Brancheverenigging Kleinschalige Zorg

Webinar

NIS2 richtlijn en de impact op Kleinschalige Zorg

Samen Digitaal Veilig

Programma

- Opening
- Welkomstwoord door Mirjam van der Veen
- Belang cyberveiligheid en impact NIS2 door Ron Vermeulen
- Demo Samen Digitaal Veilig door Ron Vermeulen
- Afsluiting & vragen

Samen Digitaal Veilig

Waarom zijn we vandaag hier?

HLN NIEUWS SPORT SHOWBIZZ NINA REGIO VIDEO PUZZEL PO

© HLN / Getty Images

“50.000 documenten met patiëntgegevens gestolen”: hackers konden communicatie met artsen onderscheppen

Gisteren meldde onze redactie nog dat het Belgische bedrijf MediCheck het slachtoffer werd van hackers, vandaag blijkt hoe groot de schade is. De cybercriminelen van ‘Killsec’ hebben 50.000 documenten buitgemaakt met daarin gevoelige gegevens. Het gaat om verslagen van meer dan 750 controleartsen, die in opdracht van MediCheck en grote klanten zoals H&M en bpost patiënten onderzoeken.

Kenneth Dee 25-09-24, 06:42 **Laatste update:** 27-09-24, 12:07 **Bron:** Eigen berichtgeving

Home Voor mij Media Uitgaan Meer

Gegevens van zorginstellingen op straat door hack

9 oktober 2024 om 20:27 • Aangepast 25 oktober 2024 om 21:14

Lees voor NL

Een hacker heeft duizenden e-mailadressen buitgemaakt van zorginstellingen en andere bedrijven waarmee de Eindhovense organisatie Combinatie Jeugdzorg zaken doet. Bij het lek zijn ook mailadressen van cliënten buitgemaakt, maar volgens de zorginstelling gaat het om ‘minder dan 10 procent’.

In totaal gaat het om meer dan tienduizend e-mailadressen waarmee Combinatie Jeugdzorg ooit heeft gemaild. Betrokkenen kregen dinsdagavond een mail van Combinatie Jeugdzorg met het bericht over de hack.

Jaarrapport Autoriteit Persoonsgegevens (AP)

Cybercriminelen die persoonlijke gegevens wilden bemachtigen hadden het vooral gemunt op de sector zorg en welzijn. Bijna een kwart van de gemelde datalekken over cyberaanvallen, een kleine negenduizend, was in 2022 afkomstig uit de zorgsector.

NOS Nieuws Sport Live Programma's

Tandartsbedrijf betaalt internetcriminelen losgeld na ransomware-aanval

Tandartsbedrijf Colosseum Dental, waar in Nederland 120 tandartsenpraktijken bij zijn aangesloten, heeft losgeld betaald aan internetcriminelen. Vorige week werd het tandartsbedrijf getroffen door een ransomware-aanval, waarbij computerbestanden versleuteld werden.

Zuyderland
De zorg van je leven

SPOED MEDEWERKERS

Ziekenhuis Zorg GGZ Zuyderland Werken & Leren

Zuyderland meldt datalek in systeem leverancier Thuiszorg en Thuishulp

27 MRT 2024

Door een fout in het systeem van een leverancier van Zuyderland, zijn persoonlijke gegevens van (een deel) van de medewerkers die werkzaam zijn of zijn geweest bij Zuyderland Thuiszorg en Zuyderland Thuishulp, openbaar geworden. Er is een grondig onderzoek ingesteld naar het ontstaan van dit datalek. De oorzaak van het datalek is inmiddels weggenomen.

Wist je dat...

Schade per jaar is 750 miljoen

De kans op een **brand** bij een bedrijf dit jaar is **1** op **8000**

De kans op een **inbraak** bij een bedrijf dit jaar is **1** op **250**

De kans op een **cyberaanval** bij een bedrijf dit jaar is **1** op **5**

Schade per jaar is >10 miljard!

