VERDONCK KLOOSTER & ASSOCIATES

FS-20161019.04A

SAMENHANG IN ICT-BEVEILIGINGSSTANDAARDEN

Verkenning en strategie voor de overheid

VERDONCK KLOOSTER & ASSOCIATES

FS-20161019.04A

SAMENHANG IN ICT-BEVEILIGINGSSTANDAARDEN

Verkenning en strategie voor de overheid

René van den Assem en Douwe Horst

DATUM	7 oktober 2016
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20152306
INTERNE TOETS	Paul Dam

MANAGEMENTSAMENVATTING

Betrouwbaarheid, integriteit en vertrouwelijkheid zijn cruciaal voor interoperabiliteit. Standaarden voor informatiebeveiliging dragen daaraan bij. Onder ICT-beveiligingsstandaarden verstaan we in dit onderzoek ook richtlijnen, normen en kaders. Er is helaas niet één bepaalde ICT-beveiligingsstandaard die alle beveiligingsrisico's afdekt. Daarom moet er een samenspel zijn van meerdere standaarden.

Bij de opname van nieuwe standaarden op de lijsten met open standaarden wordt altijd gekeken naar de relatie tot bestaande standaarden op de lijsten. Dit kan echter onvoldoende zijn omdat hierdoor geen zicht is op welke standaarden mogelijk nog meer relevant zijn, de zogenoemde 'witte vlekken'. Bovendien is de samenhang niet altijd duidelijk voor een gebruiker van de lijst. Dit is ook naar voren gekomen in het Forum. Het Forum startte daarom dit onderzoek om de samenhang tussen beveiligingsstandaarden beter inzichtelijk te maken en 'witte vlekken' te identificeren.

In dit onderzoek wordt antwoord gegeven op (samengevat) de volgende vragen:

1. Welke stappen zijn te zetten om te komen tot een effectievere en meer samenhangende benadering van het onderwerp ICT-beveiligingsstandaarden en
2. Op welke gebieden zijn welke belangrijke ontwikkelingen gaande, die vragen om aanvullende en/of nieuwe acties op het gebied van standaardisaties vanuit de Nederlandse overheid.

De belangrijkste conclusies op het gebied van punt 1 zijn:

1. Voor organisaties die ICT-beveiligingsstandaarden willen toepassen, is er sprake van een zoekplaatje. Wat verplicht is, aanbevolen dan wel 'nice-to-have' is niet eenvoudig te bepalen.
2. De governance op de nakoming van relevante eisen is in algemene zin weinig verplichtend. Met name tussen organisaties is weinig geregeld, met uitzondering van een aantal specifieke ketens of voorzieningen. Er is eerder sprake van collegiale toetsing tussen organisaties, dan dat er sprake is van een objectieve beoordeling en transparantie wat betreft de uitkomsten van die beoordeling.
3. ICT-beveiligingsstandaarden vormen een uiterst gefragmenteerd landschap. Dat bleek eerder al uit een WODC-onderzoek (uitgevoerd door Innovalor). Die standaarden variëren:
   - Van meer ICT-technisch naar meer organisatorisch;
   - Van 'klein' (bijvoorbeeld betrekking hebbend op een specifieke maatregel zoals een cryptografisch algoritme) tot 'groot' (bijvoorbeeld een norm voor de gehele informatiebeveiliging in een organisatie).
   - Van best practice tot dwingend voorschrijvend.

Er bestaat daardoor ook niet één optimale wijze van ordenen van ICT-beveiligingsstandaarden voor alle doeleinden.

Bovenstaande factoren leiden tot een schijnbare willekeur in het informatiebeveiligingsniveau dat daadwerkelijk wordt gerealiseerd door een organisatie. Dit is niet alleen van nadelige invloed voor de organisatie zelf en de partij die toezicht houdt op deze organisatie, het is ook van wezenlijk nadelige invloed op de samenwerking in ketens en netwerken!

Op basis van het voorgaande beeld formuleren wij de volgende aanbevelingen om de governance te verbeteren:

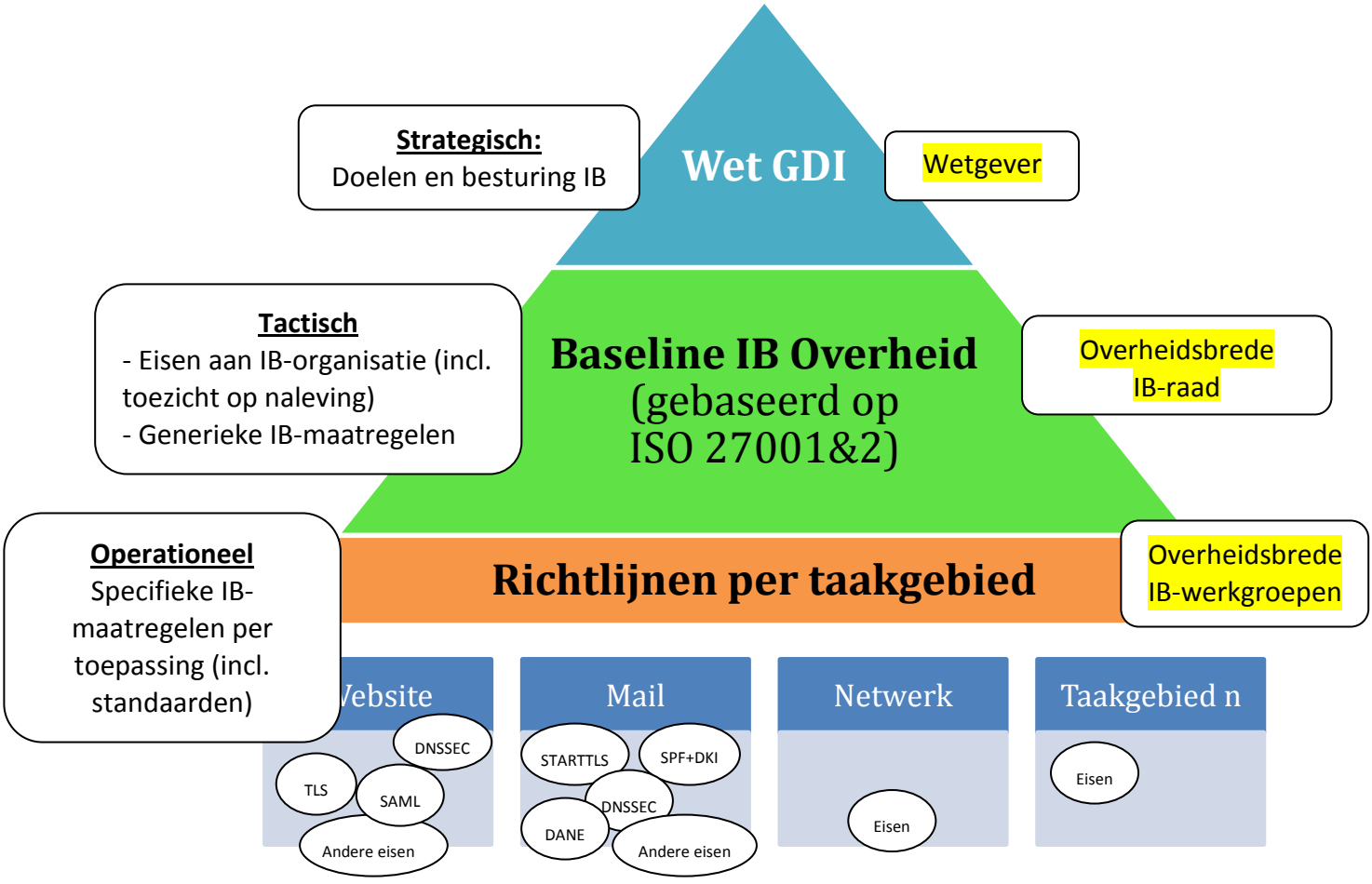
1. Neem een 'haakje' op in de wet GDI voor overheidsbrede eisen voor informatiebeveiliging.
2. Dwing goede beheersing van informatiebeveiliging af. Groei verder vanaf het huidige model van collegiale toetsing naar formele toetsing. Het uiteindelijke doel zou externe certificatie tegen de ISO 27001 kunnen zijn. Ongetwijfeld zal naar dit streven stapsgewijs toegegroeid kunnen worden. Het is bijvoorbeeld denkbaar om het goede voorbeeld te geven met de GDI-voorzieningen.
3. Harmoniseer bestaande baselines (BIR, WIG, IBI, BIWA) tot een Baseline Informatiebeveiliging Overheid (BIO). We adviseren de Baseline Informatiebeveiliging Overheid met hoge prioriteit af te ronden. Dit maakt eenvoudiger samenwerking tussen organisaties mogelijk in het kader van ketens en netwerken (uniformiteit en transparantie).
   Laat deze BIO voor concrete taakgebieden zoveel mogelijk verwijzen naar richtlijnen, zodat ook de status van die richtlijnen (verplicht, aanbevolen, nice-to-have) duidelijk wordt.
4. Hanteer het instrument van de wettelijke verplichting vaker en laat de auditor ook op genoemde wettelijke verplichtingen controleren, met name als het gaat om die technische standaarden die goed zijn op te volgen zonder al te grote externe afhankelijkheden (denk bijvoorbeeld aan TLS, DNSSEC, een veilig mailprofiel).[1]
5. Vergroot de transparantie hoe overheidsorganisaties het doen op het gebied van informatiebeveiliging. Doe dit door:
   - enerzijds door te gaan werken aan een uniforme standaard voor verantwoording (rol project ENSIA) en
   - anderzijds door de technische beveiliging van Internet-facing systemen testbaar te maken volgens de aanpak van www.internet.nl (Platform Internet Standaarden).

[1] Sommige ICT-beveiligingsstandaarden zijn door een enkele organisatie op eigen initiatief na te leven. Wij stellen voor de algemeen toepasselijke standaarden ook wettelijk te verplichten, bijvoorbeeld in de Wet GDI. Op te nemen zaken kunnen bijvoorbeeld HTTS-only, TLS 1.2 en DNSSEC zijn. Dit instrument wordt nog maar weinig gebruikt (bijvoorbeeld wel bij de toegang tot elektronische dienstverlening van de Burgerlijke Stand), maar kan slepende discussies met organisaties in de groep 'achterblijvers' of 'late majority' eenvoudig beslechten.

Daarnaast doen we de volgende aanbevelingen om tot een betere structurering van standaarden te komen:

1. Structureer en cluster de individuele normen en standaarden in richtlijnen voor duidelijk omschreven taakgebieden, met als doel om het voor de individuele overheidsorganisatie minder een zoekplaatje te maken en om onduidelijkheid weg te nemen over welke normen en standaarden toe te passen in bepaalde situaties. Hiervoor kunnen de stappen gezet worden zoals aangeduid in paragraaf 3.5.
2. Maak één van de actoren die informatiebeveiliging in de Nederlandse overheid besturen, verantwoordelijk voor een dergelijke structurering en harmonisatie. Uiteraard hoort hier een passend mandaat bij, zodat standaarden ook verplicht opgelegd kunnen worden aan partijen en de status van standaarden bepaald kan worden.
3. Bestuur al deze activiteiten in één nationale governance, waarbinnen de besluitvorming over richtlijnen (wat is hun status) plaatsvindt. Het ligt voor de hand om hierbij aansluiting te zoeken op de reeds bestaande governance op standaarden.

Ter illustratie van de relatie tussen de verschillende niveaus zie onderstaande figuur:



Ter toelichting het volgende:

- Het hoogste niveau, het strategische niveau, wordt gevormd door de Wet Generieke Digitale Infrastructuur (Wet GDI). Hierin komt de verplichting om een goede informatiebeveiliging in te richten en te onderhouden. Ook wordt hierin duidelijk hoe de governance hierop wordt geregeld, waarbij de hoge mate van vrijblijvendheid en collegiale sturing door een dwingender kader wordt vervangen.
- Het tactische kader is feitelijk de plaats waar de normen worden gesteld in algemene zin. Nemen we het voorbeeld van beveiliging van een lokaal netwerk, dan zou hier als norm kunnen worden opgenomen dat het LAN zodanig dient te worden beveiligd, dat bekend is welke lokale gebruikers er op actief zijn. Verder wordt er verwezen naar een 'Richting LAN-beveiliging', aannemende dat die er is. Aangegeven wordt of die richtlijn verplicht gevolgd dient te worden of niet. In de BIO worden dus nadrukkelijk niet alle normelementen voor de beveiliging van lokale netwerken opgenomen.
- In de 'Richtlijn LAN-beveiliging' worden wel alle normelementen voor de veilige inrichting van een LAN opgenomen en dit gaat uiteraard ook verder dan sec het benoemen van standaarden. Hierbij is duidelijk wat verplicht is, wat aanbevolen en wat 'nice-to-have' is. Eén van de zaken die in deze richtlijn wordt genoemd, is bijvoorbeeld de IEEE 802.1x standaard, een standaard die port-based netwerktoegangscontrole regelt. Daarmee zijn apparaten die aan het lokale netwerk verbinden, geauthenticeerd.

De bovenstaande aanbevelingen richten zich op systemen en structuren. Het moge duidelijk zijn dat daarnaast de mens een cruciale factor is in het bewerkstelligen van goede informatiebeveiliging. Een organisatie kan nooit goede informatiebeveiliging realiseren zonder een actieve betrokkenheid van al haar medewerkers. Dit vertaalt zich in zaken zoals een juiste cultuur, kennis en bewustzijn van de eigen rol.

