DE ONDERZOEKSRAAD
VOOR VEILIGHEID

Het DigiNotarincident

Waarom digitale veiligheid de bestuurstafel te weinig bereikt

HET DIGINOTARINCIDENT
Waarom digitale veiligheid de bestuurstafel te weinig bereikt

Den Haag, juni 2012 (projectnummer S20110V0902-03)

DE ONDERZOEKSRAAD VOOR VEILIGHEID

In Nederland wordt er naar gestreefd het gevaar van ongevallen en incidenten zoveel mogelijk te beperken. Wanneer het toch (bijna) misgaat, kan herhaling voorkomen worden door, los van de schuldvraag, goed onderzoek te doen naar de oorzaak. Het is dan van belang dat het onderzoek onafhankelijk van de betrokken partijen plaatsvindt. De Onderzoeksraad voor Veiligheid kiest daarom zelf zijn onderzoeken en houdt daarbij rekening met de afhankelijkheidspositie van burgers ten opzichte van overheden en bedrijven. De Onderzoeksraad is in een aantal gevallen wettelijk verplicht onderzoek te doen.

Bezoekadres:	Anna van Saksenlaan 50 2593 HT Den Haag	Postadres:	Postbus 95404 2509 CK Den Haag
Telefoon:	+31 (0)70 333 7000	Telefax:	+31 (0)70 333 7077
Internet:	www.onderzoeksraad.nl		

INHOUD

BESCHOUWING

In onze samenleving, die in hoog tempo digitaliseert, neemt digitale veiligheid een steeds belangrijker positie in. De overheid heeft een bijzondere verantwoordelijkheid bij het beveiligen van digitale gegevens die zij onder zich heeft. Waar burgers en bedrijven in onderling verkeer vrij zijn om te kiezen met wie zij hun gegevens wel en niet uitwisselen, geldt dat de overheid hen verplicht tot het beschikbaar stellen van gegevens. Dit betekent dat burgers en bedrijven er van op aan moeten kunnen dat de overheid alles in het werk stelt om deze gegevens zo goed mogelijk te beschermen tegen verlies en misbruik.

Digitale certificaten zijn een belangrijk instrument in het bieden van deze bescherming. De inbraak bij DigiNotar en de nasleep daarvan wierpen vragen op over de mate waarin de betrouwbaarheid van het instrument digitale certificaten gewaarborgd wordt. Bovendien ontstond kort na het incident ophef over de algemene staat van de beveiliging van onder meer gemeentelijke websites en netwerken. Beide gebeurtenissen gaven de Onderzoeksraad aanleiding tot zorg over de mate waarin en de wijze waarop overheden invulling geven aan hun verantwoordelijkheid voor de digitale veiligheid van burgers en bedrijven.

De rijksoverheid heeft zelf een vergelijkbare zorg, getuige het aantal onderzoeken dat op last van het kabinet werd verricht naar digitale veiligheid en naar de betrouwbaarheid van certificaatdienstverlening. De Onderzoeksraad is door de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie verzocht een onderzoek uit te voeren. Gezien het belang van digitale veiligheid en de bijzondere verantwoordelijkheid die de overheid heeft in het waarborgen daarvan, heeft de Onderzoeksraad in dit verzoek bewilligd. De Onderzoeksraad acht het van belang dat lessen uit het DigiNotarincident worden getrokken zodat op basis daarvan de digitale veiligheidszorg door overheidsorganisaties kan worden verbeterd.

Het onderzoek van de Onderzoeksraad verkent enerzijds hoe overheidsorganisaties op bestuurlijk niveau digitale veiligheid borgen en wat hierbij de knelpunten zijn. Anderzijds richt het zich op de rol van de overheid als schepper van randvoorwaarden voor digitale veiligheid. Hier richt de aandacht van de Onderzoeksraad zich vooral op de betrouwbaarheid van digitale certificaten en de rol die de overheid daarin speelt.

Inbraak bij DigiNotar en gevolgen
In de maanden juni en juli van 2011 drong een inbreker door tot de computersystemen van het bedrijf DigiNotar B.V. Dit bedrijf leverde digitale certificaten, die gebruikt worden om elektronisch gegevensverkeer te beschermen. De inbreker slaagde erin vervalste certificaten te genereren en in omloop te brengen. Daardoor ontstond het risico dat de gegevens van burgers en bedrijven onderschept zouden worden, hetgeen kan leiden tot misbruik van gegevens, privacyschending, identiteitsfraude en financiële schade.

Het leveren, beschikbaar stellen en gebruiken van digitale certificaten vindt plaats in een stelsel van afspraken, partijen en technologieën dat wordt aangeduid als een public key infrastructure (PKI). De inrichting van een PKI voorziet erin dat een leverancier van certificaten in wie niet langer vertrouwen bestaat, uit het stelsel verwijderd wordt. De certificaten die hij tot dan toe heeft uitgegeven worden dan onbruikbaar. Partijen moeten dan overschakelen op certificaten van een andere leverancier. In het geval van de inbraak bij DigiNotar bleek dat een dergelijke ingreep niet zonder ernstige complicaties mogelijk was. De continuïteit van diverse essentiële gegevensstromen met en tussen overheidsorganisaties bleek ernstig in gevaar te komen als alle door DigiNotar uitgegeven certificaten onbruikbaar zouden worden gemaakt. Omvangrijke economische schade en maatschappelijke ontwrichting zouden hiervan mogelijk het gevolg zijn geweest.

DigiNotar leverde onder meer PKIoverheid-certificaten. Dit zijn certificaten bestemd voor het beschermen van het elektronisch gegevensverkeer met en tussen overheidsorganisaties. De Staat der Nederlanden staat voor de betrouwbaarheid van deze certificaten in.

Na de inbraak kon de Staat der Nederlanden echter niet meer garanderen dat een burger of bedrijf, door gebruik te maken van door DigiNotar geleverde PKIoverheid-certificaten, veilig met de overheid kon communiceren.

Het DigiNotarincident kon ontstaan doordat de betrokken overheidsorganisaties ervan uitgingen dat de certificaatdienstverlening door het bedrijf in orde was. De opdrachtgever namens de minister van Binnenlandse Zaken en Koninkrijksrelaties (Logius) en de toezichthouder (OPTA) vertrouwden primair op het bedrijf en toetsing door een externe auditor. Hierdoor hadden deze overheidsorganisaties beperkt zicht op de feitelijke bedrijfsvoering van DigiNotar, terwijl dat bedrijf veiligheidskritische diensten levert die raken aan vitale belangen van de overheid.

Evenmin bleken overheidsorganisaties werkelijk rekening te hebben gehouden met de mogelijkheid dat een certificaatdienstverlener als DigiNotar gecompromitteerd raakt, waardoor goede, proportionele maatregelen ontbraken om de gevolgen van zo'n gebeurtenis effectief te beheersen. Uiteindelijk is succesvol voorkomen dat de gebeurtenissen bij DigiNotar leidden tot grote maatschappelijke ontwrichting. Deze uitkomst is te danken aan een goed vermogen tot improviseren bij de betrokken overheidsorganisaties.

Reeds getroffen maatregelen en andere onderzoeken
De gebeurtenissen bij DigiNotar hebben velen binnen de overheid wakker geschud en hebben een impuls gegeven aan allerlei initiatieven om een soortgelijke situatie in de toekomst beter het hoofd te kunnen bieden. Het belang van digitale veiligheid heeft, sinds het incident, duidelijk de aandacht van het kabinet, parlement en vele overheidsorganisaties.

Op last van het kabinet zijn verschillende onderzoeken naar certificaatdienstverlening uitgevoerd. Die hebben geleid tot het afkondigen van diverse maatregelen die een verbetering beogen van de beveiliging van gegevensverkeer met en tussen overheidsorganisaties, zoals het aanscherpen van het Programma van Eisen PKIoverheid, een duidelijker rolverdeling tussen de betrokken partijen en strikter toezicht door OPTA en Logius. Deze maatregelen zijn naar de mening van de Onderzoeksraad zinvol. De Onderzoeksraad is evenwel van oordeel dat van een structureel veiliger digitale overheid pas sprake kan zijn als ook de oorzaken van het ontstaan van problemen worden weggenomen. Daarvoor is meer nodig dan de maatregelen die het kabinet al heeft genomen.

De vraag die de Onderzoeksraad heeft gesteld is, hoe het kon gebeuren dat partijen weinig kritisch optraden en gemakkelijk vertrouwen stelden in het functioneren van het certificatenstelsel. Dit is in een situatie waar zoveel op het spel staat immers opmerkelijk en riskant. Het antwoord op deze vraag vormt de sleutel tot verbetering van de digitale veiligheid bij de Nederlandse overheid. De Onderzoeksraad onderscheidt twee belangrijke factoren.

Gebrekkig zicht op risico's bij bestuurders en ambtelijk opdrachtgevers
Ten eerste stelt de Onderzoeksraad vast dat de bij PKIoverheid betrokken partijen onvoldoende zicht hadden op factoren die de betrouwbaarheid van digitale certificaten bedreigen. Noch de minister van Binnenlandse Zaken en Koninkrijksrelaties als stelselverantwoordelijke, noch de andere betrokken partijen hebben voorafgaand aan de inbraak bij DigiNotar nagedacht over hoe de betrouwbaarheid van digitale certificaten – en daarmee de veiligheid van het elektronisch gegevensverkeer – in gevaar konden komen. Doordat de risico's niet werkelijk bekend waren, kon het gebeuren dat er onvoldoende preventieve maatregelen genomen werden en de maatregel die voorzien was bij incidenten niet adequaat en heel riskant bleek te zijn. Het uitvoeren van het voorziene scenario had kunnen leiden tot grootschalige uitval van vitale systemen en daarmee tot maatschappelijke ontwrichting.

Ook bij de onderzochte gemeenten blijkt sprake van een gebrekkig inzicht in de risico's die digitale veiligheid bedreigen. Alleen ten aanzien van de omgang met de Gemeentelijke Basisadministratie persoonsgegevens, waarop stringente wettelijke vereisten van toepassing zijn, worden risico's door toepassing van veiligheidsmanagement systematisch geïnventariseerd en beheerst. Het systematisch waarborgen van digitale veiligheid in andere gegevensverwerkende processen vindt in veel mindere mate plaats. Risicobewustzijn is hoofdzakelijk aanwezig bij de ICT-afdeling, en nauwelijks bij de top van de ambtelijke organisatie of het college van burgemeester en wethouders.

Bij de onderzochte uitvoerende overheidsdiensten, de Belastingdienst en de Sociale Verzekeringsbank, is een intensiever digitale veiligheidszorg aangetroffen. Een ongestoorde digitale gegevensverwerking is cruciaal voor de bedrijfscontinuïteit van deze organisaties. ICT en veiligheid is daarom een thema dat bij hen veel operationele en ook bestuurlijke aandacht krijgt.

Bestuurlijk onvermogen tot het nemen van verantwoordelijkheid
Ten tweede is uit het onderzoek gebleken dat er grote verschillen zijn in de manier waarop overheidsorganisaties digitale veiligheid bestuurlijk-organisatorisch borgen. In organisaties waar gegevensverwerking centraal staat in het primaire proces, zoals de Sociale Verzekeringsbank en de Belastingdienst, trof de Onderzoeksraad een sterkere bestuurlijke en operationele betrokkenheid bij digitale veiligheid aan dan bij organisaties waar dit minder het geval is. Bij deze laatste overheidsorganisaties is het bestuur en het hoger management vaak nog weinig betrokken bij het borgen van digitale veiligheid, terwijl dat naar het oordeel van de Onderzoeksraad wel nodig is. Alleen bij een groter incident zoals DigiNotar of de Lektober-actie komt het onderwerp op dat niveau in beeld.

Door recente incidenten dringt op bestuurlijk niveau meer en meer het besef door dat digitale veiligheid een bestuursaangelegenheid is, die niet alleen aan een ICT-afdeling kan worden overgelaten. De realisatie van digitale veiligheid vergt immers niet alleen technische oplossingen. Op bestuurlijk niveau moet beleid worden vastgesteld en moet besloten worden welke risico's voor digitale veiligheid op welke wijze en tot welk niveau worden beheerst. Bestuurders voelen zich echter niet altijd in staat om hun verantwoordelijkheid voor digitale veiligheid goed in te vullen. Op bestuurlijk niveau beschikken overheidsorganisaties vaak over te weinig kennis om effectief sturing te kunnen geven aan een systematische beheersing van de risico's die digitale veiligheid bedreigen, of zelfs maar te bepalen welke informatie zij hiervoor nodig hebben. Het is van belang dat bestuurders voldoende inzicht hebben in de cruciale aspecten van digitale veiligheid om de goede vragen te kunnen stellen, zodat zij zich ervan kunnen vergewissen dat digitale veiligheid in hun organisatie voldoende gewaarborgd is.

Tekort aan inzicht in digitale veiligheid op bestuurlijk en managementniveau leidt tot gebrekkig opdrachtgeverschap. Een goed opdrachtgever moet doelen kunnen formuleren en eisen kunnen stellen. Wil hij werkelijk verantwoordelijkheid kunnen nemen voor zijn opdracht, dan moet hij zich er door het stellen van de juiste vragen van kunnen vergewissen dat conform die opdracht gehandeld wordt, in plaats van daarop zonder meer te vertrouwen. Bij veel bestuurders en ambtelijk opdrachtgevers is dit momenteel onvoldoende het geval. Dikwijls wordt digitale veiligheid als gevolg daarvan 'overgelaten' aan degenen die daarmee operationeel zijn belast. De Onderzoeksraad is van oordeel dat bestuurders nadrukkelijker hun verantwoordelijkheid moeten nemen voor het waarborgen van digitale veiligheid. Enkele van de aanbevelingen bij dit rapport zijn hierop gericht.

Wat is nodig?
Het Diginotarincident heeft een impuls gegeven aan allerlei initiatieven om een soortgelijke situatie in de toekomst beter het hoofd te kunnen bieden. Voor de Onderzoeksraad staat, gezien het bovenstaande, voorop dat het bestuurlijk niveau binnen overheidsorganisaties nadrukkelijk verantwoordelijkheid neemt voor en sturing geeft aan digitale veiligheidszorg. De aanbevelingen bij dit rapport richten zich dan ook op de emancipatie van de digitale veiligheidszorg als een centraal proces in de bedrijfsvoering, dat een vergelijkbare mate van bestuurlijke betrokkenheid behoeft als bijvoorbeeld het financieel beheer.

Hiervoor is nodig dat bestuurders een betekenisvolle eindverantwoordelijkheid nemen voor digitale veiligheid, en daarover ook verantwoording afleggen. Een voorwaarde is dat op bestuurlijk niveau een zodanige mate van inzicht in en kennis over digitale veiligheid bestaat dat hieraan sturing gegeven kan worden, bijvoorbeeld door het stellen van de juiste vragen aan operationele afdelingen.

De enige manier om risico's zo goed mogelijk te beheersen, is door het toepassen van digitaal veiligheidsmanagement. Dit houdt volgens de Onderzoeksraad in dat de risico's verbonden aan de digitalisering in kaart worden gebracht en worden gewogen, dat maatregelen worden genomen om de risico's zoveel mogelijk te verminderen en dat de consequenties van de risicoafweging expliciet in ogenschouw worden genomen. Deze stappen moeten continu deel uitmaken van het organisatieproces. Een verantwoordingsplicht kan bestuurders stimuleren om een dergelijk beleid te ontwikkelen en toe te passen.