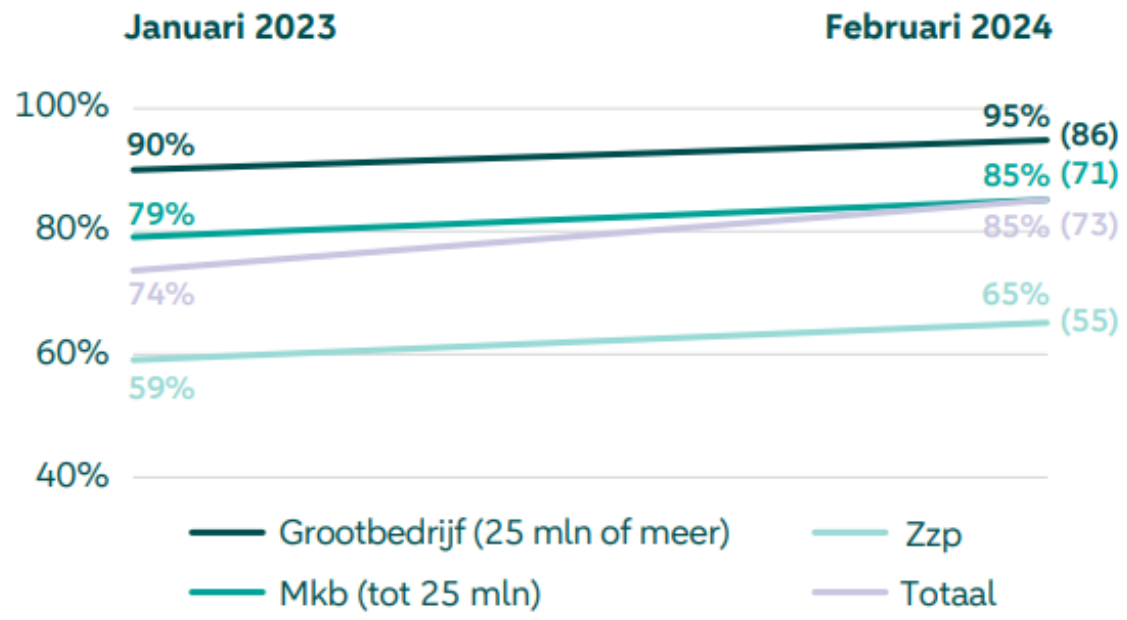
Bron: Rabobank

Samen Digitaal Veilig

Aantal cyberaanvallen groeit

Figuur 1: Een meerderheid van de bedrijven is al eens geconfronteerd met cybercriminaliteit

Percentage bedrijven dat aangeeft weleens te maken te hebben gehad met cybercriminaliteit. Het percentage tussen haakjes geeft het aandeel bedrijven weer waarbij dit (in ieder geval) in de afgelopen twaalf maanden is gebeurd.



Onderzoek ABN AMRO
April 2024

In ruim 50% van de gevallen ontstaan een hack door een menselijke fout.

Hoe ontstaan deze hacks nu precies?

En wat kan je doen om dit te voorkomen

Samen Digitaal Veilig

Klikken op verkeerde linkjes

Voorbeeldmail 1: ICS

Van: International Card Services <mailto:helpdesk@identity.com>
Verzonden: maandag 15 augustus 2016 22:10
Aan: [e-mailadres]
Onderwerp: Verfieer uw identiteit

ICS VISA
INTERNATIONAL CARD SERVICES

Geachte kaarthouder,

International Card Services vindt fraudepreventie erg belangrijk. Om fraude te voorkomen, voeren wij dan ook regelmatig de nodige controles uit. Uit deze controles is gebleken dat er mogelijk misbruik van uw creditcard gegevens is gemaakt. Om veiligheidsredenen hebben wij uw creditcard beperkt voor gebruik.

Om de beperking op te heffen dient uw identiteit te verifiëren.

Helaas moeten wij u mededelen dat uw rekening binnen 48 uur om veiligheidsredenen wordt geblokkeerd als u uw identiteit niet verifieert.

Wij adviseren u zo spoedig mogelijk om uw identiteit te verifiëren om weer direct gebruik te kunnen maken van uw creditcard zonder beperkingen.

START VERIFICATIE

Met vriendelijke groeten
International Card Services B.V.

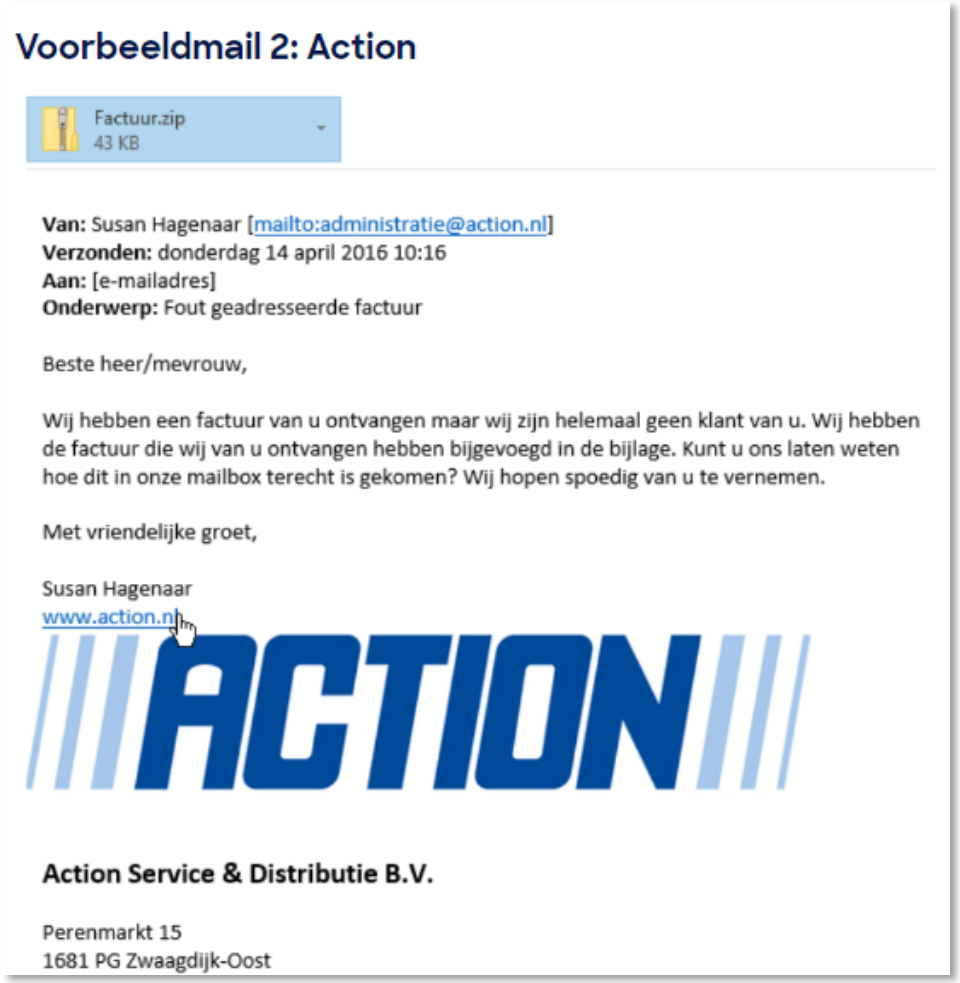
Postadres: Postbus 23225, 1100 DS Diemen © 2016 International Card Services B.V.

