
Techniek
Nederland

Samen digitaal webinar 12 november, welkom!

“Cybersecurity en dataveiligheid”

MEDEDELINGEN

- Camera’s en microfoons zijn uitgeschakeld
- Er wordt een aantal poll vragen gesteld
- **Vragen** graag stellen via de chat

- Moderator zal reageren of na de sessie volgt antwoord

- Presentatie beschikbaar via website Techniek NL
- Webinar wordt opgenomen
- Terug te kijken op Techniek Nederland YouTube

Programma

16.00 uur welkom deelnemers en introductie

16.10 uur BORIS netwerk

- Cybersecurity, wat is de urgentie?
- Welke impact heeft het op de installateur?

16.15 uur Techniek Nederland

- De 5 basisprincipes voor dataveiligheid
- Help ik ben gehacht
- Platform Samen Digitaal Veilig en NIS2
- NIS2 Quality Mark

16.45 uur Techniek Nederland

- Cybersecurity OT

- **17.00 uur** afronding

12-11-2024

Introductie

Cybersecurity en dataveiligheid

Marius Hakkesteegt
Boris Netwerk

Bart Molmans
Techniek Nederland

John van de Vugt
Techniek Nederland

POLL (1)

1. Met hoeveel deelnemers kijk je vanaf 1 scherm?

Samen Digitaal
Techniek Nederland en BORIS netwerk

Krachten & ideeën bundelen met digitaliseren

- Gebruik maken van elkaars…
  - → **Kennis** van processen, certificeringen, applicaties
  - → **Oplossingen**, zoals formulieren
  - → **Praktijkervaringen**
  - → **Expertise** die we niet allemaal in huis hebben

- Van installateurs voor installateurs
- Digitaliseren kun je niet alleen
- Vanuit de praktijk ontwikkeld

12-11-2024

Politie getroffen door datalek: namen alle medewerkers buitgemaakt

vrijdag 27 september 2024, 15:28 door **Redactie**, 57 **reacties**

De politie **waarschuwt** personeel voor een datalek nadat er is ingebroken op een politieaccount. "Hierbij zijn werkgerelateerde contactgegevens van politiemedewerkers buitgemaakt. Behalve de namen van collega's, gaat het verder niet om privégegevens of onderzoeksgegevens", aldus een verklaring van de politie. De politie is inmiddels zelf een onderzoek gestart. Tevens zijn medewerkers gevraagd extra alert te zijn op phishingmails of verdachte berichten en telefoontjes.

Minister Van Weel van Justitie en Veiligheid laat in een **brief** aan de Tweede Kamer weten dat werkgerelateerde contactgegevens van alle politiemedewerkers zijn buitgemaakt. "Behalve de namen van politiemedewerkers, gaat het verder niet om privégegevens of onderzoeksgegevens. Momenteel wordt door de politie onderzoek gedaan naar de oorzaak en de impact van het incident. De politie heeft melding gemaakt van het lek bij de Autoriteit Persoonsgegevens", aldus de bewindsman, die geen verdere details over het datalek heeft. De politie heeft inmiddels politiemedewerkers op de hoogte gesteld van het incident.

- Politie start meldpunt voor agenten met vragen over datalek
- Beveiligingslek in VLC media player kan aanvaller code laten uitvoeren

ABN Amro lanceert 'Gesprek Check' tegen bankhelpdeskfraude

dinsdag 1 oktober 2024, 10:28 door **Redactie**, 16 **reacties**

ABN Amro heeft voor gebruikers van de bank-app een nieuw feature **toegevoegd** die moet helpen tegen bankhelpdeskfraude. Via '**Gesprek Check**' kunnen klanten via de bank-app zien of ze echt een medewerker van de bank aan de lijn hebben. ABN Amro omschrijft het als een 'extra veiligheidshulpmiddel'.

"Oplichtingspraktijken zoals (bank)helpdeskfraude, waarbij een crimineel zich voordoet als bankmedewerker, worden vaak niet herkend. Uit recent onderzoek van Ipsos I&O in opdracht van ABN Amro blijkt dat ruim een kwart van de Nederlanders niet volledig op de hoogte is van wat een bank nooit aan haar klanten vraagt", zo laat de bank verder weten. Als een klant twijfelt of het echt ABN Amro aan de telefoon is, kan die om een Gesprek Check vragen. De bankmedewerker stuurt dan een (pop-up) bericht in de app en in Internet Bankieren om het gesprek te bevestigen.

"Een adviseur van ABN Amro die met een particuliere klant belt, plaatst op dat moment een bericht in Internet Bankieren of in de ABN Amro-app van de klant. Via die twee kanalen kunnen klanten vervolgens een pop-up zien met de bevestiging dat ze inderdaad met iemand van de bank spreken", zegt Jorissa Neutelings van ABN Amro. "Het voorziet echt in een belangrijke behoefte."

E-mailaccounts gemeente Den Haag gebruikt voor versturen phishingmails

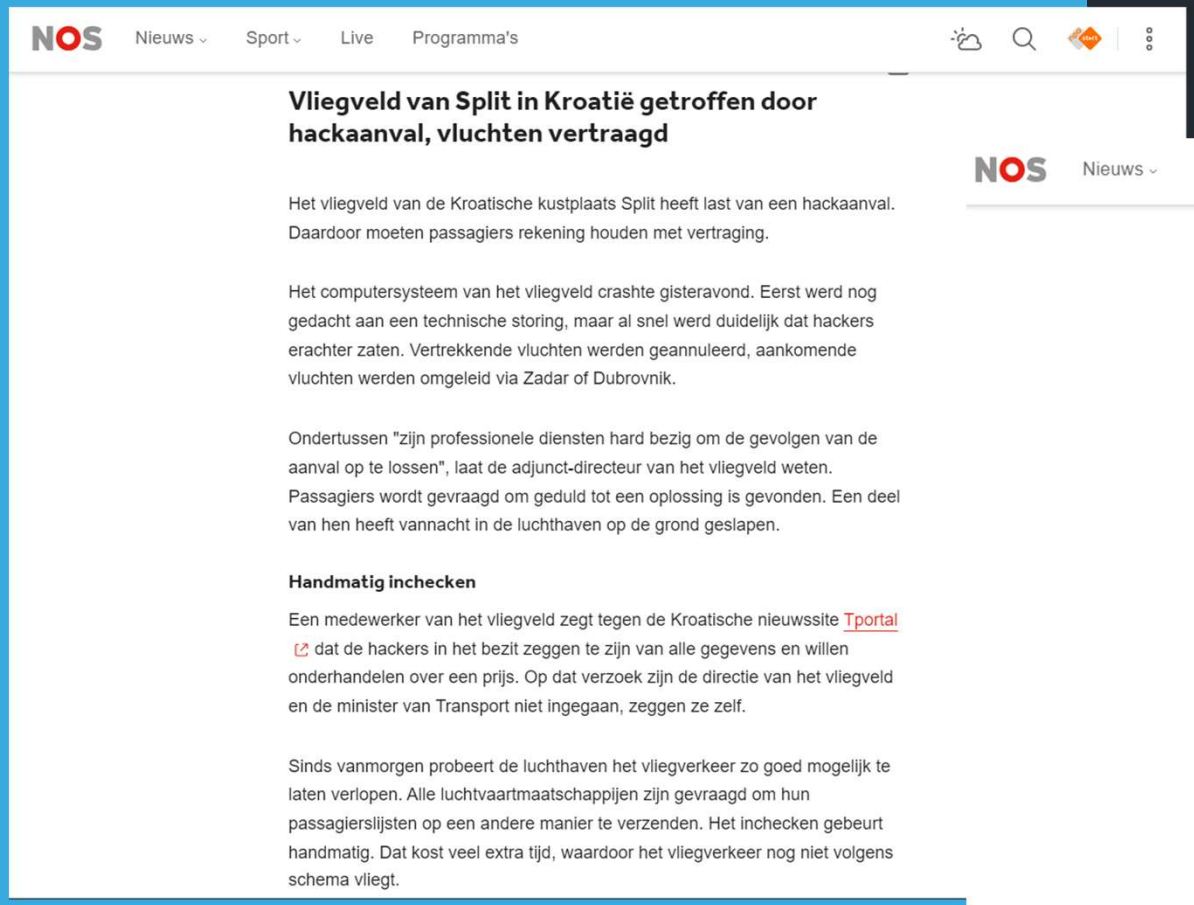
woensdag 2 oktober 2024, 09:26 door **Redactie**, 2 **reacties**

