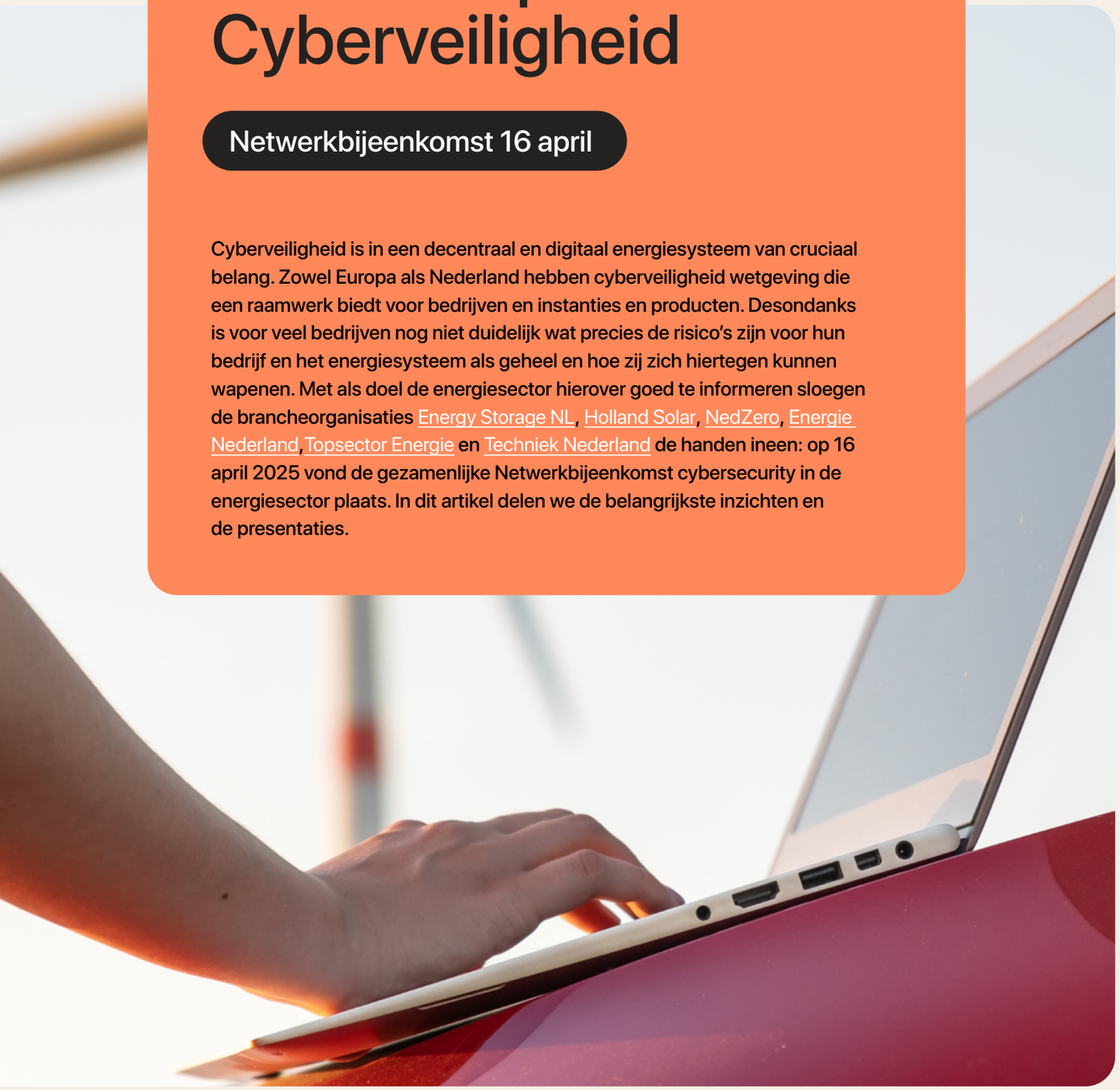
Informatiepakket Cyberveiligheid

Netwerkbijeenkomst 16 april

Cyberveiligheid is in een decentraal en digitaal energiesysteem van cruciaal belang. Zowel Europa als Nederland hebben cyberveiligheid wetgeving die een raamwerk biedt voor bedrijven en instanties en producten. Desondanks is voor veel bedrijven nog niet duidelijk wat precies de risico's zijn voor hun bedrijf en het energiesysteem als geheel en hoe zij zich hiertegen kunnen wapenen. Met als doel de energiesector hierover goed te informeren sloegen de brancheorganisaties Energy Storage NL, Holland Solar, NedZero, Energie Nederland, Topsector Energie en Techniek Nederland de handen ineen: op 16 april 2025 vond de gezamenlijke Netwerkbijeenkomst cybersecurity in de energiesector plaats. In dit artikel delen we de belangrijkste inzichten en de presentaties.



Op woensdag 16 april 2025 vond de netwerkbijeenkomst Cyberveiligheid in de duurzame energiesector plaats bij DENS op de Automotive Campus in Helmond. De bijeenkomst bracht professionals samen om de digitale weerbaarheid van de sector te bespreken en te versterken. De centrale boodschap van de dag: het is niet de vraag óf, maar wanneer een incident plaatsvindt.

Aan de hand van verschillende presentaties en experttafels werden risico's inzichtelijk gemaakt, maar vooral oplossingen gedeeld. Van scenario-oefeningen en ethisch hacken tot *lessons learned* uit de praktijk: de sessies boden concrete handvatten voor actie.

Urgentie van cyberveiligheid in energiesector

De energietransitie leidt tot een toename van digitaal verbonden apparaten en systemen, wat de sector kwetsbaarder maakt voor cyberaanvallen. Tijdens de bijeenkomst benadrukten experts dat het niet de vraag is óf er een cyberincident zal plaatsvinden, maar wanneer. De noodzaak om proactief te handelen en de digitale weerbaarheid te vergroten, stond centraal in de discussies.

Nog stappen te zetten – veel mogelijk

