e·OVERHEID
BOUW MEE AAN BETERE DIENSTVERLENING

NORA-katern

Informatiebeveiliging

Versie 1.0

MAILINGLIJST ARCHITECTUUR E-OVERHEID

Meld u aan voor deze mailinglijst en blijf daarmee op de hoogte van de ontwikkeling van NORA. U krijgt zo aankondigingen van openbare reviews van documenten, uitnodigingen voor bijeenkomsten en de nieuwsbrief Architectuur e-overheid.

http://www.overheid.nl/nieuwsbriefaanmelden/MailinglijstArchitectuur.html

Colofon

NORA-ID	: D06
Versie	: 1.0
Distributie	: 7
Datum	: 01-10-2009
Status	: versie voor openbare review
Expertgroep	: Informatiebeveiliging
Contactadres	: architectuur@overheid.nl

Dit document is ontwikkeld door RENOIR, een programma van de stichting ICTU.

Inhoudsopgave

NORA in het kort

Burgers en bedrijven verwachten een goed functionerende, dienstverlenende overheid. Samenwerking tussen overheidsorganisaties is hiervoor een belangrijke voorwaarde. Daarbij stemmen deze organisaties processen af en maken gebruik van elkaars informatie. NORA, de Nederlandse Overheid Referentie Architectuur, ondersteunt deze samenwerking.

> **Status van NORA**
>
> Het kabinet heeft NORA vastgesteld als norm voor de gehele overheid [2][3]. Deze status komt onder meer tot uitdrukking in het akkoord over het Nationaal Uitvoeringsprogramma Dienstverlening en e-overheid (NUP), dat door diverse bestuurslagen is bekrachtigd [4]. De status komt ook tot uitdrukking in het, van NORA afgeleide, Model Architectuur Rijksdienst (MARIJ) dat als referentiearchitectuur geldt voor ICT-projecten binnen de rijksdienst [3].

Goed functionerende overheid

Burgers en bedrijven verwachten een goed functionerende overheid. Zij willen een overheid [5]:

- waar je met je vragen terecht kunt: een overheid die een *state of the art* service biedt aan burgers en bedrijven en waar je zeven dagen per week, 24 uur per dag kunt aankloppen;
- die niet naar de bekende weg vraagt: een overheid die de administratieve lasten waarmee zij burgers en bedrijven confronteert, tot een onvermijdelijk minimum beperkt;
- die niet voor de gek te houden is: een overheid waarvan vaststaat dat ze slagvaardig optreedt bij fraude en bij de handhaving van wet- en regelgeving, vergunningen en dergelijke;
- die weet waarover ze het heeft: een overheid waarvan duidelijk is dat haar beleidsontwikkeling en -uitvoering op een gedegen kennis en toegang tot informatie stoelen;
- waarop je kunt vertrouwen: een overheid die zorgt voor rechtszekerheid en rechtsgelijkheid;
- die niet meer kost dan nodig is: een overheid die laat zien dat ze haar taken efficiënt vervult dankzij een goede organisatie en met inzet van moderne hulpmiddelen.

Bestuurlijke uitdagingen

Veel maatschappelijke kwesties vragen om intensieve samenwerking tussen overheidsorganisaties. Denk aan het gecombineerd afhandelen van vergunningaanvragen of de gecoördineerde aanpak van probleemjongeren door school, maatschappelijk werk en politie. Een dergelijke intensieve samenwerking is alleen goed mogelijk wanneer overheidsorganisaties interoperabel zijn. Dit wil zeggen dat zij in staat zijn om effectief en efficiënt informatie te delen. Niet alleen met elkaar, maar ook met burgers en bedrijven.

Volgens het kabinet vergroot interoperabiliteit de effectiviteit en flexibiliteit van het openbaar bestuur. Daarmee vormt dit begrip een 'essentiële randvoorwaarde voor een toekomstvaste ontwikkeling van diensten en toepassingen die door en met ICT in brede zin mogelijk

worden gemaakt' [6].

Als individuele organisaties gaan samenwerken, krijgen zij niet alleen te maken met elkaars systemen en processen, maar ook met begripsverwarring, cultuurverschillen en belangentegenstellingen. Dit wordt opgelost door afspraken te maken over de definitie van begrippen, de manier waarop gegevens worden verwerkt, de te gebruiken infrastructuur, etc. Wanneer hierbij een groot aantal partijen is betrokken, neemt de complexiteit van het maken van bilaterale afspraken zo sterk toe, dat dit praktisch ondoenlijk wordt.

Definitie interoperabiliteit

Interoperabiliteit is het vermogen van organisaties (en van hun processen en systemen) om effectief en efficiënt informatie te delen met hun omgeving. In de context van NORA betekent interoperabiliteit de informatiedeling tussen een overheidsorganisatie enerzijds en burgers, bedrijven of andere overheidsorganisaties anderzijds. Ongeacht het soort informatie en de manier van informatiedeling. Interoperabiliteit gaat over informatieverwerking, maar raakt evengoed aan de bedrijfsvoering en de technische voorzieningen.

Werken met NORA

NORA biedt een raamwerk dat het maken van afspraken tussen organisaties vereenvoudigt of in sommige gevallen zelfs overbodig maakt. NORA is een checklist van algemeen geaccepteerde principes (uitgangspunten) voor de inrichting van processen en systemen met het oog op interoperabiliteit. Organisaties die met NORA werken, kiezen voor aansluiting bij een aantal breed gedeelde uitgangspunten en bijbehorend begrippenkader. Hierdoor wordt het gemakkelijker om afspraken te maken met organisaties die dezelfde uitgangspunten hanteren.

Het zal in de praktijk moeilijk zijn om in één keer volledig aan deze principes te voldoen. Dat is ook niet nodig. Waar het om gaat, is dat overheidsorganisaties het streven naar samenwerking onderschrijven, zich aan de principes committeren en waar mogelijk sturen op het voldoen aan de principes. Overheidsorganisaties gaan daarmee een groeipad op, waarbij NORA de richting aangeeft.

De praktijk: omgevingsvergunning

Wie een huis wil bouwen, krijgt te maken met verschillende vergunningen en voorschriften. Het gaat om regelingen voor wonen, ruimte en milieu, die elk hun eigen criteria en procedures hebben. De vergunningen worden verstrekt door verschillende overheidsinstanties. Dit is voor burgers, bedrijven én de overheid onoverzichtelijk, tijdrovend en kostbaar. Het kan bovendien leiden tot tegenstrijdige beslissingen. Om in deze situatie verbetering te brengen, regelt de Wet algemene bepalingen omgevingsrecht (Wabo) de bundeling van verschillende vergunningen tot één omgevingsvergunning. Gemeenten fungeren hiervoor als loket. Achter dit loket worden de (deel)aspecten nog steeds beoordeeld door verschillende overheidsorganisaties, maar zij stemmen hun activiteiten af om tot één besluit te komen.

Kosten en baten

Samenwerking vraagt om een investering in tijd en geld. Daarbij komen de lasten vaak voor de baten. Lasten die bovendien niet altijd evenredig over alle overheidsorganisaties zijn verdeeld en baten die niet altijd in geld zijn uit te drukken. Toch zijn de voordelen aanzienlijk (voor individuele organisaties en voor de overheid als geheel):

- besparingen, door gebruik te maken van generieke oplossingen en door het voorkomen van dubbel werk;
- kwaliteitswinst, door bijvoorbeeld gebruik te maken van eenduidige, betrouwbare
- gegevens;
- waarborging van de samenhang tussen ontwikkelingen binnen en buiten de eigen
- organisatie;
- standaardisatie, waardoor de flexibiliteit toeneemt, omdat organisaties gemakkelijker
- kunnen samenwerken met andere organisaties, burgers en bedrijven.

Het gebruik van NORA verhoogt de effectiviteit van investeringen door de inspanningen van verschillende organisaties op elkaar af te stemmen. Hoewel werken met NORA initieel een extra investering vergt (in de opbouw van kennis en de toetsing van plannen), zijn deze kosten laag in verhouding tot de kosten voor het uitvoeren van de plannen zelf. De inzichten die uit de toetsing voortkomen, kunnen aanzienlijke besparingen opleveren. Tijdig bijsturen voorkomt namelijk kostbare herstelwerkzaamheden in een later stadium en helpt bij het beheersen van risico's.

Waarop is NORA gebaseerd?

NORA is gebaseerd op bestaand overheidsbeleid (nationaal en Europees) en op de instrumenten die in het kader van dat beleid zijn ontwikkeld, zoals wetten, regels, Kamerstukken, bestuursakkoorden en de resultaten van overheidsprogramma's. NORA ontsluit deze bronnen in onderlinge samenhang en plaatst ze in de context van interoperabiliteit. De beleidsuitgangspunten zijn daarvoor niet altijd direct toepasbaar. In dat geval maakt NORA een vertaalslag. Daarbij baseert NORA zich op de gedeelde inzichten onder professionals die uitvoering geven aan het beleid.

Tien basisprincipes

NORA kent tien basisprincipes die betrekking hebben op dienstverlening. Het begrip 'dienst' betekent hier alle activiteiten waarmee dienstverleners publieke taken uitvoeren. Het uitgangspunt is dat de afnemers (burgers, bedrijven en andere overheidsorganisaties) in de dienstverleningsrelatie centraal staan.

Burgers, bedrijven en overheidsorganisaties (afnemers)

...krijgen de dienstverlening waar ze behoefte aan hebben.

...kunnen de dienst eenvoudig vinden.

...hebben eenvoudig toegang tot de dienst.

...ervaren uniformiteit in de dienstverlening door het gebruik van standaardoplossingen.

...krijgen gerelateerde diensten gebundeld aangeboden.

...hebben inzage in voor hen relevante informatie.

...worden niet geconfronteerd met overbodige vragen.

...kunnen erop vertrouwen dat informatie niet wordt misbruikt.

...kunnen erop vertrouwen dat de dienstverlener zich aan afspraken houdt.

...kunnen input leveren over de dienstverlening.

De inleidende tekst is ontleend aan het NORA Katern Strategie. Dit katern kunt u vinden op https://www.surfgroepen.nl/sites/NORA-architecten/NORA-forum/review.aspx

Inleiding

Overheidsorganisaties staan voor de uitdaging om intensiever met elkaar samen te werken in hun dienstverlening aan burgers en bedrijven. In deze samenwerking staat het uitwisselen van informatie centraal. Dat is alleen goed mogelijk wanneer overheidsorganisaties en afnemers elkaar en de informatie kunnen vertrouwen. Een juiste beveiliging en transparantie hierover is een voorwaarde om dit vertrouwen te verdienen. Er is echter méér nodig. Verschillen tussen organisaties in de wijze van beveiliging vormen een hindernis voor informatie-uitwisseling. Organisaties zullen daarom hun informatiebeveiliging aan de hand van standaarden op elkaar moeten afstemmen. Dit katern biedt daartoe definities, beschrijvingen en principes.

Informatiebeveiliging

Bij het streven naar een betere dienstverlening is informatiebeveiliging een cruciale randvoorwaarde. De bestuurs- en bedrijfsprocessen die de dienstverlening mogelijk maken, zijn namelijk afhankelijk van een goed functionerende informatievoorziening. Veel processen zijn nagenoeg onmogelijk zonder de toepassing van geautomatiseerde gegevensverwerking. Uitval van computersystemen, het in ongerede raken van gegevensbestanden of manipulatie van gegevens door onbevoegden kan daarom ernstige gevolgen hebben voor de overheidsorganisatie en voor burgers en bedrijven. Politieke consequenties en imagoschade kunnen daarvan het gevolg zijn.

Informatiebeveiliging heeft betrekking op alle aspecten van de bedrijfsvoering: organisatie, processen, mensen, ICT, contracten, gebouwen, installaties etc. Het garanderen van een betrouwbare informatievoorziening en van vertrouwelijkheid, beschikbaarheid en integriteit van de gebruikte gegevens is daarbij het centrale doel. Binnen veel grotere overheidsorganisaties heeft de informatiebeveiliging een zekere volwassenheid bereikt: zo is men zich bewust van risico's en bestaat er beleid om deze risico's te beheersen. Ook zijn verantwoordelijkheden en beveiligingsbeheer belegd en speciale functionarissen aangesteld.

Al deze organisaties vertalen de voor hun relevante wetgeving en de keuze uit het grote aantal standaarden naar de eigen situatie. De consequentie daarvan is dat elke organisatie de informatiebeveiliging volgens eigen normen en methoden vormgeeft. Dat uit zich onder meer in (onnodige) barrières bij het koppelen van netwerken of in de moeizame totstandkoming van ketenspecifieke beveiligingskaders. Dit vormt een belemmering voor verdere samenwerking binnen de overheid.

