Cybersecurity:
(N)iets voor mij?

NLdigital

FME

▲ 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

CYBERVEILIG NEDERLAND

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Novel T

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

deVolkskrant

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

Het is treurig gesteld met cyberveiligheid

Twentse bedrijven zijn een makkelijke prooi voor hackers

Vrijwel geen van de veertig Twentse maakbedrijven heeft de cybersecurity op orde. Dat blijkt uit een vrijwillig onderzoek naar de beveiliging tegen hackers. Af en toe was er sprake van grote gaten in de beveiliging, soms van kleine tekortkomingen. Maar een muizengaatje in het it-netwerk is vaak al voldoende voor grote schade.

regionale bedrijven die in de achterliggende twee jaar te maken kregen met cybercrime. Maar wat er in de publiciteit komt is een topje van de ijsberg. Holterman: „Veel ondernemers schamen zich, voelen zich een zukkel. Als we die

'Pas als ik €100.000 zou betalen, kreeg ik mijn bestanden terug'

Frits Conijn, Stijn van Gils

Cyberoplichters vormen een enorme schadepost voor ondernemers. Hoe kunnen ze hun digitale veiligheid verbeteren? Drie ondernemers vertellen over een hack en de schade.

▲ Door de persoonsgegevens van alle kinderen en jongeren uit de gemeente Aalten naar een verkeerd mailadres te sturen, is die informatie mogelijk op straat komen te liggen. © Getty Images/fStop

Gigantisch datalek in Aalten: persoonlijke gegevens van 5.500 kinderen liggen op straat

BNR Nieuws Radio Programma's & Podcasts Partners

Technologie • 18 nov '22 08:47

Cybercrime kost bedrijfsleven veel meer dan in andere landen

Auteur: Jorn Lucas

De financiële schade van cybercrime is voor een Nederlands bedrijf veel hoger in vergelijking met bedrijven in andere landen. Uit onderzoek van IT-beveiliger ESET Nederland kost een cyberincident bij een mkb-bedrijf in Nederland gemiddeld zo'n 270.000 duizend euro, een halve ton meer dan het wereldwijde gemiddelde.

VDL HOME VDL GROEP VDL-BEDRIJVEN WERKEN BIJ VD

VDL Groep weer in bedrijf na cyberaanval

8 november 2021

Nadat VDL Groep op donderdag 7 oktober zelf heeft bekendgemaakt doelwit te zijn van een cyberaanval, maakt het industriële familiebedrijf met het hoofdkantoor in Eindhoven vandaag bekend dat zijn 105 werkmaatschappijen vrijwel volledig in bedrijf zijn. Door 'schone' data uit de tijdig veiliggestelde back up-omgeving terug te plaatsen, zijn lokaal digitaal veilige omgevingen gecreëerd en hebben alle VDL-bedrijven hun productieactiviteiten steeds verder weten te herstellen. Door adequaat optreden van onze medewerkers is de schade beperkt gebleven tot maximaal één dag verlies aan data.

tweakers Nieuws Reviews Pricewatch Vraag & Aanbod Forum TweakersGear Mee

Zoek naar nieuws

Wat zijn de beste smartphones van dit moment?
Lees onze Smartphone Best Buy Guide

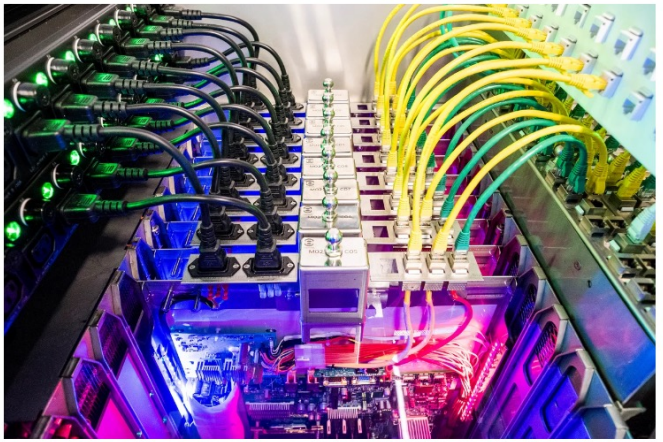
Gemeente Buren: Daders ransomwareaanval gebruikten gestolen inloggegevens

De Gelderse gemeente Buren heeft woensdag de oorzaak van de ransomwareaanval in april bekendgemaakt. De daders hebben gestolen inloggegevens van de softwareleverancier gebruikt om binnen te komen in het systeem van de gemeente.

Het onderzoek naar de aanval is deze week afgerond. Daaruit bleek dat de hackers gestolen inloggegevens van de softwareleverancier gebruikten om in te breken en de ransomware te installeren. Op het account dat de criminelen gebruikten stond geen tweestapsverificatie geactiveerd, meldt de gemeente. Om welke softwareleverancier het gaat, zegt de gemeente niet.

VERDIEPING DUURZAAMHEID&ECONOMIE RELIGIE&FILOSOFIE OPINIE C

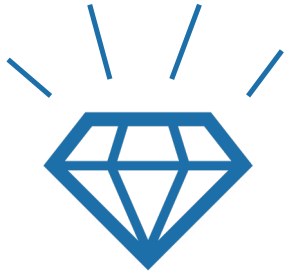
Een zwak wachtwoord legde de gemeente Hof van Twente plat



Beeld Patrick Post

Wat zijn je kwetsbaarheden

1



Kroonjuwelen in kaart

2

Risicomanagement

3

Beleid en processen

Welke data en systemen zijn cruciaal?

Beschikbaarheid

Hoe erg is het dat een systeem het niet meer doet?

WhatsApp, Instagram en Facebook komen weer online na storing - update 5

Chatdienst WhatsApp en sociale netwerken Facebook en Instagram komen langzaam maar zeker weer online na een grote storing. Daardoor konden gebruikers urenlang geen verbinding maken met deze diensten.

Ceo-fraude kostte Pathé 19 miljoen euro

Een mail met een geldverzoek voor een geheime overname kostte Pathétopvrouw Dertje Meijer en financieel directeur Edwin Slutter de kop - en het bedrijf 19 miljoen euro.

Integriteit

Hoe erg is het dat bepaalde gegevens niet juist zijn?

Betrouwbaarheid

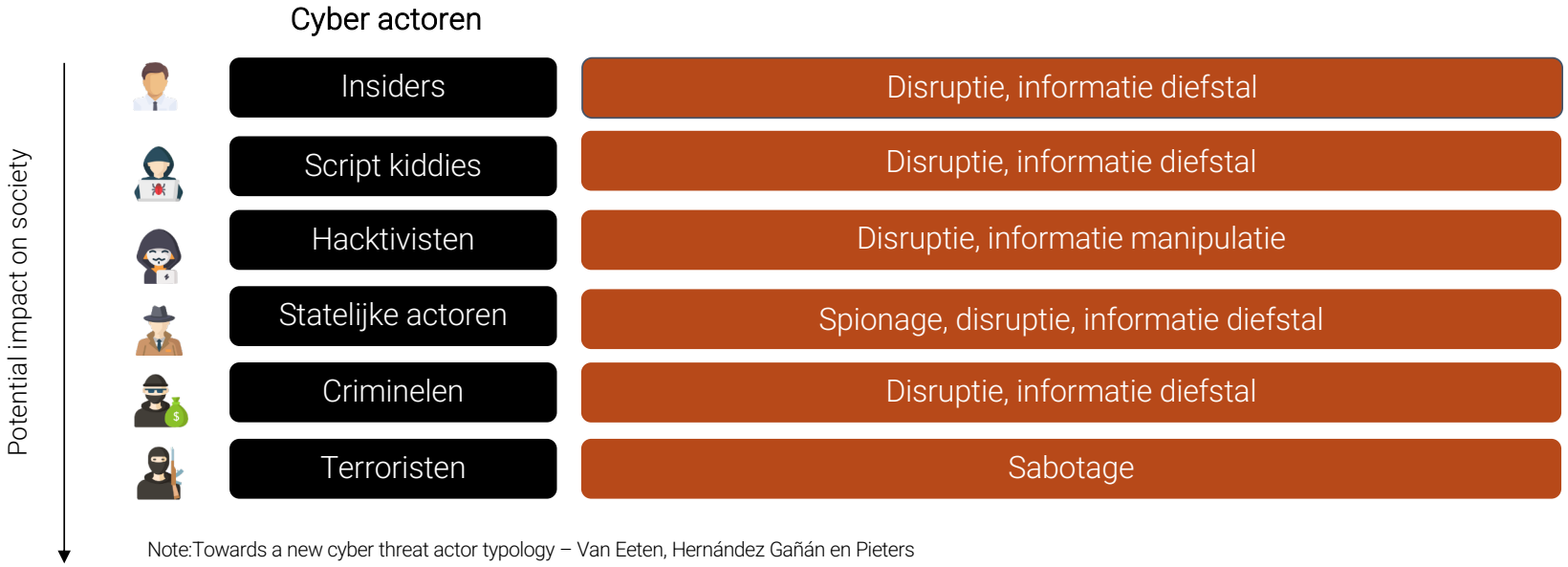
Hoe erg is het dat gegevens naar buiten lekken?