Verschillende e-mailaccounts van de gemeente Den Haag zijn gebruikt voor het versturen van phishingmails, zo heeft de gemeente zelf bekendgemaakt. De malafide berichten, met onderwerpen als 'Payment of Necessary document', waren gericht aan inwoners, organisaties en medewerkers van de gemeente. **Volgens** de gemeente leken de verstuurde phishingmails vaak betrouwbaar, omdat ze afkomstig waren van e-mailadressen van de gemeente en soms zelfs dossiernummers bevatten.

De gemeente adviseert iedereen die op 25 september een e-mail heeft ontvangen afkomstig van een e-mailadres dat eindigt op @denhaag.nl om goed te controleren of het geen phishingmail is. "Verwijder een verdachte e-mail onmiddellijk en klik niet op de links. Het doel van de mails is inloggegevens verkrijgen. Als de ontvanger op de link klikt, komt diegene op een nagemaakte pagina van de gemeente waar deze persoon wordt gevraagd om in te loggen. Doe dit niet", zo laat het advies verder weten.

Het detectiesysteem van de gemeente detecteerde vorige week een ongebruikelijke hoeveelheid verstuurde e-mails. Daarna bleek dat het om phishingmails ging. "Helaas waren veel e-mails toen al verstuurd. De gemeente ondernam direct actie door de getroffen mailaccounts te beveiligen. Zo werd voorkomen dat er meer e-mails werden verzonden", aldus de gemeente. Hoe de e-mailaccounts konden worden gecompromitteerd en of er tweefactorauthenticatie werd gebruikt staat niet in de verklaring vermeld. Security.NL heeft de gemeente vragen gesteld.

- Rackspace waarschuwt klanten voor inbraak op eigen monitoringplatform
- OM eist taakstraf tegen agent voor onbevoegd opvragen van informatie



Vliegveld van Split in Kroatië getroffen door hackaanval, vluchten vertraagd

Het vliegveld van de Kroatische kustplaats Split heeft last van een hackaanval. Daardoor moeten passagiers rekening houden met vertraging.

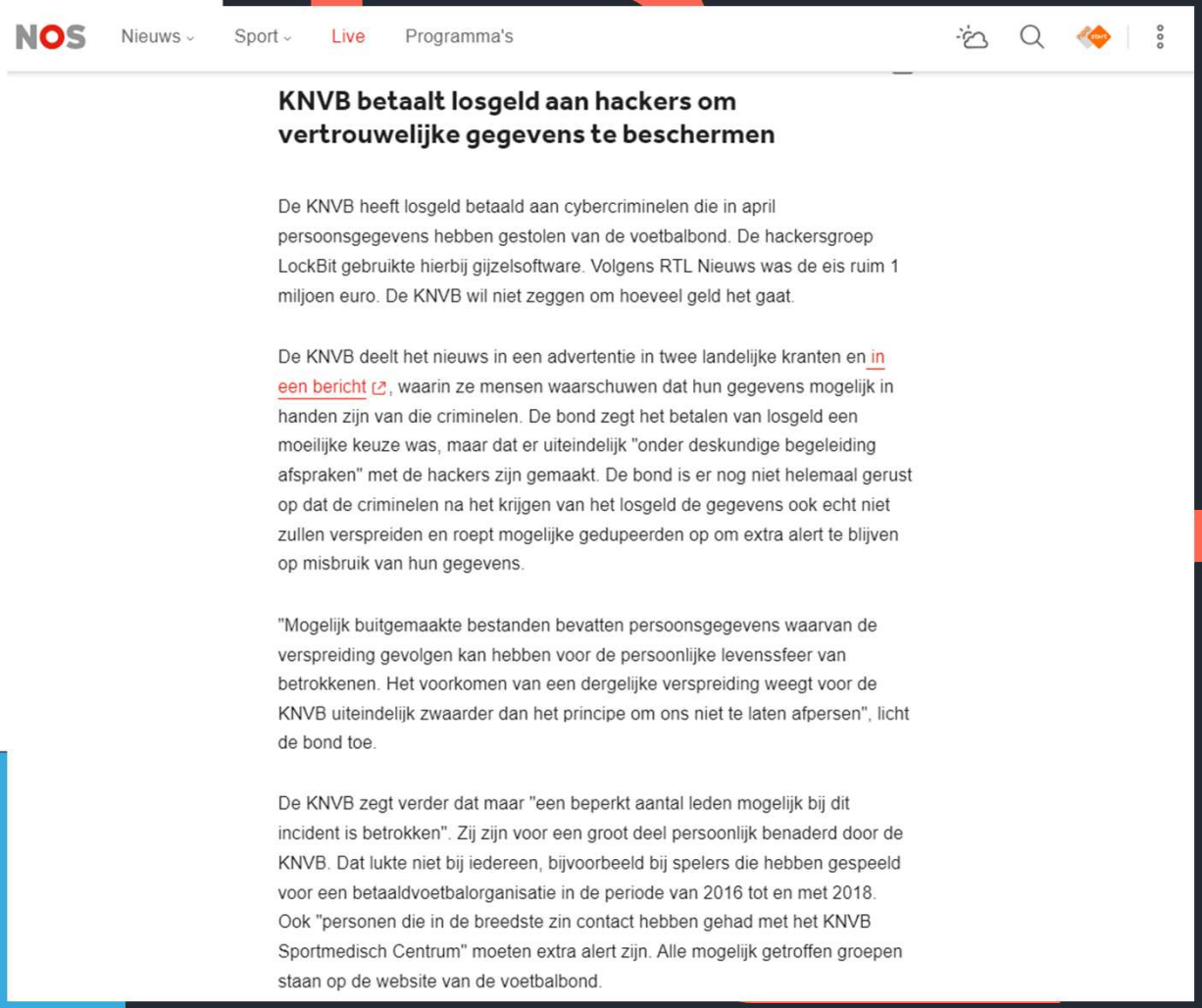
Het computersysteem van het vliegveld crashte gisteravond. Eerst werd nog gedacht aan een technische storing, maar al snel werd duidelijk dat hackers erachter zaten. Vertrekkende vluchten werden geannuleerd, aankomende vluchten werden omgeleid via Zadar of Dubrovnik.