Wat betreft de mogelijk interessante inhoudelijke ontwikkeling van standaarden zijn veel suggesties gekomen uit een workshop en interviews met stakeholders. Deze inhoudelijke onderwerpen zijn uitgewerkt in hoofdstuk 4 van dit rapport:

1. eID en vertrouwensdiensten
2. Nieuwe kanalen voor elektronische dienstverlening
3. Veilige applicatieontwikkeling
4. Veilige e-mail
5. Privacy-by-design
6. Internet of Things
7. Cloud
8. Reageren op cyber threats

INHOUDSOPGAVE

1 INLEIDING

1.1 Achtergrond

Het Forum Standaardisatie houdt zich ten behoeve van betrouwbare gegevensuitwisseling binnen de gehele (semi) publieke sector ook bezig met standaardisatie van informatiebeveiliging. Dit volgt uit het besluit van het Nationaal Beraad Digitale Overheid d.d. 10 februari 2015, bekrachtigd door de Ministerraad op 6 maart 2015 inzake de doelen, taken, werkwijze en samenstelling van het Forum Standaardisatie voor de periode 2015-2017[2]. Hierin staat dat wordt gestreefd naar “veilige en betrouwbare uitwisseling en (her)gebruik van gegevens tussen overheidsorganisaties en bedrijven”. In dit kader is een aantal informatiebeveiligingsstandaarden opgenomen op de ‘pas toe of leg uit’-lijst en lijst met gangbare/aanbevolen open standaarden. Daarnaast heeft het Forum onder andere de 'Handreiking Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten' ontwikkeld en is op verzoek van NCSC vanuit standaardisatieperspectief gereageerd op hun nieuwe concept-versie van de ‘ICT-beveiligingsrichtlijnen voor webapplicaties’ waarin ook de relevante standaarden terugkomen.

Standaarden zijn cruciaal voor informatiebeveiliging omdat betrouwbaarheid, integriteit en vertrouwelijkheid cruciaal zijn voor interoperabiliteit. Onder ICT-beveiligingsstandaarden verstaan we in dit onderzoek ook richtlijnen, normen en kaders. Er is helaas niet één bepaalde ICT-beveiligingsstandaard die alle beveiligingsrisico’s afdekt. Het gaat om een samenspel van meerdere standaarden. Bij de opname van nieuwe standaarden op de lijsten met open standaarden wordt altijd gekeken naar de relatie tot bestaande standaarden op de lijsten. Dit kan echter onvoldoende zijn omdat hierdoor geen zicht is op welke standaarden mogelijk nog meer relevant zijn, de zogenoemde ‘witte vlekken’. Bovendien is de samenhang niet altijd duidelijk voor een gebruiker van de lijst. Dit is ook naar voren gekomen in het Forum. Het Forum startte daarom dit onderzoek om de samenhang tussen beveiligingsstandaarden beter inzichtelijk te maken en ‘witte vlekken’ te identificeren.

1.2 Vraagstelling

Het Forum wil middels dit onderzoek inzicht krijgen in de huidige situatie van ICT-beveiligingsstandaarden en wil toe naar een meer gerichte aanpak van ICT-beveiligingsstandaarden.

De originele vraagstelling zoals opgenomen in de oplegnotitie “Adoptie open standaarden” van 10 juni 2015 was de volgende:

1. Lijst en blinde vlekken: Welke ICT-beveiligingsstandaarden staan nu op de lijst met open standaarden? Ontbreken er IB-standaarden op de lijst (zie bijlage A in het rapport)? Zijn er

[2] https://www.forumstandaardisatie.nl/fileadmin/user_upload/20150306_Besluit_inzake_doelen_taken_werkwijze_en_samenstelling_Forum_Standaardisatie_2015-2017.pdf

belangrijke nieuwe ontwikkelingen? (zie paragraaf 3.4 en 3.5 in het rapport)
Daarbij ook kaders/richtlijnen meenemen zoals “Grip op secure software development (SSD)” en “ICT-beveiligingsrichtlijnen voor webapplicaties”.

2. Samenhang: Hoe verhouden de geïdentificeerde ICT beveiligingsstandaarden zich tot elkaar? Hoe zou de samenhang kunnen worden versterkt? (zie paragraaf 3.5 in het rapport).
3. Adoptie: Hoe verloopt de adoptie van deze standaarden en hoe kan deze worden versneld? (ook evt. via harmonisatie om audit-/implementatiedruk te verlichten) (zie hoofdstuk 4 voor beantwoording op abstract niveau).

1.3 Visie op de vraag, aangepaste vraagstelling

Onze aanpak kenmerkt zich door aansluiting bij de behoefte van het Forum om te handelen vanuit een grotere samenhang. Daarom wordt een breder beeld van de huidige omgeving rondom ICT-beveiligingsstandaarden geschetst, waarin de ICT-beveiligingsstandaarden vervolgens hun plek krijgen. De volgende stappen zijn daarbij te onderkennen:

1. Identificeren van relevante (taak)gebieden waarin ontwikkelingen in ICT beveiliging plaatsvinden;
2. Identificatie van mogelijk interessante standaarden of taakgebieden die standaardisatie behoeven, aansluitend op bovengenoemde beleidsdoelen en ontwikkelingen. Een taakgebied is een enkele taak of verzameling van logisch samenhangende taken, waarvoor richtlijnen voor goede informatiebeveiliging zijn op te stellen.
3. Vaststellen van de gewenste vervolgacties.

Het vertrekpunt is niet zozeer de ICT-beveiligingsstandaarden zelf maar de doelen die daarmee gediend worden. Plaatsing op de lijst met open standaarden is een middel om de ‘te dienen doelen’ te bereiken. Andere middelen zijn adoptiebevorderende maatregelen, en bijvoorbeeld ook het stimuleren van bijdragen aan standaardisatietrajecten.

Omdat de denklijn die hierboven is geformuleerd een wezenlijk andere is dan een denklijn die is gericht op het aanvullen van de lijsten met open standaarden met ICT-beveiligingsstandaarden (of aanpassing van reeds opgenomen ICT-beveiligingsstandaarden), rapporteren we in het rapport slechts over deze denklijn. De aanbevelingen omtrent de opname van ICT-beveiligingsstandaarden zijn separaat gerapporteerd in het onderzoek ‘Aanvullende aanbevolen standaarden’, de uitvoering hiervan loopt gelijktijdig met dit onderzoek.

Er is in het onderzoek, naast de bovengenoemde drie stappen, een longlist van ICT-beveiligingsstandaarden in Bijlage A beschouwd, die afkomstig is uit diverse bronnen. Dit om de afleiding van beleidsdoelen naar (taakgebieden voor) ICT-beveiligingsstandaarden zo concreet mogelijk te behouden. Er is in de longlist aangegeven welke standaarden nu onderdeel zijn van het onderzoek naar ‘Aanvullende aanbevolen standaarden’ en welke standaarden op dit moment al op de lijst met open standaarden staan.

1.4 Scope

Binnen dit onderzoek worden ICT-beveiligingsstandaarden onderzocht. Het onderzoek richt zich met name op standaarden die belangrijk zijn voor de overheid. Er is wel oog voor aangrenzende sectoren, maar dit heeft niet de focus. Sectorspecifieke standaarden zijn derhalve niet beschouwd. Daarnaast dienen de standaarden 'open' standaarden te zijn en moeten de standaarden een relatie hebben met gegevensuitwisseling (interoperabiliteit).

Voor de te onderzoeken ICT-beveiligingsstandaarden valt te denken aan alles wat betrekking heeft op de beheersing en technische inrichting van informatiebeveiliging (preventie, detectie, repressie en correctie). Ook de aspecten waar informatiebeveiliging de business raakt, zoals business continuïteit, worden meegenomen in het onderzoek. Buiten de scope vallen de standaarden die geen enkele ICT-component bevatten, denk bijvoorbeeld aan fysieke beveiligingsstandaarden en personeelsbeveiligingsvoorschriften.

1.5 Proces uitgevoerde opdracht

De constatering van de huidige fragmentatie (zie H2 voor toelichting) heeft ervoor gezorgd dat binnen het onderzoek meer aandacht is gekomen voor het vaststellen van onderwerpen waar de ICT-beveiligingsstandaarden een bijdrage aan zouden moeten leveren.

Vanuit de die gedachte zijn de volgende stappen zijn doorlopen:

1. Deskresearch naar beleidsdoelen en nieuwe ontwikkelingen zoals geformuleerd door een aantal belangrijke actoren binnen de Nederlandse overheid. Bestudeerd zijn het Forum Standaardisatie, de Nationale Cybersecurity Strategie 2014 en het Digiprogramma van de Digicommissaris. Zie bijlage B voor de uitwerking hiervan.
2. Doorlopen van een workshop om beleidsdoelen, ICT beveiligingsstandaarden en vervolgacties aan elkaar te relateren.
3. Analyse en advies omtrent vervolgacties.
4. Terugkoppeling van analyse en advies met deelnemers workshop en overige respondenten.
5. Bespreking met stuurgroepleden.

In bijlage C is meer toelichting bij de processtappen gegeven.

1.6 Leeswijzer

Hoofdstuk 2 geeft op een hoog niveau overzicht van de conclusies over de stand van zaken rondom informatiebeveiliging en de positie van ICT-beveiligingsstandaarden daarbinnen. Daarbij worden twee gebieden geïdentificeerd waarop verbetering noodzakelijk is: a) De governance op ICT-beveiligingsstandaarden alsmede het structureren en harmoniseren van de onderliggende ICT-beveiligingsstandaarden en b) de actuele inhoudelijke taakgebieden waarvoor aandacht nodig is in het algemeen en in relatie tot ICT-beveiligingsstandaarden in het bijzonder. In hoofdstukken 3 en 4 worden deze twee gebieden verder uitgediept en worden aanbevelingen geformuleerd. Tezamen vormen deze aanbevelingen de strategie voor de Nederlandse overheid.

2 ONDERSCHEID: GOVERNANCE EN TAAKGEBIEDEN

Dit hoofdstuk geeft een overzicht van de conclusies over de stand van zaken rondom informatiebeveiliging en de positie van ICT-beveiligingsstandaarden daarbinnen. Zowel deskresearch, de workshop met experts evenals de aanvullende interviews hebben laten zien dat de analyse en aanbevelingen zich naar twee indelingen vertalen. Enerzijds het vraagstuk van governance met de gevolgen voor ICT-beveiligingsstandaarden en anderzijds de noodzaak om een aantal inhoudelijke taakgebieden als kapstok in te zetten ten behoeve van ICT-beveiligingsstandaarden. In onderstaande paragrafen is kort uitgewerkt wat hieraan ten grondslag ligt. In hoofdstuk 3 (Governance) en hoofdstuk 4 (Inhoudelijke taakgebieden) wordt verder ingegaan op deze vraagstukken.

2.1 Governance

De afgelopen periode is de aandacht voor informatiebeveiliging, mede door grote incidenten (zoals de Diginotar-affaire), enorm toegenomen. Standaarden (waaronder normen, richtlijnen en kaders) worden gezien als een belangrijk middel om informatiebeveiliging op voldoende niveau te krijgen, met name ook waar informatie-uitwisseling tussen organisaties en met burgers plaatsvindt. De laatste jaren zijn veel ICT-beveiligingsstandaarden ontwikkeld of voorgeschreven binnen de Nederlandse overheid. De aandacht voor en de inzet op standaarden is positief. De overheid hanteert standaarden meer dan ooit als referentiepunt en meetlat voor informatiebeveiliging. Tegelijkertijd is er een ‘woud’ met ICT-beveiligingsstandaarden ontstaan.

Overheidsorganisaties, de ‘ontvangers’, worden geconfronteerd met diverse actoren die ICT-beveiligingsstandaarden (waaronder normen, richtlijnen en kaders) opstellen of voorschrijven, de ‘afzenders’. Het opstellen en voorschrijven van standaarden zou meer gericht moeten worden op de ‘ontvangers’, de IT-organisaties die er iets mee moeten. Nu worden standaarden vooral geschreven vanuit het perspectief van de ‘afzender’ en diens beleidsmatige invalshoek of wettelijke taak. Omdat er verschillende ‘afzenders’ zijn, worden standaarden opgesteld en voorgeschreven die elkaar geregeld overlappen of tegenspreken. Harmonisatie en coördinatie zijn derhalve belangrijke aandachtspunten en daarmee is governance op ICT-beveiligingsstandaarden een belangrijk verbeterpunt.

De VIR en Baselines Informatiebeveiliging zijn in het verleden belangrijke stappen geweest, maar vervolgstappen zijn nuttig en nodig. Strakkere aansturing en eenvormigere verantwoording zijn daarbij de belangrijkste ingrediënten. De structuur van standaarden die wordt opgelegd aan overheidsorganisaties is een belangrijk aandachtspunt. Alle spelers onderkennen het probleem dat het voor overheidsorganisaties een ‘zoekplaatje’ is:

- Aan welke eisen moet nu precies worden voldaan?
- Hoe hard is de verplichting of aanbeveling om aan een bepaalde standaard te voldoen?
- Welke ICT-beveiligingsstandaarden zijn nu precies van toepassing voor een bepaald systeem?

Aanbevelingen om dit punt te verbeteren zijn opgenomen in hoofdstuk 3.

