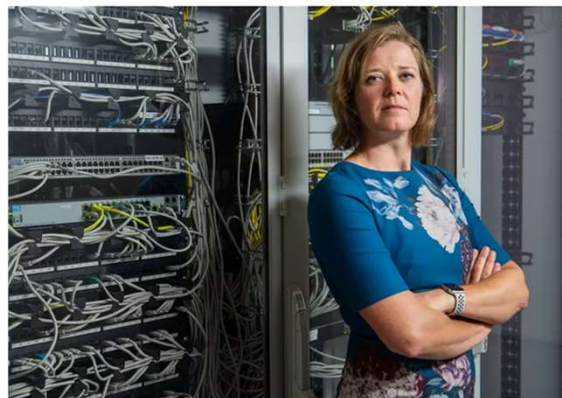


CYBERSECURITY IN DE ZORG

WIE, WAT, WAAROM en HOE?

28 juni 2022





▲ Liesbeth Holterman, manager van de cybersecurity hub van Novel-T. © Frans Nikkels Fotografie

Treurig gesteld met cyberveiligheid in Twentse maakindustrie

ENSCHEDE - Vrijwel geen van de veertig Twentse maakbedrijven die meededen aan een vrijwillige check heeft de cybersecurity op orde. Af en



Novel T



Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

de Volkskrant

Volgens Liesbeth Holterman van Cyberveilig Nederland, een brancheorganisatie van cybersecuritybedrijven en betrokken bij het initiatief, zijn bedrijven de afgelopen maanden slachtoffer geworden van een cyberaanval die voorkomen had kunnen worden als bekend was dat hun IP-adres of andere indicator was gecompromitteerd. Holterman: 'Het NCSC deelt nu vanuit de wettelijke taak alleen risico en dreigingsinformatie met bedrijven die tot de doelgroep horen, daar gaat het mis.'

Het platleggen van transportbedrijf Bakker Logistiek, waardoor er geen kaas in winkels van Albert Heijn lag, was bijvoorbeeld het gevolg van een kwetsbaarheid in Microsoft Exchange die al langer bekend was.



Den Haag

Doe de Security Check Procesautomatisering

Steeds meer ondernemingen hebben hun industriële controlesystemen (ICS) of operationele techniek (OT) verbonden met het internet. **Onbezwaarschadelijk** dat veel ICS en OT-apparaten eenvoudig toegankelijk zijn via internet. Ook in het Cybersecuritybeleid Nederland 2021 (CSB) wordt melding gemaakt dat dit bedrijven kwetsbaar maakt voor cybercriminaliteit. En dus is het tijd voor actie! Wat moet je weten en welke maatregelen moet je treffen?

Doe de Security Check Procesautomatisering

Hoe werkt deze tool?

De Security Check Procesautomatisering geeft bedrijven die gebruik maken van ICS of OT-apparaten inzicht in de veiligheid van hun procesautomatisering. Stel je voor: doe je genoeg aan de veiligheid van deze systemen? Dat hangt af van hoe ernstig de gevolgen zijn op het moment dat er een cyberincident optreedt. Zijn de gevolgen zwaaijg voor bijvoorbeeld de gezondheid, bedrijfscontinuïteit of milieu, dan wordt je geacht meer maatregelen te treffen. Valen de gevolgen mee, dan ligt de lat lager. De zelfscan start met deze inventarisatie.

Wat levert het op?

Het resultaat van de zelfscan is een praktische inventarisatie van maatregelen die jouw bedrijf nog moet nemen voor goed beschermde ICS en OT-apparaten. Behoud naar de weerbaarheid van je ICS en OT Doorloop in ongeveer 10 minuten deze gratis zelfscan en ontvang meteen een handige checklist van nog te nemen beveiligingsmaatregelen.

Met dank aan

De Security Check Procesautomatisering is ontwikkeld door de Vereniging van Nederlandse Gemeenten, het Nationaal Cyber Security Centrum, Programma Versterking Cyberweerbaarheid in de watersector, Siemens, ANSL, Deloitte, Novelt, Accertus, Stank Innovatie en het Digital Trust Center, met dank aan de ondersteuning van de Cybersecurity Alliantie.

