



Digitale weerbaarheid

Wat doet IPO en wat kunt u doen als Statenlid?

Marten Tilstra

Programmamanager Digitalisering IPO

Inhoud

- > Samen staan we sterk: de Nederlandse Digitaliseringsstrategie (NDS)
- > Digitale weerbaarheid in het IPO-programma Digitalisering
- > Wat kunt u doen als Statenlid? – enkele voorbeelden



Colofon

De Nederlandse Digitaliseringsstrategie is een initiatief van de Rijksoverheid in samenwerking met:



juni 2021

Nederlandse Digitaliseringsstrategie

Prioriteiten

1. Cloud

2. Data

3. Artificiële
intelligentie

4. Burger/ondernemer
centraal

5. Digitale
weerbaarheid en
autonomie

6. Digitaal
vakmanschap

Interventies

Versterkte aanpak
handhaven standaarden

collectieve oplossingen en
bouwstenen

Overheidsbrede IT-sourcing
strategie en bundelen
inkoopkracht

Implementatie digitale
wetgeving & juridische
belemmeringen

De vrijblijvendheid voorbij

5. Digitale weerbaarheid en autonomie

Welke belemmeringen zijn er nu?

Er is geen overheidsbrede, gecoördineerde aanpak voor cyberveiligheid gericht op de overheid.

SOC-dienstverlening is verkokerd en werkt nog onvoldoende intensief samen.

Overheidsorganisaties zijn kwetsbaar voor acute en langdurige uitval van ICT- diensten.

Er is onvoldoende inzicht in waar onze legacy-systemen zitten en de daarbij behorende kwetsbaarheden.

Iedereen werkt eigen bouwstenen individueel uit en/of koopt hetzelfde in.

Er is geen eenduidige aanpak om digitale strategische afhankelijkheden voor de overheid te verminderen.

Waar we nu als één overheid op versnellen

De implementatie van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten, als onderdeel van de Nederlandse Cybersecuritystrategie (NLCS), wordt versneld gerealiseerd.

We werken samen aan federatief SOC-stelsel.

We versterken de continuïteit en wendbaarheid van onze kritieke dienstverlening zowel onder normale als onder ongunstige omstandigheden.

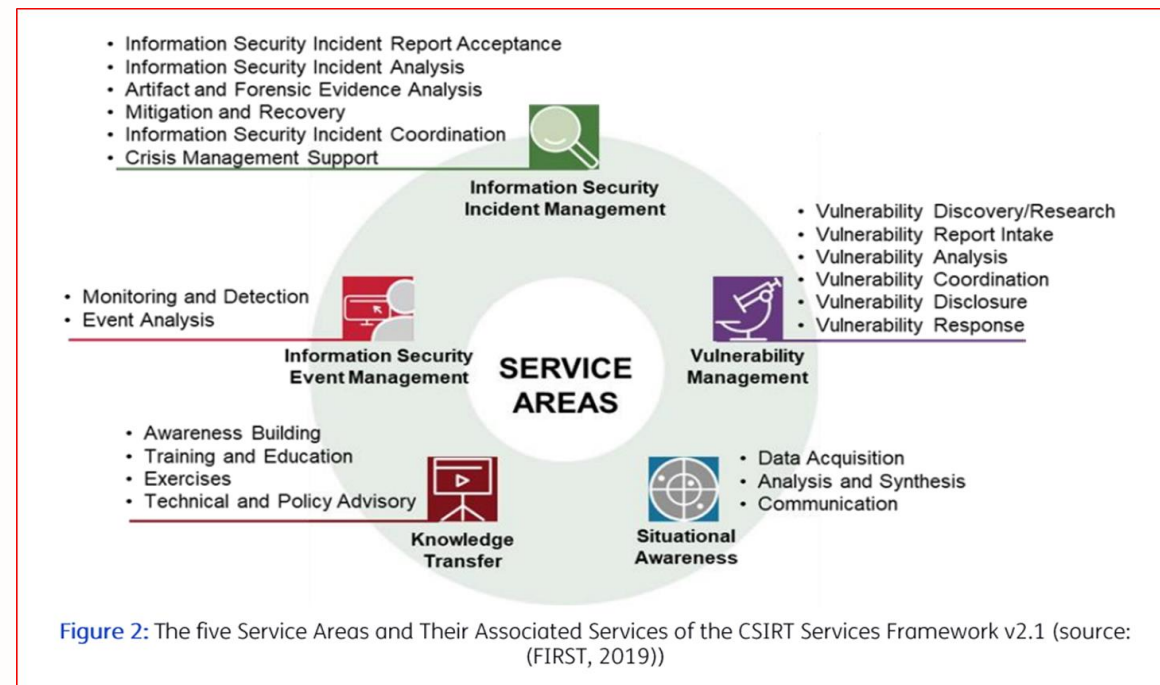
Er komt overheidsbreed inzicht in kritieke IT-dienstverlening, en de bouwstenen daarvan, inclusief legacy problematiek.

Cyberveiligheidsbouwstenen zoals quantumveilige encryptie worden collectief ontwikkeld en geïntegreerd.

Er komt beleid om gezamenlijke digitale autonomie te vergroten.

Waarom een CSIRT en een SOC?

