Festival Cybersecurity in de Zorg

20 juni 2023

Deelsessie (16.30-17.15u)

Interactief ervaringen uitwisselen; Security-incidenten & Datalekken

Erik van den Beld

Audittrail / FG Liberein

Festival Cybersecurity in de Zorg
20 juni

Zaal 1	Zaal 2	Zaal 3	Zaal 4	Zaal 5
Een cybercrisis voorkomen *Theaterzaal: Geluksfabriek*	Voorbereiden op een cybercrisis *Zaal: Sterrenstof*	Tijdens een cybercrisis *Zaal: 't Wij-land*	D[illegible]sleep va[illegible] cy[illegible]ris *Zaal: De[illegible]mis*	Leren van een cybercrisis *Zaal: De Twent*

WELKOM

	De mens als zwakste schakel? No way! **Remco Spithoven** Lectoraat Maatschappelijke Veiligheid Saxion
16.30 – 17.15	**BLOK 2**
16.30 – 17.15	Interactief ervaringen uitwisselen: Security-incidenten en datalekken
Spreker	**Erik van den Beld** Audittrail & Liberein
17.15 – 18:15	**PAUZE, INCLUSIEF BUFFET**

Interactief ervaringen uitwisselen: Security-incidenten en datalekken

Erik van den Beld
Audittrail & Liberein

Audittrail
information security | privacy | quality | grc

liberein

Even voorstellen

Erik van den Beld
06 3616 0984

Audittrail
information security | privacy | quality | grc
https://www.audittrail.nl/

Principle Consultant Gegevensbescherming | AVG

liberein
Functionaris Gegevensbescherming (FG)

SAXION

ZorgNetOost

Hoofddocent/-onderzoeker
(N.b.: van 2017 tot april 2022 Functionaris Gegevensbescherming (FG))

HAN_UNIVERSITY OF APPLIED SCIENCES

FG; jan 2021 - feb 2022

Kom ik nog op terug ..

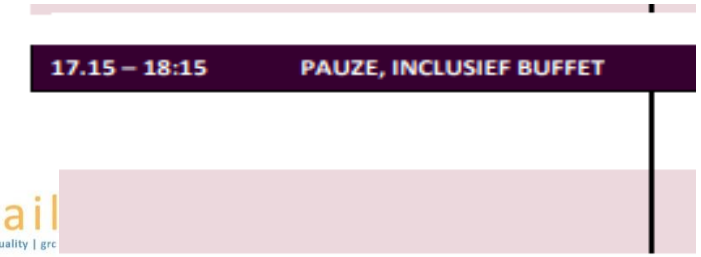
Festival Cybersecurity in de Zorg

20 juni

Deelsessie (16.30-17.15u)

Interactief ervaringen uitwisselen; Securityincidenten & Datalekken

Wat staat op het programma

- Intro
- Actualiteiten / Algemeen
- Casuïstiek; Proces & Tijdlijn – IB&P Incident-Crisis (o.b.v. hack met datadiefstal bij HAN)
- (I.h.k.v.) Voorbereiding op een IB&P Incident-/Crisis
- Afsluiting
- 

Audittrail
information security | privacy | quality | grc

Actualiteiten ...

ZORGSECTOR GOED VOOR 41% VAN ALLE DATALEKKEN

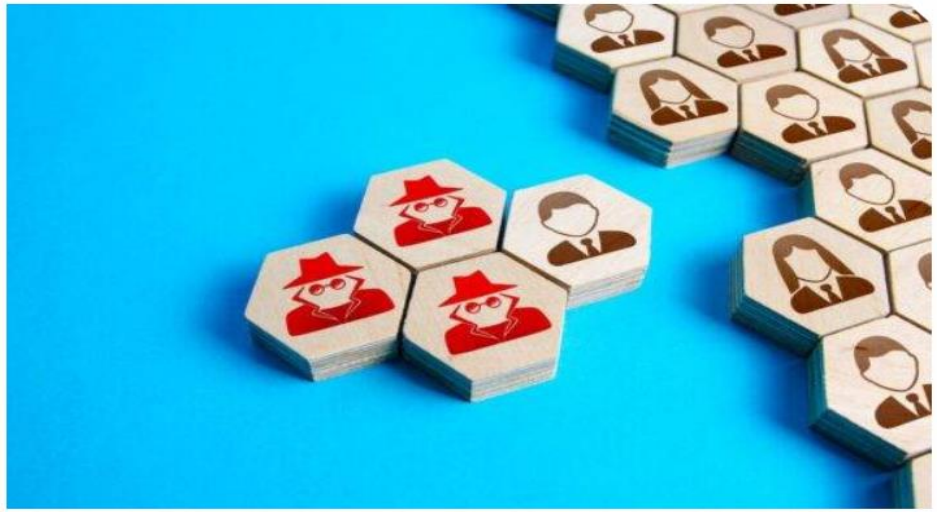
In totaal spelen 41% van de datalekken in Nederland zich af in de ziekenhuizen en aanverwante organisaties. Daarmee is de zorg de meest gehackte sector van Nederland. Dit blijkt uit de begin juni 2023 gepresenteerde datalekkenrapportage 2022 van de Autoriteit Persoonsgegevens. Het is niet toevallig dat juist bijvoorbeeld ziekenhuizen zo vaak slachtoffer van cybercriminelen zijn, want data uit medische dossiers zijn wereldwijd goede handel.

Hackers zijn met steeds modernere software en apparatuur op zoek naar datalekken en richten zich daarbij opvallend vaak op de zorgsector.

Zorgsector goed voor 41% van alle datalekken - ICT&health (icthealth.nl)

ZONDER CYBERSECURITY GEEN VEILIGE ZORG

Lies van Gennip (zelfstandig adviseur en toezichthouder en betrokken bij Informatieveilig Gedrag in de Zorg via ECP platform voor de innovatiesamenleving) en Gabriëlle Speijer (radiotherapeut-oncoloog en oprichter van CatalyzIT) maken zich ernstig zorgen over de gebrekkige aandacht in de zorg voor dataveiligheid. Er staat enorm veel op het spel om zorg te kunnen leveren in het vertrouwen dat medische data altijd en overal veilig zijn.



Dataveiligheid moet meer aandacht krijgen in de zorg. Want zonder goede cybersecurity is er geen veilig gebruik mogelijk van data om de zorg vooruit te helpen.

Zonder cybersecurity geen veilige zorg - ICT&health (icthealth.nl)

Datalekken vooral in de zorg

Carina van Aartsen 6 juni 2023, 09:22 1342 keer gelezen

Van de datalekken is 41 procent afkomstig uit de sector zorg en welzijn.

Door de drie grootste datalekken in de zorgsector kwamen in 2022 de medische gegevens van zo'n 900.000 mensen op straat te liggen. De zorg is ook de sector met de meeste cyberaanvallen. Dat staat in de jaarlijkse datalekkenrapportage van de Autoriteit Persoonsgegevens.

In 2022 ontving de AP weer een groot aantal meldingen over datalekken, in totaal 21.151. Meer dan 1.800 lekken waren het gevolg van cyberaanvallen, 23 procent vond plaats in de zorg, Het aantal meldingen uit de sector financiële dienstverlening is gedaald met 29 procent ten opzichte van 2021. Het aantal meldingen uit de sector openbaar bestuur is gedaald met 16 procent en het aantal meldingen uit de sector gezondheid en welzijn is gedaald met 6 procent. Binnen de sector politie en justitie is het aantal meldingen juist gestegen met 11 procent.

Auditdam information security | privacy | quality | grc

Datalekken vooral in de zorg - Skipr

NIEUWS HENGELO CRIMINALITEIT

Scholengemeenschap OSG Hengelo sluit deal met hackers na ransomware-aanval

Onder meer Montessori College Twente (op de foto), Bataafs Lyceum, 't Genseler voor Praktijkonderwijs, C.T. Stork College zijn onderdeel van OSG Hengelo. BEELD: 1TWENTE / PIXABAY

Scholengemeenschap OSG Hengelo heeft weer toegang tot de eigen servers gekregen na het sluiten van een deal met de hackers die verantwoordelijk zijn voor de ransomware-aanval eind vorige maand. De computersystemen waren door de cyberaanval versleuteld, waardoor de school geen toegang meer had tot de gegevens die daarop worden bewaard.

Overeenkomst

De school zegt dat via 'externe experts' contact is gezocht met de hackers en dat dit heeft geleid tot een overeenkomst, waarbij de hackers hebben toegezegd de gegevens die zij in handen hebben te vernietigen en niet openbaar zullen maken. "Bovendien kregen wij hiermee de gegevens terug die versleuteld waren. Door het terugkrijgen van deze gegevens zijn onze scholen in staat de kwaliteit van het onderwijs te blijven waarborgen." Het is op dit moment nog onduidelijk of er losgeld is betaald en zo ja hoeveel. Daarover doet de scholengemeenschap geen mededelingen.

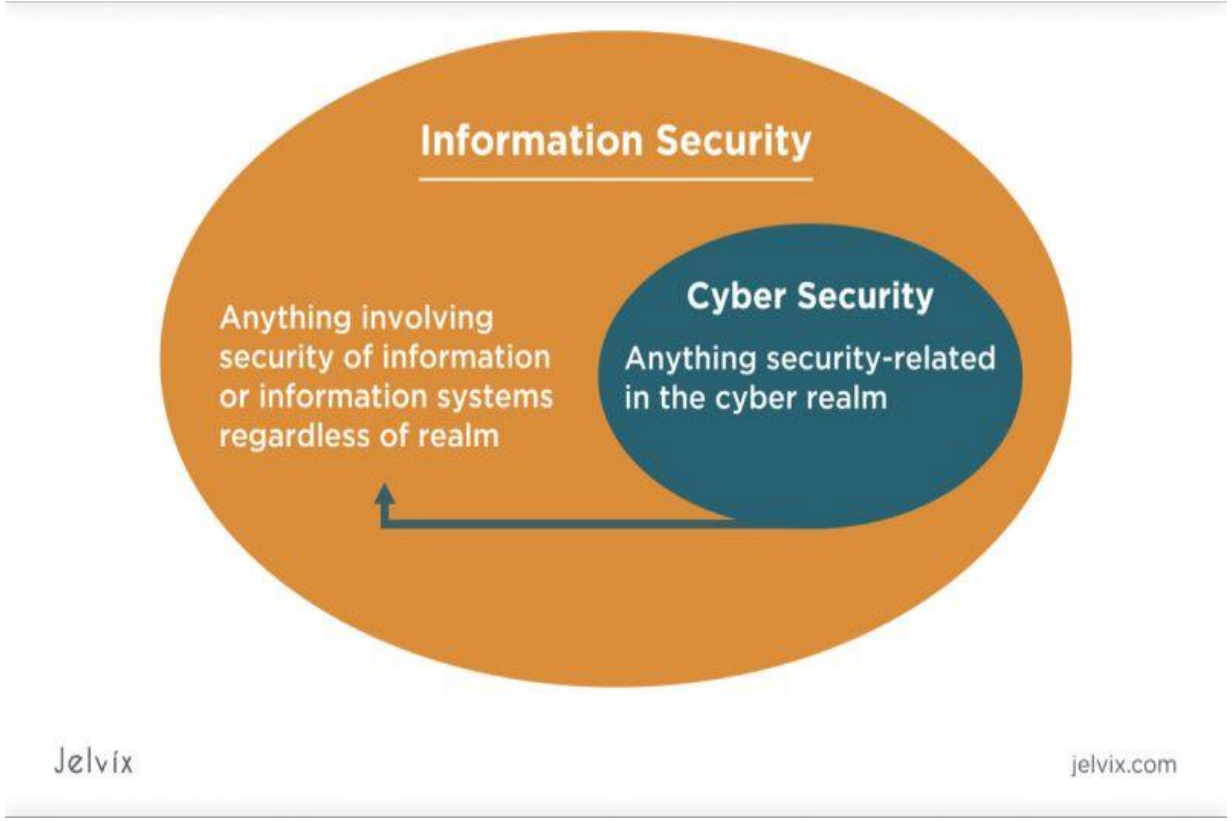
Gegevens

duidelijkheid over is, zullen we dat vertellen," zegt het bestuur in een reactie aan leerlingen en ouders. Inmiddels kunnen medewerkers en leerlingen weer gebruik maken van WiFi. Daarnaast doen bijna alle printers het weer.