Meer weten over de toestand? Komt van deze ICS-toof? Lees het nieuwsbericht over de lancering via deze link:

> Nieuwsbericht Lancering van Security Check Procesautomatisering

Handige links voor ICS beveiliging:

Meer weten om je ICS en OT-apparaten te beveiligen? Via hebben een aantal handige links voor je verzameld zodat je meteen aan de slag kunt met het verhogen van de veiligheid van je onderneming.

> Aan de slag met ICS security

Heeft deze informatie je geholpen?



Novel T

SIEMENS

Deloitte.

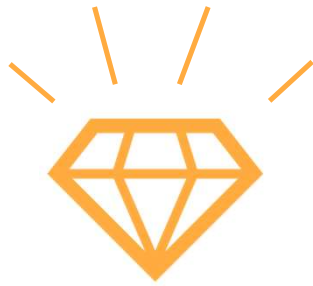


ORGANISATIE

NovelT



1



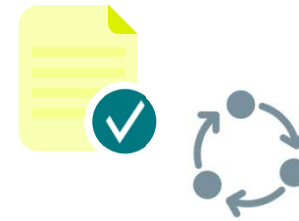
Kroonjuwelen in kaart

2



Risicomanagement

3



Beleid en proces

Beschikbaarheid
(hoe erg is het dat een systeem
het niet meer doet?)

Integriteit
(hoe erg is het dat bepaalde
gegevens niet juist zijn?)

Betrouwbaarheid
(hoe erg is het dat gegevens naar
buiten lekken?)

Kans

	Impact				
	niet merkbaar	klein	gemiddeld	groot	desastreus
dagelijks	gemiddeld	hoog	hoog	kritiek	kritiek
wekelijks	gemiddeld	gemiddeld	hoog	kritiek	kritiek
maandelijks	laag	gemiddeld	hoog	hoog	kritiek
jaarlijks	laag	gemiddeld	gemiddeld	hoog	hoog
> jaarlijks	laag	laag	gemiddeld	gemiddeld	hoog



Cybersecurity Dreigingsbeeld Zorg 2021



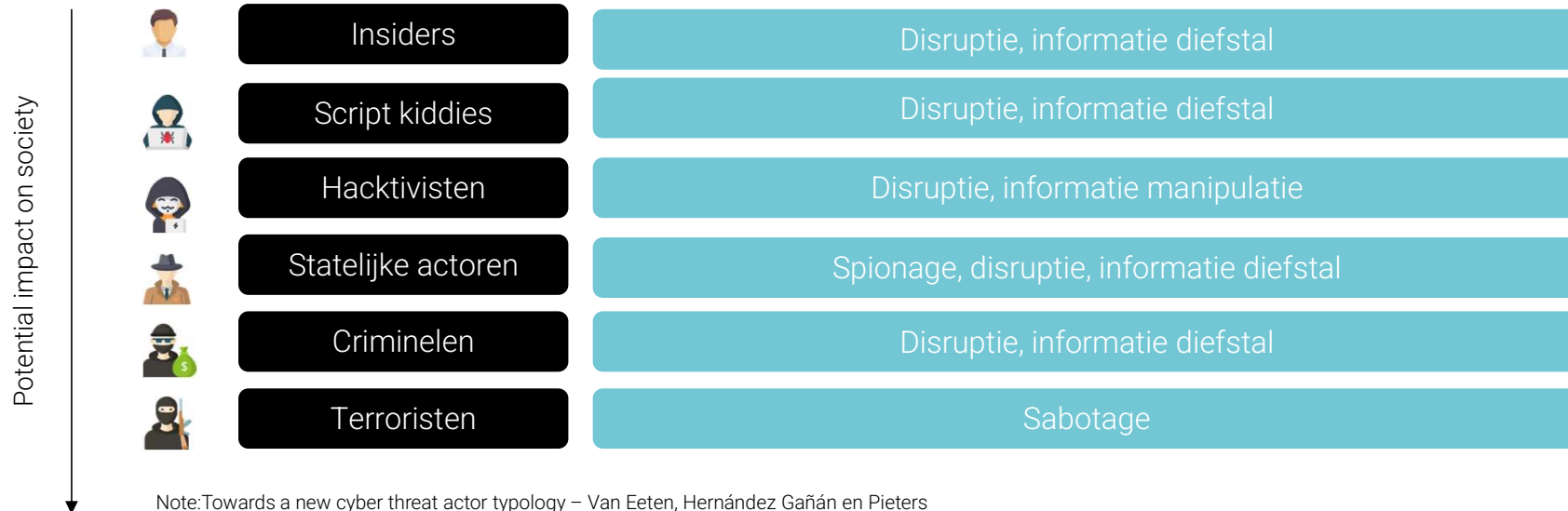
COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG





