INFORMATIE
BEVEILIGINGS
DIENST

Privacy (be)Spreekuur: Gestructureerde aanpak verhogen beveiligingsbewustzijn

Ger Lütter en John van Huijgevoort, adviseurs IBD

28 juli 2020

VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

Privacyverklaring

De IBD stelt Zoom privacyvriendelijk in (privacy by default)

Tijdens de interactieve online bijeenkomsten maakt de IBD:

- gebruik van wachtwoorden om aan vergaderingen deel te nemen.
- gebruik van unieke vergader ID’s om vergaderingen af te schermen.
- geen gebruik van:
  “cloud recording” en neemt de videoconferentie niet op.
  “local Recording”
  “automatically Transcribe Cloud Recordings”
  “attendee attention tracking”

INFORMATIE BEVEILIGINGS DIENST

Even voorstellen

Naomi Berger, Moderator

Ger Lütter en John van Huijgevoort, adviseurs IBD

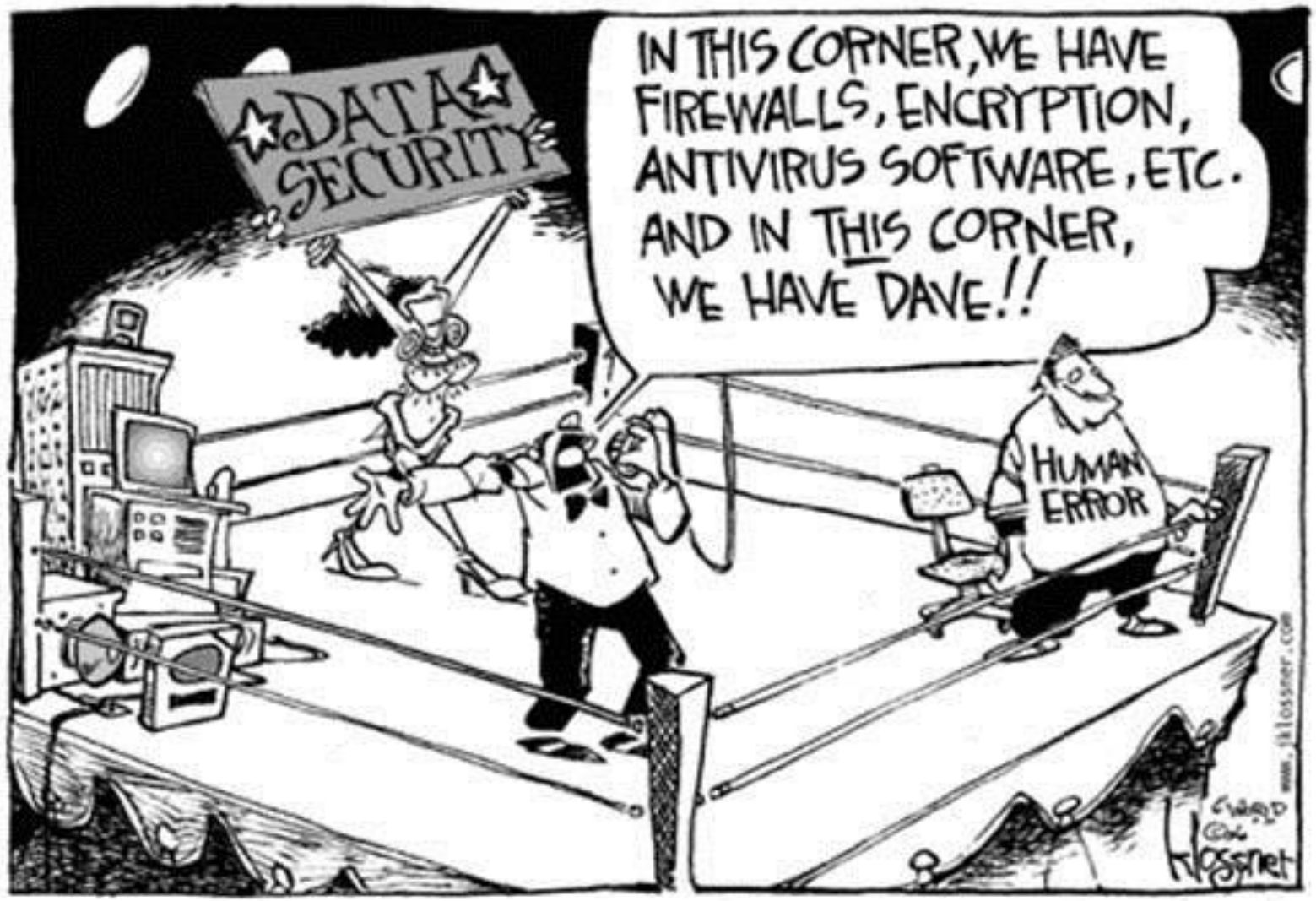
INFORMATIE BEVEILIGINGS DIENST

Doel van dit (be)Spreekuur

- Aangeven waarom IB&P-bewustzijn zo belangrijk is
- Waardoor wordt het IB&P-bewustzijn bepaald?
- Welke fasen van IB&P-bewustzijn zijn er te onderscheiden?
- Hoe pak je verhogen IB&P-bewustzijn gestructureerd aan?
- Vertaling naar de praktijk
- Checklist en tips
- Ruimte voor vragen (ook tussendoor)