NIEUWS CYBERCRIME
Onderzoek ransomware-aanval bij OSG Hengelo nog in volle gang

NIEUWS CYBERCRIME
Scholengemeenschap OSG Hengelo getroffen door ransomware-aanval

Festival Cybersecurity in de Zorg



Informatiebeveiliging ≠ cybersecurity

Twee begrippen, maar (te) vaak door elkaar gehaald. Er zijn namelijk erg belangrijke verschillen (en overeenkomsten) tussen beide.

Informatiebeveiliging omvat beveiliging van alle informatie, zowel digitaal, fysiek als intellectueel. Cybersecurity gaat alleen over het beveiligen van digitale informatie tegen cyberaanvallen zoals ransomware. Daarmee is cybersecurity een onderdeel van informatiebeveiliging.

Wat ze in elk geval gemeen hebben is dat op basis van de BIV-classificatie (beschikbaarheid, integriteit en vertrouwelijkheid) onder andere beleid en maatregelen worden geformuleerd, geïmplementeerd en geëvalueerd.

Cyber

Betekenis: Iets wat te maken heeft met digitale informatie en systemen die verbonden zijn met het internet.
(Bron: cyberwoordenboek)

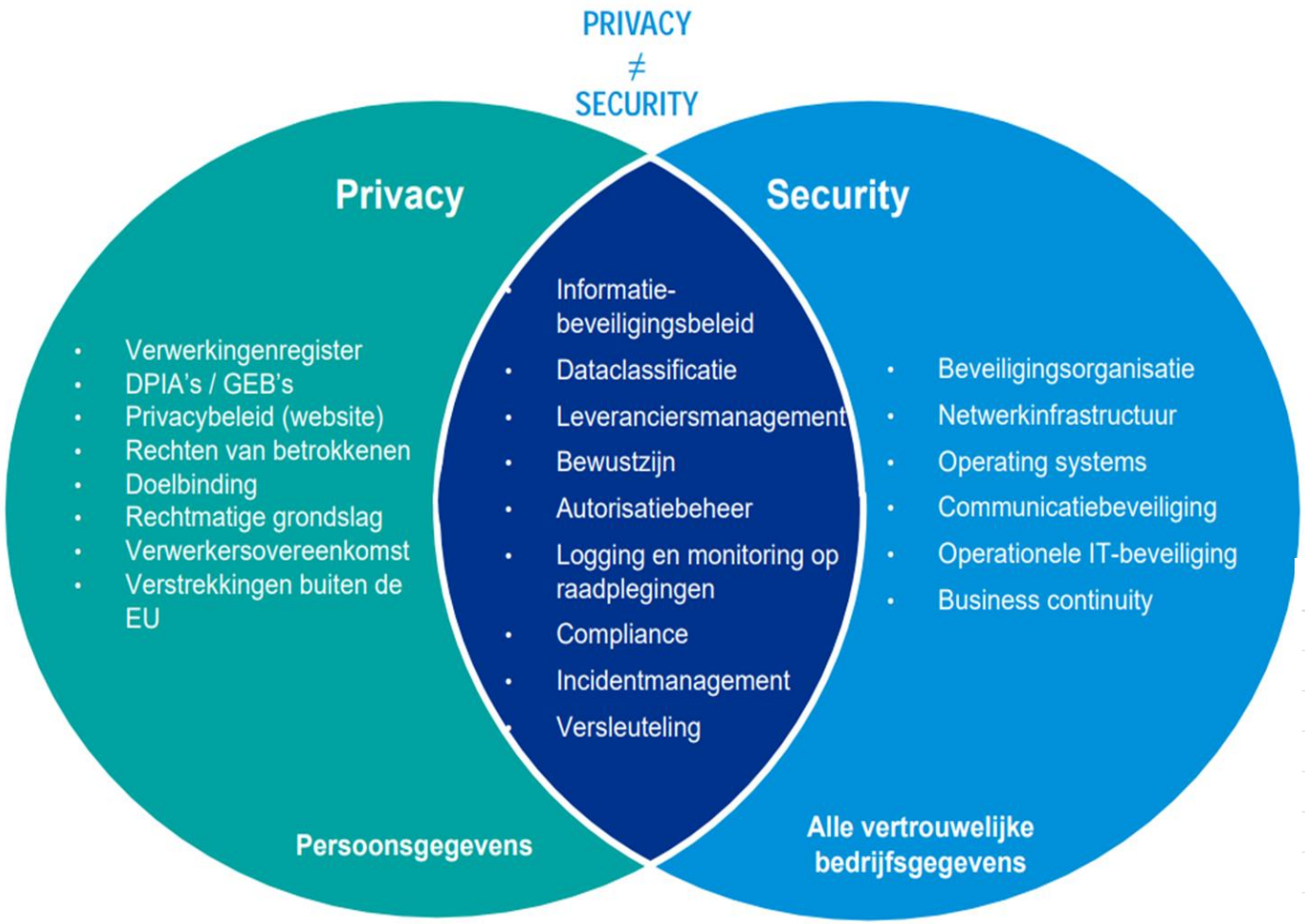
Audittrail
information security | privacy | quality | grc

Cyberloketten | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

InformatieBeveiliging en bescherming Persoonsgegevens

IB & P

Security vs. privacy



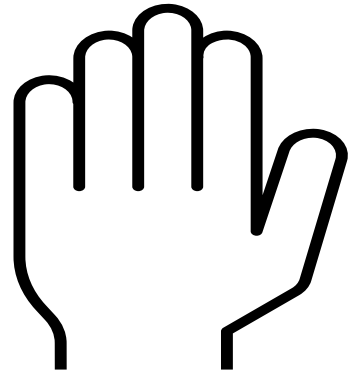
Privacy gaat over het wat we wel en niet verkiezen te delen.

Informatiebeveiliging gaat om het hoe we zorgen dat informatie die we privé willen houden, privé blijft.

Informatiebeveiliging is als zodanig ook opgenomen in de AVG en valt daarmee dus onder het toezicht van de FG. Op dat vlak heeft ook de CISO zijn toezichthoudende taak. Dit vraagt afstemming en samenwerking op dit vlak.

	Gegevensbescherming	**Informatiebeveiliging**
Normenkader:	AVG, UAVG	ISO, NEN, BIO
Naleving:	verplicht	pas toe of leg uit, keuze
Onderwerp:	rechten en vrijheden	veiligheid van bedrijfsinformatie
Doelgroep:	betrokkenen	eigen organisatie
Inbreuk door:	niet naleven wet	incident
Beoordeling:	respecteren van privacy / wet	inschatting kans × impact
Moment:	nu of zoals gepland	mogelijke situatie in de toekomst
Risicoacceptatie:	zo laag mogelijk	goede afweging
Risicocommunicatie:	transparantie	vertrouwelijk

Nog even ….



- Wie is lid van het crisisteam bij je organisatie? Ca. 50% v.d. aanwezigen
- Ook met betrekking tot Cyber-/Security en AVG/Datalekken (IB&P)?

  Ca. 30 a 40 % v.d. aanwezigen

  “Ieder datalek is een informatiebeveiligingsincident, maar andersom niet.”
- Wie heeft al een Security-incident/-crisis of Datalek meegemaakt ?

  Ca. 50 % v.d. aanwezigen
- Training / Geoefend? Ca. 30 a 40 % v.d. aanwezigen
- In welke rol? *(Management / Expert IB&P > FG/PO/CISO/SO / ~~Betrokkene Slachtoffer~~)*

Audittrail
information security | privacy | quality | grc

Zo, … dat was het interactieve deel ….

Hoe is het gesteld met de beveiliging/security?

[Basisbeveiliging – Maps (link)]