Zeven arrestaties

Datadiefstal GGD veel groter dan gemeld, gedupeerden niet geïnformeerd

12 augustus 2021 12:28
Aangepast: 12 augustus 2021 13:52

Wie willen ons “ kwaad doen”?



Note:Towards a new cyber threat actor typology – Van Eeten, Hernández Gañán en Pieters

Voorkom incidenten

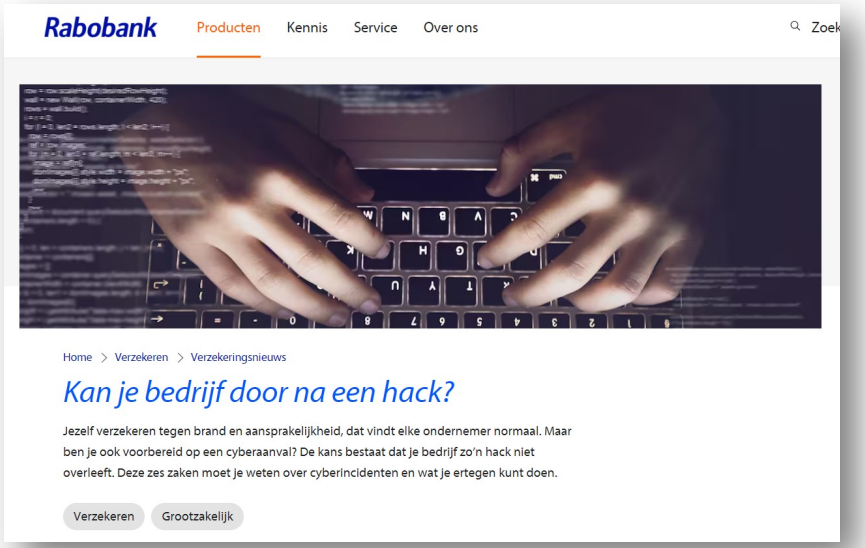
PREVENTIE
voorkom incidenten

2

Cyberincidenten

Doet je externe IT de juiste dingen?

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

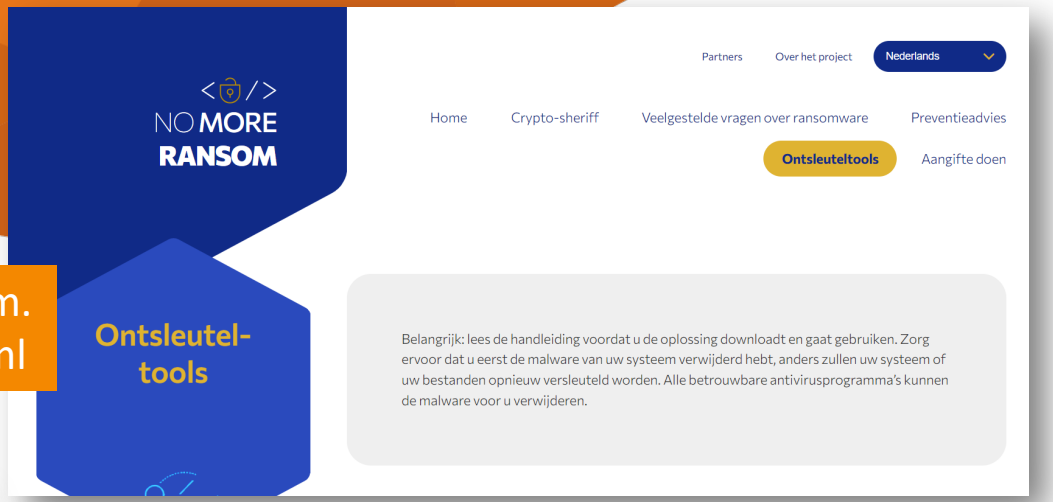


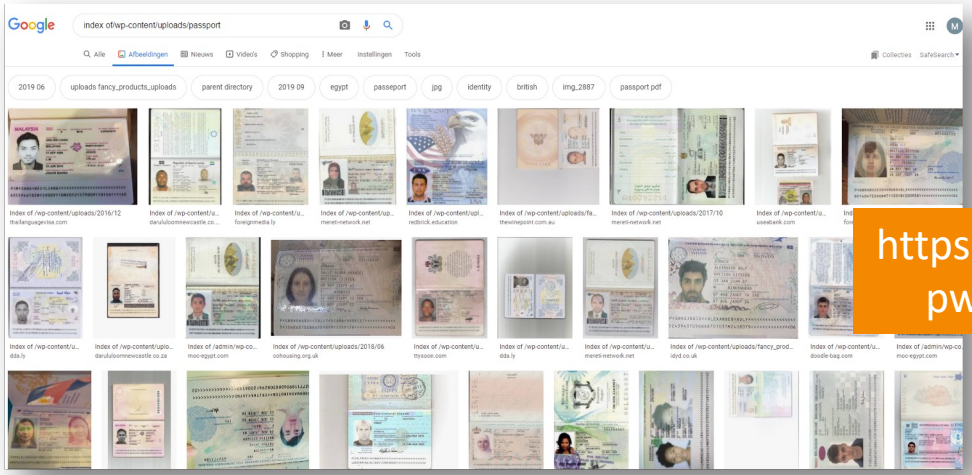
Train je medewerkers (en voed je bestuurder op!)

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

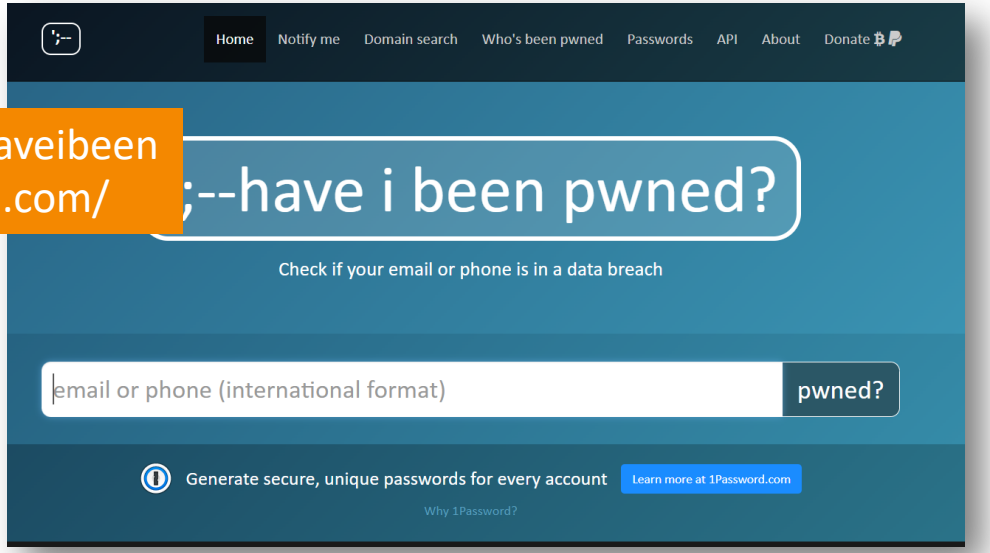
En jezelf!

