Digitalisering in de gemeentelijke uitvoeringspraktijk

1 september 2026

Regiobijeenkomst Eindhoven

Sessie Weerbaarheid

Agenda

- Definitie weerbaarheid
- Geopolitieke ontwikkelingen
- Lokale realiteit
- Digitale weerbaarheid gemeenten
- Samenhang digitale weerbaarheid gemeenten
- Agenda Digitale Veiligheid
- NDS

Definitie weerbaarheid

- Weerbaarheid betekent voorbereid zijn op verstoring, kunnen reageren en herstellen

Geopolitieke ontwikkelingen



26 aug 2026 om 8.37 u

Rusland meldt nieuwe aanval op magazijn Wildberries

Een magazijn van de Russische webwinkel Wildberries in de Russische regio Tambov staat in brand na een droneaanval, zegt de lokale gouverneur via Telegram. Eén persoon zou gewond zijn geraakt.

WORLD NEWS

Pro-Russian hackers claim responsibility for major cyberattack on Norway's public digital services

LUSA 08/08/2026

Lusa - Business News - Portugal: Cyberattack on water utility had no effect on supply - minister

Mafra, Portugal, Aug. 7, 2026 (Lusa) - The minister for the environment clarified on Friday in Ericeira that the cyberattack on several businesses belonging to the Águas de Portugal group a week ago did not affect the country's water supply.

Internationaal • 10:56

Rusland dreigt Oekraïne opnieuw de vrieskou in te bombarderen, maar moet deze winter ook zelf vrezen

Van onze redacteur

De Russen bereiden massale aanvallen voor op de Oekraïense energievoorziening. Dat meldt het Russische ministerie van Defensie. Ze willen daarmee de Oekraïense aanvallen vergelden. Volgens correspondent Joost Bosman is er wat dat betreft weinig nieuws onder de zon. 'Ze zijn van plan om door te gaan met waar ze al jaren mee bezig zijn, namelijk Oekraïne te bombarderen.' Wat wel mogelijk anders wordt deze winter, is dat mogelijk de Russen zelf nu ook in de kou komen te staan.

mericas Asia Australia **Middle East** Africa Inequality Global development

Iran-linked hackers blamed for cyber-attack that shut down UK power plant

Incident marks apparent escalation by Tehran in its in retaliation against UK over allowing US to use British bases

Zo om 10.46 u

Rusland dreigt met enorme aanvallen op energiesector Oekraïne

Rusland maakt zich op om massale aanvallen uit te voeren op de Oekraïense energievoorziening, meldt het Russische ministerie van Defensie. "Russische strijdkrachten zijn begonnen met voorbereidingen voor grootschalige aanvallen op faciliteiten in de Oekraïense energiesector, als reactie op de aanhoudende aanvallen van het regime in Kyiv op de civiele infrastructuur en het Russische olie- en energiecomplex", staat in een verklaring.

VNG Lokale realiteit

Hackers stelen gegevens inwoners Twentse gemeenten

Een bedrijf dat diensten verleent voor de afdeling Burgerzaken van Dinkellan
Tubbergen is gehackt.

ANP

Hack bij gemeente Hof van Twente veroorzaakt door te simpel wachtwoord

Cybercrime bij werkbedrijf Senzer: ‘Nog onduidelijk of er bij deze inbraak persoonsgegevens zijn gestolen’

Gemeente Buren

Home | Nieuws | Datadiefstal gemeente Buren

Datadiefstal gemeente Buren

8 JULI 2022, 08:00

Digitale autonomie als bestuurlijke opdracht in een wereld van afhankelijkheden

Jurisdictie klinkt als een juridisch detail, tot het een operationele realiteit wordt. In een digitale keten waarin data, beheer en support over landsgrenzen lopen, kan een wijziging in wetgeving, eigenaarschap of leveranciersvoorwaarden direct invloed hebben op wie toegang kán krijgen en of dienstverlening beschikbaar blijft.

CYBER SECURITY RAAD VREEST TEKORT AAN CYBERSECURI

De vraag naar cybersecurity specialisten groeit enorm h
constateert de Nederlandse Cyber Security Raad dat er
dreigt. Veel kansen dus voor cybersecurity specialisten
groeien.

NOS Nieuws • Dinsdag 9 mei 2023, 13:38

Hoe een Haagse gemeenteambtenaar topcriminelen van een nieuw paspoort voorzag

Hack gemeente Epe niet opgeëist, maar kosten lopen al in de tonnen

Erik van Dam 5 juni, 17:31 • Aangepast 5 juni, 22:13 • 3 minuten leestijd

Tienduizenden verkeerslichten in Nederland te hacken, lek nog jaren te misbruiken

Daniël Verlaan · 5 oktober 2024 · Aangepast: 25 oktober 2024

Tienduizenden verkeerslichten in Nederland zijn te hacken en op afstand te besturen. Kwaadwillenden zouden het lek kunnen misbruiken om chaos te veroorzaken of hulpdienste

Gemeenten en provincies staan voor een digitaal kantelpunt

Breng rust, overzicht en vertrouwen terug in je organisatie.

