
UNO
LEADING
YOUR
DIGITAL JOURNEY

UNO | LEADING YOUR DIGITAL JOURNEY

UNO Event | **Donderdag 30 oktober op het UNO Hoofdkantoor**

Business Continuity Management

"Ik ben gehackt, en nu?"

Gastsprekers:

Anouk van der Zanden & Ronald van der Meulen

UNO | LEADING YOUR DIGITAL JOURNEY

Programma

- **Introductie**

Floris Weij, Teammanager Customer Success en Productowner Cybersecurity bij UNO

- **De gevolgen van een geslaagde Ransomware aanval (14.15 – 15.15)**

Anouk van der Zanden, Adviseur ICT bij Laurentius

- **Pauze(15.15 – 15.30)**

15 minuten

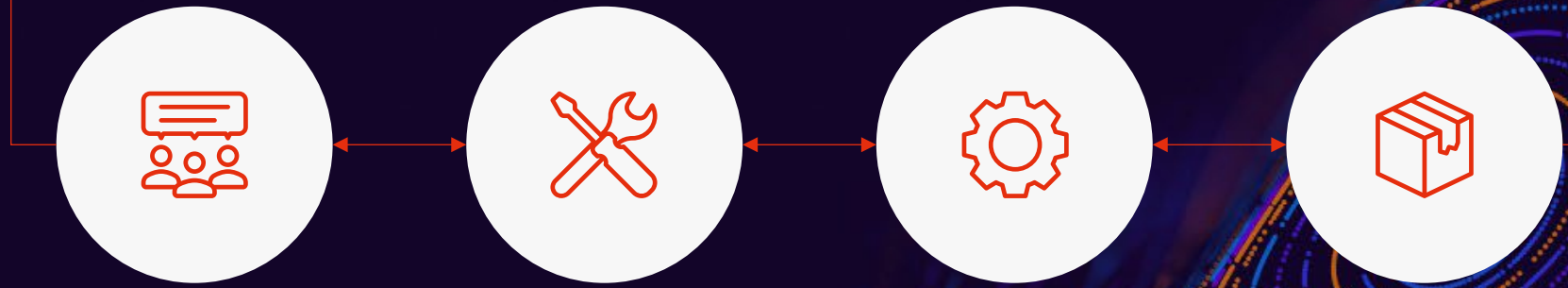
- **BCM vanuit CISO perspectief – (15.30 – 16.15)**

Ronald van der Meulen, Eigenaar Takeshape & A.I. CISO

- **Borrel (16.15 – 18.00)**

UNO | LEADING YOUR DIGITAL JOURNEY

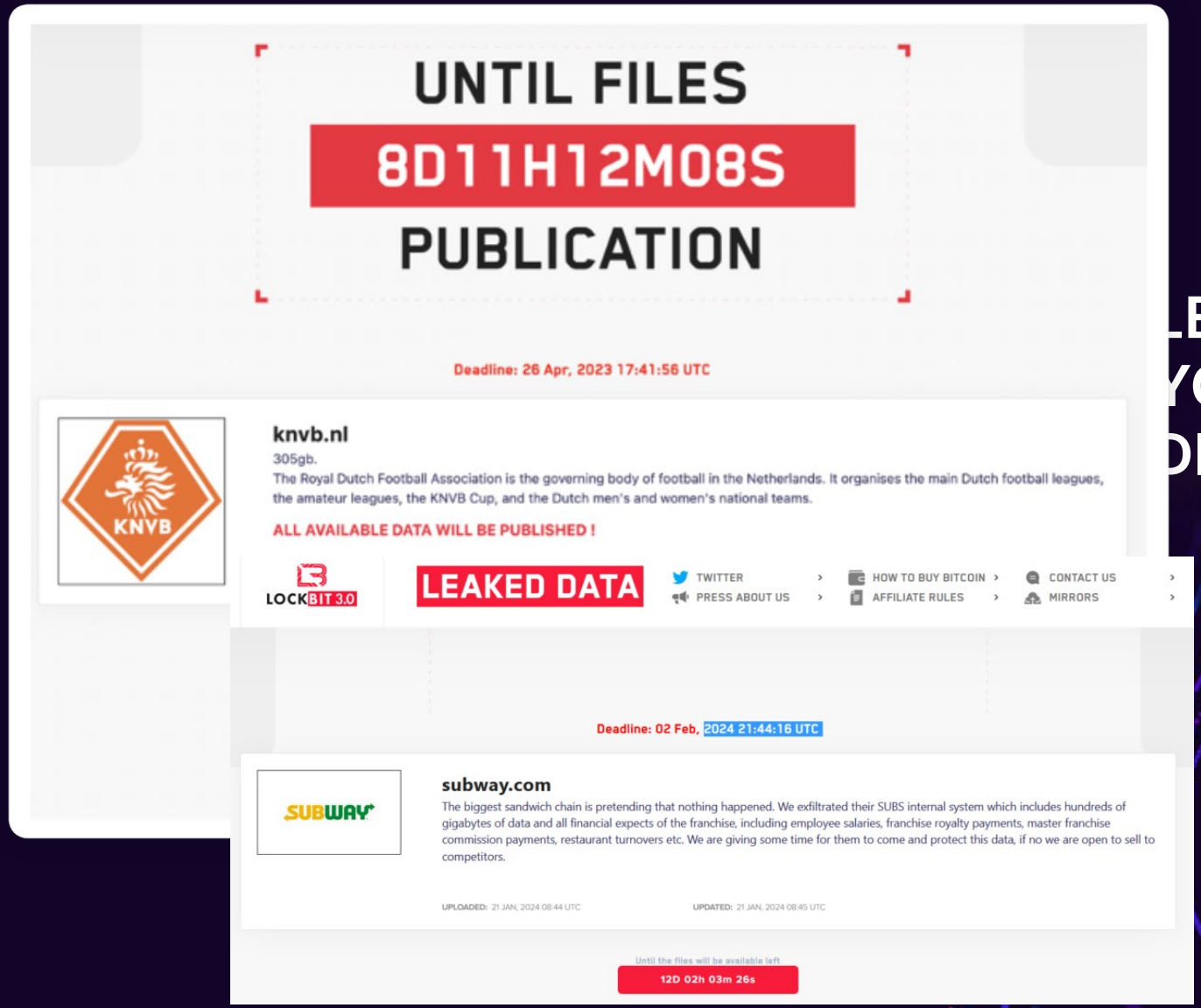
EXPLORE INNOV8

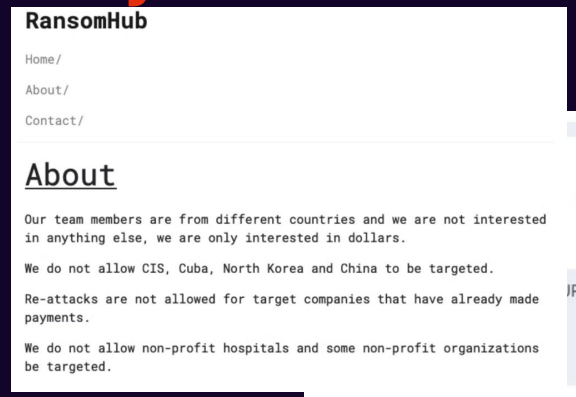


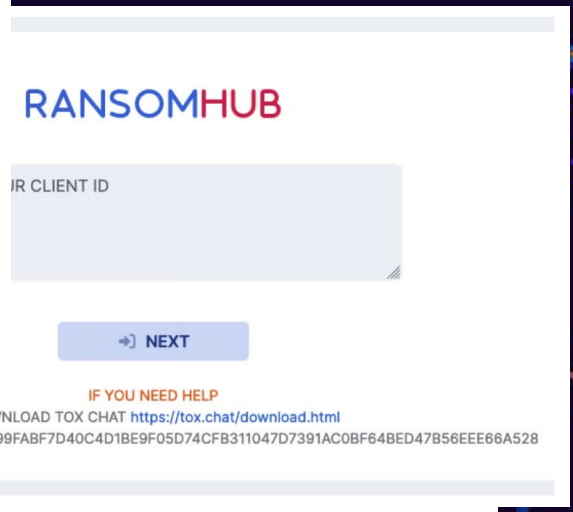
Een continu programma waarin we met jullie de digitale transformatie vorm blijven geven en samen zorgen dat we succesvol zijn **nu en in de toekomst.**