2.2 Taakgebieden

ICT-beveiligingsstandaarden worden nu op advies van Forum Standaardisatie door het Nationaal Beraad op de lijsten met open standaarden gezet. Het gaat om standaarden die een waardevolle bijdrage leveren aan de informatiebeveiliging. In de toetsingsprocedure van Forum Standaardisatie wordt ook getoetst of de standaard voldoende toegevoegde waarde biedt.

Aan de andere kant zijn de standaarden vrijwel nooit opgesteld vanuit het perspectief van de 'moeter' maar vanuit het perspectief van de op zichzelf staande standaard. Het resultaat is dan ook dat een standaard vaak over een onderwerp met een relatief kleine scope gaat. Denk aan standaarden als een cryptografisch algoritme (AES, SHA-2) of een algemeen protocol als TLS voor veilige verbindingen. Deze standaarden verkrijgen echter pas betekenis in de context van hun concrete toepassing. Als we de 'moeter' meer willen bedienen, is het zinvol om standaarden uit te vaardigen voor concrete toepassingen of taken waarin dit soort basisstandaarden een plek hebben gekregen, we stellen voor dit te doen in de vorm van actuele inhoudelijke taakgebieden.

Zo'n taakgebied betreft dan een concrete taak of samenhangende verzameling van taken, waarvoor richtlijnen voor goede informatiebeveiliging zijn op te stellen. Een taakgebied dient zo te worden gekozen dat het voor een organisatie logisch bij elkaar horende zaken betreft. Dat taakgebied vormt de context voor de toepassing van een onderliggende standaard, maar vormt tegelijkertijd het onderwerp waarvoor een richtlijn met een duidelijk herkenbare status beschikbaar komt. De relatie tussen taakgebied en richtlijn is dus één op één.

In hoofdstuk 4 hebben we een aantal inhoudelijke taakgebieden beschreven die vragen om coherent ingevuld te worden met ICT-beveiligingsstandaarden.

3 GOVERNANCE

In dit hoofdstuk is de governance van informatiebeveiliging bij de overheid toegelicht. Ten slotte worden aanbevelingen gedaan om de governance te verbeteren. Daarbij wordt specifiek gekeken naar de rol en het gebruik van ICT-beveiligingsstandaarden en de daarbij benodigde harmonisatie en coördinatie. In paragraaf 3.1-3.6 is de huidige situatie beschreven, in paragraaf 3.7 worden aanbevelingen gedaan.

3.1 Beveiligingsstandaarden van diverse 'afzenders'

We zien dat standaarden (incl. normen, richtlijnen en kaders) aan de informatiebeveiliging vanuit diverse plaatsen in de Nederlandse overheid afkomstig zijn. Zonder daarin volledig te willen zijn – er zijn namelijk ook nog allerhande sectorale eisen en afspraken – volgt hieronder een overzicht.

Bron van eisen	Actor	Toelichting
Wet Bescherming Persoonsgegevens	Min VenJ	Privacy vraagt passende beveiligingsmaatregelen (art. 13)
Richtsnoeren zoals voor 'Beveiliging persoonsgegevens'	Autoriteit Persoonsgegevens	Idem
Voorschrift Informatiebeveiliging Rijk (ook voor 'bijzondere informatie')	Min BZK	Verplichting tot risicoanalyse en managementsysteem
Baseline Informatiebeveiliging Rijk	Min BZK	Beveiligingsmaatregelen voor de Rijksoverheid
Baselines Informatiebeveiliging Gemeenten, Provincies en Waterschappen	IBD (KING en VNG), IPO, UvW	Beveiligingsmaatregelen voor lokale overheid
Richtlijnen voor o.a. webapplicaties en mobiele applicaties	NCSC	Concrete richtlijnen voor de praktische beveiliging
NORA (Katern Beveiliging)	Min BZK	Principes en ontwerppatronen voor goede informatiebeveiliging
DigiD-norm voor beveiligingsassessments	Logius	Veiligheid gekoppelde websites
Eisen toegang DigiPoort	Logius	Certificatengebruik, veilige communicatie en authenticatie
Afspraken vitale sectoren	NCSC	

Bron van eisen	Actor	Toelichting
Grip op Secure Software Development	CIP	O.a. Security Requirements for Application Software
ICT-beveiligingsstandaarden	Forum Standaardisatie en Nationaal Beraad	'pas toe of leg uit' voor o.a. DNSSEC, DKIM+SPF+DMARC, TLS, Digikoppeling, ISO27001/27002

De verschillende invalshoeken in de bovengenoemde bronnen, voortkomend uit het doel van de bijbehorende actoren, leiden in de praktijk tot een aanzienlijke overlap van de eisen die worden geformuleerd. De eindgebruikersorganisaties dienen deze eisen te interpreteren en uit te voeren en helaas ook niet zelden witte vlekken in te kleuren en inconsistenties op te lossen.

3.2 Perspectief vanuit de individuele overheidsorganisaties ('ontvangers')

Er is een uitgebreid palet aan ICT-beveiligingsstandaarden. Lang niet allemaal zijn ze echter relevant. Enerzijds wordt de relevantie begrensd door het toepassingsgebied. Anderzijds kan het zo zijn dat een standaard onvoldoende volwassen of geaccepteerd is.

De beheersing van informatiebeveiliging blijkt voor veel organisaties ook lastig. Dit begint al met onduidelijkheid over de eisen die gesteld zijn aan de organisatie:

- Vaak begint dit al bij de toepasselijkheid van wettelijk gestelde voorschriften, maar op dit punt zullen we niet nader ingaan;
- Welke brondocumenten met eisen überhaupt in scope zouden moeten zijn voor de organisatie is niet altijd bekend;
- Wat de status is van die brondocumenten waarin eisen zijn gesteld, is vaak niet helder (wat is verplicht, wat niet, wat is open voor interpretatie);
- De mate waarin bepaalde normen c.q. normelementen van toepassing zijn, is vaak niet duidelijk en lijkt deels ook willekeurig door de organisatie te kunnen worden bepaald;
- De wijze waarop die normelementen zijn te interpreteren is veelal niet eenduidig.

Dit maakt derhalve dat de norm niet zo helder is en dat een organisatie snel in de veronderstelling zou kunnen komen, dat men er een geheel eigenstandige invulling aan kan geven.

Het tweede punt is de interne beheersing zelf, waarop wij hier niet nader zullen ingaan. Welke maatregelen zijn uitgevoerd, werkt de implementatie en is het samenstel van maatregelen effectief. Dit gaat vooral over het organiseren van het management systeem, hetgeen we hier niet willen behandelen.

Ten slotte is er de verantwoording over de informatiebeveiliging. Daarbij is het in het algemeen geheel niet helder aan wie er op welke wijze verantwoording dient te worden afgelegd. Hier is geen standaard voor.

De betrekkelijke willekeur die lijkt te bestaan zowel voor het stellen van eisen als voor het verantwoorden over de beveiliging, leidt tot verschillende en letterlijk onvergelijkbare niveaus van beheersing van informatiebeveiliging. Dit is evident een stevige drempel voor de effectieve samenwerking tussen organisaties.

Het zou organisaties enorm helpen als er in deze 'ballenbak' van verschillende bronnen duidelijk zou worden:

- Wat is de status van een bepaald brondocument?
  Is het verplicht, vrijwillig, of iets er tussenin en zo ja, wat dan?
- Wat is de wijze waarop genoemde bronnen dienen te worden gehanteerd?
- Op welke wijze dient verantwoording aan wie te worden afgelegd over de verschillende bronnen?

Nu zijn er binnen de overheid verschillende partijen die orde pogen te scheppen in de diversiteit aan ICT-beveiligingsstandaarden. Ze geven advies over het gebruik van standaarden en stellen deze in sommige gevallen verplicht. Bovendien is er in sommige gevallen toezicht op de toepassing. Dit maakt het voor overheden duidelijk welke standaarden ze wanneer moeten toepassen. Toch is het nog steeds zo dat de gemiddelde overheidsorganisatie met een grote hoeveelheid ICT-beveiligingsstandaarden te maken heeft.

3.2.1 Voorbeeld: een nieuwe website

We schetsen in dit geval een voorbeeld om de situatie uit te leggen waarover we het hebben. Dit geeft een indruk, maar is niet een uitputtend voorbeeld. Zo zijn er meerdere voorbeelden te benoemen die wij voor deze situatieschets niet aan bod laten komen. Stel een Rijksoverheidsorganisatie wil een nieuwe website. Deze organisatie heeft in ieder geval te maken met een divers palet van ICT-beveiligingsstandaarden van verschillende afzenders en met uiteenlopende status. De onderstaande tabel is een uitwerking van deze casus.

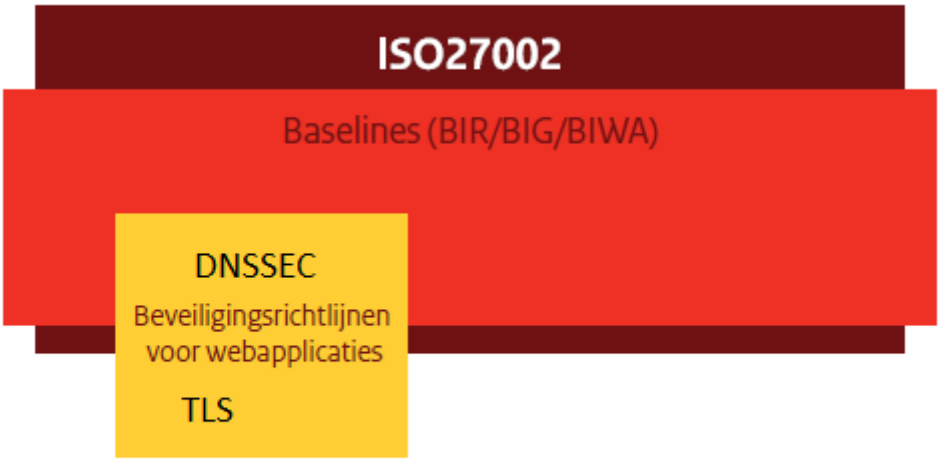
Standaard	Afzender	Status
Voorschriften Informatiebeveiliging Rijksdienst (VIR2007 en VIR-BI 2013)	BZK	Thans verplicht door Ministerraadbesluit voor Rijksdienst. In de toekomst verplichting via Wet GDI.
Baseline informatiebeveiliging (zoals BIR)	BZK, VNG, IPO, UvW	Verplichtende zelfregulering. Geborgd door interbestuurlijke afspraken.
Norm ICT-beveiligingsassessments DigiD (gebaseerd op oude versie ICT-beveiligingsrichtlijnen voor webapplicaties (2012))	Logius	Verplicht bij aansluiting op DigiD
ICT-beveiligingsrichtlijnen voor	NCSC	Advies

Standaard	Afzender	Status
webapplicaties (2015)		
Richtsnoeren en adviezen	Autoriteit Persoonsgegevens	Varieert
PIA	AP	Thans verplicht door toezichthouder (AP). In de toekomst verplicht in verband met EU Privacy Verordening
Beveiligingsstandaarden ISO27001&2, DNSSEC, TLS, SAML	Forum Standaardisatie	Pas toe of leg uit, soms aanvullende regelgeving zoals 'Besluit elektronische dienstverlening burgerlijke stand' en 'Regeling voorzieningen GDI'
PKIoverheid-certificaten	Logius	Verplicht gebruik bij een aantal generieke voorzieningen zoals Digipoort, eHerkenning etc.
Informatiebeveiligingsprincipes uit NORA en MARIJ		Advies
Secure Software Development Grip op SSD, Eisen aan Informatieveilige Applicaties	CIP	Advies

Sommige van deze standaarden en richtlijnen zijn complementair. Maar er bestaat ook overlap en in bepaalde gevallen zelfs tegenstrijdigheid.[3]

Een vereenvoudigde illustratie van deze problematiek is de onderstaande figuur. Uiteraard is ook voor de te bouwen website de ISO 27002 van toepassing. Meer specifiek en voor een groot deel overlappend zijn vervolgens de Baselines. Dan zijn daar de NCSC Beveiligingsrichtlijnen voor webapplicaties. Die geven deels een nadere invulling van het gestelde in de ISO 27002 en de Baselines Informatiebeveiliging, maar voor een groot deel bestaat dit uit vele inhoudelijk geformuleerde eisen. De status van deze richtlijnen is echter onduidelijk, het is formeel een aanbeveling, maar wel één met grote bekendheid en gezag. Binnen de verdere technische invulling ten slotte, vinden we individuele ICT- beveiligingsstandaarden die gebruikt worden om bepaalde aspecten van het webverkeer te beveiligen. Denk dan aan TLS en DNSSEC.

[3] Zo is de 'Norm ICT-beveiligingsassessments DigiD' bijvoorbeeld nog gebaseerd op de vorige versie van de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van NCSC. En zo staat er in de Operationele Handreiking Informatiebeveiliging dat de encryptiestandaard AES toegepast moet worden met twee verschillende minimale sleutellengtes, namelijk van 128 en 256 bits.



Figuur 1. Positionering Richtlijnen ten opzichte van ISO27000x en overheidsbaselines

3.2.2 Andere taakgebieden

Maar overheidsorganisaties hebben in de veilige inrichting en het veilige beheer van hun eigen IT, hun applicaties en hun digitale dienstverlening vele uitdagingen. Een greep uit de taakgebieden en bijbehorende vragen die veel overheidsorganisatie hebben:

- Hoe koop ik producten in die in de basis veilig zijn?
- Hoe configureer ik die producten veilig, zodat zij ook van de juiste standaarden gebruik maken?
- Hoe beheer ik die producten ook zodanig dat ze veilig blijven?
- Hoe richt ik standaard kantoorautomatisering met diensten als email, bestandstransport en dergelijke goed in?
- Hoe ga ik om met fenomenen als Bring Your Own en consumerization of IT?
- Hoe ga ik om met outsourcing en cloud?
- Hoe bouw ik veilige business applicaties?