We kijken terug op een waardevolle netwerkbijeenkomst om kennis en ervaringen uit te wisselen over cyberveiligheid. De gedeelde inzichten en aanbevelingen bieden een solide basis voor verdere stappen richting een veerkrachtiger en veiliger energiesysteem. Er gebeurt al ontzettend veel om risico's te voorkomen, maar we hebben als sector zeker nog een stap te zetten. Het goede nieuws: er is veel dat je als ondernemer zelf al kan doen om je eigen weerbaarheid te vergroten.

Hoogtepunten uit het programma

1. Status van de sector en urgentie

Chris van 't Hof van de DIVD gaf een overzicht van de huidige stand van zaken in de sector en de urgentie van cyberveiligheid. Hij deelde inzichten over de kwetsbaarheden binnen de energiesector en benadrukte het belang van samenwerking om deze aan te pakken. Deze presentatie gaf een uniek inkijkje in het perspectief van een ethische hacker.

DIVD-aanpak: Ethisch Hacken en Publieke Veiligheid

De Dutch Institute for Vulnerability Disclosure (DIVD) staat bekend om zijn unieke en ethische benadering van cybersecurity. Hun aanpak draait om **ethisch hacken** als kernprincipe, waarbij drie uitgangspunten centraal staan: **maatschappelijk belang**, **proportionaliteit** en **subsidiariteit**. Met andere woorden: handelen voordat problemen zich voordoen, gepast ingrijpen en alleen als het echt nodig is.

DIVD richt zich op het signaleren van kwetsbaarheden in digitale systemen, zonder daders op te sporen of te vervolgen. Ze zien zichzelf eerder als het **Rode Kruis van het internet**: gericht op hulp, bescherming en het voorkomen van schade, in plaats van bestraffing.

Grootschalige Cyberdreigingen

De noodzaak voor deze aanpak wordt duidelijk uit voorbeelden van massale cyberaanvallen. Een bekend voorbeeld is de **REvil-ransomware-aanval**, waarbij meer dan 1.500 systemen wereldwijd werden geransomed door Revil middels een kwetsbaarheid in Kaseya software en DIVD alle andere kwetsbare organisaties direct ging melden dat ze dat offline moesten halen. Zulke incidenten maken pijnlijk duidelijk hoe kwetsbaar digitale infrastructuren zijn.