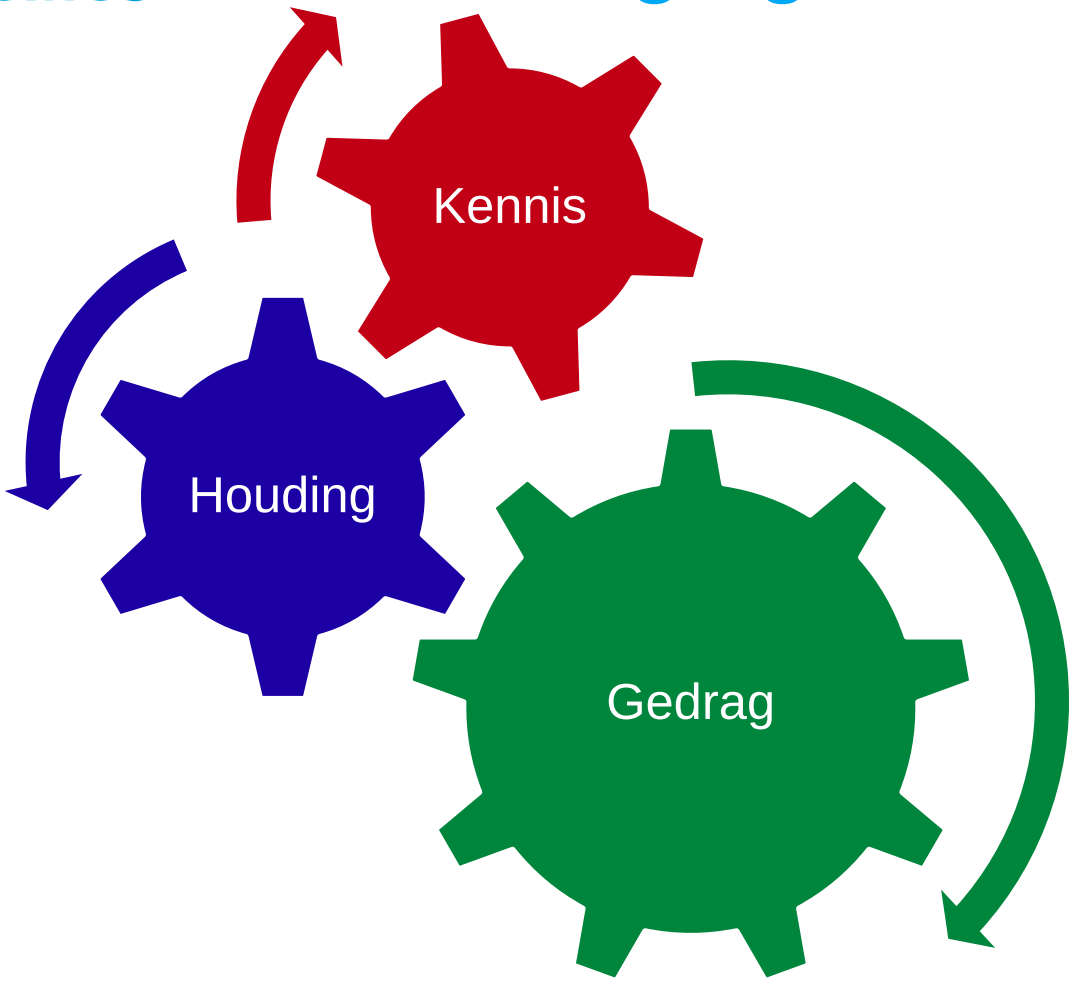
INFORMATIE
BEVEILIGINGS
DIENST

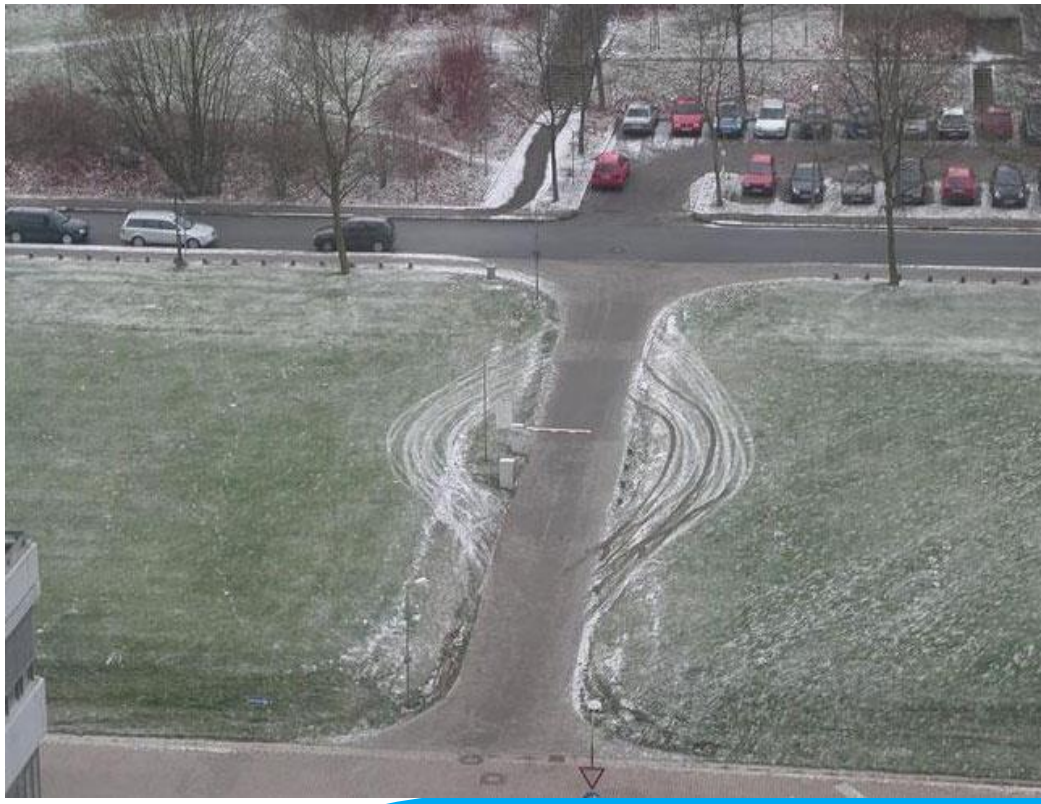
De mens is de zwakste schakel



INFORMATIE BEVEILIGINGS DIENST

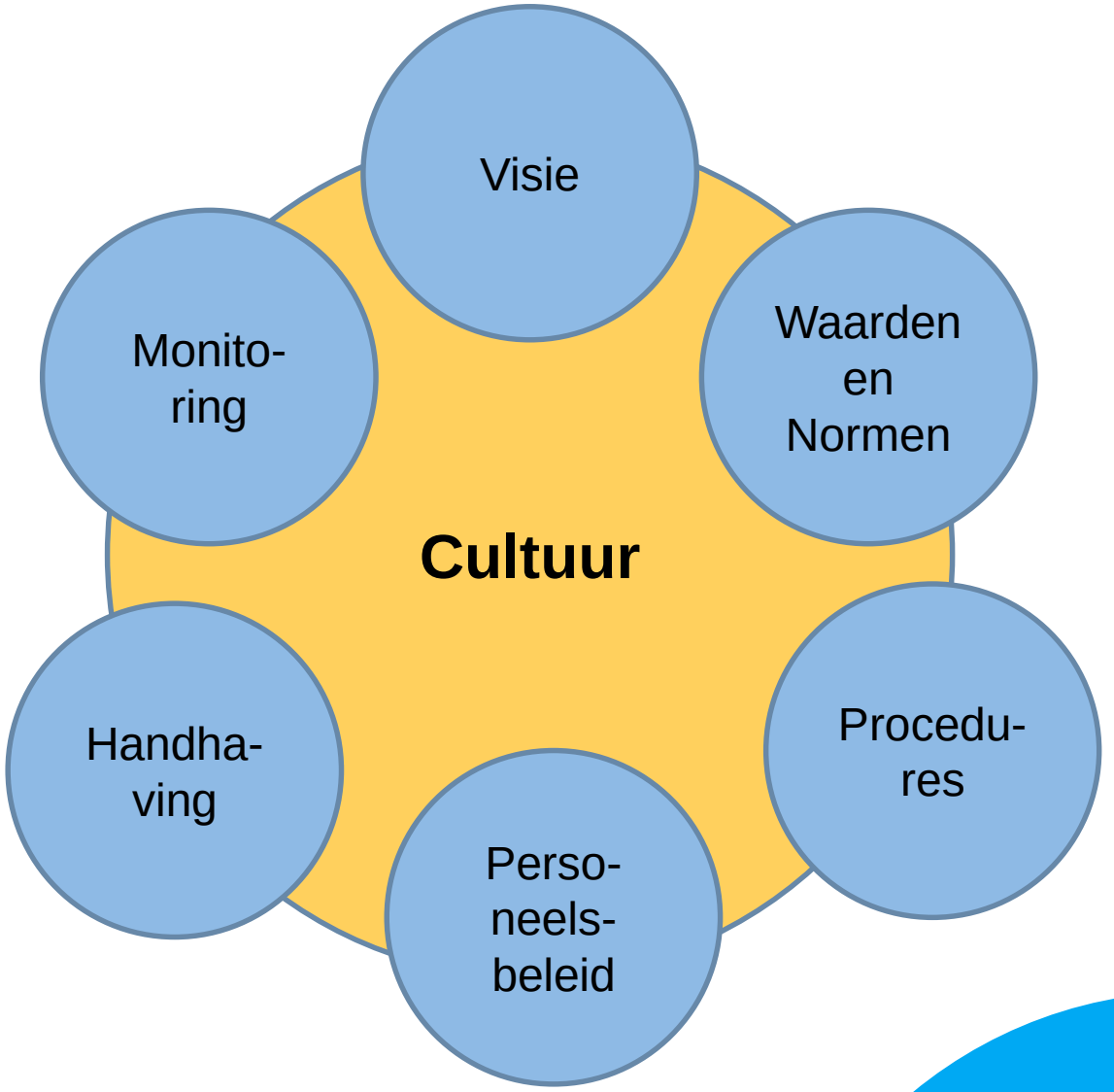