Bijzondere aandacht binnen de digitale veiligheidszorg behoeft de notie dat 100% veiligheid net als bij fysieke veiligheid niet bestaat. Schadebeperking en herstel moeten daarom naast preventie een centrale positie innemen in elk digitaal veiligheidsbeleid. De minister van Binnenlandse Zaken en Koninkrijksrelaties geeft er in haar brief van 14 maart 2012 over de onderzoeken naar aanleiding van DigiNotar blijk van het belang van deze perspectiefwisseling te zien. De Onderzoeksraad is van oordeel dat het voor een structurele verbetering van de digitale veiligheid bij overheidsorganisaties van belang is deze notie handen en voeten te geven. Overheidsorganisaties zouden in hun handelen expliciet uit moeten gaan van het gegeven dat volledig veilig elektronisch gegevensverkeer niet bestaat. Er is immers altijd sprake van een restrisico. Overheidsorganisaties moeten niet alleen voorzien in een zo goed mogelijke beveiliging van de gegevens die zij onder zich hebben, maar ook terughoudend omgaan met het verzamelen en uitwisselen ervan. Dit betekent dat de negatieve risico's die met de gegevensverwerking gepaard gaan, expliciet worden afgewogen tegen de voordelen van een dergelijke verwerking. Deze weging zou telkens expliciet op bestuurlijk niveau gemaakt moeten worden. Ook moeten herstelmogelijkheden zijn voorzien voor wanneer gegevens gecompromitteerd raken. Deze moeten zich richten op een zo snel mogelijk herstel van de beveiliging van het elektronisch gegevensverkeer en op het bieden van een doeltreffende oplossing aan burgers of bedrijven die schade geleden hebben. Met deze maatregelen kan er voor worden zorg gedragen dat burgers en bedrijven vertrouwen blijven houden in de wijze waarop de overheid met de digitale veiligheid van de gegevens van haar burgers en bedrijven omgaat.

Een belangrijke les die uit het Diginotarincident getrokken kan worden, is dat de veiligheid van digitale certificaten wordt ondergraven wanneer de betrokken overheids- en marktpartijen zich te zeer terugtrekken op hun formele rol, in plaats van gezamenlijk verantwoordelijkheid te nemen voor een veilige certificaatdienstverlening. De Onderzoeksraad merkt op dat het voor het leren van incidenten noodzakelijk is de gebeurtenissen in ogenschouw te nemen zonder te denken in termen van schuld. Alleen dan is een dialoog tussen betrokken partijen mogelijk met als gezamenlijk belang het bijdragen aan een betere borging van digitale veiligheid binnen de overheid.

Ter afsluiting: verantwoordelijkheid in een complex bestuurlijk landschap
In het voorgaande vraagt de Onderzoeksraad aandacht voor het belang van bestuurlijke betrokkenheid bij het waarborgen van digitale veiligheid. Echter, de vraag kan ook worden gesteld of de complexe structuur van de publieke sector in Nederland het nemen van verantwoordelijkheid door bestuurders niet onnodig bemoeilijkt. Nog altijd is daar de tendens om allerlei (faciliterende) taken te bundelen in afzonderlijke organisaties, en die vervolgens op afstand te plaatsen van degenen voor wie zij hun taken verrichten. Hierdoor ontstaat het gevaar dat deze taken ervaren worden 'van niemand te zijn'.

Met het bovenstaande wil de Onderzoeksraad niet suggereren dat het vervangen van 'verticale verantwoordelijkheid' (eigenaarschap) door 'horizontale verantwoordelijkheid' (opdrachtgeverschap) zonder meer een slechte zaak is. Integendeel: wanneer organisaties hun krachten bundelen en bepaalde taken gezamenlijk uitvoeren, kunnen zij ook profiteren. Zeker wanneer het gaat om taken die een zekere massaliteit kennen en een gering aantal vrijheidsgraden in hun uitvoering vertonen, kan op deze manier grote efficiency- en kwaliteitswinst worden bereikt.

Volgens de Onderzoeksraad is het van belang dat partijen in de publieke sector, alvorens te besluiten tot ingrijpende taakverschuivingen, expliciet stilstaan bij de vraag hoe en bij wie de bestuurlijke verantwoordelijkheid terecht moet komen, en wat dat voor implicaties heeft. Zo wordt gewaarborgd dat de verantwoordelijke bestuurder zijn verantwoordelijkheid ook ten volle kan waarmaken.

AANBEVELINGEN

De Onderzoeksraad richt zijn aanbevelingen in dit onderzoek op overheidsorganisaties. De reden hiervoor is dat overheidsorganisaties zelf verantwoordelijk zijn voor het veilig beheer van de gegevens die zij onder zich hebben. Als zij ervoor kiezen externe partijen hierbij te betrekken moeten zij zich er als goed opdrachtgever van vergewissen dat deze partij aan de door hen gestelde eisen en doelen voldoet.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties

1. **Zorg dat bestuurders van alle overheidsorganisaties hun verantwoordelijkheid nemen voor het beheersen van digitale veiligheid.**

   Daartoe moet u een programma ontwikkelen dat bestuurders van overheidsorganisaties doordringt van het belang van digitale veiligheid, en hen voorziet van voldoende inzicht en vaardigheden om hen in staat te stellen actief sturing te geven aan de beheersing van digitale veiligheid in hun organisatie.

   Ook moet u overheidsorganisaties verplichten om zich te verantwoorden over de wijze waarop zij digitale veiligheid waarborgen. Veranker daartoe een duidelijk omschreven openbare verantwoordingsplicht op het gebied van digitale veiligheid in de planning & controlcyclus van overheidsorganisaties, en laat bestuurders van overheidsorganisaties jaarlijks een ‘in control statement’ voor digitale veiligheid afgeven.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties; aan de minister van Veiligheid en Justitie

2. **Schep voorwaarden zodat overheidsorganisaties hun digitale veiligheid systematisch beheersen.**

   Hiertoe moet u ervoor zorgen dat alle overheidsorganisaties de open standaarden NEN-ISO/IEC 27001 en 27002 naleven, die gezamenlijk een kader voor systematische digitale veiligheidszorg bieden. Stel daarvoor een plan op waarin concrete doelen, maatregelen en een tijdspad worden benoemd. Wijs bovendien een organisatie aan die overheidsorganisaties kan begeleiden bij het tot stand brengen van adequate digitale veiligheidszorg.

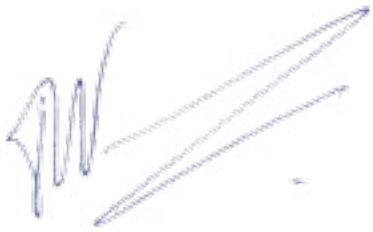
   Als onderdeel van een dergelijke systematische aanpak moet vanuit gemeenten, veiligheidsregio’s en het Rijk aandacht bestaan voor het voorbereid zijn op, en het herstellen van schade als gevolg van, digitale incidenten. Burgers en bedrijven wier gegevens door een digitaal veiligheidsincident zijn getroffen, moeten kunnen volstaan met dit één keer te melden waarna adequate maatregelen moeten worden getroffen door alle betrokken overheids-organisaties.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties; aan de minister van Economische Zaken, Landbouw en Innovatie

3. Realiseer een veiliger uitgifte en gebruik van digitale certificaten.

Pas hiervoor de rol van OPTA en Logius zodanig aan, dat sprake is van werkelijk toezicht op en handhaving van de feitelijke naleving door certificaatdienstverleners van de vigerende regelgeving ten aanzien van gekwalificeerde en PKIoverheid-certificaten.

Bevorder daarnaast een cultuuromslag bij alle partijen die bij certificaatdienstverlening betrokken zijn, in het bijzonder ten aanzien van het melden en leren van incidenten. Maak daarbij gebruik van ervaringen met veilig melden uit andere sectoren.



mr. T.H.J. Joustra
Voorzitter van de Onderzoeksraad

mr. M. Visser
Algemeen secretaris

LIJST VAN AFKORTINGEN

BAG	Basisregistratie Adressen en Gebouwen
B&W	Burgemeester en wethouders
BRP	Basisregistratie personen
COBIT	Control Objectives for Information and related Technology
CWA	CEN Workshop Agreement
DUO	Dienst uitvoering onderwijs
e-NUP	Nationaal uitvoeringsprogramma dienstverlening en e-overheid
ETSI	European Telecommunications Standards Institute
GBA	Gemeentelijke basisadministratie persoonsgegevens
GovCert	Government Computer Emergency Response Team
ICT	Informatie- en communicatietechnologie
i-NUP	Implementatie-agenda nationaal uitvoeringsprogramma
IWI	Inspectie Werk en Inkomen (per 1 januari 2012 opgegaan in Inspectie SZW)
KING	Kwaliteitsinstituut Nederlandse gemeenten
KCC	Klantcontactcentrum
NCC	Nationaal Crisiscentrum
NCSC	Nationaal Cyber Security Centrum
NCSR	Nationale Cyber Security Raad
NHR	Nieuw Handelsregister
NORA	Nederlandse Overheid Referentie Architectuur
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
PvIB	Platform voor informatiebeveiliging
RI&E	Risico-inventarisatie en -evaluatie
RNI	Registratie niet-ingezetenen
RvA	Raad voor Accreditatie
SLA	Service level agreement
SVB	Sociale Verzekeringsbank
TTP	Trusted third party
VIAG	Vereniging van coördinatoren Informatievoorziening en Automatisering in Nederlandse Gemeenten
VIR	Voorschrift informatiebeveiliging rijksdienst
VMS	Veiligheidsmanagementsysteem
VNG	Vereniging Nederlandse Gemeenten
Wet SUWI	Wet structuur uitvoeringsorganisatie werk en inkomen
Wbp	Wet bescherming persoonsgegevens
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

LIJST VAN BEGRIPPEN

BAPI-certificaat
De Belastingdienst Advanced Program Integration (BAPI) is de basis voor de digitale communicatie met de Belastingdienst om als ondernemer of belastingconsulent belastingaangifte te doen. Met deze methode kunnen gegevens veilig worden verstuurd en ontvangen. BAPI maakt gebruik van certificaten die voor de versleuteling en ondertekening zorgen.

Certificaat (digitaal certificaat)
Een elektronisch document dat de identiteit bevestigt van de persoon of instelling die een publieke sleutel beschikbaar stelt voor het versleutelen van elektronisch gegevensverkeer. Een certificaat heeft een beperkte geldigheidsduur en kan voor verschillende beveiligingsdoeleinden worden afgegeven.

Certificaatdienstverlener (certificate service provider)
Een natuurlijke of rechtspersoon die zich bezighoudt met het leveren van digitale certificaten en diensten die daarmee verband houden. In de Telecommunicatiewet en afgeleide regelgeving aangeduid als certificatiedienstverlener.

Certificaatherroepingslijst (certificate revocation list)
Een lijst die elke certificaatdienstverlener bijhoudt, waarop alle certificaten zijn opgenomen die tijdens hun periode van geldigheid zijn ingetrokken.

Certificate Policy (CP)
Een schriftelijk vastgelegde verzameling regels die de toepasbaarheid van een certificaat aangeeft voor een bepaalde gemeenschap en/of toepassingsklasse met gemeenschappelijke beveiligingseisen. Met behulp van een CP kunnen eindgebruikers en vertrouwende partijen bepalen hoeveel vertrouwen zij kunnen stellen in de relatie tussen de publieke sleutel en de identiteit van diens houder.

Certification practice statement (CPS)
Beleid van een certificaatdienstverlener, waarin deze aangeeft hoe hij invulling geeft aan de certificate policy.

Geheime sleutel (private key)
Een alleen aan de eigenaar van een sleutelpaar bekende code, met behulp waarvan gegevens ontcijferd respectievelijk versleuteld kunnen worden. Deze gegevens kunnen alleen versleuteld zijn c.q. ontcijferd worden met de corresponderende publieke sleutel, die voor iedereen toegankelijk is.

Gekwalificeerd certificaat
Een digitaal certificaat dat voldoet aan de vereisten die bij en krachtens de Telecommunicatiewet worden gesteld. Dit zijn eisen aan het certificaat zelf en eisen aan de wijze van uitgifte. Een gekwalificeerd certificaat kan worden gebruikt om een rechtsgeldige elektronische handtekening te zetten.

PKIoverheid
De public key infrastructure die de rijksoverheid heeft ingericht en onderhoudt. PKIoverheid heeft primair de verlening van certificaatdiensten aan overheidsorganisaties ten doel, maar ook private partijen kunnen PKIoverheid-certificaten gebruiken.

Public key infrastructure
Een stelsel van afspraken, technologieën en partijen dat ten doel heeft om betrouwbare versleuteling van elektronisch gegevensverkeer mogelijk te maken door de relatie te waarborgen tussen een publieke sleutel en de identiteit van diens eigenaar.

Publieke sleutel (public key)
Een voor iedereen toegankelijke code met behulp waarvan gegevens versleuteld resp. ontcijferd kunnen worden. Deze gegevens kunnen alleen ontcijferd worden c.q. versleuteld zijn met de corresponderende geheime sleutel, die alleen de eigenaar van het sleutelpaar kent.

SSL-certificaat
Een digitaal certificaat dat bestemd is voor de authenticatie van een domeinnaam op internet.

Stamcertificaat
Een digitaal certificaat dat zijn betrouwbaarheid niet ontleent aan het feit dat het ondertekend is met behulp van een ander, 'hoger' certificaat. Het stamcertificaat is de hoogste bron van vertrouwen in een hiërarchische vertrouwensketen.

Stelsel
Het geheel van actoren wier handelen een bepaald doel dient, tezamen met de regels en afspraken die dit handelen en hun onderlinge verhoudingen bepalen.

Trusted third party (TTP)
Een partij die het vertrouwen waarborgt tussen partijen in een elektronische omgeving. Een certificaatdienstverlener is een voorbeeld van een trusted third party.

TTP.NL-verklaring
Een verklaring, af te geven door een hiertoe bevoegde instelling, dat het managementsysteem van een certificaatdienstverlener in overeenstemming is met – onder meer – de vereisten in de ETSI-normen TS 101 456 en TS 102 042. Het onderzoek ter verkrijging van deze verklaring wordt uitgevoerd op grond van het certificeringsschema TTP.NL. Aan de verklaring mag volgens dit schema een gerechtvaardigd vertrouwen (justified confidence) worden ontleend dat de certificaatdienstverlener aan de vereisten in eerder genoemde ETSI-normen voldoet.

1 INLEIDING

In een nachtelijke persconferentie op 3 september 2011 maakte de minister van Binnenlandse Zaken en Koninkrijksrelaties bekend dat een digitale inbraak was gepleegd bij certificaatdienstverlener DigiNotar B.V. (verder: DigiNotar). Hierdoor waren vervalste certificaten in omloop gekomen.

Digitale certificaten spelen een cruciale rol in het beveiligen van elektronische gegevensuitwisseling via het internet. Als vervalste certificaten in omloop komen, komt de vertrouwelijke uitwisseling van gegevens onder druk te staan. De vertrouwelijkheid van die gegevens kan dan niet meer worden gegarandeerd en gegevens kunnen in verkeerde handen vallen, of door onbevoegden gemanipuleerd worden. DigiNotar leverde zowel eigen certificaten als certificaten voor PKIoverheid. Dit zijn certificaten die specifiek bestemd zijn voor het beschermen van elektronisch gegevensverkeer met en tussen overheidsorganisaties. DigiNotar was één van de acht partijen die deze certificaten namens de rijksoverheid uitgaf.

Op 19 en 20 juli 2011 ontdekte DigiNotar dat vervalste certificaten waren gegenereerd op zijn systemen. Het bedrijf heeft deze vervalste certificaten toen ingetrokken en zijn netwerkbeveiliging laten controleren. Het bedrijf verkeerde hierna in de veronderstelling dat het incident verholpen was. Op 29 augustus werd echter bekend dat een internetgebruiker in Iran een vervalst certificaat had aangetroffen dat door DigiNotar was afgegeven. Het bedrijf liet daarop het bedrijfsnetwerk nader onderzoeken. De voorlopige resultaten van dit onderzoek wezen uit dat mogelijk meer vervalste certificaten in omloop waren gebracht dan tot dan toe waren geïdentificeerd. Bovendien kon het onderzoek niet uitsluiten dat ook vervalste PKIoverheid-certificaten in omloop waren gebracht.

Dit was aanleiding voor de rijksoverheid om alarm te slaan. De minister van Binnenlandse Zaken en Koninkrijksrelaties stelde in zijn persconferentie dat overheidswebsites als gevolg van de inbraak niet langer volledig betrouwbaar waren. Burgers konden er niet meer zeker van zijn dat zij via deze websites daadwerkelijk met overheidsorganisaties communiceerden. Er zou fraude kunnen plaatsvinden. De minister verklaarde dat de veiligheid van digitale gegevens die werden beschermd met door DigiNotar uitgegeven certificaten, niet meer kon worden gegarandeerd. De minister gaf te kennen dat hij per direct het vertrouwen in DigiNotar had opgezegd. Daarom zouden alle partijen die gebruik maakten van door DigiNotar uitgegeven certificaten deze op zo kort mogelijke termijn moeten vervangen door certificaten van een andere certificaatdienstverlener. Gedurende die vervangingsoperatie zou de minister het operationeel beheer over het bedrijf DigiNotar overnemen.