Veelvoorkomende zwakke plekken blijven opvallend basaal: **simpele gebruikersnaam-wachtwoordcombinaties** en slecht beveiligde, **openbare databases** vormen nog altijd een groot risico. Zoals **Solarman** zonnepaneelomvormers. Het beheerpaneel was toegankelijk door een gelekt wachtwoord, terwijl vanuit daar de omvormers online te besturen zijn en kwaadwillenden complete stroomnetwerken konden ontregelen—met mogelijk grootschalige black-outs tot gevolg.

"Hacken is niet alleen slopen, maar maken, breken en bespreken."

"Hackers zien dingen anders dan anderen."

Inspirerende uitspraken

De mentaliteit achter de DIVD-aanpak wordt goed verwoord in enkele krachtige quotes. Deze uitspraken benadrukken het creatieve en constructieve karakter van ethisch hacken: het draait niet om destructie, maar om het verbeteren van systemen en het beschermen van de samenleving.

Projecten en Samenwerkingen

DIVD werkt actief aan bewustwording, educatie en preventie. Zo is er het IoT Hacking Lab, een initiatief gericht op educatie, onderzoek en samenwerking rondom Internet of Things-beveiliging. Samenwerkingen spelen hierbij een cruciale rol. Meer hierover en de partners waarmee DIVD samenwerkt is te zien op de website: divd.nl/energie, waar risico's en oplossingen voor de energiewereld worden besproken.

Eén interessant side-project is het ontwikkelen van een eigen radio communicatie netwerk voor als de stroom en het internet uitvallen met behulp van Meshtastic.

DIVD heeft al nieuwe kwetsbaarheden in omvormers en laadpalen gevonden en gepubliceerd. Nu zijn de batterijsystemen, slimme meters en Home Energy Managementsystemen aan de beurt. Er wordt ook samen met The Green Village en Topsector Energie een hack event georganiseerd om deze apparaten te laten hacken door security researchers en studenten.

Cyberellende
Het e-Book

2. Beleidskaders en handhaving

Joepke van der Linden van de Rijksdienst voor Digitale Infrastructuur (RDI) besprak het brede beleid rondom cyberveiligheid en de rol van handhaving, specifiek de ontwikkelingen op het gebied van de RED en haar overgang naar de CRA eind 2027. Daarnaast werd er ingegaan op de bekendheid met en uitvoering van Europese regelgeving binnen de sector, waaronder de AI-act.

Toezicht en Wetgeving rond Digitale Veiligheid

In de snel digitaliserende samenleving is digitale veiligheid geen luxe meer, maar een noodzakelijkheid. De focus ligt steeds meer op samenwerking tussen overheid, bedrijfsleven en experts om een veilig digitaal landschap te creëren. Niet straffen, maar samenwerken is het uitgangspunt – onder het motto: "Voor een veilig verbonden Nederland."

Deze benadering richt zich op drie pijlers: apparatuur, infrastructuur en de algehele digitale weerbaarheid van systemen en organisaties. Daarbij is het uitgangspunt realistisch: 100% veiligheid bestaat niet. Wat wél mogelijk is, is het voorbereiden op verschillende scenario's, zodat schade beperkt blijft en herstel snel kan worden ingezet.

Wet- en Regelgeving: Cyber Resilience Act

Om dit in goede banen te leiden, worden kaders gesteld via Europese wetgeving. Een belangrijk voorbeeld hiervan is de Cyber Resilience Act (CRA). Vooruit lopend is er al de RED 3.3 (d, e, f), waarin veiligheidseisen worden gesteld aan radioapparatuur met een digitale component. De CRA gaat echter verder dan alleen 'security'—het draait om weerbaarheid: de capaciteit om aanvallen te weerstaan, snel te reageren én te herstellen.