Beveiligingsbewustzijn





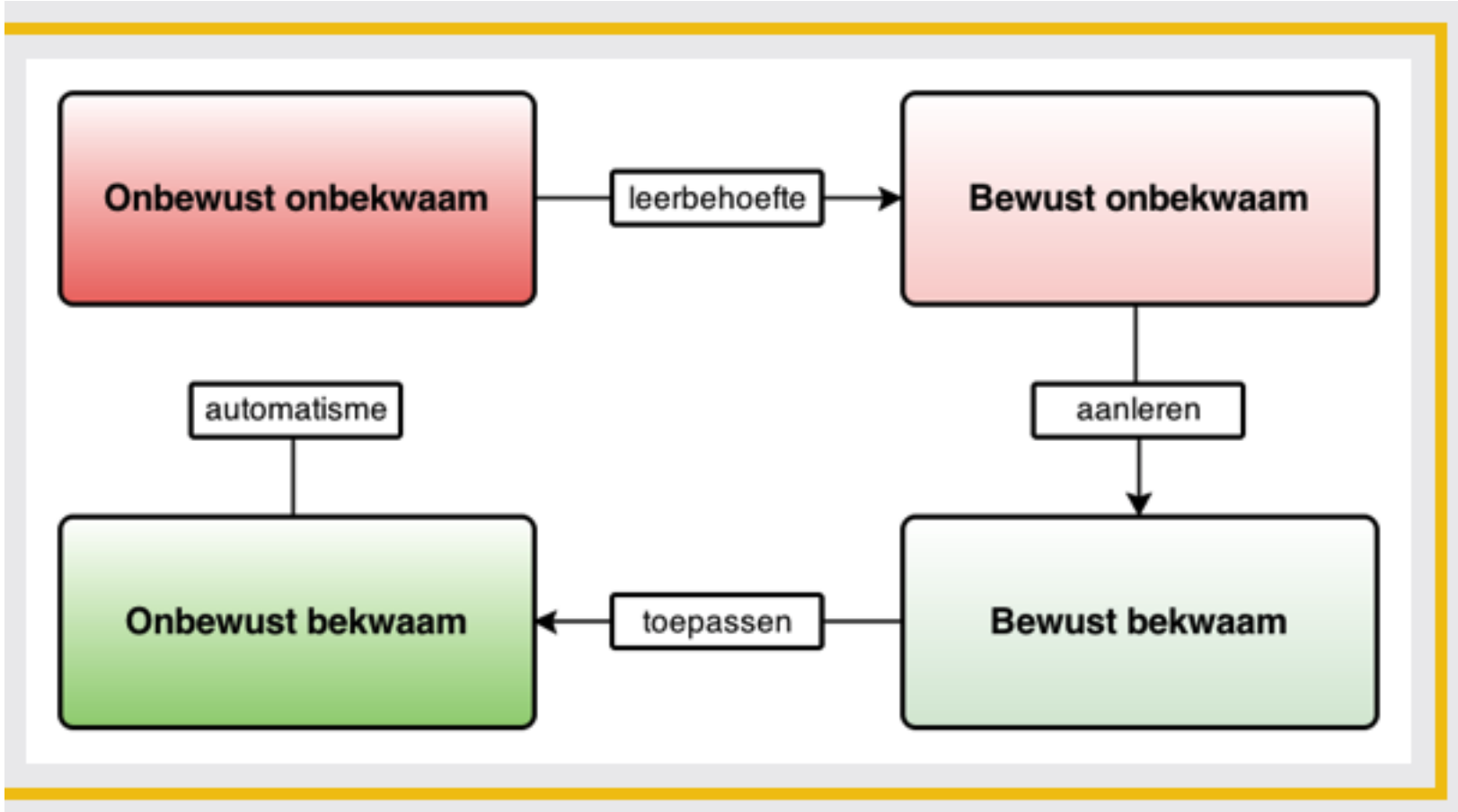
INFORMATIE BEVEILIGINGS DIENST

ORGANISATIECULTUUR



INFORMATIE BEVEILIGINGS DIENST

Fasen van bewustzijn



INFORMATIE BEVEILIGINGS DIENST

Meten is weten

Hoe bewust zijn medewerkers bij de start van het traject?

- Enquête
- Interviews
- Mystery Guest
- Phishing Mails

Hoe maak je veranderingen concreet?