Vastgesteld is dat tijdens de inbraak bij DigiNotar in elk geval 531 vervalste certificaten zijn aangemaakt, waarvan een onbekend aantal in omloop is gebracht. Of dit heeft geleid tot directe schade voor burgers of bedrijven in Nederland, financieel of anderszins, is niet bekend. Wel zijn er aanwijzingen dat in Iran e-mailverkeer is afgeluisterd met gebruikmaking van vervalste certificaten afkomstig van DigiNotar. Wat de gevolgen hier van zijn geweest, is niet bekend.

De inbraak bij DigiNotar heeft ertoe geleid dat een digitaal veiligheidsrisico plotseling in het brandpunt van de publieke belangstelling stond, dat voordien niet werd onderkend. Burgers, overheidsorganisaties en bedrijven werden ermee geconfronteerd dat de beveiliging van het elektronisch gegevensverkeer waarvan onze samenleving in toenemende mate afhankelijk is, niet onaantastbaar is. Het feit dat de schade als gevolg van de inbraak bij DigiNotar beperkt lijkt te zijn gebleven, doet niet af aan de ernst van de mogelijke gevolgen die deze had kunnen hebben. Het in omloop raken van vervalste digitale certificaten had kunnen leiden tot schade aan de belangen van individuele burgers en bedrijven in Nederland, wier gegevens door onbevoegden misbruikt hadden kunnen worden. Ook de samenleving als geheel en de overheid hadden, als gevolg van fraude en door verlies van publiek vertrouwen in de betrouwbaarheid van communicatievoorzieningen, aanzienlijke schade kunnen lijden.

1.1 Onderzoek door de Onderzoeksraad voor Veiligheid

Wanneer digitale gegevens in verkeerde handen vallen, ligt misbruik op de loer. Dit misbruik kan de belangen van de individuele burgers of bedrijven op wie deze gegevens betrekking hebben, ernstig schaden. Vaak is deze schade financieel van aard, maar daartoe blijft hij niet noodzakelijk beperkt: iemand die slachtoffer wordt van identiteitsfraude kan zich bijvoorbeeld geconfronteerd zien met strafrechtelijke vervolging voor (economische) delicten die in zijn naam worden gepleegd. Bovendien wordt door verlies of misbruik van gegevens de persoonlijke levenssfeer geschonden van degene op wie de gegevens betrekking hebben. Daarnaast kan misbruik van gegevens de belangen van de overheid schaden, bijvoorbeeld wanneer iemands digitale identiteit door een ander wordt misbruikt om uitkerings- of belastingfraude te plegen. Grootschalig misbruik kan ertoe leiden dat burgers en bedrijven hun vertrouwen verliezen in elektronische gegevensuitwisseling, hetgeen grote economische schade of maatschappelijke ontwrichting tot gevolg kan hebben.

De Onderzoeksraad vindt dat overheidsorganisaties een bijzondere verantwoordelijkheid hebben ten aanzien van het beveiligen van digitale gegevens die zij onder zich hebben. Immers, waar burgers en bedrijven in onderling verkeer vrij zijn om te kiezen met wie zij hun gegevens wel en niet uitwisselen, geldt dat de overheid hen verplicht tot het beschikbaar stellen van gegevens. Dit betekent echter ook dat burgers en bedrijven erop moeten kunnen vertrouwen dat de overheid alles in het werk stelt om deze gegevens zo goed mogelijk te beschermen tegen verlies en misbruik.

Digitale certificaten zijn een essentieel instrument in het bieden van deze bescherming. De inbraak bij DigiNotar en de nasleep daarvan werpen vragen op over de mate waarin de betrouwbaarheid van het instrument digitale certificaten gewaarborgd wordt. Bovendien ontstond kort na het DigiNotarincident ophef over de algemene staat van de beveiliging van gemeentelijke websites en netwerken. In de zogenaamde 'Lektober-actie' (najaar 2011) toonde ICT-journalist De Winter aan dat onbevoegden toegang konden krijgen tot vertrouwelijke gegevens door misbruik te maken van veiligheidslekken op gemeentelijke websites en websites van bedrijven. Beide gebeurtenissen gaven de Onderzoeksraad aanleiding tot zorg over de mate waarin en de wijze waarop overheidsorganisaties invulling geven aan hun verantwoordelijkheid voor de digitale veiligheid van burgers en bedrijven.

De rijksoverheid heeft zelf een vergelijkbare zorg, getuige het aantal onderzoeken dat op last van het kabinet wordt verricht naar digitale veiligheid en de betrouwbaarheid van certificaatdienstverlening. Ook de Onderzoeksraad is door de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Veiligheid en Justitie verzocht een onderzoek uit te voeren. Gezien het belang van digitale veiligheid, en de bijzondere verantwoordelijkheid die de overheid heeft in het waarborgen daarvan, heeft de Onderzoeksraad dit verzoek ingewilligd.

1.2 Onderzoeksvraag

Zoals hierboven is gesteld, moeten overheidsorganisaties die gegevens van burgers en bedrijven verwerken ervoor zorgen dat deze gegevens bij hen zo veilig mogelijk zijn. Anders gezegd, zij dragen ten aanzien van deze gegevens verantwoordelijkheid voor de digitale veiligheid van die burgers en bedrijven.

Definitie digitale veiligheid
De term digitale veiligheid is ontleend aan het *Nationaal Trendrapport Cybercrime en Digitale veiligheid 2010*. In dit rapport verwijst digitale veiligheid naar ongecompromitteerde verwerking van digitale gegevens die betrekking hebben op burgers en bedrijven. Dit betekent dat deze gegevens gevrijwaard blijven van inzage of manipulatie door onbevoegden, en van misbruik.

De Onderzoeksraad onderzoekt wat de inbraak bij DigiNotar en de nasleep daarvan zeggen over de veiligheid van digitale certificaten. In bredere zin bekijkt de Onderzoeksraad de algehele beheersing van digitale veiligheid door overheidsorganisaties. Daartoe beschouwt hij de aangetroffen feiten vanuit het voor hem kenmerkende veiligheidsgedachtegoed.

Centraal staat dat de Onderzoeksraad de betrokken partijen in staat wil stellen lessen te trekken uit het gebeurde, opdat zij aan hun verantwoordelijkheid voor digitale veiligheid zo goed mogelijk invulling kunnen geven. De Onderzoeksraad kiest hierbij een bestuurlijk-organisatorisch perspectief, vanuit de overtuiging dat een goede inrichting en aansturing van de zorg voor digitale veiligheid essentieel is. Een en ander leidt tot de volgende centrale vraagstelling:

"Op welke manier waarborgen overheidsorganisaties bestuurlijk-organisatorisch digitale veiligheid en wat zijn hierbij knelpunten?"

De probleemstelling en deze vraag leidden tot drie onderzoeksvragen:

1. Bij het verlenen van certificaatdiensten door DigiNotar en bij het beheersen van de gevolgen van de inbraak bij het bedrijf waren verschillende partijen betrokken. Hoe hebben deze gefunctioneerd, en wat waren hierbij de knelpunten?
2. Hoe wordt de betrouwbaarheid van PKIoverheid-certificaten gewaarborgd en wat zijn hierbij de knelpunten?
3. Hoe geven overheidsorganisaties hun verantwoordelijkheid voor digitale veiligheid bestuurlijk-organisatorisch vorm en wat zijn hierbij de knelpunten?

Op basis van de uitkomsten van het onderzoek naar deze vragen heeft de Onderzoeksraad conclusies en aanbevelingen geformuleerd.

1.3 Uitgangspunten Onderzoeksraad

De Onderzoeksraad gaat ervan uit dat in elk bedrijfsproces dingen kunnen misgaan die direct of indirect kunnen leiden tot blootstelling aan gevaar of tot schade. Het is noodzakelijk het optreden van zulke gebeurtenissen te kunnen verklaren. Het kennen en aanpakken van verklarende factoren kan immers helpen het risico, dat wil zeggen de kans op toekomstige ongevallen en de ernst daarvan, te verkleinen.

De risicoloze maatschappij bestaat niet; er bestaat niet zoiets als 100% veiligheid, ook niet ten aanzien van digitale veiligheid. De Onderzoeksraad hanteert daarom als uitgangspunt dat de verantwoordelijke partijen het risico zo ver moeten beperken als redelijkerwijs mogelijk is. Dat wil zeggen dat beschikbare maatregelen ter vermindering van het risico steeds moeten worden genomen, tenzij daaraan aantoonbaar onredelijke kosten of andere negatieve consequenties zijn verbonden. Deze maatregelen kunnen zich richten op het voorkomen van ongewenste gebeurtenissen, of op het beperken van de gevolgen daarvan.

Organisaties kunnen de risico's van hun bedrijfsprocessen beheersbaar maken door veiligheidsmanagement toe te passen. De Onderzoeksraad hanteert de volgende uitgangspunten om het veiligheidsmanagement van betrokken partijen te beoordelen (zie Hoofdstuk 3 voor een meer uitgebreide behandeling):

1. Het veiligheidsmanagement is gebaseerd op inzicht in de risico's;
2. het veiligheidsmanagement is realistisch en expliciet vastgelegd;
3. het veiligheidsmanagement wordt uitgevoerd;
4. het veiligheidsmanagement wordt doorlopend geëvalueerd en waar nodig aangepast;
5. het veiligheidsmanagement is een verantwoordelijkheid van het management.

Vergelijkbare uitgangspunten vormen de basis van talrijke normen en standaarden die organisaties in alle geledingen van de maatschappij hanteren om hun veiligheidsmanagement in te richten.
Soms kunnen activiteiten van een bepaalde partij risico's met zich meebrengen voor een andere partij, of kan een andere partij juist iets doen om dat risico te beheersen. In dat geval hebben partijen een gezamenlijke verantwoordelijkheid de risico's te beheersen.

Ten overvloede merkt de Onderzoeksraad op, dat de vijf hierboven geformuleerde uitgangspunten van veiligheidsmanagement ook gelden voor een stelselverantwoordelijke. Immers, ook die heeft een bedrijfsproces, dat bestaat uit het inrichten en aanpassen van het stelsel waarvoor hij verantwoordelijkheid draagt. Ook in dit proces is het van belang om alle risico's zo goed mogelijk te beheersen en hieraan op planmatige wijze vorm te geven.

1.4 Focus van het onderzoek

Dit onderzoek richt zich enerzijds op de inbraak bij DigiNotar en de nasleep daarvan. De Onderzoeksraad heeft getracht te achterhalen hoe de partijen telkens hebben gehandeld op grond van de hun beschikbare informatie, en wat dit zegt over de wijze waarop zij de betrouwbaarheid van digitale certificaten waarborgen. De Onderzoeksraad heeft geen eigen technisch onderzoek naar de inbraak verricht.

Ten tweede kijkt het onderzoek naar de wijze waarop overheidsorganisaties invulling geven aan hun verantwoordelijkheid voor het waarborgen van de digitale veiligheid van burgers en bedrijven. Het onderzoek richt zich primair op de bestuurlijk-organisatorische inrichting hiervan. Een evaluatie van de specifieke technische maatregelen die organisaties daartoe treffen blijft achterwege. Overigens tekent de Onderzoeksraad hierbij aan dat in het onderzoek slechts een klein aantal overheidsorganisaties betrokken is. Hoewel naderhand is geprobeerd de bevindingen zo breed mogelijk te toetsen, zijn zij niet zonder meer te generaliseren. Het deelonderzoek naar de beheersing van digitale veiligheid heeft dan ook een verkennend karakter, in tegenstelling tot het deelonderzoek naar de veiligheid van digitale certificaten en certificaatdienstverlening door DigiNotar.

De Inspectie Veiligheid en Justitie (voorheen IOOV) is na het DigiNotarincident door de minister van Veiligheid en Justitie gevraagd onderzoek te doen naar de structuur van de crisisopschaling. De onderzoeken van de Inspectie Veiligheid en Justitie en de Onderzoeksraad richten zich op hetzelfde incident, maar met een andere invalshoek. De Inspectie Veiligheid en Justitie richt zich op de vraag *hoe de crisis na de hack werd beheerst*. De Onderzoeksraad richt zich op de vraag *hoe de gebeurtenissen konden optreden*.

1.5 Onderzoeken door derden

Verscheidene partijen hebben onderzoek verricht naar de inbraak bij DigiNotar. De Onderzoeksraad heeft informatie uit de hieronder genoemde onderzoeken bij zijn eigen onderzoek betrokken, voor zover deze op het moment van schrijven van dit rapport beschikbaar waren.

De Onderzoeksraad heeft zich in zijn eigen onderzoek primair gericht op de bestuurlijk-organisatorische aspecten van de digitale veiligheid van de overheid. Daarbij zijn elementen van de hieronder genoemde onderzoeken van belang. Het onderzoek van de Onderzoeksraad richt zich op het gehele stelsel van digitale veiligheidszorg van overheidsorganisaties en beziet wat daarin de knelpunten en mogelijke verbeteringen zijn.

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft in de brief van 14 maart 2012 aan de Tweede Kamer de maatregelen toegelicht die zij treft naar aanleiding van deze onderzoeken. Die maatregelen zijn hieronder tevens opgenomen.[1]

1 Brief d.d. 14 maart 2012, van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer. Kamerstuk TK 26643-230. Het Kabinet zet, blijkens de brief, in op een driesporenbeleid: het vergroten van de weerbaarheid tegen inbreuken; het vergroten van het herstelvermogen bij geslaagde inbreuken en structurele systeemverbeteringen op mondiaal niveau.

1.5.1 Onderzoek Evaluatie PKI

Het onderzoek Evaluatie PKI had ten doel vast te stellen welke risico's PKIoverheid en het stelsel voor gekwalificeerde certificaten bevatten, of het normenstelsel toereikend is en of het toezichtarrangement adequaat functioneert.[2]

Dit onderzoek toont aan dat er in beide stelsels licht zit tussen de verwachte betrouwbaarheid en de feitelijk gerealiseerde betrouwbaarheid. De normenstelsels, de toezichthouders, de auditors en de accreditering zijn bedoeld om een deugdelijke grondslag te leveren voor het vertrouwen, maar op al deze aspecten zijn aanscherpingen en verbeteringen nodig. Samengevat blijkt uit het onderzoek dat:

- Het toezichtarrangement niet is ingericht om het beoogde vertrouwen te rechtvaardigen;
- de normenstelsels te complex en op onderdelen onvoldoende concreet zijn, met name als het gaat om bijvoorbeeld het aspect informatiebeveiliging;
- de uitvoering en opvolging van risicoanalyses in de stelsels niet de rol spelen die op grond van snel veranderende dreigingsprofielen zou mogen worden verwacht. Risicobeheersing van de maatschappelijke risico's is stelseloverstijgend en niet structureel ingericht;
- voor belanghebbenden de feitelijk geleverde betrouwbaarheid onvoldoende transparant is;
- de stelsels primair nationaal georiënteerd zijn en er in de praktijk vrijwel geen grensoverschrijdende Europese markt voor deze diensten is.

Afsluitend wordt aangegeven dat op korte termijn een aantal verbeteringen kan worden doorgevoerd. Daarbij dient een aantal samenhangende beleidsmatige keuzes te worden gemaakt. Bij deze keuzes kunnen fundamentele discussies een rol spelen, waaronder die van de rol van de overheid versus de rol van de markt, de gewenste vorm van handhaving, de rol van Europa en de verantwoordelijkheid van de overheid voor beveiliging binnen vitale sectoren. Het rapport geeft aan dat een scenarioanalyse zou kunnen helpen bij verdere besluitvorming.

De door de minister voorgestelde maatregelen om het certificatenstelsel robuuster en betrouwbaarder te maken zijn:

- Aanscherpen van het Programma van Eisen PKIoverheid door de Logius met andere eisen op het gebied van netwerkbeveiliging, computerbeveiliging en logging;
- gedeeltelijk wegnemen van de overlap tussen PKIoverheid en het stelsel voor gekwalificeerde handtekeningen;
- herzien van de Richtlijn Elektronische Handtekeningen (1993/93/EG) door de betreffende raadswerkgroep in Brussel, onder meer ten aanzien van de complexiteit van normen, risicobeheersing en het gebruik van audits;
- opnieuw en duidelijker definiëren van de rollen van normbeheerders, auditors en toezichthouders en hun instrumenten;
- uitbreiden van managementsysteem audits met elementen van een IT-audit;
- verkorten van de termijn waarbinnen bij audits geconstateerde afwijkingen kunnen worden opgelost;
- sneller aanpassen van de normenstelsels aan nieuwe risico's en dreigingen;
- afleggen van bedrijfsbezoeken bij certificaatdienstverleners door OPTA en Logius voor PKioverheid;
- aanpassen van de Europese Richtlijn inzake elektronische handtekeningen, zodat hierin een wettelijke basis voor webcertificaten komt waardoor toezicht houden mogelijk wordt.