Voor sommige van deze taken zijn richtlijnen beschikbaar, maar voor andere weer niet. Al met al is het voor een overheidsorganisatie en de daarin aanwezige projectleiders een zoekplaatje om te bepalen welke ICT-beveiligingsstandaarden van toepassing zijn en welke status die hebben (verplicht, aanbevolen, nice-to-have).

Doordat het zo'n zoekplaatje is en de naleving niet extern wordt getoetst, bepalen veel organisaties zelf welke ICT-beveiligingsstandaarden en richtlijnen zij van toepassing vinden. Feitelijk bestaan er daardoor grote verschillen in de gerealiseerde beveiliging.
Als er op deze oorzaken geen verbetering optreedt (minder een zoekplaatje en grotere transparantie) dan zullen grote verschillen tussen individuele overheidsorganisaties in stand blijven. Met alle gevolgen van dien: daadwerkelijk risico's ('de keten is zo sterk als de zwakste schakel') en gering onderling vertrouwen.

3.3 Ketenperspectief

De voorafgaande paragraaf ging met name in op het perspectief van de individuele organisatie die aan de verschillende eisen invulling dient te geven voor de verschillende taakgebieden. In de samenwerking met andere organisaties is het echter ook van belang om inzicht te hebben in hoe andere organisaties hun informatiebeveiliging invullen. Enerzijds is daarvoor de eenduidige verantwoording noodzakelijk zoals eerder genoemd. Anderzijds, is ook standaardisatie van de baselines en bijbehorende richtlijnen en standaarden hiervoor noodzakelijk. Doet men dit niet dan is men de facto verplicht om voor elke keten of elk samenwerkingsverband een eigen systematiek van stellen van eisen en controleren op de aanlevering door te voeren. In dit verband is de ontwikkeling van een Baseline Informatiebeveiliging Overheid (BIO) alsmede het ontwikkelen van een eenduidige standaard voor verantwoording (rol project ENSIA) van groot belang. In het verlengde hiervan geldt dat ook voor de onderliggende richtlijnen en standaarden.

3.4 ICT-beveiligingsstandaarden: een versnipperd plaatje

We zien dat het onderwerp ICT-beveiligingsstandaarden een zeer gefragmenteerd beeld geeft. De ICT-beveiligingsstandaarden worden op allerlei gebieden gezien en vele doorsnijdingen zijn mogelijk. De eerdere WODC studie van Innovalor[4] toont dit ook aan. Er is niet één indeling voor standaarden te maken voor alle doeleinden. Bovendien worden er vanuit verschillende verantwoordelijkheden eisen gesteld aan organisaties: de wetgever, de toezichthouders, de sector en de ketens waarin men betrokken is. Standaarden zijn er bovendien in alle soorten en maten:

- Van meer ICT-technisch naar meer organisatorisch;
- Van ‘klein’ (bijvoorbeeld betrekking hebbend op een specifieke maatregel zoals een cryptografisch algoritme) tot ‘groot’ (bijvoorbeeld een norm voor de gehele informatiebeveiliging in een organisatie).
- Van best practice tot dwingend voorschrijvend.

Niet één advies kan helpen een eenvoudig overzichtelijk plaatje te maken van een wereld die zo complex is. Wel kunnen we ‘in overheidsland’ beter aansluiten bij de belevingswereld van de verschillende overheidsactoren. Zodat een overheidsorganisatie beter weet waar die zich aan te houden heeft. Zodat een overheidsorganisatie ook eenvoudig kan nagaan hoe een andere overheidsorganisatie zijn zaken op informatiebeveiligingsgebied geregeld heeft. Zodat duidelijk is voor gangbare zaken waar men zich aan te houden heeft als het gaat om informatiebeveiliging, privacy en datalekken.

[4] https://www.wodc.nl/onderzoeksdatabase/2552-inventarisatie-van-standaarden-en-normen-voor-cyber-security.aspx?nav=ra&l=veiligheid_en_preventie&l=veiligheid

3.5 Gebrekkige controle en verantwoording

De governance op informatiebeveiliging is tot op heden nog vrij informeel en onvolledig:

- Tot op heden is vooral gewerkt met VIR en de verschillende Baselines Informatiebeveiliging. De controle op de naleving is vooral gebaseerd op collegiale toetsing.
- Aan de basis van VIR en Baselines Informatiebeveiliging ligt de invoering van een management systeem (ISMS). Hoewel daarbij wordt gerefereerd aan ISO 27001 en ISO 27002, wordt er geen externe certificering verplicht gesteld.
- Voor 'pas toe of leg uit'-standaarden geldt wel een verantwoording bij afwijken, alhoewel ook hier niet op de naleving wordt toegezien.
- Alleen voor de DigiD-norm voor beveiligingsassessments vindt een verplichte audit plaats.

Het risico in de huidige situatie bestaat dat de eisen verder worden geformaliseerd en zelfs wettelijk worden afgedwongen maar dat de toetsing op de naleving nog steeds informeel blijft. De kans is dan aanzienlijk dat organisaties zich gedwongen voelen om een te rooskleurig beeld te schetsen van de feitelijke situatie. Beter kan uit worden gegaan van een groeiscenario, waarbij er middels onafhankelijke externe toetsing een objectief beeld wordt verkregen. Hierin kan het project ENSIA (Eenduidige Normering Single Information Audit) een rol spelen. Er dient daarnaast een cultuur te ontstaan waarin het acceptabel is om een slecht rapportcijfer te krijgen en vervolgens de ruimte te krijgen om dat te verbeteren. Vergelijk dit met het verhogen van de transparantie in de zorg, waar bijvoorbeeld het publiceren van sterftecijfers in ziekenhuizen aanvankelijk op grote weerstand stuitte. Uiteindelijk leidt deze transparantie echter wel tot de gewenste verbeteracties op de plaatsen waar dat nodig is.

Het gebrek aan transparantie leidt er eveneens toe dat voor ketenpartners niet helder is waar ze aan toe zijn en hoe de ketenpartner in kwestie de informatiebeveiliging heeft geregeld. In de huidige situatie zullen ketens dan eigen standaarden en ketengovernance gaan inrichten om toch maar de beveiliging te kunnen borgen (denk bijvoorbeeld aan Suwinet). Dit is niet per se verkeerd, maar voor elke keten moet het wiel opnieuw worden uitgevonden.

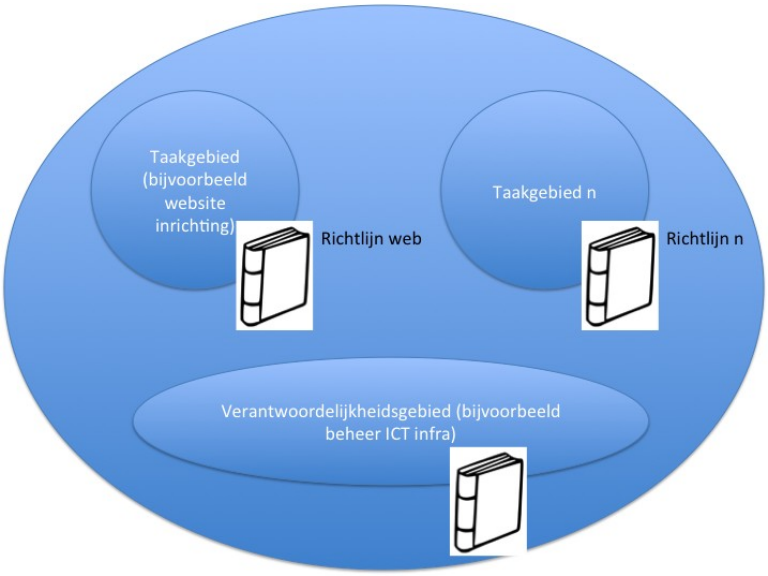
3.6 Versnippering voorkomen vraagt om inhoudelijke coördinatie

Zoals hierboven gesteld, is het gewenst om vanuit het standpunt van de 'ontvanger', meer eenheid te bereiken en versnippering weg te nemen. Dit is één specifieke aanbeveling die we hier uitwerken.

Dat kan door een volgende structurering door te voeren:

1. Maak een standaard indeling van taakgebieden, verantwoordelijkheidsgebieden en overkoepelende kennisgebieden (zoals cryptografie) in een overheidsorganisatie.
2. Een taakgebied is bijvoorbeeld 'het maken van een website'. Voor een dergelijk taakgebied worden richtlijnen opgesteld.
3. Per richtlijn dient een taak of verantwoordelijkheidsgebied integraal te worden behandeld. In een richtlijn kunnen normatieve referenties naar standaarden worden opgenomen. De richtlijnen gezamenlijk zouden het totale werkterrein van een overheidsorganisatie dienen af te dekken. Punten 1 t/m 3 zijn als volgt schematisch weer

te geven. Verplicht standaarden in samenhang. Maak individuele ICT-beveiligingsstandaarden steeds deel van de richtlijnen, zoals hieronder benoemd.



4. Ondersteun het bovenstaande met een samenhangend logisch bouwwerk van normelementen / eisen per object en realiseer hiervoor ICT-tooling om dit bouwwerk op te stellen, te gebruiken en te onderhouden.
5. Er is één coördinerende partij die bepaalt wat de indeling van taakgebieden en verantwoordelijkheidsgebieden is en wie daar richtlijnen voor opstelt. (Dit punt komt ook terug in de overkoepelende aanbevelingen in paragraaf 3.7)
6. Het is ook deze partij die ervoor zorg draagt dat de richtlijnen worden opgesteld in overeenstemming met de scope van het taakgebied of verantwoordelijkheidsgebied, om ongewenste witte vlekken of overlap te vermijden.
7. Omdat er ook samenhang is met bijvoorbeeld overkoepelende kennisgebieden als cryptografie, moet de coördinerende partij ook de consistentie tussen richtlijnen bewaken.
8. Er is één nationale governance, waarbinnen de besluitvorming over richtlijnen (wat is hun status) plaatsvindt. Het ligt voor de hand om hierbij aansluiting te zoeken op de reeds bestaande governance op standaarden. Verbinding met de huidige governance op baselines dient hiervoor wel te worden georganiseerd. (Dit punt komt ook terug in de overkoepelende aanbevelingen in paragraaf 3.7).

Consequenties hiervan zijn ondermeer:

1. Eén consequentie hiervan is dat de baselines ook veelvuldig zullen refereren (normatieve referenties) aan dergelijke richtlijnen in plaats van zelf die onderwerpen inhoudelijk te behandelen. Dit heeft als aanvullend voordeel dat inconsistentie tussen de baseline en specifieke richtlijnen verdwijnt (inconsistentie tussen verschillende richtlijnen blijft echter een belangrijk aandachtspunt).

2. Inkoop en sourcing zijn in dit model te behandelen als een taakgebied en hiervoor is een richtlijn op te stellen.
3. Samenwerking met semi-publieke of private instanties krijgt vorm in ketens. Ketens zijn een bijzondere vorm van een verantwoordelijkheidsgebied, waarin meerdere taakgebieden ondergebracht kunnen zijn. Op die wijze worden de eisen die in ketens worden gesteld, voor het grootste deel opgebouwd uit gestandaardiseerde bouwblokken.