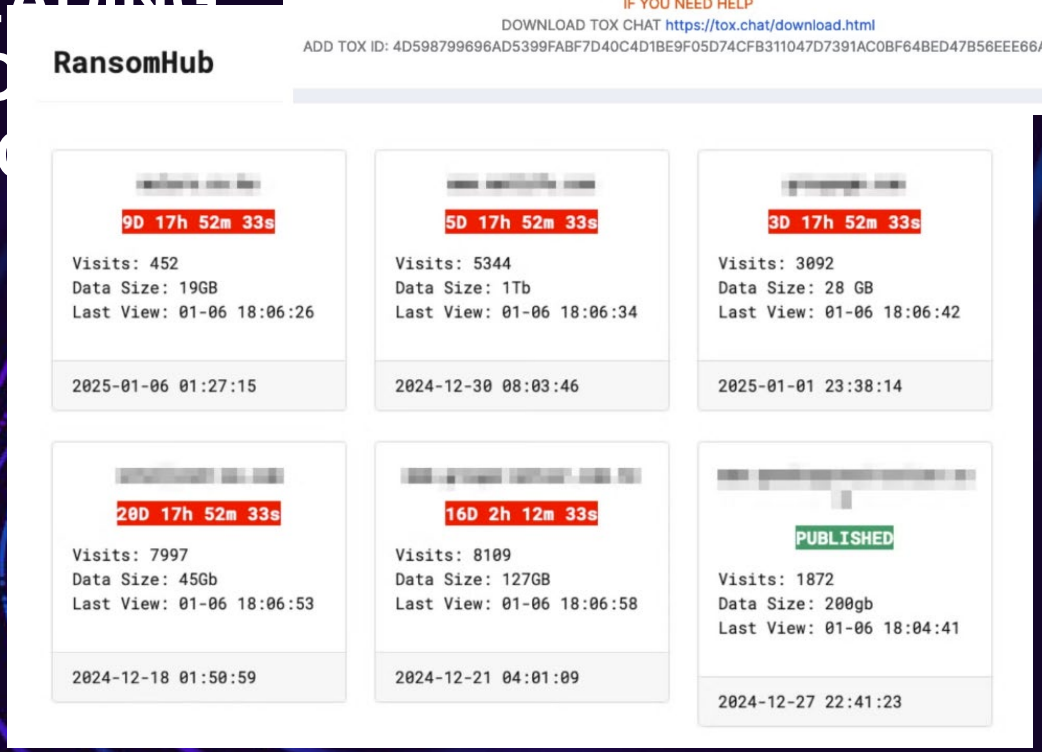
UNO | LEADING YOUR DIGITAL JOURNEY

Ransomware aanvallen zijn een commodity









UNO | LEADING YOUR DIGITAL JOURNEY

'Jaguar-hack is schadelijkste cyberaanval in Britse geschiedenis'

De recente cyberaanval op Jaguar Land Rover kostte de Britse economie naar schatting bijna twee miljard pond, omgerekend 2,18 miljard euro. Vijfduizend organisaties werden mogelijk indirect getroffen door de cyberaanval. Het zou daarmee het meest economisch schadelijke incident ooit voor het Verenigd Koninkrijk zijn.

Volgens onderzoekers van het Cyber Monitoring Centre was de economische schade zo groot omdat JLR ongeveer vijf weken gesloten werd, waardoor de autofabrikant geen voertuigen kon produceren. In tegenstelling tot de meeste cyberaanvallen waren hackers bij JLR in staat veel bedrijven en organisaties te treffen door een specifiek doelwit uit te schakelen. Normaal zou het andersom zijn en zouden veel partijen tegelijkertijd uitgeschakeld worden.

JLR werd in augustus getroffen door een cyberaanval, waarna meerdere fabrieken en systemen 'proactief' stilgelegd werden om verdere schade te voorkomen. Veel bedrijven zijn direct of indirect afhankelijk van de autofabrikant, bijvoorbeeld voor de levering van onderdelen. Deze toeleveringsketen heeft naar schatting honderdduizend mensen in dienst. De Britse regering heeft JLR een lening van omgerekend 1,75 miljard euro verstrekt om te herstellen van de financiële schade door de cyberaanval.

Human-operated ransomware attacks are up more than

200%

$10.5 trillion

The cost of cybercrime is projected to hit an annual $10.5 trillion by 2025.

70%

of organizations ecountering human-operated ransomware had fewer than 500 employees.

156.000 daily

BEC attempts observed April 2022-April 2023

80-90%

of all compromises originate from unmanaged devices.

UNO | LEADING YOUR DIGITAL JOURNEY

Ook statelijke actoren zijn in beweging..

EUROPE

'We are already in conflict with Russia' — Merz says Putin destabilizing Germany

August 30, 2025 2:43 pm • 2 min read

by Kollen Post

Bron: Bert Hubert

German Chancellor Friedrich Merz talking to journalists at the NATO summit in The Hague, Netherlands, on June 25, 2025. (Nick Allard/The Kyiv Independent)

Map 0.1: **Methods of Russian hybrid-warfare activity across Europe, January 2018–June 2025**

Zorgelijke 'wen er maar aan'-reactie van overheid op storing: 'Zien ernst niet in'

UNO | LEADING YOUR DIGITAL JOURNEY

AD NIEUWS REGIO SPORT SHOW KIJK PODCAST PUZZEL 9-2025 • 06:00

Drie storingen in zes weken: kan Odido het vertrouwen in zijn netwerk redden?

Door Ir
Redact
Feedb

Klanten van Odido hadden het de afgelopen weken niet altijd makkelijk met hun internetverbinding. In anderhalve maand kampte de provider meerdere keren met een langdurige storing. Klanten tastten vaak uren in het duister over de oorzaak en het moment waarop hun verbinding hersteld zou worden.

Op 15 en 16 juni ondervonden gebruikers problemen door een storing in de DNS-servers. Een dag later hadden klanten in delen van Zeeland, rond Rotterdam en op plaatsen in Noord-Holland minder tot geen bereik door een kabelbreuk. Op 25 juni, rond de NAVO-top, had Odido meerdere storingen op zijn mobiele netwerk. Op 1 augustus volgde de zwaarste storing: een deel van de klanten was 15 uur offline.

Voor die laatste storing besloot Odido zijn klanten twee euro compensatie te geven. Dat ligt boven het wettelijk minimum van één euro, maar volgens veel klanten is het een schamele vergoeding voor de problemen die zij eind juni tot begin augustus ondervonden. Veel tweakers voelen zich, in reacties en op

© REUTERS

Uren geen Teams, Outlook en Office 365 door storing Microsoft, ook problemen bij Nederlandse overheden

Bron: Bert Hubert

Rijkswaterstaat Verkeersinformatie
@RWSverkeersinfo

Translate post

De afritten Delft op de #A13 zijn dicht door een pinstoring bij de nabijgelegen Ikea. Alle winkelbezoekers vertrekken namelijk tegelijk, wat voor veel drukte zorgt. Het verkeer op de snelwegen kan een afrit verderop en binnendoor alsnog naar bestemming (tenzij dat de Ikea was).

UNO | LEADING YOUR DIGITAL JOURNEY

Frameworks- en (wettelijke) kaders

- NIS 2
- BIO 2.0
- NEN 7510
- ISO27001
- SOC 2
- ISAE3402
- NIST

UNO | LEADING YOUR DIGITAL JOURNEY

De gevolgen:
van een geslaagde ransomware aanval

Anouk van der Zanden

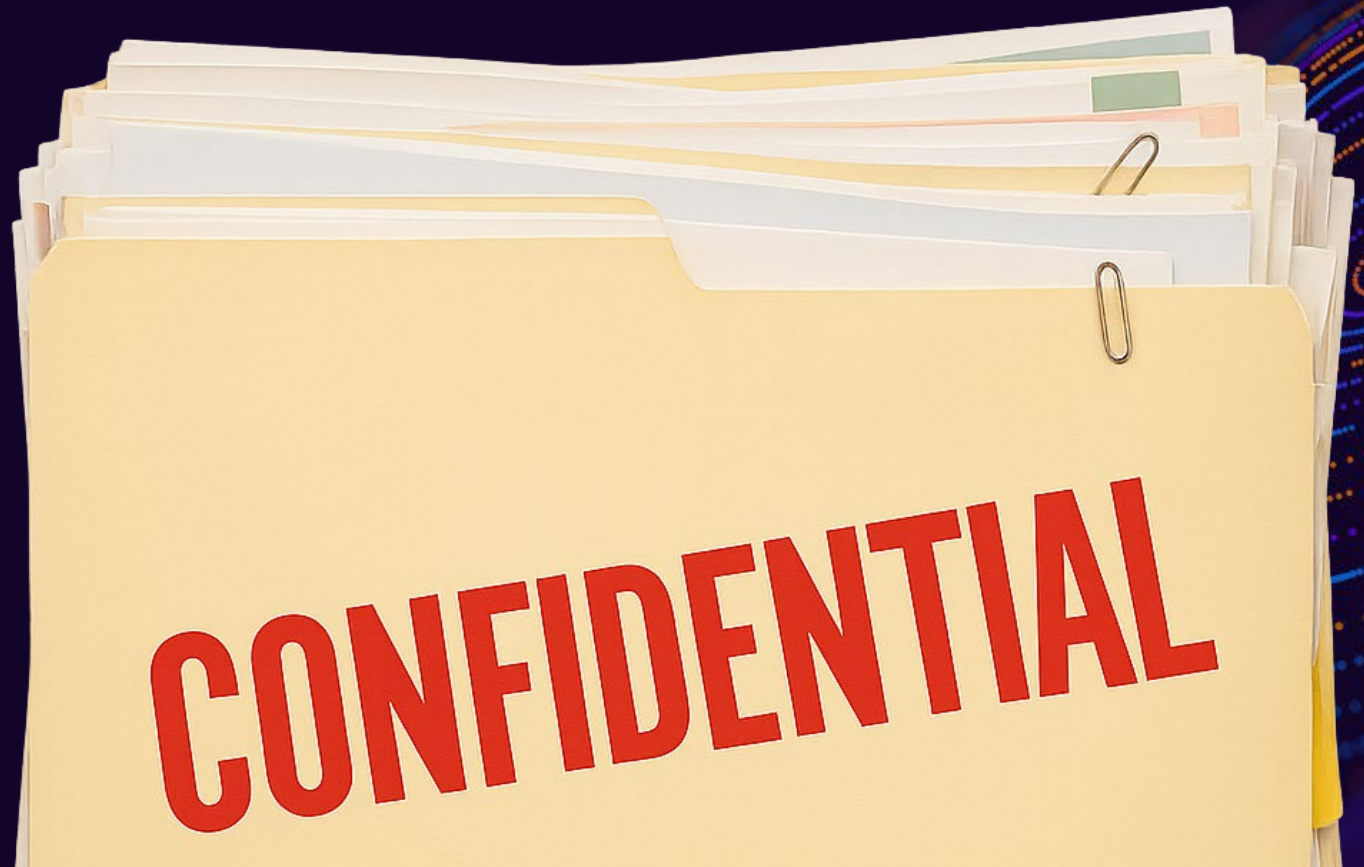
Adviseur ICT

LAURENTIUS
Samen voor een thuis

UNO | LEADING YOUR DIGITAL JOURNEY

Eerst even dit!