Aan het intensiveren van het rijkstoezicht op certificaatdienstverleners wordt al gewerkt. Datzelfde geldt voor het intensiveren van de samenwerking tussen OPTA en Logius. Ten slotte zijn onderzoeken gaande naar het verplicht stellen van PKIoverheid voor overheidsorganisaties, en naar het betrouwbaar en ongestoord functioneren van de markt van het PKIoverheidstelsel.

2 Evaluatie PKI. Rapportage, 8 maart 2012. Logica Business Consulting, in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Economische zaken, Landbouw en Innovatie. Bijlage bij Kamerstuk TK 26643-230. Een toelichting op deze stelsels is in dit rapport opgenomen in Hoofdstuk 5.

1.5.2 Onderzoek Black Tulip

Dit onderzoek heeft ten doel om een technische reconstructie te geven van de inbraak bij DigiNotar.[3] In Paragraaf 4.1.1 wordt nader ingegaan op de inhoud van dit rapport.

1.5.3 De zaak-DigiNotar: handelde de overheid adequaat?

Dit onderzoek beoordeelt of de bij PKIoverheid betrokken overheidspartijen adequaat hebben gereageerd inzake de inbraak bij DigiNotar, gegeven de toen geldende regels.[4]

De Rijksauditdienst concludeert dat het DigiNotarincident in september 2011 bij de rijksoverheid een trendbreuk teweeg heeft gebracht. De wijze van denken over en omgaan met risico's van beveiliging van websites is veranderd. Samenwerking tussen de betrokken partijen (publiek, privaat, internationaal) heeft een belangrijke impuls gekregen. Voorts concludeert de Rijksauditdienst dat de rijksoverheid snel en adequaat heeft gehandeld om verdere schade te voorkomen. Zo werden burgers en bedrijven gewaarschuwd, werd Microsoft met succes benaderd om een voorziene update voor Nederland met een week uit te stellen, en werd de operationele bedrijfsvoering van DigiNotar met betrekking tot de uitgifte van certificaten overgenomen. Ook werd direct nader onderzoek ingesteld naar het falen van de beveiliging. Voorafgaand aan de digitale inbraak bij DigiNotar was er feitelijk geen sprake van extra alertheid in dit verband. Alle overheidspartijen vertrouwden, voor wat betreft het toezicht op PKIoverheid, op de activiteiten van de betreffende auditpartij. Wellicht mede als gevolg van dit vertrouwen, was een aantal standaardzaken niet aanwezig: zo ontbrak een risicoanalyse waarbij de ketenpartners betrokken waren, was er onvoldoende inzicht in aantal en aard van de uitstaande PKIoverheid-certificaten, en was er geen helderheid over toezichtcriteria.

De belangrijkste maatregelen die de minister naar aanleiding van dit onderzoek aankondigt in haar brief van 14 maart 2012 zijn het aanpassen van het Programma van Eisen, zodat er meer continuïteitsmaatregelen komen. Te denken valt aan het hebben van reservecertificaten van andere leveranciers, en het verbeteren van de communicatie van de overheid bij een toekomstige crisissituatie.

1.5.4 Onderzoek veiligheid diensten in de Digitale Agenda.nl

Dit onderzoek had ten doel in kaart te brengen in hoeverre de ICT-diensten die het ministerie van Economische Zaken, Landbouw en Innovatie ter beschikking stelt aan ondernemers, veilig zijn.[5] In de Digitale Agenda.nl is een negental voorzieningen opgenomen ten behoeve van de elektronische dienstverlening aan bedrijven. Het onderzoek doet de volgende aanbevelingen:

- Zorg voor een goede verdeling van verantwoordelijkheden tussen ministerie, ontwikkel- en beheersorganisaties en marktpartijen en maak deze afspraken transparant. Hierbij dient tevens de (politieke) verantwoordelijkheid de minister van Economische Zaken, Landbouw & Innovatie geëxpliciteerd te worden, zowel de ontwikkel- als de beheersfase. Detailafspraken over audits en penetratietesten dienen onderdeel van deze afspraken te zijn;
- zorg voor voldoende monitoring van de getroffen veiligheidsmaatregelen;
- maak duidelijk wat het restrisico is dat door belanghebbenden als acceptabel wordt beschouwd;
- laat opdrachtgever van de diensten bepalen welke scope en diepte gewenst is bij uit te voeren audits ten behoeve van de veiligheid van de dienst;
- maak voor diensten die een hoog niveau van veiligheid vereisen niet alleen gebruik van audits en penetratietesten, maar gebruik ook andere technische maatregelen om operationele risico's te verkleinen.

3 Black Tulip. Investigation update DigiNotar Certificate Authority breach. Interim report, september 5, 2011. Fox-IT B.V., in opdracht van DigiNotar B.V., later in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Bijlage bij Kamerstuk TK 26643-188.

4 De zaak 'DigiNotar': handelde de overheid adequaat? Onderzoek naar alertheid en adequaatheid van handelen van de overheid ten tijde van de 'DigiNotar'-problematiek, 8 maart 2012. Rijksauditdienst, in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Bijlage bij Kamerstuk TK 26643-230.

5 Onderzoek veiligheid diensten in de Digitale Agenda.nl, 8 maart 2012. Collis en HEC, in opdracht van het Ministerie van Economische zaken, Landbouw en Innovatie. Bijlage bij Kamerstuk TK 26643-230.

2 EEN VERANDERDE WERELD: DIGITALE VEILIGHEID ONDER DRUK

Dit hoofdstuk geeft een kort overzicht van de context waarin digitale veiligheid zich afspeelt. Het gaat in op de ontwikkeling van digitalisering, en de veranderende aard en omvang van de risico's die digitale veiligheid bedreigen.

2.1 Toenemende digitalisering: een wereld van ongekende mogelijkheden

Het gebruik van informatie- en communicatietechnologie (ICT) is sinds de jaren negentig van de vorige eeuw binnen de Nederlandse samenleving sterk toegenomen. De overheid, bedrijven en burgers maken steeds meer gebruik van informatietechnologie. Internet is niet meer uit ons dagelijks leven weg te denken; we leven in een digitale wereld en dat zal zo blijven.

Overheidsorganisaties besteden veel aandacht aan het ontwikkelen van de digitale dienstverlening voor de burger. Goede toegang tot overheidsproducten voor burgers en bedrijven is een belangrijke prioriteit. Overheidsbeleid zet al langere tijd in op groei van het aantal digitaal beschikbare overheidsproducten, om lagere administratieve lasten voor burgers en bedrijven te realiseren. In 2007 concludeerde de Overheid.nl-monitor dat al 67% van de overheidsproducten elektronisch beschikbaar was voor burgers en bedrijven.[6] Zo kan een burger digitaal belastingaangifte doen en biedt de Dienst Uitvoering Onderwijs (DUO) zijn diensten online aan. Bij de Sociale Verzekeringsbank (SVB) kan de AOW-uitkering of de kinderbijslag on-line worden aangevraagd. Ook gemeenten bieden diverse diensten digitaal aan, bijvoorbeeld het doorgeven van een binnengemeentelijk verhuisbericht of het in ondertrouw gaan. Bovendien kunnen verschillende documenten digitaal worden aangevraagd zoals een uittreksel uit de gemeentelijke basisadministratie, allerlei vergunningsaanvragen of een milieupas.

Behalve voor dienstverlening wordt ICT bij de overheid steeds meer ingezet ten behoeve van beleid. Te denken valt aan bestandskoppelingen in het kader van preventie, zoals in de verwijsindex risicojongeren, of fraudebestrijding, zoals de koppelingen in het domein van de sociale zekerheid. Daarnaast is ICT ook van belang voor het stroomlijnen van de eigen organisatie: werkprocessen worden steeds verder geautomatiseerd en geïntegreerd met ICT-systemen van andere organisaties om bijvoorbeeld digitale gegevensuitwisseling te faciliteren.

In zijn recente rapport *iOverheid* stelt de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) dat de ontwikkeling van de digitale samenleving wordt gekenmerkt door een opeenstapeling van ad hoc besluiten over nieuwe technieken, het ontbreken van het besef van het ontstaan van een e-overheid en het gebrek aan debat daarover.[7] Ook is de onderlinge digitale verwevenheid van organisaties in het publieke en het private domein toegenomen. Grenzen aan de verspreiding van de individuele applicaties en de verknoping van informatiestromen zijn er niet en niemand voelt zich hoeder over het geheel. De voordelen zoals gebruiksgemak, klantvriendelijkheid en efficiency worden belangrijker geacht dan een toename van kwetsbaarheid voor digitale verstoringen. De verwevenheid van aanbieders en afnemers van digitale diensten en producten heeft geleid tot ketens en netwerkachtige informatiestromen en samenwerkingsstructuren en vele koppelvlakken en schakelpunten in en tussen de ketens en netwerken. Daarvan is niet meer duidelijk waar deze beginnen of eindigen en welke partij het overzicht heeft, laat staan wie een regierol vervult. Gevolg is een grote mate van onderlinge digitale afhankelijkheid, waarbij de zwakste schakel de sterkte van de hele keten bepaalt.

6 Voortgangsrapportage elektronische overheid 2007. Bijlage bij kamerstuk TK 29362-120.
7 Wetenschappelijke Raad voor het Regeringsbeleid (2011). iOverheid, rapport 86. Amsterdam / Den Haag: Amsterdam University Press.

2.2 Spanning tussen de mogelijkheden en risico's van digitalisering

De digitalisering van de samenleving biedt vele mogelijkheden maar kent ook risico's. Een moedwillige of een onopzettelijke verstoring als gevolg van technisch of menselijk falen of door natuurlijke oorzaken kan leiden tot maatschappelijke ontwrichting.[8] Nieuwe vormen van criminaliteit als *hacken, phishing* en *skimmen* doen zich voor.[9] Daarbij veranderen ze voortdurend van verschijningsvorm en spelen zich grotendeels op een voor het grote publiek onzichtbare wijze af. Niettemin zijn verschillende incidenten de afgelopen tijd in de media gekomen, zoals onderstaand overzicht illustreert.

Recente incidenten digitale veiligheid

LinkedIn accounts gelekt
Op 6 juni 2012 maakt LinkedIn via een blogpost naar aanleiding van een hack bekend dat "een aantal wachtwoorden" van LinkedIn-accounts waren gelekt. Een lijst met circa 6,5 miljoen versleutelde wachtwoorden was online gezet door een hacker. Onduidelijk bleef of ook de bijbehorende e-mailadressen waren gestolen. De getroffen accounts werden tijdelijk afgesloten en gebruikers werden via e-mail door het sociale netwerk benaderd om hun wachtwoord zelf te resetten. De FBI onderzoekt samen met het bedrijf de diefstal.

Medische dossiers toegankelijk
In een aflevering van televisieprogramma ZEMBLA op 20 april 2012 wordt bekend gemaakt dat medische en persoonlijke gegevens van meer dan 300.000 werknemers door een lek in de software van het computerprogramma Humannet van IT-bedrijf VCD maandenlang toegankelijk geweest bleken te zijn voor onbevoegden. Organisaties als FC Twente, Gemeente Deventer, Praxis, Bijenkorf, V&D, Hornbach, Beter Bed, Action en vele andere bedrijven en arbodiensten werken met dit computerprogramma. Ze verwerken daarin adres-, verzuim-, herstel- en re-integratiegegevens van hun werknemers, evanals medische dossiers van bedrijfsartsen en burgerservicenummers.

NVVP
De Nederlandse Vereniging van Vrijgevestigde Psychologen & Psychotherapeuten (NVVP) kwam op 14 maart 2012 in het nieuws. Een cliënt moest na een behandeling een online vragenlijst invullen, maar kwam in plaats daarvan terecht bij een zoekscherm. Hier kon van tientallen cliënten de naam, geboortedatum, geslacht en burgerservicenummer worden opgezocht. Het lek heeft minstens een week bestaan.

Videobelsysteem Defensie
Op 12 maart 2012 wordt bekend dat militair overleg af te luisteren was door een niet adequaat afgeschermd videovergadersysteem van Defensie. Met het fabriekswachtwoord, te vinden in de handleiding van de programmatuur, kon volledige toegang worden verkregen tot het communicatiesysteem. Zelfs als het wachtwoord wel veranderd zou zijn geweest, was het voor een hacker alsnog redelijk eenvoudig om in te breken. Er was namelijk geen beperking ingesteld op het aantal in te voeren wachtwoordpogingen. Het vergadersysteem was toegankelijk via internet en zonder barrières

8 Nationale Cyber Security Strategie (2011). Bijlage bij Kamerstuk TK 26643-174.
9 *Hacken* is het vinden van toepassingen die niet door de maker van het middel bedoeld zijn, speciaal met betrekking tot computers. De term wordt vaak gebruikt als synoniem voor *cracking* of computercriminaliteit. *Phishing* is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website en ze daar nietsvermoedend te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens. *Skimmen* is een vorm van betaalpasfraude. Het is het op onrechtmatige wijze bemachtigen en kopiëren van betaalkaartgegevens. Criminelen kopiëren de magneetstrip van een pas en bemachtigen de pincode op het moment dat er een betaaltransactie wordt verricht.

Nationale Theaterkassa
Op 22 februari 2012 verschijnt een bericht dat uit de database van de Nationale Theaterkassa een hacker de persoonsgegevens van bijna 100.000 mensen heeft kunnen achterhalen. Hieronder vielen ook de gegevens van 226 nog in gebruik zijnde credit-cards. De hacker had ontdekt dat de volledige database van de website zonder wachtwoord te benaderen was. Het betrof een oude database die gebruikt werd voor de nieuwsbrief. Sinds 2010 gebruikte de website een ander systeem, waardoor het merendeel van de onderschepte gegevens ongeldige credit-cards betrof.

KPN
Op 16 januari 2012 worden diverse servers van KPN gehackt. Op 8 februari 2012 wordt dit bekend gemaakt in de media. Twee dagen later verschijnt op internet een bestand met daarin de vermoedelijke gegevens van ruim 500 KPN-klanten. In het document staan ook e-mailadressen en wachtwoorden. Later blijkt dat deze gegevens afkomstig zijn van het bedrijf Baby Dump.

Philips
Op 14 februari 2012 claimt een hacker toegang te hebben gehad tot een server van Philips, waarop marketingsites werden gehost. Zo zou hij onder meer 200.000 e-mailadressen en telefoonnummers hebben verkregen. Philips bevestigde dat de beveiliging was aangetast.

Sluizen, gemalen en bruggen
In de media verschijnen op 14 februari 2012 berichten dat het kinderlijk eenvoudig is om op afstand via internet sluizen, gemalen en zelfs bruggen te bedienen. Uit een reportage van televisieprogramma EenVandaag blijkt dat de rioleringspompen en gemalen van de gemeente Veere slecht zijn beveiligd.

Zorginstelling De Hoop
Op 9 december 2011 verschijnt het bericht in de media dat persoonlijke gegevens op straat liggen van deze instelling voor verslaafden en psychiatrische patiënten. Het betreft geen patiëntgegevens, maar wel van klanten. Naam, adres, bankrekeningnummer, e-mailadres, inlognaam en wachtwoord waren toegankelijk. Ook werd een beheerderswachtwoord achterhaald, waardoor verschillende andere websites toegankelijk werden.

Publieke omroep
Op 28 november 2011 komt een bericht in het nieuws dat door een lek in een beheersysteem bij publieke omroepen 160 websites toegankelijk geworden waren voor een hacker. Gevolg hiervan was dat 2,3 miljoen persoonsgegevens openbaar zijn geworden via websites van onder andere SLAM FM, 3FM en QMusic, maar ook sites van televisieprogramma's zoals het Klokhuis. Een van de gehackte beheerderswachtwoorden bleek voor alle sites te werken, waardoor het ook mogelijk werd om de websites aan te passen.