Ondertussen "zijn professionele diensten hard bezig om de gevolgen van de aanval op te lossen", laat de adjunct-directeur van het vliegveld weten. Passagiers wordt gevraagd om geduld tot een oplossing is gevonden. Een deel van hen heeft vannacht in de luchthaven op de grond geslapen.

Handmatig inchecken

Een medewerker van het vliegveld zegt tegen de Kroatische nieuwssite Tportal dat de hackers in het bezit zeggen te zijn van alle gegevens en willen onderhandelen over een prijs. Op dat verzoek zijn de directie van het vliegveld en de minister van Transport niet ingegaan, zeggen ze zelf.

Sinds vanmorgen probeert de luchthaven het vliegverkeer zo goed mogelijk te laten verlopen. Alle luchtvaartmaatschappijen zijn gevraagd om hun passagierslijsten op een andere manier te verzenden. Het inchecken gebeurt handmatig. Dat kost veel extra tijd, waardoor het vliegverkeer nog niet volgens schema vliegt.



KNVB betaalt losgeld aan hackers om vertrouwelijke gegevens te beschermen

De KNVB heeft losgeld betaald aan cybercriminelen die in april persoonsgegevens hebben gestolen van de voetbalbond. De hackersgroep LockBit gebruikte hierbij gijzelsoftware. Volgens RTL Nieuws was de eis ruim 1 miljoen euro. De KNVB wil niet zeggen om hoeveel geld het gaat.

De KNVB deelt het nieuws in een advertentie in twee landelijke kranten en in een bericht, waarin ze mensen waarschuwen dat hun gegevens mogelijk in handen zijn van die criminelen. De bond zegt het betalen van losgeld een moeilijke keuze was, maar dat er uiteindelijk "onder deskundige begeleiding afspraken" met de hackers zijn gemaakt. De bond is er nog niet helemaal gerust op dat de criminelen na het krijgen van het losgeld de gegevens ook echt niet zullen verspreiden en roept mogelijke gedupeerden op om extra alert te blijven op misbruik van hun gegevens.

"Mogelijk buitgemaakte bestanden bevatten persoonsgegevens waarvan de verspreiding gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen. Het voorkomen van een dergelijke verspreiding weegt voor de KNVB uiteindelijk zwaarder dan het principe om ons niet te laten afpersen", licht de bond toe.

De KNVB zegt verder dat maar "een beperkt aantal leden mogelijk bij dit incident is betrokken". Zij zijn voor een groot deel persoonlijk benaderd door de KNVB. Dat lukte niet bij iedereen, bijvoorbeeld bij spelers die hebben gespeeld voor een betaaldvoetbalorganisatie in de periode van 2016 tot en met 2018. Ook "personen die in de breedste zin contact hebben gehad met het KNVB Sportmedisch Centrum" moeten extra alert zijn. Alle mogelijk getroffen groepen staan op de website van de voetbalbond.

Cybercrime & AI

NIEUWS

Eén op de vijf klikt op links in AI-gegenereerde phishingmails

APRIL 24, 2023 REDACTIE

Cybersecurity-experts van SoSafe waarschuwen dat AI betere phishing-mails kan schrijven dan mensen. Onderzoek van SoSafe toont aan dat deze dreiging inmiddels de realiteit is. Uit de resultaten blijkt dat AI-gegenereerde phishing-mails door 78 procent van de mensen geopend wordt en dat 21 procent op schadelijke links in de mails klikt.

Daarnaast werd zelfs 65 procent van de ontvangers van de met kunstmatige intelligentie (AI) gegenereerde mails verleid tot het invoeren van persoonlijke gegevens op invulvelden van de gelinkte websites. Door mensen opgestelde phishing-mails worden door eenzelfde percentage geopend. En hoewel de clickrate bij handmatige phishing iets hoger ligt (27 procent), is er bij deze mails minder interactie (60 procent) in de vorm van het geven van aanvullende (persoonlijke) gegevens. Deze cijfers laten zien dat mensen door AI-gegenereerde phishing-mails niet kunnen onderscheiden van handmatige phishingaanvallen.

Nog gevaarlijker

Dr. Niklas Hellemann, CEO en mede-oprichter van SoSafe: "De resultaten zijn opvallend omdat we de mails hebben opgesteld met het ChatGPT-3.5 model, met algemene thema's en onderwerpen. Zelfs met deze basis AI-gegenereerde phishing-sjablonen blijkt uit onze gegevens dat mensen moeite hebben met het herkennen van AI-gegenereerde phishing-aanvallen. Naarmate de technologie vordert met geavanceerdere modellen zoals Chat GPT-4 en geschaalde personalisatie, verwachten we dat aanvallen nog gevaarlijker worden, want het grootste gevaar schuilt in de potentiële schaalgrootte."

Evil-GPT is the latest malicious AI chatbot to hit the darknet

More often than not, if a tool can be used for good, it can also be used for evil. After all, tools are largely neutral – it's what people do with them that sets the moral level.

David Hollingworth • Fri, 11 Aug 2023 • TECH SHARE

So it's unsurprising that hackers are turning to creating their own generative artificial intelligence engines, designed from the ground up to cause mischief and create malicious code or the writing of phishing emails.