Vanwege de gevoeligheid van het volgende onderwerp zal deze sessie niet worden opgenomen.



LAURENTIUS
Samen voor een thuis

UNO | LEADING YOUR DIGITAL JOURNEY

LAURENTIUS
Samen voor een thuis

INHOUD:

Woningcorporatie in Breda

100 medewerkers

8000 woningen

UNO | LEADING YOUR DIGITAL JOURNEY

Wie zijn jullie?

- **In welke categorie valt je functie:**
  - Operationeel
  - Tactisch
  - Strategisch
- **Ben je al eens betrokken geweest bij een digitale aanval?**
- **Wie is betrokken geweest bij een hack waarbij zijn of haar persoonlijke gegevens gelekt zijn?**
- **Wie heeft er een Continuïteitsplan of Incident Respons Plan?**

LAURENTIUS
Samen voor een thuis

UNO | LEADING YOUR DIGITAL JOURNEY

27 MAART 2022

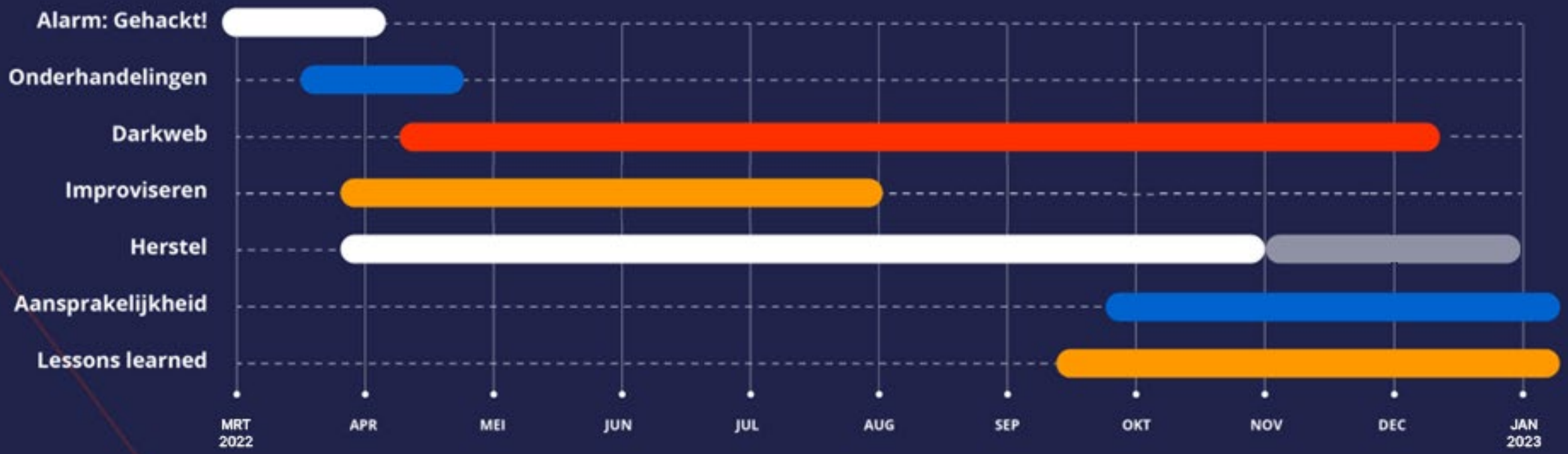
“De Hack”

LAURENTIUS
Samen voor een thuis

UNO | LEADING YOUR DIGITAL JOURNEY

Alarm: Gehackt! Tijdlijn

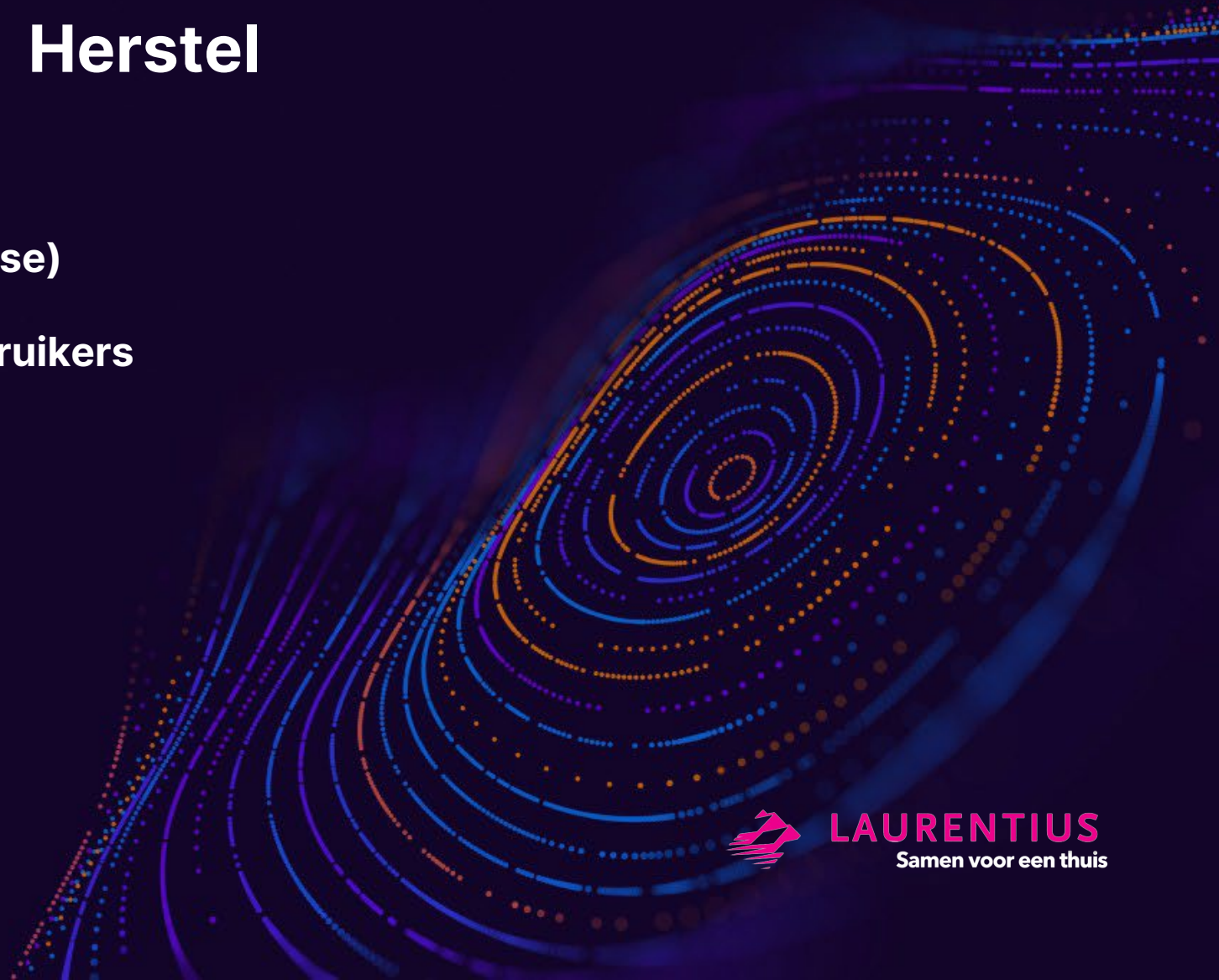
LAURENTIUS
Samen voor een thuis



UNO | LEADING YOUR DIGITAL JOURNEY

Herstel

- Of doorpakken?
- Procesmatige aanpak (Risico-analyse)
- Prioritering: overleg met je eindgebruikers



LAURENTIUS
Samen voor een thuis

UNO | LEADING YOUR DIGITAL JOURNEY

Lessons learned – tijdens de hack

- Logboek
- Onderhandelingen met de hackers
- Betrokkenheid bij forensisch onderzoek
- Impact op organisatie en medewerkers

UNO | LEADING YOUR DIGITAL JOURNEY

Lessons learned - voorbereiding

- Incident Respons Plan
  - Samenstelling First Respons Team (geen ICT-feestje)
  - Communicatie:
    - Collega’s
    - Bewoners/klanten
    - Stakeholders (RvC/brancheorganisatie/toezichthouders)
    - Media vs Hackers
  - Herstel o.b.v. risico-analyse
- Data op de juiste locatie
- Cyberverzekering ja of nee?
- Zorg dat je juiste kennis in huis hebt!

LAURENTIUS
Samen voor een thuis

UNO | LEADING YOUR DIGITAL JOURNEY

Lessons learned – voorkomen is beter dan....

- Awareness
- Managed Detection and Response
- Wees kritisch op je leverancier
  - ISO 27001 incl toepasselijkheidsverklaring en auditrapport
  - ISAE 3402 type 2 verklaring incl rapport van bevindingen
  - Verwerkersovereenkomst
  - Autorisatie- en toegangsbeheer
  - Incident Respons plan
  - Continuiteitsplanning

UNO | LEADING YOUR DIGITAL JOURNEY

VRAGEN?