Oplossing

- Controleer de afzender van de mail
- Vraag je IT-beheerders om onbekende afzenders te kenmerken!
- Klik niet zomaar op linkjes. Controleer de achterliggende link!
- Klik niet als je het niet vertrouwd

Samen Digitaal Veilig

Downloaden van verkeerde bestanden



Voorbeeldmail 2: Action

Factuur.zip
43 KB

Van: Susan Hagenaar [mailto:administratie@action.nl]
Verzonden: donderdag 14 april 2016 10:16
Aan: [e-mailadres]
Onderwerp: Fout geadresseerde factuur

Beste heer/mevrouw,

Wij hebben een factuur van u ontvangen maar wij zijn helemaal geen klant van u. Wij hebben de factuur die wij van u ontvangen hebben bijgevoegd in de bijlage. Kunt u ons laten weten hoe dit in onze mailbox terecht is gekomen? Wij hopen spoedig van u te vernemen.

Met vriendelijke groet,

Susan Hagenaar
www.action.nl

ACTION

Action Service & Distributie B.V.

Perenmarkt 15
1681 PG Zwaagdijk-Oost

Oplossing

- Download nooit zip-bestanden als je de afzender niet kent of het niet vertrouwt
- Neem contact op met afzender om te checken of de afzender klopt

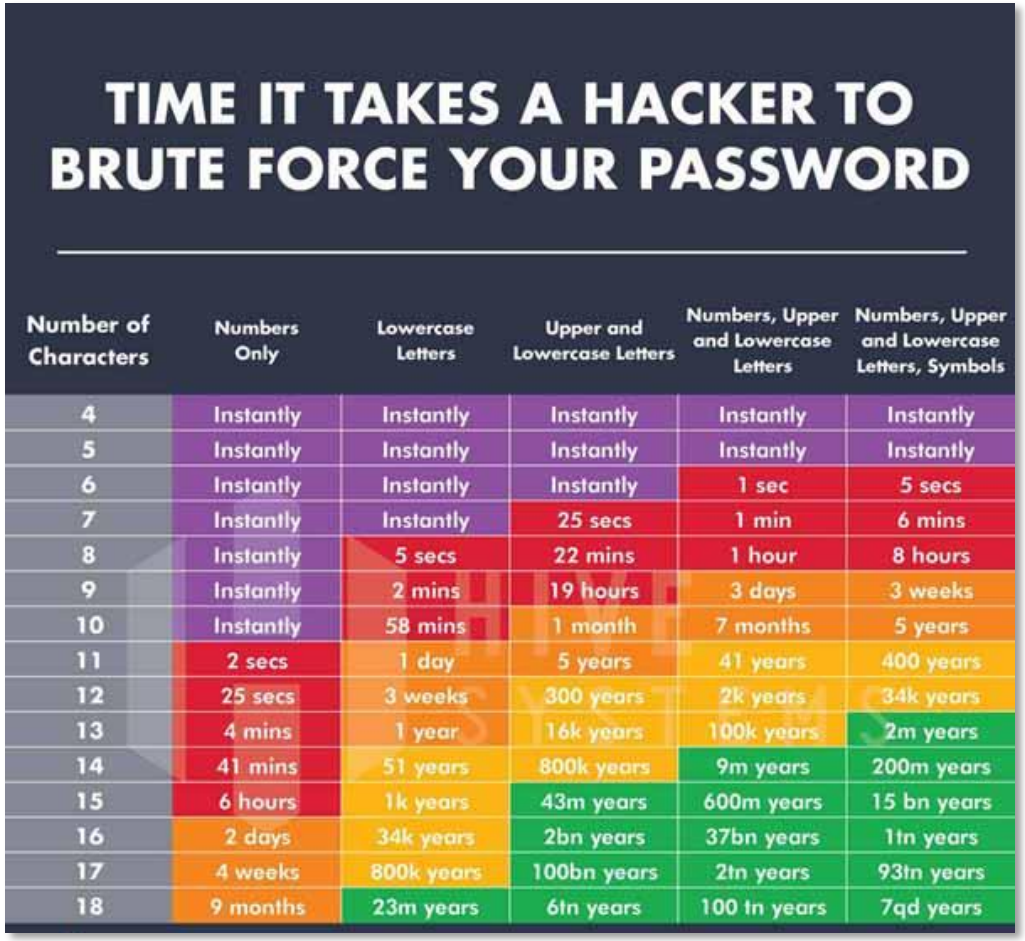
Samen Digitaal Veilig

Gebruiken van onveilige wachtwoorden

“Het duurt voor een hacker maar 1 minuut om een wachtwoord van 7 karakters met cijfers, letters en hoofdletters te kraken!”