Sinterklaasjournaal
Op 28 november 2011 blijkt dat door een beveiligingsprobleem op de website van het Sinterklaasjournaal een hacker de gegevens van circa 13.000 kinderen heeft kunnen inzien. De gegevens bestonden onder andere uit hun naam, e-mailadres en leeftijd.

In *iOverheid* stelt de Wetenschappelijke Raad voor het Regeringsbeleid:
"Wie het discours over digitalisering anno 2011 overziet, moet vaststellen dat deze wordt gedomineerd door bijdragen in twee (conflicterende) toonsoorten. Enerzijds onderbouwen beleidsplannen, rapporten en Kamerstukken de nieuwe mogelijkheden en ambities van de overheid met enthousiaste en wervende uiteenzettingen over de kansen die digitalisering biedt: een veilige samenleving waarin maatschappelijke risico's tijdig in beeld komen; een efficiëntere overheid die zich kenmerkt door dienstverlening op maat aan burgers en die openstaat voor de kennis en kunde van diezelfde burgers. Anderzijds is het debat, met name in wetenschappelijke en maatschappelijke fora, vaak ook negatief van toonzetting. Het gaat over aantasting van de privacy van burgers, verloren miljoenen door mislukte ICT-projecten, niet gerealiseerde verwachtingen, nieuwe kwetsbaarheden als identiteitsfraude en onvoldoende aandacht voor beveiliging van systemen en informatie." (iOverheid, pp. 44-45)

In het debat wordt de spanning zichtbaar tussen enerzijds de mogelijkheden die ICT biedt, en anderzijds de risico's die eraan verbonden zijn. Beide aspecten zouden niet tegenover elkaar moeten staan: het zijn twee kanten van dezelfde medaille. Beleidsmakers en bestuurders dienen bij iedere beslissing over digitalisering een afweging te maken waarin zowel de voordelen als de risico's op een evenwichtige wijze worden meegewogen. Het is de vraag of dit gebeurt en zo ja, welk aspect het zwaarst weegt. De vraag hoe overheidsorganisaties met deze afwegingen omgaan, is een van de onderwerpen die in de verkenning in Hoofdstuk 6 is meegenomen.

Daarnaast is het van belang dat bestuurders, beleidsmakers en burgers zich realiseren dat elke vorm van informatietechnologie onveilig is. Het besef dat elk ICT-systeem, net als ieder huis of kluis, te kraken is, moet het uitgangspunt zijn: het oordeel 'veilig' kan nooit gegeven worden. Van Eeten (2011: 134) zet uiteen dat het erom gaat dat duidelijk is wat de resterende risico's zijn en hoe deze gereduceerd kunnen worden. Of iets veilig genoeg is, hangt in de praktijk af van de kans op en de gevolgen van de specifieke vorm of mate van onveiligheid. Het kan bijvoorbeeld gaan om het uitvallen van vitale producten en diensten, om het schenden van privacy van burgers, om identiteitsfraude of economische schade. Allemaal gevolgen die gewogen dienen te worden. In het debat over digitale veiligheid is het van belang te bezien hoe bereikt wordt dat overheidsorganisaties en bedrijven de gevolgen van een veiligheidskeuze voor anderen proportioneel meewegen in de besluitvorming. Het proportioneel meewegen van de mogelijke gevolgen voor anderen zal leiden tot maatschappelijk verantwoorde uitkomsten.[10]

Het feit dat onveiligheid een gegeven is, betekent ook dat niet alleen op beveiliging van ICT-systemen ingezet moet worden, aangezien die nooit volledig veilig zullen zijn. Dit vergt enerzijds een expliciete afweging of het verzamelen en uitwisselen van gegevens noodzakelijk is en welke beveiliging mogelijk is, en anderzijds een adequaat terugvalscenario op het moment dat een incident zich voordoet. Bij een terugvalscenario hoort het herstellen van de veiligheid, maar ook het oplossen van problemen die anderen door onveiligheid hebben ondervonden.

Iedere organisatie heeft een eigen verantwoordelijkheid voor informatiebeheer, zo ook de overheidsorganisaties. Hierover zegt het kabinet in de kabinetsreactie op *iOverheid:*

"Het ligt op de weg van de overheid, en binnen de verantwoordelijkheid van elk van de overheidslagen, om slechts na een zorgvuldige afweging te besluiten tot uitwisseling van persoonsgegevens. Daarnaast moeten de datastromen die de overheid beheert zo goed mogelijk worden onderhouden en beveiligd. Hiervoor moeten blijvend passende structuren worden gecreëerd."[11]

De Hert (2011) betoogt dat de overheid vanuit mensenrechtelijk perspectief ook een verantwoordelijkheid heeft voor de informatiemaatschappij. Hiermee doelt hij op een verantwoordelijkheid van de overheid voor het maatschappelijk gebruik van ICT. Dit houdt in dat de rijksoverheid andere overheidsorganisaties moet stimuleren en in staat stellen, digitale veiligheid te waarborgen. De overheid moet er vanuit deze verantwoordelijkheid voor zorgen dat burgers beschermd worden tegen mensenrechtenschendingen (waaronder privacyschendingen) en dat voorkomen wordt dat systemen falen.[12] Vanuit de coördinerende verantwoordelijkheid voor overheids-ICT heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties het stelsel PKIoverheid opgezet, met als doel veilige en betrouwbare gegevensuitwisseling tussen de overheid, burgers en bedrijven en tussen overheidsorganisaties onderling te waarborgen. In Hoofdstuk 5 van dit rapport wordt onder meer beschreven in hoeverre dit stelsel de betrouwbaarheid van gegevensuitwisseling met behulp van digitale certificaten waarborgt en wat hierbij de knelpunten zijn.

10 Van Eeten, Michel (2011). Gedijen bij onveiligheid, afwegingen rond de risico's van informatietechnologie. In *De Staat van informatie*, Dennis Broeders, Colette Cuijpers en Corien Prins (red.), pp. 133-164. Verkenningen van de Wetenschappelijke Raad voor het Regeringsbeleid. Amsterdam / Den Haag: Amsterdam University Press.

11 Reactie van de Minister van Binnenlandse Zaken en Koninkrijksrelaties op het rapport iOverheid van de Wetenschappelijke Raad voor het Regeringsbeleid, oktober 2011. Kamerstuk TK 26643-211.

12 De Hert, Paul (2011). Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting. In *De Staat van informatie*, pp. 33-96.

2.3 Bedreigingen digitale veiligheid permanent, en voortdurend in beweging

De afgelopen jaren is cybercrime en digitale veiligheid steeds prominenter op de beleidsagenda van de rijksoverheid verschenen, zoals een greep uit de vele beleids- en strategiedocumenten laat zien:[13]

- Nationaal Trendrapport Cybercrime en Digitale Veiligheid (november 2010);
- Nationale Risicobeoordeling Bevindingenrapportage; ministerie van Veiligheid & Justitie, (november 2010);
- Nationale Cyber Security strategie (maart 2011);
- Reactie van de minister van Binnenlandse Zaken en Koninkrijksrelaties op het rapport *iOverheid* van de WRR (oktober 2011);
- I-Strategie Rijk; minister van Binnenlandse Zaken en Koninkrijksrelaties (november 2011);
- Cybersecuritybeeld Nederland (december 2011).

Als uitvloeisel van de Nationale Cyber Security Strategie is in juni 2011 de Cyber Security Raad geïnstalleerd. Deze Raad heeft tot taak om de regering en private partijen gevraagd en ongevraagd te adviseren over relevante ontwikkelingen op het gebied van digitale veiligheid. De Raad stelt prioriteiten in de aanpak van ICT-bedreigingen, bekijkt de behoefte aan onderzoek en ontwikkeling, en kijkt hoe de opgebouwde kennis van de Cyber Security Raad vervolgens het beste kan worden gedeeld met de samenwerkende publieke en private partijen.

Teneinde de digitale weerbaarheid van de Nederlandse samenleving te vergroten, is in januari 2012 bovendien een Nationaal Cyber Security Centrum (NCSC) ingesteld. Het NCSC heeft ten doel kennis en expertise te bundelen op het gebied van het voorkomen en tegengaan van dreigingen in het digitale domein. Daarnaast heeft het NCSC een kennis- en adviesfunctie in brede zin naar de samenleving. Het centrum concentreert zich op het bundelen van expertise die binnen de overheid aanwezig is, maar de ambitie is om gaandeweg ook samenwerking met private partijen te zoeken. Een van de taken van het NCSC is het opstellen van een dreiging- en risico analyse. Onderdeel van het NCSC is het *Government Computer Emergency Response Team* (GovCert), dat zich sinds 2002 richt op het zo snel mogelijk herstellen van eventuele aantastingen van de digitale veiligheid, en op het helpen bestrijden van eventuele gevolgen daarvan.

Alle hierboven genoemde ontwikkelingen plaatsen het toegenomen gebruik van ICT in de samenleving in de context van voortdurende en veranderende dreigingen voor digitale veiligheid. Zij onderkennen dat deze niet meer zijn weg te denken uit de (digitale) samenleving en dat de samenleving zich hier bewust van moet zijn en hiermee moet leren leven. Het Cybersecuritybeeld Nederland uit 2011 onderscheidt drie soorten dreigingen:

- Informatiegerelateerde dreigingen, gericht op het verkrijgen van vertrouwelijke informatie van economische of politieke waarde;
- systeemgerelateerde dreigingen, die ontstaan als men de intentie heeft om de dienstverlening of de bedrijfsvoering van een organisatie te verstoren;
- indirecte dreigingen, die neveneffecten zijn van de bovengenoemde bedreigingen, zoals verstoring van de bedrijfsvoering door *malware*-besmetting of verstoring van dienstverlening door een aanval bij een derde partij.[14]

Uitingen van bovengenoemde dreigingen zijn digitale spionage en het steeds geavanceerder worden van cybercriminaliteit, digitale identiteitsfraude en het publiceren van persoonsgegevens. Ook de kwetsbaarheid van burgers, overheidsorganisaties en bedrijven voor digitaal misbruik, het onder druk staan van privacy en de toenemende moeilijkheid om ICT te beveiligen door uitbesteding en *cloud computing*, worden als nieuwe dreigingen geïdentificeerd.[15]

13 Bibliografische details van de hier genoemde documenten zijn opgenomen in de literatuurlijst.
14 *Malware* is software met als doel schade aan te richten bij degenen die de software installeren.
15 *Cloud computing* is het via het internet op aanvraag beschikbaar stellen van hardware, software en gegevens.

Daarnaast wordt onderkend dat de risicobeleving van de burger niet overeenkomt met de werkelijke risico's en wordt gewezen op de gebrekkige coördinatie van initiatieven betreffende digitale veiligheid.

2.4 Conclusie

De grote vlucht die digitalisering de afgelopen decennia heeft genomen, heeft de samenleving veel gebracht. We leven steeds meer in een digitale wereld en het eind van de mogelijkheden is nog lang niet in zicht. Tegelijkertijd wordt steeds duidelijker dat de groei van en het optimisme over de voordelen van digitalisering uit het begin van het digitale tijdperk voorbij zijn. De samenleving bevindt zich in feite al geruime tijd in het stadium van steeds zichtbaarder wordende risico's en een toename van digitale verstoringen in verschillende verschijningsvormen. Daarmee wordt zichtbaar dat het een illusie is dat een ICT-systeem volledig veilig gemaakt kan worden. Risico is de maat en niet de uitzondering. Het moment is aangebroken dat iedereen, bedrijfsleven, overheid en burgers, zich hiervan bewust moet zijn en hiernaar moet handelen.

Het treffen van preventieve maatregelen en het voorhanden hebben van passende terugvalscenario's en herstelmaatregelen, zijn daar onderdeel van. Preventie behelst onder meer een goede risico-afweging voordat overgegaan wordt tot de volgende stap in de digitalisering van diensten zoals het uitwisselen van gegevens. Het is noodzakelijk zicht te hebben op de risico's en de belangen die spelen en op de actuele dreiging. Alleen dan kan beoordeeld worden wat de consequenties van onveiligheid zijn en in hoeverre die consequenties op een aanvaardbaar niveau gebracht kunnen worden. Wat een aanvaardbaar niveau is, zal per geval verschillen. Passende terugvalscenario's bieden burgers een oplossing als hun gegevens misbruikt worden en moeten zo veel als mogelijk voorkomen dat gegevensuitwisselingen of computersystemen stil komen te liggen.

Door de steeds grotere verwevenheid van ICT-systemen is het steeds moeilijker de gevolgen van falen van te voren te overzien. De informatiesamenleving groeit intussen gestaag verder. Elke nieuwe koppeling lijkt op zich niet zo spannend. Echter, het geheel aan koppelingen en uitwisselingen leidt tot toenemende risico's voor burgers en systemen. Risico's waarvan nu niet altijd duidelijk is of deze bij alle betrokkenen in beeld zijn en of passende beheersmaatregelen getroffen zijn.

3 BEOORDELINGSKADER

De Onderzoeksraad voor Veiligheid maakt in zijn onderzoeken gebruik van een beoordelingskader. Dat kader bestaat uit drie delen. Het eerste deel is een eigen beoordelingskader van de Onderzoeksraad. Dit kader gaat over de toepassing van de principes van veiligheidsmanagement vanuit de eigen verantwoordelijkheid van een organisatie. Het tweede deel van het beoordelingskader bestaat uit wet- en regelgeving die van toepassing is op het onderwerp van onderzoek. Het derde deel bestaat uit eigen normen en richtlijnen van bijvoorbeeld de branche waarvan een organisatie die door de Onderzoeksraad wordt onderzocht, deel uitmaakt.

3.1 Beoordelingskader Onderzoeksraad voor Veiligheid

Het eigen beoordelingskader van de Onderzoeksraad gaat uit van de eigen verantwoordelijkheid van een organisatie voor de veiligheidsrisico's die zijn verbonden met haar bedrijfsvoering en functioneren. De enige manier om risico's te beheersen, is verantwoordelijkheid te nemen. Het nemen van die verantwoordelijkheid houdt volgens de Onderzoeksraad in dat de risico's verbonden aan de bedrijfsvoering in kaart worden gebracht en worden gewogen, dat maatregelen worden genomen om de risico's te verminderen en dat de consequenties van de risicoafweging in ogenschouw worden genomen. Deze stappen vinden niet eenmalig plaats, maar maken continu deel uit van het organisatieproces. Dit is veiligheidsmanagement. De Onderzoeksraad heeft dit vorm gegeven in zijn beoordelingskader aan de hand van een vijftal principes van veiligheidsmanagement. Door invulling te geven aan deze uitgangspunten kan een organisatie de risico's die met de bedrijfsvoering zijn verbonden zo goed mogelijk beheersen.

In deze paragrafen worden de principes van veiligheidsmanagement geoperationaliseerd voor het onderzoek en de analyse in dit rapport. Dat betekent dat zij worden toegepast op digitale veiligheid.

3.1.1 Veiligheidsmanagement gebaseerd op inzicht in risico's

Het eerste uitgangspunt van veiligheidsmanagement is dat een organisatie de risico's moet kennen die de organisatiedoelstellingen of -processen kunnen bedreigen, en de mechanismen moet begrijpen waardoor deze risico's zich kunnen manifesteren. Het proces dat in dit onderzoek centraal staat, is het elektronisch verwerken van gegevens.[16] De organisatie moet identificeren welke gevaren digitale veiligheid kunnen bedreigen en welke gevolgen een onvoldoende beheersing van digitale veiligheid kan hebben. Hiertoe moet een organisatie de gevaren zo goed mogelijk en op systematische wijze inventariseren, inschatten wat de kans is dat die gevaren optreden en inschatten wat de aard en de omvang van de gevolgen kunnen zijn. Dit wordt veelal aangeduid als een risico-inventarisatie en -evaluatie (RI&E). Een organisatie doet dit het best aan de hand van een eenvoudige beschrijving van scenario's. Een scenario beschrijft welke ongewenste gebeurtenis zou kunnen optreden (bijvoorbeeld het hacken van een website) en welke mogelijke gevolgen dit zou kunnen hebben (de inhoud van de website wordt aangepast, of via de website krijgt een hacker toegang tot de computersystemen van de organisatie).