- ook in de pauze of bij de borrel ☺ -

LAURENTIUS
Samen voor een thuis

UNO | LEADING YOUR DIGITAL JOURNEY

Pauze

15 minuten

UNO | LEADING YOUR DIGITAL JOURNEY

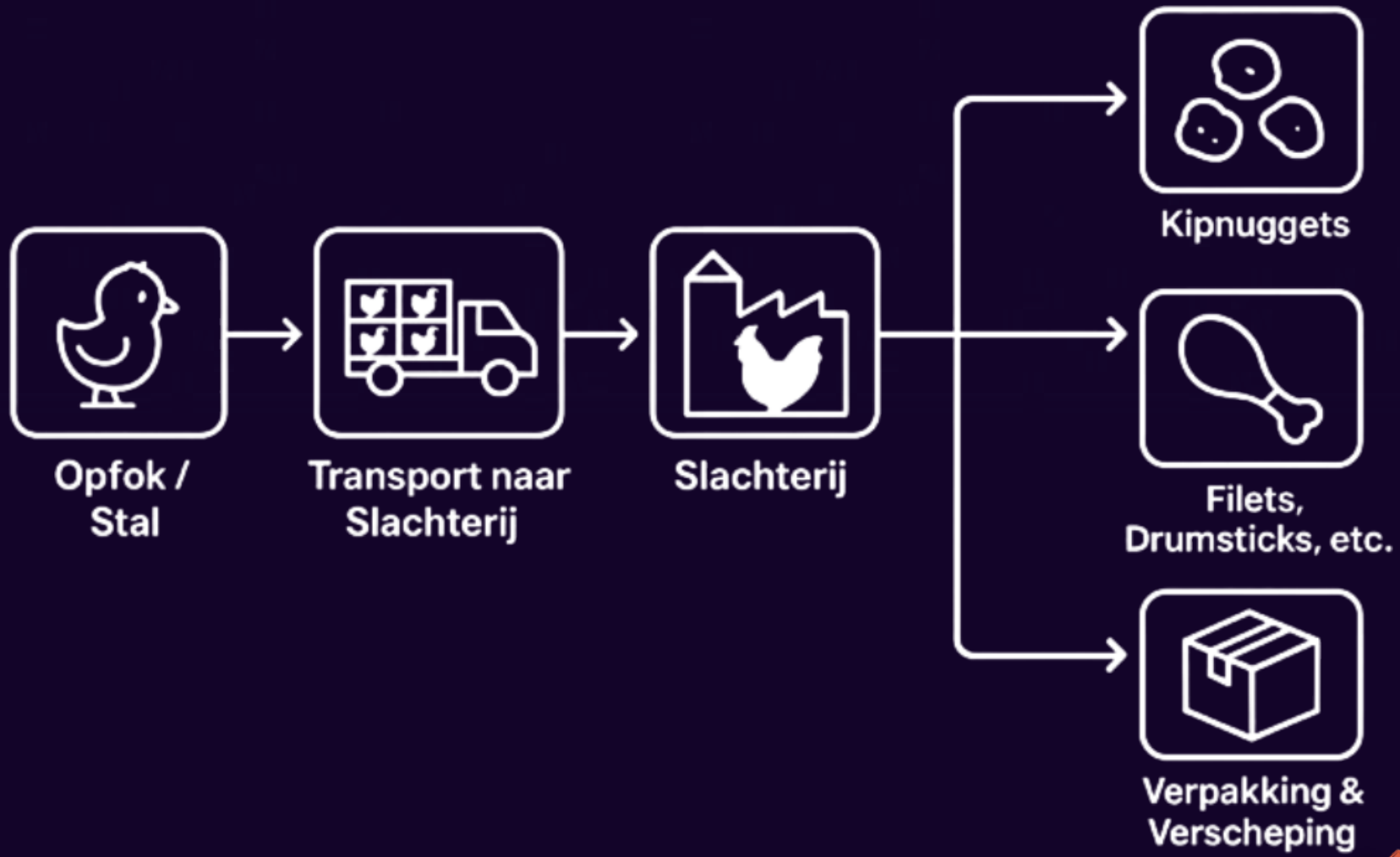
BCM vanuit CISO perspectief

Ronald van der Meulen

Eigenaar Takeshape en ervaren CISO

takeshape

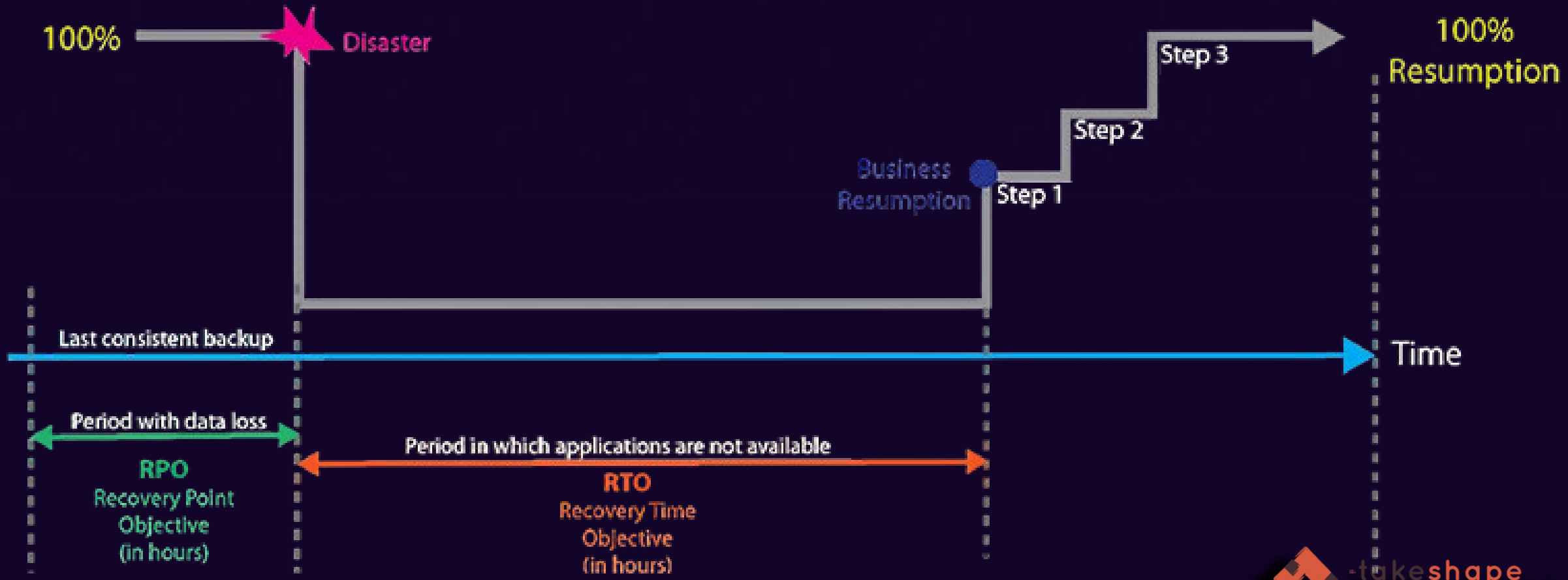
UNO | LEADING YOUR DIGITAL JOURNEY



takeshape

UNO | LEADING YOUR DIGITAL JOURNEY

Bedrijfscontinuïteit



takeshape

UNO | LEADING YOUR DIGITAL JOURNEY

takeshape

Kansen

1:8.000

1:250

1:5

Bron: Rabobank

UNO | LEADING YOUR DIGITAL JOURNEY

takeshape

Cybercrime als economie

$ 27 triljoen

$ 20 triljoen

$ 11 triljoen

Bron Hans de Vries Enisa – presentatie Hunt & Hackett 16 oktober 2025

UNO | LEADING YOUR DIGITAL JOURNEY

takeshape

NIS 2 artikel 21 - zorgplicht

2. De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende:

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;

b) incidentenbehandeling;

c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;

d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

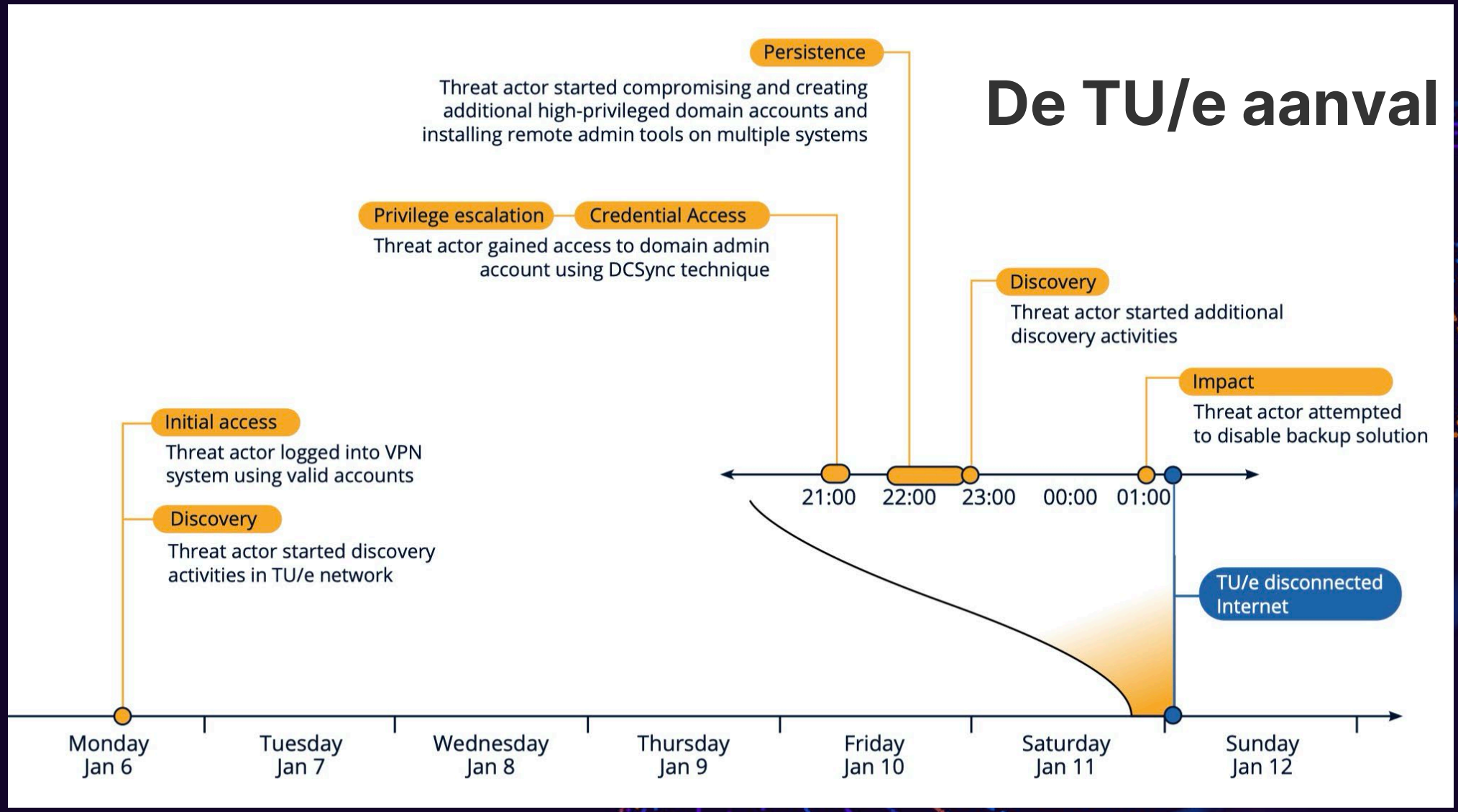
j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Vicevoorzitter van het College van Bestuur Patrick Groothuis en CISO Martin de Vries stonden vanochtend de pers te woord over de rapportages van de cyberaanval. Foto: Bart van Overbeeke