Geen samenwerking zonder vertrouwen...

Samenwerking vraagt van organisaties dat zij zich afhankelijk maken van elkaar en hun eigen dienstverlening baseren op dienstverlening van anderen. Veel organisaties besteden bijvoorbeeld het beheer van hun ICT-verwerking uit aan een serviceprovider. Zijn vertrouwelijke gegevens bij de serviceprovider wel in veilige handen? Beschikken zijn systemen wel over voldoende capaciteit en zijn die systemen op het gewenste tijdstip in de lucht? Vergelijkbare vragen gelden wanneer de ene overheidsorganisatie voor serviceverlening aan burgers en bedrijven actuele gegevens van een andere organisatie nodig heeft. Alleen wanneer ketenpartners vertrouwen hebben in de antwoorden op deze vragen, kunnen zij goed samenwerken. Dit vertrouwen ontstaat wanneer de informatiebeveiliging transparant en onafhankelijk is getoetst.

...en geen vertrouwen zonder standaardisatie, toetsing en verantwoording

Zoals hierboven is geschetst, verschillen de normen en methoden van beveiliging van organisatie tot organisatie. Hierdoor is het bieden van inzicht aan ketenpartners en het beoordelen van elkaars beveiliging een enorme uitdaging.

In het kader van de samenwerking zullen veel organisaties eisen willen stellen aan elkaars informatiebeveiliging en hierover afspraken maken. Volgens de regelen der kunst zouden deze eisen gebaseerd moeten zijn op uitgebreide risicoanalyses. Het maken van dergelijke risicoanalyses (op zich al monnikenwerk) en bijbehorende normenkaders wordt met de toenemende complexiteit van ketenverwerkingsprocessen een steeds grotere opgave. Nog buiten beschouwing gelaten dat een organisatie dit voor tientallen diensten moet doen en dat hierover met tientallen organisaties afspraken gemaakt moeten worden. Al met al is dit een onwerkbare ambitie.

NORA staat voor een benadering die effectiever en efficiënter is. Hierin sluiten organisaties zich aan bij standaarden (normen en methoden) voor informatiebeveiliging. Overheidsorganisaties richten hun informatiebeveiliging op basis van dezelfde standaarden in. Laten deze inrichting onafhankelijk toetsen en leggen over de toetsresultaten verantwoording af. Het doel van dit katern is om de gebruikers van NORA met behulp van een samenhangend instrumentarium van principes, architectuurmodellen en best practices hiertoe in staat te stellen.

De praktijk: informatiebeveiliging bij UWV en Belastingdienst

De Belastingdienst en UWV hebben allebei gegevens nodig van werkgevers, voor de loonheffing en om uitkeringen en toeslagen te kunnen berekenen. Om de rechtmatigheid van hun werkzaamheden vast te stellen, zouden beide organisaties bepaalde gegevens bij de werkgevers moeten controleren. Men heeft de taken echter zodanig verdeeld dat de Belastingdienst de controles uitvoert en heffingen int, terwijl UWV voor beide organisatie een gemeenschappelijke registratie voert. Daardoor hebben werkgevers maar met één partij te maken voor de heffing, en het controleproces is efficiënt. Het maakt de Belastingdienst en UWV voor de betrouwbaarheid van een belangrijk onderdeel van hun primaire processen wel afhankelijk van elkaar.

Beide organisaties hebben meer processen waar andere ketenpartners een belang bij hebben. Accountantsmededelingen of gemeenschappelijke audits geven hier zekerheid over de betrouwbaarheid. Die verklaringen kunnen worden uitgewisseld zodat elke ketenpartner voor zich 'dekkende' verklaringen heeft voor zijn gehele proces, inclusief de ketenprocessen. De accountants baseren zich voor het afgeven van deze verklaringen vaak op speciaal voor een bepaalde keten ontwikkeld normenkader. UWV en Belastingdienst vinden dat deze werkwijze (het per deelproces verzekeren van de betrouwbaarheid) niet efficiënt is.

Beide organisaties zien de aansluiting bij een standaard normenkader, dat alle ketenpartijen hanteren, als oplossing. Op basis hiervan kan verantwoording afgelegd worden in het jaarverslag, waarbij de accountant tevens een oordeel geeft over die verantwoording. Ketenpartners kunnen dan eenvoudig hiernaar verwijzen. Indien andere partners van UWV en Belastingdienst ook zouden kiezen voor deze aanpak, betekent dat een verdere vereenvoudiging: geen tijdrovende formulering van normen, geen moeizame invlechting in de eigen kaders en geen aparte accountantsmededelingen. Bovendien neemt de transparantie hierover naar burgers en bedrijven toe.

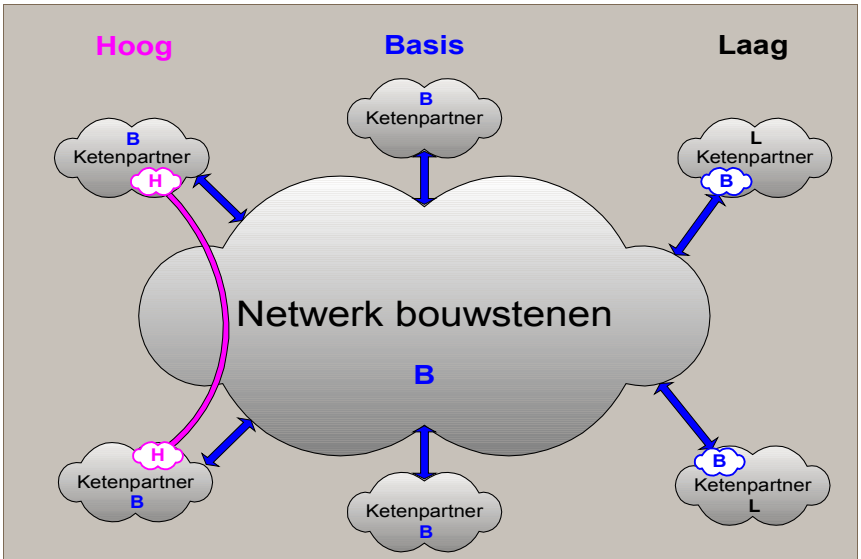
Standaarden

Voor informatiebeveiliging bij de overheid zijn het Voorschrift Informatiebeveiliging Rijksdienst [VIR] en de ISO-NEN 27002 [Code2] de meest relevante standaarden. Zij zijn daarom voor dit katern de basis. Beide standaarden hebben ook tekortkomingen. Zo is het VIR alleen ontwikkeld voor het Rijk. Dit katern stelt voor om het VIR, met enige aanvullingen en opmerkingen, als standaard voor de gehele overheid in te zetten. De ISO-NEN 27002 [Code2] heeft als tekortkoming dat zij weinig aanknopingspunten biedt voor toepassing van ICT in ketens. Dit katern formuleert daarom principes die de ISO-NEN 27002 [Code2] op dit punt aanvullen. De toepasbaarheid van deze twee standaarden voor alle overheidsorganisaties staat daarbij voorop.

Basisniveau informatiebeveiliging

In dit katern is een zogenaamd *basis beveiligingsniveau* uitgewerkt. Dit niveau is voldoende voor de beveiliging van massale verwerking van persoons- en financiële gegevens. Organisaties die vanuit een lager beveiligingsniveau willen communiceren, zullen op het basisniveau aan aansluitvoorwaarden moeten voldoen. Het in dit katern opgenomen principe met betrekking tot zonering zal daarbij kunnen worden toegepast.

Verwerking van gegevens van gevoelige aard, zoals opsporingsgegevens of staatsgeheimen, vraagt om een hoog beveiligingsniveau. De uitwerking van dit hoge niveau staat op de NORA -agenda [NVIB]. In afwachting hiervan zullen organisaties die gevoelige gegevens willen uitwisselen voorlopig zelf onderling afspraken moeten maken. E-overheid-bouwstenen kunnen overigens hogere niveaus van vertrouwelijkheid faciliteren door het aanbieden van gescheiden logische verbindingen, die ook niet binnen het besloten netwerk van de bouwstenen kunnen worden beïnvloed. Deze logisch gescheiden verbindingen maken al wel onderdeel uit van het basisniveau. Zie ook figuur 1.



Figuur 1: Communiceren op verschillend beveiligingsniveau

Uitgangspunten

Het katern met de bijbehorende best practices is bedoeld als algemeen advies- en toetsingskader. Tijdens de ontwikkeling zijn de volgende uitgangspunten gehanteerd:

- *Pragmatisme:* putten uit ervaring en deskundigheid van grote uitvoeringsorganisaties; aansluiten bij hun issues en prioriteiten.
- *Realisme:* rekening houden met bestaande systemen, die vaak nog vele jaren mee moeten. Geen ambities op te lange termijn.
- *Verbinding:* informatiebeveiliging als kwaliteitsborg op alle aspecten van bedrijfsvoering, zoals ICT en medewerkers. Geen informatiebeveiliging zonder context.
- *Acceptatie*: samenwerking met beroepsgroepen (PvIB[1], NOREA[2]) om breed gedragen principes te krijgen.

Doelgroep

Dit katern is bedoeld voor beveiligingsspecialisten, zoals functionarissen informatiebeveiliging en privacy, beveiligingsarchitecten, -adviseurs en -auditors. Daarnaast

1 Platform voor Informatiebeveiliging

2 Nederlandse Orde van Register EDP-auditors

is het katern bedoeld voor de bredere NORA-doelgroep: bestuurders, managers, architecten en ICT-uitvoerders.

De specialisten kunnen met behulp van dit katern het informatiebeveiligingsbeleid in hun organisatie vormgeven. Bestuurders en managers moeten op hoofdlijnen weten wat dit voor hun organisatie betekent; zij zijn verantwoordelijk voor de toetsing van het beleid op dit punt en de verantwoording hierover. Architecten en ICT-uitvoerders kunnen aan de hand van dit katern beter rekening houden met de informatiebeveiligingsaspecten in hun eigen werk.

Leeswijzer

Het katern Informatiebeveiliging bevat de volgende hoofdstukken:

1. *Onderwerpen en definities:* Welke onderwerpen en begrippen zijn belangrijk voor de interoperabiliteit?
2. Algemene beveiligingsprincipes: Aan welke principes moeten organisaties voldoen?
3. *Principes voor ICT-voorzieningen:* Aan welke principes moeten de ICT-voorzieningen van de diensten voldoen?
4. *Basismodellen informatiebeveiliging in de ICT-voorzieningen:* Hoe kan het model voor informatiebeveiligingsfuncties gebruikt worden om informatiebeveiliging mee te ontwerpen in de ICT-voorzieningen?

In bijlage I worden, in aanvulling op hoofdstuk 1, enkele algemene begrippen gedefinieerd. In bijlage II is, met bronnenverwijzing, onder meer een overzicht opgenomen van relevante wet- en regelgeving en is de verwijzing te vinden naar een aantal NORA-dossiers, die op ICT-gebied nog een verdere uitwerking geven aan de principes en modellen.

1. Onderwerpen en definities

Dit hoofdstuk schetst de belangrijkste onderwerpen in informatiebeveiliging vanuit het perspectief van interoperabiliteit. Daarnaast definieert het een aantal basisbegrippen. Deze definities zijn zoveel mogelijk ontleend aan de regelgeving en standaarden voor het vakgebied.

Het aantal risico's én de te nemen maatregelen op het gebied van informatiebeveiliging zijn buitengewoon omvangrijk en divers van aard. Dit bemoeilijkt niet alleen de inrichting en het toezicht, maar ook het afstemmen van informatiebeveiliging tussen organisaties. Een eerste stap in de richting van standaardisatie binnen de overheid is de introductie van een eenduidig begrippenkader. Dit begrippenkader is noodzakelijk om de principes op de juiste manier te begrijpen. De definities van de meer gangbare begrippen zijn opgenomen in bijlage II.

INFORMATIEBEVEILIGING (definitie 800)

Informatiebeveiliging betreft het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Bovendien gaat informatiebeveiliging over het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

Informatiebeveiliging maakt onderdeel uit van de kwaliteitsaspecten van informatie. Het begrip betrouwbaarheid (de mate waarin de organisatie zich voor de informatievoorziening kan verlaten op een informatiesysteem) kan als synoniem voor informatiebeveiliging worden gebruikt. Het aspect controleerbaarheid speelt een belangrijke rol bij het afleggen van verantwoording over alle aspecten van informatiebeveiliging.