Oplossing

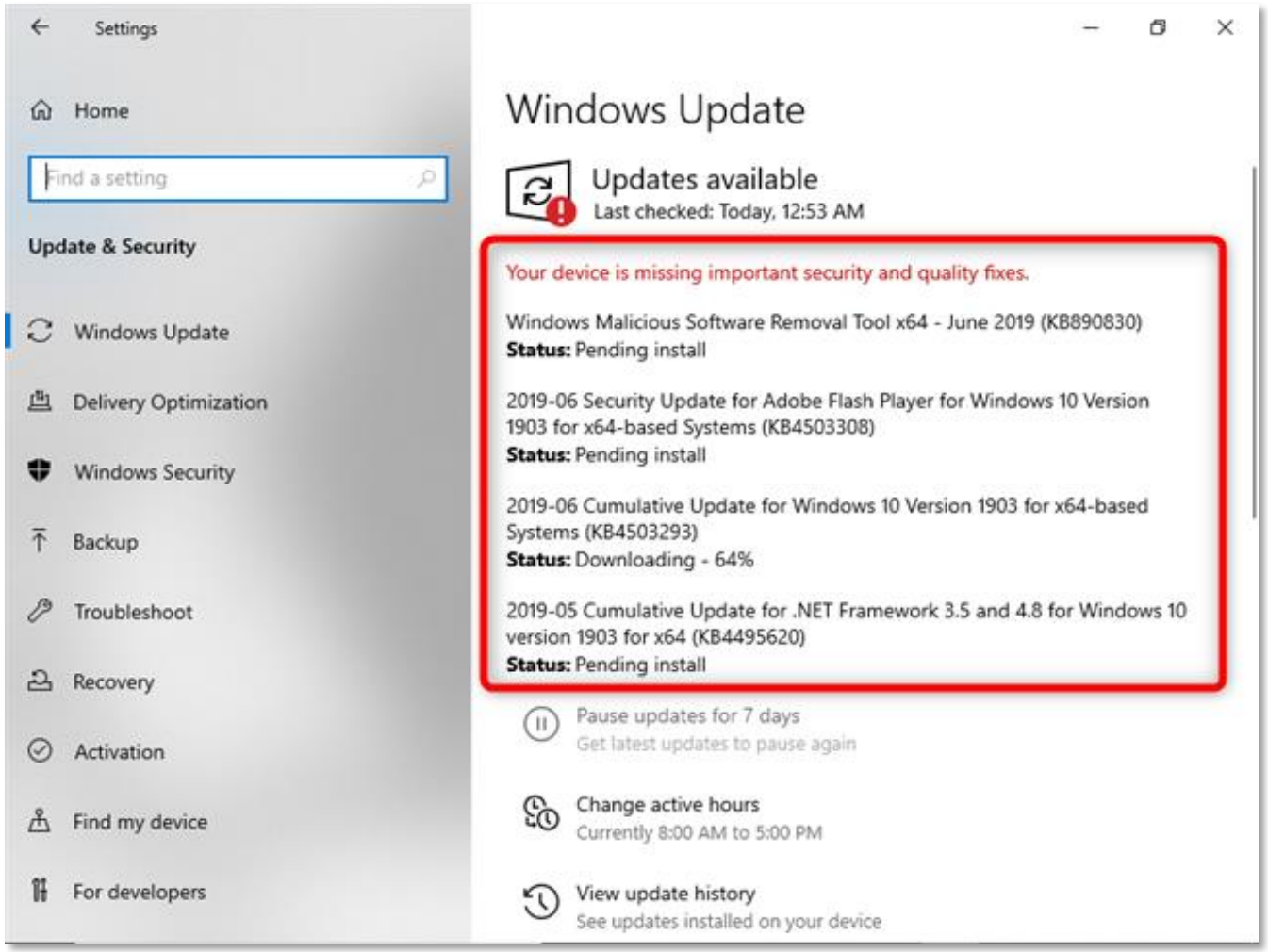
- Gebruik een wachtwoord manager
- Gebruik zoveel mogelijk MFA!



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Updates uitstellen



Oplossing

- Altijd updaten. Niet uitstellen.
- Ook de apparaten thuis!

Samen Digitaal Veilig

Geen beveiliging op je apparaten

“Elk jaar zijn er bijna 50.000 apparaten kwijt of gestolen!”

Oplossing

- Gebruik een virus / malware scanner op mobiele apparaten
- Installeer geen apps zoals Temu!