AFAS Software 21 mei 2026

digitaal/nieuws

Groot IT-onderzoek: overheden zetten in op minder Amerikaanse cloud

Ook AI speelt een groeiende rol in de manier waarop overheden hun IT-partners beoordelen.

Digitale Weerbaarheid | Nieuws

Gemeente Epe gaat 1000 ID-bewijzen gratis vervangen

Van nagenoeg alle inwoners van de gemeente Epe zijn bij de datadiefstal van 12 maart jl. bij de gemeente gegevens gestolen.

Fysieke en digitale veiligheid: een wereld van
schil

Gerelateerde onder
Informatiesamenleving, Digitale veiligheid en privacy

ackers

veiligheid. Dit vergroot de awarene
vordt makkelijker gevoerd.

Proef noodsteunpunten van start gegaan in bijna 70 gemeenten

25 feb 2026, 07:38

In bijna 70 gemeenten in alle 25 veiligheidsregio's is een proef met noodsteunpunten begonnen. Dat maakte de VNG (Vereniging van Nederlandse

Datalek krijgt pijnlijk staartje voor Odido: klantgegevens mogelijk te lang bewaard

Door onze nieuwsredactie

26 mrt 2026 om 14:40

502 reacties Delen

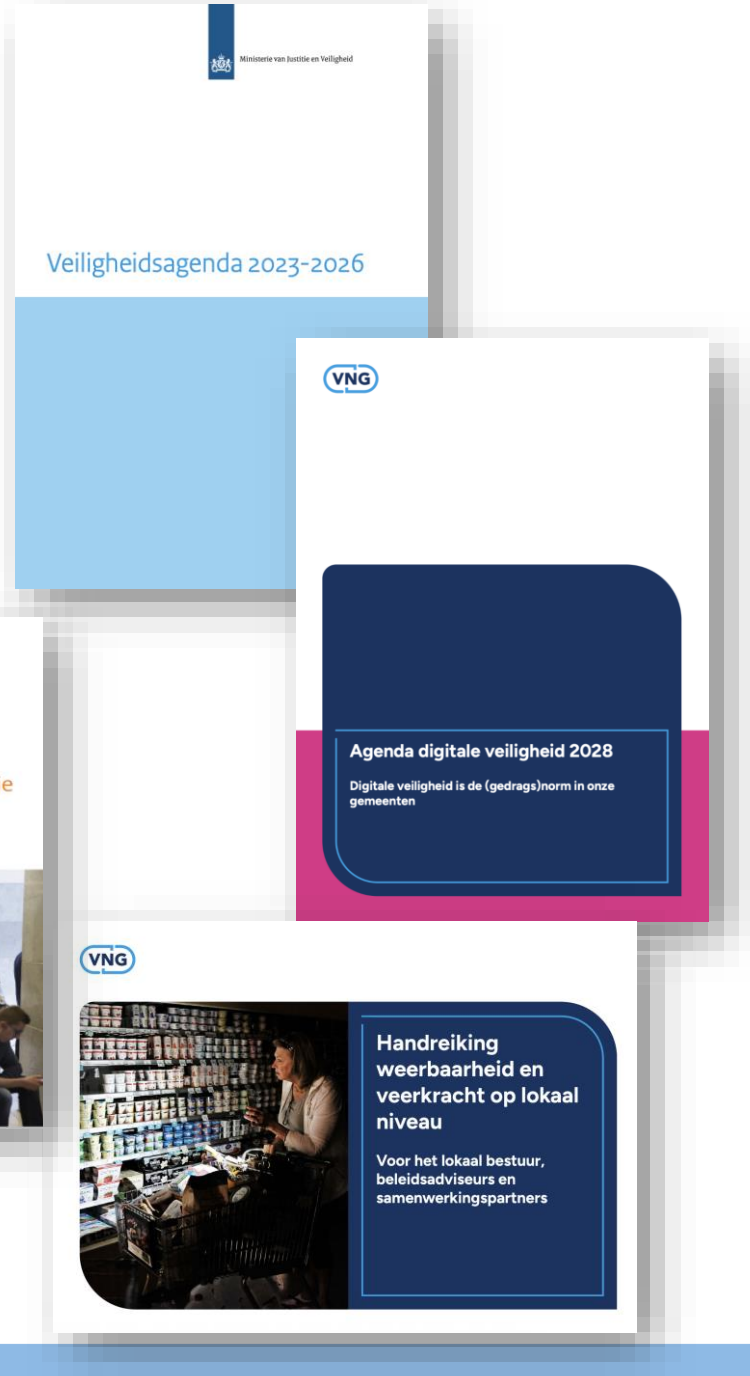
De Autoriteit Persoonsgegevens onderzoekt of provider Odido gegevens