INFORMATIEBEVEILIGINGSBELEID (definitie 801)

Dit beschrijft de uitgangspunten en randvoorwaarden die de organisatie op dit gebied hanteert. In het bijzonder gaat het om de inbedding in het algemene beveiligingsbeleid en het informatievoorzieningsbeleid.

Volgens het VIR regelt een overheidsorganisatie in dit beleid de volgende zaken:

- de rol van de informatiebeveiliging in de organisatie
- de verantwoordelijkheden, taken en bevoegdheden van (IB-)functionarissen
- de verantwoordelijkheid van lijnmanagers voor ketens van informatiesystemen
- de vaststelling van gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn
- de evaluatiefrequentie van het beleid
- de bevordering van het beveiligingsbewustzijn.

IN CONTROL STATEMENT (definitie 802)

Een 'In control statement' (ICS) is een certificaat inzake de kwaliteit van de bedrijfsvoering. Een ICS geeft daarmee antwoord op de vraag in hoeverre het management voldoende grip heeft op de bedrijfsprocessen.

Het huidige ICS beperkt zich tot de bedrijfsprocessen, die tot financiële informatie leiden. De werking van het ICS kan echter verbreed worden, zodat het ook informatiebeveiliging omvat. Aanknopingspunt voor de verbreding van het ICS zijn de normen voor integriteit en controleerbaarheid. Deze normen zijn gerelateerd aan normen voor informatiebeveiliging. Veel e-overheidsdiensten leiden eveneens tot financiële informatie, dus dat is een ander

aanknopingspunt. Voor deze verbreding van het ICS is wel een aangepaste formulering vereist. Uitwerking daarvan staat op de NORA-agenda [NVIB].

> **De Nederlandse Corporate Governance Code (Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen) d.d. 9 december 2003 bevat de volgende stelling:**
>
> II.1.4 In het jaarverslag verklaart het bestuur dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn en geeft hij een duidelijke onderbouwing hiervan. Het bestuur rapporteert in het jaarverslag over de werking van het interne risicobeheersings- en controlesysteem in het verslagjaar. Het bestuur geeft daarbij tevens aan welke eventuele significante wijzigingen zijn aangebracht, welke eventuele belangrijke verbeteringen zijn gepland en dat één en ander met de auditcommissie en de raad van commissarissen is besproken.

Voor een voorbeeld van een ICS dat reeds een heel eind in de gewenste richting gaat, zie [7].

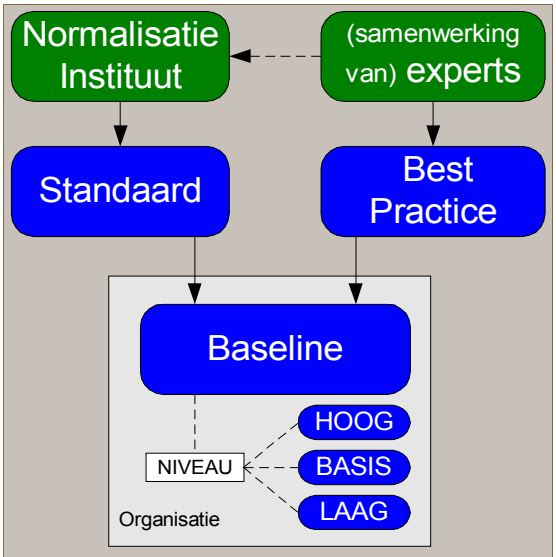
STANDAARD, BEST PRACTICE, BASELINE EN RISICOANALYSE

De begrippen 'standaard', 'best practice' en 'baseline' worden vaak door elkaar heen gebruikt. Om verwarring te voorkomen worden deze begrippen in NORA in samenhang gedefinieerd en toegelicht vanuit het perspectief van informatiebeveiliging. Vervolgens worden deze begrippen in verband gebracht met de begrippen beveiligingsniveau en risicoanalyse.

Een *IB-standaard* is een gemeenschappelijk normenstelsel van betrouwbaarheidseisen, maatregelen en/of implementatierichtlijnen, dat is uitgebracht door een gerenommeerd normalisatie-instituut, zoals ISO[3], NEN[4] of NIST[5].

Een *best practice* kan dezelfde soort inhoud hebben als een IB-standaard, maar heeft niet dezelfde status. Het is de verzamelde kennis van een groep deskundigen over een bepaald onderwerp. Een NORA-expertgroep of een beroepsvereniging kan bijvoorbeeld een best practice uitbrengen.

Een *baseline* is eveneens een normenstelsel, maar dan een die binnen een organisatie is vastgesteld om op basis daarvan maatregelen te treffen per informatiesysteem. Een baseline kan betrekking hebben op meer beveiligingsniveaus. Gebruikelijk is om uit te gaan van een hoog, basis en laag niveau. Figuur 2 laat de samenhang van de verschillende normenstelsels zien.



Figuur 2: Samenhang normenstelsels

Een baseline is gericht op het merendeel van de informatiesystemen dat in een organisatie

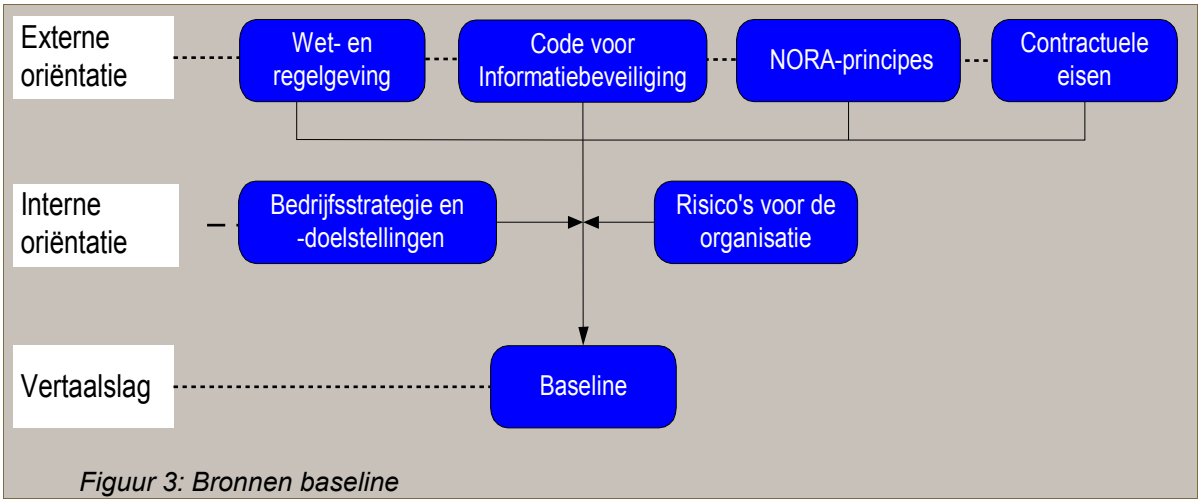
3 International Organization for Standardization

4 Nederlands Normalisatie Instituut (NEN = NEderlandse Normen)

5 National Institute of Standards and Technology (US)

gebruikt wordt. Dat merendeel van de informatiesystemen heeft dan een overeenkomstig beveiligingsbelang in termen van beveiligingsrisico's, waarbij het meestal gaat om het soort gegevens dat in die systemen wordt verwerkt. Bij de risico's is vooral bepalend de mate van vertrouwelijkheid, het bedrijfs- en/of financieel belang. De betekenis van baselines is, dat niet meer in alle gevallen per informatiesysteem een uitgebreide risicoanalyse hoeft plaats te vinden.

Alvorens in te gaan op de risicoanalyse, komt eerst aan de orde op basis waarvan een baseline tot stand komt. Dat is gevisualiseerd in figuur 3.

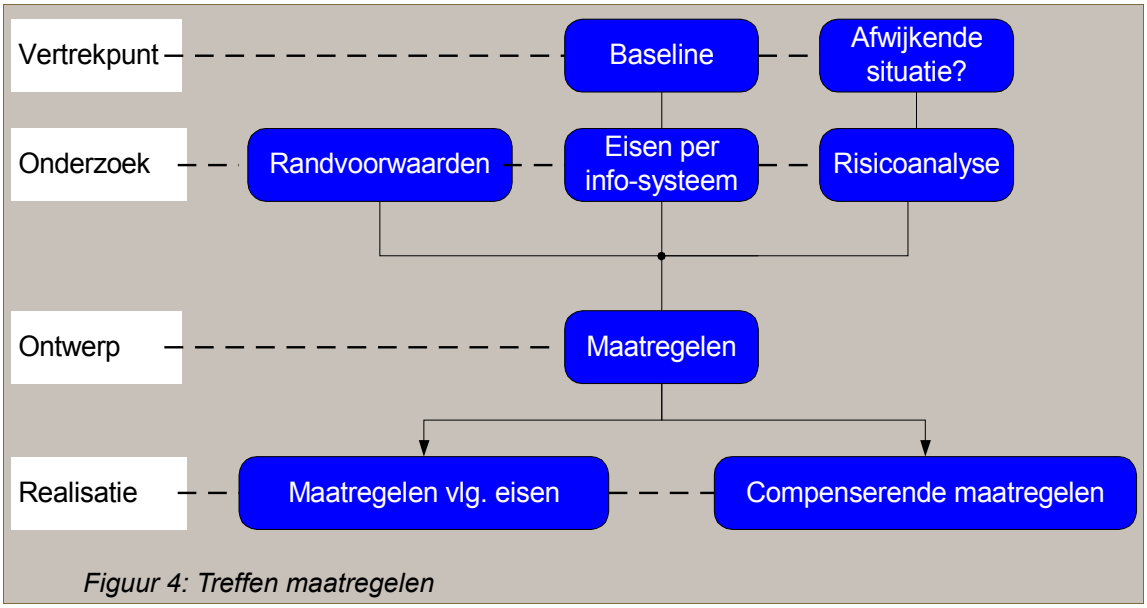


Figuur 3: Bronnen baseline

In paragraaf 0.3 van ISO-NEN 27002 [Code2] is aangegeven dat een organisatie voor het vaststellen van de beveiligingseisen haar beveiligingsbehoeften moet bepalen. Daarvoor zijn hoofdbronnen aan te wijzen, die in de figuur bij externe oriëntatie zijn aangegeven. In Bijlage III Bronnen is een opsomming gegeven van relevante wet- en regelgeving. Naarmate meer informatiesystemen betekenis hebben voor de e-overheidsdienstverlening, zullen NORA-principes integraal in de baseline worden verwerkt. Met branchegenoten, ketenpartners, leveranciers en afnemers worden vaak overeenkomsten afgesloten. Hieruit kunnen algemene verplichtingen voortvloeien inzake informatiebeveiliging, welke als externe eis worden meegenomen in de baseline. Externe bronnen kunnen elkaar overlappen of aanvullen. In ieder geval zullen ze vaak aanleiding geven tot het maken van een eigen interpretatie, gezien de keuzemogelijkheden die ze bieden of het hoge abstractieniveau waarvan ze uitgaan.

Niet elke organisatie heeft hetzelfde risicoprofiel: een belastingheffende instelling, die zijn transacties via internet met klanten regelt, zal bijvoorbeeld meer informatiebeveiligingsrisico's kennen dan een afvalverwerkingsbedrijf. Hoe hoger de risico's, des te meer of hogere eisen er in de baseline zullen worden opgenomen. De aard van de eisen en gewenste maatregelen hangt voorts samen met keuzes die een organisatie wil maken: veel of weinig eigen verantwoordelijkheid voor de medewerkers, wel of geen centrale, centraal geautomatiseerde maatregelen, faciliteren i.p.v. verbieden, etc.

Als op deze wijze de baseline tot stand is gekomen, kunnen vervolgens de maatregelen per informatiesysteem worden getroffen. Hiertoe dient figuur 4 als illustratie.



Figuur 4: Treffen maatregelen

Voor het merendeel van de informatiesystemen worden de maatregelen getroffen op basis van de baseline. Daarbij is het van belang om per informatiesysteem vast te stellen of er sprake is van afwijkende situaties, die risico's met zich brengen die onvoldoende in de baseline zijn begrepen. Afwijkende situaties kunnen onder meer betrekking hebben op hogere beschikbaarheidseisen, ander dan standaard gebruik van de technologie, toepassing van nieuwe technologie, gegevens met een bijzonder belang en extra conversieproblematiek.