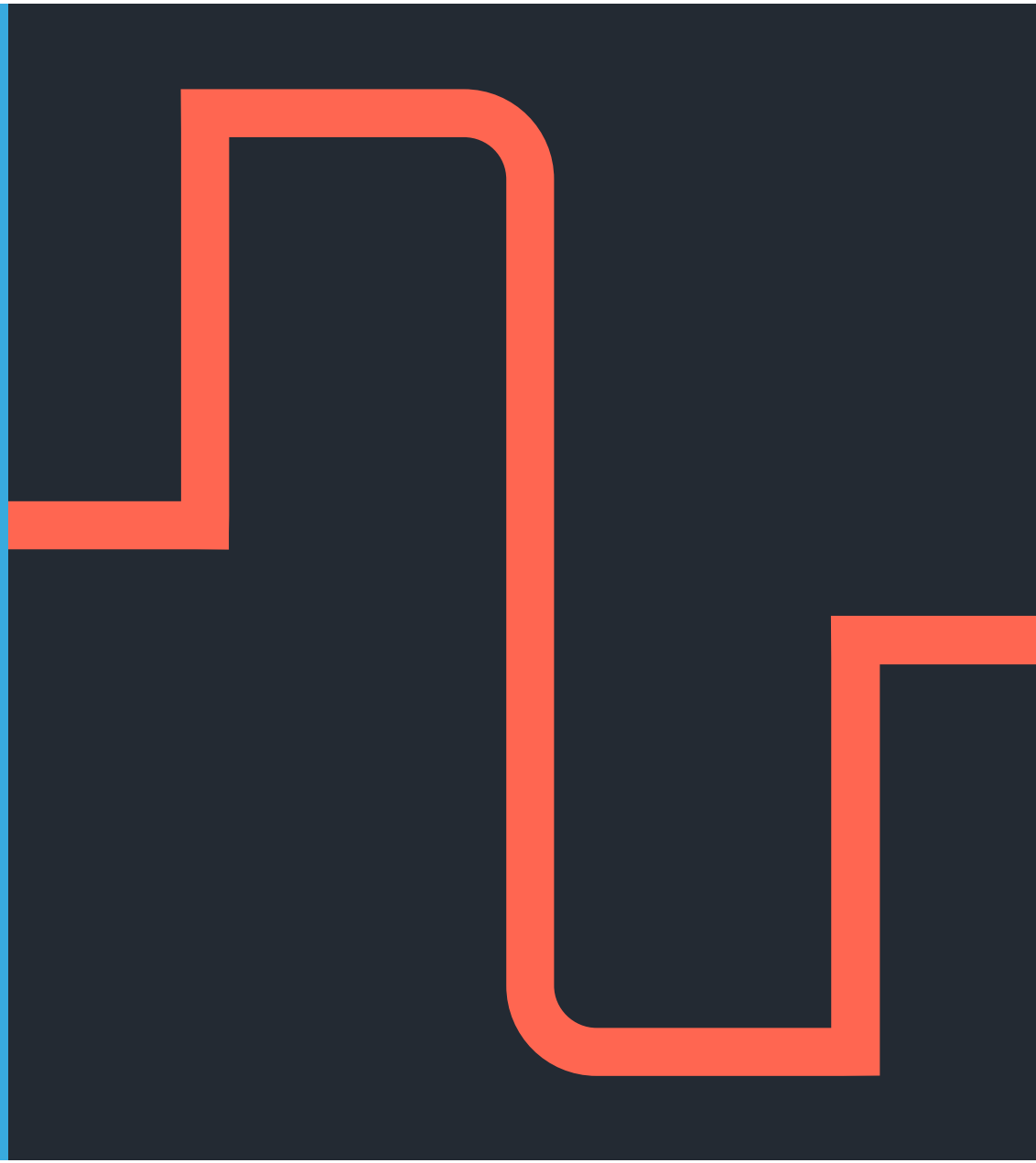
It's also a fast-moving industry. WormGPT only began to make headlines last month in July, but it's already being joined by a raft of similar tools. The latest, discovered by security researchers at threat intelligence outfit Falcon Feeds, is Evil-GPT.

A user by the name of AMLO posted the chatbot for sale on a darknet hacking forum for the somewhat impressively low price of US$10.

Praktijkvoorbeeld én ervaring

Poll (2)

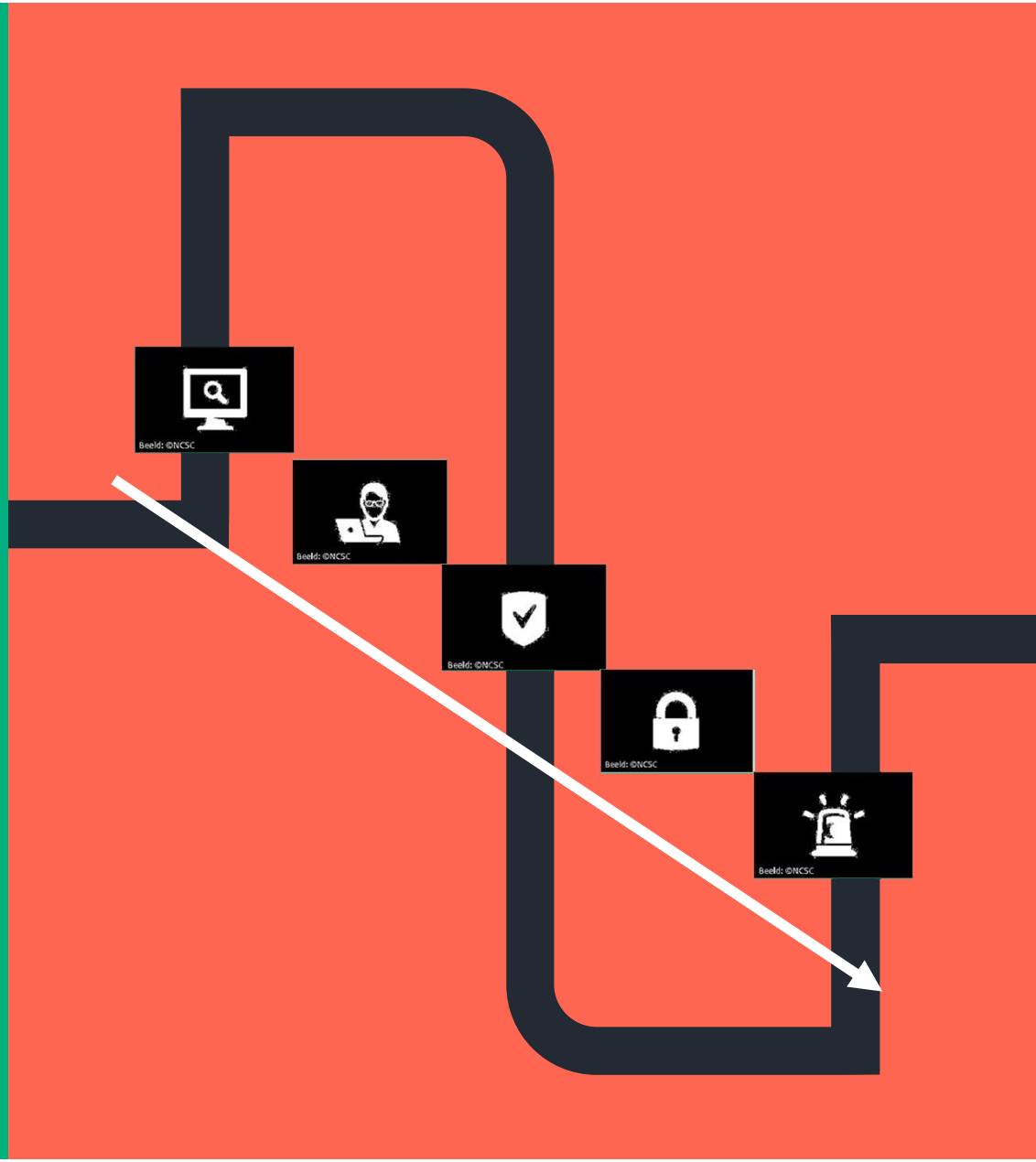
Heeft u al maatregelen genomen om cyberweerbaar te zijn?