3.7 Aanbevelingen

Op basis van het voorgaande beeld formuleren wij de volgende aanbevelingen om de governance te verbeteren:

1. Neem een 'haakje' op in de wet GDI voor overheidsbrede eisen voor informatiebeveiliging.
2. Dwing goede beheersing van informatiebeveiliging af. Groei verder vanaf het huidige model van collegiale toetsing naar formele toetsing. Het uiteindelijke doel zou externe certificatie tegen de ISO 27001 kunnen zijn. Ongetwijfeld zal naar dit streven stapsgewijs toegegroeid kunnen worden. Het is bijvoorbeeld denkbaar om het goede voorbeeld te geven met de GDI-voorzieningen.
3. Harmoniseer bestaande baselines (BIR, WIG, IBI, BIWA) tot een Baseline Informatiebeveiliging Overheid (BIO). We adviseren de Baseline Informatiebeveiliging Overheid met hoge prioriteit af te ronden. Dit maakt eenvoudigere samenwerking tussen organisaties mogelijk in het kader van ketens en netwerken (uniformiteit en transparantie).
   Laat deze BIO voor concrete taakgebieden zoveel mogelijk verwijzen naar richtlijnen, zodat ook de status van die richtlijnen (verplicht, aanbevolen, nice-to-have) duidelijk wordt.
4. Hanteer het instrument van de wettelijke verplichting vaker en laat de auditor ook op genoemde wettelijke verplichtingen controleren, met name als het gaat om die technische standaarden die goed zijn op te volgen zonder al te grote externe afhankelijkheden (denk bijvoorbeeld aan TLS, DNSSEC, een veilig mailprofiel).[5]
5. Vergroot de transparantie hoe overheidsorganisaties het doen op het gebied van informatiebeveiliging. Doe dit door:
   - enerzijds door te werken aan een uniforme standaard voor verantwoording (rol project ENSIA) en

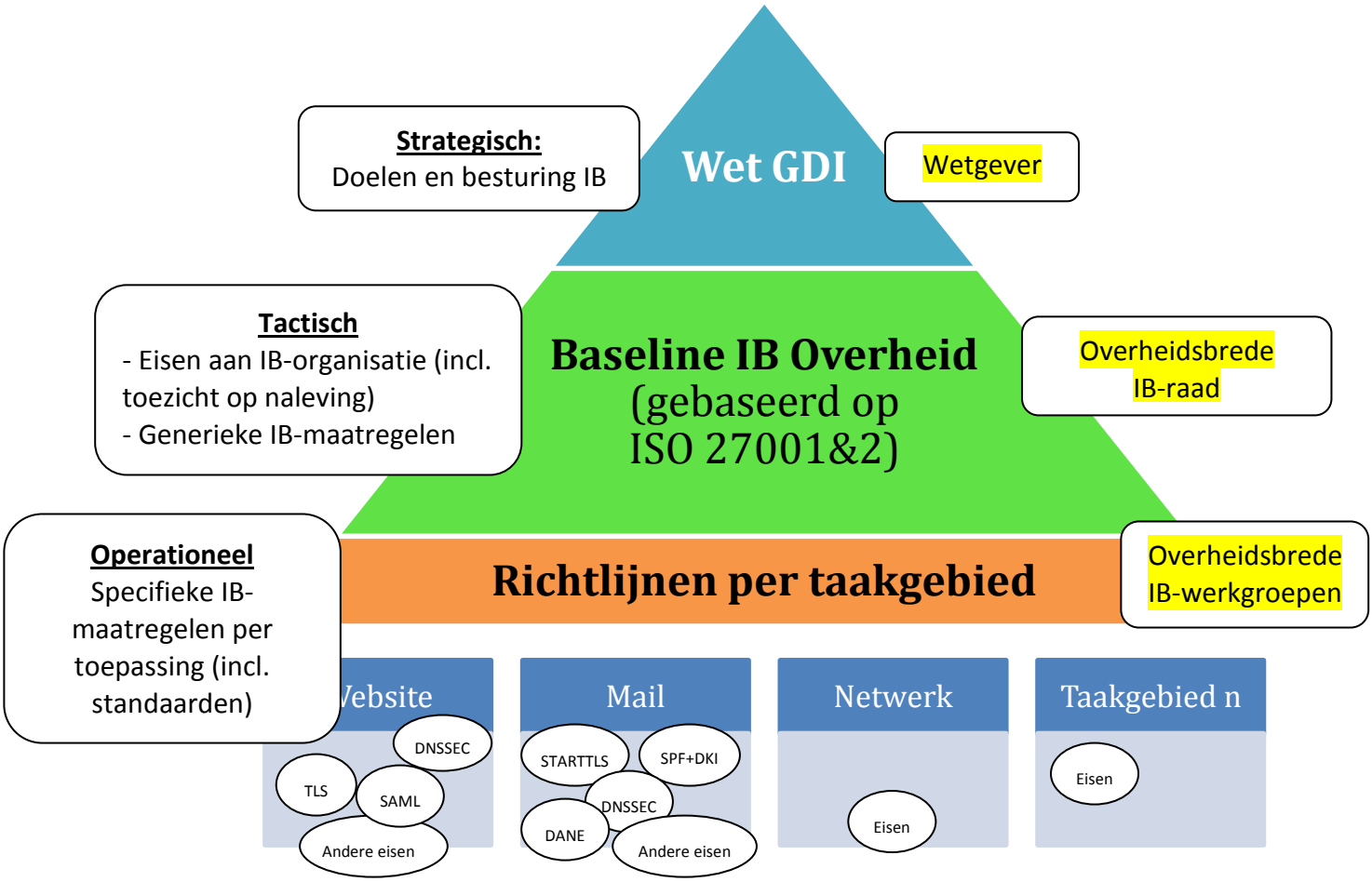
[5] Sommige ICT-beveiligingsstandaarden zijn door een enkele organisatie op eigen initiatief zijn na te leven. Wij stellen voor de algemeen toepasselijke standaarden ook wettelijk te verplichten, bijvoorbeeld in de Wet GDI. Op te nemen zaken kunnen bijvoorbeeld HTTS-only, TLS 1.2 en DNSSEC zijn. Dit instrument wordt nog maar weinig gebruikt (bijvoorbeeld wel bij de toegang tot elektronische dienstverlening van de Burgerlijke Stand), maar kan slepende discussies met organisaties in de groep 'achterblijvers' of 'late majority' eenvoudig beslechten.

- anderzijds door de technische beveiliging van Internet-facing systemen testbaar te maken volgens de aanpak van www.internet.nl (Platform Internet Standaarden). Het hangt in dit geval af van de sturing op de cultuurverandering die nodig is.

Daarnaast doen we de volgende aanbevelingen om tot een betere structurering van standaarden te komen:

1. Structureer en cluster de individuele normen en standaarden in richtlijnen voor duidelijk omschreven taakgebieden, met als doel om het voor de individuele overheidsorganisatie minder een zoekplaatje te maken en om onduidelijkheid weg te nemen over welke normen en standaarden toe te passen in bepaalde situaties. Hiervoor kunnen de stappen gezet worden zoals aangeduid in paragraaf 3.6.
2. Maak één van de actoren die informatiebeveiliging in de Nederlandse overheid besturen, verantwoordelijk voor een dergelijke structurering en harmonisatie. Uiteraard hoort hier een passend mandaat bij, zodat standaarden ook verplicht opgelegd kunnen worden aan partijen en de status van standaarden bepaald kan worden et cetera.
3. Bestuur al deze activiteiten in één nationale governance, waarbinnen de besluitvorming over richtlijnen (wat is hun status) plaatsvindt. Het ligt voor de hand om hierbij aansluiting te zoeken op de reeds bestaande governance op standaarden.

Ter illustratie van de relatie tussen de verschillende niveaus zie onderstaande figuur:



Ter toelichting het volgende:

- Het hoogste niveau, het strategische niveau, wordt gevormd door de Wet Generieke Digitale Infrastructuur. Hierin komt de verplichting om een goede informatiebeveiliging in te richten en te onderhouden. Ook wordt hierin duidelijk hoe de governance hierop wordt geregeld, waarbij de hoge mate van vrijblijvendheid en collegiale sturing door een dwingender kader wordt vervangen.
- Het tactische kader is feitelijk de plaats waar de normen worden gesteld in algemene zin. Nemen we het voorbeeld van beveiliging van een lokaal netwerk, dan zou hier als norm kunnen worden opgenomen dat het LAN zodanig dient te worden beveiligd, dat bekend is welke lokale gebruikers er op actief zijn. Verder wordt er verwezen naar een ‘Richting LAN-beveiliging’, aannemende dat die er is. Aangegeven wordt of die richtlijn verplicht gevolgd dient te worden of niet. In de BIO worden dus nadrukkelijk niet alle normelementen voor de beveiliging van lokale netwerken opgenomen.
- In de ‘Richtlijn LAN-beveiliging’ worden wel alle normelementen voor de veilige inrichting van een LAN opgenomen en dit gaat uiteraard ook verder dan sec het benoemen van standaarden. Hierbij is duidelijk wat verplicht is, wat aanbevolen en wat ‘nice-to-have’ is.

Eén van de zaken die in deze richtlijn wordt genoemd, is bijvoorbeeld de IEEE 802.1x standaard, een standaard die port-based netwerktoegangscontrole regelt. Daarmee zijn apparaten die aan het lokale netwerken verbinden, geauthenticeerd.

4 INHOUDELIJKE (TAAK)GEBIEDEN

In het vorige hoofdstuk is aangegeven om minder vanuit standaarden en meer vanuit samenhangende taakgebieden te opereren. Voor de belangrijkste taakgebieden hebben wij in dit hoofdstuk een aantal adviezen geformuleerd. De keuzes die hierin zijn gemaakt komen voort uit deskresearch, een workshop met experts en aanvullende interviews.

4.1 Taakgebieden en externe ontwikkelingen

De inhoudelijke taakgebieden berusten op het globale beeld van externe ontwikkelingen. Op basis van deskresearch, workshop en aanvullende adviezen, gaat het om de volgende taakgebieden:

1. eID en vertrouwensdiensten
2. Nieuwe kanalen voor elektronische dienstverlening
3. Veilige applicatieontwikkeling
4. Veilige e-mail
5. Privacy-by-design
6. Internet of Things
7. Cloud
8. Reageren op cyber threats

Op het gebied van **cybersecurity** zijn de volgende ontwikkelingen te herkennen:
De externe ontwikkelingen op cybersecurity gebied zijn als volgt te kenmerken:

- Toenemende kennis en kunde van aanvallers.
- Verschuiving naar cybercrime die door de georganiseerde misdaad of overheden wordt opgezet of aangejaagd.
- Grotere doelgerichtheid en vasthoudendheid van aanvallers.

Omdat perfecte preventie niet realistisch is vraagt het bovenstaande om:

- Betere en meer tijdige detectie van aanvallen of voorbereidingen van aanvallen (anomalie-detectie).
- Early warning netwerken.
- Betere uitwisseling van informatie tussen de ‘good guys’.

Op het gebied van **generieke digitale infrastructuur** zien we de volgende ontwikkelingen:

- Het frequenter gebruik van andere kanalen dan alleen de website voor dienstverlening. E-mail, instant messaging zoals Whatsapp en natuurlijk telefonische dienstverlening nemen in populariteit toe omdat veel mensen niet direct hun weg weten te vinden in de meestal formulier-georiënteerde elektronische dienstverlening en ook omdat deze middelen bij het grote publiek in populariteit toenemen.
- De digitalisering en striktere toepassing van privacyregels leidt tot een behoefte aan authenticatiemiddelen met een hoger betrouwbaarheidsniveau dan het huidige DigiD Midden. Daar komt bij dat de eIDAS verordening stringente eisen stelt aan de authenticatie om zo elektronische dienstverlening tussen lidstaten mogelijk te maken.

Op het gebied van de **baselines en managementsystemen** speelt het reeds onderkende streven naar harmonisatie tussen de verschillende baselines die binnen de Nederlandse overheid worden gehanteerd (BIR, BIG, IBI, BIWA) tot één generieke baseline (BIO, Baseline Informatiebeveiliging Overheid). Daarnaast zijn de huidige Baselines IB nog gebaseerd op de vorige versie van de ISO27001/2-normen.

Op het gebied van de **privacy** is de toepassing van privacy-by-design relevant.

Verder zien we dat de technische omgeving verandert, met meer gebruikmaking van **cloud**, de opkomst van het **Internet of Things** en trends als **bring your own** en het nog verder doordringen in onze omgeving van **mobile** en **wearable computing**. Evident allemaal ontwikkelingen waar een goede beveiliging nodig is.

4.2 Aanbevelingen per inhoudelijk taakgebied

Hieronder zijn de aanbevelingen per inhoudelijke taakgebied samengevat weergegeven. Per actie is tevens aangegeven in welke categorie deze valt, zie hieronder

Verken	Verken het speelveld om te analyseren wat er speelt en of er actie op het gebied van standaardisatie gewenst is en zo ja, welke
Participeer	Doe mee aan een bestaand standaardisatie-initiatief
Ontwikkel	Ontwikkel zelf een standaard, profiel of richtlijn
Stimuleer	Stimuleer bepaalde actoren tot het bijdragen aan standaardisatiewerk of het meer conformeren aan standaarden

Acties van deze typen dragen alle in hun aard per definitie bij aan standaardisatie en interoperabiliteit.

#	Taakgebied	Aanbevelingen	
1	eID en vertrouwensdienten	- Actieve participatie in ETSI ESI standaardisatie.	Participeer
		- In OASIS verband werken aan SAML profiel voor stelseltoepassingen.	Participeer
		- Ontwikkelen in Europees verband van alternatieven of gemeenschappelijke maatregelen ter versterking systeem van webcertificaten.	Ontwikkel
2	Nieuwe kanalen voor elektronische	- Ontwikkel standaarden en/of een infrastructuur voor veilige tweeweg end-to-	Ontwikkel

#	Taakgebied	Aanbevelingen	
	dienstverlening	end berichtenverkeer, al dan niet in aanvulling op de Berichtenbox. (Regieraad Interconnectiviteit)	
		- Ontwikkel richtlijnen voor veilige dienstverlening per telefoon.	Ontwikkel
		- Ontwikkel richtlijn voor veilige instant messaging diensten en hun gebruik in elektronische dienstverlening.	Ontwikkel
3	Veilige applicatieontwikkeling	- Adoptieonderzoek Secure Software Development.	Verken
		- Ontwikkel richtlijnen voor veilige mobiele applicaties (apps).	Ontwikkel
4	Veilig profiel voor email	- Ontwikkel een 'technisch' profiel (oftewel richtlijn) voor veilige e-mail.	Ontwikkel
		- Stel een invoeringsplan in en voer dat uit.	Stimuleer
5	Privacy-by-design	- Participeer in standaardisatie internet identity workshops (UMA) en eventuele andere standaardisatieinitiatieven. (Digicommissaris)	Participeer
		- De infrastructuur voor personal data stores ontwikkelen, zowel in te passen in eID stelsel als in Stelsel Basisregistraties.	Stimuleer
		- Verken beschikbare standaarden voor privacy.	Verken
6	Internet of Things	- Verkenning uitvoeren Internet of Things.	Verken
7	Cloud	- Verkenning uitvoeren Cloud.	Verken
8	Reageren op cyberthreats	- Actieve betrokkenheid bij standaarden voor early detection en uitwisselen van dreigingsinformatie, in het bijzonder TAXII, CybOX en STIX.	Participeer

Bovenstaande aanbevelingen zijn hieronder per taakgebied nader toegelicht.

