Betrek Raad en College bij NIS2

Nikki Nguyen (ADV)
Peter van Enk (ADV)
Jule Hintzbergen (IBD)

Agenda

- Welkom en introductie
- Verlanglijstje digitale veiligheid
- NIS2: Bestuurdersverantwoordelijkheid
- Team op Sterkte
- Betrek de Raad


VNG

Verlanglijstje CISO

Frans Hut

(CISO gemeente Haarlem en gemeente Zandvoort)

Een leeg hoofd

- Zodat er ruimte is voor de strategische rol, zonder dat allerlei verstoringen het hoofd continu verrommelen.

  - Iemand anders die met projecten meedoet, risicoanalyses doet, gebruikersvragen beantwoordt, … (ISO?)
  - Iemand anders die technische beveiliging doet (TISO?)
  - Iemand anders die ENSIA doet (ENSIA coördinator?)
  - Iemand anders als Eerste Hulp bij privacy (Privacy adviseur?)

Coördinatiekracht bij aansturen van derde partijen

- Je komt alleen effectief aan tafel als je in één keer zaken kunt doen voor veel gemeenten tegelijk.

Verlanglijstje CISO

Michiel Broekman
(CISO gemeente Oss)

Informatiebeveiliging in haarvaten van organisatie

- Zorg voor eigenaarschap in de lijn.
- Zorg voor voldoende capaciteit binnen bedrijfsprocessen om het werk te doen dat hoort bij eigenaarschap.

NIS2: Bestuurdersverantwoordelijkheid

Artikel 20

Governance

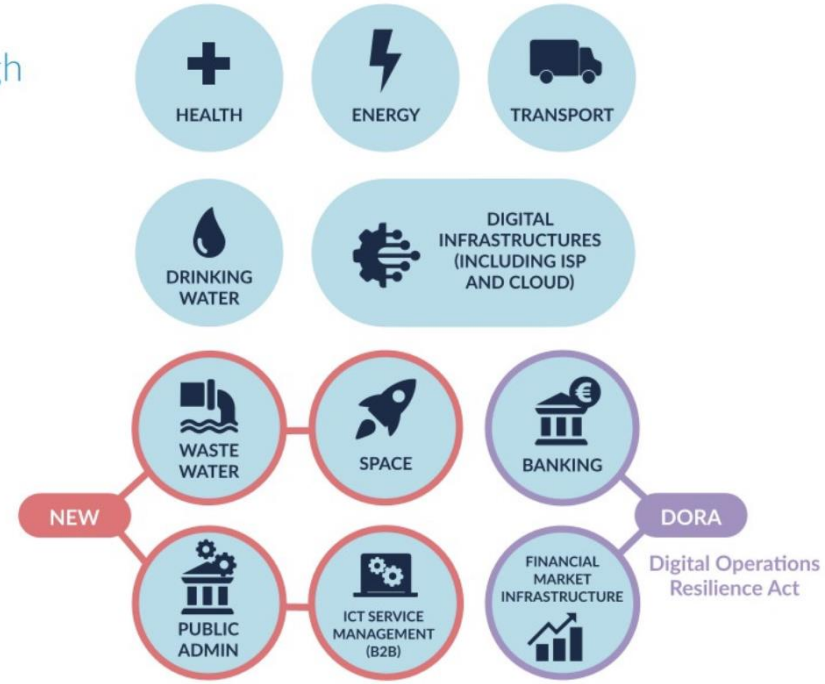
1. De lidstaten zorgen ervoor dat de bestuursorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren om te voldoen aan artikel 21, toezien op de uitvoering ervan en aansprakelijk kunnen worden gesteld voor inbreukendoor de entiteiten op dat artikel.

De toepassing van dit lid doet geen afbreuk aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.

2. De lidstaten zorgen ervoor dat de leden van de bestuursorganen van essentiële en belangrijke entiteiten een opleiding moeten volgen, en moedigen essentiële en belangrijke entiteiten aan om regelmatig een soortgelijke opleiding aan hun werknemers aan te bieden, zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.

Sectoren in scope

Annex 1 - Sectors of High Criticality



Annex 2 - Other Critical Sectors

Essentiële en belangrijke entiteiten

Voor welke sectoren geldt de NIS2-directive?