Digitale Weerbaarheid gemeenten

Bestuurlijk Convenant Digitale Veiligheid Gemeenten







- Ontwikkelingen
  - Collectivisering digitalisering gemeenten
  - Nederlandse DigitaliseringsStrategie (NDS)
- Randvoorwaarden
- Successen

Digitale veiligheid voor gemeenten

- Ontwikkelingen
  - Collectivisering digitalisering gemeenten
  - Nederlandse DigitaliseringsStrategie (NDS)
- Randvoorwaarden
- Successen



Kernthema's 2026

Eigen huis op orde (informatiebeveiliging)
| regels, processen, beheerssystemen, zorgplicht

Voorbereid op digitale ontwrichting
| incidenten- en crisisrespons, online aangejaagde ordeverstoring, desinformatie, rechtstaat, bevoegdheden

Weerbare inwoners en ondernemers
| Digitale weerbaarheid, verschuiving traditionele criminaliteit naar cybercrime

Arbeidsmarktkrapte
| Continuïteit en kwaliteit van digitale veiligheid

Professionalisering en leiderschap
| Leiderschap, arbeidscapaciteit, bewustwording

Wet- en regelgeving
| Europees en nationaal

Randvoorwaarden

Veiligheidsstelsel
| koppeling fysieke en digitale veiligheid

Sterke informatiepositie

Structurele financiering

VNG-diensten (GGU)

IBD
| informatiebeveiligingsdienst, sectorale CSIRT

ENSIA
| verantwoording informatieveiligheid, datakwaliteit

GGI-Veilig/BIZOB
| inkoopmantel advies, diensten, producten

Digitale veiligheid voor gemeenten

Kernthema's 2026

Eigen huis op orde (informatiebeveiliging)
| regels, processen, beheerssystemen, zorgplicht

Voorbereid op digitale ontwrichting
| incidenten- en crisisrespons, online aangejaagde ordeverstoring, desinformatie, rechtstaat, bevoegdheden

Weerbare inwoners en ondernemers
| Digitale weerbaarheid, verschuiving traditionele criminaliteit naar cybercrime

Arbeidsmarktkrapte
| Continuïteit en kwaliteit van digitale veiligheid

Professionalisering en leiderschap
| Leiderschap, arbeidscapaciteit, bewustwording

Wet- en regelgeving
| Europees en nationaal

Belangrijke links

https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/
| Ondersteuningspakket BIO2, Regeling positie CISO en meer.

https://vng.nl/sites/default/files/2024-08/handreiking-voorbereiding-op-digitale-ontwrichting.pdf
| Maar ook Wwke, doorontwikkeling LCD, nieuwe cyberoefendriehoek

https://vng.nl/sites/default/files/2025-08/handreiking_weerbaarheid_en_veerkracht_op_lokaal_niveau_definitief158.pdf

https://vng.nl/projecten/arbeidsmarktkrapte-aanpak-gemeenten
| Structurele samenwerkingen rijk en mede-overheden, communicatiecampagne

https://vng.nl/trainingen/serious-game-raadsleden-grip-op-cyberbeveiliging

https://vng.nl/artikelen/cyberbeveiligingswet-nis2-nieuws-en-updates
| Input en lobby met departementen, informeren gemeenten en leveranciers

Informatiebeveiliging | IBD

Situatie

- Gemeenten werken met de IBD samen aan informatiebeveiliging
- Doel: vanaf 2030 geen vermijdbare digitale incidenten
- Rol IBD: sectorale CERT/CSIRT voor gemeenten, schakelpunt met het Nationaal Cyber Security Centrum (NCSC)
- IBD monitort dreigingen met Enterprise Attack Surface Management (EASM)-tool (NIS2-eis)
- Ondersteuningspakket Verhogen Digitale Weerbaarheid: dienstverlening, tooling en kennis voor gemeenten

Onze acties

- De rol en dienstverlening van IBD als CSIRT helder
- Diensten: EASM, kwetsbaarhedenmanagement, incidentondersteuning, crisiscoördinatie, woordvoering
- Dreigingsbeelden gemeenten
- Ondersteuningspakket BIO2: voldoen aan vereisten
- Regeling positie CISO
- Collectief leverancierscontrolemechanisme
- Position papers over OT
- Crisisoefeningen
- Verkennen en uitwerken collectiviseringsvoorstellen

Voorbereid op digitale ontwrichting

Situatie

- Het dreigingsbeeld: toename van cyberaanvallen, digitale spionage en beïnvloeding door statelijke actoren
- De online en offline leefwereld vloeien samen, druk op gemeentebestuurders neemt toe
- Een sterke informatiepositie over vitale processen in de gemeente en heldere rolverdeling bij crises noodzakelijk voor digitale veiligheid
- Een lokaal integraal informatiebeeld: cruciaal voor effectief handelen