https://www.nomoreransom.org/nl/decryption-tools.html





https://haveibeenpwned.com/



Onderken incidenten

PREVENTIE
voorkom incidenten

DETECTIE
detecteer incidenten

TIJD

Cyberincidenten

Reageer effectief op een incident

PREVENTIE	DETECTIE	RESPONS
voorkom incidenten	*detecteer incidenten*	*reageer effectief op incidenten*

Cyberincidenten

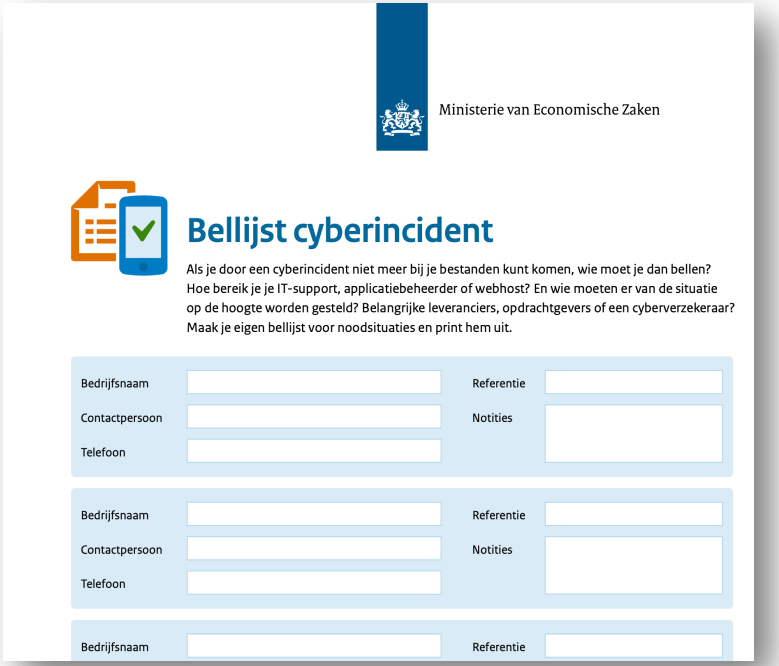
Voorbereid zijn op een (ransomware) incident

Zijn we voldoende in staat om een calamiteit het hoofd te bieden?

- [ ] Hebben we een goed functionerende crisisstructuur, inclusief escalatiemanagement en crisiscommunicatie met de woordvoeringslijn?
- [ ] Hebben we voor ogen welke groepen (keten)partners door incidenten kunnen worden geraakt en informeren we deze groepen tijdig en juist?
- [ ] Hebben we goed voor ogen welke partijen ons kunnen bijstaan bij het oplossen van cyberincidenten en hebben we goed contact met ze?
- [ ] Moeten we een cyberverzekering afsluiten?
- [ ] Voldoen wij aan wet- en regelgeving, zoals de Algemene verordening gegevensbescherming (AVG)[11] en de Wet beveiliging netwerk- en informatiesystemen (Wbni)[12]?

Zijn we voldoende in staat om van een calamiteit te herstellen?

- [ ] Hebben we onze herstelprocedures op orde en is dit onderdeel van ons Business Continuity Plan en/of Disaster Recovery Plan?
- [ ] Hebben we onze nazorg inclusief interne en externe communicatie op orde?
- [ ] Hebben we een goed evaluatieproces ingericht met het oog op 'lessons learned' en het doorvoeren van aanpassingen?
- [ ] Hebben we een proces ingericht dat zorgt voor aangifte bij de politie?



Ministerie van Economische Zaken

Bellijst cyberincident

Als je door een cyberincident niet meer bij je bestanden kunt komen, wie moet je dan bellen? Hoe bereik je je IT-support, applicatiebeheerder of webhost? En wie moeten er van de situatie op de hoogte worden gesteld? Belangrijke leveranciers, opdrachtgevers of een cyberverzekeraar? Maak je eigen bellijst voor noodsituaties en print hem uit.

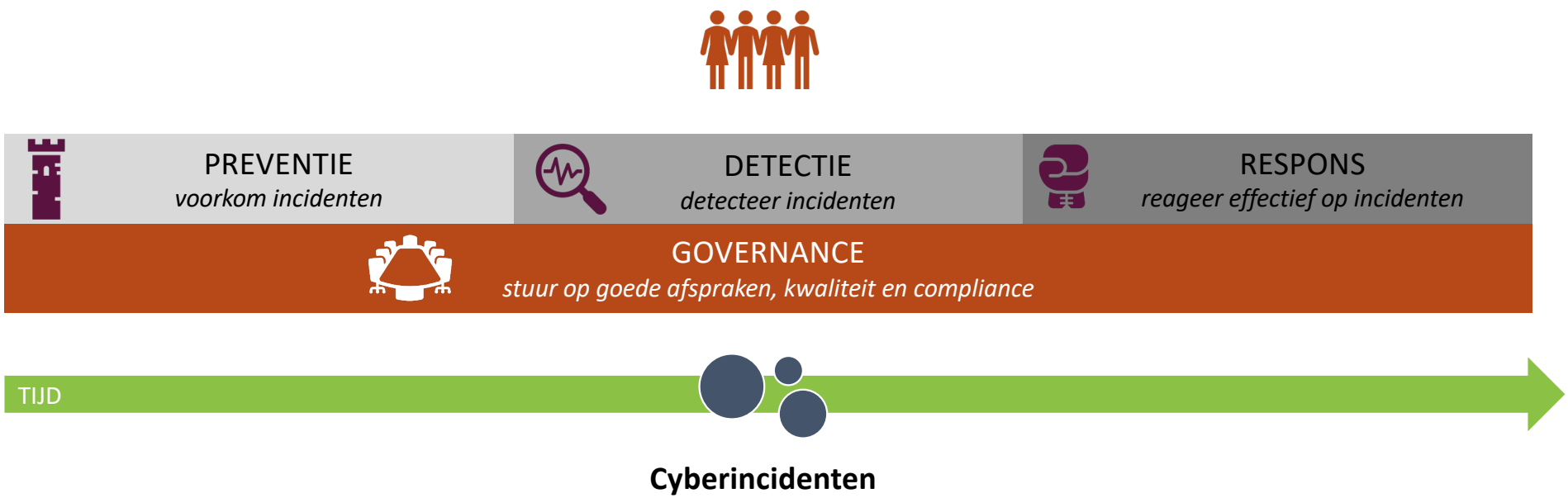
Bedrijfsnaam		Referentie	
Contactpersoon		Notities	
Telefoon			

Bedrijfsnaam		Referentie	
Contactpersoon		Notities	
Telefoon			

Bedrijfsnaam		Referentie	

https://www.digitaltrustcenter.nl/sites/default/files/2024-09/Bellijst_bij_cyberincident.pdf

Zorg voor duidelijke rollen en verantwoordelijkheden



Ransomware = ransom + software

Ransomware	...	*Gijzelsoftware*
Gijzelsoftware	Kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat zijn digitale systeem of de bestanden erop met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat hij er weer bij kan. Maar zelfs dat is niet zeker.	

De hoogste bazen in de wereld van cybercrime leggen zichzelf niet alleen maar in de watten, ze gebruiken de luxegoederen ook als marketinginstrument om anderen over te halen bij hen te komen werken. Wereldwijd horen rond de 80 procent van de *black hat*-hackers bij een georganiseerde groep.