Inhoud

Colofon	4
Voorwoord Wim Hafkamp	5
Dreiging Ransomware	6
Thema Het risico van de cloud	14
Column Daan Brinkhuis	16
Dreiging Datalekken	18
Dreiging DDoS	22
Tien gouden tips tegen ransomware	24
Column Mark Janssen	26
Dreiging Fraude	28
Dreiging Cyberspionage door statelijke actoren	32
Thema Log4j	34
Samenvatting	36
Bibliografie	40



AFSPRAKEN MET JE IT

NovelT



Bespreek digitale veiligheid met jouw IT-dienstverlener

Jouw bedrijf is afhankelijk van digitale systemen zoals software en websites. Als bedrijf is het belangrijk om je eigen data en systemen en de data van je klanten goed te beschermen. Een bestaande of toekomstige IT-dienstverlener is daarin een belangrijke partner.

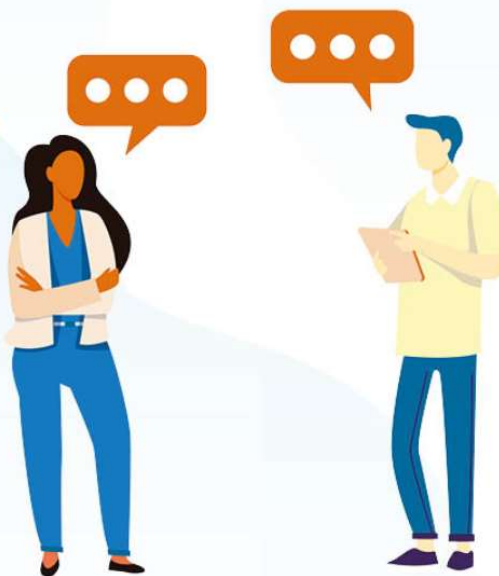
Het uitbesteden van IT betekent niet automatisch dat digitale veiligheid geregeld is. De bescherming van jouw data en continuïteit van jouw bedrijfsprocessen, is een gezamenlijke verantwoordelijkheid. Om duidelijk te krijgen waar de verantwoordelijkheden liggen zal je in gesprek moeten gaan en blijven met je IT-dienstverlener.

Door in gesprek te blijven met je IT-dienstverlener krijg je inzicht in:

- Afspraken over rollen en verantwoordelijkheden
- De volledigheid van de IT-dienstverlening
- Potentiële aanpassingen die nodig zijn
- De verdeling van verantwoordelijkheden voor digitale veiligheid

In gesprek blijven met jouw IT-dienstverlener over digitale veiligheid is belangrijk maar waar begin je? Zie ommezijde voor de onderwerpen die kunnen helpen als leidraad in het gesprek.

Deze praatplaat is een initiatief van en mogelijk gemaakt door Cybersecurity Alliantie



Belangen van jouw bedrijf

✓ Ga na welke data en bedrijfsprocessen belangrijk zijn voor jouw bedrijf. Bespreek met je IT-dienstverlener welke processen en data beschermd moeten worden.

⌚ Risico's kunnen op basis van dat gesprek worden geïdentificeerd.

Resultaat:

Gezamenlijk beeld van digitale dreigingen



Maatregelen tegen digitale dreigingen

Noodzakelijke digitale veiligheid maatregelen kunnen verschillen op basis van specifieke belangen voor jouw bedrijf.

Vraag je IT-dienstverlener welke maatregelen zij nemen en waarom. Bespreek tenminste de volgende maatregelen:

✓ Back-up - Hoe gaat jouw IT-dienstverlener met back-ups om?

⌚ Heb je een automatische back-up?
Een back-up kan je laatste redding zijn. Dat kan alleen als hier van te voren goed over nagedacht is. Zo moet een back-up de juiste data bevatten, veilig worden opgeslagen en in geval van een incident moet je er tijdig over kunnen beschikken.