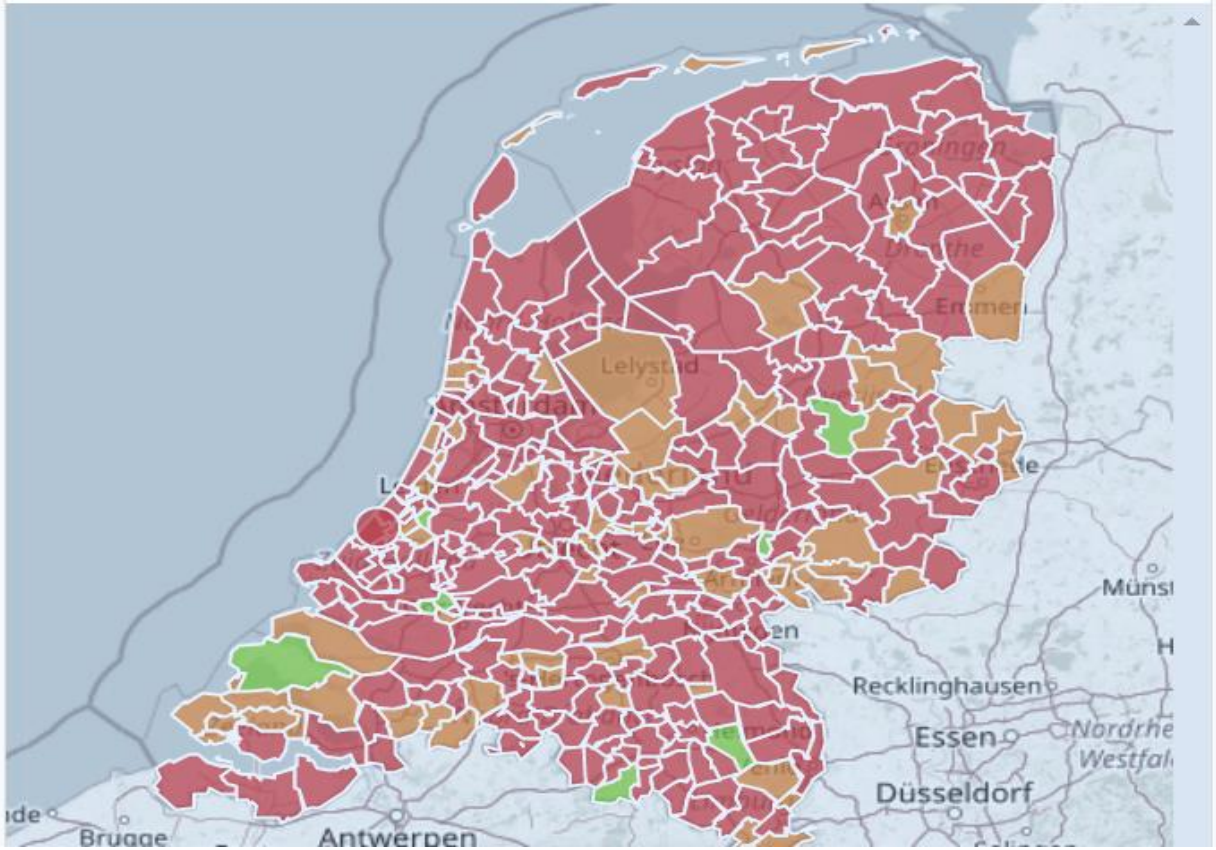
Gemeenten

343 organisaties

3 | 22% | 76%

12301 domeinen

78% | 11% | 12%



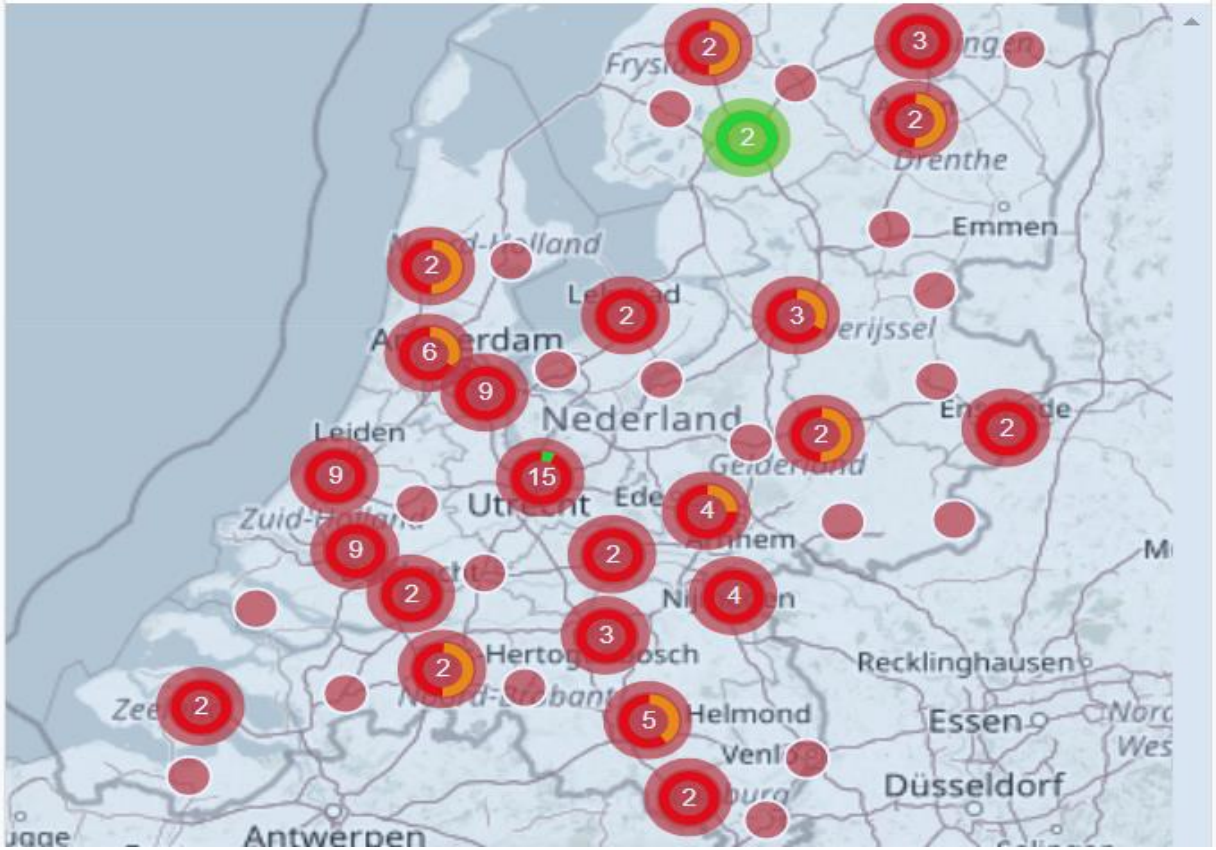
Gezondheidszorg

119 organisaties

3 | 9% | 88%

7344 domeinen

51% | 19% | 30%



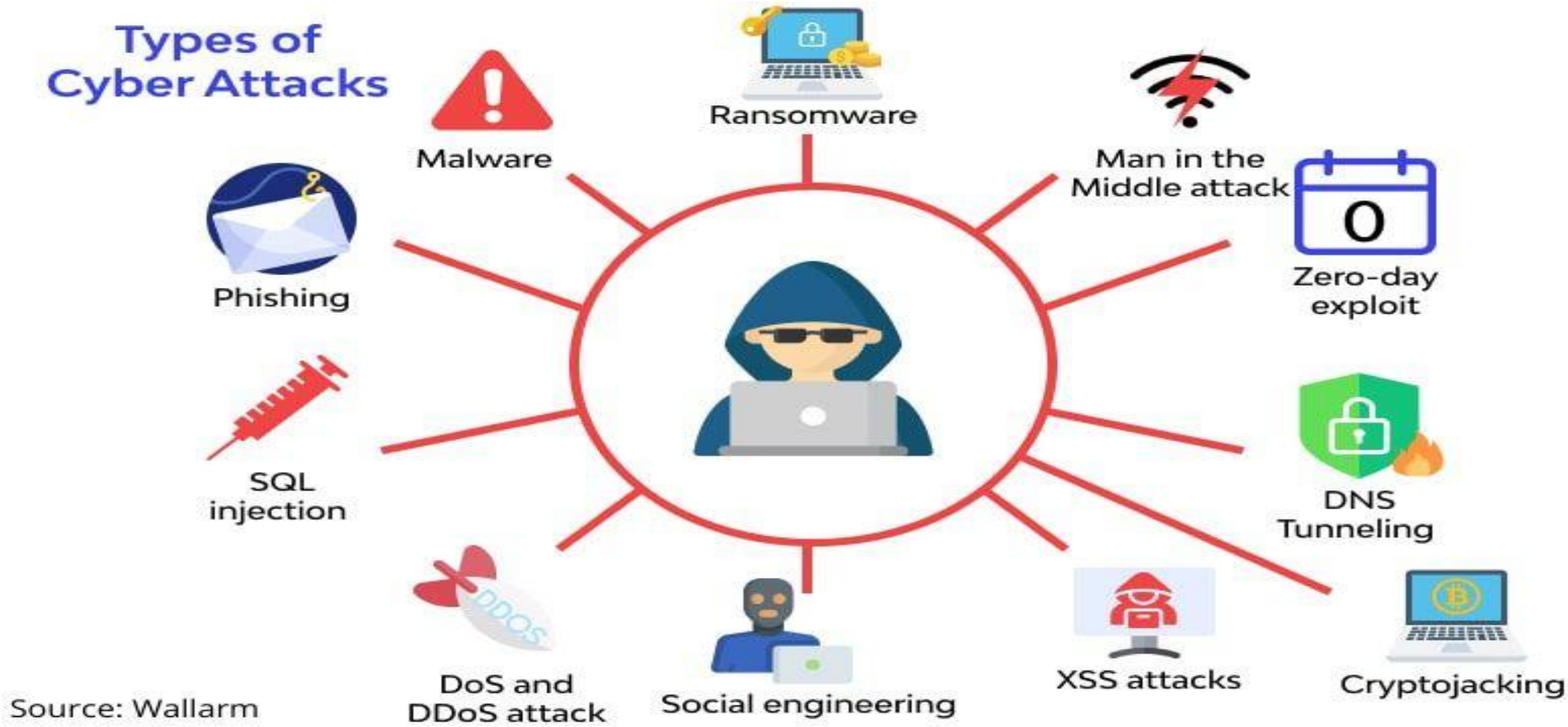
Basisbeveiliging

Deze site toont waar de overheid wel en niet voldoet aan beveiligingseisen. Het toepassen van deze eisen is gangbaar en noodzakelijk om beschikbaarheid, integriteit en vertrouwelijkheid te garanderen. De overheid, naast vele andere organisaties, stelt deze eisen zelf.

Deze site laat zien of het ook gebeurt.

Audittrail
information security | privacy | quality | grc

Dreigingen ….

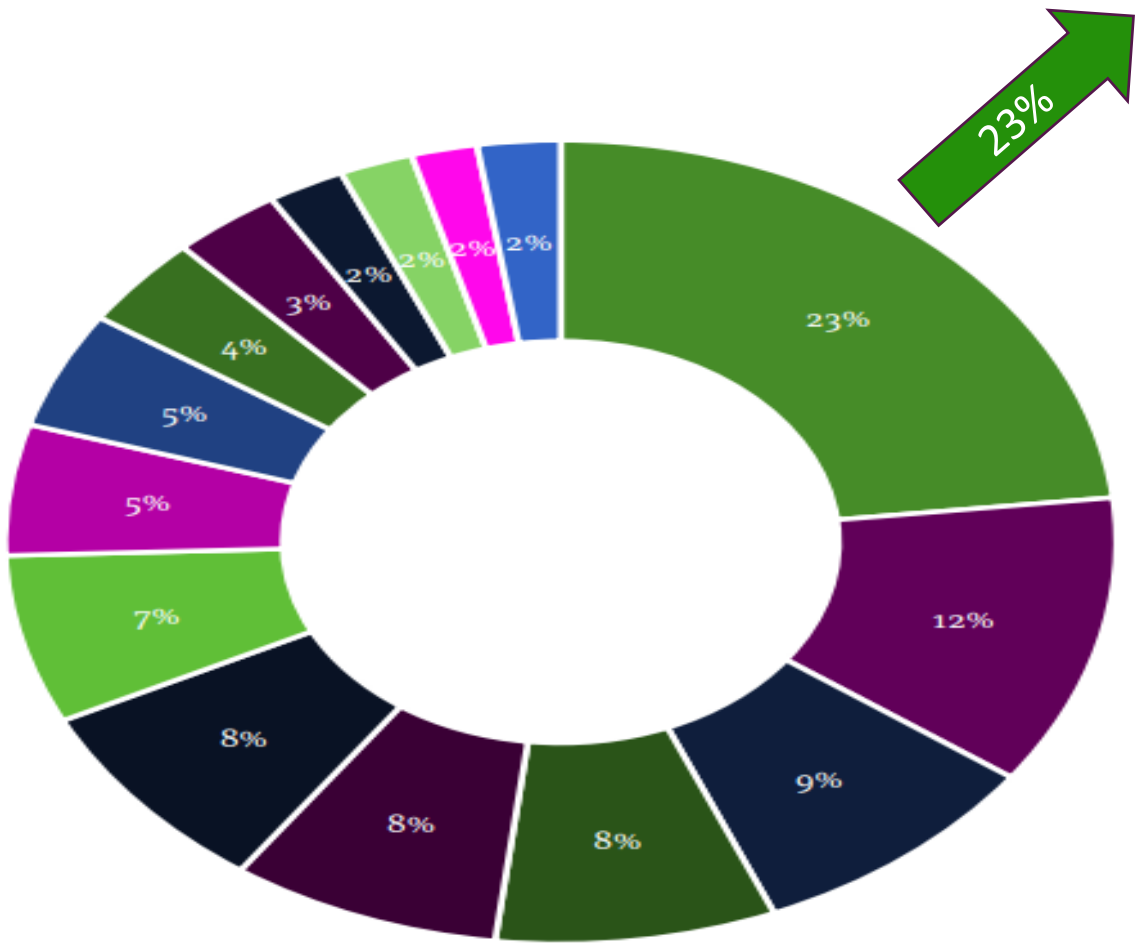


Ook Interne dreigingen en via Leveranciers ….