Samen Digitaal Veilig

Gebruik van openbare WiFi netwerken

- Openbare en onbeveiligde WiFi netwerken zijn niet veilig!
- Al het verkeer kan worden afgeluisterd
- Een hacker kan eenvoudig een wifinetwerk opzetten met dezelfde naam

Oplossing

- Gebruik je data van mobiele telefoon
- Maak een hotspot met je telefoon
- Gebruik een VPN

Samen Digitaal Veilig

Kansen en bedreigingen AI

Samen Digitaal Veilig

NIS2 wetgeving

NIS2-Richtlijn Europa

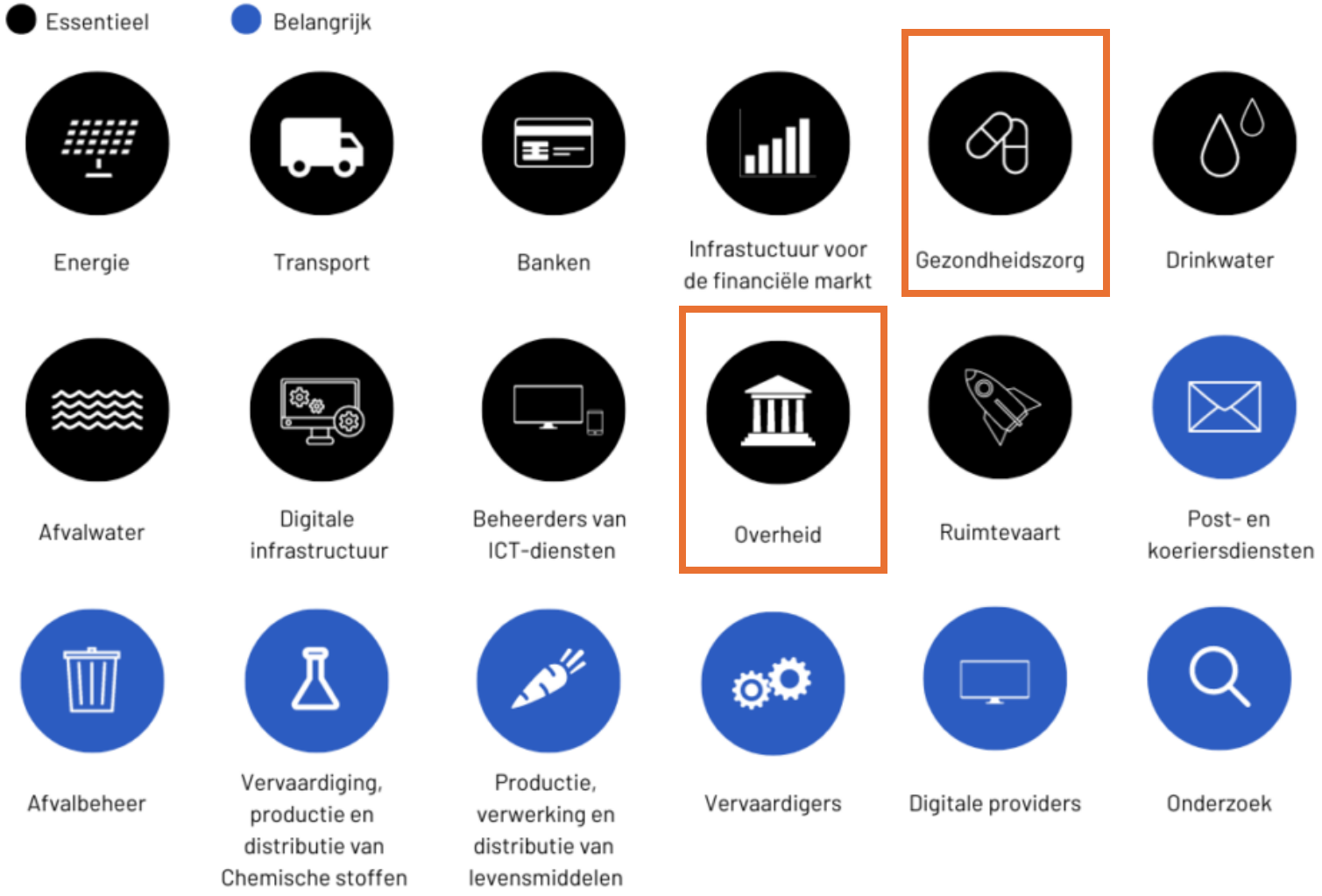
- De NIS2-richtlijn is sinds 17 oktober 2024 geldig in de Europese Unie
- Cyberbeveiligingswet halverwege 2025 van kracht in Nederland

Ruim 10.000 bedrijven in Nederland vallen direct onder de wet

- ✓ Registratieplicht
- ✓ **Zorgplicht** (ook voor de ketenpartners)
- ✓ Meldplicht
- ✓ Toezicht

Samen Digitaal Veilig

Sectoren die direct onder de NIS2 vallen



NIS2 bedrijven krijgen een zorgplicht voor hun leveranciers.

Samen Digitaal Veilig

Hoe werkt de keten in geval van risico?