✓ Updates - Hoe gaat jouw IT-dienstverlener om met updates?

⌚ Installeert jouw IT-dienstverlener de updates tijdig?
Het tijdig installeren van beveiligingsupdates is belangrijk voor de veiligheid en het functioneren van jouw software. Bespreek met jouw IT-dienstverlener hoe zij er voor zorgen dat alle systemen op tijd en juist worden geüpdatet.



Rapportage

✓ Vraag de IT-dienstverlener om structureel een rapportage te leveren van de dienstverlening.

⌚ Hoe vaak ontvang jij een rapportage van jouw IT-dienstverlener?
Deze rapportages geven jou de mogelijkheid te controleren, bij te sturen en input te geven in een volgend gesprek. Zo'n rapportage bevat minimaal de genomen maatregelen (back-ups, updates etc.) en het effect hiervan over een bepaalde tijd.

Resultaat:

Controle en verantwoording



Inventariseren verantwoordelijkheid

✓ Wat houdt de dienstverlening in, waar ben je zelf verantwoordelijk voor en welke verantwoordelijkheden liggen bij jouw IT-dienstverlener? Zijn die verantwoordelijkheden voldoende om je bedrijf digitaal veilig te houden?

⌚ Het is belangrijk om een beeld te hebben van de verantwoordelijkheden van jouw IT-dienstverlener en inzicht in wie wat doet.

Resultaat:

Overzicht dienstverlening en verantwoordelijkheden



✓ Wachtwoordbeleid - Welk wachtwoordbeleid wordt er door jouw IT-dienstverlener gehanteerd?

⌚ Heb jij al tweefactorauthenticatie ingesteld?
Toegang tot systemen en software moet worden beheerd om basale veiligheid te garanderen. Bespreek tweefactorauthenticatie om ongewenste indringers buiten jouw netwerk te houden.

✓ Antivirus - Welk antivirus beleid hanteert jouw IT-dienstverlener?

⌚ Hoe voorkomt jouw IT-dienstverlener geïnfecteerde computers door een virus? Bescherming tegen malware software, beter bekend als 'malware' is actueel. Denk bijvoorbeeld aan ransomware aanvallen. Bespreek met je IT-dienstverlener hoe zij jouw bedrijf beschermen en hoe ze dit monitoren.

Resultaat:

Basismaatregelen

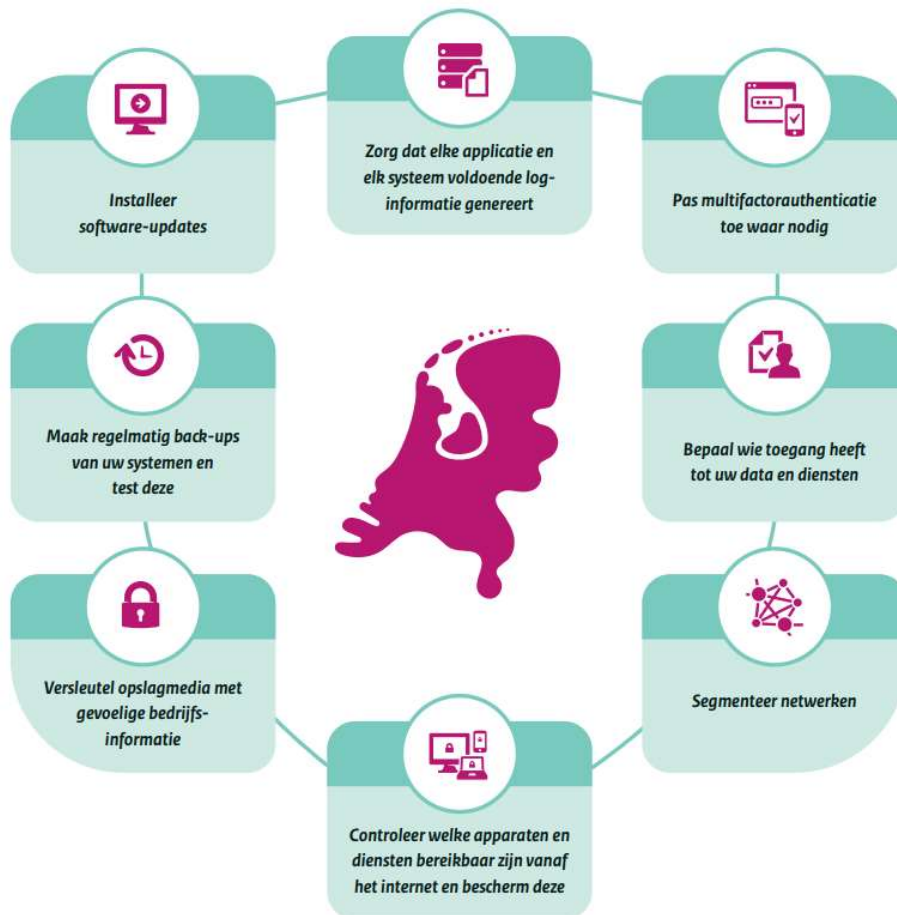
Wil je meer weten over digitale veiligheid, bezoek dan de website van het DTC: [digitaltrustcenter.nl](https://www.digitaltrustcenter.nl).