Aandacht voor digitale veiligheid

1. Breng je risico’s in kaart
2. Bevorder veilig gedrag
3. Bescherm systemen, applicaties en apparaten
4. Beheer toegang tot data en diensten
5. Bereid je voor op incidenten

Home | Digital Trust Center (Min. van EZ)



12-11-2024

1. Breng je risico’s in kaart

- Inventariseer de ICT onderdelen: oa. einde garantie en ondersteuning, welke software en versie draaien op welke systemen.
- Plan elke 6 maanden een update van deze inventarisatie
- Leg afspraken met bijvoorbeeld externe IT leveranciers vast (in een service-level-agreement)
- Maak een noodplan voor het geval dat systemen niet meer te benaderen zijn en maak een bellijst met relevante contactpersonen en bedrijven in geval van nood. Zorg voor een uitgeprinte versie van deze lijst op een toegankelijke plaats.

2. Bevorder veilig gedrag

- Bouw aan een veiligheidscultuur, moedig medewerkers aan om te melden.
- Help medewerkers met bewustwording door en training. Bijvoorbeeld in herkennen van phisingmail, gebruik van sterke wachtwoorden en wachtwoordmanagers.
- Test: https://haveibeenpwned.com/

3. Bescherm systemen, applicaties en apparaten

- Check de instellingen van apparatuur, software, netwerk –en internetverbindingen. Vooral nieuwe software, computer en netwerkapparatuur wordt vaak afgeleverd met standaardinstellingen inclusief een standaard wachtwoord.
- Bepaal kritisch bij de functies en diensten die automatisch “aan” staan of je die nodig hebt.
- Up-to-date houden van software is essentieel. Inventariseer en plan wat je kunt updaten en bepaal wat je automatisch wilt updaten met de test: Test: Is automatisch updaten verstandig? | Digital Trust Center (Min. van EZ)
- Denk ook aan al je mobiele apparaten
- Gebruik een firewall
- Versleutel je data op harde schrijven, laptops, USB sticks maar ook in de cloud.

4. Beheer toegang tot data en diensten

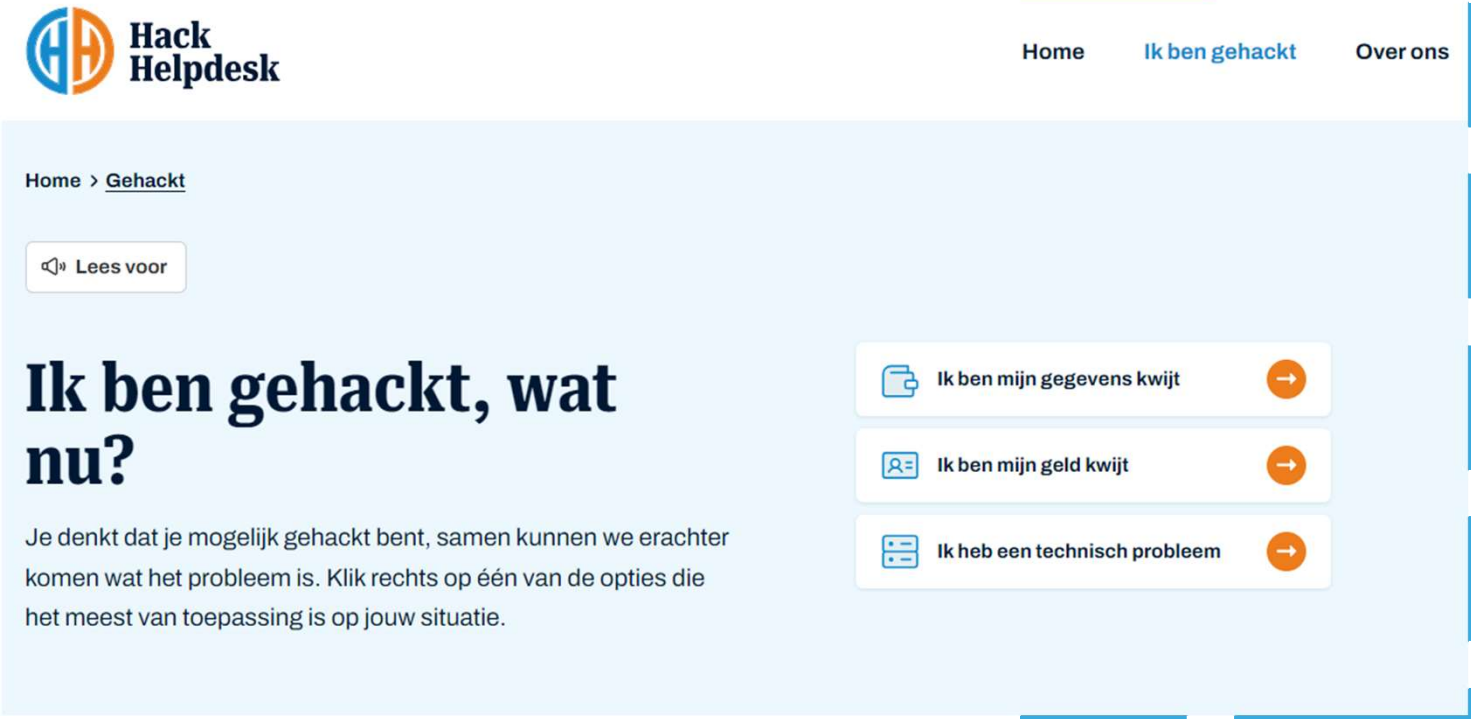
- Gebruik veilige, sterke en verschillende wachtwoorden
- Stel extra beveiliging in. Denk aan bankzaken, bedrijfsgegevens in de cloud of administratieve gegevens. Bijvoorbeeld door multifactorauthenticatie (MFA) of tweefactorauthenticatie (2FA) en inloggen met een token.
- Bepaal toegang en gebruik een rechtenmatrix.
- Pas toegangsrechten aan en hou ze actueel.
- Maak een proces voor in- en uitdiensttreding van medewerkers
- Gebruik persoonsgebonden accounts
- Vergrendel werkplekken en belangrijke systemen

5. Bereid je voor op incidenten

- Weet hoe je op incidenten moet reageren. Gebruik een risicoanalyse en leg scenario's vast in een incident-responseplan.
- Herstellen van incidenten; bepaal niet alleen de schade om de systemen en bedrijfsvoering te kunnen herstellen maar bepaal ook wie je informeert. Denk hierbij aan het beperken van reputatieschade maar ook verplichte meldingen aan instanties.
- Oefenen, testen en trainen; er zijn cyberoefeningen: Oefen en bereid je voor op een cyberincident | Digital Trust Center (Min. van EZ)
- Ontwikkel een back-up strategie

Help ik ben gehackt

- HackHelpdesk - Gratis eerste hulp bij cybercriminaliteit
- Opgezet door Platform veilig ondernemen



Poll (3)

Heeft u al een noodplan/ draaiboek klaarliggen en bent u voorbereid op cyberincidenten?