Cyberloketten | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

Datalekkenrapportage_AP_2022.pdf

Cyberaanvallen per sector



- Gezondheid en welzijn (23%)
- Overige organisaties (12%)
- Informatie en communicatie (9%)
- Onroerend goed (8%)
- Bouw (8%)
- Financiële dienstverlening (8%)
- Onderwijs (7%)
- Handel en autobranche (5%)
- Specialistische zakelijke dienstverlening (5%)
- Industrie (4%)
- Openbaar bestuur (3%)
- Overige zakelijke dienstverlening (2%)
- Cultuur, sport en recreatie (2%)
- Vervoer (2%)
- Overig (2%), waaronder Engerie, Horeca, Water en milieu, Landbouw, bosbouw en visserij, Politie en Justitie en Mijnbouw. (allen <1%)

Audittrail
information security | privacy | quality | grc

‘Rat-Race’ > wapen je!

Datalekkenrapportage_AP_2022.pdf

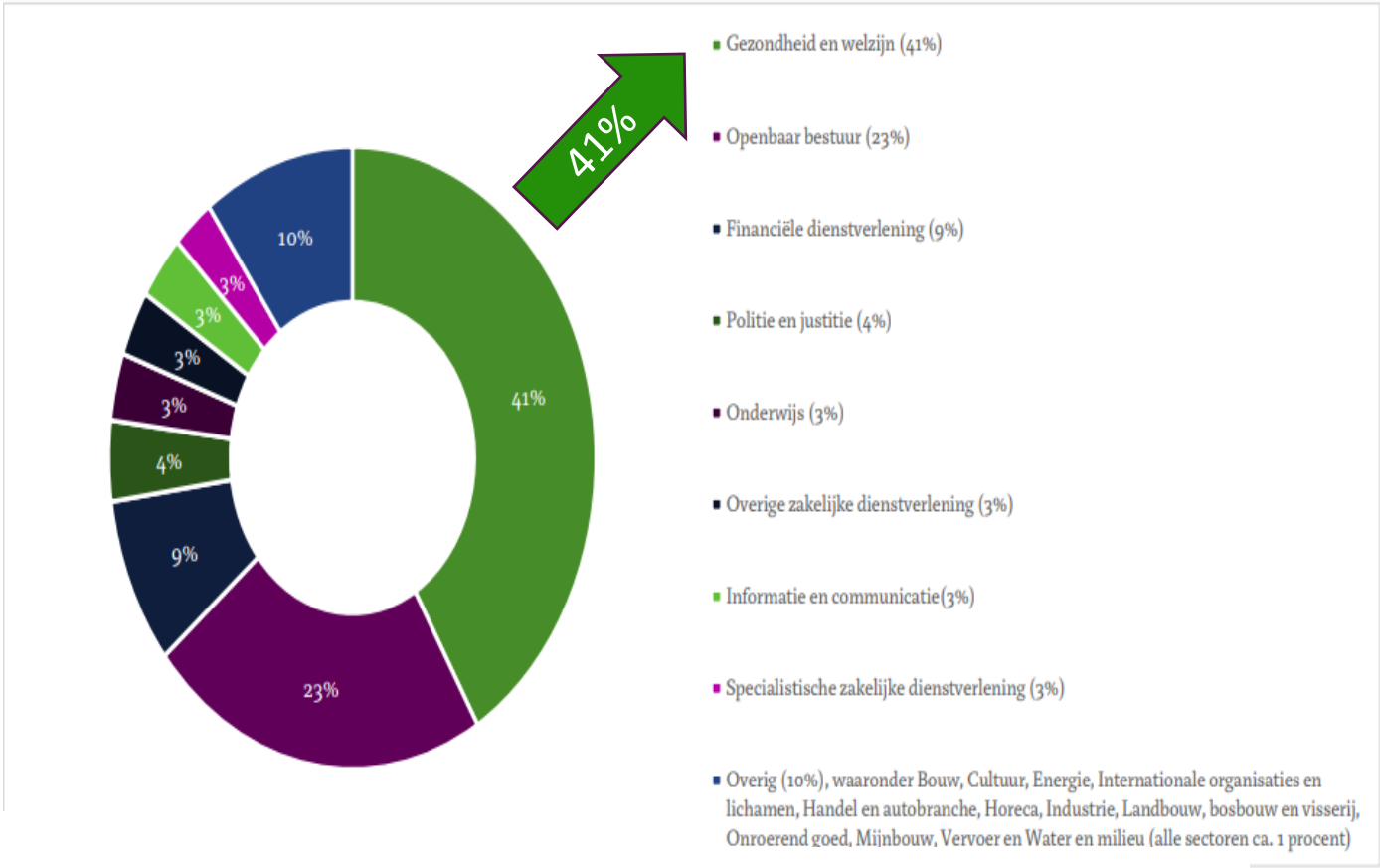
Datalekkenrapportage 2022

Aantal datalekmeldingen 2022	Aantal meldingen van cyberaanvallen 2022	Aantal datalekmeldingen afgelopen 5 jaar
21.151	1.826	114.258

5 jaar datalekken: iedereen kan slachtoffer worden

Aantal datalekmeldingen per sector

In 2022 is het aantal meldingen uit de sector financiële dienstverlening gedaald met 29% ten opzichte van 2021. Het aantal meldingen uit de sector openbaar bestuur is gedaald met 16% en het aantal meldingen uit de sector gezondheid en welzijn is gedaald met 6%.



Het afgelopen jaar zijn door de drie grootste cyberaanvallen in de zorg naar schatting 900.000 patiënten getroffen. Van hen zijn medische gegevens op straat komen te liggen. Bijna een kwart van de gemelde datalekken over cyberaanvallen was in 2022 afkomstig uit de zorgsector.

Audittrail
information security | privacy | quality | grc

Datalekkenrapportage AP 2022

Datalekkenrapportage 2022

Aantal datalekmeldingen 2022	Aantal meldingen van cyberaanvallen 2022	Aantal datalekmeldingen afgelopen 5 jaar
21.151	1.826	114.258

5 jaar datalekken: iedereen kan slachtoffer worden

Gezondheid & Welzijn:
Cyberaanvallen 23%
Datalekken 41%

Audittrail
information security | privacy | quality | grc

Casus: Hack met datadiefstal - Hogeschool Arnhem en Nijmegen

1 sep 2021 e.v.

VEELGESTELDE VRAGEN OVER HET DATALEK BIJ DE HAN

Datalek (han.nl)

Op 1 september 2021 hebben we bericht ontvangen dat er persoonsgegevens in handen zijn gekomen van derden. Ondanks al onze inspanningen om een digitaal veilige omgeving te bieden, waren we helaas niet bestand tegen deze aanval. Onze excuses aan iedereen die op de een of andere manier last ondervindt van dit incident. We proberen je zo goed mogelijk bij te staan met de concrete tips en adviezen op deze pagina. De veelgestelde vragen op deze pagina worden bijgewerkt op basis van de updates en de vragen die leven.

NOS Nieuws • Vrijdag 3 september 2021, 12:46

Hacker perst hogeschool van Arnhem en Nijmegen af

Een onbekende perst de hogeschool van Arnhem en Nijmegen af. Hij heeft mogelijk data van studenten en medewerkers in handen en eist een onbekend bedrag. Dat meldt een bron aan de NOS en een woordvoerder van de HAN bevestigt dat.

Foto ter illustratie © Getty Images/fStop

Datalek bij HAN groter dan gedacht, hacker vroeg om veel meer losgeld dan 10.000 euro

Het datalek bij de Hogeschool van Arnhem en Nijmegen blijkt nog omvangrijker dan gedacht. Een hacker heeft toegang gekregen tot 530.000 mailadressen. Hij eiste voor de buitgemaakte gegevens losgeld. Dat was volgens de HAN een veelvoud van het bedrag van 10.000 euro dat tot dusver circuleerde.

Rob Berends 05-10-21, 13:28

NIEUWS

Persoonsgegevens gelekt bij Hogeschool Arnhem Nijmegen

SEPTEMBER 3, 2021 REDACTIE

De Hogeschool van Arnhem en Nijmegen (HAN) heeft bericht ontvangen dat er persoonsgegevens in handen zijn gekomen van derden. Er zijn direct maatregelen genomen en onafhankelijke experts ingeschakeld die onderzoeken wat de exacte impact is.

De onderwijsinstelling heeft contact opgenomen met het Team High Tech Crime van de politie en er is melding gemaakt bij de Autoriteit Persoonsgegevens. Toegezegd is dat zo snel mogelijk de mensen worden geïnformeerd, van wie de gegevens zijn gelekt.
De Hogeschool van Arnhem en Nijmegen telt 37.000 studenten, ruim 4.000 medewerkers en bestaat uit veertien academies met opleidingen, onderzoek en advies. Het is niet bekend gemaakt van hoeveel personen de gegevens zijn gelekt en om wat voor gegevens het gaat.

Foto ter illustratie © Getty Images/fStop

Hacker wil geld zien van HAN voor datalek waarbij '180.000 gegevens' in verkeerde handen terechtkwamen

VIDEO **ARNHEM/NIJMEGEN - De hacker die via het computersysteem van de Hogeschool van Arnhem en Nijmegen (HAN) persoonsgegevens van studenten en medewerkers in handen heeft gekregen, eist geld van de**

Gestolen data HAN openbaar na mislukte afperspoging

rtlnieuws 24° 63 km

Hogeschool betaalt hacker niet, honderdduizenden privégegevens op straat

Door Daniël Verlaan
7 september 2021 11:47 • Aangepast 7 september 2021 20:14

ONDERWIJS 06/10/2021

Onderzoek: half miljoen gedupeerden bij hack hogeschool

E-mailadressen, maar soms ook BSN-nummers, functiebeperkingen en politieke voorkeuren... het is een greep uit de gegevens van 530 duizend mensen die een hacker buitmaakte bij de hogeschool van Arnhem en Nijmegen.

DOOR HOGER ONDERWIJS PERSBUREAU AFBEELDING SOLARSEVEN / SHUTTERSTOCK

Oud-student HAN naar de rechter wegens hack op hogeschool

ANP 23 februari 2023 17:26

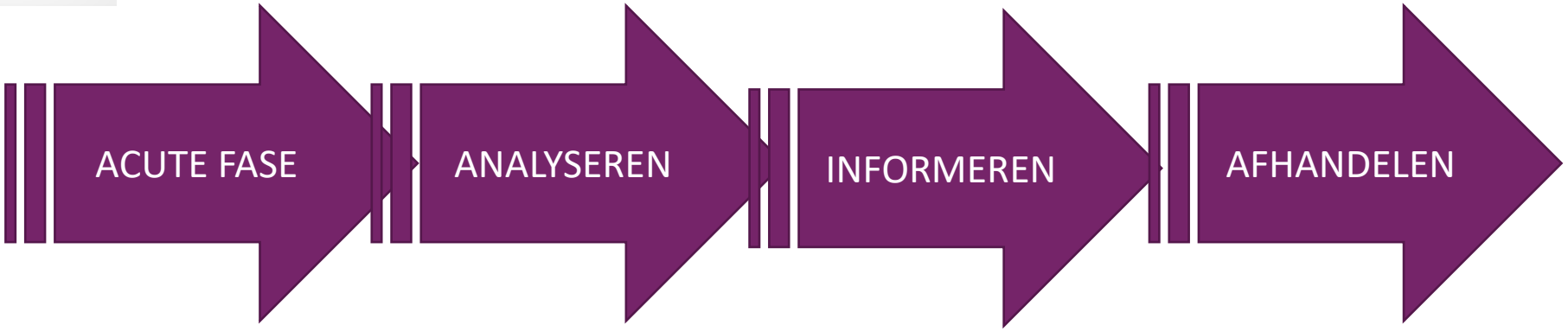
BINNENLAND

Een 28-jarige oud-student van de Hogeschool van Arnhem en Nijmegen (HAN) wil van de onderwijsinstelling een „redelijke" schadevergoeding, omdat zijn privégegevens in andere handen zijn geraakt. Dat gebeurde bij een datalek in september 2021. Bram Kleisterlee, inmiddels afgestudeerd in de communicatie, stapt ervoor naar de rechter in Arnhem, aldus studentenvakbond AKKU.