digital trust
center.

<https://www.digitaltrustcenter.nl/gesprek-met-it-dienstverlener>

TECHNIEK

NovelT



Er zijn veel informatieve kennisproducten (zie bijv. <https://www.ncsc.nl/documenten> en <https://www.digitaltrustcenter.nl/informatie-advies>)

Cybersecuritybedrijven kunnen passend advies geven over benodigde maatregelen

BRON:
file:///C:/Users/liesb/Downloads/NCSC+Cybersecuritymaatregelen+def.pdf

MENS

1



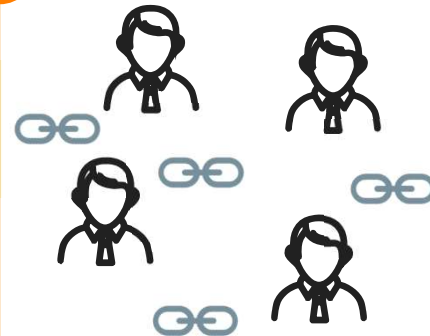
Positieve cultuur

2



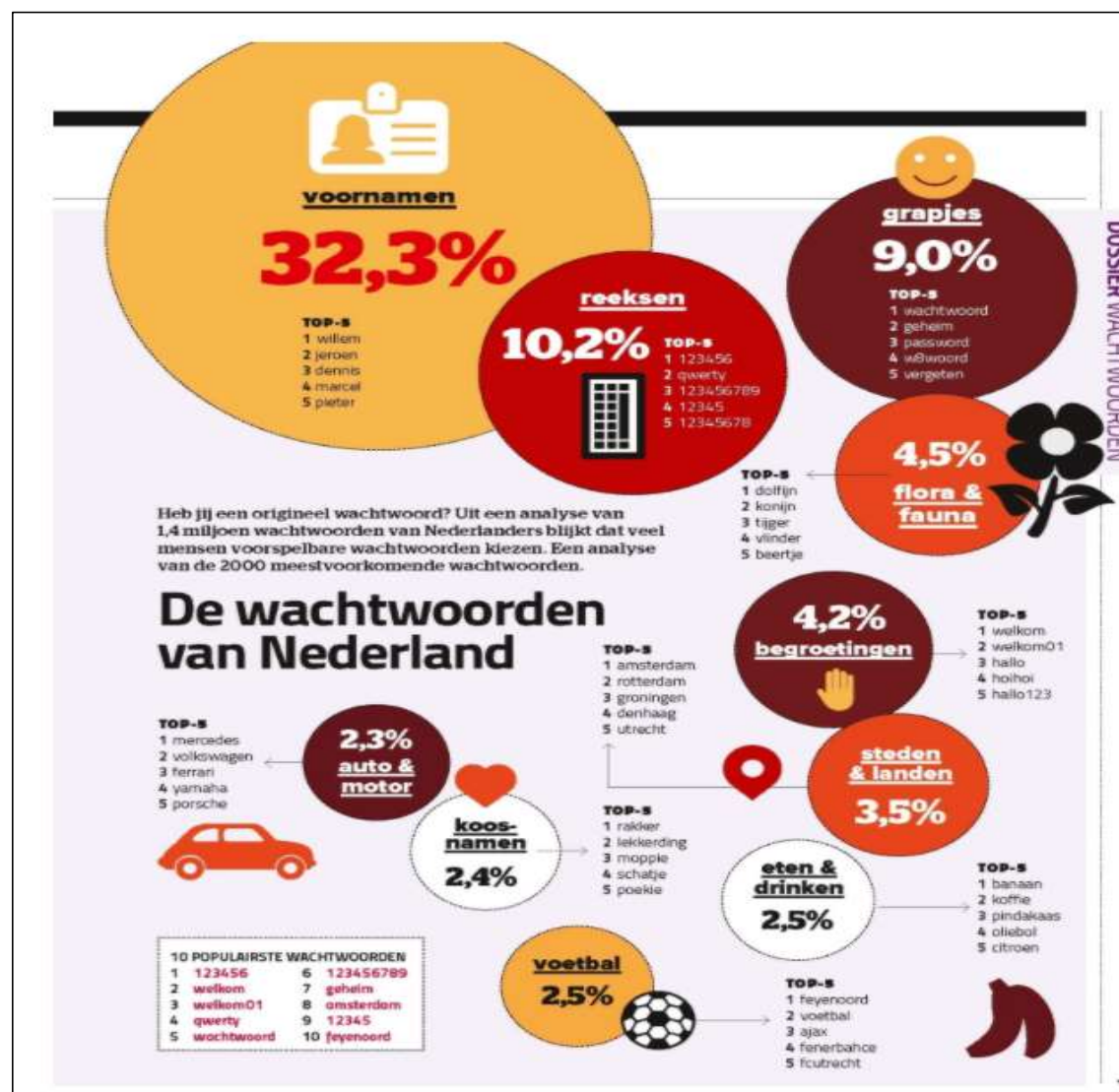
Awareness

3



Trainen crisis

Novel T



Beantwoord de volgende vragen

1 Hoe lang is jouw wachtwoord? (Tel alle letters, cijfers en/of andere tekens op.)



5 karakters

2 Welke karakters staan er in jouw wachtwoord? (Meer opties mogelijk.)



Kleine letters (a-z)



Hoofdletters (A-Z)



Cijfers (0-9)



Speciaal (#,&,!)



OMG! Directe hack! Jouw wachtwoord is in 1 minuut gekraakt!

Je loopt gevaar! Met een veel te kort wachtwoord ben je direct te hacken en liggen je persoonlijke bestanden, bank- en inloggegevens in feite op straat...Je wachtwoord moet echt veel langer, minimaal 12 karakters, liefst nog langer.

<https://veiliginternetten.nl/wachtwoordkraak-test/>

NovelT



Home

Notify me

Domain search

Who's been pwned