Onze acties

- Uitvoeringstoets ministeriële regelingen Wet Kritieke entiteiten (Wwke)
- Ontwikkelen VNG-standpunten en beleidsadviezen over implementatie van de Wwke en het Besluit weerbaarheid kritieke entiteiten
- Scenariosessies met NCTV en BZK: doorontwikkeling Landelijk Crisisplan Digitaal
- Verkenning gemeentelijke cyberwaakzaamheid: kennen gemeenten en veiligheidsregio's de digitaal risicovolle bedrijven, zijn de (cascade)effecten bekend?
- Ontwikkelen nieuwe cyberoefendriehoek voor gemeenten, politie en OM
- Verkennen en uitwerken collectiviseringsvoorstellen

Digitaal weerbare inwoners en ondernemers

Situatie

- Traditionele criminaliteit verschuift naar de online wereld
- Voor effectief bestrijden online criminaliteit is meer inzicht nodig
- De VNG is platform voor kennisdeling, best practices en onderzoek
- De VNG ondersteunt gemeenten bij het vergroten van de digitale weerbaarheid van inwoners en ondernemer

Onze acties

- Aanjagen van toegang tot uniforme en bruikbare cyberbeelden, met snelle trenddeling en betere gegevensuitwisseling
- Blauwdruk ontwikkelen voor de lokale aanpak via best practices, knelpunten en een praktische handleiding voor gemeenten
- Landelijke partijen (o.a. rijk, CCV, PVO) structureel betrekken om digitale weerbaarheid van inwoners en ondernemers te versterken
- Centrale databank voor interventies onderzoeken in samenwerking met partners
- De community digitale weerbaarheid versterken
- Verkennen en uitwerken collectiviseringsvoorstellen

Professionalisering | krappe arbeidsmarkt

Situatie

- Het aantrekken, behouden en opleiden van goed personeel is een uitdaging voor de continuïteit en kwaliteit van digitale veiligheid
- De VNG ondersteunt de verbinding met jong cybertalent door opdrachten, stages en traineeships
- Kernuitdagingen:

  - Meer mensen, door het bevorderen van het imago van digitale veiligheidsfuncties, instroom van jong talent en loopbaanontwikkeling

  - Meer efficiëntie in uitvoering, centraal, decentraal, gezamenlijk of ondersteund door AI

Onze acties

- Structurele samenwerkingen met het rijk en mede-overheden bij stage-matching en voorbeeld-opdrachten (NDS)
- Arbeidsmarkt-communicatiecampagne, gastcolleges en online informatiesessies
- Verkenning van het veilig gebruik van AI voor veelvoorkomende digitale veiligheidstaken
- Verkennen en uitwerken collectiviseringsvoorstellen: samenwerkingsvormen en gezamenlijk invullen van arbeidskracht mede door collectivisering

Professionalisering | leiderschap

Situatie

- De VNG versterkt het bewustzijn op digitale veiligheid en biedt handelingsperspectief voor bestuurders op een overzichtelijke wijze aan
- Via opleidingen ondersteunt de VNG zowel bestuurders (burgemeesters, wethouders, raadsleden, gemeentesecretarissen) als ambtelijke experts (OOV'ers, CISO's, FG's)
- De VNG heeft een platformfunctie voor kennisdeling en ondersteuning bij implementatie (VNG Academie)

Onze acties

- Creëren meer handelingsrepertoire bestuurders:
  - opleidingsplan digitale veiligheid
  - uitwerken verplichte training onder de Cbw
  - ontwikkeling passende leermiddelen
- Structurele samenwerkingen opzetten met het rijk en andere mede-overheden bij ontwikkeling leermiddelen (NDS)
- Verkennen behoefte aan leermiddelen voor ambtelijke experts (NDS)
- Analyseren hoe gemeenten door een betere informatiepositie ook beter gaan handelen
- Verkennen en uitwerken collectiviseringsvoorstellen

EU/NL wet- en regelgeving

Situatie

- Voor gemeenten: 36 nieuwe EU-wetten en richtlijnen, waarvan zes over cybersecurity en privacy (EU Digital Decade)
- Doel is om de Cyberbeveiligingswet (Cbw), Wet weerbaarheid kritieke entiteiten (Wwke) en bijbehorende regels haalbaar, uitvoerbaar en betaalbaar te maken
- De VNG bevordert dat bestuurders de Cbw en Wwke kennen, de impact ervan begrijpen en weten welke acties nodig zijn
- En dat gemeenten weten welke eisen zij aan leveranciers moeten stellen en hoe zij daarop kunnen sturen

Onze acties

- Inzet bij inwerkingtreding Cbw (Q2 26): signaleren knelpunten, overleg BZK, pleiten voor structurele ondersteuning en financiering, verkennen van samenwerking en collectivisering tussen gemeenten
- Leveranciers informeren over verplichtingen uit Cbw, CER, RED en de Cyber Resilience Act, contractonderzoek en het opdrachtgeverschap versterken via het programma Samen Controleren
- Input en lobby met departementen over EU-keurmerken en de verdeling van verantwoordelijk-heden tussen leveranciers en gemeenten/overheden
- Vertaling wetgeving naar inkoopeisen voor gemeentelijke aanbestedingen