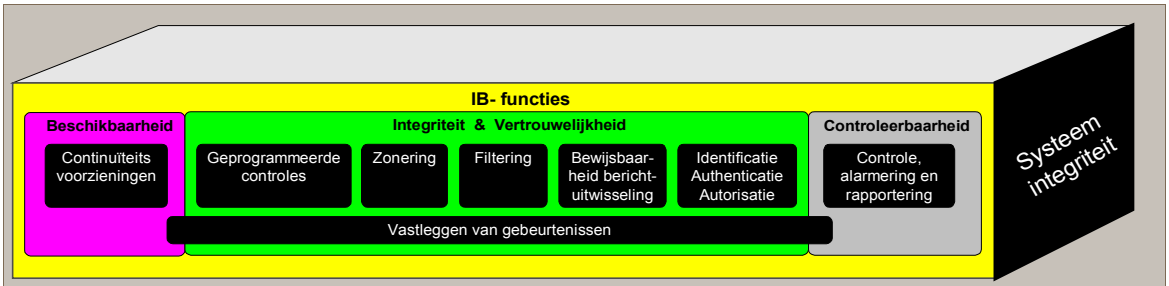
Bij een risicoanalyse worden bedreigingen benoemd en in kaart gebracht. Per bedreiging wordt de kans van het optreden ervan bepaald. Vervolgens wordt berekend wat de schade is die zou kunnen optreden als een bedreiging zich daadwerkelijk voordoet. Daarna worden analyses gemaakt van de kosten van te treffen maatregelen versus de baten van de hiermee te vermijden schaden. Dit alles is een zeer tijdrovend en arbitrair proces. Tijdbesparende kwalitatieve in plaats van kwantitatieve methoden lossen hierbij het arbitraire aspect maar ten dele op. Het bepalen van een geschikte methodiek voor risicoanalyse is één van de NORA-agendapunten [NVIB]. Op basis van de onderkende risico's van de specifieke situatie die bij een informatiesysteem aan de orde kan zijn, worden compenserende maatregelen (extra maatregelen, bovenop de baseline) getroffen.

Er zijn meer factoren op grond waarvan er in specifieke situaties afgeweken kan worden van de baseline-maatregelen: te hoge kosten, onvoldoende haalbaarheid, de mate van effectiviteit in de specifieke situatie, de levensfase van de desbetreffende ICT-voorzieningen, etc. Die factoren worden hier samengevat onder het begrip “randvoorwaarden”.

IB-FUNCTIES (definitie 803)

Een Informatiebeveiligings (IB-)functie is een logische groepering van geautomatiseerde activiteiten die een bepaald doel dienen in de informatiebeveiliging.

Deze doelen zijn in hoofdstuk 3 per IB-functie (zie figuur 5) geformuleerd als principes voor ICT-voorzieningen. De negen IB-functies als geheel worden dekkend geacht voor de informatiebeveiliging van die voorzieningen. De IB-functies zijn in de figuur geprojecteerd op de deelaspecten van informatiebeveiliging: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.



Figuur 5: IB-functies

De betekenis van de IB-functies kan als volgt worden toegelicht:

CONTINUÏTEITSVOORZIENINGEN (definitie 804)
Continuïteitsvoorzieningen zorgen ervoor dat de juiste informatie op het juiste moment beschikbaar komt voor de dienstverlening.

Zij voorkomen dat de dienstverlening door storingen en calamiteiten onaanvaardbaar lang stil komt te liggen. Maatregelen in dit kader zijn onder meer het dubbel uitvoeren van componenten, waardoor de ene component de functie van de ander kan overnemen bij uitval.

GEPROGRAMMEERDE CONTROLES (definitie 805)
Geprogrammeerde controles voeren automatische controles uit of leveren informatie voor het uitvoeren van handmatige controles door gebruikers of beheerders.

Geprogrammeerde controles in applicaties (daarom ook wel aangeduid als Application Controls) zijn onmisbaar om de integriteit van de informatie(voorziening) te waarborgen. Het spreekt voor zich dat geprogrammeeerde controles veel efficiënter én effectiever zijn dan handmatige controles. De betrouwbaarheid is simpelweg hoger. Het belang van geprogrammeerde controles neemt toe, omdat delen van de infrastructuur waarop de applicaties draaien, zich ook buiten de eigen beheeromgeving kunnen bevinden en dan extra risico's opleveren. Dat speelt vooral bij toepassingen die via internet lopen.

ZONERING (definitie 806)
Zonering is het afbakenen van delen van het netwerk waarbinnen gegevens vrijelijk kunnen worden uitgewisseld.

Informatie-uitwisseling naar buiten verloopt via koppelvlakken. Het primaire doel van zonering is isolatie van risico's, waardoor bedreigingen en incidenten in de ene zone niet doorwerken in een andere. Hierbij gaat het er niet alleen om de interne tegen de externe, onvertrouwde zone te beschermen, maar ook om interne zones (zoals ontwikkeling, test, acceptatie en productie-omgevingen) van elkaar te scheiden. Zonering maakt het voorts mogelijk om met verschillende beveiligingsniveaus binnen een infrastructuur te werken en informatiestromen en risicovolle beheercommando's te reguleren. Zonering is als middel om toegang tot voorzieningen te beperken op zich krachtiger dan toegangsbeveiliging via aanlogprocedures bij servers. Zonering maakt het netwerk overzichtelijker voor beheer en dat is tevens van belang voor beveiliging.

Elke zone kent dus andere risico's, die samenhangen met de diensten of ICT-voorzieningen die erin opgenomen zijn. Binnen zones kunnen met standaard maatregelen subzones worden ingericht als het risicoprofiel dat vereist. Bijvoorbeeld om verschillende productieomgevingen uit elkaar te houden, die niet het zelfde

beveiligingsniveau hebben. Externe netwerken worden in dit zoneringsconcept ook als aparte zone gezien.

FILTERING (definitie 807)
Filtering controleert informatiestromen op locatie, vorm (protocol) of inhoud van gegevens, afhankelijk van de aard van de informatiestromen en de zones waar ze vandaan komen of naar toe gaan.

Filtering beschermt zones tegen aanvallen, indringers, ongewenste inhoud en virussen, waardoor diensten onbereikbaar worden. Filtering controleert geen identiteiten van individuele gebruikers.

De communicatie tussen twee zones wordt getoetst op ongewenst gedrag. Daarvoor wordt een elektronisch profiel vastgelegd van de zenders in de betrokken zones. Van het communicatiegedrag wordt elektronisch een ‘reputatie score’ vastgelegd, die enerzijds wordt vergeleken met beleidsregels voor het doorlaten van communicatie en anderzijds met bekende patronen van ongewenste communicatie.

Bij end-to-end beveiliging waarbij de berichten of documenten zelf beveiligd zijn, zal minder filtering noodzakelijk zijn, maar dat doet vooralsnog niets af aan het zonerings- en filteringsconcept.

BEWIJSBAARHEID BERICHTUITWISSELING (definitie x808
Bewijsbaarheid van elektronische berichtuitwisseling houdt in dat:
- **De zender[6] van een bericht niet kan ontkennen een bepaald bericht verstuurd te hebben;**
- **De ontvanger van een bericht niet kan ontkennen het bericht van de zender in de oorspronkelijke staat te hebben ontvangen.**

Dit risico wordt door middel van wederzijdse authenticatie van zender en ontvanger aangevuld met controle op de integriteit van het bericht. Hiermee wordt een bericht *onweerlegbaar* verstuurd. Dit wordt ook wel non-repudiation genoemd. Dit kan met behulp een zogenoemde elektronische handtekening. Public Key Infrastructure (PKI) biedt de hiervoor benodigde technieken en organisatorische en procedurele maatregelen. Certificaten voor toepassing van PKI worden door onafhankelijke, voor deze dienstverlening gecertificeerde instanties verstrekt.

PKI is bedoeld voor onweerlegbaarheid van berichten over lange verwerkingsketens en onvertrouwde zones, waarmee rechten en verplichtingen worden aangegaan. PKI is niet bedoeld om de vertrouwelijkheid van de berichten te bewerkstelligen. Hiervoor worden voornamelijk encryptiemechanismen toegepast. Het ‘bewijs-element' van de elektronische handtekening wordt als een juridische log in de werkstroom van een informatieketen zodanig gecombineerd met de originele data bewaard, dat het bewijs altijd weer is te reproduceren. Een grote hoeveelheid voorwaarden voor onweerlegbaarheid is in wetgeving vastgelegd.

IDENTIFICATIE, AUTHENTICATIE, AUTORISATIE (definitie 809)
Identificatie, authenticatie, autorisatie zorgen ervoor dat altijd eerst logische toegangscontrole plaatvindt, voordat een persoon, organisatie of ICT-voorziening daadwerkelijk gebruik kan maken van een geautomatiseerde functie.

Deze functie wordt ook wel aangeduid met Identitity and Access Management (IAM).

De drie hier gebruikte begrippen zijn als volgt afzonderlijk toe te lichten:

6 Zender en ontvanger kunnen natuurlijke personen, organisaties of ICT-voorzieningen zijn.

- Identificatie is het bekend maken van de identiteit van personen, organisaties of ICT-voorzieningen: wie ben je?
- Authenticatie is het aantonen dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft: ben je het ook echt?
- Autorisatie is het controleren van rechten voor de toegang tot geautomatiseerde functies en/of gegevens in ICT-voorzieningen: mag je de gevraagde functies of gegevens wel benaderen en wat mag je ermee doen: raadplegen of ook muteren?

VASTLEGGEN VAN GEBEURTENISSEN (definitie 810)

Vastleggen van gebeurtenissen betreft het vastleggen van handelingen van natuurlijke personen en meldingen van besturingsprogrammatuur.

Een andere term voor het vastleggen van gebeurtenissen is logging. Voorbeelden van handelingen door natuurlijke personen zijn het wijzigen van parameters. Een foutmelding door een ICT-voorziening is een voorbeeld van een gebeurtenis.

Het vastleggen van gebeurtenissen is noodzakelijk om achteraf controle te kunnen uitoefenen en/of foutsituaties te kunnen uitzoeken. Het vastleggen is tevens noodzakelijk als bewijsmiddel voor private- of strafrechtelijke vordering.

Veel gebeurtenissen die voor het beheer van ICT-voorzieningen van belang zijn, hebben tevens betekenis in het kader van informatiebeveiliging.

Logging moet niet verward worden met het begrip audittrail, dat betrekking heeft op het vastleggen van mutaties op gegevensdragers (papier, record in database) die bij toepassingen behoren. Deze categorie vastleggingen valt onder het principe geprogrammeerde controles.

CONTROLE, ALARMERING EN RAPPORTAGE (definitie 811)

Controle, alarmering en rapportage zijn signaleringsfuncties die erop gericht zijn te kunnen vaststellen dat de ICT-voorzieningen overeenkomstig het operationeel beveiligingsbeleid functioneren.

De tooling die in de markt verkrijgbaar is, maakt het mogelijk al deze functies geïntegreerd te behandelen. Zonder integratie zijn deze functies niet effectief te beheersen. Om die reden worden de hier bedoelde signaleringsfuncties als één geheel behandeld.

De drie hier gebruikte begrippen zijn als volgt afzonderlijk toe te lichten:

- Controle is de toets of een ICT-voorziening is ingesteld conform een goedgekeurd operationeel beleidsdocument.
- Alarmering is een functie, die onmiddellijk signalen naar systeembeheerders kan afgeven als beleidsregels (grenswaarden) worden overschreden.
- Rapportering maakt het mogelijk beveiligingsincidenten, zoals hacking (ook van binnenuit) te onderkennen op basis van analyse en correlatie van vastleggingen.

SYSTEEMINTEGRITEIT (definitie 812)

Met systeemintegriteit wordt bedoeld dat de ICT-voorzieningen de beoogde bewerkingen foutloos uitvoeren.

De hier bedoelde borging blijft beperkt tot enkele specifieke aspecten, die niet logisch zijn onder te brengen onder de andere IB-functies.

2. Algemene beveiligingsprincipes

Algemene beveiligingsprincipes zijn principes, die in het algemeen gelden voor organisaties, waarin vertrouwen gesteld moet kunnen worden in het kader van dienstverlening aan burgers, bedrijven en andere overheidsorganisaties.

HOOFDVERANTWOORDELIJKE (principe 813)

De hoogstverantwoordelijke bij de dienstverlener is ook verantwoordelijk voor het informatiebeveiligingsbeleid.