Op basis van de risico-inventarisatie en -evaluatie dient een organisatie te bepalen welke gevaren zij tot welk niveau beheerst. Zij formuleert hiertoe bij voorkeur meetbare doelstellingen. Hierbij moet worden opgemerkt dat een gebrek aan digitale veiligheid niet alleen de eigen organisatiedoelstellingen maar ook belangen van anderen raakt. Zo heeft het onbevoegd kopiëren van gegevens misschien niet noodzakelijk negatieve consequenties voor de organisatie, maar mogelijk wel voor degenen op wie de gegevens betrekking hebben. In de hierboven bedoelde afweging kan de organisatie dus niet slechts haar eigen belangen betrekken, maar dient zij nadrukkelijk ook de belangen van deze derden mee te wegen.

16 'Verwerken' wordt hier gebruikt in de zin van Wet bescherming persoonsgegevens, en omvat elke handeling die met gegevens wordt uitgevoerd.

3.1.2 Veiligheidsmanagement realistisch en expliciet vastgelegd

Het tweede uitgangspunt van veiligheidsmanagement is dat een organisatie op basis van de RI&E een veiligheidsaanpak formuleert. Deze aanpak is realistisch, wat betekent dat uitvoering ervan werkelijk zal leiden tot het behalen van de geformuleerde veiligheidsdoelstellingen. Een realistische veiligheidsaanpak richt zich dus ook op het beheersen van bedreigingen die de belangen van derden raken. Bovendien heeft deze aanpak oog voor het feit dat ongewenste gebeurtenissen nooit volledig kunnen worden uitgesloten, en voorziet deze dus ook in maatregelen die de gevolgen van deze gebeurtenissen beperken.

Een realistische veiligheidsaanpak voorziet in een heldere verdeling van taken, bevoegdheden en verantwoordelijkheden van alle betrokkenen. Bovendien voorziet hij niet alleen in het voorkomen van gevaren, maar ook in herstelmaatregelen die de gevolgen van een ongewenste gebeurtenis beperken. Terugval- en herstelscenario's maken daar onderdeel van uit. Een realistische veiligheids-aanpak past ten slotte in het kader van vigerende wet- en regelgeving, brancherichtlijnen en *best practices.*

3.1.3 Veiligheidsmanagement uitvoeren

Ten derde moet de organisatie de veiligheidsaanpak uitvoeren. Dit betekent onder meer dat zij degenen die een rol in de veiligheidsaanpak hebben in staat stelt invulling te geven aan hun taken, bevoegdheden en verantwoordelijkheden. Hiervoor stelt zij onder meer voldoende middelen beschikbaar, voorziet in actuele procesbeschrijvingen en zorgt ervoor dat de betrokkenen voldoende deskundig zijn. Ook moet de organisatie op alle niveaus toezien op strikte naleving van de veiligheidsaanpak.

Het is van belang dat alle functionarissen binnen een organisatie precies weten welk aandeel zij hebben in het waarborgen van digitale veiligheid, hoe digitale veiligheid zich verhoudt tot hun takenpakket en wat van hen wordt verwacht, bijvoorbeeld ten aanzien van het gebruik van e-mail en gegevensdragers als usb-sticks. De veiligheidsaanpak moet duidelijk maken dat iedereen binnen een organisatie een rol heeft in het waarborgen van digitale veiligheid.

Bij het beheersen van de veiligheid van een bedrijfsproces, zoals de elektronische verwerking van persoonsgegevens, kunnen meerdere organisaties betrokken zijn. In een dergelijk geval is het belangrijk dat die organisaties duidelijke afspraken maken over ieders taken, bevoegdheden en verantwoordelijkheden ten aanzien van het waarborgen van de veiligheid. Voorts is van belang dat zij er niet slechts op vertrouwen dat de ander deze afspraken naleeft, maar afspreken hoe zij over en weer toezien op naleving ervan. Alleen zo kan betrouwbaarheid worden gewaarborgd. Dit geldt voor alle samenwerkingsvormen tussen organisaties, dus zowel voor ketenpartners als voor opdrachtgevers en opdrachtnemers.

3.1.4 Aanscherpen veiligheidsaanpak

Om gestelde veiligheidsdoelstellingen te kunnen blijven behalen, moet de organisatie de veiligheidsaanpak steeds aanscherpen. Hiertoe moet zij gegevens verzamelen over het functioneren van de aanpak, bijvoorbeeld aan de hand van periodieke (interne) *audits*, maar ook door incidentenonderzoek. Naar aanleiding van deze gegevens moet de effectiviteit van de getroffen beheersmaatregelen worden geëvalueerd, en moeten deze zo nodig worden aangepast.

Best practices spelen hierbij een belangrijke rol, maar ook ongewenste gebeurtenissen. Een voor-beeld van een dergelijke ongewenste gebeurtenis is een internetstoring, waarbij gegevens niet op de normale tijd en manier kunnen worden verzonden. Ongewenste gebeurtenissen ontstaan alleen maar als er afwijkingen plaatsvinden op de geplande processen. Ongeplande afwijkingen op de geplande processen zijn daarom de eerste aanwijzingen dat er iets fout zou kunnen gaan en daarom heel zinvol om (vroegtijdig) van te leren. In het voorbeeld van de internetstoring zou het kunnen zijn dat, door de verzending op een ander moment, gebruikelijke controles niet of op een andere wijze plaatsvinden waardoor het proces op dat moment gevoelig wordt voor fouten.

3.1.5 Veiligheidsmanagement een verantwoordelijkheid van het management

Voor het functioneren van de veiligheidsaanpak is betrokkenheid van het management van de organisatie essentieel. Het management dient verantwoordelijkheid te nemen voor het formuleren en behalen van de veiligheidsdoelstellingen die aansluiten op de primaire processen van de organisatie, en voor het opstellen van een daarbij passende veiligheidsaanpak. Ook dient het management zich betrokken te tonen bij de uitvoering van die aanpak. Dit betekent dat het zich periodiek laat informeren over de uitvoering en effectiviteit van de veiligheidsaanpak, beslist welke gegevens het hiervoor nodig heeft, en op basis hiervan sturing geeft.

Ten slotte dient het management het belang van digitale veiligheid zichtbaar uit te dragen *(tone from the top)*. Dit is in het bijzonder van belang binnen organisaties waar de verwerking van elektronische gegevens niet gezien wordt als een primair bedrijfsproces. In organisaties waar van een proactieve, risicobewuste cultuur op het gebied van informatieveiligheid (nog) geen sprake is, moet het management deze bevorderen.

Burgers en bedrijven moeten weten hoeveel veiligheid zij kunnen verwachten. De betrokken partijen moeten er daarom helder over zijn dat het elektronische gegevensverkeer nooit volledig veilig is. Er zullen incidenten voorkomen. Hierbij is het van belang dat het management van een organisatie aangeeft wat de overgebleven risico's zijn en wat de organisatie doet als een incident zich voordoet.

3.1.6 Veiligheidsmanagement leidt tot proportionele risicobeheersing

Een goede toepassing van de uitgangspunten van veiligheidsmanagement geeft een organisatie veel mogelijkheden om greep te krijgen op haar bedrijfsvoering, en waarborgt daarmee een hoge mate van risicobeheersing. De hier geschetste beginselen van veiligheidsmanagement vormen een leercirkel die continue verbetering mogelijk maakt. Een organisatie kan dan steeds in kaart brengen welke risico's nog onvoldoende zijn afgedekt om ze beheersbaar te noemen. Op enig moment bereikt de organisatie dan het punt dat de kosten van verder investeren in reductie van de risico's niet in verhouding staan tot de daarmee gerealiseerde toename van veiligheid. Op dat moment is het restrisico zo gering als redelijkerwijs mogelijk is.[17] Het feit dat er altijd een restrisico zal zijn is vanzelfsprekend geen vrijbrief voor digitale onveiligheid. Er moet altijd gezocht worden naar een manier om dit risico zo veel als redelijkerwijs mogelijk te verkleinen.

3.2 Wet- en regelgeving

Deze paragraaf beschrijft de wet- en regelgeving die richtinggevend is in dit onderzoek. Hij bevat een kort overzicht van wetten, Europese richtlijnen en verdragen.[18]

3.2.1 Europese Richtlijnen en wetgeving

Bepalingen ten aanzien van de veiligheid van digitale gegevens vloeien overwegend voort uit het grondrecht op eerbiediging van de persoonlijke levenssfeer en de beperkingen die dit recht impliceert voor de (geautomatiseerde) verwerking van persoonsgegevens. Onder meer het verdrag van Straatsburg, de Europese richtlijn inzake de bescherming van persoonsgegevens en de Nederlandse Grondwet geven hierover nadere bepalingen.[19] Die komen er kortweg op neer dat er een noodzaak moet zijn voor de verwerking van persoonsgegevens, en dat degene die persoonsgegevens verwerkt een zo groot mogelijke zorgvuldigheid moet betrachten.

17 Dit wordt ook wel aangeduid als ALARP: *as low as reasonably practicable*.

18 Deze en volgende paragrafen beschrijven het stelsel van wet- en regelgeving zoals van toepassing ten tijde van de affaire-DigiNotar. Naar aanleiding van het incident is de wet- en regelgeving op een aantal punten aangepast.

19 Zie CETS 108, verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens. Raad van Europa, Straatsburg 1981. Door Nederland geratificeerd in 1990; Richtlijn 95/46/EG, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens; artikel 10 Grondwet.

Voor andere dan persoonsgegevens geldt dat wie deze verwerkt de plicht heeft om hiermee zorgvuldig om te springen, om andere belanghebbenden bij deze gegevens (zoals degene op wie ze betrekking hebben) niet onevenredig in hun belangen te schaden. Deze verplichting kent niet één wettelijke oorsprong, maar berust op maatschappelijke normen in het verkeer tussen burgers onderling, en tussen burgers en overheden.[20]

In de Wet bescherming persoonsgegevens (Wbp) wordt de beveiliging van persoonsgegevens nader uitgewerkt. De Wet bepaalt hierover het volgende:

"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen." (art. 13 Wbp)

Onder 'onrechtmatige verwerking' vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. In het begrip 'passende' ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek, maar ook met de aard van de te beschermen gegevens. Technische en organisatorische maatregelen dienen hiertoe cumulatief te worden getroffen.[21]

Om de voorgeschreven beveiligingsdoelstelling te bereiken, schrijft de Wet niet het gebruik van specifieke maatregelen voor, noch de vereisten waaraan zulke middelen moeten voldoen. Evenmin doet de Wet uitspraken over de wijze waarop verantwoordelijken de veiligheid van informatie organisatorisch moeten borgen. Wel is in andere wetten vastgelegd hoe specifieke gegevens of specifieke registraties beveiligd dienen te worden.[22]

3.2.2 Regels en voorschriften

Naast wetten in formele zin, Europese richtlijnen en verdragen wordt het waarborgen van informatieveiligheid door overheidsorganisaties gereguleerd in enkele regels en voorschriften.

Voorschrift informatiebeveiliging rijksdienst (VIR)

Het Voorschrift bepaalt hoe onderdelen van de rijksoverheid (ministeries en daaronder ressorterende diensten en bedrijven) moeten omgaan met het waarborgen van informatieveiligheid.[23] Het Voorschrift stelt globale eisen aan het informatiebeveiligingsbeleid dat deze organisaties moeten opstellen. De secretaris-generaal van elk ministerie stelt dit beleid vast, draagt dit uit en legt verantwoording af.

Krachtens het Voorschrift is het lijnmanagement verantwoordelijk voor de beveiliging van zijn informatiesystemen. Lijnmanagers moeten daartoe een risico-inventarisatie uitvoeren en de gewenste mate van beveiliging vaststellen, beheersmaatregelen kiezen en implementeren, toezien op de implementatie van die maatregelen en het geheel periodiek evalueren.

Voorschriften lagere overheden

Lagere overheden mogen eigen informatieveiligheidsbeleid formuleren. Zij hebben in beginsel volledige vrijheid om zelf te bepalen of en hoe zij dit doen. De wijze waarop lagere overheden invulling geven aan hun informatieveiligheidsbeleid vertoont dan ook grote onderlinge verschillen (zie verder hoofdstuk 6).

---

20 Zie in dit verband ook de wettelijke definitie van de onrechtmatige daad in het privaatrecht (art 6:162 BW), en de algemene beginselen van behoorlijk bestuur in het bestuursrecht.

21 Memorie van toelichting Wbp. Kamerstuk TK 25892-3.

22 Voorbeelden hiervan zijn de elektronische verwerking van politiegegevens, zoals geregeld in de Wet politiegegevens, de elektronische verwerking van gegevens in de keten werk en inkomen, zoals geregeld in de Wet SUWI en de verwerking van gegevens in de Gemeentelijke Basisadministratie, zoals geregeld in de Wet GBA.

23 Op informatie waarmee staatsbelangen zijn gemoeid, is het VIR – Bijzondere Informatie (VIR-BI) van toepassing.

3.3 Normen, standaarden, handboeken, *best practices*

Het veld van informatiebeveiliging en digitale veiligheid kenmerkt zich door zelfregulering. Hierin spelen (certificeerbare) internationale normen en standaarden een grote rol. Ook de wetgeving verwijst naar deze normen voor de invulling van het beleid ten aanzien van informatiebeveiliging en digitale veiligheid. Er bestaan talloze normen en standaarden voor informatiebeveiliging, die verschillen vertonen in toepassingsgebied, reikwijdte en diepgang. Het is aan elke organisatie om te bepalen of en aan welke normen zij zich wil conformeren.

3.3.1 ISO 27000-reeks

Ten aanzien van informatiebeveiliging heeft het College Standaardisatie in 2008 twee ISO-normen aangewezen als open standaard voor de gehele publieke sector, waarop het 'pas toe of leg uit'-principe van toepassing is.[24] Dit betekent dat alle organisaties in de publieke sector gehouden zijn te voldoen aan deze normen, tenzij zij met redenen omkleed kunnen aangeven waarom zij daarvan afwijken. Deze normen zijn de ISO 27001 en ISO 27002 die hieronder nader worden toegelicht.

De ISO 27000-serie is een gezaghebbende normenreeks voor informatieveiligheid, die tevens aan de basis staat van een aantal richtlijnen en handboeken, zoals het VIR en de handreiking informatiebeveiliging gemeenten (zie verderop in deze paragraaf). De reeks bestaat uit een aantal normen, die verschillende aspecten van informatieveiligheidsbeleid belichten.

ISO 27001

Deze norm specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd managementsysteem voor informatiebeveiliging (ISMS).[25] Tegen deze norm is certificering mogelijk. ISO 27001 kent een structuur die vergelijkbaar is met die van andere ISO-normen voor managementsystemen, zodat een organisatie deze managementsystemen op elkaar kan afstemmen of met elkaar kan integreren. De norm volgt de principes van het Plan-Do-Check-Act model of leercyclus. De eisen in de norm zijn algemeen en van toepassing voor alle typen organisaties: commercieel, overheid, non-profit.

De eisen in de norm hebben betrekking op de volgende onderdelen van het ISMS:

- vaststellen en beheren van het ISMS, waaronder de organisatie van informatiebeveiliging;
- implementeren en uitvoeren van het ISMS;
- controleren en beoordelen van het ISMS;
- bijhouden en verbeteren van het ISMS;
- documentatie, documentatiebeheersing en beheersing van registratie;
- directieverantwoordelijkheid waaronder betrokkenheid van de directie, beheer van middelen, training, bewustzijn en bekwaamheid van personeel;
- het uitvoeren van interne ISMS-audits;
- directiebeoordeling van het ISMS en verbetering van het ISMS waaronder continue verbetering, corrigerende en preventieve maatregelen.

Per onderdeel van het ISMS geeft de norm de doelstelling en de bijbehorende beheersmaatregel(en). Hiervan is in Figuur 1: Systematiek van ISO 27001figuur 1 een voorbeeld opgenomen.

24 Open standaarden beogen de digitale samenwerking tussen overheidsorganisaties en marktpartijen te vergroten, en de leveranciersafhankelijkheid te verminderen. Het gebruik van open standaarden is onder meer vastgelegd in de bestuursakkoorden tussen Rijk, gemeenten en provincies (2007, 2008), de Overheidsbrede implementatie-agenda voor dienstverlening en e-overheid (2011), en de Digitale agenda 2011 – 2015 (2011).