Passwords

API

About

Donate 

';--have i been pwned?

Check if your email or phone is in a data breach

pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](https://1password.com)

[Why 1Password?](#)

<https://haveibeenpwned.com/>

AANDACHTSPUNTEN...

Gebaseerd op de uitvoering van ongeveer 75 cybersecurity scans bij bedrijven in Overijssel (variërend tussen 12 en 200 FTE)

- IT-beheer vaak uitbesteed, maar zonder afspraken
- Geen rollen en verantwoordelijkheden vastgesteld
- Patchen (updaten) blijft aandachtspunt
- Back-up (ook productie-omgeving) wordt vaak vergeten
- Digitalisering productieomgeving in de kinderschoenen
- Weinig afspraken in de supply-chain
- Geen 2-factor authenticatie ingesteld

CALL TO ACTION

- Deel ervaringen met elkaar. Een incident kan grote impact hebben
- Denk na over je kritische assets en neem maatregelen
- Weet waar je afhankelijkheden in de keten zitten: maak afspraken
- Zorg dat iedereen in en buiten de organisatie weet wie waarvoor verantwoordelijk is
- Train je medewerkers

VRAGEN, OPMERKINGEN, SUGGESTIES?

Liesbeth Holterman

E-mail: l.holterman@novelt.com

Website: novelt.com/cybersecurity

Tel: +31(0)6 36 26 89 57

Henk van Ee

E-mail: h.m.vanee@saxion.nl

Website: saxion.nl

Tel: +31(0)6 22 67 48 04