Audittrail
information security | privacy | quality | gro

Proces & Tijdlijn incident / crisis

1 sep. '21: Hack met datadiefstal



Dag/Dagen | Week/Weken | Week/Weken | Weken/Maanden

Voorbereiding op incident / crisis: Weet (oefen) wat er op je af kan komen ..

HAN_UNIVERSITY OF APPLIED SCIENCES

1 sep. '21: Hack met datadiefstal

Melding/Constatering; in welke vorm dan ook ..

ACUTE FASE

Alarmering; procedure


STAD EN STREEK 11

'The Show Must Go On' gaat niet door

door Pierre van Damme

Dienstverlening/Processen (impact?)

Crisisteam *(Kern-/Beleids- & Operationeel-)*
(en SURF-CERT (***Z-CERT***) en 'Fox-IT/Northwave/…')

Contact Hacker / Betalen Ja/Nee?

Communicatie /-Kanaal – en *Transparantie*; in-&extern (mdw's / cliënten)

Media / **Pers (rol / regie behouden**)

(Relevante) Externe Stakeholders; RvT/RvC, leveranciers, AP, Politie, eigen medewerkers, ..

Auditrail information security | privacy | quality | grc

Scenario-denken; *what-if*

HAN_UNIVERSITY OF APPLIED SCIENCES

1 sep. '21: Hack met datadiefstal

Stakeholders

Betrokkenen
AP (vervolgmelding)
Politie

Media
Medewerkers
..

Wat is er gebeurt?
Zicht op IMPACT

Analyseresultaten:
Oorzaak en
Hoeveelheid en Gevoeligheid gegevens
en
Vervolgacties

Partijen / Rollen

Systemen / Data

Forensisch onderzoek / Sporen 'inbraak'

Interne afstemming en communicatie

Audittrail
information security | privacy | quality | grc

HAN_UNIVERSITY OF APPLIED SCIENCES

1 sep. '21: Hack met datadiefstal

Starten informeren Betrokkenen (incl. afweging wel/niet en wie/wat)

Informeren stakeholders
Informeren Samenwerkingspartners

Vervolgmelding AP
Politie (i.r.t. aangifte, *let op i.r.t. communicatie (dader-info, b.v. eisen/losgeld)*

Live Blog
Media / Persbericht (behouden eigen regie / 'druk')

RESPONSE – Organisatie (1e lijns; tel./mail en 2e lijns (IB&P-team; opgelijnd)

Extra: (AVG) Inzage- en verwijderverzoeken / claims

Audittrail
information security | privacy | quality | grc

HAN_UNIVERSITY OF APPLIED SCIENCES

1 sep. '21: Hack met datadiefstal

1e en 2e Lijns Vragen / Onduidelijkheden
Inzage- & verwijderverzoeken

Claims (JZ)

AP Melding vervolmaken > Definitieve melding

…

Evaluatie

Geleerde lessen / - delen

Audittrail
information security | privacy | quality | grc

HAN_UNIVERSITY
OF APPLIED SCIENCES

1 sep. '21: Hack met datadiefstal

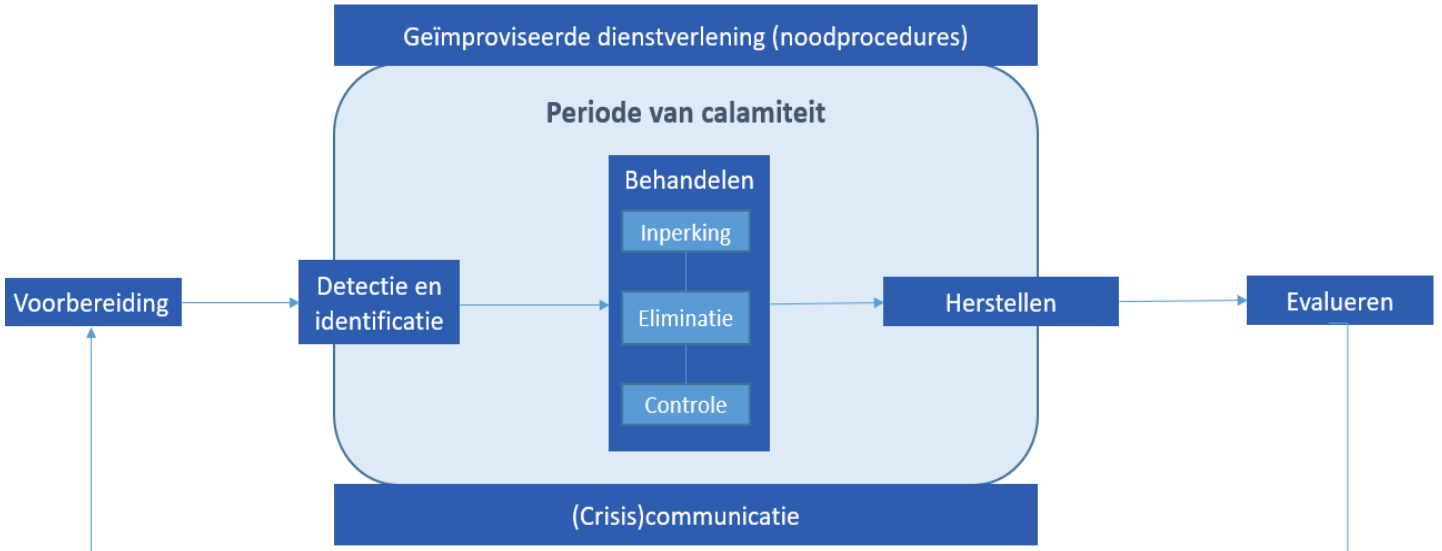
Vragen ?

Audittrail
information security | privacy | quality | grc

Zaal 1	Zaal 2	Zaal 3	Zaal 4	Zaal 5
Een cybercrisis voorkomen *Theaterzaal: Geluksfabriek*	Voorbereiden op een cybercrisis *Zaal: Sterrenstof*	Tijdens een cybercrisis *Zaal: 't Wij-land*	De nasleep van een cybercrisis *Zaal: De Optimist*	Leren van een cybercrisis *Zaal: De Twent*

Hoe bereid ik mij voor op een IB en/of P incident/crisis ?

Zijn er aspecten naar voren gekomen waarvan je denkt, hè daar moet ik aan (gaan) denken ?!
Iets vergeten ? / Aanvullingen ?



Procedures & Fasering

Audittrail
information security | privacy | quality | grc

Zaal 1	Zaal 2	Zaal 3	Zaal 4	Zaal 5
Een cybercrisis voorkomen *Theaterzaal: Geluksfabriek*	Voorbereiden op een cybercrisis *Zaal: Sterrenstof*	Tijdens een cybercrisis *Zaal: 't Wij-land*	De nasleep van een cybercrisis *Zaal: De Optimist*	Leren van een cybercrisis *Zaal: De Twent*

Voorbereiden op een IB en/of P incident/crisis ?

Crisisorganisatie (ook Security-&AVG-incidenten)
Calamiteitenplan / Incidenten proces (Procedure(s))
Bewustzijn – Monitoring en Meldingen
Oefenen – Scenario's

Dreigingsbeeld Sector / Nationaal - Aanvalsvectoren (in-&extern) – Risico's

Kritieke processen in beeld - Workarounds
IT Landschap – 'Kroonjuwelen' (B-I-V)
Leveranciers/-management

Business Continuïty Planning (BCP) / Management (BCM)


fd.

PRIVACY EN CYBERSECURITY

Cyberaanval via leverancier vormt nieuwe bedreiging voor bedrijven

Hackers vallen bedrijven steeds vaker binnen via leveranciers en andere bedrijven waar ze zaken mee doen. De meeste zaken komen niet aan het licht.

Vooraf: Wel/niet betalen?

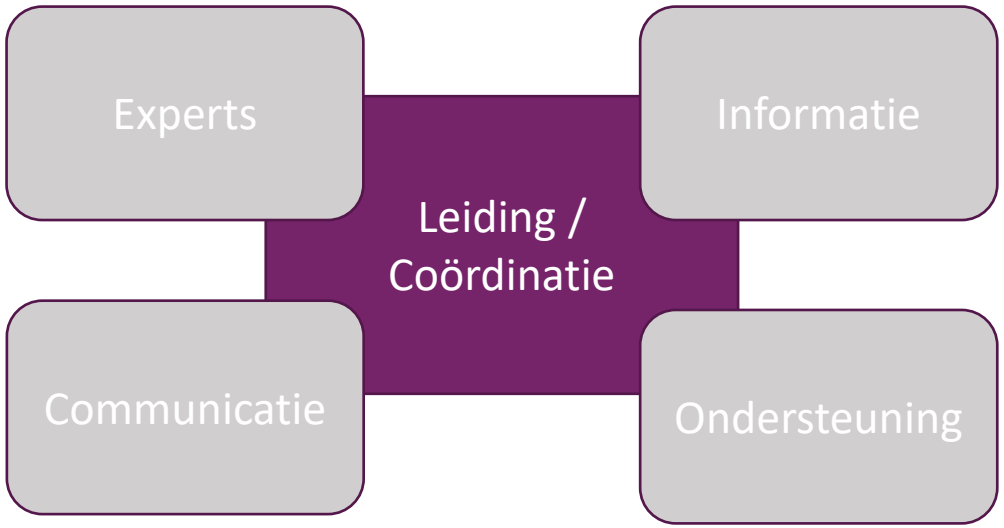
Verzekeren?
Testen?