De TU/e heeft ‘snel, doeltreffend' en 'voorbeeldig’ gereageerd op de cyberaanval afgelopen

LEADING
YOUR
DIGITAL JOURNEY

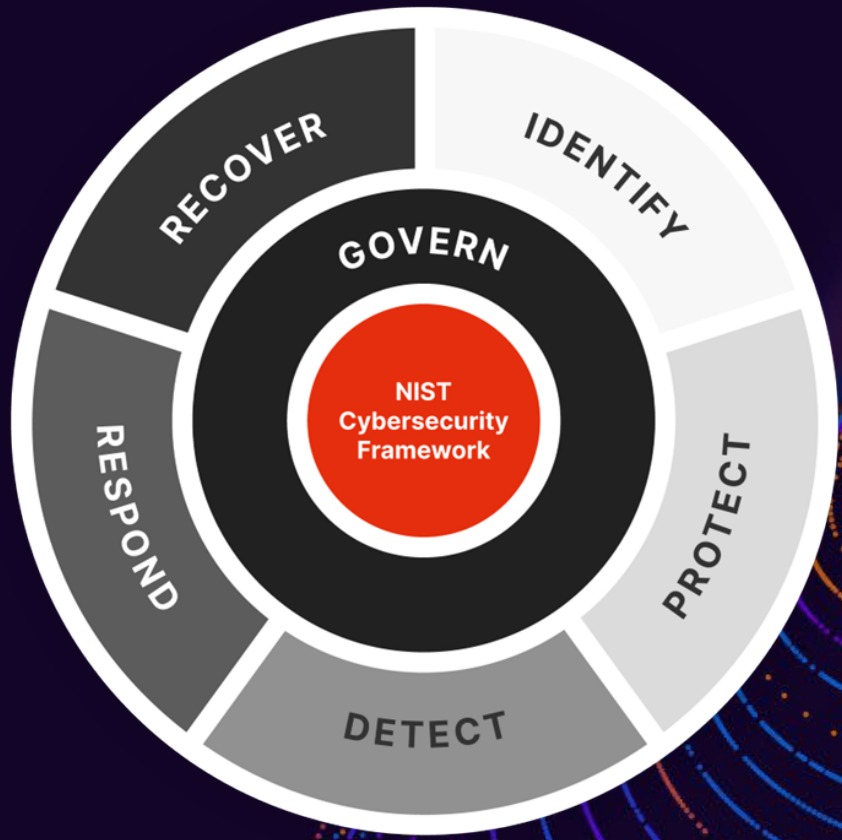
De TU/e aanval



Bron: Fox-IT rapportage "The TU/e cyberattack of January 2025 from Fox-IT's incident response perspective"

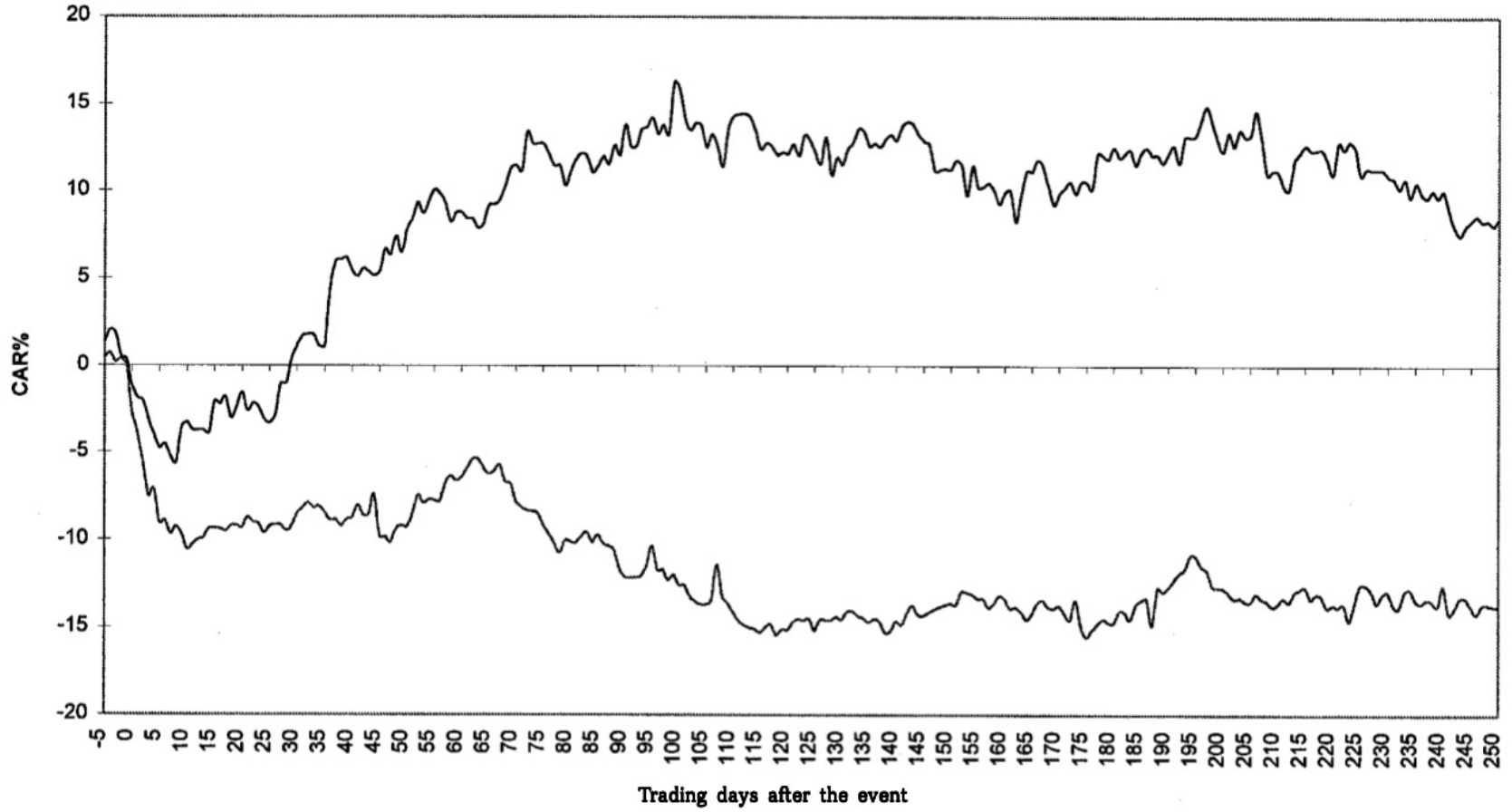
UNO | LEADING YOUR DIGITAL JOURNEY

NIST Cybersecurity Framework



takeshape

Figure 4: Recoverers vs Non-Recoverers



Bron: The Impact of Catastrophes on Shareholder Value Rory F. Knight & Deborah J. Pretty, Oxford University

UNO | LEADING YOUR DIGITAL JOURNEY

Maar waar ben ik nu?

takeshape

UNO | LEADING YOUR DIGITAL JOURNEY

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Auditdienst Rijk
Ministerie van Financiën

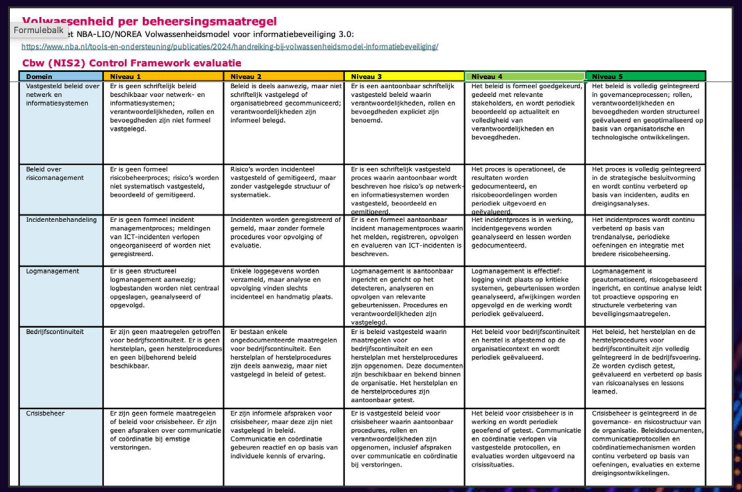
Studierapport Cbw (NIS2) Control Framework

Een praktisch framework bij de implementatie van de Cyberbeveiligingswet (NIS2-richtlijn), voor het versterken van de digitale operationele weerbaarheid.