NIS2 cyberwetgeving op komst

Doel NIS2-Richtlijn Europa

- ✓ Cyberbeveiliging in EU harmoniseren en weerbaarheid vergroten
- ✓ Opleggen strenge beveiligingsnormen

Essentiële en belangrijke organisaties

- ✓ Digitale Veiligheid organisatie op orde brengen
- ✓ Ruim 50 zaken controleren / regelen
- ✓ Risicoanalyse maken (ook van de leveranciers)

Toeleveranciers

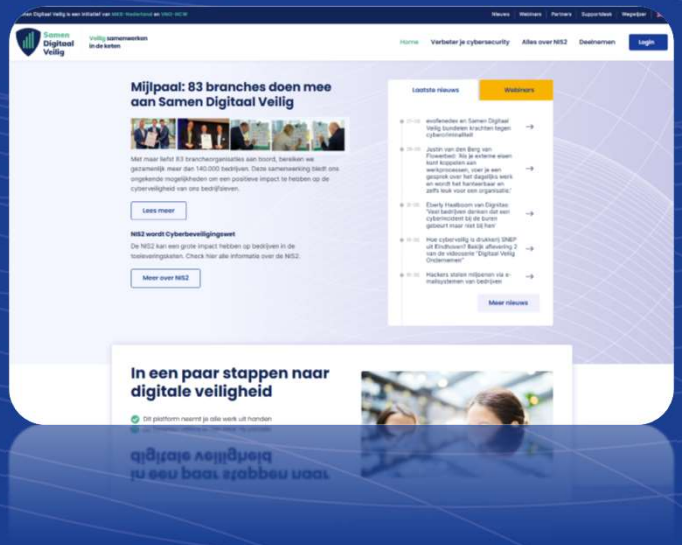
- ✓ Leveranciers die diensten en producten leveren aan NIS2 bedrijven moeten passende maatregelen nemen.

>10.000
NIS2 bedrijven
+
> 50.000
leveranciers

Samen Digitaal Veilig

Samen Digitaal Veilig

"Een online platform voor elke onderneming om aantoonbaar te kunnen voldoen aan een behapbaar cybersecurity niveau en cyberwetgeving."



Samen Digitaal Veilig

Hoe werkt de keten?

"Cybersecurity is moeilijk af te spreken zonder norm."

"Kost veel tijd en geld."

"Leveranciers moeten op tijd beginnen."

Samen Digitaal Veilig

NIS2 sectoren

Sectoren bijlage I	Sectoren bijlage II
Energie	Digitale aanbieders (online marktplaatsen)
Transport	Post- en koeriersdiensten
Bankwezen	Afvalstoffenbeheer
Infrastructuur financiële markt	Levensmiddelen
Gezondheidszorg	Chemische stoffen (productie, opslag en distributie)
Drinkwater	Onderzoek (onderzoeksinstellingen)
Digitale infrastructuur	Vervaardiging / manufacturing
Beheerders van ICT-diensten (MSP's)	
Afvalwater	
Overheidsdiensten	
Lokale overheden (gemeenten)	
Ruimtevaart	

Samen Digitaal Veilig

Verplichtingen NIS2 bedrijven

1. Registratieplicht

Organisaties die vallen onder de Cyberbeveiligingswet registreren in het entiteitenregister (wordt nog aan gewerkt).

2. Zorgplicht

Organisaties zijn verplicht een risicoanalyse uit te voeren voor de leveranciers. De leden van het bestuur moeten een opleiding volgen en toezicht houden op de uitvoering ervan.

3. Meldplicht

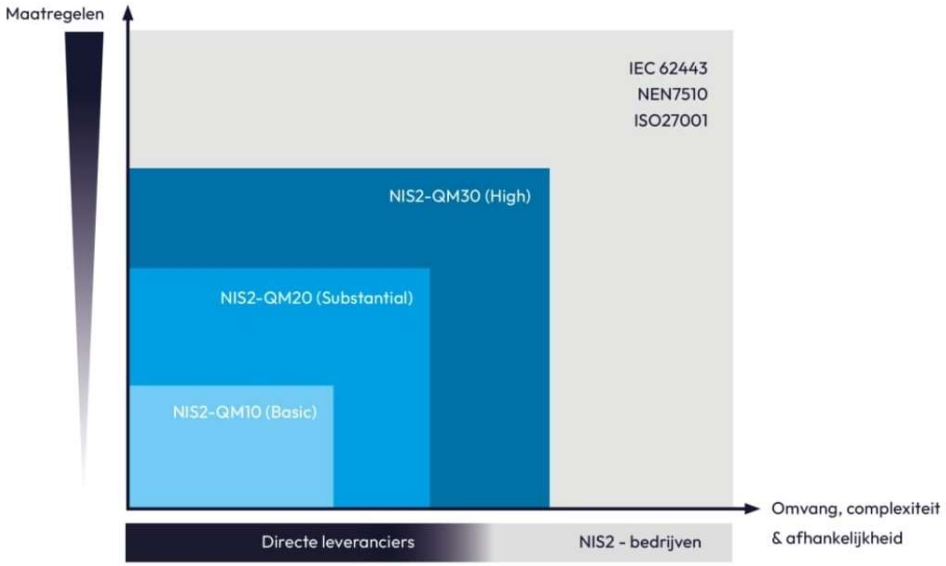
Significante incidenten (drempelwaarden worden nog uitgewerkt) moeten binnen 24 uur worden gemeld bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder.

4. Toezicht

NIS2 organisaties vallen zijn onderworpen aan toezicht via verschillende toezichthouders (per sector). Naast bepaalde handhavingsinstrumenten kunnen zij ook bestuurlijke boetes kunnen opleggen.

Samen Digitaal Veilig

Risiconiveau en passende normen



NIS2 Quality Mark abonnement

Met dit abonnement haal je het NIS2 Quality Mark.
- NIS2 Quality Mark BASIC, lijst met alle passende maatregelen
- Stappenplan met invulvelden
- Video-uitleg en praktische voorbeelden, alles in begrijpelijke taal
- Downloads inbegrepen
- Veilig-online-omgeving. Altijd beschikbaar, makkelijk in gebruik
- Reminder-functie inbegrepen
- Juridisch gecheckt
- 1-op-1 opstartsessie inbegrepen
- Invulondersteuning inbegrepen
- Supportdesk inbegrepen

ISO 27001
Internationale cybersecurity norm voornamelijk bedoeld voor grote bedrijven. →

ISO 27002
Internationale cybersecurity norm voornamelijk bedoeld voor grote bedrijven. →

NEN 7510
Nederlandse cybersecurity normering specifiek gemaakt voor de zorgsector. →

NIS2 Quality Mark
Het beste keurmerk voor mkb-bedrijven die toeleverancier zijn van grote bedrijven die aan NIS2 moeten voldoen. →

Cyra
Zet de eerste stappen naar een cyberweerbare onderneming. →

- Techniek Nederland leden krijgen 50% korting op NIS2 Quality Mark certificaat met code **TECHNIEKNIS2**
- Maak eerst account aan op: Samen Digitaal veilig
- Bepaal aan welke norm je wilt voldoen: NIS2 checklist mkb-leveranciers V2

Werk aan de winkel

Begin niet te laat

- Maatregelen nemen kost tijd
- We verwachten dat de wet in Nederland uiterlijk 1 juli 2025 ingaat
- Andere omringende landen voeren de wet mogelijk eerder in
- Groot tekort aan cyberspecialisten
- Bescherm je bedrijf

Techniek Nederland Verzekeringen - Cyberverzekering

Poll (4)

Was u al bekend met het platform Samen Digitaal Veilig en de NIS2 Quality Mark?