Detectie/Meldpunt

Communicatie (in-&extern en transparantie)

Audittrail
information security | privacy | quality | grc

Crisisorganisatie (theorie)



Crisisbeleidsteam (strategisch)

Crisiscoördinator

Operationeel Crisisteam

Uitvoerende diensten en afdelingen

Bron:
Leidraad crisisorganisatie in de zorgsector (oto)

Audittrail
information security | privacy | quality | grc

HAN_UNIVERSITY OF APPLIED SCIENCES

1 sep. '21: Hack met datadiefstal

Samenstelling
Alarmering(-swijze)

Crisisorganisatie (praktijk / voorbeeld)

Crisisteam / Crisismanagementteam

-Voorzitter
-Plotter
-Communicatieadviseur – Woordvoerder
-Vertegenwoordiger(s) Staf IM /& Dienst/Services / Fac. & IT
-Crisiscoördinator IV
-Lid / CIO
-CISO *(en FG Beschikbaar / advies)*
-Vertegenwoordiger business / primaire proces/dienst/product

Extern:
-Expert Crisiscommunicatie (beginfase)
-IT&Privacy-recht advocaat
-Forensisch Team & SURF-CERT (indirect)

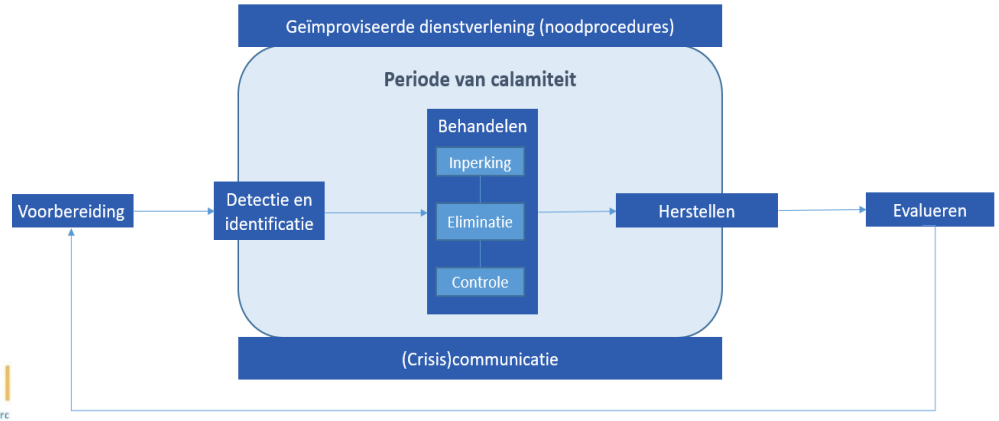
Teams
-Scenario/Communicatie
-Techniek/CERT
-Forensisch/Compliance

Auditrail information security | privacy | quality | grc

Groot incident > doorlooptijd lang > vervanging

Samenwerking
Competenties

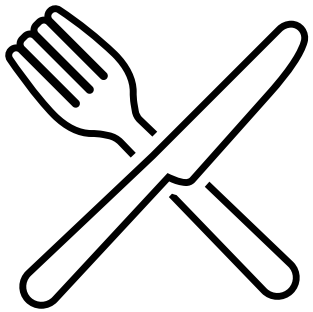
Aanvullingen / Wat nog meer :



Audittrail
information security | privacy | quality | grc

Afsluitend:

Bedankt
voor jullie aandacht en inbreng!
Nog veel plezier.



N.b.: ik blijf nog even .. Heb je (individuele) vragen; kom gerust / zoek mij op.

Audittrail
information security | privacy | quality | grc

BLIJF IN VERBINDING.

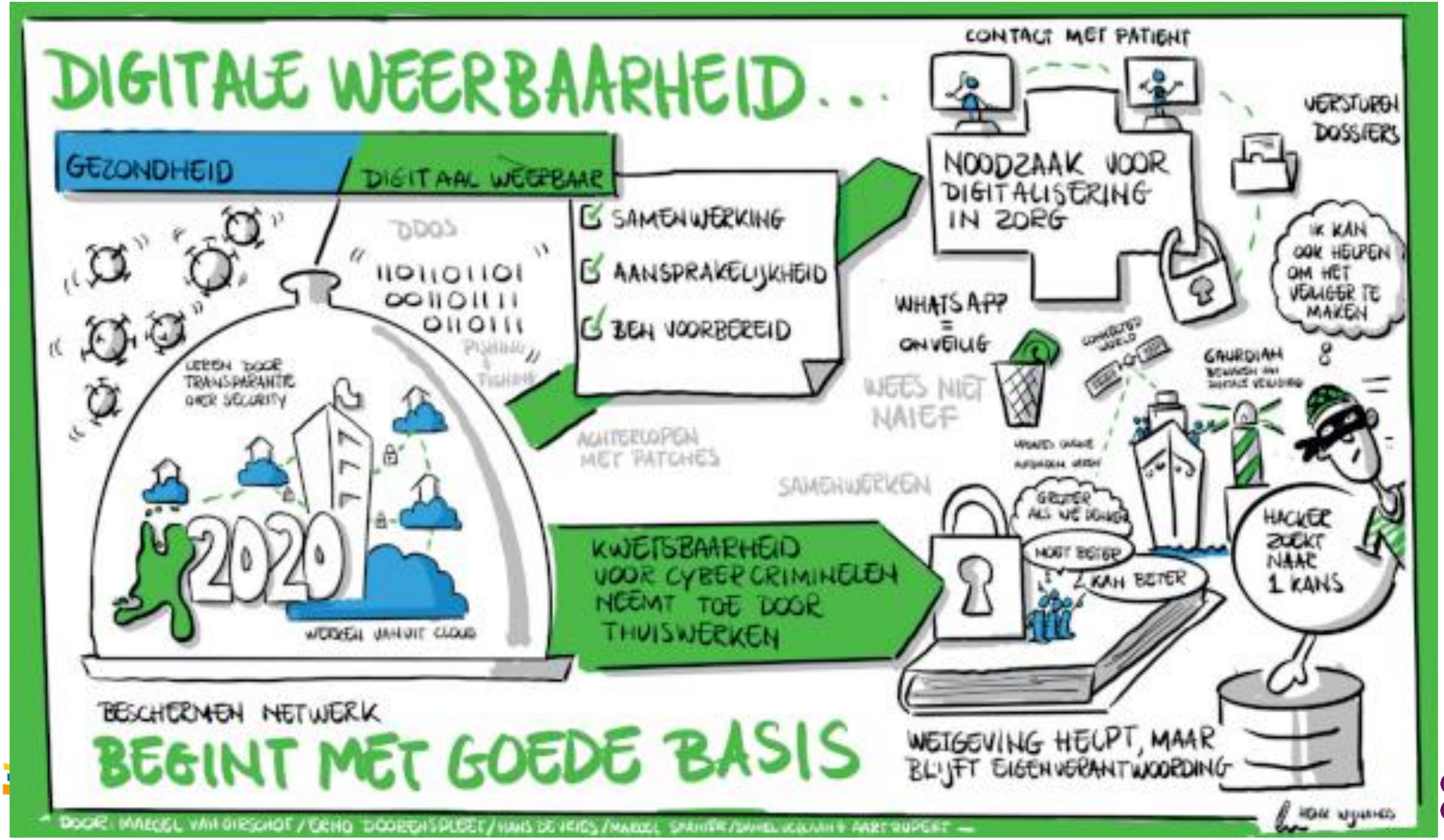
+ Volg ons op LinkedIn

communicatie@zorgnetoost.nl

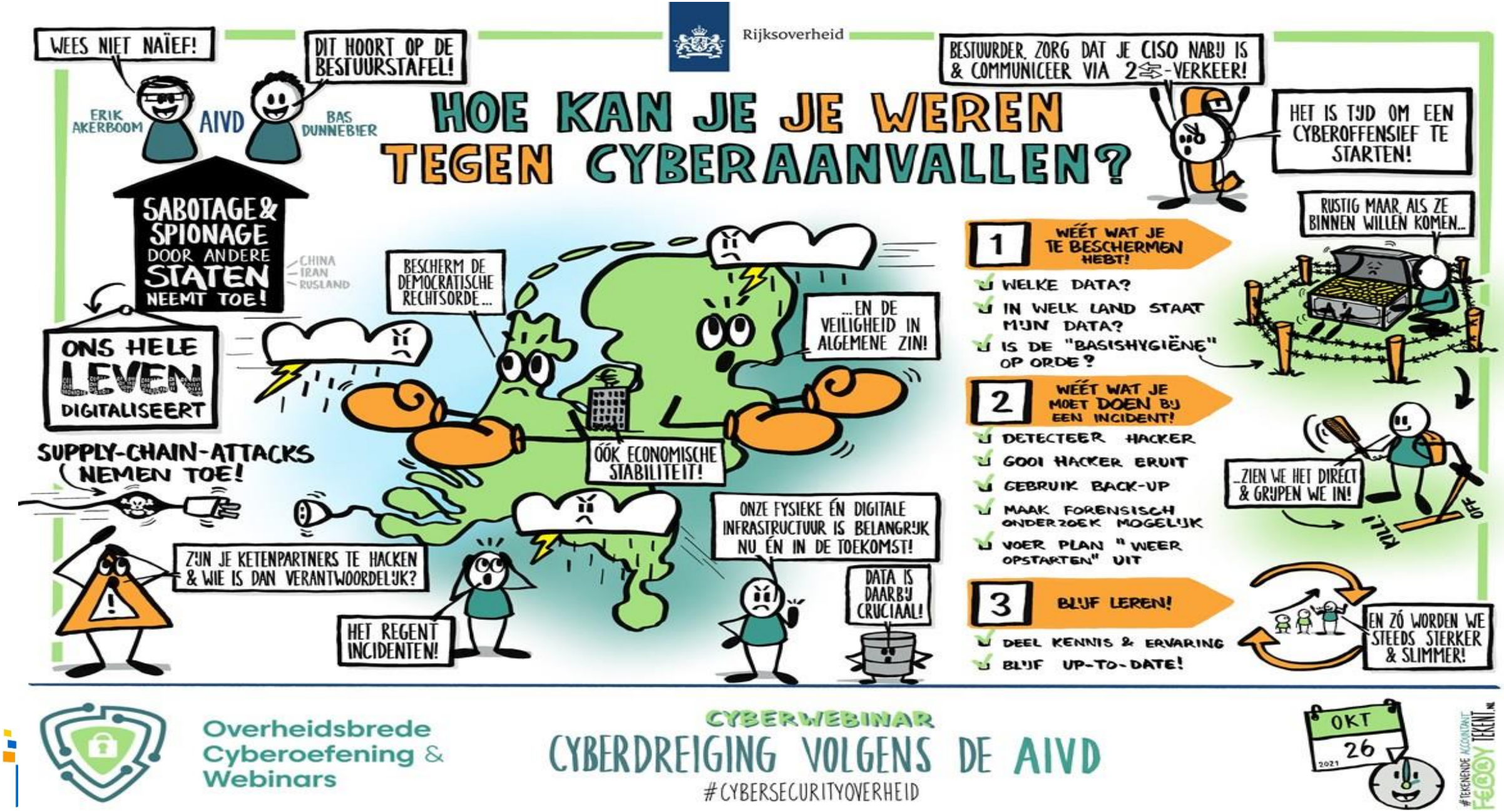
www.zorgnetoost.nl

Audittrail
information security | privacy | quality | grc

EXTRA / ACHTERGROND INFORMATIE


DIGITALE WEERBAARHEID...
GEZONDHEID
DIGITAAL WEERBAAR
SAMENWERKING
AANSPRAKELIJKHEID
BEN VOORBEREID
CONTACT MET PATIENT
NOODZAAK VOOR DIGITALISERING IN ZORG
VERSTUREN DOSSIERS
IK KAN OOK HELPEN OM HET VEILIGER TE MAKEN
WHATSAPP = ONVEILIG
WEES NIET NAIEF
GUARDIAN
DDOS
PHISHING
LEREN DOOR TRANSPARANTIE OVER SECURITY
2020
WERKEN VANUIT CLOUD
ACHTERLOPEN MET PATCHES
SAMENWERKEN
KWETSBAARHEID VOOR CYBERCRIMINELEN NEEMT TOE DOOR THUISWERKEN
GROTER ALS VROEGER
HOUT BEGER
KAN BETER
HACKER ZOEKT NAAR 1 KANS
BESCHERMEN NETWERK
BEGINT MET GOEDE BASIS
WEIGEVING HELPT, MAAR BLIJFT EIGEN VERANTWOORDING