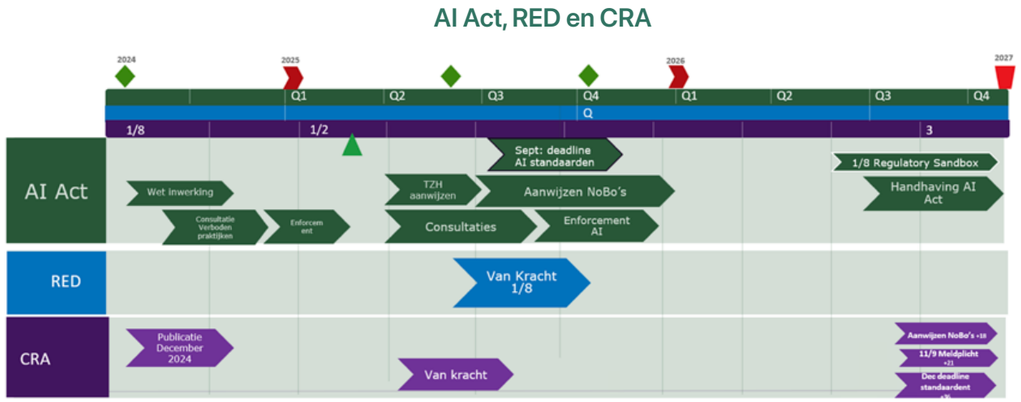
De deadline hiervoor is vastgesteld op 11 december 2027—in de sector ook wel bekend als 'CRA D-Day'. Vanaf die datum moeten alle digitale producten op de markt voldoen aan de gestelde eisen. En ja, dat gaat ver: zelfs chips in consumentenproducten vallen hieronder. Fabrikanten, importeurs en distributeurs krijgen dus een flinke verantwoordelijkheid op hun bord.

RDI & DIVD: Samenwerking in de Praktijk

Een goed voorbeeld van die samenwerking is de relatie tussen de Rijksinspectie Digitale Infrastructuur (RDI) en het Dutch Institute for Vulnerability Disclosure (DIVD). Vanaf 1 augustus kan de RDI formeel actie ondernemen op basis van kwetsbaarheden die door DIVD worden gesignaleerd. Dit betekent dat ontdekte risico's niet langer alleen gemeld worden, maar ook daadwerkelijk kunnen leiden tot handhaving en maatregelen.

Deze nauwe samenwerking versterkt de keten van digitale veiligheid in Nederland: van het opsporen van kwetsbaarheden tot het handhaven van regels. Zo ontstaat een systeem dat niet alleen waarschuwt, maar ook daadwerkelijk beschermt.

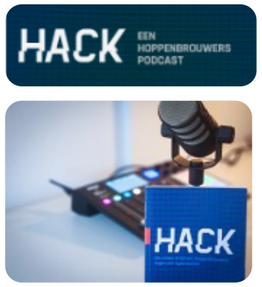
AI Act, RED en CRA



3. Praktijkvoorbeelden en handvatten

Marcel de Boer van Hoppenbrouwers besprak de grote cyberaanval die het bedrijf onderging in 2021 en hoe het herstelproces verliep, een echt gebeurde thriller. De belangrijkste leerpunten hiervan waren het belang van het hebben van een cyberverzekering, de recente investering in nieuwe storage technologie, hulp van de eigen medewerkers en de transparante communicatie richting klanten, pers en stakeholders. Dit zorgde voor een voorspoedig herstelproces en minimalisering van de schade. Meer weten, lees dan het boek of luister de podcast!

Hack
Het eBook



Hack
De podcast

Ervaringsverhaal: Leren van een Grote Cyberaanval

Vier jaar geleden werd Hoppenbrouwers onverwachts getroffen door een zware cyberaanval. Wat begon als een normale werkdag, eindigde in totale digitale chaos. Alle systemen lagen plat, toegang tot bestanden was geblokkeerd, en de schade liep al snel op tot bijna één miljoen euro. De daders hadden de bedrijfsdata gegijzeld en eisten €50.000 losgeld om de toegang te herstellen.

Het incident was niet alleen technisch ingrijpend, maar vooral ook menselijk en organisatorisch. Er was **geen noodplan**, geen draaiboek, geen team dat wist wat te doen. De eerste uren waren dan ook gekenmerkt door **paniek en verwarring**.

De Weg Naar Herstel

Gelukkig was er op papier wél iets geregeld: **een cyberverzekering** via Northwave. Die bleek cruciaal. Binnen korte tijd stond er een gespecialiseerd team klaar dat hielp met coordinatie, forensisch onderzoek en communicatie. Tegelijkertijd werd het eigen personeel direct gemobiliseerd: medewerkers **haalden hardware op**, en systemen gingen letterlijk door de digitale '**wasstraat**' – opgeschoond, gecontroleerd en opnieuw ingericht.