Auteurs
L.M. Molewijk, ADR
S. Gangaram Panday, Brightlyn
E. Hummel, ADR
T. Meeuws, ADR

Auditdienst Rijk
Postbus 20201, 2500 EE Den Haag
Telefoon: 088 – 442 80 00
E-mail: adrcommunicatie@minfin.nl

NOREA
Postbus 242, 2130 AE Hoofddorp
Telefoon: 088 – 496 03 80
E-mail: norea@norea.nl



Volwassenheid per beheersingsmaatregel

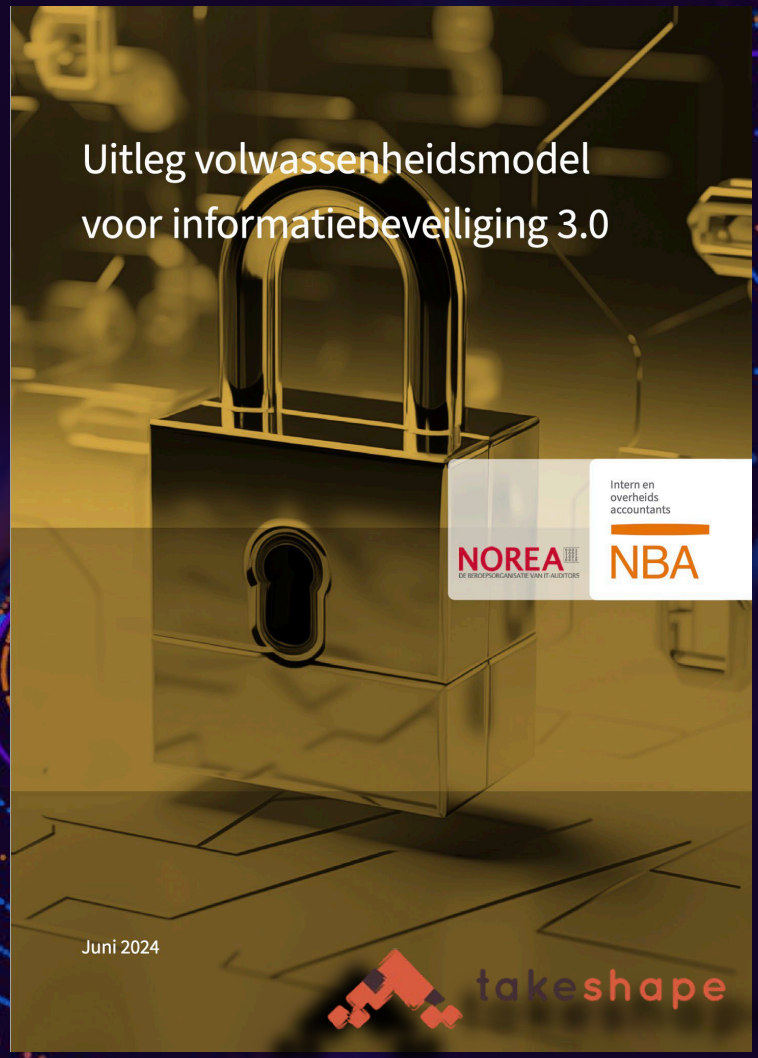
Formulebalk

t NBA-LIO/NOREA Volwassenheidsmodel voor informatiebeveiliging 3.0:

https://www.nba.nl/tools-en-ondersteuning/publicaties/2024/handreiking-bij-volwassenheidsmodel-informatiebeveiliging/

Cbw (NIS2) Control Framework evaluatie

Domein	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Vastgesteld beleid over netwerk en informatiesystemen	Er is geen schriftelijk beleid beschikbaar voor netwerk- en informatiesystemen; verantwoordelijkheden, rollen en bevoegdheden zijn niet formeel vastgelegd.	Beleid is deels aanwezig, maar niet schriftelijk vastgelegd of organisatiebreed gecommuniceerd; verantwoordelijkheden zijn informeel belegd.	Er is een aantoonbaar schriftelijk vastgesteld beleid waarin verantwoordelijkheden, rollen en bevoegdheden expliciet zijn benoemd.	Het beleid is formeel goedgekeurd, gedeeld met relevante stakeholders, en wordt periodiek beoordeeld op actualiteit en volledigheid van verantwoordelijkheden en bevoegdheden.	Het beleid is volledig geïntegreerd in governanceprocessen; rollen, verantwoordelijkheden en bevoegdheden worden structureel geëvalueerd en geoptimaliseerd op basis van organisatorische en technologische ontwikkelingen.
Beleid over risicomanagement	Er is geen formeel risicobeheerproces; risico's worden niet systematisch vastgesteld, beoordeeld of gemitigeerd.	Risico's worden incidenteel vastgesteld of gemitigeerd, maar zonder vastgelegde structuur of systematiek.	Er is een schriftelijk vastgesteld proces waarin aantoonbaar wordt beschreven hoe risico's op netwerk- en informatiesystemen worden vastgesteld, beoordeeld en gemitigeerd.	Het proces is operationeel, de resultaten worden gedocumenteerd, en risicobeoordelingen worden periodiek uitgevoerd en geëvalueerd.	Het proces is volledig geïntegreerd in de strategische besluitvorming en wordt continu verbeterd op basis van incidenten, audits en dreigingsanalyses.
Incidentenbehandeling	Er is geen formeel incident managementproces; meldingen van ICT-incidenten verlopen ongeorganiseerd of worden niet geregistreerd.	Incidenten worden geregistreerd of gemeld, maar zonder formele procedures voor opvolging of evaluatie.	Er is een formeel aantoonbaar incident managementproces waarin het melden, registreren, opvolgen en evalueren van ICT-incidenten is beschreven.	Het incidentproces is in werking, incidentgegevens worden geanalyseerd en lessen worden gedocumenteerd.	Het incidentproces wordt continu verbeterd op basis van trendanalyse, periodieke oefeningen en integratie met bredere risicobeheersing.
Logmanagement	Er is geen structureel logmanagement aanwezig; logbestanden worden niet centraal opgeslagen, geanalyseerd of opgevolgd.	Enkele loggegevens worden verzameld, maar analyse en opvolging vinden slechts incidenteel en handmatig plaats.	Logmanagement is aantoonbaar ingericht en gericht op het detecteren, analyseren en opvolgen van relevante gebeurtenissen. Procedures en verantwoordelijkheden zijn vastgelegd.	Logmanagement is effectief: logging vindt plaats op kritieke systemen, gebeurtenissen worden geanalyseerd, afwijkingen worden opgevolgd en de werking wordt periodiek geëvalueerd.	Logmanagement is geautomatiseerd, risicogebaseerd ingericht, en continue analyse leidt tot proactieve opsporing en structurele verbetering van beveiligingsmaatregelen.
Bedrijfscontinuïteit	Er zijn geen maatregelen getroffen voor bedrijfscontinuïteit. Er is geen herstelplan, geen herstelprocedures en geen bijbehorend beleid beschikbaar.	Er bestaan enkele ongedocumenteerde maatregelen voor bedrijfscontinuïteit. Een herstelplan of herstelprocedures zijn deels aanwezig, maar niet vastgelegd in beleid of getest.	Er is beleid vastgesteld waarin maatregelen voor bedrijfscontinuïteit en een herstelplan met herstelprocedures zijn opgenomen. Deze documenten zijn beschikbaar en bekend binnen de organisatie. Het herstelplan en de herstelprocedures zijn aantoonbaar getest.	Het beleid voor bedrijfscontinuïteit en herstel is afgestemd op de organisatiecontext en wordt periodiek geëvalueerd.	Het beleid, het herstelplan en de herstelprocedures voor bedrijfscontinuïteit zijn volledig geïntegreerd in de bedrijfsvoering. Ze worden cyclisch getest, geëvalueerd en verbeterd op basis van risicoanalyses en lessons learned.
Crisisbeheer	Er zijn geen formele maatregelen of beleid voor crisisbeheer. Er zijn geen afspraken over communicatie of coördinatie bij ernstige verstoringen.	Er zijn informele afspraken voor crisisbeheer, maar deze zijn niet vastgelegd in beleid. Communicatie en coördinatie gebeuren reactief en op basis van individuele kennis of ervaring.	Er is vastgesteld beleid voor crisisbeheer waarin aantoonbaar procedures, rollen en verantwoordelijkheden zijn opgenomen, inclusief afspraken over communicatie en coördinatie bij verstoringen.	Het beleid voor crisisbeheer is in werking en wordt periodiek geoefend of getest. Communicatie en coördinatie verlopen via vastgestelde protocollen, en evaluaties worden uitgevoerd na crisissituaties.	Crisisbeheer is geïntegreerd in de governance- en risicostructuur van de organisatie. Beleidsdocumenten, communicatieprotocollen en coördinatiemechanismen worden continu verbeterd op basis van oefeningen, evaluaties en externe dreigingsontwikkelingen.