Organisaties moeten hier (dus) ook ‘iets’ aan doen … *(compliance - governance - …)*



Overheidsbrede Cyberoefening & Webinars

CYBERWEBINAR

CYBERDREIGING VOLGENS DE AIVD

#CYBERSECURITYOVERHEID

OKT 26 2021

#TEKENENDE ACCOUNTANT FEBBY TEKENT.NL

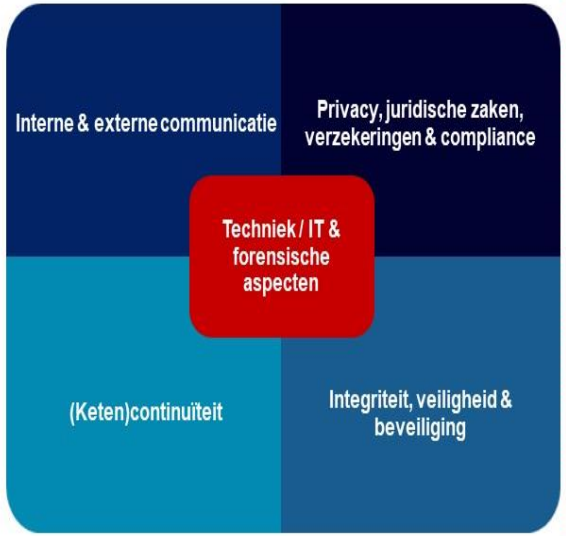
CYBER & CRISISMANAGEMENT

Thema's & valkuilen – 26 mei 2021

Aon Empower Results® | COT Instituut voor Veiligheids- en Crisismanagement An Aon Company | www.cot.nl

Terugkerende thema's bij een cybercrisis

Een cyberincident kan uitgroeien tot een crisis. Het samenspel tussen betrokken specialisten en eindbeslissers is cruciaal in het crisismanagement. In de praktijk zien wij dat er terugkerende thema's zijn die aandacht behoeven. Ook zijn er terugkerende valkuilen.



Terugkerende valkuilen

- Te late detectie
- Te late escalatie
- Interne rolverdeling, mandaten & taken onduidelijk
- 'Taalbarrière' tussen IT & directie: technisch-bestuurlijk gat
- BCM niet voorbereid
- Assets & gerelateerde processen niet in beeld
- Besluitvorming (o.a. rondom ransomware) niet doordacht
- Te passieve communicatie
- Onzichtbaar leiderschap

Auditrail
information security | privacy | quality | grc

CYBER & CRISISMANAGEMENT

TIPS VOOR GEMEENTEN

Aon Empower Results® | COT Instituut voor Veiligheids- en Crisismanagement An Aon Company | www.cot.nl

TIPS VOOR DE RESPONS

Iedere gemeente kan te maken krijgen met een cyberincident dat uit kan groeien tot een crisis. Goede preventie en security zijn cruciaal. Maar wat als het toch mis gaat? Op basis van eerdere incidenten en oefeningen geven we 10 tips.

1. Zorg voor mitigerende maatregelen om impact te beperken. Schakel zo snel benodigde forensische expertise in: onderzoek, advies & attributie

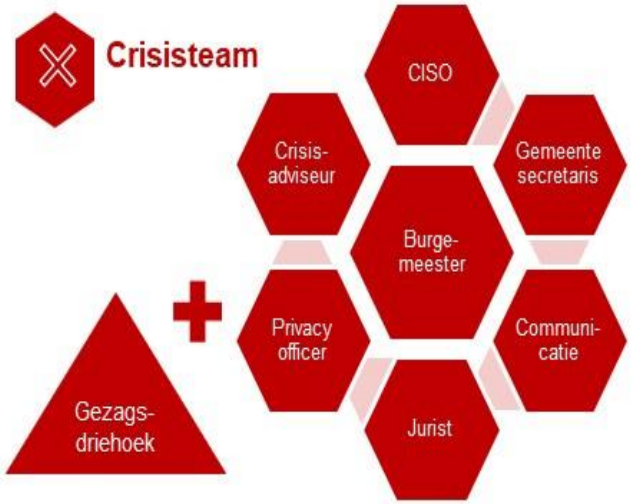
2. Escaleer tijdig naar de gemeentesecretaris en de burgemeester.

3. Formeer een crisisteam en benoem ondersteunende teams (IT, communicatie, continuïteit).

4. Schakel tijdig hulplijnen in: IBD (informatie, advies & netwerk), politie, veiligheidsregio. Weet wat je wel en niet kunt verwachten qua hulp.

5. Wees transparant in de publiekscommunicatie maar houd rekening met de risico's (zoals reactie aanvallers of anderen die misbruik willen maken van de situatie).

Crisisteam



6. Bij ransomware: houd een moreel beraad om tot zorgvuldige afwegingen en besluiten te komen.

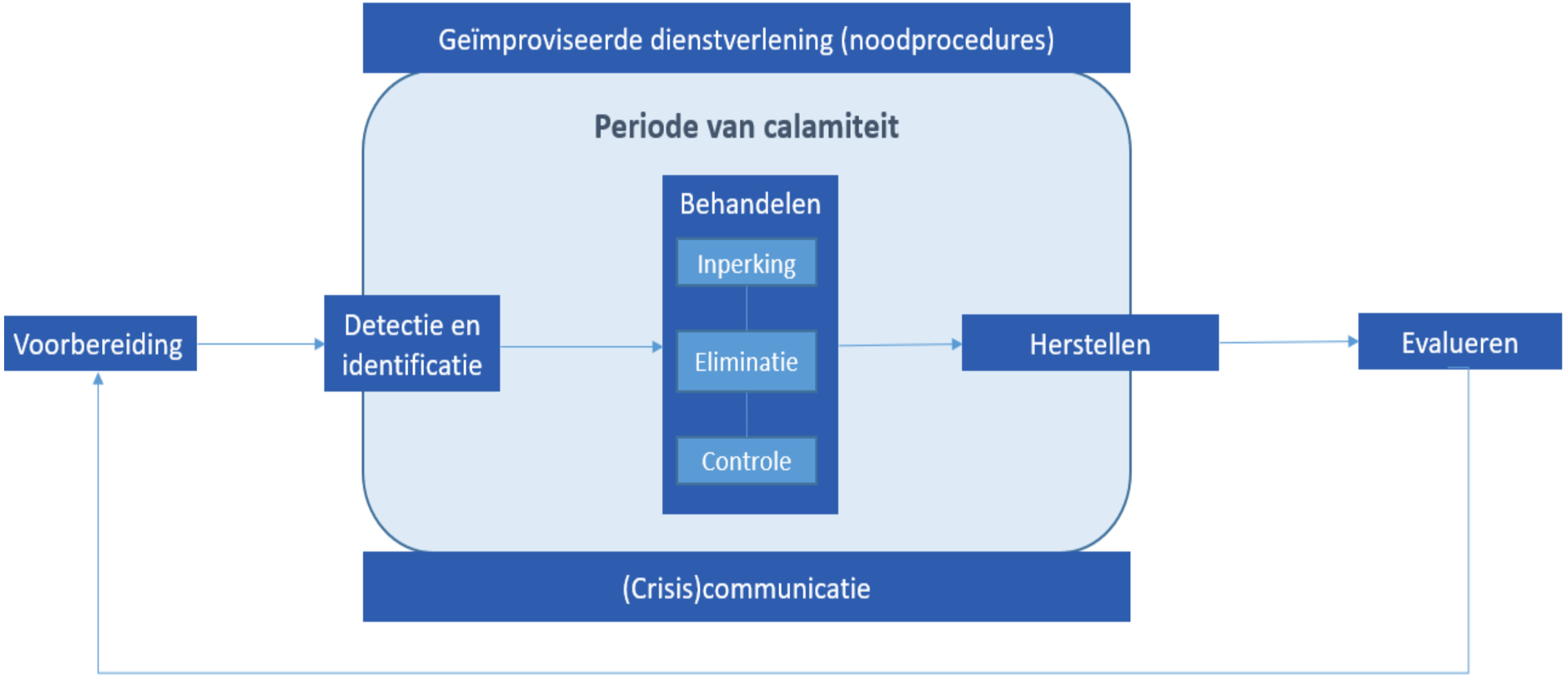
7. Bij datalek: volg procedures voor melden aan Autoriteit Persoonsgegevens.

8. Betrek de gemeenteraad bij sleutelbesluiten.

9. Houd rekening met langdurige impact, intensief herstel en forse kosten.

10. Zorg voor nazorg intern.

BCM / Incident Response



Audittrail
information security | privacy | quality | grc

1. Fasen aanval

Fase 1
Aanval

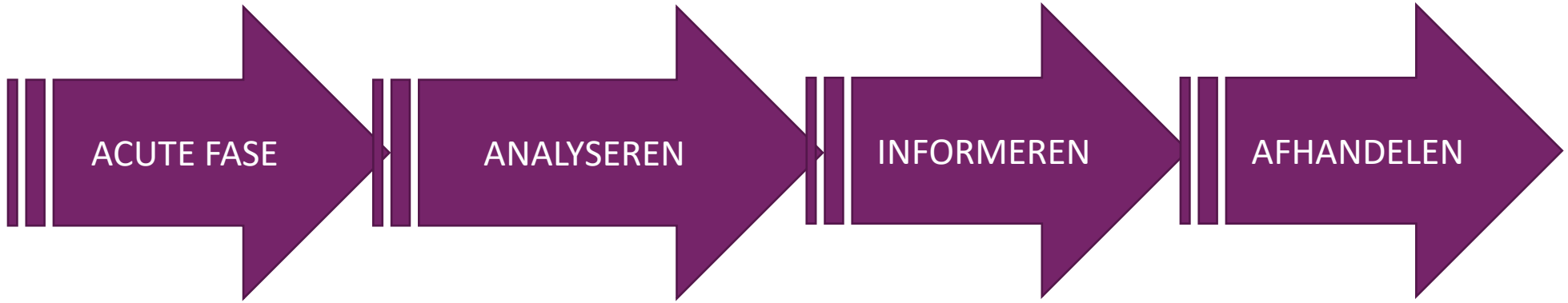
Fase 2
Detectie

Fase 3
Response

Fase 4
Brand meester

Fase 5
Nazorg

Bron: UvA/HvA (2021)



IB/Security	AANVAL	DETECTIE	RESPONSE	LEK GEDICHT	NAZORG & EVALUATIE
AVG/Datalek	WERKFOUT / MELDING MOGELIJK DATALEK	ONDERZOEK & VASTSTELLING DATALEK	IMPACT VERMINDEREN / RISICO-MITIGATIE BETROKKENEN	MELDING AP / BETROKKENEN	NAZORG & EVALUATIE

Auditrail
information security | privacy | quality | grc

Bron: Erik van den Beld

Speelveld AVG / GDPR

25 mei 2018

Jullie !

empowerment

'Betrokkenen'

FG

Delen direct of indirect hun persoonsgegevens

Stellen doel van & middelen voor verwerking vast

Verwerken persoons-gegevens

Verwerkings-verantwoordelijken

Verwerkers

X

Jullie !