Weerbare samenleving

https://vng.nl/artikelen/hulpmiddelen-en-publicaties-over-digitale-veiligheid





Digitale veiligheid is de norm

Vragen? Mail naar teamADV@vng.nl

Agenda Digitale Veiligheid 2024 - 2028

De Nederlandse Digitaliseringsstrategie **Samen versnellen**



Nederlandse Digitaliseringsstrategie

De Nederlandse Digitaliseringsstrategie

NDS - Digitale Weerbaarheid & Autonomie - 6 versnellers:

1. Implementeren bestuurlijk convenant gemeenten

- Het convenant (dec 2022) beoogt de gezamenlijke inzet op digitale veiligheid van gemeenten verder uit te werken.

2. Werken aan een federatief SOC-stelsel

- SOC (Security Operations Center) stelsel Rijk
  - verbreding naar andere overheden en
  - versterking van de tactische inzetbaarheid.

3. Versterken continuïteit van kritieke dienstverlening

- Overheidsdienstverlening is verregaand gedigitaliseerd. Dat is een kracht, maar het maakt ons ook kwetsbaar. Daarom is het noodzakelijk om de continuïteit van kritieke overheidsdienstverlening zo snel als mogelijk te versterken.

4. Inzicht in kritieke dienstverlening en IT bouwblokken

- Inzicht is de basis van veel processen, waaronder risico management, als uitgangspunt voor te maken keuzes. Dit geldt voor zowel kritieke dienstverlening als voor de IT, OT, IoT die ingezet wordt om de diensten uit te kunnen voeren (IT assetmanagement).
- Dit inzicht is op veel plaatsen ook binnen de overheid van onvoldoende kwaliteit. Deze versneller beoogt hier verandering in te brengen.