25 NEN-ISO/IEC 27001:2005, Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen. ICS 35.040, november 2005.

A.7 Beheer van bedrijfsmiddelen		
A.7.1 *Verantwoordelijkheid voor bedrijfsmiddelen* ***Doelstelling:*** Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.		
A.7.1.1	Inventarisatie van bedrijfsmiddelen	*Beheersmaatregel* Alle bedrijfsmiddelen moeten duidelijk zijn geïdentificeerd en er moet een inventaris van alle belangrijke bedrijfsmiddelen worden opgesteld en bijgehouden.

Figuur 1: Systematiek van ISO 27001

ISO 27002
Deze norm staat bekend als de Code voor informatiebeveiliging.[26] Hij geeft voor 39 hoofdbeveiligingscategorieën aan, welke beheersmaatregelen gehanteerd moeten worden. Voor het toepassen van de Code voor informatiebeveiliging geldt het 'pas toe of leg uit'-principe.

De norm geeft richtlijnen en algemene principes voor het initiëren, implementeren, handhaven en verbeteren van informatiebeveiliging in een organisatie. Hij kan dienen als praktische handleiding voor het opstellen van beveiligingsnormen en doeltreffend beheer van informatiebeveiliging die specifiek op de organisatie zijn toegesneden.

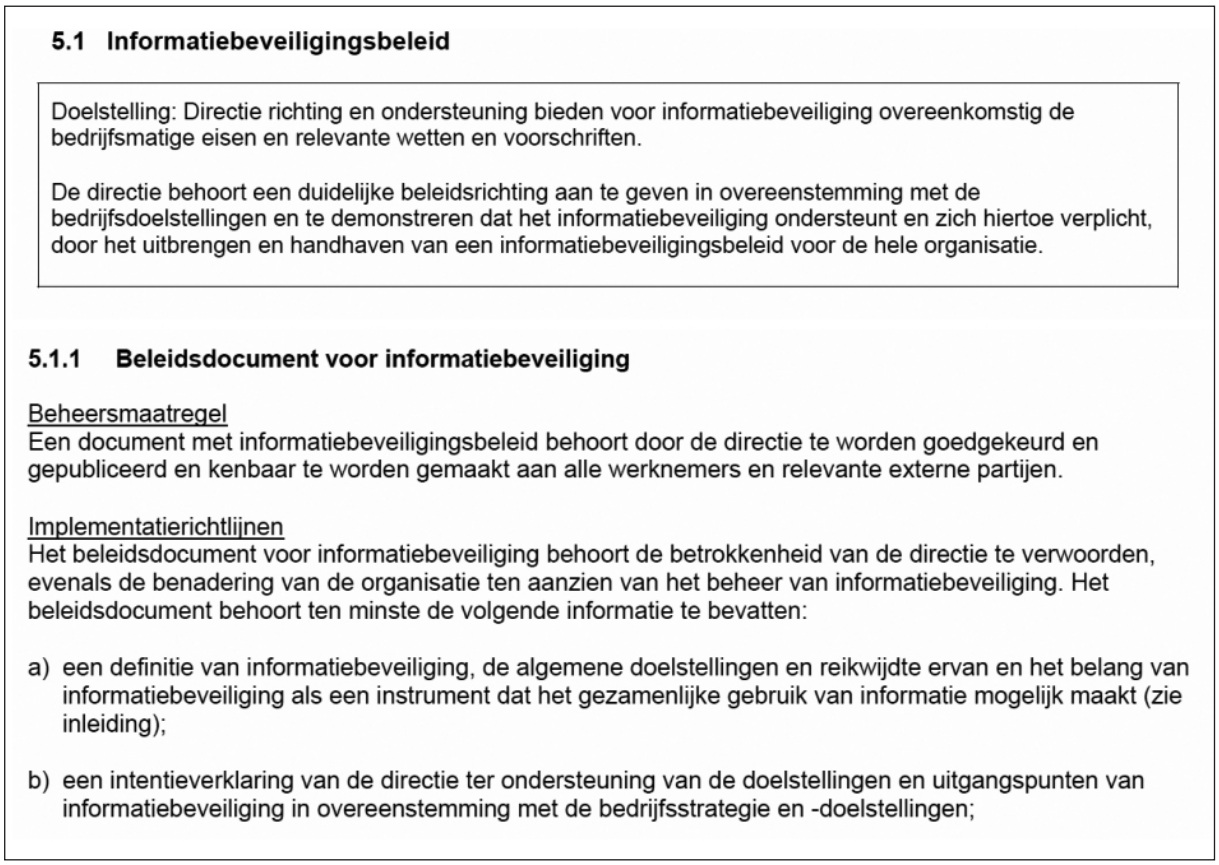
Volgens de norm is informatie een bedrijfsmiddel (*asset*), dat net als andere bedrijfsmiddelen waarde heeft en voortdurend op een geschikte manier moet zijn beschermd. Informatiebeveiliging is volgens de norm daarom belangrijk voor alle organisaties en instanties in de publieke en private sector en voor bescherming van vitale infrastructuur. De norm stelt dat veel informatiesystemen niet ontworpen zijn met het oog op veiligheid en dat de beveiliging die met technische middelen kan worden bereikt, beperkt is. De beveiliging met behulp van technische middelen dient te worden ondersteund door geschikt beheer en procedures, zoals beschreven in de norm.

De norm gaat in op een aantal succesfactoren die van wezenlijk belang geacht worden voor een geslaagde implementatie van informatiebeveiliging in een organisatie. Een daarvan is dat het informatiebeveiligingsbeleid, de doelstellingen en activiteiten de bedrijfsdoelstellingen weerspiegelen.

De norm heeft betrekking op de volgende onderwerpen: een algemene inleiding over risicobeoordeling en risicobehandeling; beveiligingsbeleid; organisatie van informatiebeveiliging; beheer van bedrijfsmiddelen; beveiliging van personeel; fysieke beveiliging en beveiliging van de omgeving; beheer van communicatie- en bedieningsprocessen; toegangsbeveiliging; verwerving, ontwikkeling en onderhoud van informatiesystemen; beheer van informatiebeveiligingsincidenten; bedrijfscontinuïteitsbeheer en naleving.

Per hoofdbeveilingscategorie geeft de norm de doelstelling, beheersmaatregel, implementatierichtlijnen en overige informatie weer. Hiervan is inFiguur 2: Systematiek van ISO 27002 figuur 2 een voorbeeld opgenomen.

26 NEN-ISO/IEC 27002:2005, Informatietechnologie – Beveiligingstechnieken – Code voor informatiebeveiliging. ICS 35.040, november 2007.



5.1 Informatiebeveiligingsbeleid

Doelstelling: Directie richting en ondersteuning bieden voor informatiebeveiliging overeenkomstig de bedrijfsmatige eisen en relevante wetten en voorschriften.

De directie behoort een duidelijke beleidsrichting aan te geven in overeenstemming met de bedrijfsdoelstellingen en te demonstreren dat het informatiebeveiliging ondersteunt en zich hiertoe verplicht, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid voor de hele organisatie.

5.1.1 Beleidsdocument voor informatiebeveiliging

Beheersmaatregel
Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

Implementatierichtlijnen
Het beleidsdocument voor informatiebeveiliging behoort de betrokkenheid van de directie te verwoorden, evenals de benadering van de organisatie ten aanzien van het beheer van informatiebeveiliging. Het beleidsdocument behoort ten minste de volgende informatie te bevatten:

a) een definitie van informatiebeveiliging, de algemene doelstellingen en reikwijdte ervan en het belang van informatiebeveiliging als een instrument dat het gezamenlijke gebruik van informatie mogelijk maakt (zie inleiding);

b) een intentieverklaring van de directie ter ondersteuning van de doelstellingen en uitgangspunten van informatiebeveiliging in overeenstemming met de bedrijfsstrategie en -doelstellingen;

Figuur 2: Systematiek van ISO 27002

De Onderzoeksraad merkt op dat een werkend managementsysteem voor informatiebeveiliging vooral bepaald wordt door de wijze waarop de norm ISO 27001 wordt toegepast. ISO 27002 beoogt handreikingen te geven die zien op een praktische uitwerking daarvan. Niettemin blijft altijd een vertaalslag nodig die recht doet aan de bijzonderheden van de organisatie. Het is aan organisaties zelf om aan beide normen invulling te geven.

3.3.2 Overige normen, standaarden en best practices

NORA-dossier informatiebeveiliging
De Nederlandse Overheid Referentie Architectuur (NORA) is het gedeelde kader voor het ontwerpen van ICT-architecturen door alle overheidsorganisaties in Nederland. Het NORA-dossier biedt verschillende architectuurmodellen voor informatiebeveiliging, die de betrokken organisaties kunnen gebruiken als referentiemodel voor het vormgeven van hun informatieveiligheidsbeleid.

Handreiking informatiebeveiliging gemeenten
Het Kwaliteitsinstituut Nederlandse Gemeenten (KING) geeft een handreiking uit die Nederlandse gemeenten aanknopingspunten biedt om beveiligingsbeleid te ontwikkelen en te implementeren. De handreiking onderscheidt maatregelen op strategisch, tactisch en operationeel niveau.

Handboeken informatiebeveiliging
De Vereniging van Coördinatoren Informatievoorziening en Automatisering in Nederlandse Gemeenten (VIAG) geeft een handboek informatiebeveiliging uit dat alle facetten behandelt van het informatieveiligheidsbeleid van een gemeentelijke organisatie. Een vergelijkbaar handboek wordt uitgegeven door het Platform voor Informatiebeveiliging (PvIB).[27]

27 VIAG Handboek informatiebeveiliging (2005); Hintzbergen et al. (2011), *Basiskennis beveiligen van informatie*. Zaltbommel: Van Haren Publishing.

Information security governance framework
Er bestaat een omvangrijke literatuur over de governance van informatieveiligheid, die zich richt op de vraag op welke manieren bestuurders kunnen waarborgen dat hun organisatie de gestelde doelen op het gebied van informatieveiligheid bereikt. Vermeldenswaard in dit opzicht is een tweetal praktische handreikingen voor eindverantwoordelijken in organisaties, respectievelijk uitgegeven door het Nederlandse CIO platform en het Amerikaanse IT Governance Institute.[28]

3.4 Certificaatdienstverlening

Deze paragraaf gaat in op wet- en regelgeving die van toepassing is op het leveren van digitale certificaten en daarmee verbonden diensten. Hiervoor gelden in beginsel geen wettelijke vereisten. Iedereen die dat wenst, kan certificaatdiensten aanbieden. Er is echter een aantal uitzonderingen, dat in de navolgende paragrafen wordt besproken.

Wet- en regelgeving inzake gekwalificeerde certificaten
Een van de uitzonderingen vormen zogeheten gekwalificeerde certificaten. Omdat deze certificaten onder meer de grondslag vormen van de rechtsgeldige elektronische handtekening, is bij de Telecommunicatiewet vastgelegd aan welke eisen deze certificaten en de wijze van uitgifte ervan moeten voldoen.[29] Het Besluit elektronische handtekeningen stelt hiertoe open normen. De Regeling elektronische handtekeningen stelt bovendien dat een certificaatdienstverlener vermoed wordt aan deze normen te hebben voldaan, wanneer hij voldoet aan de vereisten in de Europese ETSI-norm TS 101 456 (zie onder).

Regels inzake PKIoverheid
Een andere uitzondering wordt gevormd door PKIoverheid, de public key infrastructure die de rijksoverheid zelf heeft ingericht. Binnen PKIoverheid gelden de regels zoals het ministerie van Binnenlandse Zaken en Koninksrijksrelaties die heeft vastgelegd in het Programma van Eisen PKIoverheid (verder: PvE PKIo). Het stelsel van regels en afspraken op basis waarvan PKIoverheid functioneert, wordt in detail besproken in hoofdstuk 5.

ETSI-normen
De European Telecommunications Standards Institute (ETSI) is een door de Europese Unie erkend standaardisatie-instituut voor de telecommunicatiebranche. De European Telecommunications Standards Institute heeft een tweetal normen opgesteld waaraan certificaatdienstverleners hun processen kunnen toetsen.[30] Deze normen beschrijven de voorwaarden waaraan certificaatdienstverleners bij de inrichting van hun ICT-systemen en hun werkprocessen moeten voldoen. Beide normen zijn voor een belangrijk deel als open normen geformuleerd, en moeten door de certificaatdienstverleners zelf nader worden ingevuld.

ETSI TS 101 456
Deze norm heeft betrekking op het leveren van certificaatdiensten met betrekking tot gekwalificeerde certificaten in de zin van de Europese richtlijn 1999/93/EC inzake de elektronische handtekening. Bijlagen I en II bij deze richtlijn bevatten generiek geformuleerde eisen ten aanzien van gekwalificeerde certificaten en certificaatdienstverleners die deze certificaten afgeven. De ETSI-norm is op te vatten als een operationalisatie van deze eisen, maar specificeert uitdrukkelijk niet hoe naleving ervan getoetst kan worden.

28 Informatiebeveiliging in control (CIO Platform Nederland, 2007); Information Security Governance. Guidance for Boards of Directors and Executive Management (IT Governance Institute, 2006).
29 Op grond van artikel 18.15 Telecommunicatiewet. Dit is de Nederlandse implementatie van de Europese Richtlijn 99/93/EG, betreffende een gemeenschappelijk kader voor elektronische handtekeningen.
30 ETSI TS 101 456, *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates*; ETSI TS 102 042, *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*. European Telecommunications Standards Institute. Deze normen zijn zogenaamde *technical specifications*. Een TS bevat normatieve vereisten en wordt opgesteld door een technisch comité waarin leden van ETSI vertegenwoordigd zijn voor wie de inhoud van de standaard relevant is. Anders dan een *European standard* (EN) kent de totstandkoming van een TS geen inzageprocedure.

De eerste hoofdstukken van de ETSI-norm schetsen de generieke inrichting van een certificaatdienstverlener, de structuur van (Europese) wet- en regelgeving die ziet op zijn diensten, en de rechten en plichten van de certificaatdienstverlener versus die van andere betrokken partijen. De hoofdstukken 7 en 8 bevatten de vereisten waaraan een certificaatdienstverlener moet voldoen. Deze vereisten hebben betrekking op de inhoud van het certification practice statement, het beheer van geheime sleutels, de uitgifte en intrekking van certificaten, management en bedrijfsvoering, en algemene inrichtingseisen.

Alle vereisten zijn zo geformuleerd dat zij enerzijds een nadere invulling geven aan de open geformuleerde eisen uit de Europese richtlijn, maar anderzijds wel nog een specifieke 'vertaalslag' vergen door de certificaatdienstverlener zelf. Zo bevat de ETSI-norm geen concrete voorschriften ten aanzien van te hanteren technologieën of werkvoorschriften, maar geeft slechts de randvoorwaarden waaraan deze moeten voldoen. Bij wijze van voorbeeld wordt hieronder één vereiste aangehaald dat representatief is voor de mate van concreetheid van de ETSI-norm:

Article 7.2.1, key generation
d. the selected key length and algorithm for CA signing key shall be one which is recognized as being fit for the purposes of qualified certificates as issued by the CA

Dit vereiste verplicht de certificaatdienstverlener om eerst zelf vast te stellen voor welke doeleinden de door hem uit te geven gekwalificeerde certificaten bestemd zijn, om vervolgens aan de hand hiervan te bepalen hoe complex de sleutel moet zijn waarmee hij deze certificaten bekrachtigt. Door ETSI worden regelmatig aanbevelingen op dit gebied gedaan, die partijen naar eigen inzicht kunnen opvolgen. Veruit de meeste vereisten in de ETSI-norm zijn op een dergelijke manier geformuleerd. Dit legt de verantwoordelijkheid bij de certificaatdienstverlener zelf en bij de partijen aan wie deze verantwoording verschuldigd is, om te bepalen welke invulling van de vereisten acceptabel is.

Certificeringsschema TTP.NL
Certificaatdienstverleners kunnen hun managementsysteem door een geaccrediteerde auditor laten certificeren volgens het certificeringsschema TTP.NL. Voor certificaatdienstverleners die PKIoverheid-certificaten aanbieden, is dit verplicht. Voor certificering moet een certificaatdienstverlener voldoen aan de voor hem geldende wettelijke voorschriften en de hierboven genoemde ETSI-normen. Voorts moet hij periodiek de eigen bedrijfsvoering onderzoeken op naleving van deze voorschriften, en waarborgen dat ook partijen met wie hij samenwerkt daaraan, voor zover van toepassing, voldoen.