- Herhalen
- Gebruik meetindicatoren

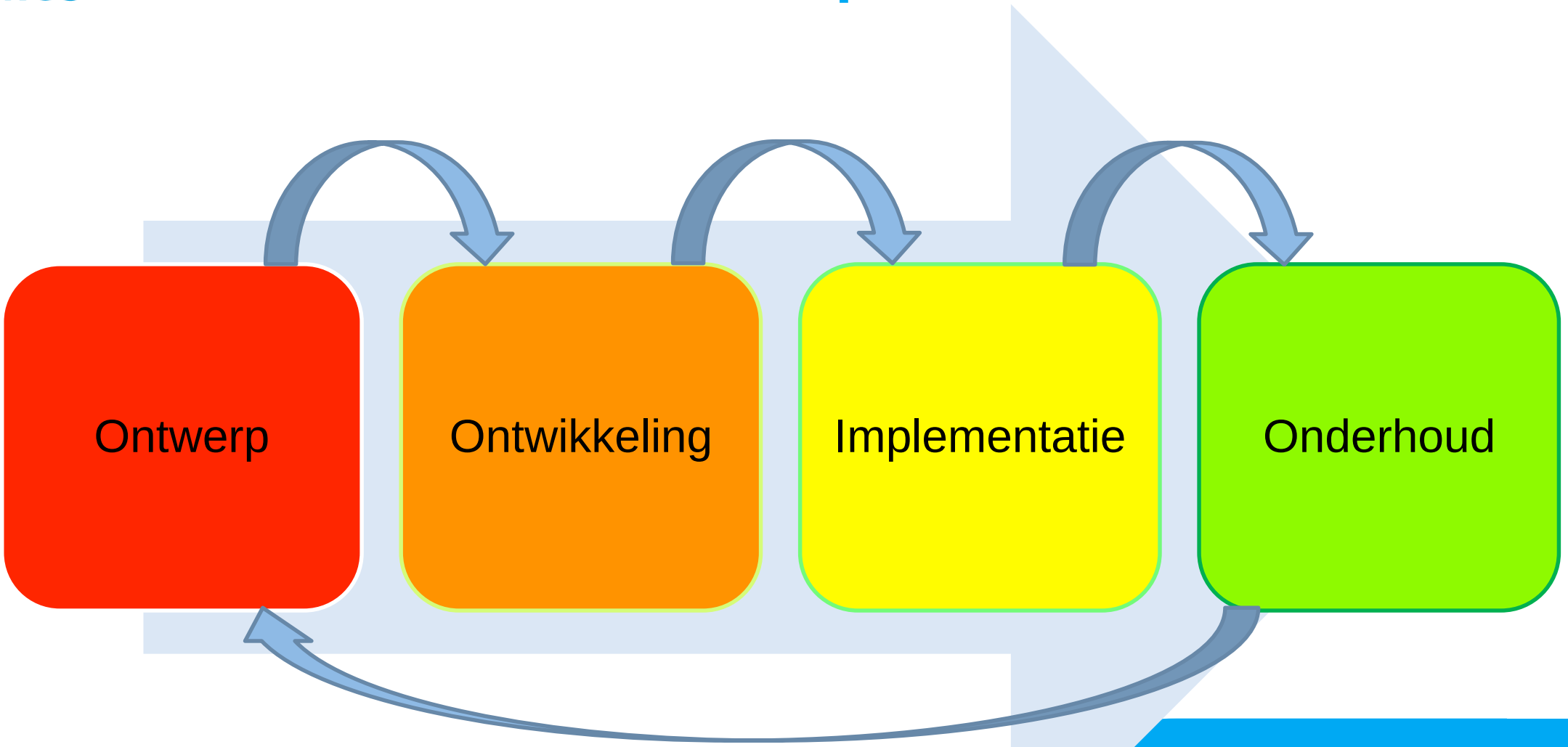
INFORMATIE BEVEILIGINGS DIENST

Meetindicatoren (voorbeelden)

- Aantal datalekken dat wordt gemeld
- Aantal beveiligingsincidenten in bepaalde periode
- Aantal keren dat geklikt wordt op (georganiseerde) phishing-link
- Aantal keren dat een phishing-mail als beveiligingsincident wordt gemeld
- Aantal incidenten met mobiele apparatuur
- Aantal verzoeken om wijziging van wachtwoorden
- Aantal medewerkers dat geen geheimhoudingsverklaring heeft ondertekend
- Aantal computers dat na verlaten van de werkplek niet vergrendeld is
- Aantal medewerkers dat aan het eind van de werkdag een ‘clear desk’ achterlaat