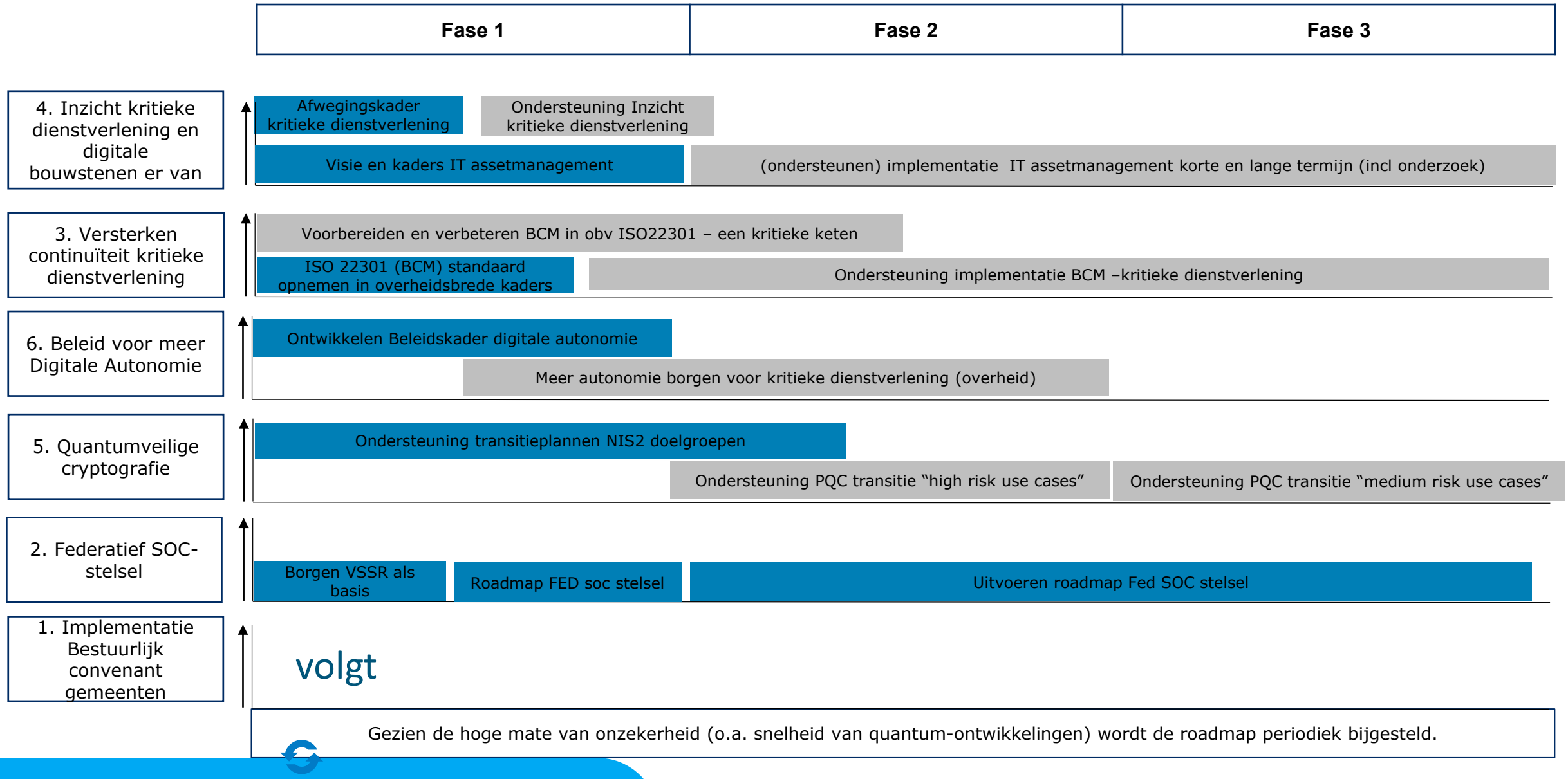
5. Quantumveilige encryptie

- Cryptografie vormt een fundament voor de informatiebeveiliging. Met de realisatie van een krachtige quantumcomputer, verliest veelgebruikte cryptografie zijn beveiligingswaarde.
- Het is daarom urgent om te starten met de migratie van huidige cryptografie naar Post Quantum Cryptografie (PQC).
- De transitie naar PQC is complex en kennis en capaciteit zijn schaars. Samenwerken moet.

6. Digitale autonomie

- De digitale autonomie van de gehele Nederlandse overheid moet significant worden versterkt omdat we voor veel processen afhankelijk zijn van een klein aantal (niet-Europese) leveranciers, wat leidt tot verschillende risico’s.

NDS Roadmap DW & A



NDS - Synergie en afhankelijkheden

Kansen synergie en hergebruik

Cloud
De soevereine overheidscloud moet voortbouwen op de kennis van digitale autonomie

Burger en ondernemer centraal
Herontwerp ketenprocessen – specifiek gericht op onderlinge uitwijkingsmogelijkheden binnen een keten

Data
Classificeren welke data belangrijk zijn voor kritieke dienstverlening vraagt samenwerking tussen beide prioriteiten.

Onderlinge afhankelijkheid

Interventie – wegnemen juridische belemmeringen
Overheidsbreed inkopen, aanbesteden, leveren diensten stuit op juridische voorwaarden Huidige financieringsstructuren borgen onvoldoende continuïteit en weerbaarheid/kwaliteit van collectieve bouwstenen/ voorzieningen