UNO | LEADING YOUR DIGITAL JOURNEY

Bedrijfscontinuïteit - volwassenheidsniveaus

Domein	Niveau 1 Initieel	Niveau 2 Herhaalbaar	Niveau 3 Gedefinieerd	Niveau 4 Beheerst en meet-baar	Niveau 5 Continu verbete-ren
Bedrijfs-continuiteït	Er zijn geen maatregelen getroffen voor bedrijfscontinuïteit. Er is geen herstelplan, geen herstelprocedures en geen bijbehorend beleid beschikbaar.	Er bestaan enkele ongedocumenteerde maatregelen voor bedrijfscontinuïteit. Een herstelplan of herstelprocedures zijn deels aanwezig, maar niet vastgelegd in beleid of getest.	Er is beleid vastgesteld waarin maatregelen voor bedrijfscontinuïteit en een herstelplan met herstelprocedures zijn opgenomen. Deze documenten zijn beschikbaar en bekend binnen de organisatie. Het herstelplan en de herstelprocedures zijn aantoonbaar getest.	Het beleid voor bedrijfscontinuïteit en herstel is afgestemd op de organisatiecontext en wordt periodiek geëvalueerd.	Het beleid, het herstelplan en de herstelprocedures voor bedrijfscontinuïteit zijn volledig geïntegreerd in de bedrijfsvoering. Ze worden cyclisch getest, geëvalueerd en verbeterd op basis van risicoanalyses en lessons learned.

takeshape

https://www.auditdienstrijk.nl/documenten/2025/september/30/cbw-nis2-control-framework
https://www.nba.nl/tools-en-ondersteuning/publicaties/2024/handreiking-bij-volwassenheidsmodel-informatiebeveiliging/

UNO | LEADING YOUR DIGITAL JOURNEY

Security frameworks

Domein	Niveau 1 Initieel	Niveau 2 Herhaalbaar	Niveau 3 Gedefinieerd	Niveau 4 Beheerst en meet-baar	Niveau 5 Continu verbete-ren
Bedrijfs-continuiteit	Er zijn geen maatregelen getroffen voor bedrijfscontinuïteit. he her en geen bijbehorend beleid beschikbaar.	Er bestaan enkele ongedocumenteerde maatregelen voor bedrijfscontinuïteit. erstelplan of lprocedures els aanwezig, maar niet vastgelegd in beleid of getest.	Er is beleid vastgesteld waarin maatregelen voor bedrijfscontinuïteit organisatie. Het herstelplan en de herstelprocedures zijn aantoonbaar getest.	Het beleid voor bedrijfscontinuïteit en herstel is afgestemd op de	Het beleid, het hers telplan en de hers procedures or inuïteit eerd d op van risi alyses en les ons learned.

NCSC 5 basisprincipes

KVK 6 stappen

NIS2

takeshape

https://www.auditdienstrijk.nl/documenten/2025/september/30/cbw-nis2-control-framework
https://www.nba.nl/tools-en-ondersteuning/publicaties/2024/handreiking-bij-volwassenheidsmodel-informatiebeveiliging/

Oefenen

Niveau 1 – Initiëel / Ad-hoc
Er zijn geen maatregelen getroffen voor bedrijfscontinuïteit. Er is geen herstelplan, geen herstelprocedures en geen bijbehorend beleid beschikbaar.
Doel:
Bewustzijn creëren en basis leggen voor formeel beleid.
Geschikte oefeningen:
- Awareness sessies / workshops over bedrijfscontinuïteit en risico's van het ontbreken van plannen. - Tabletop oefening op basis van een eenvoudig scenario, bijv. stroomuitval of uitval van kritieke systemen. Geen formeel plan nodig, puur om discussies op gang te brengen. - Risico-identificatie oefening: Laat teams nadenken over de grootste operationele risico's. - Stakeholder mapping sessie: Wie zijn belangrijk bij een incident? Wie moet geïnformeerd worden?

UNO | LEADING YOUR DIGITAL JOURNEY

Wat te doen bij een **hack** of **ransomware**?

1. Zorg voor continuiteit van de belangrijkste dienstverlening. → *Lees wat u moet doen in uw bedrijfscontinuïteitsplan.*
2. Los het incident op en herstel de schade. → *Lees in uw Incidentmanagement-plan hoe u dit aanpakt.*
3. Zorg voor goede interne en externe communicatie. → *Werk volgens de aanpak in uw crisiscommunicatieplan.*

De 7 gouden regels

1. Zet de apparatuur **niet** uit
2. **Verbreek** de netwerkverbinding
3. Stel de **back-ups** veilig
4. Zet de automatische back-ups **uit**
5. Stel **logfiles** veilig
6. **Informeer** interne organisatie
7. **Documenteer** genomen stappen

Let op: nieuw telefoonnummer IBD
070 204 55 11

Leveranciers

Leveranciers
Noteer hier de locatie van contactgegevens van en afspraken met de security-contactpersonen van uw leveranciers & dienstverleners.

Netwerk & Storage	Locatie documenten
Burgerzaken	
Website / Hosting	
Zaaksysteem	
Databases	

Incident Response
Noteer hier de contactgegevens van de partijen die u nodig heeft bij de bestrijding van een incident. Noteer ook de afspraken over reactietijden en kosten of geef de locatie aan van het overzicht.

Incident Response		
Data Recovery		
Digitaal Forensisch Onderzoek		

Wat doet de IBD?

1. **Telefonische ondersteuning**
   - Advies techniek en proces
   - ondersteuning communicatie/woordvoering
   - privacyadvies
2. Online **deelname crisisteam** als adviseur
3. **Schakelpunt** met rijksoverheid, leveranciers en gemeenten
   - advies en waarschuwing
   - inzet netwerk VNG(-bestuurders)
4. **Bemiddeling** capaciteit en steun andere gemeenten (gemeentelijk responsnetwerk)
5. **Second opinion** op adviezen en voorstellen derden
6. Hulp bij **evaluatie** en opstellen lessen voor de toekomst

Rollen Crisisteam

	Naam	Telefoonnummer
Voorzitter		
Vastleggen acties / Notulen		
Technisch advies		
Beveiligingsadvies		
Privacyadvies		
Communicatie / Woordvoering		
Aansturing ICT-intern		
Aansturing Leveranciers		
Juridisch advies		
Overig: oa domeinadvies		

Zorg voor een app-groep met de belangrijkste stakeholders

Aandachtspunten

- Maak afspraken over **opschaling/afschaling** en over het **informeren** van bestuurders
- Maak gebruik van de kennis en kunde van de **veiligheidsregio** bij crisismanagement
- Sluit aan bij de **faciliteiten van de reguliere crisisstructuur**. Denk aan ICT-middelen, aflossingsprotocollen, catering
- Aarzel niet om de **hulp van andere gemeenten** in te roepen, de IBD kan hierin bemiddelen

Rol directie (koude fase)

- Bewaakt ieder halfjaar **paraatheid** organisatie
- Bewaakt ieder kwartaal **preventieve maatregelen**
- Bewaakt ieder kwartaal **impactbeperkende maatregelen**
- **Rapporteert** aan bestuur

Belangrijke documenten

	Datum actuele versie	Fysieke locatie
Bedrijfscontinuïteitsplan(en)		
Incidentmanagementplan		
ICT Crisiscommunicatieplan		

Mindmaps

Voor mindmaps over essentiele maatregelen en processen kijkt u op: www.informatiebeveiligingsdienst.nl/vdw

INFORMATIE BEVEILIGINGS DIENST | VNG Realisatie

Bron https://www.informatiebeveiligingsdienst.nl/

takeshape

UNO | LEADING YOUR DIGITAL JOURNEY

Oefenen

Niveau 2 – Herhaalbaar / Initiatiefase
Er is enig bewustzijn en men begint met het opstellen van plannen.
Doel:
Eerste plannen en basisprocessen ontwikkelen.
Geschikte oefeningen:
- Business Impact Analysis (BIA) workshop: wat zijn de kritieke processen? - Eenvoudige tabletop-oefening met bestaande procesverantwoordelijken, op basis van eerste versies van plannen. - Incident response simulatie met focus op communicatie en coördinatie. - Review-oefening van bestaande inventarisatie van IT-assets en afhankelijkheden.

takeshape

UNO | LEADING YOUR DIGITAL JOURNEY

RTV Utrecht

Voorpagina Sport Kijk Radio M Utrecht Podcasts Bureau Hengeveld

Lees voor

Geen schadelijke stoffen in poederbrief Amersfoort

26 oktober 2006, 15:32 • 1 minuut leestijd

AMERSFOORT - De poederbrief, die woensdag werd aangetroffen bij een bedrijf in Amersfoort, bevatte geen schadelijke stoffen.
Dat heeft onderzoek in een laboratorium in Lelystad uitgewezen.

Als er ergens een poederbrief wordt gevonden, treedt altijd meteen een protocol in werking. De medewerkers van het bedrijf aan de Amersfoortse Stationsweg mochten daarom pas na een paar uur naar buiten.

takeshape

UNO | LEADING YOUR DIGITAL JOURNEY

Oefenen

Niveau 3 – Gedefinieerd
BCM is formeel beschreven en gedocumenteerd.
Doel:
Testen van plannen en verbeteren op basis van feedback.
Geschikte oefeningen:
- Volledige tabletop-oefening op directieniveau, met realistische scenario's. - Simulatieoefening van specifieke verstoringen, bijv. cyberaanval, brand, uitval datacenter. - Test communicatieplannen: hoe wordt interne/externe communicatie afgehandeld? - Oefening RTO/RPO-berekeningen: testen of de beoogde hersteldoelen haalbaar zijn.

takeshape

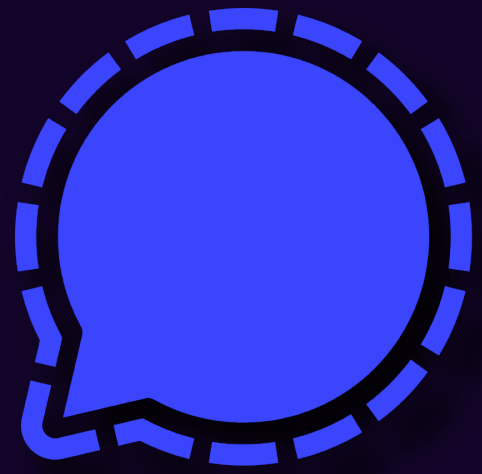
UNO | LEADING YOUR DIGITAL JOURNEY

takeshape

Oefenen

Niveau 4 – Beheerst en meetbaar
BCM is formeel beschreven en gedocumenteerd.
Doel:
Verbeteren op basis van realistische simulaties en meten van prestaties.
Geschikte oefeningen:
- End-to-end ketenoefeningen, inclusief leveranciers en partners. - Black box crisis response simulatie zonder voorafgaande briefing. - Evaluatie van herstelcapaciteiten vs. afgesproken RTO/RPO’s. - Lessons learned workshop na elke oefening, met update van plannen.