Motivering

Informatiebeveiliging heeft betrekking op alle aspecten van de bedrijfsvoering. Beveiligingsmaatregelen maken namelijk onderdeel uit van organisatie, processen, mensen, inrichting en beheer van ICT, contracten, gebouwen en installaties. Maatregelen moeten onderling samenhangen en er kunnen keuzen worden gedaan hoe en waar ze geïmplementeerd worden. De eindverantwoordelijkheid hiervoor kan alleen op het hoogste bestuurlijke niveau in een organisatie worden gedragen.

Onderbouwing

Artikel 3 van het VIR stelt dat de Secretaris-Generaal het informatiebeveiligingsbeleid vaststelt, uitdraagt en hierover verantwoording aflegt.

AFLEGGEN VERANTWOORDING (principe 814)

Het jaarverslag van de dienstverlener bevat een verantwoording over het informatiebeveiligingsbeleid in de vorm van een 'in control statement'.

Motivering

Verantwoording in het jaarverslag zorgt voor transparantie ten aanzien van de prestaties van de organisatie op het gebied van informatiebeveiliging. Third Party Mededelingen in het besloten maatschappelijk verkeer door onafhankelijke auditors over de naleving van afspraken over informatiebeveiliging worden hiermee (in het kader van NORA) overbodig.

Onderbouwing

Dit principe is in opereenstemming met artikel 3 van het VIR en de toelichting daarop in het voorwoord. Het afleggen van verantwoording is voorts een invulling van het basisprincipe “betrouwbaar”: afnemers kunnen erop vertrouwen dat de dienstverlener zich aan afspraken houdt.

Implicaties

Voor veel overheidsorganisaties kan het opnemen van een ICS inzake informatiebeveiliging in het jaarverslag een aanzienlijke impact hebben, bijvoorbeeld als er geen Plan Do Check Act cyclus voor informatiebeveiliging is geregeld en/of de IT-auditor dit soort controle-opdrachten niet heeft. Naarmate een organisatie een hoger volwassenheidsniveau heeft ten aanzien van informatiebeveiliging, zal een ICS minder impact hebben. Bij een laag volwassenheidsniveau zal realisatie van dit principe een eigen groeipad vragen.

MANAGEMENTSYSTEEM VOOR INFORMATIEBEVEILIGING (principe 815)

Dienstverleners voldoen aan NEN-ISO 27001 [Code1].

Een managementsysteem voor informatiebeveiliging is gebaseerd op een Plan Do Check Act cyclus. In de Planfase stelt de lijnmanager op systematische wijze de

betrouwbaarheidseisen vast. In de Do-fase worden op basis van deze eisen de maatregelen in de informatiesystemen getroffen. In de Check-fase wordt gecontroleerd of de maatregelen het hele jaar zijn nageleefd. Dit is noodzakelijk omdat er gedurende een jaar allerlei wijzigingen kunnen plaatsvinden. Bovendien kan ook blijken dat de maatregelen in de praktijk niet tot het gewenste betrouwbaarheidseffect hebben geleid. Op basis van een evaluatie van onder meer de controleresultaten wordt nagegaan of de maatregelen en/of de betrouwbaarheidseisen moeten worden bijgesteld (Act).

Motivering

Voor het systematisch beheersen van eisen, normen en maatregelen van informatiebeveiliging is het noodzakelijk een Plan Do Check Act cyclus in te stellen. De norm NEN-ISO 27001 [Code1] geeft hiervan de uitwerking.

Onderbouwing

Forum Standaardisatie heeft deze NEN-norm aangemerkt als open standaard waarvoor het ‘pas toe of leg uit'-principe geldt.

Deze norm geeft invulling aan artikel 4 van het VIR.

Implicaties

De impact is sterk afhankelijk van het volwassenheidsniveau van een organisatie op het gebied van informatiebeveiliging en kan bij een laag niveau vragen om een langer groeipad.

BASELINE (principe 816)
De baseline beveiliging is gebaseerd op standaarden en best practices, in het bijzonder NEN-ISO 27002 [Code2].

Motivering

Door voor het merendeel van de informatiesystemen een interne baseline op te stellen kan veel gerichter binnen een organisatie worden gestuurd op gewenste en vereiste maatregelen. Door interne baselines minimaal op dezelfde standaard te baseren, ontstaat er een goede basis voor het onderlinge vertrouwen van in ketens samenwerkende organisaties.

Onderbouwing

Dit principe kan worden beschouwd als een nadere invulling van het NORA-basisprincipe 'Betrouwbaar: Afnemers kunnen erop vertrouwen dat de diensten zich aan afspraken houden', en is conform artikel 3.d van het VIR. Forum Standaardisatie heeft deze standaard aangemerkt als open standaard waarvoor het ‘pas toe of leg uit'-principe geldt.

Implicaties

Het opstellen van een interne baseline vergt een zorgvuldig proces en voldoende expertise. Voorts zal een interne baseline regelmatig moeten worden onderhouden, enerzijds wegens veranderingen van de externe bronnen, anderzijds op basis van evaluatie en interne beleidswijzigingen.

TREFFEN MAATREGELEN (principe 817)
Maatregelen voor informatiebeveiliging worden getroffen op basis van de interne baseline, aangevuld met een risicoanalyse in afwijkende situaties.

Voor het merendeel van de informatiesystemen worden de maatregelen getroffen op basis van de interne baseline. Per informatiesysteem moet echter wel worden vastgesteld of er

sprake is van afwijkende -risicovolle- situaties, waarvoor de baseline geen afdoende maatregelen biedt. Afwijkingen vergen maatwerk. In overleg met beveiligingsdeskundigen zullen compenserende maatregelen moeten worden getroffen.

Motivering

Het treffen van maatregelen op grond van een interne baseline voorkomt tijdrovende, integrale risicoanalyses per informatiesysteem, die afhankelijk van de gevolgde methodiek en betrokken medewerkers arbitrair kunnen uitpakken. Door het onderscheid te maken tussen standaard risico's (waarvoor de baseline geldt) en bijzondere risico's (waarvoor maatwerk aan de orde is), wordt een effectieve aanpak bij het treffen van maatregelen bevorderd.

Onderbouwing

Conform VIR artikel 3 lid a. Zie toelichting VIR in het geval dat een organisatie of organisatieonderdeel een baseline benadering wenst toe te passen.

Implicaties

Er moet in de organisatie een actuele, interne baseline zijn opgesteld en goedgekeurd. Bovendien moeten afwijkingen en de gevolgen daarvan voor te treffen maatregelen in kaart worden gebracht.

VERANTWOORDELIJKEN INFORMATIESYSTEMEN (principe 818)
Lijnmanagers zijn verantwoordelijk voor de beveiliging van informatiesystemen.

Motivering

Een (interne) beveiligingsfunctionaris wordt normaliter verantwoordelijk gesteld voor de informatiebeveiliging in een organisatie. Deze functionaris kan echter uitsluitend een adviserende en toetsende rol vervullen, omdat informatiebeveiliging betrekking heeft op alle aspecten van de bedrijfsvoering en er een integraal onderdeel van uitmaakt. Daarbij zijn er allerlei keuzes te maken met soms verstrekkende gevolgen voor organisatie, processen, personeel, ICT-voorzieningen, etc. Alleen de lijnmanager kan deze keuzes maken en alle tegengestelde belangen (kosten en regels stellen versus baten en vrijheid van handelen) afwegen. Het begrip lijnmanagement wordt hierbij ruim opgevat. In voorkomende gevallen kan ook een afdelingshoofd of een manager van een stafafdeling onder het lijnmanagement worden verstaan.

Onderbouwing

Conform artikel 4 van het VIR.

Implicaties

Er moet een toedeling van verantwoordelijkheden voor informatiebeveiliging plaatsvinden, die samenhangt met de primaire verantwoordelijheidsverdeling in een organisatie. Indien er keuzes zijn te maken voor maatregelen in verschillende verantwoordelijkheidsgebieden, moet er op het hoogste niveau in een organisatie een sturend en coördinerend beveiligingsorgaan worden ingesteld om belangenconflicten te voorkomen of in goede banen te leiden.

Functionarissen informatiebeveiliging hebben een adviserende en toetsende rol.

3. Principes ICT-voorzieningen

Standaardisatie van beveiligingsnormen voor ICT-voorzieningen is voor de afstemming van e-dienstverlening tussen organisaties van groot belang. In dit hoofdstuk zijn daarvoor principes geformuleerd, in aanvulling op de ISO-NEN 27002 [Code2]. Daarbij is uitgegaan van de negen IB-functies, zoals beschreven in hoofdstuk 1.

In dit hoofdstuk worden principes voor de beveiliging van ICT-voorzieningen als een samenhangend geheel uitgewerkt. De principes, behalve die gaan over geprogrammeerde controles, hebben betrekking op de instelmogelijkheden van algemeen, op de markt verkrijgbare, ICT-componenten. Het instellen van ICT-voorzieningen kan door parametrisering: het kiezen uit variabelen, die verschillende geautomatiseerde functies aansturen. De principes hebben eveneens betrekking op de wijze waarop afzonderlijke ICT-voorzieningen gegroepeerd worden ingezet, bijvoorbeeld in netwerkzones.

De implicaties van de principes zijn verder uitgewerkt tot implementatierichtlijnen in een NORA best practice [NIBI], waardoor duidelijk wordt wat ermee wordt bedoeld. In deze best practice is de referentie naar de ISO-NEN 27002 [Code2] gedocumenteerd.

Voor het handhaven van deze op de techniek gerichte principes zijn beheerprocedures randvoorwaardelijk. Deze zijn in de ISO-NEN 27002 [Code2] dan wel in ander ISO-NEN-materiaal of via de NORA onvoldoende vanuit de optiek van beveiliging behandeld. De beroepsorganisaties NOREA en PvIB hebben deze beheerprocedures vanuit de optiek van beveiliging uitgewerkt in een eigen publicatie, die als NORA-dossier is opgenomen, zie [NBUI].

CONTINUÏTEITSVOORZIENINGEN (principe 819)
De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid.

Motivering

Deze maatregelen voorkomen dat verstoringen en calamiteiten in de ICT tot gevolg hebben dat de dienstverlening onaanvaardbaar lang niet ondersteund wordt.

Implicaties

In de ISO-NEN 27002 [Code2] zijn onder het hoofd 'Fysieke beveiliging en beveiliging van de omgeving' veel preventieve maatregelen opgenomen, die van belang zijn voor de beschikbaarheid van de ICT-voorzieningen. Denk aan maatregelen gericht op onderbrekingsvrije stroomvoorziening, klimaatbeheersing, brandpreventie, waterdetectie, toegangsbeperking, etc. Onder dit principe worden alleen ICT-maatregelen opgesomd, die in de ISO-NEN 27002 [Code2] ontbreken en in de praktijk inmiddels gangbaar zijn:

- Door dubbele uitvoering van ICT-voorzieningen of onderdelen daarvan worden single points of failure vermeden.
- Verwerkingen zijn herstelbaar.
- ICT-voorzieningen anticiperen op dreigende discontinuïteit van die voorzieningen.
  Toelichting: Denial of Service attacks (het onbereikbaar maken van een dienst door een overvloed aan berichten te sturen) en controles op te grote omvang van e-mailberichten zijn specifiek van betekenis voor de beschikbaarheid van de ICT-voorzieningen, maar worden vanwege de samenhang van maatregelen behandeld bij het principe Filterfuncties.

GEPROGRAMMEERDE CONTROLES (principe 820)

In toepassingsprogrammatuur worden geprogrammeerde controles opgenomen, gericht op invoer, verwerking en uitvoer.

Motivering

Geprogrammeerde controles bieden de beste waarborgen dat de integriteit van de informatie(voorziening) gehandhaafd kan worden.

Implicaties

In de ISO-NEN 27002 [Code2] worden de geprogrammeerde controles beperkt uitgewerkt in hoofdstuk 12.2: Correcte verwerking in toepassingen. Een verdergaande uitwerking leidt tot de volgende implicaties:

- Niemand in een organisatie of proces mag op uitvoerend niveau in staat worden gesteld om een gehele cyclus van handelingen te beheersen.
- Alle ingevoerde gegevens vanuit een systeemvreemde omgeving worden op juistheid, tijdigheid en volledigheid gecontroleerd voordat verdere verwerking plaatsvindt.

De uitvoerfuncties van programma's maken het mogelijk om de juistheid en volledigheid van de gegevens bij ontvangst in een systeemvreemde omgeving te kunnen vaststellen.