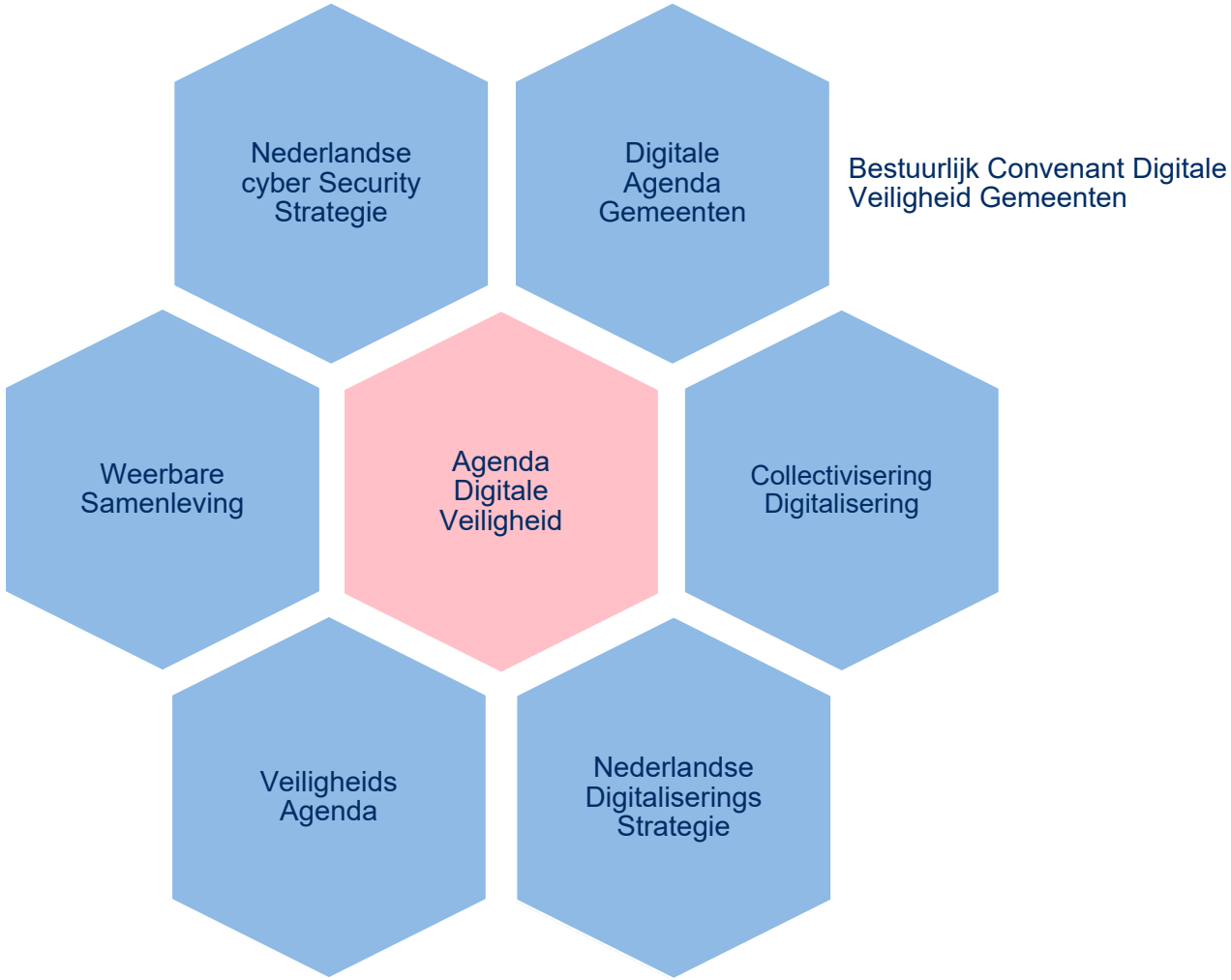
Input vanuit prio Cloud

Classificatie soevereiniteit. Dit betreft het categoriseren van digitale diensten, data en infrastructuur op basis van de mate van controle, onafhankelijkheid en juridische bescherming tegen buitenlandse inmenging. Classificatie soevereiniteit helpt ons om te bepalen welke oplossingen als veilig genoeg beschouwd worden.

Met versneller standaardisatie: Nieuwe kaders en instrumenten voor cybersecurity worden overgenomen uit deze prioriteit voor zover ze betrekking hebben op clouddiensten.

Afhankelijkheid tussen Cloud versneller 3 “we zorgen voor een centraal inzicht in de behoeftes van cloud, door de verschillende vragen te bundelen” en
DW versneller 4 “er komt overheidsbreed inzicht in kritieke IT-dienstverlening, en de bouwstenen daarvan, inclusief legacy problematiek.

Samenhang Digitale Weerbaarheid gemeenten



Samenhang en overlap

Agenda Digitale Veiligheid	Convenant	Covo's	NDS/mede overheden
Wet en regelgeving	Structurele financiering	Consultatie, beleid Structurele financiering	Structurele financiering Convenant
Eigen huis/basis op orde	IBD-CSIRT	IBD-CSIRT en IB advies	CSIRT-stelsel
	Invoering BIO2	Regio ondersteuning CISO's	Continuïteit kritieke dienstverlening
	Monitoringdienst IBD	Monitoringdienst	Gezamenlijk Security Operation Centre
	Samen controleren	leveranciersmanagement	leveranciersmanagement
		Standaardiseren SSC's	
			Quantum Veilige Encryptie (PQC)
	ENSIA	Uitbreiding ENSIA	ENSIA Rijk/Provincies
Vakmanschap/ professionalisering		As-a-service: CISO, PO, FG, Aditor Opleiding bestuurders Overige opleidingen	Opleiding bestuurders Overige opleidingen
Voorbereiding digitale ontwrichting	Informatiepositie Digitaal veiligheidsstelsel verantwoordelijkheden Oefenscenario's	Oefenscenario's	Oefenscenario's
Weerbaarheid inwoners/ondernemers	Regio ondersteuning OOV	BOA's	Regio ondersteuning OOV
Online aangejaagde ordeverstoringen/ desinformatie	Onderzoekstool	Onderzoekstool	
		Besparingsmotor	
Veiligheid		BOA's	
Privacy		Privacy Office	**KEN!**

Roadmap

CBW

ALV

ALV

	Q1 2026	Q2 2026	Q3 2026	Q4 2026	Q1/2 2027	Q3/4 2027	2028
IBD-BZK	Wettelijke aanwijzingen CSIRT	Structurele financiën Juridische toetsing Vastleggen aanwijzing	Nadere afspraken nav aanwijzing / Structurele financiering	Verantwoording ingericht			
IBD-CERT	Planvorming CSIRT	Basis CSIRT	Doorontwikkeling CSIRT	Robuuste CSIRT met structurele financiering		Robuuste CSIRT met structurele financiering	
IBD-Advies	Planvorming CSIRT	Basis CSIRT	Doorontwikkeling IB-Advies	Robuuste IBD CSIRT en IB-Advies		Robuuste IBD CSIRT en IB-Advies	
Scanning monitoring	Besluit over scope en starten heraanbesteding EASM tooling	Starten heraanbesteding, PvE. wettelijke CSIRT-taak	Opleveren nieuwe tooling Opzeggen huidig contract wettelijke CSIRT-taak	wettelijke CSIRT-taak Opgenomen in structurele financiering?	Aansluiting SOC/ andere overheden?		
BIO2 ondersteuning	Regio ondersteuning BIO2	Regio ondersteuning BIO2 Structurele financiering	Regio ondersteuning BIO2 Structurele financiering	Wel/geen vervolg financiering? Uitbreidbaar ook andere overheden?	Wel/geen vervolg financiering? Uitbreidbaar ook andere overheden?		
Samen controleren	Uitkomsten pilot IBD Burgerzaken app Aantrekken PM	Kwartiermakersfase Ook voor OT leveranciers	Bestendigen controle dienst Wel/geen vervolg financiering?	Wel/geen vervolg financiering? Uitbreidbaar ook andere overheden			
Inkoop IB	Mantelcontract BIZOB: -Monitoring-beveiligingstechniek -Adviesdiensten -Forensisch digitaal onderzoek		Uitbreiden met…			Mantelcontract BIZOB: -Monitoringtools -Adviesdiensten -Beveiligingstechniek -Forensisch digitaal onderzoek	