De Russische groep was heel erg act[redacted]. De leden verwenden zichzelf met luxe vakanties naar bijvoorbeeld Monte Carlo en Bali.

"We hadden een foto van een van die mannen in een duikbril aan de muur hangen," vertelde Ryan McGeehan, die namens Facebook onderzoek deed, aan de *New York*

Een ander briljant verhaal gaat over de Russische groep Koobface, die Tanase een paar jaar geleden onderzocht.

"Ze vonden het gewoon heerlijk om 's ochtends wakker te worden van het geluid van geld. Elke ochtend kreeg elk lid een sms waarin stond hoeveel geld ze hadden verdiend in de afgelopen 24 uur," vertelde hij.

Ze kregen allemaal berichten rond 9-10 uur in de ochtend, behalve de baas, die hield niet van vroeg op staan. Hij kreeg zijn sms rond het middaguur.

Cybercriminaliteit: ransomware

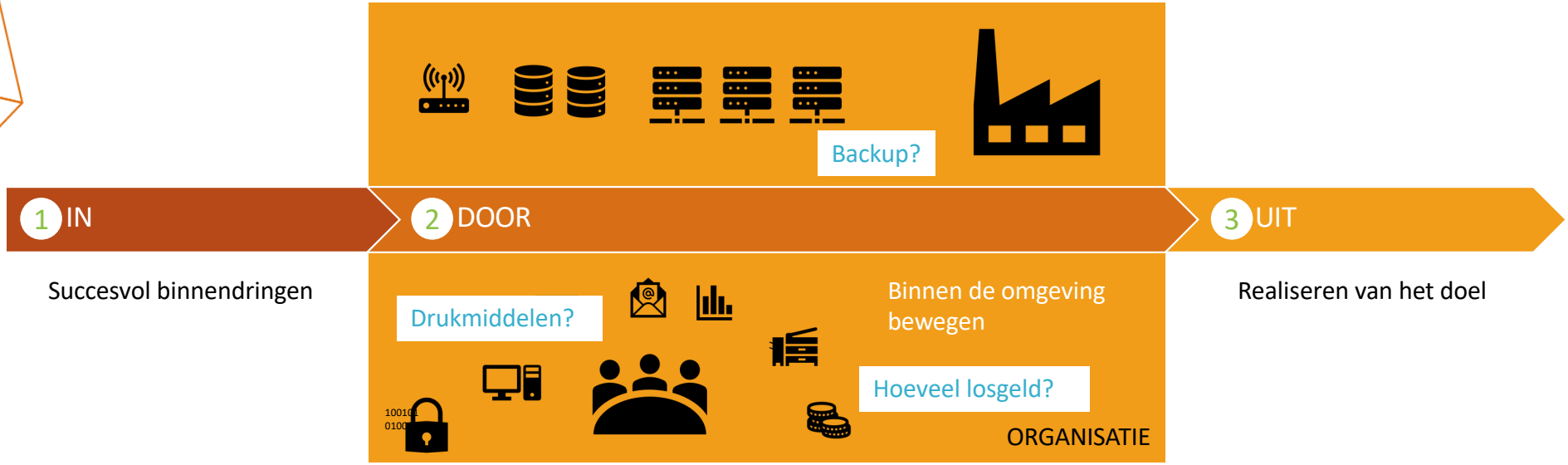
Een ransomware-aanval kent doorgaans drie fasen

Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

In de IN fase wordt handig gebruik gemaakt van actualiteit

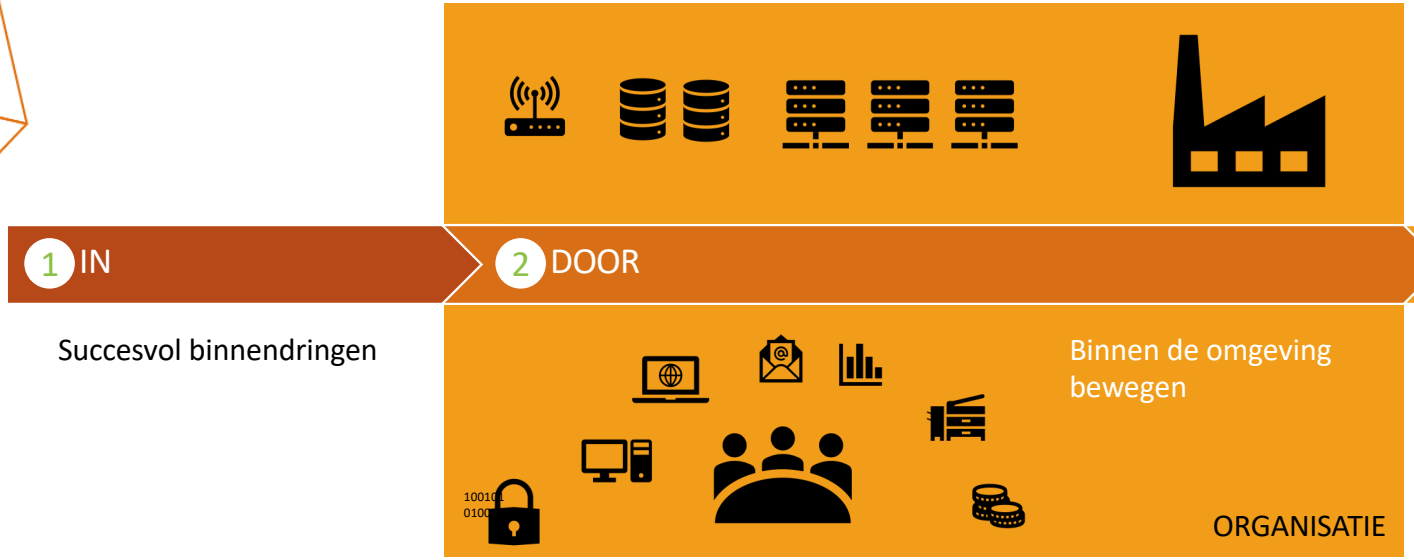
Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

In de DOOR fase wordt geprobeerd maximale toegang en informatie te verkrijgen



Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

De UIT fase bestaat voor ransomware uit twee stappen



1. Aanrichten van schade (versleutelen, backup vernietigen, gegevens stelen)
2. Afpersen van een slachtoffer (extortion)

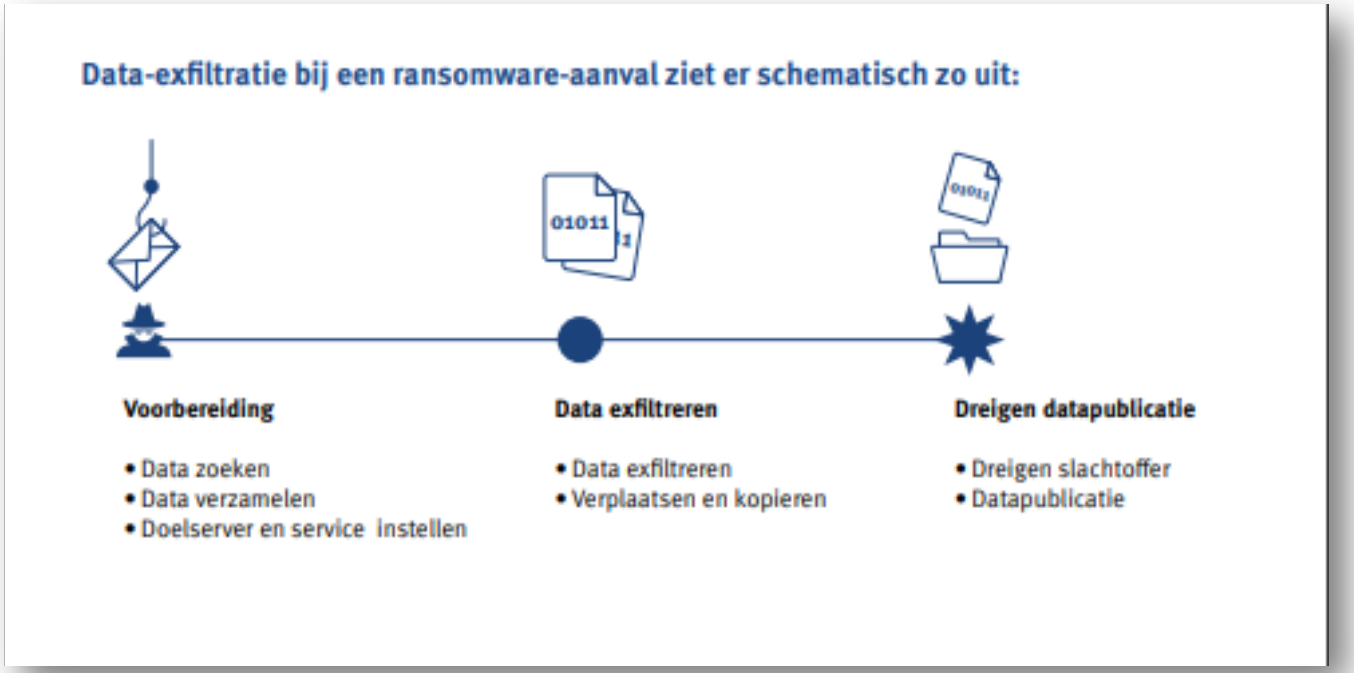
Vereenvoudigd model van de Unified Kill Chain - https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