Cybersecurity OT

John van Vugt

12-11-2024

Poll (5)

Heeft u al aandacht gegeven aan cyberweerbaarheid op gebied van Operationele technieken (OT)?

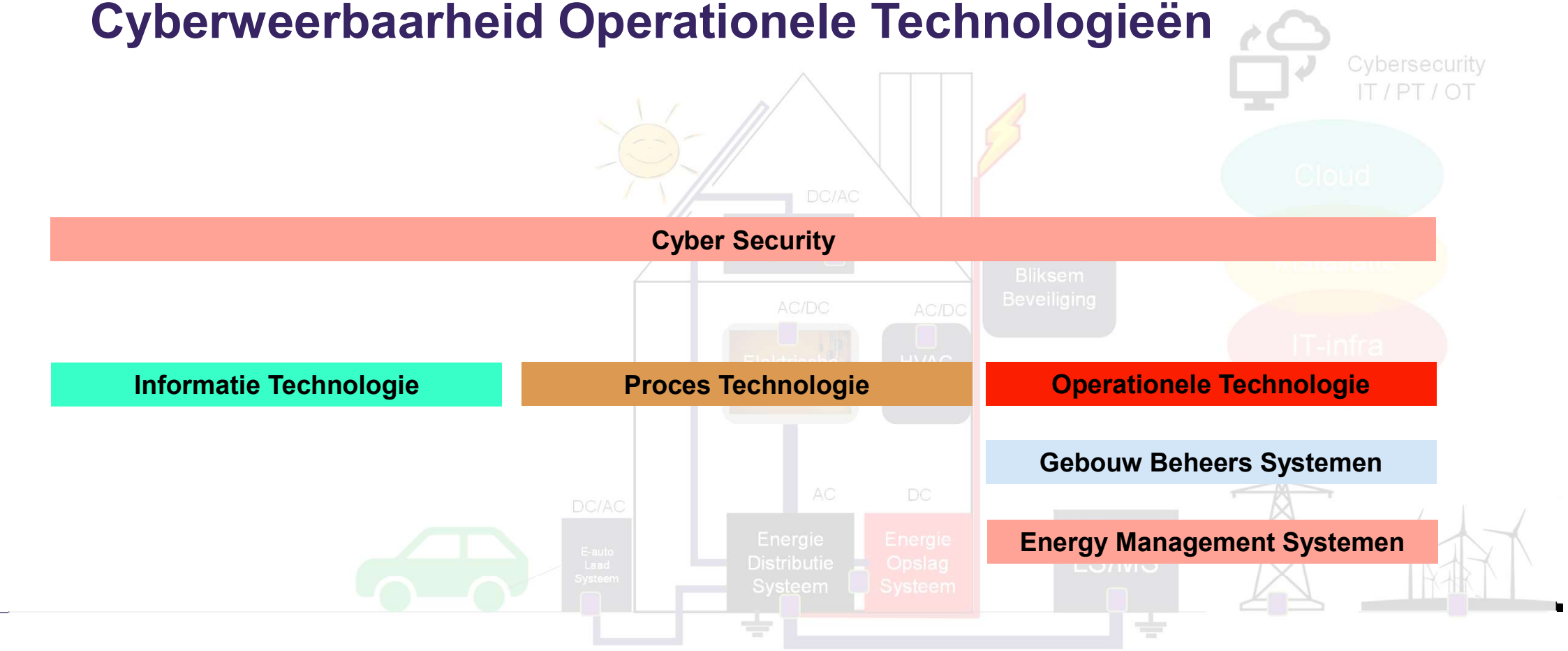
Cybersecuritybeeld Nederland

Het Cybersecuritybeeld Nederland (CSBN) wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid gepubliceerd en komt tot stand in samenwerking met publieke en private partners.

Dit rapport laat een toenemende kwetsbaarheid zien voor o.a. installatieonderdelen die gekoppeld zijn aan internet.

En concludeert hierbij dat de weerbaarheid van individuen en organisaties achter blijft bij de groei van de dreiging.

Cyberweerbaarheid Operationele Technologieën



Cyber Security

Informatie Technologie	Proces Technologie	Operationele Technologie
		Gebouw Beheers Systemen
		Energy Management Systemen

Systeem Integratie van Elektro, Klimaat en Sanitair Installatie

Techniek Integratie van Elektro, Klimaat en Sanitair Installatie

Applicaties

Systemen

Infrastructuur

EPBD IV

Gebouw Energie Management Systeem

Industriële / Gebouw Automatiserings- en Controle Systeem

Cybersecurity
IT / PT / OT

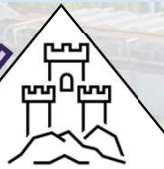
Cloud

Installatie

Netbeheer

Vakmanschap
Vakbekwaamheid

Samenwerking
Organisatie



Zonne (warmte)
Systeem

Bliksem
Beveiliging

Elektrische
Installatie

Heating
Vent.
Aircon.
Cooling

Energie Management Systeem

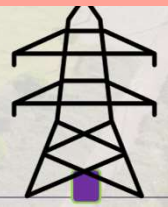
DC/AC
V2H-V2G

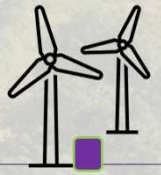
E-auto
Laad
Systeem

Energie
Distributie
Systeem

Energie
Opslag
Systeem

LS/MS





Meten is Weten

ENERGIENET

Techniek Nederland

Cybersecurity Operationele Technologieën

Installatie Internet/Cloud oplossingen brengen een groot scala aan technische mogelijkheden: kwetsbaarheid van installaties neemt toe.

Internet of things (IoT) toepassingen brengen een groot scala aan applicaties: kwetsbaarheid van installaties neemt toe.

De digivaardigheden zijn redelijk op orde maar de cybervaardigheden zeker nog niet.

Cybersecurity Operationele Technologieën

De verhoging van cyberveiligheid is van belang voor alle type operationele installaties ook voor niet-vitale ondernemingen.

Cyberincidenten hebben grote gevolgen voor alle partijen in de toeleveringsketen.

De lidbedrijven spelen een cruciale rol als intermediair tussen vraag en aanbod. Iedereen is onze klant, dus in potentie is iedereen kwetsbaar.

Ondernemerschap Cybersecurity Operationele Technologie

Verbinden :

Bewustwording creëren voor de eigen onderneming en in de toeleveringsketen.