NIS1	
Energie	Transport
Bankwezen	Infrastructuur financiële markt
Gezondheidszorg	Drinkwater
Digitale infrastructuur	Digitale dienstverleners

NIS2	
Energie	Transport
Bankwezen	Infrastructuur financiële markt
Gezondheidszorg	Drinkwater
Digitale infrastructuur	Digitale aanbieders
Afvalwater	Overheidsdiensten
Ruimtevaart	Post- en koeriersdiensten
Afvalstoffen-beheerder	Levensmiddelen
Chemische stoffen	Wetenschap
Vervaardiging/ Manufacturing	

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

T.a.v. koepelvertegenwoordigers: Interprovinciaal Overleg (IPO), Vereniging Nederlandse Gemeenten (VNG) en Unie van Waterschappen (UvW)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag

Kenmerk
2023-0000564311

Datum 20 NOV 2023
Betreft NIS2 bij de overheid

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Kenmerk
2023-0000564311

Dit betekent dat de centrale overheid in de richtlijn als essentieel is aangemerkt. Dit is met inbegrip van zelfstandige Bestuursorganen (ZBO's) op wie de Kaderwet Zelfstandige Bestuursorganen van toepassing is. Tevens worden alle medeoverheden als essentiële entiteit aangewezen. Overheden zijn ook verantwoordelijk voor het aanbieden van meerdere essentiële diensten, zoals het wegbeheer of de afvalwater-voorziening, en vallen om die reden ook onder de reikwijdte van de NIS2. Tevens vallen gemeenschappelijke regelingen onder de werking van de richtlijn, voor zover zij voldoen aan de criteria die NIS2 hanteert om een overheidsentiteit te zijn.

C 324/6 NL Publicatieblad van de Europese Unie 14.9.2023

— Overheid
— Overheidsinstanties van centrale overheden
— Overheidsinstanties op lokaal niveau

NIS2: Bestuurdersverantwoordelijkheid

BIO 2.0 Baseline Informatiebeveiliging Overheid

Overwegende hetgeen volgt:

(1) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([4]) heeft tot doel capaciteiten op het gebied van cyberbeveiliging in de hele Unie op te bouwen, de bedreigingen voor netwerk- en informatiesystemen die worden gebruikt om essentiële diensten in belangrijke sectoren aan te bieden, te beperken en de continuïteit van dergelijke diensten te waarborgen wanneer zij worden geconfronteerd met incidenten, en aldus bij te dragen tot de veiligheid van de Unie en tot de doeltreffende werking van haar economie en samenleving.

Een aantal verschillen tussen NIS2 en de huidige BIO (opmaat):

- **Incidentregistratie** kent aanvullende eisen ten opzichte van de BIO. De NIS is, **naast interne organisatie**, **ook** sterk gericht op **externe notificatie**.
- **Bedrijfscontinuiteit, crisis(beheer) en de (toeleverings)keten** heeft **meer aandacht in de NIS 2** dan nu in de BIO staat. De NIS2 vereist een meer actieve rol van de organisatie.
- **2FA, beveiligde spraak-/tekst- en videoverbindingen** en beveiligde **noodcommunicatiesystemen** moeten worden **ingezet wanneer gepast**.
- **NIS maakt geen onderscheid in type systemen** en is daarmee allesomvattend, **inclusief OT/procesautomatisering**. Uit de evaluatie van de BIO blijkt dat respondenten OT/procesautomatisering onvoldoende terug vinden komen in de BIO.

Artikel 21

Maatregelen voor het beheer van cyberbeveiligingsrisico's

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in de eerste alinea bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

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;

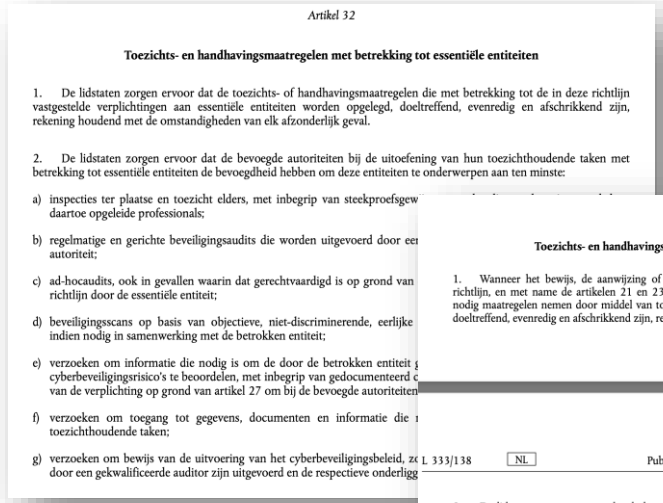
h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

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.