- Sectoraal CSIRT → wettelijk verplicht op grond van meldplicht NIS2-verordening
- Sectoraal SOC → zorgplicht NIS2 én vergroten *feitelijke* veiligheid



Bestuursprogramma IPO 2023-2027 – Thema Digitalisering



Weerbaarheid in het IPO-programma Digitalisering

I. Strategieontwikkeling lagen public stack

Strategievorming lagen public stack (Ian O'Hagan)

II. Versterken informatiepositie voor de opgaven

Versterken informatiepositie voor opgaven K&E en LG

Verkenning open sources provincies

Interprovinciaal stelsel gegevenswoordenboeken

Structureren, org. en aanjagen innovatieproces

Dutch Societal Innovation Hub (DSIH)

Digitale ethiek

III. Weerbaarheid, Digitaliseringswetgeving en Digitaal Vakmanschap

Data- en informatiehuishouding op orde

Oprichting interprovinciaal SOC en aansluiting op CSIRT NCSC

Verkenning Strategische Autonomie/Digitale soevereiniteit provincies

Coördinatie implementatie digitaliseringswetgeving

Ontwikkeling 21ste-eeuwse vaardigheden



Interprovinciaal Overleg
van, voor en door provincies

De rol van de provincie (extern en intern)

Op gebied van weerbaarheid heeft de provincie een externe en een interne rol:

- *Richting de samenleving (als middenbestuur en ketenpartner):* indien gewenst andere organisaties helpen die ook met weerbaarheid bezig zijn (bijvoorbeeld gemeenten en veiligheidsregio's)
- *Op het gebied van de eigen dienstverlening/de interne organisatie:* versterken van de weerbaarheid van de provinciale organisatie door “Business Continuity Management” te borgen: welke processen moet je zo snel mogelijk weer opstarten als deze door omstandigheden stilvallen, en hoe doe je dat? Inclusief plannen, voorzieningen, en trainingen/opleiding.



Wat kunt u doen als Statenlid? – Enkele voorbeelden

Kaderstellende rol:

- Verdiep u in het bestaande informatiebeveiligingsbeleid en ga bij vernieuwing van dit beleid na of dit goed aansluit op nieuwe wetgeving (Cbw/Wwke) en actuele ontwikkelingen in uw provincie, en of risico's afdoende worden beheerst;
- Ga na of het geldende informatiebeveiligingsbeleid ook van toepassing is voor Provinciale Staten en de griffie, of dat daar een eigen beleid voor is;
- Ga bij de Kadernota en de Programmabegroting na of de middelen voor de uitvoering van het beleid toereikend zijn, en neem waar nodig initiatief om hierbij prioriteiten te leggen of accenten aan te brengen;
- Vanuit het perspectief “Samen versnellen” van de NDS: beoordeel voorstellen van het college mede vanuit de mogelijkheden die interbestuurlijke samenwerking biedt.



Wat kunt u doen als Statenlid? – Enkele voorbeelden

Controlerende rol:

- Check of uw provincie voldoet aan geldende wet- en regelgeving, zoals de Baseline Informatieveiligheid Overheid (BIO), en hoe uw provincie zich voorbereidt op de BIO2 en de invoering van de Cbw en de Wwke.
- Ga na of uw provincie vitale infrastructuur beheert (bijvoorbeeld grote bruggen/sluizen), hoe de beveiliging van deze belangrijke objecten is geregeld, en wat hier aanvullend nodig zou zijn;
- Ga na of en hoe uw provincie deelneemt aan het interprovinciale initiatief om aan te sluiten op het CSIRT van NCSC, en hoe in uw provincie SOC-dienstverlening is geregeld (via het interprovinciale project bij IPO, zelfstandig, of anderszins);
- Vraag hoe cruciale data/gegevens die nodig zijn voor de opgaven van provincies worden beveiligd (“kroonjuwelen”);
- Ga na of informatiebeveiligingsrisico's periodiek worden geëvalueerd, of er incidenten zijn geweest en hoe die zijn geëvalueerd;
- Vraag na welke leveranciers uw provincie gebruikt, en of er maatregelen zijn genomen om de digitale autonomie van de provincie te borgen.
 - Aandachtspunt: het is juridisch niet mogelijk om Amerikaanse “big tech” aanbieders als Microsoft (kantoorapplicaties) of Esri (voor geo-informatie) uit te sluiten in aanbestedingen. Wel kunnen maatregelen worden genomen om verlies van gegevens te voorkomen en bij wegvallen van diensten over te kunnen stappen naar een alternatief.

Wat kunt u doen als Statenlid? – Enkele voorbeelden

Volksvertegenwoordigende rol:

- Ga na hoe het college ethische vraagstukken bij informatiebeveiliging meeneemt in voorstellen die aan u worden voorgelegd (voorbeeld: bescherming van privacy bij cameratoezicht op vitale infrastructuur);
- Plaats informatiebeveiliging in bredere context (“all hazards approach”): welke andere risico’s zijn te onderkennen naast informatieveiligheidsrisico’s, en wat is daarbij het risico voor inwoners en ondernemers? Voorbeeld: risico op aanslagen op vitale infrastructuur.



Discussie



Achtergrondslide (indien nodig) – wettelijk kader