4.2.1 eID en vertrouwensdiensten

Aanbevelingen

- Actieve participatie in ETSI ESI standaardisatie.
- In OASIS verband werken aan SAML profiel voor stelseltoepassingen.

- Ontwikkelen in Europees verband van alternatieven of gemeenschappelijke maatregelen ter versterking systeem van webcertificaten.

Toelichting

De rijksoverheid ontwikkelt een generieke digitale infrastructuur, waarop de Digicommissaris de regie voert. Het idee is dat de belangrijkste generieke functies in bouwblokken worden geïmplementeerd en dat deze verplicht gebruikt dienen te worden door alle overheden. Er zijn al veel bouwblokken geïmplementeerd, zoals DigiD, Digikoppeling, Digilevering, Berichtenbox etc.. Deze bouwblokken worden in het algemeen gebouwd met oog op de juiste ICT beveiliging. Het verplichte gebruik van deze bouwblokken in de toekomst zal dus helpen.

Een specifiek deel van de generieke digitale infrastructuur zijn de elektronische identiteiten en vertrouwensdiensten. In de loop van de jaren zijn hiervoor verschillende stelsels / voorzieningen gerealiseerd: PKIoverheid, DigiD en de eID Stelsels eHerkenning en Idensys, elk met hun eigen doelgroepen en functies.

We zien momenteel dat de regie hierop krachtig wordt gepakt. Er is echter de behoefte aan meer standaarden om de eID Stelsels die we in Nederland realiseren ook goed in te bedden in de (Internationale) ICT standaardisatie. Dit gebeurt echter in mindere mate.

Het risico van niet handelen is dat de oplossingen uiteindelijk matig in internationale standaarden passen. Hieronder analyseren we de verschillende gebieden waar inpassing in erkende standaard profielen van basisstandaarden als SAML van belang is:

- EU interoperabiliteit. Omdat de Nederlandse eID in de europese context is aangesloten op de eIDAS infrastructuur, zijn de risico's van technische interoperabiliteit minimaal.
- Implementatie-inspanning. Qua technische implementatie zien we dat het soort gebruik dat een eID Stelsel maakt van de SAML basisstandaard, niet met een set standaard profielen wordt ondersteund. Dit maakt de implementatie-inspanning mogelijk ongewenst hoog.
- EU verschillen in betrouwbaarheidsniveaus. Door verschillende interpretaties en verschillende kwaliteit in de uitvoering is wel degelijk enige ongelijkloop tussen EU-lidstaten aan de orde. Dit zou – ondanks de verplichte wederzijdse erkenning van eID's op de niveaus substantieel en hoog – kunnen leiden tot ongewenste drempels in het verlenen van diensten waarvoor wel verplicht toegang wordt verleend.

We maken in Nederland gebruik van vele standaarden voor eID diensten en vertrouwensdiensten. Voor de (PKI) vertrouwensdiensten is met name ETSI van belang. Maar normen voor PKI komen in de praktijk ook van de browserfabrikanten af. Browserfabrikanten stellen in overleg met CSP's normen vast in het CA / Browser Forum (CABF) (Logius participeert in CABF). In het PvE PKIoverheid worden deze normen aangehaald.
In de praktijk wordt er door Logius wel in het CABF geparticipeerd maar wordt er vanuit Nederland niet of nauwelijks in de standaardisatieactiviteiten van ETSI geparticipeerd. Dit terwijl hier wel voor Nederland relevante normen worden vastgesteld, die verwerkt zijn in het PvE van PKIoverheid.
We zien bijvoorbeeld nog steeds dat men onvoldoende doordrongen is van de noodzaak voor

betere technische preventieve beveiliging van de CA's, terwijl bijvoorbeeld het Diginotar-incident daar wel aanleiding toe vormt.

Een vergelijkbare situatie doet zich voor met betrekking tot SAML, die wordt gebruikt in DigiD en het stelsel Elektronische Toegangsdiensten (eHerkenning en Idensys). Hoewel de basisstandaard SAML de ruimte biedt voor steltoepassingen, is een meer gericht profiel op basis van SAML gewenst dat zich specifiek op deze stelseltoepassingen richt. Een gericht initiatief in de context van OASIS (de beheerorganisatie van SAML) zou hiervoor door Logius kunnen worden verkend. Logius is recent ook lid geworden van OASIS, zodat de stap hiervoor ook kleiner wordt.

Voorts is er veel te zeggen om in tenminste Europees verband te werken aan een alternatief voor c.q. versterking van het systeem van uitgifte van digitale certificaten. Het bestaande systeem is inherent zwak omdat het falen van een enkele CA grote, wereldwijde consequenties kan hebben. Dit probleem en de mogelijke lijnen waarlangs men een oplossing kan vinden, is beschreven in het ICA study group report over de beveiliging van web certificaten (zie www.ica-it.org). Maatregelen die de huidige situatie rondom webcertificaten versterken, zoals *certificate transparency,* helpen zeker, maar zijn ook geen panacee.

4.2.2 Nieuwe kanalen voor elektronische dienstverlening

Aanbevelingen

- Ontwikkel standaarden en/of een infrastructuur voor veilige tweeweg end-to-end berichtenverkeer, al dan niet in aanvulling op de Berichtenbox.
- Ontwikkel richtlijnen voor veilige dienstverlening per telefoon.
- Ontwikkel een richtlijn voor veilige instant messaging diensten en hun gebruik in elektronische dienstverlening.

Toelichting

De overheid gaat massaal digitaal. Meestal betekent dit dat het klantcontact verloopt via de website van de overheidsorganisatie. Daarna volgt er veelal een fase met één-op-één communicatie. Dit is vaak maar matig beveiligd. E-mail, telefoon, soms zelfs Whatsapp worden gebruikt om te communiceren.

Het is aan te bevelen om de noodzakelijke richtlijnen en standaarden te ontwikkelen waarmee digitale dienstverlening langs de nieuwe kanalen alsnog goed beveiligd kunnen worden, al dan niet in combinatie met activiteiten om generieke infrastructuur hiervoor te ontwikkelen. Deels kunnen standaarden en richtlijnen worden ontwikkeld, met als adressant de individuele overheidsorganisatie (zie taakgebied 3). Deels kan ook infrastructuur worden ontwikkeld hiervoor. Vooralsnog zien we dat een instant messaging infrastructuur nog niet voldoende prioriteit heeft voor opname in de generieke digitale infrastructuur en denken we dat richtlijnen voldoende zijn. Wel zou het zinvol zijn om een bruikbare betrouwbare tweewegcommunicatie met de burger mogelijk te maken. Denk in dat verband aan een uitbreiding van de Berichtenbox voor

tweewegcommunicatie met de burger of andere vormen om end-to-end berichten met de burger uit te kunnen wisselen (bijvoorbeeld via een app).
De Regieraad Interconnectiviteit zou hiertoe een opdracht kunnen verstrekken.
Daarnaast kan het Nationaal Beraad dan sturen op de adoptie van dergelijke richtlijnen.

4.2.3 Veilige applicatieontwikkeling

Aanbevelingen

- Adoptieonderzoek Secure Software Development
- Ontwikkel richtlijnen voor veilige mobiele applicaties (apps)

Toelichting

De behoefte is al lang aanwezig om toepassingen te ontwikkelen, die minder en minder ernstige beveiligingskwetsbaarheden bevatten. Concrete richtlijnen zoals de NCSC richtlijnen voor webapplicaties kunnen hierbij helpen, alsmede raamwerken zoals Secure Software Development. De voorgestelde acties zijn een adoptieonderzoek voor SSD en – indien akkoord bevonden voor opname op een van de lijsten van het Forum – ook een bijpassende kennisdisseminatie operatie. Tevens zien we een snelle opkomst van de mobiele telefoon en de tablet als platforms waarop elektronische dienstverlening wordt afgeleverd. We staan nu aan de vooravond van het omarmen van het app-kanaal voor deze mobiele platforms voor elektronische dienstverlening. Het is daarbij echter wel zaak om dergelijke app-ontwikkeling op een veilig manier te doen. Recente ontwikkelingen hebben aangetoond dat ook ontwikkeling in erkende kenniscentra binnen de overheid geen garanties biedt en kan leiden tot fundamenteel onveilige apps. De kunst is om de juiste partijen en de juiste kennis bij elkaar te brengen om een richtlijn voort te brengen waarin de juiste kennis is neergeslagen en waarbij de participanten gezamenlijk voor een afdoende draagvlak zorgdragen.

4.2.4 Veilig profiel voor email

Aanbevelingen

- Ontwikkel een profiel voor veilige e-mail.
- Stel een invoeringsplan in en voer dat uit.

Toelichting

Het belang van email staat buiten kijf. Initieel zat er veel inspanning op het end-to-end beveiligen van email met vercijfering en digitale handtekeningen (S/MIME, PGP). Het is echter lastig om email end-to-end te beveiligen omdat niet alle clients de benodigde cryptografie ondersteunen en omdat ook niet iedereen over de benodigde digitale certificaten beschikt.

Over de laatste jaren zijn er vele toevoegingen op mailprotocollen geweest om stapsgewijs mail steeds beter te beveiligen (SPF, DKIM, DMARC). Recent wordt ook DANE ingezet om email te beveiligen. Toegang tot postbussen kan het beste ook plaatsvinden over een TLS verbinding.
We bevelen aan om – in analogie met Duitsland – een profiel of richtlijn te ontwikkelen voor

veilige email. Bovendien dient de adoptie bij voorkeur verplicht te worden gesteld, met inachtname van een redelijke implementatieperiode.

4.2.5 Privacy-by-design

Aanbevelingen

- Participeer in standaardisatie UMA en eventuele andere standaardisatieinitiatieven
- De infrastructuur voor personal data stores ontwikkelen, zowel in te passen in eID stelsel als in Stelsel Basisregistraties.
- Verken beschikbare standaarden voor privacy.

Toelichting

Er is met de komst van de EU privacy verordening veel aandacht voor privacy-by-design. Privacy Impact Assessments zijn tevens inmiddels verplicht gesteld voor de rijksdienst.

We zien veel aandacht voor concepten, waarbij de burger meer dan voorheen ‘aan de knoppen zit’ van zijn eigen gegevens. Regie op gegevens en empowerment van de burger is steeds meer gewenst voor wat betreft privacyrechten zoals toestemming, inzage, correctie en verantwoording over derdenverstrekking. De afgelopen jaren is deze visie steeds meer uitgekristalliseerd, zowel in de context van identity management als in de context van het stelsel van basisregistraties.

Het gaat dus om concepten als user consent, elektronische invulling van het inzagerecht en implementaties van ‘kluisjes’, van waaruit de gebruiker zelf kan kiezen aan wie hij welke gegevens verstrekt (personal data stores).

De uitdaging is om hier nu één of meer voorzieningen voor te realiseren, conform opkomende standaarden. In dit verband is de UMA standaard erg interessant, die wordt ontwikkeld in de Kantara context. In de context van de Internet Identity Workshop wordt veel gesproken en geschreven over Vendor Relationship Management. Actieve participatie in deze en wellicht andere standaardisatieinitiatieven is aan te bevelen.

Qiy, Trusttester en IRMA zijn dan in Nederland voorzieningen / concepten die nuttig bruikbaar zouden kunnen zijn. Hoewel hier over wordt nagedacht zowel vanuit de invalshoek van de vorming van een eID Stelsel als vanuit het stelsel basisregistraties, is er nog geen sprake van een duidelijk uitgekristalliseerd beeld hoe deze en dergelijke voorzieningen / concepten inpasbaar zouden kunnen zijn. Bovendien zijn er nog geen algemeen geaccepteerde standaarden voor personal data stores.

Als dit onderwerp niet actief wordt behandeld dan zou wildgroei het gevolg kunnen zijn waarin op diverse plaatsen verregaand overlappende functies worden ontwikkeld als personal data storen, of kan een situatie ontstaan dat overheidsvoorzieningen in het geheel geen rekening houden met de opkomst van personal data stores.

Naast bovenstaande specifieke ontwikkelingen zijn er uiteraard diverse ontwikkelingen op het gebied van standaarden die kunnen bijdragen aan een goede privacy. Hoewel het vroeg dag is voor veel van deze standaarden bevelen wij aan om een inventarisatie te plegen van de relevante standaardisatieontwikkelingen zodat bepaald kan worden op welke ontwikkelingen Nederland nadere actie dient uit te voeren.

4.2.6 Internet of Things

Aanbeveling

- Verkenning uitvoeren Internet of Things

Toelichting

De techniek van ICT schrijdt nog steeds met rappe schreden voort. ICT rukt steeds verder in onze persoonlijke omgeving op, met steeds meer functies en apps op de mobiel, smart watches, sensoren en rekenfuncties in kleding. Ook de steeds verdere samenwerking en verbondenheid van apparaten (de spreekwoordelijke koelkast die de voorraden bewaakt en zelf bijbestelt), slimme thermostaten enzovoorts, kortom het Internet-of-Things.
Daarmee ontstaat ook de behoefte aan standaarden voor een veilig Internet of Things. De devices moeten zelf veilig zijn, zich betrouwbaar kunnen identificeren en veilig kunnen communiceren. Ze moeten, indien van toepassing, ook de gebruikers kunnen identificeren en authentiseren. Tenslotte moeten ze, conform ingestelde policies, gegevens met elkaar en andere toepassingen kunnen uitwisselen die conform de intenties van de gebruikers is.