Hoe te voorkomen?

	IN	DOOR	UIT
MENS	Awareness training	Positieve security cultuur	Training crisis-scenario's
ORGANISATIE	Wachtwoordbeleid Patch management	Kritieke processen beheren	Incident response plan
TECHNIEK	End point detection & response	Netwerksegmentatie Access control Network monitoring	Offline back-up (3-2-1 principe)

Er zijn veel informatieve kennisproducten (zie bijv. https://www.ncsc.nl/documenten en www.digitaltrustcenter.nl)
Cybersecuritybedrijven kunnen passend advies geven over benodigde maatregelen

Data-exfiltratie (datadiefstal) komt steeds meer voor



Data-exfiltratie is een proces tijdens een ransomware-aanval waarbij data wordt gestolen en eventueel openbaar gepubliceerd als het slachtoffer niet betaald. Het doel van aanvallers is dus om druk uit te oefenen op het slachtofferdeze data.

Voorkom datadiefstal

1. Zicht op je data:
- Gedeelde mappen op file servers
- Publieke cloudopslag providers (bijvoorbeeld Microsoft SharePoint)
- Back-up locaties
- Mailboxen van werknemers

2. Dataminimalisatie
- Verwijderen van data die niet meer nodig zijn.
- Het offline archiveren van data die niet dagelijks nodig zijn.
- Het offline halen van informatie die online beschikbaar is gemaakt.

3. Extra beschermen van data
- toegangsbeperking.
- Monitoring van je netwerk (SOC/SIEM)
- etc

https://www.cyberveilignederland.nl

Bij bedrijven ligt de losgeldeis vaak tussen de 0,4% en 2% van de jaaromzet

•Draagkracht is een belangrijk criterium voor de hoogte van de losgeldeis

Een aanval zorgt in het klein ook voor grote persoonlijke schade voor betrokkenen (baanverlies, privéproblemen, etc.)

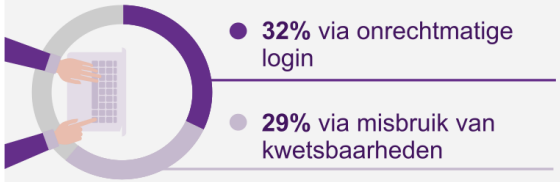
Ruim 30% was bereid losgeld te betalen

35% van de slachtoffers in 2023 had een downtime van meer dan een maand

Daarnaast zijn er nog kosten voor:

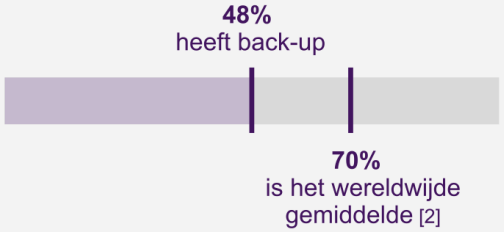
- Oplossen incident (communicatie, reputatieschade, etc.)
- Investeringen heropbouw en beveiligen netwerk
- Doorbetalen mensen en apparatuur
- Etc.

Ransomware-incidenten volgen de gebaande paden voor toegang



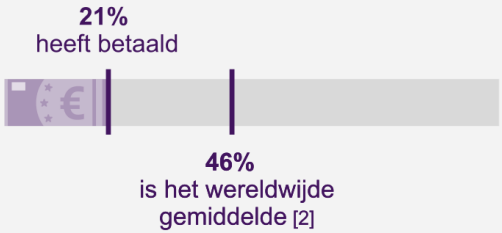
Ongeoorloofde toegang voorkomen? Zorg dus dat de basismaatregelen op orde zijn. [1]

Er zijn meer back-ups nodig



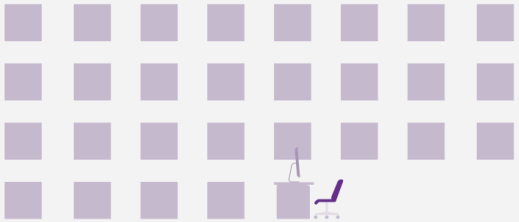
Jammer. Zorg voor goede back-up-strategie, zo kan je snel van incidenten herstellen. [3]

Betaalbereidheid binnen incidenten relatief laag



Positief! Want door niet te betalen geven we een sterk signaal tegen cybercriminelen. [4]

Dreiging vanuit groot aantal ransomware-families



Met **29** unieke ransomware-families is de dreiging opvallend breed. Informatiedeling en samenwerking is dus cruciaal.

https://cyberveilignederland.nl/upload/userfiles/files/Jaarbeeld_Ransomware_2023_Final_2.pdf

Voorbereid zijn op een incident

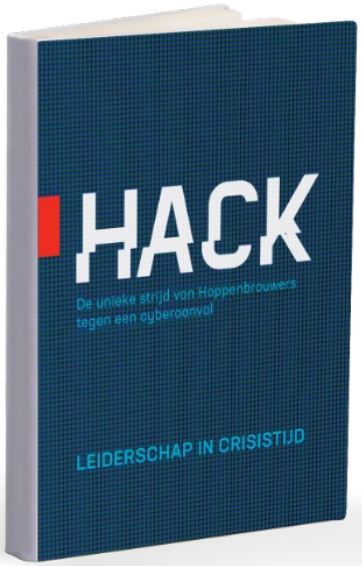
MITIGATIE
Analyse: wat is de aard, reikwijdte en impact van de aanval
Containment (inperking): zorgdragen dat de aanval zich niet verder over het netwerk verspreidt
Eradication (eliminatie): de dreiging volledig van het netwerk verwijderen
Recovery (herstel): de functionaliteit van het netwerk herstellen

Schakel waar nodig professionele hulp in

COMMUNICATIE (o.b.v. een plan)
Medewerkers
Stakeholders, ketenpartners, afnemers
Juristen
Autoriteit Persoonsgegevens
De pers
De politie

Wees waar mogelijk transparant naar de buitenwereld zodat anderen met deze informatie zich beter kunnen beschermen

Tenslotte: deel informatie (indien mogelijk) over incidenten



*"Om het groeiende probleem van ransomware de baas te kunnen worden, **is openheid over incidenten essentieel**. Veel bedrijven kiezen ervoor hierover te zwijgen, omdat ze vrezen voor reputatieschade. Of openheid reputatieschade veroorzaakt is echter nog maar de vraag. Bovendien kan openheid voor **meer bewustzijn** zorgen. Het delen van inhoudelijke informatie over incidenten draagt bovendien bij aan het **verhogen van de cyberweerbaarheid** van andere organisatie. Hopelijk bereiken we in de toekomst een situatie waarin het verzwijgen van incidenten leidt tot reputatieschade, maar zover zijn we helaas nog niet"*