INFORMATIE BEVEILIGINGS DIENST

Gestructureerde aanpak



INFORMATIE BEVEILIGINGS DIENST

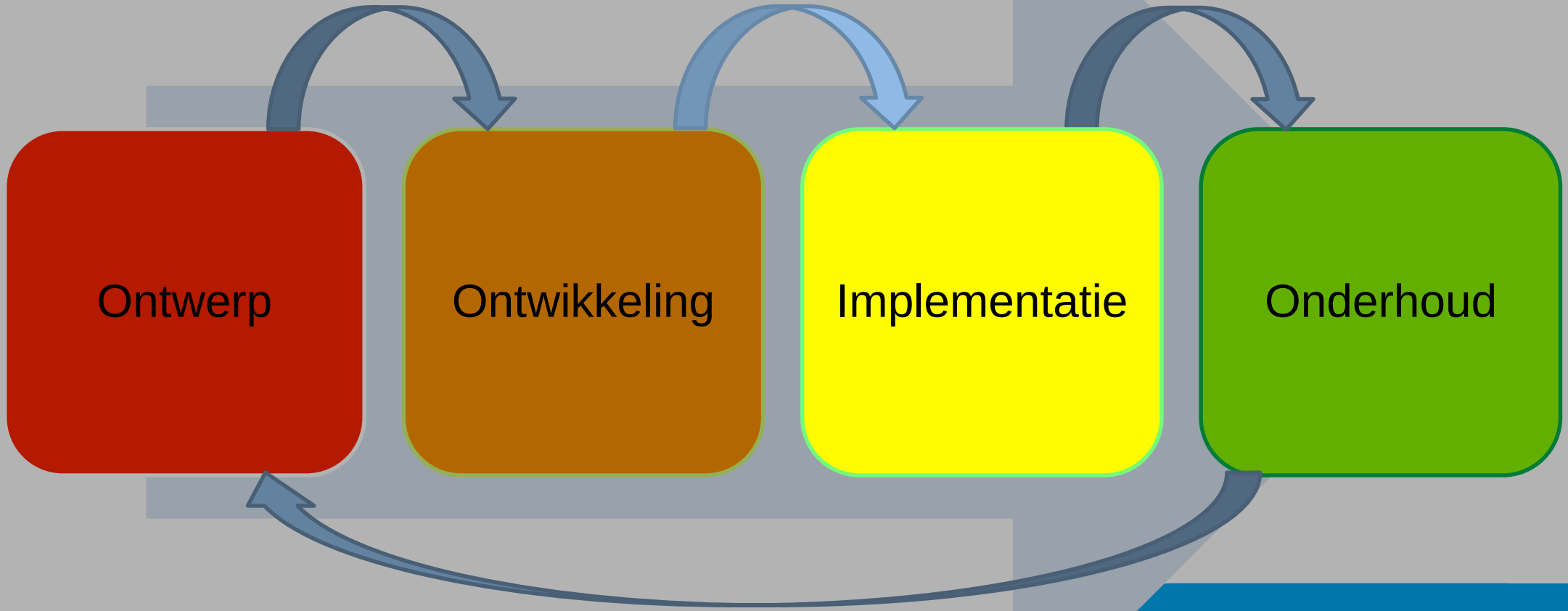
Gestructureerde aanpak

INFORMATIE BEVEILIGINGS DIENST

Gestructureerde aanpak

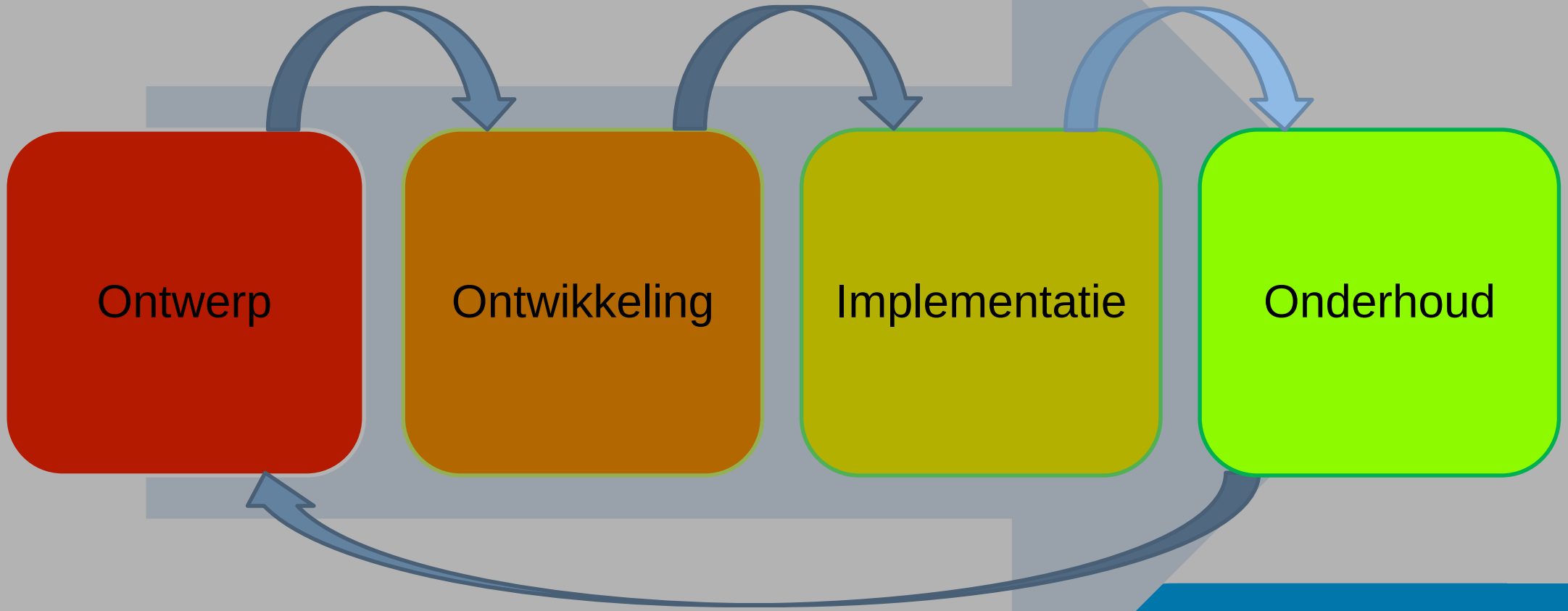
INFORMATIE BEVEILIGINGS DIENST

Gestructureerde aanpak



INFORMATIE BEVEILIGINGS DIENST

Gestructureerde aanpak

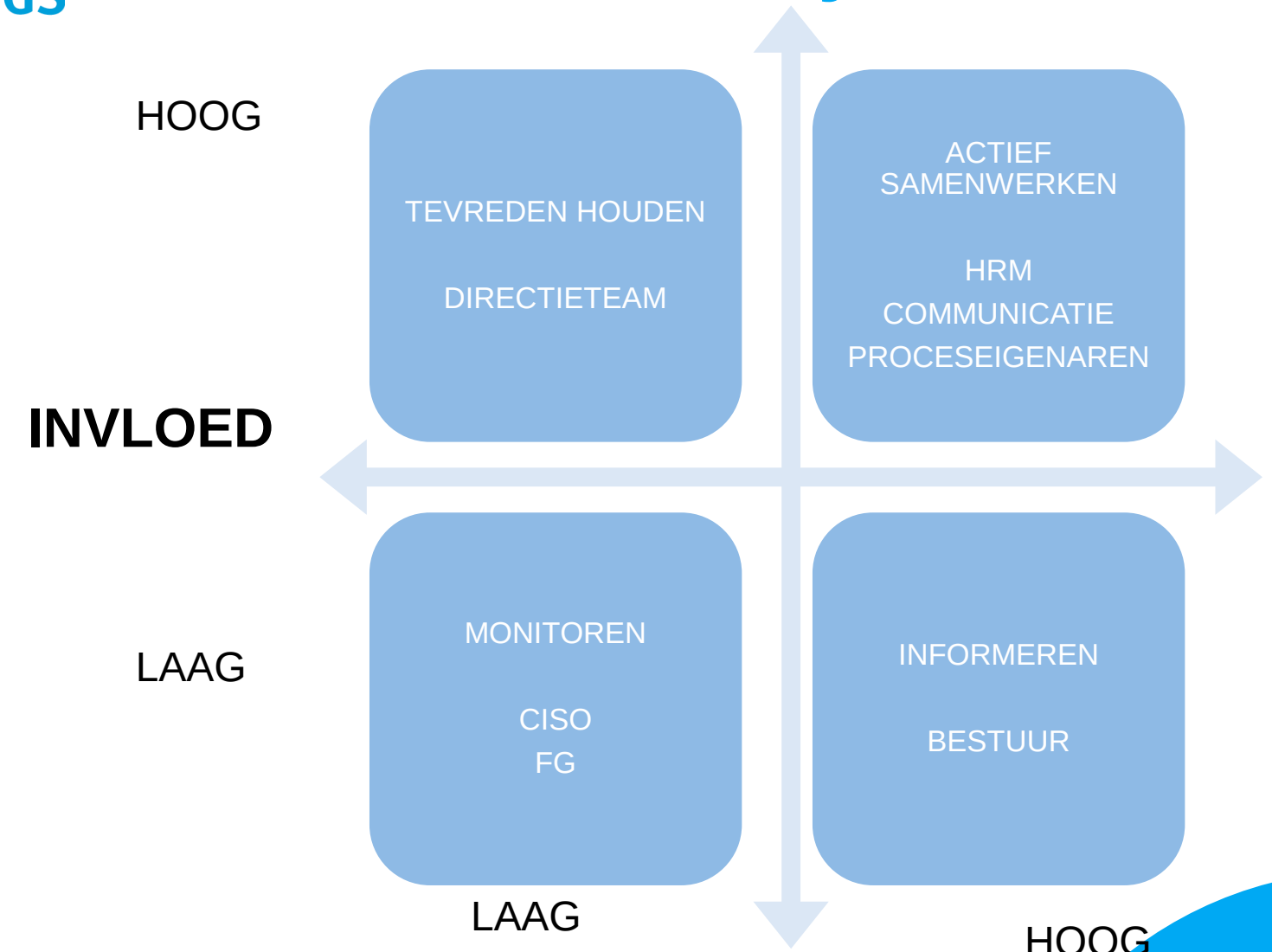


INFORMATIE BEVEILIGINGS DIENST

Gestructureerde aanpak

INFORMATIE BEVEILIGINGS DIENST

Stakeholderanalyse



INFORMATIE BEVEILIGINGS DIENST

Middelen

Online	Hybride	Offline
E-mail	Scenario's, Oefeningen	Trainingsessies
Video's	Verhalen met goed gedrag	Flyers FAQ's
Serious games	Beloningen, competities	Workshops
Webinars/ Zoom-sessies	Tip sheets	Lunchbijeenkomsten
Online trainingen/ e-learning	Nepaanvallen	Posters
Intranet, social media		

INFORMATIE BEVEILIGINGS DIENST

Voorbeeldcasus Handreiking

INFORMATIE BEVEILIGINGS DIENST

Gestructureerde aanpak bij uw gemeente

Organisatie bij de gemeente (deel 1)	Van toepassing?	Heeft aandacht nodig?	Actiehouder
• Er is een plan van aanpak.			