Het is onwaarschijnlijk dat er zoiets komt als een ‘IoT beveiligingsstandaard’. Het zal grotendeels gaan om een verzameling van bekende standaarden en technieken, waarmee het IoT wordt beveiligd. Maar daarbij vormt de opschaling naar zeer grote aantallen apparaten en gebruikers echter een issue. Een ‘klassiek’ uitgifteproces voor digitale certificaten schaalt bijvoorbeeld slecht en dus zijn hier andere mechanismes en standaarden voor nodig. Er is dus impact te verwachten op de bekende beveiligingsmechanismen en de hiervoor ingerichte stelsels.

Deze trends brengen hun eigen beveiligingsuitdaging met zich mee en de kans is groot door er in de beginfase te weinig tijd aan te besteden, dat we geconfronteerd worden met een onbeheersbare situatie. We willen zelf immers bepalen welke apparaten in onze omgeving wat voor acties mogen ondernemen ten behoeve van ons. Daarvoor moet zowel de basistechniek, zoals de veilige ontwikkeling van apps, geregeld zijn, maar ook een gebruikersvriendelijke manier van configureren van het samenspel van dergelijke devices.

Omdat het onvoldoende duidelijk is wat het IoT is voor overheidsorganisaties en wat daar de beveiligingsuitdaging vormt, is allereerst een verkenning nodig, waarin de volgende vragen worden geadresseerd:

- wat is het IoT in de context van (verschillende soorten) overheidsorganisaties,
- wat zijn de soorten te verwachten gebruik,
- wat zijn dan de bijhorende beveiligingsissues,
- welke doelstellingen zouden er dan bereikt moeten worden,
- welke commerciële verhoudingen spelen er en

- welke standaarden horen bij dit alles?

4.2.7 Cloud

Aanbevelingen

- Verkenning uitvoeren Cloud.

Toelichting

Overheden gaan steeds meer gebruik maken van cloud. Dit kan een rijkscloud betreffen, het kan een gemeentecloud betreffen, een zuivere private cloud, het kan wellicht op termijn ook gaan om hybride vormen van cloud dienstverlening. In al deze vormen is de beheersing van informatiebeveiliging van groot belang. Dit wordt ook onderkend door de industrie waardoor er verschillende control frameworks beschikbaar zijn om een beheerste informatiebeveiliging in de cloud te realiseren. Organisaties als CSA en Eurocloud houden zich hier specifiek mee bezig. Er zijn ook meer generieke standaardisatie organisaties die op dit punt standaarden hebben ontwikkeld. De relevante vraag voor de overheid is welke standaarden er zijn of komen en wat de verschillen zijn. Op basis daarvan dient de overheid te bepalen op welke standaard of standaarden zij dient in te zetten.

4.2.8 Reageren op cyber threats

Aanbevelingen

- Actieve betrokkenheid bij standaarden voor early detection en uitwisselen van dreigingsinformatie, in het bijzonder TAXII, CybOX en STIX.

Toelichting

Het dreigingsbeeld dat het NCSC opstelt laat een verontrustende trend zien. Aanvallers worden steeds vaardiger, vasthoudender en professioneler. De georganiseerde misdaad en vreemde mogendheden houden zich op een hoog niveau bezig met cyberaanvallen.
Tegen dit soort aanvallen is een overwegend preventieve benadering niet meer houdbaar. Tenminste vergelijkbare inspanningen zijn noodzakelijk op het gebied van detectie en analyse van dreigingen en de daaropvolgende tegenmaatregelen (repressie en correctie). Vergaande samenwerking tussen organisaties is nodig om dit te bewerkstelligen, zowel in de context van het Nationaal Detectie Netwerk en daarbuiten. Ook het vergroten van het weerstandsvermogen – het handelend vermogen om aanvallen tegen te gaan – is een belangrijk aandachtspunt.

Het risico is vooral daarin gelegen dat Nederlandse organisaties en vitale infrastructuren onvoldoende weerbaar blijken en mogelijkerwijs ook (permanent) geïnfiltreerd worden door criminele organisaties en/of vreemde mogendheden. Dit heeft mogelijk vergaande consequenties voor de veiligheid van de Nederlandse samenleving.

Anomalie detectie, analyse en verspreiding van kennis over dreigingen zijn van groot belang voor het beter reageren op cyberthreats. De ontwikkeling en adoptie van standaarden hiervoor is dus belangrijk. In dat verband zijn jonge standaarden als STIX, CybOX en TAXII interessant. Actieve betrokkenheid van met name NCSC bij de (door)ontwikkeling van die standaarden is aan te raden.

4.3 Overige aanbevelingen

1. Stimuleer dat concrete oplossingen en in het bijzonder ICT innovaties zoveel mogelijk conform ICT standaarden functioneren.

Nederland wil een cybersecurity-industrie die meedoet op wereldniveau. Daarvoor stimuleert de Nederlandse overheid ook innovatie in het aanbod van informatiebeveiligingsproducten en -diensten, ondermeer met SBIR-oproepen. Innovatieve producten hebben een betere kans op de internationale cybersecurity markt indien zij voldoen aan (open) standaarden of indien er – parallel aan de ontwikkeling van het product – gewerkt wordt aan de ontwikkeling van de relevante open standaarden, waar het nieuwe product dan ook aan voldoet.

In dit verband is het aan RVO aan te bevelen een voorwaarde te verbinden aan innovatiesubsidie, namelijk het in kaart brengen van standaardisatiemogelijkheden dan wel het ontwikkelen van het product of de dienst in de context van standaardisatie, afhankelijk van het stadium waarin de innovatie zich bevindt.

Daarnaast kan gedacht worden aan het gericht stimuleren van het (internationaal) standaardiseren van inmiddels ontwikkelde innovatieve producten, zulks op aanvraag van de eigenaar van het product in kwestie.

Sommige open standaarden worden sterk bevorderd door de aanwezigheid van open source implementaties die als basis voor verdere ontwikkeling worden gebruikt door vele fabrikanten of als referentieimplementatie. Eerder heeft de Tweede Kamer al het initiatief genomen om encryptiesoftware als OpenSSL, LibreSSL te ondersteunen.

We bevelen aan om een stimuleringsbudget aan te leggen waarmee open sources initiatieven kunnen worden gesteund die een wezenlijke bijdrage leveren aan de adoptie en goede implementatie van kritische ICT-beveiligingsstandaarden.

2. Organiseer onderliggende en taakgebied-overstijgende kennisgebieden.

In het algemeen geldt dat het zinvol is om onderliggende kennisgebieden te organiseren en de inbreng van die kennis in andere richtlijnen te borgen. Het belangrijkste onderwerp van deze categorie is voor nu cryptografie. Hiermee kan dan ook ervaring worden opgedaan met het op deze wijze organiseren.

Voor authenticatie van de communicerende partijen, vertrouwelijke gegevensuitwisseling tussen die partijen, wordt veelal cryptografie gehanteerd in standaarden. Dat kan op allerlei niveaus: diep in het netwerktransport, maar ook end-to-end in emailtoepassingen tussen corresponderende personen.

Cryptografie is voer voor experts en is bovenal een dynamisch terrein. Algoritmes en sleutellengtes die vandaag nog als veilig worden beschouwd kunnen over enkele jaren afgeraden worden voor nieuwe systemen, en over nog een aantal jaren als zonder meer onveilig worden beschouwd. Een voorbeeld vormen de operationele normen in de BIR, waarin achterhaalde en tegenstrijdige adviezen omtrent de veilige sleutellengtes voor AES zijn opgenomen.

Tegelijkertijd is cryptografie een essentieel onderdeel voor de goede beveiliging in een steeds meer genetwerkte wereld. Cryptografie vormt de sloten en de sleutels in de cyberwereld.

Aanbevelingen over het goede gebruik van cryptografie zijn dan ook hard nodig. Op zich staan er al twee ETSI rapporten met aanbevelingen omtrent algoritmes en sleutellengtes voor elektronische handtekeningen op de lijst van aanbevolen standaarden (ETSI TR 102 076-1 en -2) (ten behoeve van electronic signature algo's). Daarnaast zijn er meer goede bronnen voor dergelijke aanbevelingen, zoals het Algorithms, key sizes and parameters report van ENISA.

We bevelen aan dat NCSC, mogelijkerwijs in samenwerking met het NBV, een dergelijke publicatie nationaal verzorgt en onderhoudt en bovendien aan kennisdisseminatie en advies rondom dit onderwerp doet, zodat partijen op hun situatie toegesneden adviezen gevraagd en ongevraagd ontvangen.

Een aandachtspunt is ook de toepassing van crypto in het standaardisatieproces zelf. In het verleden is geregeld geconstateerd dat partijen standaardisatie op een zodanige manier beïnvloed hebben dat dit in minder goede cryptografie resulteerde. Partijen die belang hebben bij goede cryptografie in standaarden dienen dus een actieve betrokkenheid bij de ontwikkeling van die standaarden te behouden, specifiek op dit punt. Het is aan te bevelen dit zo mogelijk op Europees niveau te organiseren.

A Bijlage: longlist ICT-beveiligingsstandaarden

De onderstaande longlist van ICT-beveiligingsstandaarden is tot stand gekomen door vanuit toepassingsgebieden ICT-beveiligingsstandaarden te selecteren die mogelijk van toegevoegde waarde konden zijn binnen het onderzoek. Vervolgens is binnen het onderzoek getoetst welke standaarden binnen het advies, de governance en inhoudelijke taakgebieden, pasten. Acties rondom die standaarden vallen daardoor altijd binnen het hoger liggende doel, een bredere strategie rondom ICT-beveiligingsstandaarden.

In de tabel is opgenomen welke standaarden nu onderdeel zijn van het onderzoek naar aanvullende aanbevolen standaarden. TOTP, SCIM en HSTS komen daarmee in aanmerking om op de lijst te komen.

In de laatste kolom van de tabel is weergegeven welke ICT-beveiligingsstandaarden nu zijn opgenomen op de lijst met open standaarden, er is toegevoegd in welk geval dat ‘pas toe of leg uit’ (PToLU) betreft.

Toepassingsgebied	Naam standaard	Standaard opgenomen in onderzoek aanvullende aanbevolen standaarden	Standaard staat op lijst open standaarden
(Veilige software-ontwikkeling en) product certificatie	ISO/IEC 15408		
Cloud	CSA		
Cloud	Eurocloud		
Cloud	SOC 2 en 3		
Control frameworks en baselines	Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR BI)		
Control frameworks en baselines	Baseline Informatiebeveiliging Rijksdienst		
Control frameworks en baselines	Voorschrift Informatiebeveiliging Rijksdienst (VIR)		
Control frameworks en baselines	Baselines		

Toepassingsgebied	Naam standaard	Standaard opgenomen in onderzoek aanvullende aanbevolen standaarden	Standaard staat op lijst open standaarden	
	Informatiebeveiliging overheid inclusief operationele normenkader (BIG, BIWA, IBI)			
Control frameworks en baselines	NEN-ISO/IEC 27002			
Control frameworks en baselines	NEN-ISO/IEC 27001			
Control frameworks en baselines	ISO 22301			
Control frameworks en baselines	ISO 25010			
Cryptografie	RSA			
Cryptografie	ETSI TS 102 176-1 en -2			
Cryptografie	AES			
Cryptografie	ESI ASiC (ETSI TS 103 174)			
Cryptografie	SHA-2			
Cryptografie	Diffie-Helman			
Cryptografie	DSA			
Cryptografie	ECDSA			
Cryptografie	FIPS 140-2			
Cryptografie	Algorithms, Key Sizes and Parameters Report			
Cryptografie en Identitymanagement	X509			
E-mail	STARTTLS			
E-mail	DANE			
E-mail	DKIM, SPF			PToLU
E-mail	SMTP/SMTPS/IMAP/SSL-POP3			
E-mail	PGP GNUGP			
E-mail	S/MIME			
Identitymanagement	Open ID Connect			

Toepassingsgebied	Naam standaard	Standaard opgenomen in onderzoek aanvullende aanbevolen standaarden	Standaard staat op lijst open standaarden
Identitymanagement	LEI		
Identitymanagement	FIDO		
Identitymanagement	OAUTH		Procedure 2016
Identitymanagement	Xades, Pades en Cades (esignatures)		Procedure 2016
Identitymanagement	OCSP		
Identitymanagement	KMIP		
Identitymanagement	XACML		
Identitymanagement	SAML		PToLU
Identitymanagement	SASL		
Identitymanagement	CA browserforum Baseline Requirements		
Identitymanagement	e-Herkenning overheidskoppelvlak		
Identitymanagement	Handreiking Betrouwbaarheidsniveaus Forum Standaardisatie / STORK / ISO29115		
Identitymanagement	LDAP		
Identitymanagement	PKIoverheid PvE		
Identitymanagement	SSH-2		
Identitymanagement	TOTP		
Identitymanagement	WS Policy		
Identitymanagement	BAFIN		
Identitymanagement	Kerberos		
Identitymanagement	SPML		
Identitymanagement en Cloud	SCIM		
Identitymanagement en Privacy	UMA		
Incident management	CybOX		