Maken van risico-inventarisatie

Opleggen passende maatregelen

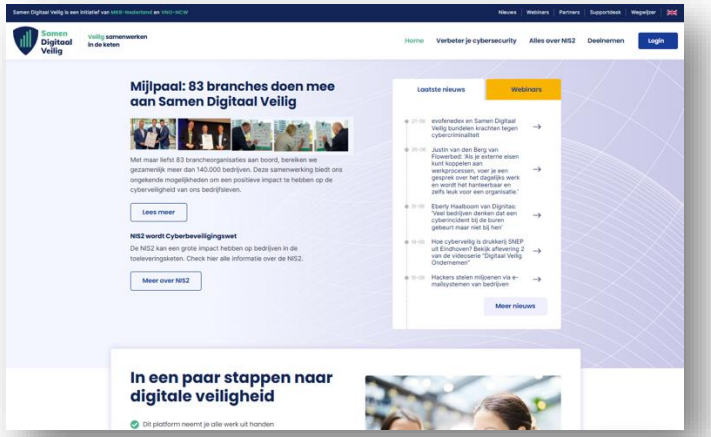
Aantonen dat je voldoet

Opleggen passende maatregelen

Aantonen dat je voldoet

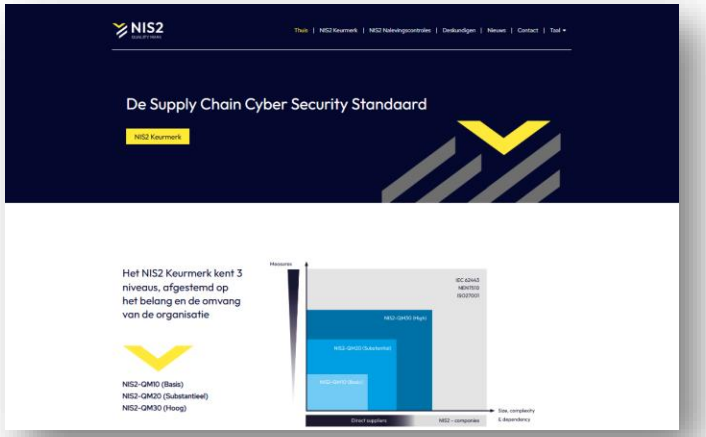
Twee initiatieven: Samen Sterk!

Samen Digitaal Veilig



- ✓ >80 branches & >60 kennis- en marktpartijen
- ✓ Praktische tools en hulpmiddelen
- ✓ Maatregelenlijsten NIS2 Quality Mark
- ✓ 1-op-1 ondersteuning & helpdesk

NIS2 Quality Mark



- ✓ Standaard normering cybersecurity & NIS2
- ✓ Open norm: door iedereen te gebruiken
- ✓ 3 niveaus: Basic / Substantial / High
- ✓ Audit en certificering mogelijk