• Iemand binnen de organisatie is verantwoordelijk voor privacybewustzijn.			
• Er zijn voldoende middelen (geld, tijd, capaciteit) beschikbaar.			
• Er is zichtbare betrokkenheid van leidinggevenden.			
• HRM is direct betrokken bij privacybewustzijn.			
• Communicatie(adviseur) is direct betrokken bij privacybewustzijn.			
• Processen opgesteld voor bij indiensttreding.			
• Processen opgesteld voor bij uitdiensttreding.			

INFORMATIE BEVEILIGINGS DIENST

structurele aanpak bij uw gemeente

Organisatie bij de gemeente (deel 2)	Van toepassing?	Heeft aandacht nodig?	Actiehouder
• Bewustwordingscampagnes zijn structureel van karakter.			
• Alle medewerkers worden periodiek bewust gemaakt door; online trainingen, bijeenkomsten, video's of andere vormen van bewustwordingscampagnes.			
• Gebruik van een Leermanagementsysteem (LMS).			
• Met enige regelmaat wordt gecontroleerd op onveilig gedrag (phishing-test, mystery guest, security walks, aantal verzoeken tot wachtwoordwijziging, etc.)			
• Op het moment dat iemand onveilig gedrag vertoont, dan is de kans groot dat die persoon erop wordt aangesproken.			