- Toepassingen bieden mogelijkheden om te constateren dat alle ter verwerking aangeboden invoer juist, volledig en tijdig is verwerkt.
- Kritische gegevens (bjivoorbeeld identificerende en financiële gegevens), die in verschillende gegevensverzamelingen voorkomen, worden periodiek met elkaar vergeleken, tenzij inconsistenties per definitie niet kunnen voorkomen.
- In applicaties zijn geen functies opgenomen, waarvoor kwalitatief betere generieke voorzieningen beschikbaar zijn, zoals die voor identificatie, authenticatie, autorisatie, onweerlegbaarheid en encryptie.

ZONERING (principe 821)

ICT-voorzieningen zijn in zones ingedeeld.

Motivering

Door zonering kunnen risico’s worden geïsoleerd, waardoor bedreigingen en incidenten die optreden in de ene zone niet doorwerken in een andere zone.

Implicaties

In de ISO-NEN 27002 [Code2] wordt de zonering beperkt uitgewerkt. Een meer systematische benadering van het zoneringsconcept leidt tot de volgende implicaties:

- De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd.
- Zones zijn als eenheid van beveiliging en beheer gedefinieerd.
- De communicatie en de opslag van gegevens die buiten de invloedssfeer van de logische en fysieke toegangsbeveiliging vallen of waarvoor deze maatregelen onvoldoende zijn, zijn door encryptie beschermd.
- De sterkte van de encryptiemechanismen voldoet aan eisen van de tijd.
- De vertrouwelijkheid en integriteit van geheime cryptografische sleutels is gewaarborgd tijdens het gehele proces van generatie, transport en opslag van de sleutels.

FILTERING (principe 822)

Op het koppelvlak tussen zones zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens.

Motivering

Filterfuncties zijn onlosmakelijk verbonden aan het principe van zonering en ontlenen daaraan ook hun motivering.

Implicaties

In de ISO-NEN 27002 [Code2] worden filterfuncties beperkt uitgewerkt. Een meer systematische uitwerking leidt tot de volgende implicaties:

- In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om aanvallen te signaleren en te kunnen blokkeren die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is (Distributed Denial of Service attacks).
- Al het gegevensverkeer vanuit externe of onvertrouwde zones wordt real-time inhoudelijk geïnspecteerd op inbraakpogingen. Een update van de aanvalspatronen vindt frequent geautomatiseerd plaats.
- E-mail-berichten met bijlagen worden uitsluitend doorgelaten op basis van geformaliseerde afspraken over het formaat van de bijlage. Het formaat van een bijlage wordt door een inhoudelijke inspectie vastgesteld.
- E-mail-berichten met een omvang boven een vastgestelde grenswaarde worden geblokkeerd om problemen wegens onbeschikbaarheid te voorkomen.
- Er is antivirusprogrammatuur actief die e-mail-berichten met een kwaadaardige code (virussen, wormen, trojans, spyware, etc.) in zowel ontvangen als verzonden e-mails blokkeert. Een update van antivirusdefinities vindt zeer frequent geautomatiseerd plaats.
- Er is een (spam)filter geactiveerd voor zowel ontvangen als verzonden berichten. Een update van het spamfilter vindt periodiek geautomatiseerd plaats.
- Op alle werkstations is antivirusprogrammatuur resident actief. Een update van virusdefinities en/of antivirusprogrammatuur kan op ieder moment (handmatig) uitgevoerd worden en vindt periodiek geautomatiseerd plaats.
- Alle PC-servers worden periodiek geautomatiseerd gecontroleerd op virussen, nadat een update van de virusdefinities en/of antivirusprogrammatuur geautomatiseerd plaats heeft gevonden. De controle moet op ieder gewenst tijdstip ook handmatig gestart kunnen worden.
- In een keten van zones wordt antivirusprogrammatuur van verschillende leveranciers toegepast.

BEWIJSBAARHEID BERICHTUITWISSELING (principe 823)

Bij berichtuitwisseling wordt de bewijsbaarheid van verzending en ontvangst geborgd.

Motivering

Als er geen specifiek daarop afgestemde maatregelen zijn, wordt het risico gelopen dat een ontvanger van een bericht kan ontkennen ooit een bericht te hebben ontvangen of kan ontkennen een bericht te hebben ontvangen met de inhoud zoals deze door de verzender is verstuurd. In het elektronisch berichtenverkeer zijn aanmerkelijk meer risico's in deze te onderkennen dan in het fysieke postverkeer.

Onderbouwing

In de ISO-NEN 27002 [Code2] wordt deels een referentie gevonden. In de Wet op de Elektronische Handtekening zijn de eisen opgenomen, waaraan een elektronische handtekening moet voldoen om als bewijs te kunnen dienen.

Implicaties

Met deze bewijsbaarheid wordt het volgende bereikt:

- Bij berichtuitwisseling waaruit rechten en plichten ontstaan tussen partijen bestaat de zekerheid dat het ontvangen bericht afkomstig is van de verzender en dat de inhoud niet door derden is beïnvloed.
- Bij berichtuitwisseling waaruit rechten en plichten ontstaan tussen partijen kan de ontvanger van het bericht niet ontkennen het bericht te hebben ontvangen van de afzender.
- De beschikbaarheid van bewijs is gewaarborgd binnen de termijn waarin de aantoonbaarheid van dat bewijs noodzakelijk wordt geacht door de systeemeigenaar.

IDENTIFICATIE, AUTHENTICATIE EN AUTORISATIE (principe 824)
Vóór het gebruiken van ICT-voorzieningen vindt logische toegangscontrole plaats.

Motivering

Het kunnen handhaven van functiescheiding, de herleidbaarheid van handelingen en het beperken van de toegang tot gegevens behoren tot de belangrijkste maatregelen van informatiebeveiliging. Identificatie, authenticatie en autorisatie zijn de functies waarmee aan deze doeleinden invulling kan worden gegeven.

Implicaties

Dit principe is op vergelijkbaar niveau uitgewerkt in de ISO-NEN 27002 [Code2]. Samenvattend leidt dit principe tot de volgende implicaties:

- Alle toegangsvragers tot een geheel van ICT-voorzieningen zijn uniek herleidbaar tot één natuurlijk persoon, organisatie of ICT-voorziening.
- Alvorens een systeem toegang verleent, wordt de authenticiteit van de gebruiker vastgesteld op basis van de identificatie.
- Het systeem dwingt het gebruik van sterke wachtwoorden af.
- Instellingen met betrekking tot het aanmelden op een systeem zijn erop gericht te voorkomen dat iemand werkt onder een andere dan de eigen gebruikersnaam.
- Op alle ICT-voorzieningen is toegangsbeveiliging van toepassing op basis van: “Niets mag, tenzij dit is toegestaan”.
- Er zijn maatregelen getroffen die onbedoeld gebruik van toegekende autorisaties voorkomen.
- Handelingen worden uitgevoerd met zo weinig mogelijk rechten.
- Verleende toegangsrechten zijn inzichtelijk en beheersbaar.

VASTLEGGEN VAN GEBEURTENISSEN (principe 825)
Handelingen in en meldingen van ICT-voorzieningen in de technische infrastructuur worden vastgelegd in logging.

Motivering

Het vastleggen van meldingen van besturingsprogramma's en andere systemen in de technische infrastructuur is noodzakelijk om achteraf controle te kunnen uitoefenen en/of foutsituaties te kunnen uitzoeken. Het vastleggen is tevens noodzakelijk als bewijsmiddel

voor private of strafrechtelijke vordering.

Implicaties

In de ISO-NEN 27002 [Code2] is dit type maatregelen op vergelijkbare wijze opgenomen:

- In de logging wordt informatie vastgelegd waarmee reproduceerbaar is wie waar en wanneer welke cruciale handelingen heeft verricht.
- De integriteit van opgeslagen logbestanden is gewaarborgd.
- De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht.

CONTROLE, ALARMERING EN RAPPORTERING (principe 826)
In de technische infrastructuur zijn signaleringsfuncties werkzaam ter controle op operationeel beveiligingsbeleid.

Motivering

Dit type maatregelen is noodzakelijk om verstoringen in de productieverwerking te voorkomen of om beveiligingsrisico's in de werking van een infrastructuur te kunnen beheersen.

Implicaties

- Instellingen van functies die voor de informatiebeveiliging van belang zijn en wijzigingen daarin worden automatisch gecontroleerd.
- Tevoren gespecificeerde afwijkende gebeurtenissen volgens de loginformatie worden tijdig gesignaleerd en zo nodig gealarmeerd.
- Logbestanden worden periodiek geanalyseerd en gecorreleerd ten einde beveiligingsincidenten dan wel de juiste werking van het systeem te detecteren.

SYSTEEMINTEGRITEIT (principe 827)
In de technische infrastructuur zijn functies werkzaam, die de systeemintegriteit ondersteunen.

Motivering

In de huidige technologie resteren een aantal risico´s, die onder de noemer van systeemintegriteit als kapstokbegrip onder implicaties zijn aangegeven. Deze restrisico's zijn aan de praktijk ontleend.

Implicaties

De implicaties zijn deels in de ISO-NEN 27002 [Code2] benoemd. Een meer systematische benadering van het zoneringsconcept leidt tot de volgende implicaties:

- De instellingen (parametrisering) van de programmatuurpakketten doorbreken - voor zover ze niet bepaald zijn door de andere principes - de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid niet. Toelichting: Het is niet mogelijk voor alle beveiligingsrelevante instellingen productonafhankelijke normen te formuleren, dus is het noodzakelijk alle overige instellingen op beveiligingsaspecten te bezien.
- Programmatuurpakketten zijn ingesteld volgens de aanwijzingen van de leverancier.
- Als gebruik van 'mobile code' is toegelaten, zorgt de configuratie ervoor dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid en voorkomt de configuratie dat onbevoegde 'mobile code' wordt uitgevoerd. Toelichting: 'Mobile code' is programmatuur die kan worden overgedragen van de ene naar de andere computer, die automatisch wordt uitgevoerd en die een specifieke functie verricht zonder of met weinig

tussenkomst van de gebruiker. ‘Mobile code’ werkt samen met besturingsprogrammatuur (zogenoemde middleware) die de informatie-uitwisseling regelt tussen de cliënt-software en de software die de bedrijfsgegevens beheert. Vaak gaat het om gedistribueerde systemen en meer platforms.

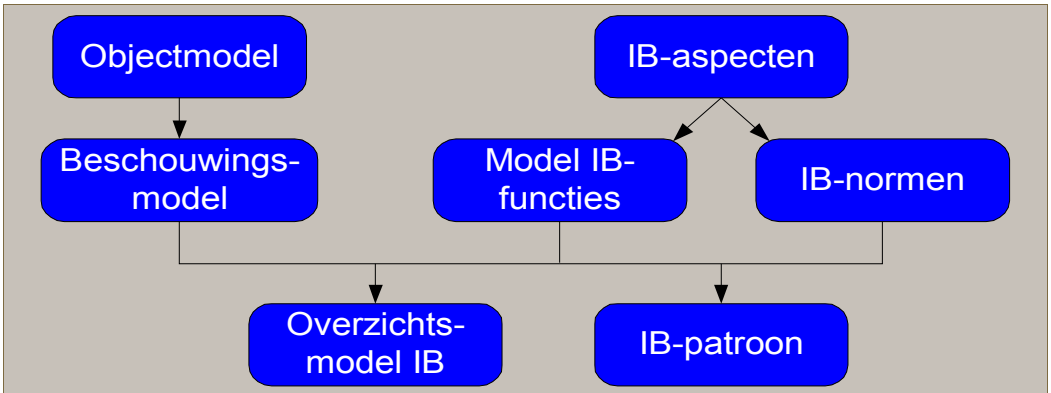
- De technische infrastructuur is zodanig ontworpen en ingericht, dat foutsituaties worden voorkomen of herkend en dat functioneel beheer over foutbestanden mogelijk is.
- Bij batchverwerking borgen de generieke productieplannings- en/of bewakingssystemen dat invoerbestanden niet of dubbel worden verwerkt, dat uitvoerbestanden niet of dubbel worden verzonden en dat onderlinge afhankelijkheid van de verwerkingen niet wordt doorbroken.

4. Basismodellen informatiebeveiliging in de ICT-voorzieningen

In dit hoofdstuk wordt een modelleringsaanpak behandeld die de verbinding legt tussen de principes van ICT-beveiliging volgens hoofdstuk 3 en de ICT-objecten, die aan deze principes moeten voldoen. Het geeft inzicht en overzicht en maakt de principes hanteerbaar. Beveiligingsdeskundigen kunnen deze modellen gebruiken bij analyse, advies en toetsing. Deze modelleringsaanpak kan ook in projecten worden toegepast voor het ontwikkelen van een architectuur van de concrete IB-oplossingen.