Petra Oldengarm, directeur Cyberveilig Nederland in het voorwoord van Hack

Hopelijk bereiken we ooit de situatie dat een organisatie reputatieschade leidt door het verzwijgen van incidenten

Bron: https://www.cybersecurityraad.nl/binaries/Report_Scientific_Research_DBNO_20200211_DEF_tcm107-431346.pdf

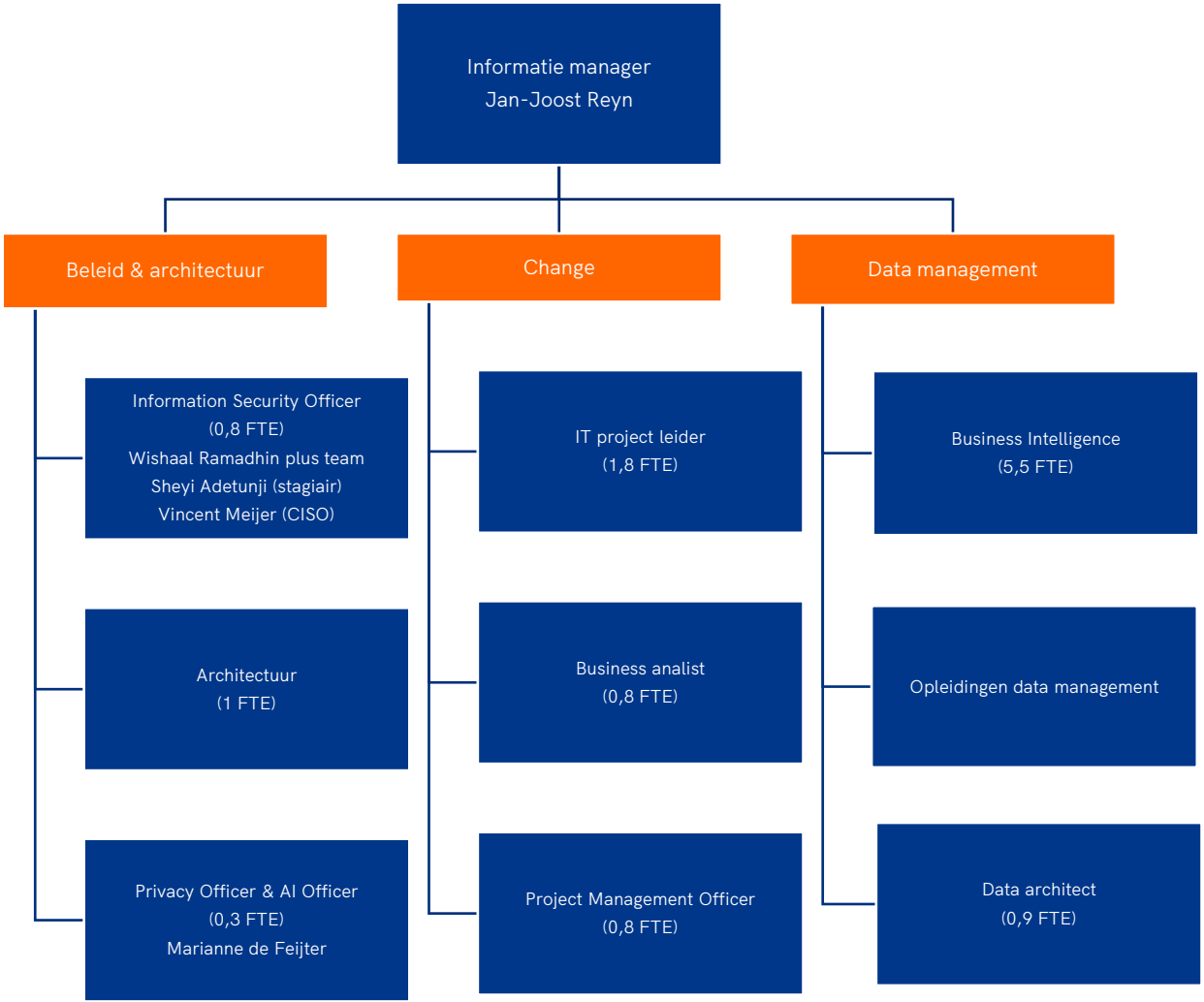
VRAGEN?

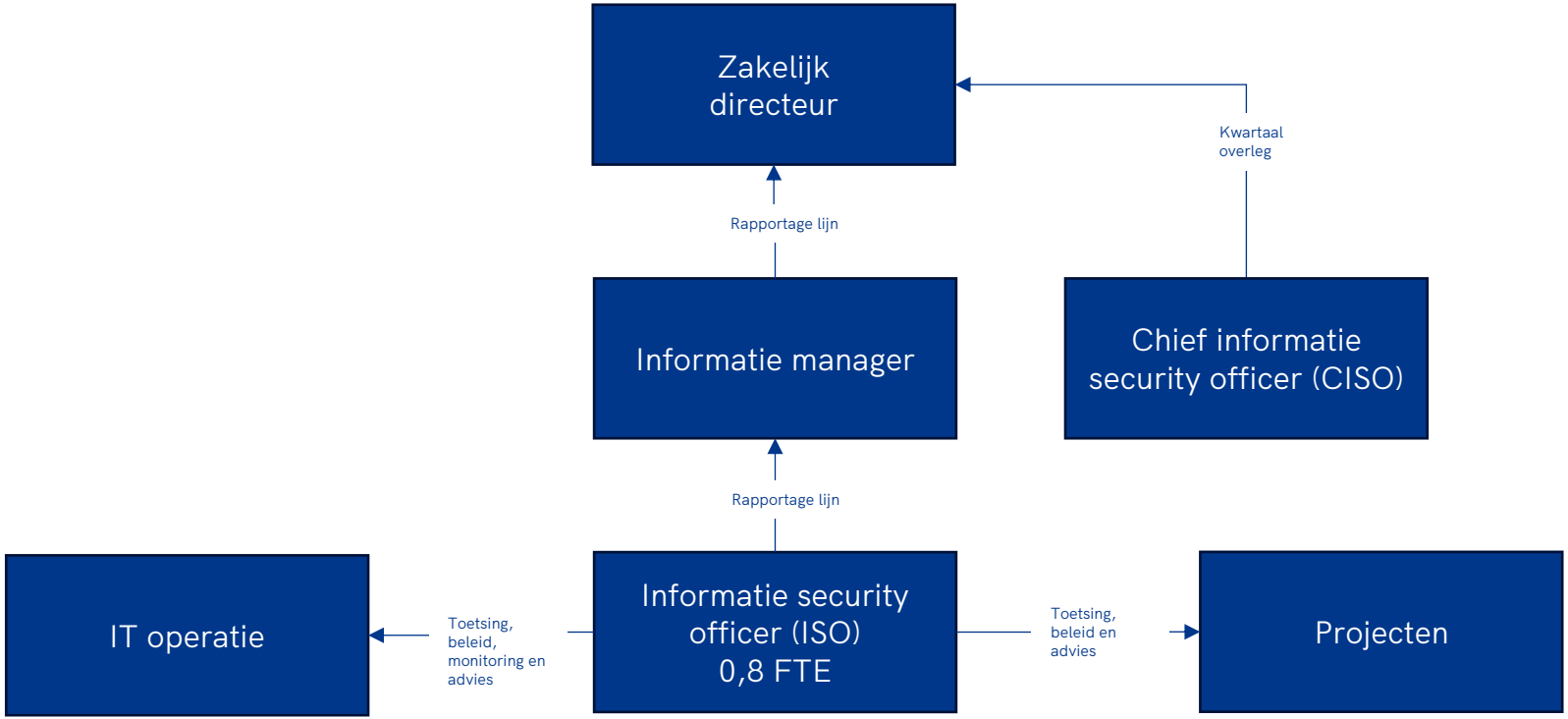
Liesbeth Holterman
info@konega.nl
06-36268957