>85 branches en >150.000 bedrijven









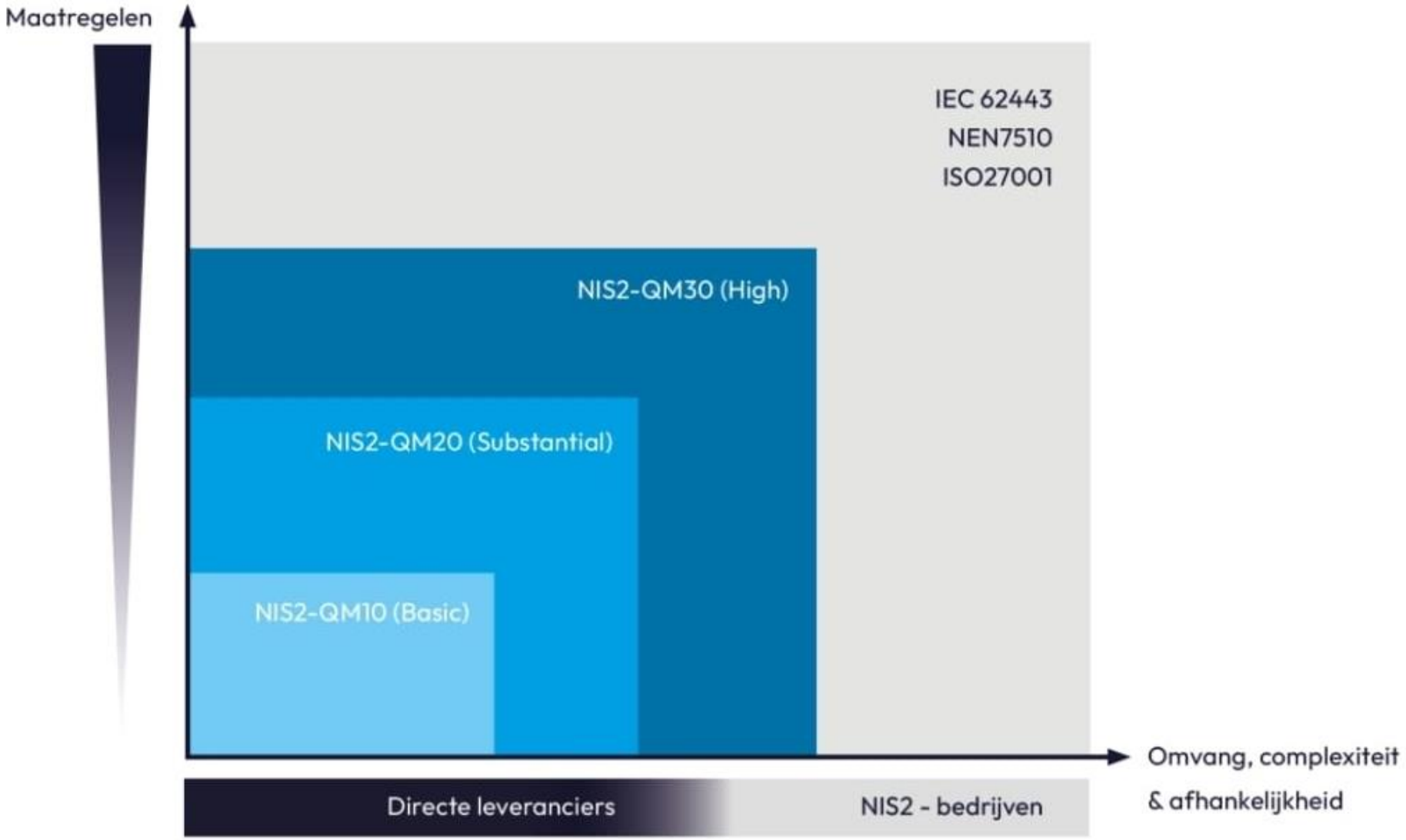






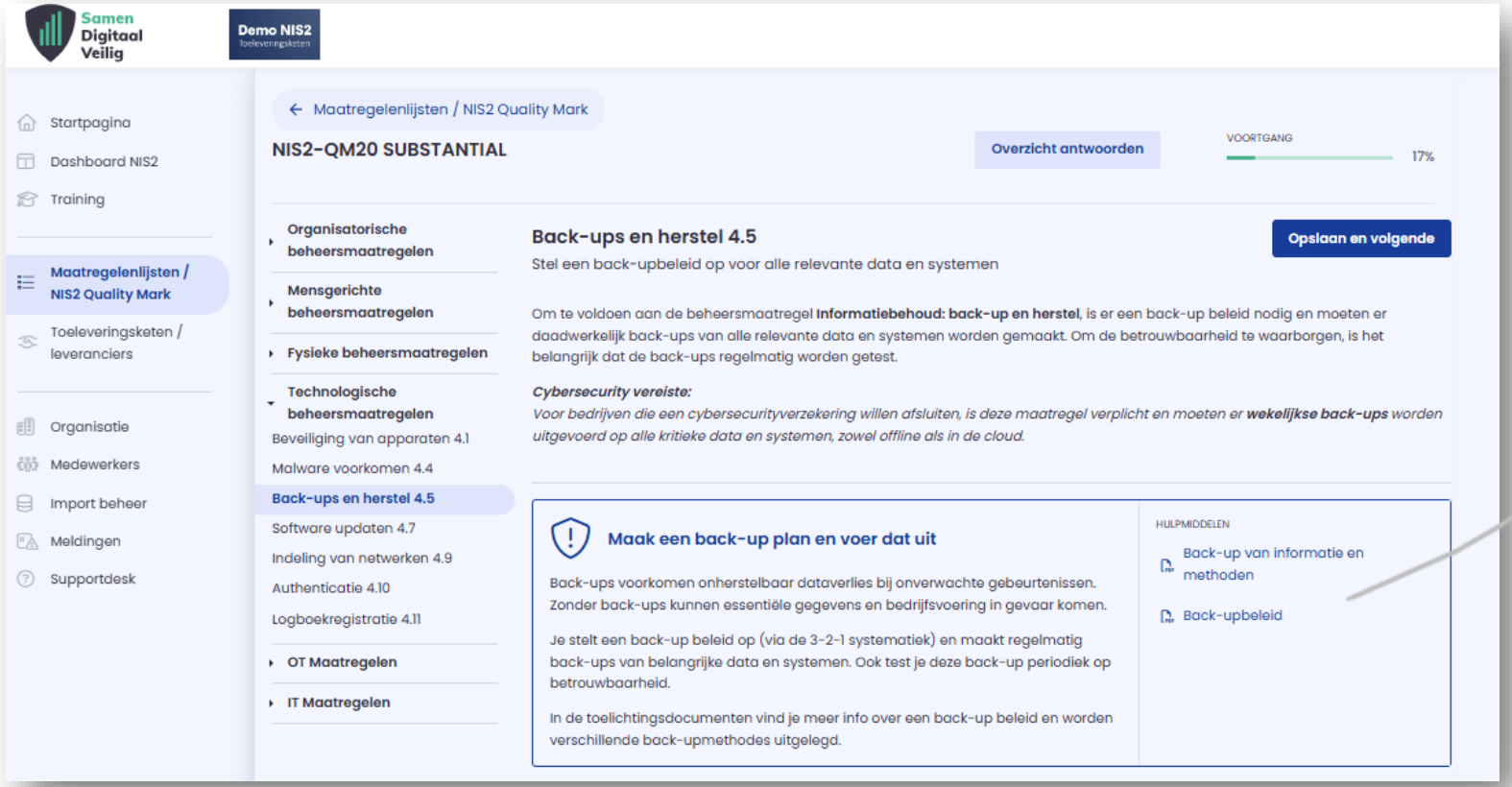
Samen Digitaal Veilig

Risiconiveau en passende normen



Praktische oplossing

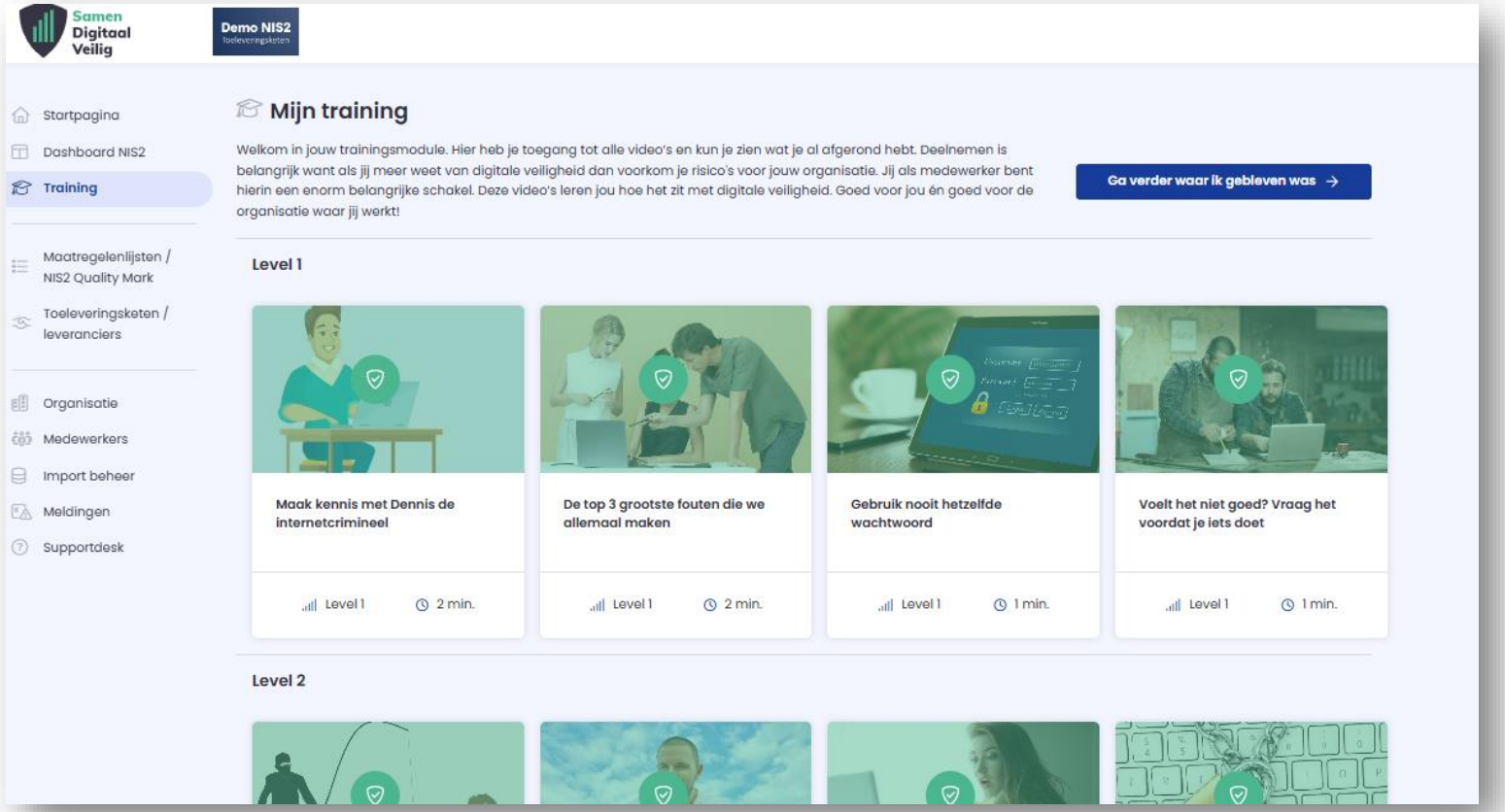
Maatregelenlijsten met hulpmiddelen



Samen Digitaal Veilig

Praktische oplossing

Trainingsvideo’s voor je medewerkers



Samen Digitaal Veilig

Impact Kleinschalige Zorg

- **Ga je bedrijf beschermen.** Het MKB is steeds vaker slachtoffer. Door een paar simpele maatregelen wordt je een stuk veiliger.
  - Start bijvoorbeeld met het gratis startpakket van Samen Digitaal Veilig
  - Of pak het gelijk goed aan en haal het NIS2 Quality Mark basic

Network and Information Security

- **Werk je met zorginstellingen?** Verwacht vragen of opgelegde maatregelen.
- **Maatregelen van software leveranciers.** Denk hierbij aan verplicht gebruik van MFA of uitgebreide back-up en herstel diensten.
- Verwacht dus ook **meer kosten** om je IT veilig te houden in de toekomst.
- Ga ook zelf aan de slag. **Vertrouw niet blindelings op je IT-leverancier**.

Samen Digitaal Veilig

Vragen

Samen Digitaal Veilig

Brancheverenigging Kleinschalige Zorg

Winnaar anti-phishing campagne

t.w.v. €1.500

Signtaal

Patricia Buijs

Samen Digitaal Veilig