Modelleringsaanpak

Voordat de verschillende stappen in de modelleringsaanpak worden beschreven, wordt eerst in figuur 6 een kort overzicht van deze stappen gegeven.



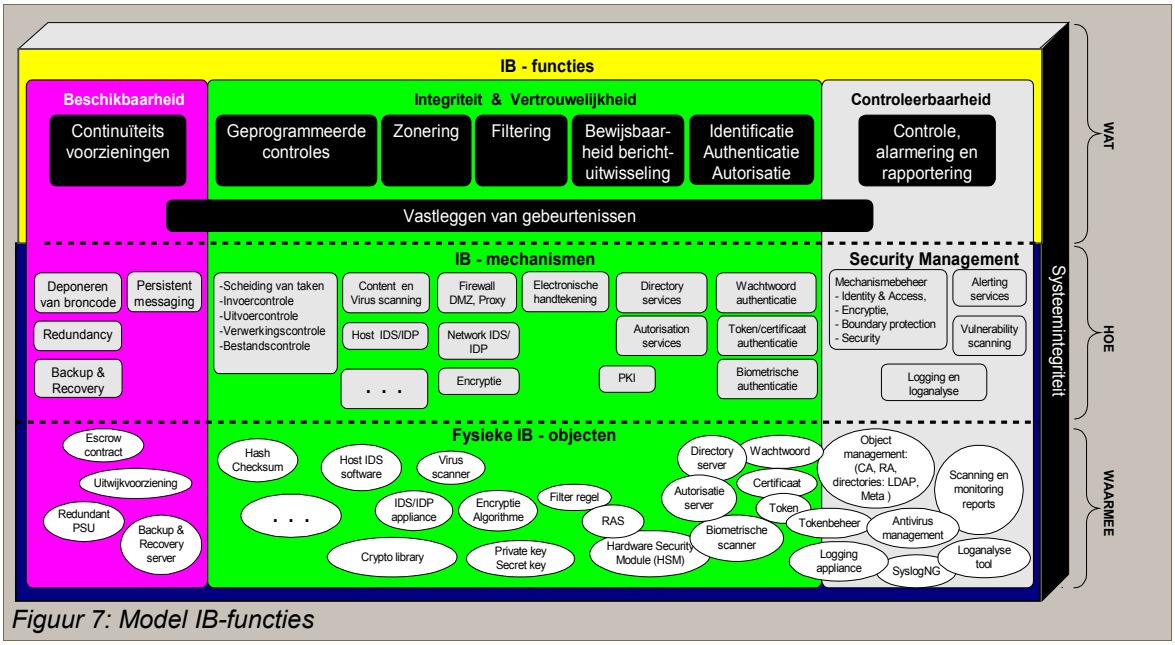
Figuur 6: NORA-aanpak IB-architectuur

De principes voor ICT-voorzieningen zijn nader geconcretiseerd in een Model IB-functies. In hoofdstuk 3 is voor elke IB-functie een principe geformuleerd. Bij deze principes zijn implicaties aangegeven, die in een NORA best practice [NIBI] nog een niveau dieper zijn uitgewerkt naar implementatierichtlijnen per implicatie. Het geheel van principes, implicaties en implementatierichtlijnen geven we in de figuur aan met IB-normen.

Omdat beveiliging een aspect is van de bedrijfsvoering, is er een objectmodel nodig om te laten zien waar de principes c.q. functies werkzaam moeten zijn. Architectuur als objectmodel is meestal niet direct geschikt om IB-functies op te projecteren. Daarom wordt eerst een beschouwingsmodel gemaakt, waarin de belangrijkste ordening voor ICT-beveiliging is verwerkt: de netwerkzonering (als IB-functie). Tussen dit beschouwingsmodel en de IB-functies worden de relaties gelegd, waaruit een architectuur voor Informatiebeveiliging kan ontstaan. Voor een globaal inzicht worden IB-functies op de gehele architectuur geprojecteerd. Voor meer details worden IB-patronen gebruikt. Een IB-patroon is een abstractie van een probleem en oplossing binnen een bepaalde context waardoor de oplossing algemener inzetbaar wordt. Patronen zijn te beschouwen als bouwstenen op architectuurniveau. De hier geschetste modelleringsaanpak wordt momenteel verder uitgebouwd door het modelleren van veel voorkomende beveiligingssituaties. Daarvoor is een community opgericht onder de vlag van de beroepsvereniging Platform voor Informatiebeveiliging, die de IB-patronen uitwerkt. Deze komen als best practices ten behoeve van NORA ter beschikking, zie [IBPTR].

Model IB-functies

Het vertrekpunt voor de modelleringsaanpak wordt gevormd door het model IB-functies, dat is bedoeld als voertuig om te ordenen en te verbinden (zie Figuur 7). Dit model is een eigen doorontwikkeling van ISO-NEN 7498-2 OSI-Basisreferentiemodel - Beveiligingsarchitectuur 1991.

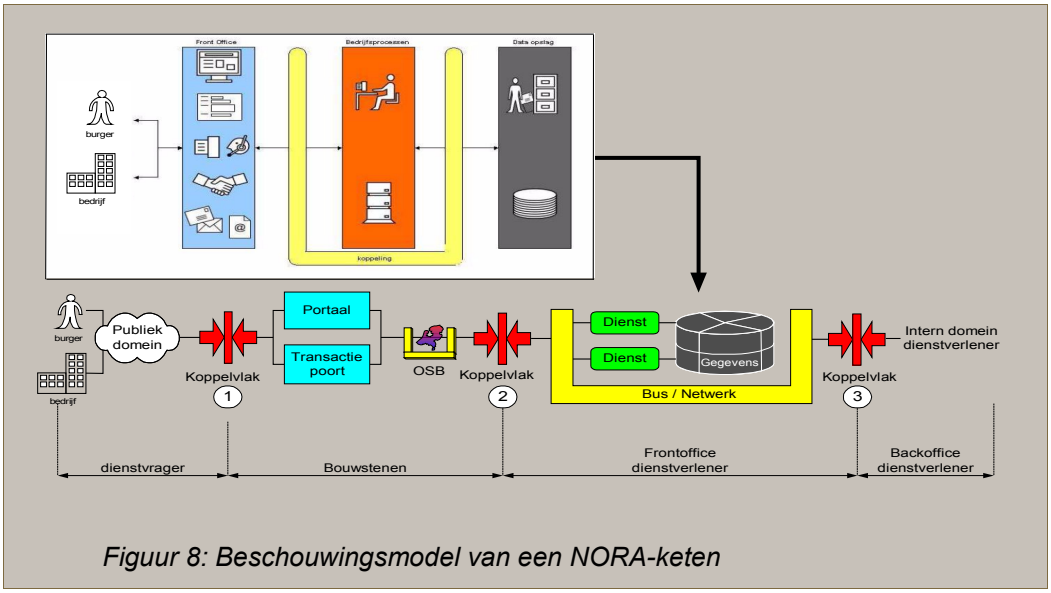


Figuur 7: Model IB-functies

De IB-functies en bijbehorende mechanismen en objecten zijn in deze figuur voor de eenvoud op de criteria geprojecteerd, die ze primair ondersteunen. De functies voor Integriteit en Vertrouwelijkheid bijvoorbeeld dragen immers ook bij aan het deelaspect Beschikbaarheid. De IB-mechanismen vormen de HOE-laag, waarmee technische concepten (technieken) worden bedoeld, die het WAT van de IB-functies invullen. Hiervoor zijn NORA best practices uitgewerkt (zie [NIBI]). Omdat techniek zich steeds verder ontwikkelt, illustreert de figuur slechts een aantal bekende voorbeelden. Fysieke IB-objecten, de “WAARMEE”-laag in het model, zijn ICT-onderdelen die de IB-mechanismen daadwerkelijk uitvoeren. Ze kunnen onderdeel zijn van een besturingsprogramma of een applicatie, maar ze kunnen ook als afzonderlijke fysieke modules zijn uitgevoerd. In een referentiearchitectuur is het feitelijk niet passend om dit niveau te beschrijven. Het dient hier als voorbeeld om concreet te maken hoe een beveiligingsfunctie uiteindelijk werkzaam kan zijn in de ICT.

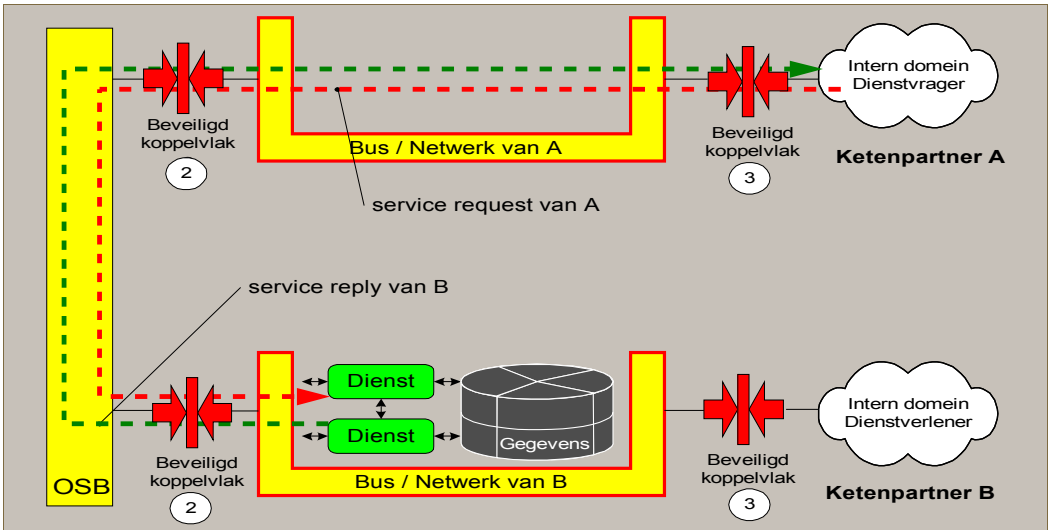
Stap 1: Beschouwingsmodel maken

Architectuurmodellen van ICT-voorzieningen zijn zelden rechtstreeks geschikt om IB-functies op te projecteren. Daarom wordt in de modelleringsaanpak eerst een beschouwingsmodel gemaakt. Als voorbeeld gebruiken we de Basisarchitectuur overheidsorganisatie (zie Strategisch katern) als objectmodel. Op deze basisarchitectuur worden de te beveiligen zones geprojecteerd met koppelvlakken daartussen, zie Figuur 8 Beschouwingsmodel van een NORA keten. De koppelvlakken zijn voor de herkenbaarheid genummerd.



Figuur 8: Beschouwingsmodel van een NORA-keten

In het beschouwingsmodel is aan de voorkant van de keten (links) de aanvrager van de overheidsdiensten en rechts de dienstverlener gepositioneerd. In veel gevallen zal een dienstverlener echter ook zelf overheidsdiensten willen afnemen en dus tevens als dienstvrager fungeren. Een voorbeeld daarvan (als afgeleide van het beschouwingsmodel) is geschetst in Figuur 9: Ketenpartner B fungeert als dienstverlener voor ketenpartner A.



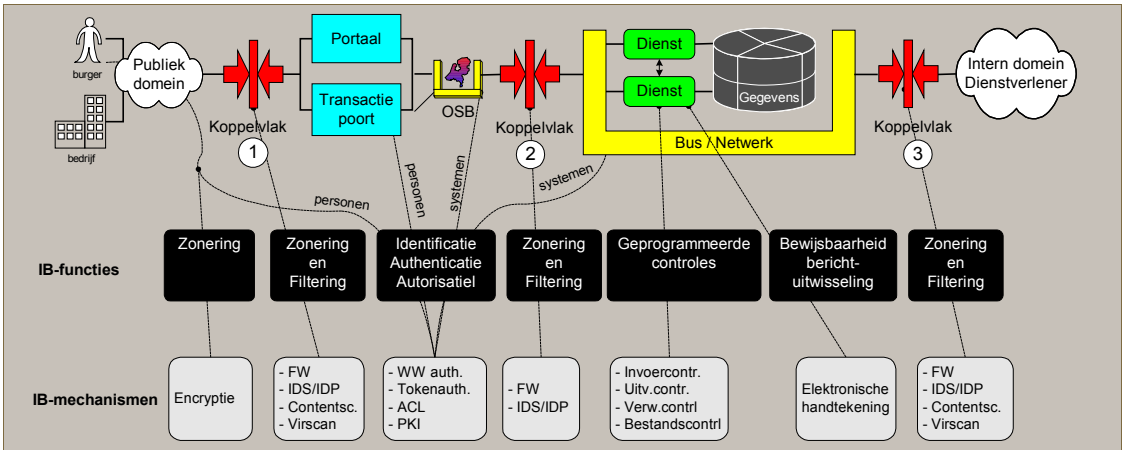
Figuur 9: Ketenpartner B fungeert als dienstverlener voor ketenpartner A

Aangegeven is hoe ketenpartners via de Overheid Service Bus (OSB) informatie kunnen uitwisselen. Ketenpartner A zet een vraag naar informatie uit op de OSB en ontvangt vanuit ketenpartner B een bericht terug. De OSB fungeert hier als netwerk met een routeringsfunctie voor berichten.