Cybersecurity bij NOC*NSF

20 Maart 2025

#wewinnenveelmetsport

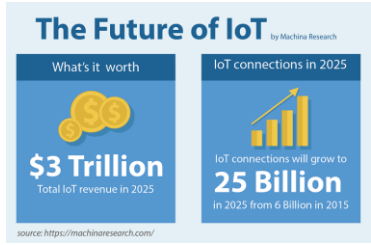

Informatie manager
Jan-Joost Reyn
Beleid & architectuur
Change
Data management
Information Security Officer
(0,8 FTE)
Wishaal Ramadhin plus team
Sheyi Adetunji (stagiair)
Vincent Meijer (CISO)
Architectuur
(1 FTE)
Privacy Officer & AI Officer
(0,3 FTE)
Marianne de Feijter
IT project leider
(1,8 FTE)
Business analist
(0,8 FTE)
Project Management Officer
(0,8 FTE)
Business Intelligence
(5,5 FTE)
Opleidingen data management
Data architect
(0,9 FTE)



avit CONNECTING IT SERVICES

cybertrust

EMERGING TECHNOLOGY




ATTACK ORIGINS
Country
599 United States
163 China
91 Netherlands
60 Canada
45 Hong Kong
33 France
25 Mil/Gov
21 Taiwan
19 Italy
16 Turkey
TARGET OF
OPPORTUNITY
OR
TARGET OF CHOICE
ATTACK TARGETS
Country
887 United States
51 Hong Kong
39 Spain
32 Thailand
28 Argentina
22 Canada
21 Norway
20 Portugal
17 Australia
17 Bulgaria
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-06-25 08:32:59.06 CHINANET-HN Hengyang Changsha, China 218.77.79.43 Kirksville, United States ms-term-services 3389
2014-06-25 08:32:59.97 LLC Kvazar Telecom unknown, Russia 195.254.186.227 Saint Louis, United States ssh 22
2014-06-25 08:32:59.98 Primesoft NZ LTD unknown, New Zealand 202.36.227.103 Saint Louis, United States unknown 52359
ATTACK TYPES
Service Port
328 http 80
77 domain 53
66 ms-term-services 3389

OLYMPIC CYBER THREATS TIMELINE TOWARDS PARIS

Olympic cyber assaults that affect athletes, coaches, attendees, even ordinary citizens have increased exponentially and reached **450 million** in the Tokyo Games, accompanied by a staggering **4.4 billion threats** – equating to approximately 800 threats per second. Experts foresee a **potentially escalated scenario** for the Paris 2024 Games and predict that attacks at Paris 2024 could be **eight to ten times greater** than those experienced in Tokyo.

2012

Officials hebben hun zorgen geuit over een mogelijke **cyberaanval gericht op de Openingsceremonie** van de Spelen in Londen 2012

Bovendien zijn bij de Olympische Spelen van 2012 in **Londen meer dan 212 miljoen cyberaanvallen** geconstateerd.

2014

Het Amerikaanse ministerie van Buitenlandse Zaken heeft een reiswaarschuwing uitgegeven. In de waarschuwing werd specifiek vermeld dat individuen **voorzichtig moeten zijn bij het delen van gevoelige of persoonlijke informatie** op Russische elektronische communicatienetwerken.

2016

Is het **doelwit geweest van een 540 Gbps DDoS-aanval**, naast andere cyberaanvallen.

2018

De nachtmerrie van de openingsceremonie werd werkelijkheid toen er een **aanval** gelanceerd werd op de **centrale systemen** van de organisatie om **chaos en verwarring** te veroorzaken.

Met behulp van de kwaadaardige worm **'Olympic Destroyer'** werd de officiële Olympische website offline gehaald.

2020

Er zijn maar liefst **4,4 miljard cyberdreigingen gelanceerd** tegen de event.

(**twintig keer hoger** dan het aantal gerapporteerde cyberaanvallen tijdens de Olympische Spelen in Londen)

2022

De officiële anti-Covid-19-applicatie, bekend als 'My2022', leidde tot controverse vanwege de veiligheid van deze applicatie en de **potentiële kwetsbaarheden voor spionagedoeleinden**.

2024

?

Massaal datalek: gevoelige informatie van duizenden Poolse atleten openbaar na hack bij antidopingagentschap

Hackers hebben meer dan 50.000 bestanden van het Poolse Antidopingagentschap (POLADA) gelekt, waardoor gevoelige gegevens van duizenden Poolse atleten zijn onthuld. Het gaat om medische dossiers en resultaten van antidopingtests.

Sam Vergauwen

Bron: Notes from Poland

Woensdag 14 augustus 2024 om 12:54

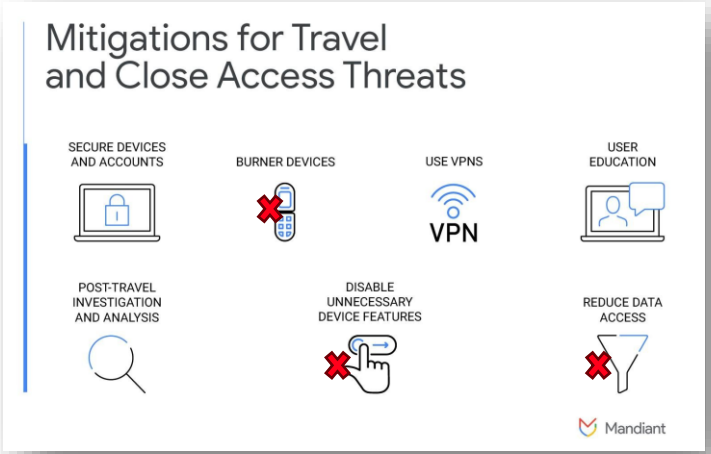
De groep haalde ook de website van POLADA neer. De hackers waarschuwden eerder al voor het aankomende lek op hun Telegram-kanaal, Beregini, dat in verband wordt gebracht met Russische desinformatiecampagnes.

"De Olympische Spelen zijn al lang een politiek onderdrukkingsinstrument geworden", schreven ze. "Daarom besloten we het voorbeeld van een van de EU-landen te gebruiken om te laten zien wat er echt gaande is in de antidopingagentschappen van landen die door de Verenigde Staten worden gecontroleerd en vonden we een hoop 'skeletten' in hun kast."

Bekende namen

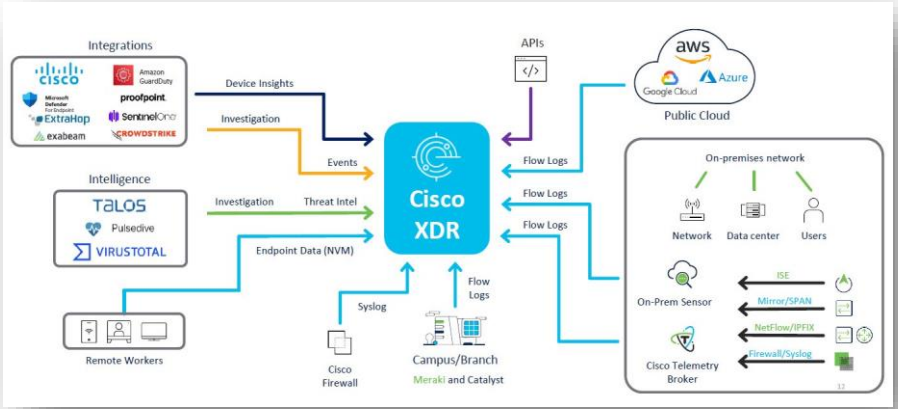
POLADA waarschuwde Poolse atleten voor het incident in een e-mail die later door de Poolse wielrenner Wojciech Pszczolarski op X werd gedeeld. In het bericht bood het agentschap zijn excuses aan voor het incident en verzekerde de atleten dat de wetshandhavingsinstanties en de autoriteit voor gegevensbescherming op de hoogte waren gesteld. POLADA bevestigde ook dat de gelekte documenten namen, huis- en e-mailadressen en telefoonnummers van atleten bevatten, waaronder die van voetballer Lewandowski en tennisster Swiatek.