UNO | LEADING YOUR DIGITAL JOURNEY



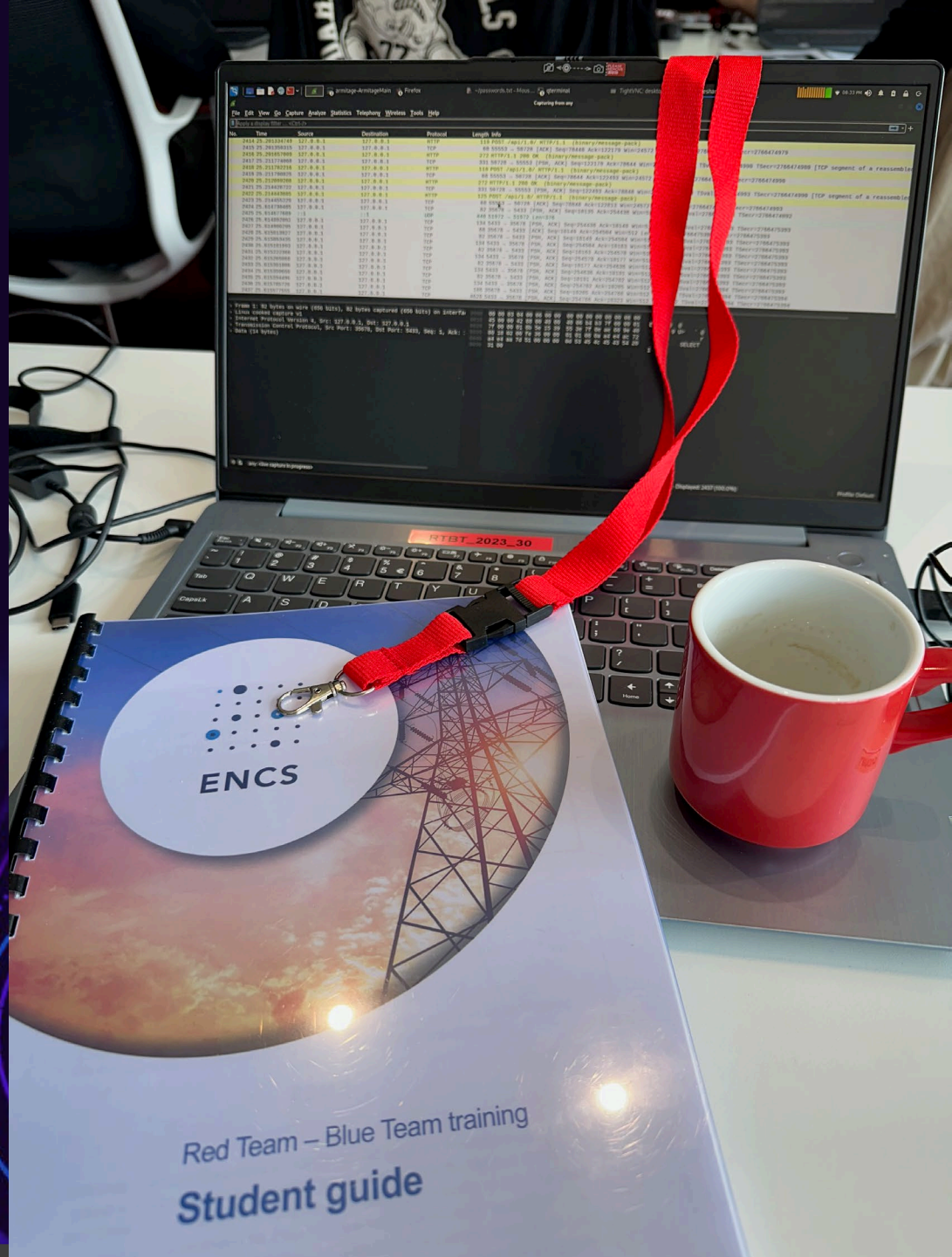
Signal

takeshape

Oefenen

Niveau 5 – Continu verbeteren
Continu verbeteren op basis van lessons learned, audits en nieuwe dreigingen.
Doel:
Fine-tunen van processen, integratie met risicomanagement en strategische planning.
Geschikte oefeningen:
- Red team / blue team oefeningen (bijv. bij cyberdreigingen). - Combinatie-oefeningen (cyber + fysiek) om multi-domein scenario's te testen. - Oefeningen gekoppeld aan strategische besluitvorming: bijv. reputatieschade, juridische gevolgen. - Benchmarks en maturity assessments voor vergelijking met sectorstandaarden. - Sectorale oefeningen zoals ISIDOOR, TIBER e.d.

UNO | LEADING YOUR DIGITAL JOURNEY



UNO | LEADING YOUR DIGITAL JOURNEY

10 Vragen die de directie kan stellen

1. Wat zijn onze kritieke diensten en hoe lang mogen die onbeschikbaar zijn?
2. Wie heeft het stekkermandaat en is dit beschreven en bekend?
3. Hoe is crisisbesluitvorming geregeld buiten kantooruren?
4. Welke scenario's (ransomware, SaaS-uitval, OT-storing) zijn geoefend en wat waren de bevindingen?
5. Hebben we onwijzigbare/offline back-ups en zijn herstelprocedures recent getest?
6. In welke volgorde gaan we systemen herstellen?
7. Wanneer was de laatste end-to-end hersteloefening en haalde die de RTO?
8. Welke top-10 afhankelijkheden (incl. leveranciers) bepalen onze doorstart?
9. Hoe borgen we leverancierscontinuïteit?
10. Van wie krijgen we hulp als er zich een cyberincident voordoet? Hebben we een IR-retainer?

takeshape

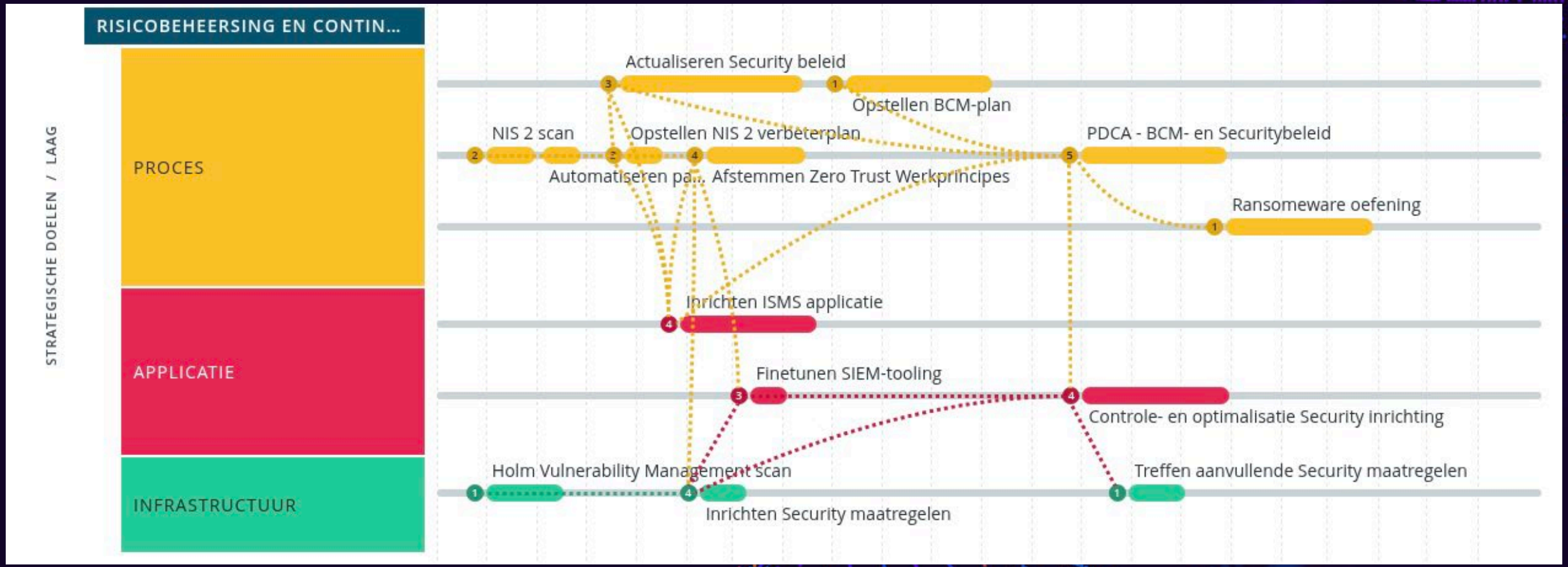
UNO | LEADING YOUR DIGITAL JOURNEY

Vragen?

takeshape

UNO | LEADING YOUR DIGITAL JOURNEY

Security Roadmap



BEDANKT VOOR JE AANWEZIGHEID!