Stap 2: Projecteren IB-functies

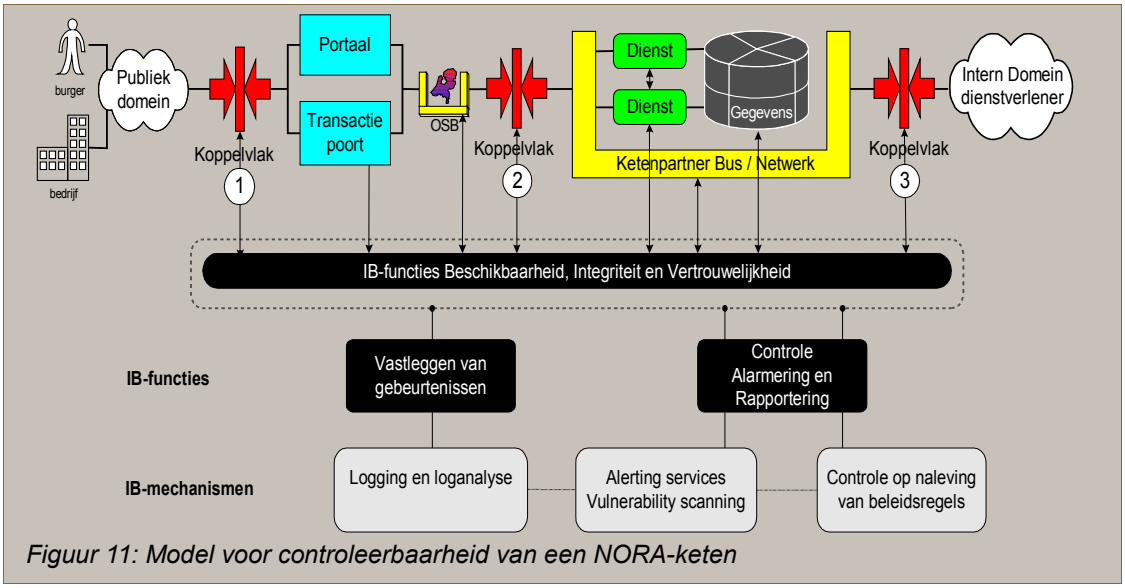
Uitgaande van het beschouwingsmodel voor een NORA-keten (Figuur 8) kunnen de IB-functies hierop worden geprojecteerd. Afhankelijk van de positionering ten opzichte van dit beschouwingsmodel kunnen de IB-functies met hun verschillende IB-mechanismen worden gerealiseerd. Op dit globale niveau is het niet zinvol fysieke IB-objecten van het functiemodel in dit overzichtsmodel te betrekken.

De overzichtsmodellen zijn uitgewerkt voor de aspecten Integriteit, Vertrouwelijkheid en Controleerbaarheid. Beschikbaarheid leent zich minder goed voor uitwerking in een dergelijk abstract model. Daarvoor is een gedetailleerder, meer fysiek georiënteerd model nodig, zoals een configuratieschema.



Figuur 10: Model voor Integriteit en vertrouwelijkheid van een NORA-keten

Figuur 10 schetst de positionering van IB-functies voor de aspecten integriteit en vertrouwelijkheid in de NORA-keten. Voor betrouwbare communicatie tussen burger en overheid is encryptie toegepast, waardoor een vertrouwd toegangspad tot het portaal van de overheid wordt verkregen. Vanaf het portaal is er sprake van een besloten netwerk tot aan de interne zone van de ketenpartner: ook dit kan als een vertrouwd toegangspad worden beschouwd, mede door de daarin gepositioneerde andere IB-functies.



Figuur 11: Model voor controleerbaarheid van een NORA-keten

Figuur 11 geeft aan welke IB-functies voor controleerbaarheid werkzaam zijn in een NORA-keten. IB-mechanismen voor Integriteit en Vertrouwelijkheid worden ingesteld en beheerd door afzonderlijke tools of met tooling die in de ICT-voorzieningen zelf is geïntegreerd.

Beveiligingsgebeurtenissen die in de ICT-keten hebben plaatsgevonden, worden vastgelegd voor controledoeleinden. Dit vastleggen (loggen) vereist aparte infrastructurele voorzieningen. Wanneer drempelwaarden van bijvoorbeeld een firewall, IDS of virusscanner

worden overschreden, moet een mechanisme kunnen zorgdragen voor alarmering naar systeembeheer of een CERT[7].

Net als voor de criteria Integriteit en Vertrouwelijkheid worden voor Controleerbaarheid door de keten heen steeds dezelfde functies toegepast, maar de toegepaste mechanismen en objecten kunnen verschillen.

7 Computer Emergency Rescue Team

Bijlage I: Participanten

Leden van de NORA-expertgroep Informatiebeveiliging

Annemarie v.Grunsven (Prov. Utrecht), Bart Bokhorst (ICTU - Programma RENOIR – trekker), Bart v.Staveren (UWV), Carl Adamse (BZK), Jaap Hoekman (Nijmegen Universiteit), Jan Breeman (BKWI), Jan Harskamp (Gemeente Woerden), Kees Terlouw (Vts Politie Nederland), Niko Visser (Kadaster), Peter Arxhoek (GBO), David Campbell (RAD), Henk-Jan vd.Molen (IVW), Jaap vd.Veen (Belastingdienst), Thomas Wijsman (Rekenkamer), Tim Berkelaar (ICTU - Programma RENOIR).

Auteurs NORA-katern Informatiebeveiliging

Bart Bokhorst (ICTU - Programma RENOIR), Jaap van der Veen (Belastingdienst), Jasper van Lieshout (ICTU - Programma RENOIR).

Sponsors

De Belastingdienst treedt op als sponsor door detachering van de trekker bij het kenniscentrum.

Diverse bijdragen aan NORA-katern

Piet Goeyenbier (RAD), Boris Goranov (Siemens), Rob Kloots (CSF).

Reviewers

Wordt nog ingevuld na openbare review

Bijlage II: Overige begrippen

BESCHIKBAARHEID (definitie 828)
Beschikbaarheid is de waarborg, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (waaronder informatiesystemen).

CONTROLEERBAARHEID (definitie 829)
Controleerbaarheid is de mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere "werkelijkheden of representaties daarvan", zodat objectieve oordeelsvorming mogelijk wordt.

Dit aspect is feitelijk een onderdeel van de andere aspecten en is daarom arbitrair om te onderscheiden. Tegelijkertijd leert de praktijk dat controleerbaarheid lang niet altijd als vanzelfsprekend in beschouwing wordt genomen. In de ICT leidt controleerbaarheid bovendien vaak tot apart te onderscheiden functies, zoals vastlegging van systeemgebeurtenissen.

ICT-VOORZIENING (definitie 830)
Een ICT-voorziening is een hardware- en/of software-component.

Voorbeelden hiervan zijn PC's, servers, firewalls, netwerkapparatuur, besturingssystemen, database management systemen, programmapakketten, beheer- en beveiligingstools, applicaties en opslagmedia.

INFORMATIESYSTEEM (definitie 831)
Een informatiesysteem is een samenhangend geheel van gegevensverzamelingen, gegevensstromen, gegevensverwerkende activiteiten en de bij het systeem betrokken mensen, procedures, processen, programmatuur en technische voorzieningen voor opslag, verwerking en communicatie.

Een informatiesysteem is niet per definitie een geautomatiseerd (digitaal) systeem. Werken met papieren documenten valt eveneens onder de reikwijdte van deze definitie.

INTEGRITEIT (definitie 832)
Integriteit is het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan.

Ook tijdigheid wordt wel apart onderscheiden als onderdeel van het aspect integriteit.

KOPPELVLAKKEN (definitie 833)
Een koppelvlak is de voor gegevensuitwisseling bedoelde toegangs- en vertrekpoort van een zone, waar gegevens gefilterd kunnen worden en waar gegevens niet omheen kunnen.

PARAMETRISEREN (definitie 834)
Parametrisering is het kiezen uit variabelen, die verschillende geautomatiseerde functies aansturen.

TECHNISCHE INFRASTRUCTUUR (definitie 835)
Het geheel van generieke ICT-voorzieningen waarop de toepassingen draaien.

VERTROUWELIJKHEID (definitie 836)
Vertrouwelijkheid is het waarborgen dat informatie alleen toegankelijk is voor diegenen, die hiertoe zijn geautoriseerd.

Het gaat hier onder andere om het beveiligen van gebouwen, informatiesystemen en ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, trojan horses). Maar ook om maatregelen, die ervoor zorgen dat eigen medewerkers geen toegang krijgen tot informatie die niet voor hen is bedoeld. Techniek speelt bij dit aspect een grote rol in de randvoorwaardelijke sfeer.

Bijlage III: Bronnen

Wetten

[WCC] Wet Computer Criminaliteit II 1999 (wijziging van div. bestaande wetten)

[WBP] Wet Bescherming Persoonsgegevens 2000

[WEH] Wet Elektronische Handtekeningen 2003

[WEB] Wet Elektronisch Bestuurlijk Verkeer 2003

Besluiten

[VB WBP] Vrijstellingsbesluit WBP 2001

[BEH] Besluit Elektronische Handtekeningen 2003

[VIR-BI] Besluit Voorschrift Informatiebeveiliging Rijksdienst–Bijzondere Informatie 2004

[VIR] Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR)

Standaarden

[CODE1] Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen NEN-ISO/IEC 27001:2005 nl

[CODE2] Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging NEN-ISO/IEC 27002:2007 nl

NORA-dossiers

[IB PTR] *IB-patronen*, https://www.surfgroepen.nl/sites/NORA-architecten/NORA-forum/review.aspx

[NVIB] *Katern Informatiebeveiliging – Verantwoording*, https://www.surfgroepen.nl/sites/NORA-architecten/NORA-forum/review.aspx

[NBUI] *Normen voor de beheersing van uitbestede ICT-beheerprocessen*, NOREA/PvIB 2007, gratis te downloaden: https://www.pvib.nl/boeken#ICT-beheerprocessen

[NIBI] *Normen Informatiebeveiliging ICT-voorzieningen*, https://www.surfgroepen.nl/sites/NORA-architecten/NORA-forum/review.aspx

Verwijzingen

[1] *Website RENOIR.* http://www.e-overheid.nl/sites/renoir

[2] *Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties*. Kamerstuk 26 643,nr 136. http://www.overheid.nl/op/

[3] *Brief minister BZK over grote ICT-projecten*. Kamerstuk 26 643, nr. 128

[4] *Website Nationaal Uitvoeringsprogramma Dienstverlening en e-overheid*. http://www.e-overheid.nl/sites/nup

[5] J. Rothenberg, M. Botterman & C. van Oranje-Nassau. *Towards a Dutch Interoperability Framework. Recommendations to the Forum Standaardisatie*. (2008) http://www.rand.org/pubs/technical_reports/2008/RAND_TR552.pdf

[6] *Model Architectuur RIJksdienst (MARIJ)*. (2007) Kamerstuk 26 643, nr. 98. http://www.e-overheid.nl/atlas/referentiearchitectuur/marij

[7] UWV, *Jaarverslag 2008, paragraaf 4.3 Risicomanagement en 4.7 Gegevensbeveiliging*

[8] *Informatietechnologie - Service management - Deel 1: Specificatie* NEN-ISO/IEC 20000-1:2006 nl

[9] *Informatietechnologie - Service management -Deel 2: Praktijkcode* NEN-ISO/IEC 20000-2:2006 nl

[10] *de Bruin et al, Ketengovernance, startpunt voor keteninrichting en ketenauditing, de EDP-auditor, nummer 1 2006*