nieuwe duurzame en digitale energiesysteem hierop voor?

Met de energietransitie gaan we als het ware over van Russisch gas naar een afhankelijkheid van "Chinese stroom"

Is het mogelijk dat een cyber security incident in de zonnestroom sector voor grootschalige problemen in Nederland kan leiden?

A. Ja zeker.

C. Misschien.

B. Nee.

D. Geen idee?

Bedankt voor jullie aandacht!

Contact

Soe van Dijk
Soe.vandijk@topsectorenergie.nl
www.topsectorenergie.nl/digitalisering

Frank Ruedisueli
frank.ruedisueli@secura.com
https://www.secura.com/

Secura
A BUREAU VERITAS COMPANY

topsector energie