Toezicht vooraf en achteraf

ESSENTIAL ENTITIES	IMPORTANT ENTITIES
✓ Ex Ante & Ex Post Supervision	✓ Ex Post Supervision
✓ On-site inspections and off-site supervision	✓ On-site inspections and off-site ex post supervision
✓ Regular & Targeted Security Audits	✓ Targeted Security Audits
✓ Security Scans	✓ Security Scans
✓ Information Requests	✓ Information Requests
✓ Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned.	✓ Requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned.
✓ Ad hoc audits, for example after a significant incident	✗



Artikel 32

Toezichts- en handhavingsmaatregelen met betrekking tot essentiële entiteiten

1. De lidstaten zorgen ervoor dat de toezichts- of handhavingsmaatregelen die met betrekking tot de in deze richtlijn vastgestelde verplichtingen aan essentiële entiteiten worden opgelegd, doeltreffend, evenredig en afschrikkend zijn, rekening houdend met de omstandigheden van elk afzonderlijk geval.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot essentiële entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:

a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgew… daartoe opgeleide professionals;

b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door ee… autoriteit;

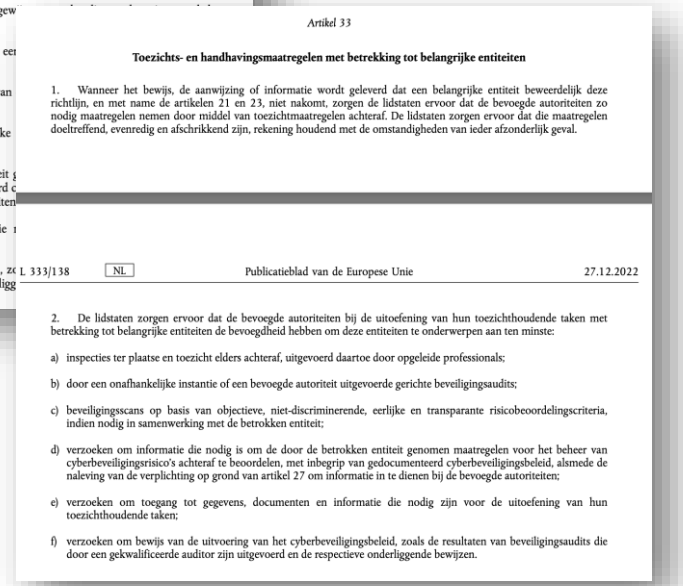
c) ad-hocaudits, ook in gevallen waarin dat gerechtvaardigd is op grond van … richtlijn door de essentiële entiteit;

d) beveiligingsscans op basis van objectieve, niet-discriminerende, eerlijke … indien nodig in samenwerking met de betrokken entiteit;

e) verzoeken om informatie die nodig is om de door de betrokken entiteit … cyberbeveiligingsrisico's te beoordelen, met inbegrip van gedocumenteerd … van de verplichting op grond van artikel 27 om bij de bevoegde autoriteiten…

f) verzoeken om toegang tot gegevens, documenten en informatie die … toezichthoudende taken;

g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zo… door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderligg…



Artikel 33

Toezichts- en handhavingsmaatregelen met betrekking tot belangrijke entiteiten

1. Wanneer het bewijs, de aanwijzing of informatie wordt geleverd dat een belangrijke entiteit beweerdelijk deze richtlijn, en met name de artikelen 21 en 23, niet nakomt, zorgen de lidstaten ervoor dat de bevoegde autoriteiten zo nodig maatregelen nemen door middel van toezichtmaatregelen achteraf. De lidstaten zorgen ervoor dat die maatregelen doeltreffend, evenredig en afschrikkend zijn, rekening houdend met de omstandigheden van ieder afzonderlijk geval.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot belangrijke entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:

a) inspecties ter plaatse en toezicht elders achteraf, uitgevoerd daartoe door opgeleide professionals;

b) door een onafhankelijke instantie of een bevoegde autoriteit uitgevoerde gerichte beveiligingsaudits;