Toepassingsgebied	Naam standaard	Standaard opgenomen in onderzoek aanvullende aanbevolen standaarden	Standaard staat op lijst open standaarden
Incident management	STIX		
Incident management	TAXII		
Internet	RPKI		
Internet	BGP-SEC		
Internet	MANRS		
Internet	DNSSEC		PToLU
Internet	IPsec		
Internet	BCP38		
Internet	TLS		PToLU
Internet	DTLS		
Internet	Security of time protocols (NTP, PTP)		
Internet	FTP		
Internet	NTP		
Internet	Schematron		
Internet	SNMP Security		
Internet en Identitymanagement	Govroam / WPA 2 Enterprise (laatste staat sinds kort op PToLU)		WPA 2 Enterprise PToLU
Internet of Things	OWASP Internet-of-Things Top 10 Project		
Privacy	Handreiking PIA van NOREA		
Privacy	Richtsnoeren beveiliging van persoonsgegevens (privacy impact assesment)		
Privacy	Toetsmodel PIA Rijksoverheid		
Veilige software-ontwikkeling en certificatie	Framework Secure Software - Secure		

Toepassingsgebied	Naam standaard	Standaard opgenomen in onderzoek aanvullende aanbevolen standaarden	Standaard staat op lijst open standaarden	
	Software Foundation			
Veilige software-ontwikkeling en certificatie	Secure Software Development (SSD) van CIP			
Veilige websites	Rijkswebsites: Verplichte richtlijnen			
Veilige websites	HTTP security headers			
Veilige websites	HSTS	□		
Veilige websites	HTTPS		□	
Veilige websites	ICT-beveiligingsrichtlijnen voor webapplicaties van NCSC			
Veilige websites	Leidraad responsible disclosure van NCSC			
Veilige websites	OWASP top 10			
Vertrouwensdiensten en eID's	EIDAS			
Webservices	WS Security			
Webservices	XML Signature			
Webservices	Digikoppeling		□	PToLU
Webservices	XML Encryption			
Webservices	ASVS			

B Bijlage: actoren rond ICT-beveiligingsstandaarden

Hieronder beschrijven we de rollen van enkele van de belangrijkere actoren die direct een rol hebben in het verplichten of aanbevelen van ICT-beveiligingsstandaarden.

Forum Standaardisatie
Forum Standaardisatie heeft conform het besluit van het Nationaal Beraad Digitale Overheid d.d. 10 februari 2015 (bekrachtigd door de Ministerraad op 6 maart 2015) inzake de doelen, taken, werkwijze en samenstelling van het Forum Standaardisatie voor de periode 2015-2017[6] ook een rol met betrekking tot informatiebeveiliging. Daarbij ziet men duidelijk ook plaats voor standaarden die de informatiebeveiliging bij verschillende partijen verhoogt, zonder dat de standaard in kwestie zelf direct betrekking heeft op informatie-uitwisseling. Zo zien we bijvoorbeeld dat het Forum de ISO 27001 op de lijst heeft gezet, terwijl informatie-uitwisseling geen hoofdonderwerp is in die standaard. Een dergelijke ruime interpretatie is echter ook logisch en gerechtvaardigd. Immers, alleen als organisaties weten dat hun gegevens bij de andere organisatie ook in goede handen zijn, zal er sprake kunnen zijn van de “veilige en betrouwbare uitwisseling van gegevens”. Kortom: het beheersen en inzichtelijk maken van de informatiebeveiliging van een organisatie bevordert de interoperabiliteit tussen die organisatie en andere organisaties waarmee die organisatie verondersteld wordt gegevens uit te wisselen.

Digicommissaris
De Digicommissaris heeft primair tot doel om de regie te voeren op de ontwikkeling van de Generieke Digitale Infrastructuur van de Nederlandse overheid.

Het op orde hebben van de informatieveiligheid is een voorwaarde voor de continuïteit van de overheidsdienstverlening. De overheid moet ervoor waken dat er geen weeffouten in de digitale infrastructuur ontstaan waarvan misbruik gemaakt kan worden en dient bij gegevensuitwisseling duidelijke afspraken te maken over ieders verantwoordelijkheid met betrekking tot de veiligheid in de keten.

De Regieraad Interconnectiviteit voert de regie op een aantal zaken, die direct van belang zijn voor een goede informatiebeveiliging:

- Standaarden (onder meer de ‘pas-toe-of-leg-uit’-lijst). Onder standaarden zijn expliciet ook ICT-beveiligingsstandaarden onderkend;
- PKIoverheid(certificaten);
- Digipoort (overheidstransactiepoort(OTP) en ProcesInfrastructuur(PI));
- Diginetwerk;
- Nederlandse Overheids Referentie Architectuur (NORA).

---

6 https://www.forumstandaardisatie.nl/fileadmin/user_upload/20150306_Besluit_inzake_doelen_taken_werkwijze_en_samenstelling_Forum_Standaardisatie_2015-2017.pdf

De voorzieningen die onder de Regieraad Interconnectiviteit vallen, vormen het infrastructuur-fundament voor de Digitale Overheid. Zonder fysieke netwerken, standaarden, architectuur en gegevensuitwisseling kan er geen eOverheid zijn. De producten en standaarden in dit cluster zijn dus *Vitaal* voor de BV Nederland. Dit houdt in: verantwoordelijkheid voor een adequate infrastructuur op het gebied van borging van continuïteit, informatieveiligheid, privacybescherming en via borging door voldoende wettelijke kaders en beleidsplannen.

Met Digipoort en Diginetwerk worden ook beveiligde koppelvlakken gerealiseerd. Deze koppelvlakken zorgen voor een beveiligde verbinding tussen het bedrijfsleven en de overheid. De Regieraad Interconnectiviteit heeft aandacht voor juiste toepassing van de beveiligde koppelvlakken opdat de informatieveiligheid ook op netwerk- en voorzieningsniveau bij bedrijfsleven en overheid is geborgd.

Naast Informatiebeveiliging valt ook privacy onder de Regieraad Interconnectiviteit. Privacy raakt het vraagstuk ‘regie op gegevens’. In het rapport ‘Basisregistraties, vanuit het perspectief van de burger’, is de aanbeveling van de Rekenkamer om privacybescherming zo eenduidig mogelijk in te richten en te zorgen voor toezicht op de handhaving.
De vormgeving hiervan in wet- en regelgeving, maar ook in voorzieningen voor de burger om hiermee een hogere mate van transparantie en een hoge mate van regie op gegevensverstrekkingen te realiseren, is derhalve een aandachtspunt voor de Regieraad.

Naast technologische en nationale ontwikkelingen moet ook afstemming plaatsvinden met ontwikkelingen in de internationale omgeving. Enerzijds om zicht te houden of Nederland voldoende snelheid houdt bij de realisatie van de digitale overheid en om ervaringen uit andere landen te benutten. Anderzijds, om te borgen dat de nationale infrastructuur interoperabel is met de internationale omgeving zodat overheden ook gemakkelijker grensoverschrijdende gegevensuitwisselingen kunnen realiseren en zo een positieve invloed hebben op de concurrentiepositie van Nederland. Het realiseren van een generieke koppeling naar Europa past in de beleidsverantwoordelijkheid van EZ/BZK, waarvan de andere (vak)departementen gebruik kunnen maken.

Mensen, bedrijven en instellingen zullen ook steeds meer internationaal digitaal zaken met andere overheden willen regelen. Denk bijvoorbeeld aan studenten die over de grens willen studeren of mensen die in het ene land wonen en in het andere werken.

De GDI gaat nu vooral nog over het nationale verkeer. Maar Europese bouwstenen die ontwikkeld en gefinancierd worden binnen Europese projecten en programma’s als: Electronic Simple European Networked Services (eSens), Connecting Europe Facility (CEF) en Interoperability Solutions for European Public Administrations (ISA) en de beoogde opvolger daarvan, gaan over het grensoverschrijdende verkeer. Soms ligt hieraan (verplichte) Europese wet- en regelgeving ten grondslag, zoals de eIDAS verordening, over de erkenning van digitale identiteiten en handtekeningen. Deze werelden moeten, om effectief samen te kunnen werken en elkaar te kunnen versterken, bij elkaar worden gebracht.

NCSC en de Nationale Cybersecurity strategie 2
Het NCSC draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief.

Nu NCSC staat voor het centrum van kennis en diensten ter vergroting van de cybersecurity, is het zaak om, meer nog dan voorheen, de samenwerking met andere partijen te versterken. Zo kan de weerbaarheid tegen ICT-verstoringen en cyberaanvallen worden verhoogd. Die samenwerking is zo belangrijk omdat de ICT-infrastructuur en de kennis van deze infrastructuur grotendeels in handen is van (internationale) private partijen. Cybersecurity is daarom de optelsom van de gezamenlijke inspanningen van overheden, bedrijfsleven, organisaties en burgers, zowel nationaal als internationaal.

De visie is daarbij dat Nederland, samen met (nationale en internationale) partners, inzet op een veilig en open 'cyber' domein, waarin de kansen van digitalisering worden benut, dreigingen het hoofd worden geboden en fundamentele rechten beschermd.

De maatregelen in het kader van cybersecurity vergen maatwerk. Dat wordt op drie manieren vormgegeven. Ten eerste door maatregelen toe te snijden op het probleem dat ze moeten oplossen (risk-based), ten tweede door cybersecurity steeds in samenhang te bezien met maatschappelijke groei (zowel de economische als sociale voordelen die digitalisering biedt) en ten derde door het waarborgen van fundamentele rechten en waarden. Deze samenhang tussen veiligheid, vrijheid en maatschappelijke groei is een dynamische balans die tot stand moet komen in een constante open en pragmatische dialoog tussen alle stakeholders, zowel nationaal als internationaal.

De overheid treedt indien nodig sturend op. Daarbij kunnen regels, normen of standaarden worden (vast-) gesteld, bijvoorbeeld voor de vitale infrastructuur. Samen met vitale partijen stelt de overheid cybersecurity vereisten op waar dat nog niet het geval is. Bestaande (sectorale) toezichthouders zullen vervolgens eveneens daar waar dat nog niet het geval is hun rol moeten verbreden om ook cybersecurity te omvatten, waarbij overlap/dubbeling dient te worden voorkomen.

Het is bij dit alles de ambitie dat Nederland voorop loopt op het terrein van cybersecurity. Dit is van strategische waarde in de verdediging tegen dreigingen, zodat men optimaal van de voordelen van digitalisering kan profiteren. Maar ook de economische dimensie is een deel van de strategie, omdat cybersecurity een snel groeiende markt is.

Om de dialoog tussen verschillende stakeholders te laten leiden naar een nieuw volwassenheidsniveau van cybersecurity zijn in het bijzonder de volgende drie sturingsdimensies van belang: (zelf)regulering, transparantie en kennisontwikkeling.

De inzetten worden hoger en aanvallen geavanceerder

Inmiddels wordt wel duidelijk uit het Cybersecurity Beeld Nederland (CSBN) dat de grootste dreiging uitgaat van staten en georganiseerde criminaliteit. Staten vormen een directe dreiging in de vorm van diefstal van vertrouwelijke of concurrentiegevoelige informatie (cyberspionage). Tevens voeren staten verkenningen uit om in het geval van een conflict snel schade te kunnen toebrengen. Criminelen richten zich met name op digitale fraude en diefstal van informatie.

Concreet zijn de speerpunten in de komende tijd:

- Aanpak vitaal: risicoanalyses, veiligheidseisen en informatiedeling
- Versterkte aanpak cyberspionage
- Haalbaarheidsonderzoek gescheiden netwerk vitaal
- Versterking civiel-militaire samenwerking
- Versterking Nationaal Cyber Security Centrum
- Internationale aanpak cybercriminaliteit: actualisatie en versterking (straf)wetgeving

C Bijlage: toelichting workshop, interviews en stuurgroep

Doel workshop

De workshop had tot doel om samen met experts na te denken over de invulling van een strategie voor de overheid voor ICT-beveiligingsstandaarden.

Aanwezigen workshop en interviews

De aanwezigen bij de workshop waren:

- René van den Assem - VKA
- Rob van Dorsten - Ministerie van Binnenlandse Zaken
- Peter Groothuis - Platform voor Informatiebeveiliging
- Thomas de Haan - Ministerie van Economische Zaken
- Douwe Horst - VKA
- Ad Kint - UWV
- Bart Knubben - Bureau Forum Standaardisatie
- Eric Nieuwland - ICTU
- Wilfried Olthof - NOREA
- René Reith - Provincie Zuid-Holland
- Ad Reuijl - UWV
- Tobias Schaap - Ministerie van Financiën
- Michiel Steltman - Digitale Infrastructuur Nederland

Na de workshop is een tweetal interviews afgenomen met partijen die niet aanwezig waren tijdens de workshop. De interviews hebben verdieping gegeven in de reeds opgehaalde informatie. De interviews zijn afgenomen met:

- Erik Jonker - Bureau Digicommissaris
- Pieter Rogaar - Nationaal Cyber Security Centrum

Stuurgroep

De stuurgroep voor het onderzoek bestond uit:

- Erwin Bleumink - SURFnet
- Guus Bronkhorst - Ministerie van Buitenlandse Zaken & Koninkrijksrelaties
- Nico Romijn – KING

Met Erwin Bleumink, Nico Romijn, Nausika Efstratiades (IBD) en Erik Jonker is het concept rapport besproken en de aandachtspunten zijn opgenomen in de definitieve versie van het rapport.