INFORMATIE BEVEILIGINGS DIENST

10 tips om mee naar huis te nemen

1. Claim een plek op het intranet of in de nieuwsbrief en overleg hierin met communicatie adviseur + HR hoe de boodschap het beste overkomt.

2. Laat een mystery guest verkennen hoe ver die kan binnendringen en toegang verkrijgt tot informatie.

3. Maak gebruik van actuele beveiligingsincidenten uit het nieuws. Laat daarmee zien hoe dezelfde incidenten ook (kunnen) voorkomen bij de eigen organisatie, zodat het herkenbaar wordt en analyseer eigen beveiligingsincidenten die hebben plaatsgevonden.

4. Organiseer bijeenkomsten via Zoom over privacy vraagstukken (bijv. i.v.m. corona en thuiswerken). Dit kan meer instrumenteel zijn of meer over het *waarom* van privacy gaan.

5. Maak handig gebruik van bestaande bewustwordingscampagnes, een overzicht hiervan is te vinden op de website.

6. Dwing veiligheid organisatorisch af. Bijvoorbeeld met functiescheidingen, vier-ogenprincipe, etc.

7. Wijs ambassadeurs aan bij iedere afdeling en haak zelf aan bij werkoverleggen. Als je aanhaakt, vraag ook vanuit het team een casus aan te brengen, want *'de kennis ligt bij jullie',* en dan kun je samen kijken hoe het privacy technisch aan te vliegen.

8. Haak de kwaliteitsmedewerkers aan en organiseer een kennistraining voor hun, zodat ze meedenken over wat beter kan in processen.

9. Maak gebruik van e-learning/nano-learning om privacybewustzijn te bevorderen.

10. Speel de Privacy Pubquiz van de IBD en koppel dit aan een kennissessie over privacy en de AVG.

INFORMATIE
BEVEILIGINGS
DIENST

Tip uit het veld

Een reep voor elke melder van een beveiligingsincident

Gouden regels

Veilig thuiswerken – via VMware

COVID-19

Hilversum Mediastad

Wanneer je thuiswerkt vragen we je om het onderstaande te doen

- Maak gebruik van een **vertrouwd** en **beveiligd** (wifi)netwerk.
- Maak gebruik van **VMware** om op een veilige manier te werken.
- Houd rekening met een langere reactiesnelheid door gelimiteerde netwerkcapaciteit, je ziet dan bijvoorbeeld dat je muis trager werkt.
- Gebruik Webmail liever niet.
- Ga bewust om met informatie thuis en let erop wat je bespreekt in berichtenapps of tijdens een videoconference.

Extra alert zijn op cybercrime

- Houd rekening met het ontvangen van phishingmails en valse e-mails omtrent het Coronavirus. Het is bekend dat criminelen gebruik maken van de huidige ontwikkelingen door het versturen van phishingmails of het verspreiden van malware. Ga niet in op de phishingmail.
- Klik niet op links in e-mailberichten, open geen onbekende bijlagen en vul geen gegevens in bij e-mailberichten die u niet verwacht of van een onbekende afzender zijn.
- Download geen programma's die over het Corona virus gaan. Er is bijvoorbeeld een malafide app 'COVID19 Tracker' in omloop deze installeert de CovidLock ransomware op apparaten met het Android besturingssysteem. We kunnen verwachten dat er nog meer van dit soort cybercrime rond zal gaan, wees alert.

Ook als je thuiswerkt ga je integer om met informatie

- Je bent verplicht tot geheimhouding van alle vertrouwelijke informatie.
- Sla geen bedrijfsinformatie (langdurig) op op je privé apparatuur, nu je via VMware kunt werken vragen we je om de informatie naar de Hilversum omgeving te verplaatsten.
- De gegevens (data) die je voor je werk gebruikt hebben bescherming nodig; denk aan gebruik van sterke wachtwoorden en schermbeveiliging.
- Lock thuis ook je scherm als je even iets anders gaat doen.
- Met persoonsgegevens of vertrouwelijke onderwerpen ga je uiterst discreet om.

Ook als je thuiswerkt moet je erop letten dat je veilig met de gegevens van burgers, instellingen en bedrijven in Hilversum blijft omgaan

- Als je een malafide e-mail hebt ontvangen, meldt dit dan bij ons ICT team via [redacted]
- Als je twijfelt dan kun je van de privacy of security officer hulp krijgen bij een datalek of informatiebeveiligingsincident. Mail naar [redacted].
- Je meldt datalekken en informatiebeveiligingsincidenten zo snel mogelijk. Er is een meldingsformulier op intranet.

INFORMATIE BEVEILIGINGS DIENST

Nuttige links

- https://www.informatiebeveiligingsdienst.nl/product/handreiking-verhogen-bewustzijn-informatiebeveiliging/
- https://www.informatiebeveiligingsdienst.nl/overzicht-bewustwordingscampagnes/
- https://www.securityforum.org/research/from-promoting-awareness-to-embedding-behaviours/
- http://people.umass.edu/aizen/index.html
- https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

INFORMATIE BEVEILIGINGS DIENST

INFORMATIE
BEVEILIGINGS
DIENST

Nassaulaan 12
2514 JS Den Haag

CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)

privacy@vng.nl / incident@IBDGemeenten.nl

VNG
Realisatie