Het was een race tegen de klok. Er werd het hele weekend doorgewerkt. Wat begon als een crisis op vrijdag, was op maandagochtend alweer operationeel. Niet perfect, niet zonder littekens – maar wel weer draaiend.

Wat we hebben geleerd

De aanval heeft diepe sporen achtergelaten, maar ook gezorgd voor waardevolle inzichten en structurele verbeteringen:

- **Open cultuur**: Medewerkers mogen fouten benoemen en bespreken zonder angst voor repercussies. Openheid is cruciaal voor digitale veiligheid.
- **Nieuwe technologie**: Er is geïnvesteerd in moderne, robuuste storage-oplossingen om herhaling te voorkomen.
- **Interne kracht**: Er wordt actief ingezet op de kennis en betrokkenheid van eigen mensen, onder andere voor controles en bewustwording.
- **Transparantie**: Er is bewust gekozen voor open communicatie richting klanten, de pers en andere stakeholders. Verstoppen heeft geen zin; vertrouwen ontstaat door eerlijkheid.
- **Crisisstructuur**: Elk projectteam fungeert nu als een mini-crisisteam, getraind om in noodsituaties snel en zelfstandig te kunnen handelen.

Q&A met Hoppenbrouwers Techniek over cybersecurity

Wat is de belangrijkste maatregel die jullie ná de aanval hebben genomen, die je eigenlijk liever vóóraf al had ingevoerd?
Sinds de aanval hebben we veel aanvullende technische en organisatorische maatregelen genomen. De belangrijkste directe actie was het inrichten van structurele monitoring en bewaking van onze systemen. Achteraf gezien hadden we dat liever al vóór de aanval op orde gehad.

Welk deel van de schade werd door de cybersecurityverzekering gedekt?
De verzekering heeft de volledige schade vergoed, met uitzondering van het eigen risico. Dat heeft ons enorm geholpen in het herstelproces.

Dit verhaal laat zien dat zelfs een zware klap kan leiden tot structurele veerkracht. Niet alleen door technologie of externe hulp, maar vooral door mensen die in actie komen, leren en samen sterker terugkomen.

Hoogtepunten uit het programma

4. Hoe bereid je je voor op een cybercrisis?

Kelvin Rorive van het Cyber Chain Resilience Consortium (CCRC) gaf een aantal handvatten aan de hand van een eerste hulp crisis gids. Creëer bewustwording in de organisatie, train medewerkers, leg cybersecurity niet alleen bij IT maar betrek ook de directie en management en maak cybersecurity onderdeel van het DNA van de organisatie. Een belangrijk inzicht is dat de maatregelen genomen kunnen worden met behulp van het hack motief, e.a. Hacktivisme, spionage, sabotage of bijvoorbeeld criminaliteit.

Is jouw bedrijf digitaal veilig?

Meer en meer bedrijven worden slachtoffer van cyberaanvallen. Ze zijn uit op je klantgegevens, je backup en op je geld.

Neem nu gelijk de eerste stappen via dit platform:

- toegang tot online stappenplan en veiligheids-dashboard
- opleidingsvideo's voor jezelf en je medewerkers
- Energy Storage NL, Techniek Nederland, etc...

CCRC Kennisplatform
www.ccrc.nl/kennisplatform/

Voorbereiden op een Cybercrisis

Volgens Kelvin Rorive van het Cyber Chain Resilience Consortium (CCRC) is het niet de vraag óf je organisatie wordt aangevallen, maar wanneer. Voorbereiding is daarom essentieel. Rorive benadrukt het belang van cyberoefeningen: pas als je weet waar je kwetsbaar bent, kun je gericht actie ondernemen.

Maar weerbaar zijn betekent niet streven naar onhaalbare perfectie. «100% veiligheid bestaat niet,» stelt Rorive. Het draait om balans: risico's in kaart brengen, beheersen waar mogelijk, en snel reageren als het toch misgaat.