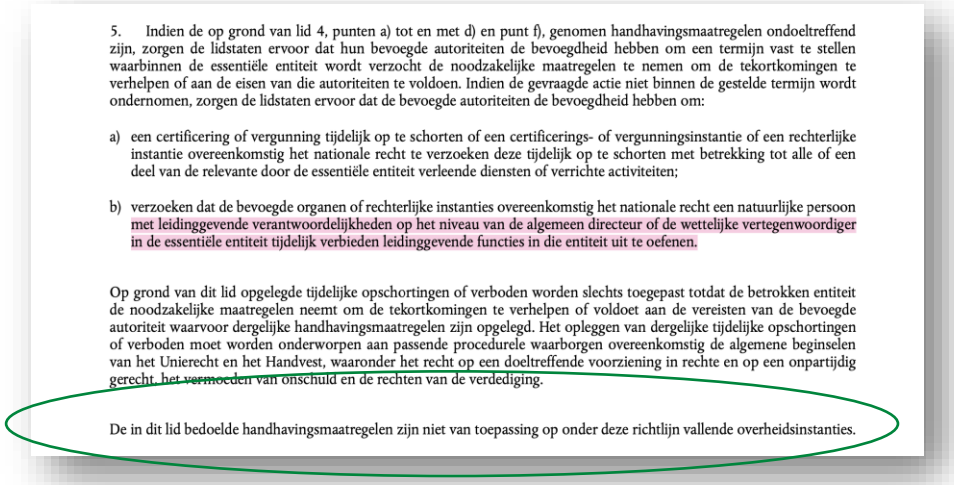
c) beveiligingsscans op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;

d) verzoeken om informatie die nodig is om de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's achteraf te beoordelen, met inbegrip van gedocumenteerd cyberbeveiligingsbeleid, alsmede de naleving van de verplichting op grond van artikel 27 om informatie in te dienen bij de bevoegde autoriteiten;

e) verzoeken om toegang tot gegevens, documenten en informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken;

f) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

Nieuw in de NIS2 is de bestuursverantwoordelijkheid. Niet IT-managers, maar bestuurders zelf spelen een cruciale rol in het toezicht op cyberveiligheid. Doen ze dat niet, dan lopen ze het risico op hoge boetes (tot 10 miljoen euro en 2% van de omzet).



5. Indien de op grond van lid 4, punten a) tot en met d) en punt f), genomen handhavingsmaatregelen ondoeltreffend zijn, zorgen de lidstaten ervoor dat hun bevoegde autoriteiten de bevoegdheid hebben om een termijn vast te stellen waarbinnen de essentiële entiteit wordt verzocht de noodzakelijke maatregelen te nemen om de tekortkomingen te verhelpen of aan de eisen van die autoriteiten te voldoen. Indien de gevraagde actie niet binnen de gestelde termijn wordt ondernomen, zorgen de lidstaten ervoor dat de bevoegde autoriteiten de bevoegdheid hebben om:

a) een certificering of vergunning tijdelijk op te schorten of een certificerings- of vergunningsinstantie of een rechterlijke instantie overeenkomstig het nationale recht te verzoeken deze tijdelijk op te schorten met betrekking tot alle of een deel van de relevante door de essentiële entiteit verleende diensten of verrichte activiteiten;

b) verzoeken dat de bevoegde organen of rechterlijke instanties overeenkomstig het nationale recht een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de essentiële entiteit tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen.

Op grond van dit lid opgelegde tijdelijke opschortingen of verboden worden slechts toegepast totdat de betrokken entiteit de noodzakelijke maatregelen neemt om de tekortkomingen te verhelpen of voldoet aan de vereisten van de bevoegde autoriteit waarvoor dergelijke handhavingsmaatregelen zijn opgelegd. Het opleggen van dergelijke tijdelijke opschortingen of verboden moet worden onderworpen aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het Unierecht en het Handvest, waaronder het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, het vermoeden van onschuld en de rechten van de verdediging.

De in dit lid bedoelde handhavingsmaatregelen zijn niet van toepassing op onder deze richtlijn vallende overheidsinstanties.

- Artikel 32 essentiële entiteiten: toezicht voor- en achteraf
- Artikel 33 belangrijke entiteiten: toezicht achteraf

Titel II. De inrichting en samenstelling van het gemeentebestuur

Hoofdstuk I. Algemene bepaling

Artikel 6

In elke gemeente is een raad, een college en een burgemeester.