Roadmap

CBW

ALV

ALV

Start verantwoordingsjaar 2026 obv BIO2

	Q1 2026	Q2 2026	Q3 2026	Q4 2026	Q1/2 2027	Q3/4 2027	2028
ENSIA bestaand	Verbetering inzicht in feitelijke veiligheid, BIO2 vragenlijst Communicatie nieuwe formats	Communicatie nieuwe formats Ondersteuning gebruik	Voorbereiden op verantwoorden over de BIO2, Start verantwoording obv aanwezige info	Start verantwoording obv aanwezige info	Opzeggen huidig contract		
ENSIA herontwerp	Vooronderzoek/markt consultatie heraanbesteding -betrekken mede-overheden (Geo-basis)	Starten heraanbesteding PvE: ISMS aansluiting, OT/PA, modulair uitbreidbaar ook andere overheden	Heraanbesteding ENSIA	Inrichting tooling ENSIA ENSIA andere overheden	Opleveren nieuwe tooling Opzeggen huidig contract	Starten verantwoording in nieuwe tooling obv BIO2	
Vakmanschap	Training raadsleden, wethouders, gemeentesecretarissen	Opleiding bestuurders cbw Samen met andere overheden	Actueel trainingsaanbod Overige trainingen communicatie	Voorbereiding Poolvorming?	Poolvorming?		
Beleid DV	Consultatiereactie wet- en regelgeving Digital Decade cyber, privacy, AI / Samenhang / Structurele financiering	Gemeenschappelijke regelingen? Duidelijkheid toezicht Structurele financiering	Nadere afspraken cbw, samenwerking rijk-gemeenten / Implementatie ondersteuning / Structurele financiering		Standaardiseren van de diensten, processen en systemen van gemeentelijke SSC's?	Consultatiereactie wet- en regelgeving Digital Decade cyber, privacy, AI / Samenhang / Implementatie ondersteuning/ Structurele financiering	
PQC	Post Quantum Cryptografie	Quantum Veilige Encryptie/mede overheden	Gemeentelijke activiteiten??				
Privacy	IBD- Privacyteam	**Samenvoeging met KEN! uitbreiding KEN+?**	Centraal Privacy Office?	Besparingsmotor			
BOA's	BOA dienstverlening		BOA dienstverlening	Besparingsmotor			

Aandachtspunten en hulpvragen

- Nog meer gezamenlijk, denken, delen en doen: financiering, capaciteit etc. Breid het netwerk verder uit (bv fintech/DNB), sluit aan bij zaken zoals de NORA, maak gebruik van bodies of knowledge etc.

- Hoe zorgen voor goed en breed bezette kernteams en werkgroepen vanuit alle overheidslagen?
  - Interesse? Geef je op!

- Onder politieke en bestuurlijke druk: hoe voorkomen we dat dergelijke druk leidt tot extra belasting die ons afhoudt van het bereiken van resultaten?

- Hoe zorgen we voor budget: wat loopt nog, waar zijn nog mogelijkheden, EU subsidies? Dit heeft ook een relatie met de politieke en bestuurlijke verwachtingen.

Succesfactoren

Welke elementen in je aanpak maken dat je succesvol bent en kunnen bruikbaar zijn voor anderen?

- Actieve, ondernemende portefeuillehouders/aanjaagteam
- Brede vertegenwoordiging in aanpak en werkgroepen
- Focus op concrete resultaten met goede kwaliteit en draagvlak. Planning is secundair: een valse start diskwalificeert
- Klein beginnen met partijen die willen, zo iedere keer ‘no regret’ resultaten halen en pas daarna groter maken
- Samenwerking met specifieke stakeholders en deze zichtbaar maken. (Denk aan de financiële sector, fysieke infrastructuur (spoor, water), andere EU lidstaten...)
- Op de politieke golven surfen: dat zijn kansen om vooruit te komen.



Meer weten?

Doe mee in de community:
https://Digitaleveiligheid.pleio.nl/
Agenda Digitale Veiligheid

Of:
mail **teamadv@vng.nl**