Aantoonbare Kennis en Kunde:

Vakmanschap en concrete tools ontwikkelen die lidbedrijven ondersteunen in hun bedrijfsvoering.

Kwaliteitsborging:

Rol van de lidbedrijven versterken in de markt als aanspreekpartner voor cybersecurity vraagstukken.

Ld0 niet alleen installatiebedrijven maar ook technische detailhandel; deze nemen we neem ik aan in de 'slipstream' mee. Al was het alleen maar om het beeld naar onze (andere) belangrijke ledengroep neer te zetten. Denk bijv ook aan Coolblue en BCC die nu al een dubbeldooier met installatie zijn.
Linden Remco van der; 2022-11-02T08:26:54.908

VJv0 0 Eens!
Vugt, John van; 2022-11-02T08:32:20.593

Cyberweerbaarheid ambitie Techniek Nederland

Niet achter lopen op mogelijke dreigingen.

Ondernemen en innoveren in de toeleveringsketen.

Kennen, kunnen, beheersen.

Continuïteit in de bedrijfsvoering in de toeleveringsketen.

Techniek Nederland

De leden van Techniek Nederland hebben een cruciale centrale rol bij het realiseren en beheren van cyberveilige installaties.

Techniek Nederland Cyebersecurity OT project

- Voldoen alle toegepaste producten/systemen aan de eisen/normen?
- Kunnen producten/systemen digitaal worden bediend/geschakeld?
- Delen producten/systemen digitaal informatie onderling?
- Delen producten/systemen digitale informatie met derden?
- Wie hebben er digitale toegang tot producten/systemen?
- Hebben we voldoende perceptie van het risico voor de klant?
- Zijn de verantwoordelijkheden van de verschillende partijen duidelijk?
- Hebben we, leden Techniek Nederland en keten, voldoende kennis?

Techniek Nederland

2023 en 2024 :

Bewustwording (publicaties), onderzoek(rapporten).

2025: Producten, diensten en activiteiten voor leden

DigiBouw, het digitaliseringsevent in de bouw

20 november 2024 tussen 10:00 - 18:00 uur

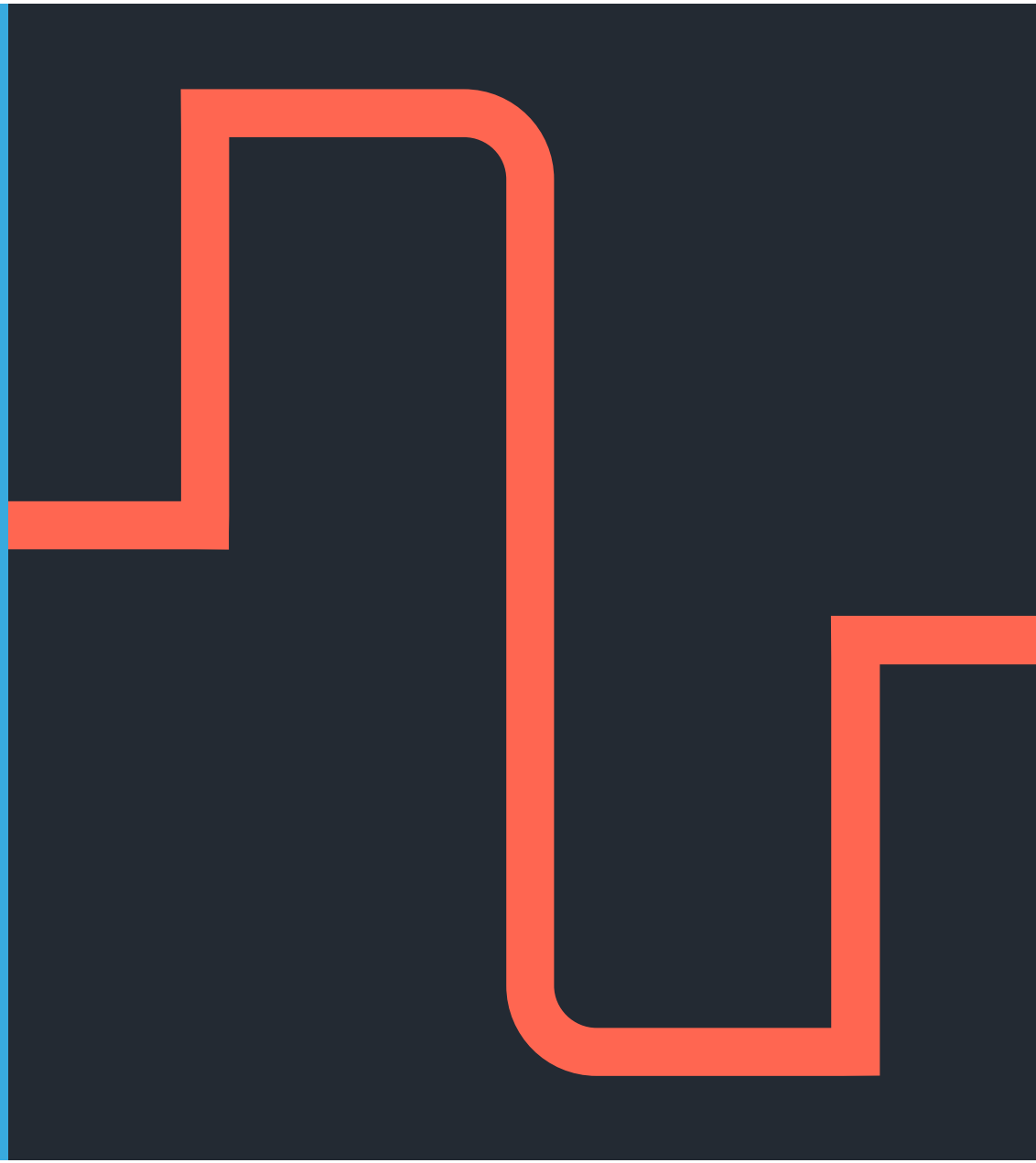
Jaarbeursplein 6, 3521 AL UTRECHT (Jaarbeurs Utrecht (Beatrixgebouw))

Poll (6)

Voldeed de geboden informatie van deze webinar aan uw verwachtingen?

Poll (7)

Over welk onderwerp zou u nog meer informatie willen ontvangen vanuit Techniek Nederland?



Dank voor uw deelname!

Samen Digitaal 2024

- ☑ 12 maart. 1e ervaringen WKb
- ☑ 12 sep. Formulieren digitaliseren
- ☑ 12 nov. Cybersecurity en dataveiligheid

Samen digitaal 2025

- ☐ 12 maart Simpel en effectief stappenplan
- ☐ 12 mei Slim data delen en data inzicht
- ☐ 12 nov. Digitaliseren en vaardigheden

Terugkijken : https://www.techniekneder land.nl/extra/kennisuitwisseling-platform-samen-digitaal/

Contact voor meer info en opvolging:
Bart Molmans B.molmans@techniekneder land.nl