- **Approve the adequacy** of the cybersecurity risk management measures taken by the entity;
- **Supervise the implementation** of the risk management measures;
- **Follow training** in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity
- **Offer similar training to their employees** on a regular basis;
- **Be accountable** for the non-compliance

Handelingsperspectief

- B&W: belang uitdragen bestuurlijke en ambtelijke organisatie, en toezien op naleving NIS2, team op sterkte, goed laten adviseren
- Raad: inhoudelijke en financiële kaders, controleren college van B&W


NTR

B&W

Samenvattend NIS2

- Strengere beveiligingseisen
- Verplichte rapportage van beveiligingsincidenten
- Passende maatregelen nemen
- Verzwaring van toezicht en handhaving
- Verplichte informatiedeling
- Training en bewustzijn van medewerkers
- Bestuurlijke aansprakelijkheid voor B&W en de Raad

Handelingsperspectief

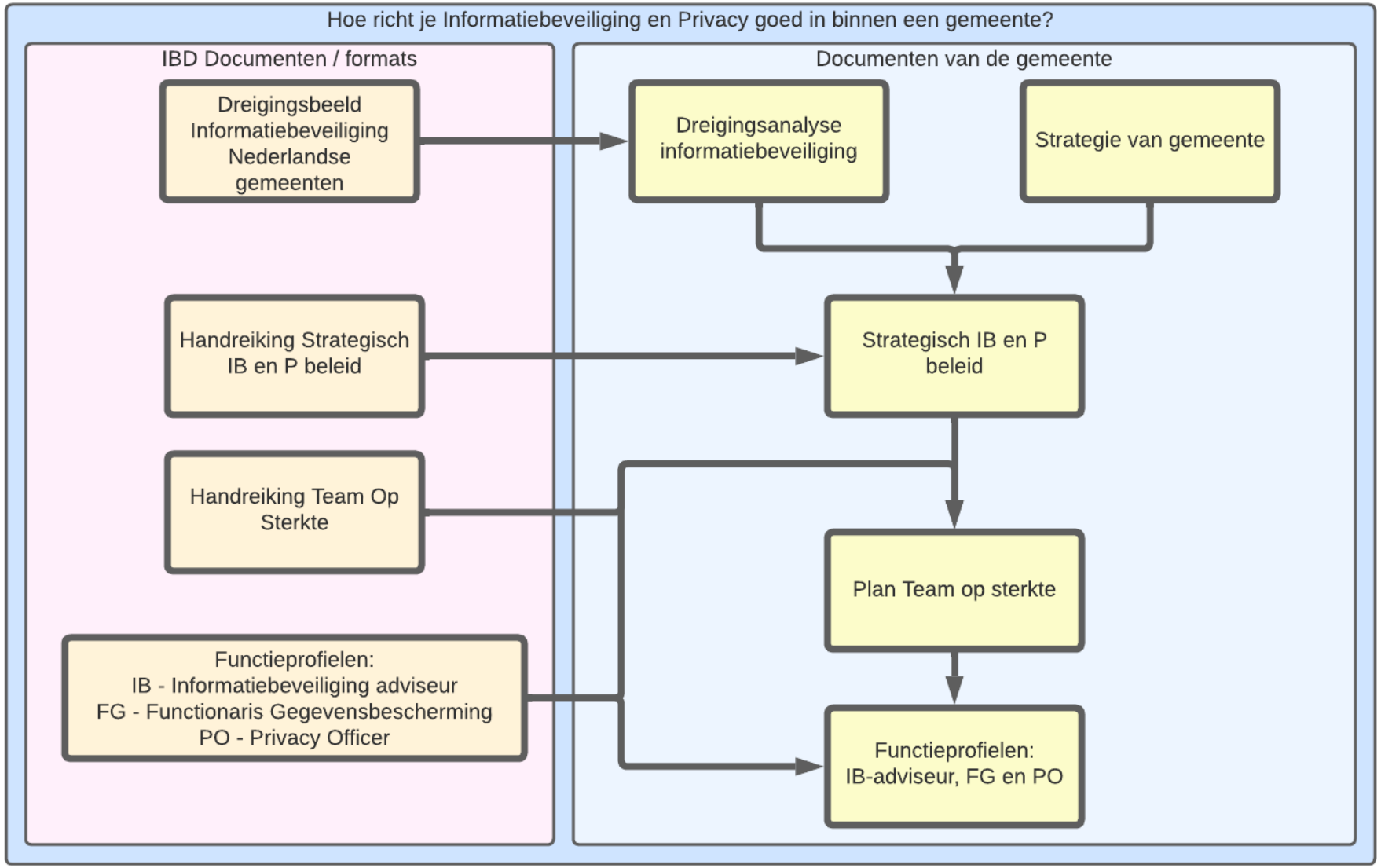
- Positioneer de CISO
- Zorg voor een sterk team die jou als bestuurder ondersteund
- Zet IB op de agenda bij alle besprekingen
- Budget?