Specifieke maatregelen



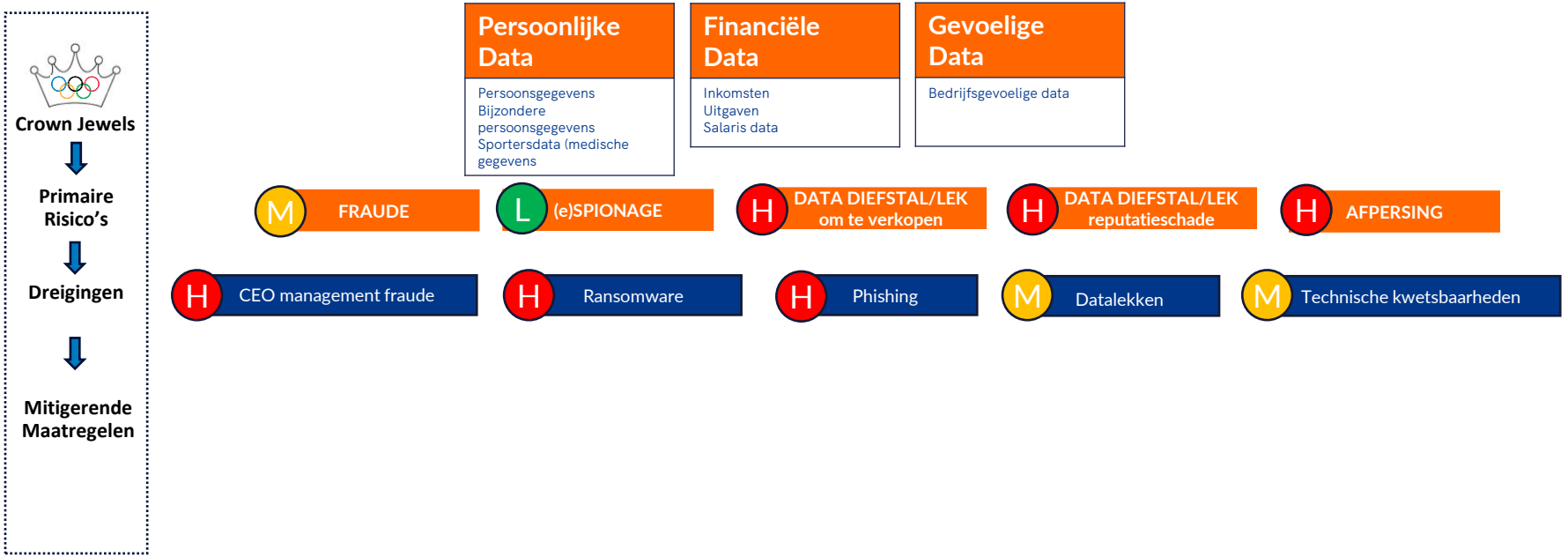
Calamiteiten plan

Incident response plan



CYBERSECURITY IN DE CONTEXT VAN NOC*NSF

Wat is ons risico?



CYBERSECURITY NOC*NSF 2024

*Phishing & Poging tot aanmelden NOC*NSF Netwerk*

Phishing

- **109 (maart) → 265 (nov.)**
  Phishing/Spam-emails ontvangen door NOC*NSF de afgelopen 30 dagen
- **45 (maart) → 97 (nov.)**
  Pogingen tot credentials phishing de afgelopen 30 dagen
- **19**
  Pogingen met randsomware
- **35%**
  Van de geadresseerde (268) hebben geklikt op de laatste phishing test (93 medewerkers)
- **13%**
  Van de geadresseerde (268) hebben geprobeerd in te loggen (35 medewerkers)

Poging tot aanmelden

1000
Succesvolle pogingen

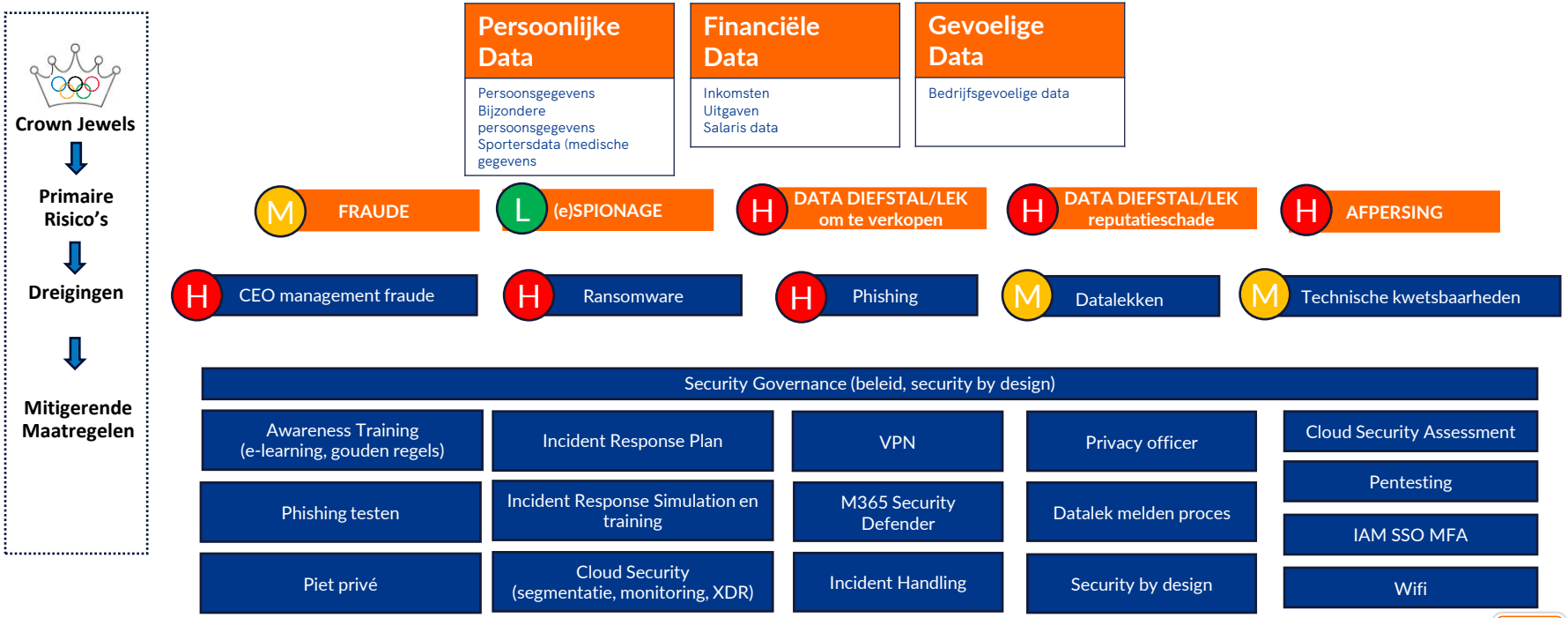
25 000
Niet succesvolle pogingen

1 security incident/ datalek

Hack

CYBERSECURITY IN DE CONTEXT VAN NOC*NSF

Wat is ons risico?



Security Governance (beleid, security by design)				
Awareness Training (e-learning, gouden regels)	Incident Response Plan	VPN	Privacy officer	Cloud Security Assessment
Phishing testen	Incident Response Simulation en training	M365 Security Defender	Datalek melden proces	Pentesting
Piet privé	Cloud Security (segmentatie, monitoring, XDR)	Incident Handling	Security by design	IAM SSO MFA
				Wifi

BIO | Baseline Informatiebeveiliging Overheid

Clember

NOC*NSF