Ketenverantwoordelijkheid

Houden toezicht & behandelen klachten

Toezichthoudende Autoriteiten

In Nederland is dit

AUTORITEIT PERSOONSGEGEVENS

Monitort de toepassing van de GDPR

accountability

European Data Protection Board

Speelveld van de GDPR

Audittrail
information security | privacy | quality | grc

3Lines-model

‘IB&P- Governance’

1

Eerste lijn

Het lijnmanagement (de business) is verantwoordelijk voor haar eigen processen

2

Tweede lijn

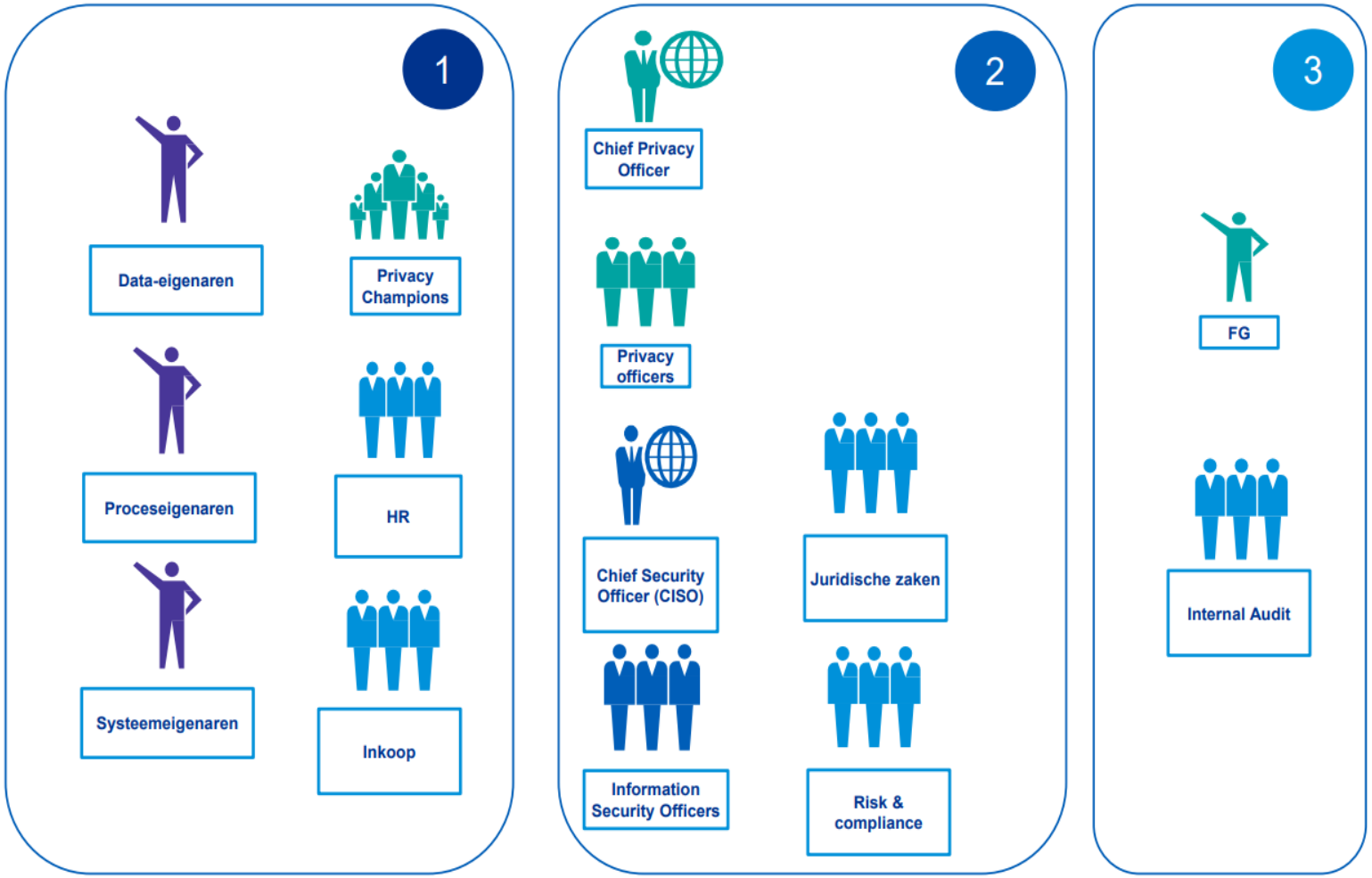
Ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijk heden neemt.

3

Derde lijn

Controleert de eerste en tweede lijn, en velt daarover een objectief, onafhankelijk oordeel tot verbetering.

Privacyrollen en -verantwoordelijkheden



Audittrail
information security | privacy | quality | grc

5_tips_voor_zorginstellingen_om_datalekken_te_voorkomen.pdf

AUTORITEIT
PERSOONSGEGEVENS

5 tips voor zorginstellingen om een datalek te voorkomen

Zorginstellingen kunnen bepaalde maatregelen nemen om de kans op een datalek te verkleinen, of de gevolgen ervan te beperken. Met deze maatregelen kunt u een aantal veel voorkomende typen datalekken voorkomen.

Door menselijke fouten kunnen medische gegevens bij een verkeerde ontvanger terecht komen, bijvoorbeeld door een typefout in het e-mailadres, of door een verkeerde geadresseerde aan te klikken.

- Dit kunt u voorkomen door ervoor te kiezen om de gevoelige gegevens als bijlage op te nemen in het e-mailbericht en deze bijlage te versleutelen met een wachtwoord.
- Dit wachtwoord kunt u vervolgens via een apart kanaal (bijvoorbeeld door te bellen of per SMS) doorgeven aan de ontvanger.
- U kunt zich ook afvragen of e-mail wel het juiste digitale communicatie middel is om dit soort gevoelige gegevens te versturen en bijvoorbeeld overwegen om communicatie via een portaal te organiseren.

Gevoelige dossiers zoals medische dossiers, (jeugd)hulpdossiers, en verslagen over behandeltrajecten worden weleens meegenomen naar huis, bijvoorbeeld in het kader van thuiswerken. Dossiers worden per abuis verloren, vergeten in de trein, of soms zelfs gestolen.

- Voorkom dit door nooit gevoelige papieren zorgdossiers mee naar huis te nemen.
- Scan de dossiers op kantoor en bewaar deze op een beveiligde (versleutelde) harde schijf, USB-stick of in een veilig documentmanagementsysteem binnen het IT-netwerk van uw organisatie. U kunt in het laatstgenoemde geval de dossiers dan thuis raadplegen wanneer u inlogt op de beveiligde netwerkomgeving.

Zorginstellingen slaan soms medische gegevens van patiënten lokaal op draagbare apparatuur, zoals tablets, smartphones, laptops of USB-sticks op. Medewerkers nemen deze gegevensdragers weleens mee naar huis. Met risico's op verlies en diefstal waardoor persoonsgegevens in verkeerde handen kunnen vallen.

- Voorkom dit door geen medische gegevens op te slaan op draagbare apparatuur.
- Maakt u wel gebruik van draagbare apparatuur? Zorg dan dat u deze persoonsgegevens altijd versleuteld opslaat. Zo beperkt u de risico's voor de betrokkenen, wanneer u een draagbaar apparaat verliest of wanneer deze wordt gestolen.

Zorginstellingen, met name ziekenhuizen, zijn vaak doelwit zijn van dit phishing-aanvallen. Daardoor kan een hacker toegang krijgen tot het account van de medewerker. Vaak misbruiken hackers het account vervolgens om nieuwe phishing- of spamberichten te versturen. Dat kan tot nieuwe inbreuken leiden, en/of tot (financiële) schade voor de betrokkenen.

- Verklein de kans op phishing-aanvallen door uw medewerkers bewust te maken van phishing.
- Zorg ervoor dat medewerkers phishing e-mails kunnen herkennen.
- Installer goede firewalls en update deze tijdig, zodat u ongewenste e-mailberichten, zoals spam- en phishing berichten, zoveel mogelijk kunt onderscheppen en blokkeren.

Met name kleinere zorginstellingen en zorgverleners zoals fysiotherapeuten en huisartsen worden regelmatig getroffen door ransomware. Vaak als gevolg van gebrekkige (kennis over) beveiliging. Als gevolg van ransomware kunnen de gegevens op uw systeem in handen komen van hackers, en kunt u permanent of tijdelijk de toegang tot uw gegevens verliezen.

Maatregelen waarmee u het risico op een datalek bijvoorbeeld door ransomware verkleint:

- Installeer software-updates op tijd
- Gebruik geen verouderde (netwerk)protocollen
- Zorg voor gesegmenteerde (gescheiden) computernetwerken en -systemen
- Maak regelmatig back-ups te zodat u altijd beschikking heeft tot de persoonsgegevens, ook wanneer u getroffen wordt door een ransomware-aanval.

Stappenplan: kom in actie bij een datalek

Heeft uw organisatie te maken met een datalek? Dan is het belangrijk dat u als privacycontactpersoon snel in actie komt. Met dit stappenplan helpen we u op weg.

Stap 1: zorg voor overzicht

Analyseer onmiddellijk de situatie. Zorg dat u weet wat er is gebeurd en wat de omvang van het lek is. Gaat het om een inbreuk door gelekte, vernietigde of gewijzigde gegevens? Indien gegevens zijn gelekt, onderzoek dan wie er (mogelijk) toegang hebben (gehad) tot welke persoonsgegevens. Deze informatie heeft u nodig voor de vervolgstappen.

Stap 2: Beperk de schade!

Bepaal op basis van stap 1 of er maatregelen zijn die u meteen kunt nemen om het datalek te beëindigen en de schade te beperken. En zo ja, neem deze maatregelen onmiddellijk. Bijvoorbeeld door een gestolen laptop op afstand te wissen. Maak tegelijkertijd een inschatting van het (mogelijke) risico dat het datalek oplevert (stap 3).

Stap 3: Wel/niet melden bij de AP

Bepaal of u het datalek verplicht moet melden bij de Autoriteit Persoonsgegevens (AP). Zo ja, zorg dat u dit ***binnen 72 uur*** nadat u het lek heeft ontdekt doet. U moet een datalek melden bij de AP tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.

Heeft u bij de eerste melding nog niet alle informatie over het datalek?
Doe dan een eerste melding binnen 72 uur en doe later een vervolgmelding.

Naar het meldloket datalekken
Zie ook: voorbeeldlijst 'datalek wel/niet melden bij AP en betrokkenen'

Stap 4: Wel/niet melden aan de betrokken personen

Bepaal of u het datalek verplicht moet melden aan de betrokken personen. Zo ja, zorg dat u dit zo snel mogelijk doet. U moet een datalek melden aan de betrokken personen wanneer er sprake is van een *hoog* risico voor de rechten en vrijheden van de betrokken personen.

Stap 5: Registreer het datalek

Registreer het datalek in uw verplichte datalekregister. Ook wanneer u het datalek niet meldt aan de AP.

Zie ook: 10 praktische tips voor betere datalekregistratie

Heeft u bovenstaande stappen doorlopen? En alles gedaan om de schade te beperken?
Start dan een evaluatie om een herhaling van het datalek te voorkomen.

Audittrail
information security | privacy | quality | grc

stappenplan_actie_datalek.pdf