Tenslotte

- De IBD heeft hier ondersteuning voor

Hoe krijgen wij ons IB en P team op sterkte?

Ondersteuning IBD



Betrek de Raad

- Peter van Enk - projectleider bestuurlijke gesprekken Digitale Veiligheid bij de VNG
- Ongeveer 60 Bestuurlijke gesprekken gedaan
- In 50% is de raad niet aangehaakt op het thema Digitale veiligheid
- Ik wil ‘good practices’ bespreken waarin dit *wel* is gelukt

De Raad en digitale veiligheid

- Waarom de raad betrekken?
  - De Raad stelt inhoudelijke en financiële kaders (ook voor Digitale Veiligheid)
  - De raad controleert het College
  - Bedreigingen en complexiteit nemen toe
  - Gemeentelijke dienstverlening steeds afhankelijker van digitalisering
  - Kosten digitalisering gestegen
  - NIS2 komt eraan

Good practice gemeente Westerkwartier

Gemeente Westerkwartier

Aanbevelingen rekenkameronderzoek Digitale Veiligheid:

Wees alert op mogelijke vertragingen in de implementatie van het beleid informatieveiligheid en informeer actief naar de voortgang en de mogelijke knelpunten daarin

Laat je eens per jaar actief en specifiek informeren over het informatieveiligheidsbeleid

Vraag bij het college actief naar de aandacht voor informatieveiligheid bij het inrichten van werkprocessen, naast de inhoudelijke kwaliteit en control

Vraag het college te streven naar BIO-niveau 3 en faciliteer in wat daarvoor nodig is in termen van formatie en techniek

Vraag het college zich actief in te zetten op het voorwaardelijk maken van een training privacy en informatieveiligheid voor toegang tot het systeem

Good practice gemeente Nieuwegein

Nieuwegein

In de gemeente Nieuwegein heeft de raad het Manifest Digitaal Nieuwegein vastgesteld. Het is een handzaam document waarin de belangrijkste inhoudelijke kaders in de vorm van publieke waarden voor de ontwikkeling van de digitale samenleving zijn vastgelegd. Naast waarden als ‘inclusief’ en ‘privacy’ is ook ‘veiligheid’ opgenomen in het manifest. Deze waarde is als volgt omschreven:

- ‘Informatie is waardevol, daar gaan we zorgvuldig mee om. We beveiligen onze systemen en data tegen verlies, diefstal en misbruik. We maken van onze stad een veilige digitale plek om in te werken en te leven.’

Het manifest heeft ervoor gezorgd dat de raad betrokken is op het thema en het belang van digitale veiligheid onderkent.

Good practice gemeente oude ijsselstreek

De gemeenteraad is actief meegenomen in het nieuwe IVP, waar digitale veiligheid onderdeel van uitmaakt. In de aanloop naar dit IVP is een bewustwordingsprogramma uitgevoerd met drie onderdelen:

- Een escaperoom waarbij de raadsleden in teams aan de slag zijn gegaan met de thema's privacy, informatiebeveiliging, AVG en datalekken.
- Een bijeenkomst over het thema 'eigen huis op orde'.
- Een inhoudelijke bijeenkomst voor de raad had als thema digitale weerbaarheid voor burgers en bedrijven.

Als resultaat onderkennen raadsleden nu het belang van het thema digitale veiligheid. Ook zijn zij intrinsiek geïnteresseerd in dit onderwerp.

De raad is beter in staat om de rol op het gebied van digitale veiligheid in te vullen

Advies van de VNG

- Pleio Themagroep NIS2
  - https://digitaleveiligheid.pleio.nl/groups/view/b3c589f0-a7e9-48f3-a65f-cb73254540a4/nis-2-richtlijn
- NIS2 Nieuws
  - https://vng.nl/nieuws/nieuwe-stappen-nis2-vragen-blijven
- Checklist digitale veiligheid voor raadsleden
  - https://vng.nl/sites/default/files/2023-04/checklist-raadsleden-digitale-veiligheid.pdf
- Agenda Digitale Veiligheid 2020 – 2024 – Een veilige (digitale) gemeente
  - https://vng.nl/sites/default/files/2020-02/vng_agenda_digitale_veiligheid_2020-2024_def.pdf
- Ook een bestuurlijk gesprek of aanvullende vragen? Mail naar teamadv@vng.nl