Bewustwording als Eerste Verdedigingslinie

Een van de grootste risico's blijft de mens. Uit cijfers blijkt dat slechts 10% van phishing-pogingen correct wordt herkend. Rorive ziet dit als een wake-up call: bewustwording is cruciaal. Technologie helpt, maar uiteindelijk zijn het mensen die klikken – of juist niet.

Aanbevelingen van Rorive

Om organisaties écht weerbaar te maken, doet Rorive een aantal concrete aanbevelingen:

- **Train medewerkers regelmatig**, met aandacht voor phishing, veilige wachtwoorden en algemene digitale hygiëne.
- **Betrek directie en management** bij cybersecurity. Het is geen exclusieve taak van IT, maar een verantwoordelijkheid van de hele organisatie.
- **Beperk toegangsrechten, monitor gedrag** en **herstel kwetsbaarheden snel**. Snelheid is essentieel bij incidenten.
- Maak heldere afspraken met leveranciers over wie waarvoor verantwoordelijk is bij een incident. De keten is zo sterk als de zwakste schakel.
- **Opruimen helpt**: verwijder ongebruikte accounts en gevoelige mails die onnodig lang bewaard blijven. Minder data = minder risico.
- **Veranker cybersecurity in het DNA** van je organisatie. Het moet geen los project zijn, maar een vaste mindset.
- En tot slot: **wet- en regelgeving zijn een goed begin**, maar geen garantie. Voldoen aan regels betekent niet automatisch dat je ook veilig bent.

Rorive's boodschap is duidelijk: echte cyberweerbaarheid vraagt om een cultuurverandering, waarbij techniek, beleid én gedrag samenkomen. Alleen dan kun je als organisatie met vertrouwen de volgende crisis tegemoetzien.

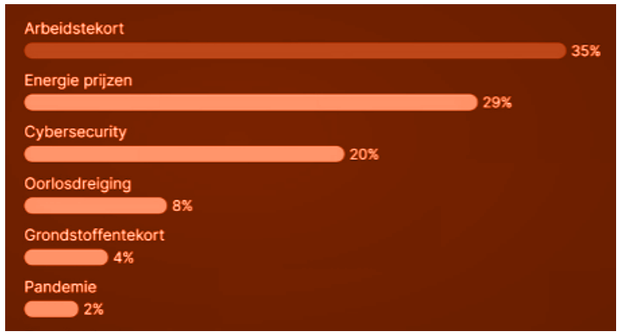
Enquêtes en live votes

Uit een live peiling tijdens het event werd duidelijk dat cybersecurity al wel op de radar staat, maar nog relatief weinig impact wordt gevoeld. 20% van de aanwezigen gaf aan dit onderwerp te zien als meest impactvolle bedreiging voor het eigen bedrijf. Uit een enquete door VNO-NCW bleek dat dit industrie-breed ongeveer 30% is, en dat 73% van de bedrijven de kans op een cyber-incident als groot tot heel groot beschouwt.* Tegelijkertijd gaf slechts 31% van de bedrijven aan hierop maatregelen te hebben getroffen. Er zijn dus nog belangrijke stappen te zetten.

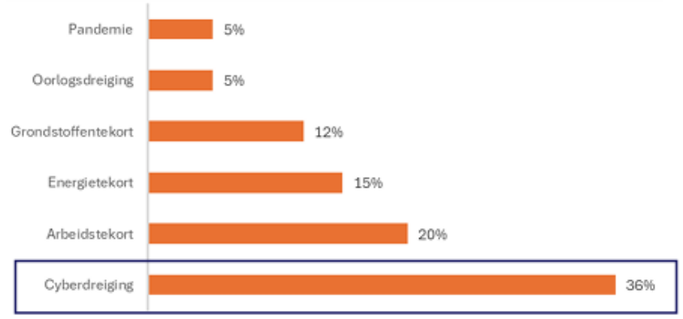
Inzichten van de experttafels

Na de presentaties konden de aanwezigen gezamenlijk lunchen en netwerken en was er gelegenheid om aan te schuiven aan de expert tafels, zoals die van DENS, Techniek Nederland, Digital Trust Center en DIVD met TheGreenVillage, waardevolle inzichten en praktische voorbeelden.

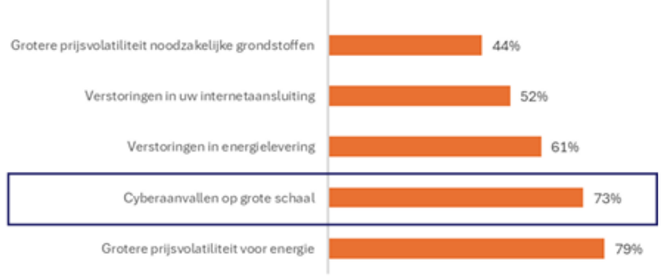
Welke bedreiging heeft de meeste impact op uw bedrijf?



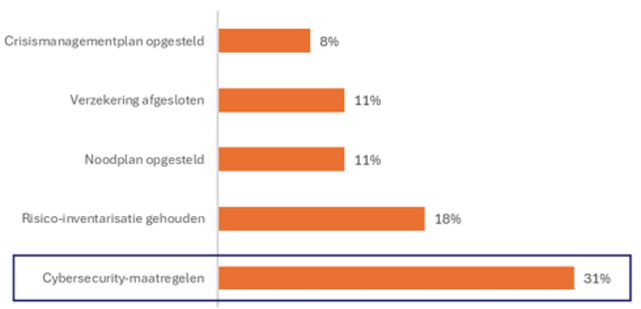
Welke dreiging heeft de meeste impact op uw bedrijf?



Op welke onverwachte gebeurtenis acht u de kans groot tot heel groot?



Welke maatregelen heeft u genomen om uw bedrijf voor te bereiden op onverwachtse gebeurtenissen?



*Over deze enquête: Jaarlijkse enquête van VNO-NCW. 225 mensen hebben de vragenlijst ingevuld, (28%) zakelijke dienstverlening, (20%) industrie, (13%) handel, transport en opslag, (10%) bouw, (9%) IT, (20%) overig.

Starten met cybersecurity?

Begin met deze maatregelen

Het Digital Trust Center (DTC) is een initiatief van het ministerie van Economische Zaken en Klimaat (EZK) en heeft als missie om meer dan 2 miljoen Nederlandse bedrijven – van zzp'ers tot grootbedrijven in de niet-vitale sectoren – weerbaarder te maken tegen toenemende cyber-dreigingen

Doelgroep

De diensten van het DTC richten zich op alle bedrijven in Nederland die niet tot de vitale sectoren behoren. Vitale sectoren (zoals banken, energie en telecom) vallen onder het Nationaal Cyber Security Centrum (NCSC)

Community

Het DTC heeft ook een besloten online community waar ruim 6.000 cybersecurity professionals kennis uitwisselen, samenwerken en elkaar helpen. Ga voor meer informatie naar digitaltrust-community.nl

De gegeven presentaties

Netwerkbijeenkomst Cybersecurity
Het programma

RDI & Toezicht
Rijksinspectie Digitale Infrastructuur, Joepke van der Linden

Hack Hoppenbrouwers
Hoppenbrouwers, Marcel de Boer

Hoe cybercriminelen ons elektriciteitsnet kunnen verstoren (en wij helpen dat te voorkomen)
DIVD, Chris van 't Hof

Praktijk handvatten om te starten met cyberveiligheid
Cyber Chain Resilience Consortium (CCRC), Kelvin Rorive

Colofon

Informatiepakket Cyberveiligheid
Netwerkbijeenkomst april 2025

Uitgave:
Topsector Energie – Programma Digitalisering

In samenwerking met:
- Energy Storage NL
- Holland Solar
- NedZero
- Energie Nederland
- Techniek Nederland

Redactie en samenstelling:
Energy Storage NL

Vormgeving en productie:
Vrije Stijl

Locatie netwerkbijeenkomst:
DENS, Automotive Campus, Helmond, 16 april 2025

Met dank aan:
- Rijksinspectie Digitale Infrastructuur (RDI)
- Dutch Institute for Vulnerability Disclosure (DIVD)
- Cyber Chain Resilience Consortium (CCRC)
- Hoppenbrouwers Techniek
- Digital Trust Center (DTC)
- DENS

Versie:
Mei 2025