Het certificeringsschema schrijft voor dat de auditerende instelling zowel documentenonderzoek als een implementatie-audit verricht, uitgevoerd door ter zake gekwalificeerde auditors.[31] Hun handelwijze moet voldoen aan de daarvoor relevante ISO-normen. Aan de verklaring mag volgens dit schema een gerechtvaardigd vertrouwen (justified confidence) worden ontleend dat de certificaatdienstverlener aan de vereisten in eerder genoemde ETSI-normen voldoet.

3.5 Conclusie

De Onderzoeksraad gaat in dit onderzoek uit van het hiervoor beschreven beoordelingskader. De essentie van dit beoordelingskader is vastgelegd in de vijf uitgangspunten voor veiligheidsmanagement zoals de Onderzoeksraad die hanteert. Het gaat er daarbij om dat een organisatie verantwoordelijkheid neemt voor zowel de risico's die verband houden met de bedrijfsvoering.

31 Een implementatie-audit beoordeelt of de plannen in de documenten daadwerkelijk in de organisatie zijn geïmplementeerd.

De uitgangspunten in dit hoofdstuk hebben betrekking op overheidsorganisaties die verantwoordelijk zijn voor het waarborgen van digitale veiligheid, maar ook op partijen die op enige manier een rol spelen in het verstrekken van digitale certificaten. Als aan deze punten wordt voldaan, heeft de betrokken organisatie op onverwachte en ongewenste, maar niet onvoorziene gebeurtenissen een antwoord. Dat hoeft geen pasklaar antwoord te zijn, maar kan bijvoorbeeld zijn het opschalen naar een crisisorganisatie of het doorlopen van een stappenplan voor herstel.

Ten aanzien van de van toepassing zijnde wet- en regelgeving, zowel op het gebied van informatieveiligheid als op het gebied van certificaatdienstverlening, constateert de Onderzoeksraad dat deze open geformuleerde bepalingen bevat. Wetten en regels schrijven niet in detail voor welke maatregelen een organisatie moet treffen, maar slechts welke doelen zij moet bereiken. In het domein van informatieveiligheid is de wet- en regelgeving bovendien overwegend procedureel van aard; hij beschrijft uitgebreid het beheerssysteem dat een organisatie moet inrichten om informatieveiligheid te waarborgen, maar niet waarin die informatieveiligheid precies moet bestaan.

De alomtegenwoordigheid van open normen is begrijpelijk, aangezien zowel informatieveiligheid als certificaatdienstverlening sterk leunt op het gebruik van technologie die zich nog altijd in hoog tempo ontwikkelt. Het voorschrijven van concrete maatregelen is in zo'n situatie onwenselijk. Wat vandaag de best denkbare maatregel is, kan immers morgen achterhaald zijn. Het beschrijven van te behalen doelen, zoals de regelgeving overwegend doet, is dan een betere optie. Dit betekent echter wel dat elke organisatie een grote eigen verantwoordelijkheid heeft om aan deze open normen adequaat invulling te geven.

De Onderzoeksraad merkt op dat de rijksoverheid ten aanzien van digitale veiligheid een tweeledige verantwoordelijkheid heeft. Zij is – vanzelfsprekend – verantwoordelijk voor de kwaliteit van de voorzieningen die zij zelf ter beschikking stelt aan overheidsorganisaties, om de digitale veiligheid te waarborgen. Daarnaast heeft zij, naar het oordeel van de Onderzoeksraad, een verantwoordelijkheid om zodanige omstandigheden te scheppen dat afzonderlijke (overheids)organisaties optimaal invulling geven aan hun eigen verantwoordelijkheid voor het waarborgen van digitale veiligheid. Deze laatste verantwoordelijkheid wordt verder aangeduid als de stelselverantwoordelijkheid van de rijksoverheid voor digitale veiligheid.

4 HET DIGINOTARINCIDENT

Dit hoofdstuk gaat in op de inbraak bij DigiNotar en de wijze waarop de betrokken partijen hiermee omgingen. De gebeurtenissen beslaan de periode tussen 19 juli 2011, de dag waarop DigiNotar de eerste vervalste certificaten op haar bedrijfssystemen aantrof, en zaterdagochtend 3 september 2011, de persconferentie van toenmalig minister Donner van Binnenlandse Zaken en Koninkrijksrelaties. Zoals eerder is aangegeven, reconstrueert dit rapport niet tot in detail het verloop van de crisisbeheersing. Dit is onderzocht door de Inspectie Veiligheid en Justitie.

Korte bedrijfsgeschiedenis DigiNotar B.V.
DigiNotar werd in 1997 op initiatief van de toenmalige Koninklijke Notariële Broederschap opgericht om, onder meer door het uitgeven van digitale certificaten, technologische ondersteuning te bieden aan notarissen die hun dienstverlening uitbreidden tot de elektronische wereld. Het bedrijf bood, naast certificaatdiensten, onder meer diensten aan met betrekking tot gewaarmerkte archivering en de beveiligde uitwisseling van documenten.

In 2003, kort na de inwerkingtreding van de Wet op de elektronische handtekeningen, liet DigiNotar zich registreren bij de OPTA als leverancier van gekwalificeerde certificaten. Gaandeweg trok het bedrijf een bredere klantenkring aan waartoe ook allerlei overheidsorganisaties behoorden, zoals de Belastingdienst.

In 2004 trad het bedrijf toe tot PKIoverheid, het stelsel van de rijksoverheid voor het verstrekken van met extra waarborgen omgeven digitale certificaten. Sindsdien verstrekte DigiNotar PKIoverheid-certificaten aan een groeiend aantal overheidsorganisaties. Naast PKIoverheid-certificaten verstrekte DigiNotar ook eigen certificaten aan zowel private als overheidspartijen. Tot deze categorie behoorden onder meer de BAPI-certificaten waarmee de Belastingdienst zijn gegevensverkeer beveiligt.[32]

In 2006 verwierf DigiNotar het Webtrust-keurmerk voor certificaatdienstverleners. Hiervoor werd het bedrijf jaarlijks onderworpen aan een onderzoek door een auditerende instelling. Tevens was het bedrijf, als leverancier van gekwalificeerde en PKIoverheid-certificaten, in het bezit van een TTP.NL-verklaring. Ook hiervoor werd het bedrijf jaarlijks onderzocht.

In 2011 werd DigiNotar overgenomen door het Amerikaanse Vasco Data Security International Inc. (hierna: Vasco). Met de overname wilde Vasco met name toegang krijgen tot de kennis die DigiNotar bezat op het gebied van certificaatdienstverlening. Vasco wilde de kennis en expertise van DigiNotar inzetten ten behoeve van hun eigen diensten voor bestaande en nieuwe klanten wereldwijd.

Dit hoofdstuk onderscheidt drie stadia in de inbraak bij DigiNotar. De inbraak zelf wordt besproken in 4.1. De ontdekking van de inbraak en de aanvankelijke reactie komen aan de orde in 4.2. Paragraaf 4.3 behandelt de escalatie van het incident.

De reconstructie van de gebeurtenissen is gebaseerd op documentenonderzoek, gesprekken die de Onderzoeksraad voerde met betrokkenen, en op de uitkomsten van onderzoeken die in opdracht van betrokkenen zijn uitgevoerd. De Onderzoeksraad heeft geen eigen technisch onderzoek laten verrichten naar de inbraak.

32 De Belastingdienst maakt gebruik van dit type certificaten omdat PKIoverheid bij ingebruikname van deze certificaten nog niet beschikbaar was en er later geen noodzaak was over te stappen naar PKIoverheid.

4.1 De inbraak

Gedurende een aaneengesloten periode in de maanden juni en juli van 2011 drong een inbreker via internet door tot de computersystemen van DigiNotar.[33] Via computersystemen (servers) van het bedrijf die in verbinding stonden met het internet verschafte hij zich toegang tot afgeschermde gedeelten van het bedrijfsnetwerk, waaronder ook verscheidene servers waarop zich processen voor certificaatdienstverlening afspeelden. De inbreker slaagde erin beheersrechten voor deze servers te verkrijgen en vervalste digitale certificaten te genereren. Ook slaagde hij erin gebruik te maken van de sleutels waarmee deze certificaten digitaal ondertekend moeten worden als bewijs van hun echtheid.

Digitale certificaten en certificaatdienstverlening
Elektronisch gegevensverkeer wordt beveiligd door gebruik te maken van encryptie. Hiervoor bestaan verschillende technieken, waaronder één die bekend staat als asymmetrische encryptie. Deze techniek is zeer geschikt voor situaties waarin partijen met elkaar communiceren tussen wie geen sprake is van een vooraf gevestigde vertrouwensband, zoals tussen een overheidsorganisatie als publieke dienstverlener en diens 'klanten'.

Asymmetrische encryptie maakt gebruik van twee sleutels, waarmee informatie gecodeerd en gedecodeerd wordt. Deze sleutels vormen een paar; informatie die gecodeerd is met de ene sleutel van het paar, kan alleen worden gedecodeerd met de andere sleutel van het paar. Bovendien is van elk sleutelpaar één sleutel openbaar. Iedereen kan deze sleutel gebruiken om informatie mee te coderen. Alleen degene die beschikt over de corresponderende geheime sleutel, kan deze informatie vervolgens decoderen.[34] Wanneer een overheidsorganisatie de openbare sleutel van een paar beschikbaar stelt aan degene die gegevens moet insturen, heeft deze de zekerheid dat alleen de beoogde ontvanger de gegevens kan decoderen.

Asymmetrische encryptie kan alleen functioneren als de verzender van gegevens erop kan vertrouwen dat de openbare sleutel die hij gebruikt om de gegevens te coderen, werkelijk correspondeert met de geheime sleutel[35] van de ontvangende partij. Als dat niet het geval is, en de verzender maakt (abusievelijk) gebruik van de verkeerde openbare sleutel, dan kan niet de ontvangende partij maar een ander de gegevens decoderen; namelijk, degene die beschikt over de met deze verkeerde openbare sleutel corresponderende geheime sleutel.

Een digitaal certificaat bekrachtigt de relatie tussen een openbare sleutel en de identiteit van de houder van de corresponderende geheime sleutel. Degene die gebruik maakt van een openbare sleutel die is opgenomen op een geldig certificaat, kan er met redelijke zekerheid op vertrouwen dat de inhoud van de aldus gecodeerde boodschap alleen ontcijferd kan worden door de persoon, organisatie of internetdomein die als houder op het certificaat vermeld staat.

Digitale certificaten worden uitgegeven door certificaatdienstverleners. Deze partijen staan ervoor in dat de houder van het certificaat werkelijk degene is aan wie de op het certificaat vermelde sleutel toebehoort.

33 Het is niet zeker of er sprake was van één individuele inbreker of een collectief.
34 Dezelfde techniek wordt ook gebruikt voor gegevensauthenticatie. Deze toepassing blijft in dit rapport buiten beschouwing.
35 Er bestaat ook een vorm van asymmetrische encryptie die geen gebruik maakt van digitale certificaten, maar van zogenaamde *webs of trust*. In deze vorm van encryptie wordt de betrouwbaarheid van een aangeboden publieke sleutel niet bepaald door een certificaat, maar op grond van de berekende betrouwbaarheid van een communicerende partij in een netwerk van *peers*. Deze vorm van encryptie wordt door overheidsorganisaties echter niet gebruikt.

Bij een vervalst certificaat is deze relatie doorbroken. De op het certificaat vermelde sleutel behoort in dat geval niet toe aan de vermelde houder van het certificaat, maar aan een onbevoegde derde partij. Vergelijkbaar als met een vals paspoort kan deze onbevoegde zich voordoen als de houder van het certificaat. De beveiliging is in dat geval niet effectief. Het beveiligde gegevensverkeer vindt immers niet plaats met de vermelde houder van het certificaat, maar met de onbevoegde partij die eigenaar is van de sleutel.

De uitgifte van certificaten verloopt volgens vaste processtappen. In de eerste stap wordt de identiteit van de aanvrager geverifieerd. Vervolgens wordt het certificaat aangemaakt en daarna ondertekend. Als laatste stap wordt het certificaat uitgegeven aan de houder. Afhankelijk van het type certificaat verloopt die uitgifte via internet, of via de overhandiging van een beveiligd medium.

Zo slaagde de inbreker erin om, verspreid over meerdere weken, in elk geval 531 vervalste certificaten te genereren. Van slechts een zeer klein gedeelte daarvan staat vast dat zij daadwerkelijk in omloop zijn gekomen. Van succesvol misbruik in Nederland van in omloop gekomen vervalste certificaten is niets bekend. Wel is in Iran intensief geprobeerd misbruik te maken van een van DigiNotar afkomstig vervalst certificaat, om zo e-mailverkeer te onderscheppen van Iraanse gebruikers van Gmail. Of de pogingen succesvol waren en of dit de betrokken gebruikers in gevaar heeft gebracht, heeft de Onderzoeksraad niet onderzocht.

4.1.1 Staat van de beveiliging DigiNotar

Een gespecialiseerd ICT-beveiligingsbedrijf heeft onderzoek gedaan naar het verloop van de inbraak.[36] Hoewel die slechts in beperkte mate gereconstrueerd kon worden, heeft dat onderzoek vijf omstandigheden geïdentificeerd die ertoe hebben bijgedragen dat de inbraak kon plaatsvinden.

Allereerst heeft DigiNotar niet gehandeld op vroege signalen dat het bedrijf het mikpunt van een gerichte inbraak kon zijn. Uit het onderzoek komt bovendien naar voren dat het netwerk van DigiNotar mogelijk al op 1 juni 2011 voor het eerst door de inbreker benaderd werd, vermoedelijk met het oogmerk verkennende bewegingen uit te voeren.

Het bedrijf was van mening dat er op dat moment geen aanleiding was voor extra maatregelen. Logius, de stelselbeheerder van PKIoverheid, had de aangesloten certificaatdienstverleners in mei en juni 2011 per e-mail op de hoogte gesteld van geïntensiveerde hack-activiteiten.[37] Naar aanleiding van deze mededeling had DigiNotar de betrokken medewerkers hierover geïnformeerd, en enkele IP-adressen geblokkeerd. Het bedrijf zag dit, mede omdat interne en externe audits geen aanleiding gaven om te vermoeden dat de beveiliging niet in orde was (zie 4.1.3), niet als een unieke situatie. DigiNotar werd vaker aangevallen, en had zijn bedrijfsnetwerk uitgerust met een beschermingssysteem (Intrusion Prevention System) dat pogingen tot ongeoorloofde toegang detecteert en vervolgens probeert om deze te blokkeren.

Ten tweede bleek de inbreker in staat om allerlei voorbereidende handelingen uit te voeren op enkele servers in het netwerk van DigiNotar, die hem uiteindelijk in staat stelden dieper in het netwerk door te dringen. Hiertoe heeft hij zwakheden benut in verouderde software op deze servers, wat mogelijk was omdat updates op twee servers ontbraken of niet tijdig waren uitgevoerd.

36 Aanvankelijk werd dit onderzoek uitgevoerd in opdracht van DigiNotar zelf, op last van het agentschap Logius. In een later stadium heeft de rijksoverheid het opdrachtgeverschap overgenomen.

37 In het bijzonder werd in dit bericht verwezen naar een inbraak bij certificaatdienstverlener Comodo, in maart 2011. Naar later bleek, vertoonde de inbraak bij DigiNotar sterke gelijkenissen met deze inbraak.

Ten derde waren de veiligheidskritische gedeelten van het bedrijfsnetwerk waarop de processen voor certificaatuitgifte zich afspeelden niet zodanig afgescheiden van de servers die in verbinding stonden met het internet dat een inbraak voorkomen kon worden. Het onderzoek heeft uitgewezen dat de inbreker erin slaagde verbindingen (zogenaamde *tunnels*) tussen de verschillende segmenten in het netwerk te leggen, omdat de centrale veiligheidsvoorziening in het netwerk (de interne *firewall*) dataverkeer tussen deze segmenten toestond.

Ten vierde lukte het de inbreker om een beheerderswachtwoord te achterhalen waarmee hij beheerderstoegang kreeg tot de servers waarop de software voor certificaatdienstverlening draaide. In dit wachtwoord kwamen bestaande woorden voor, waardoor het middels een zogenaamde *dictionary attack* kon worden achterhaald.

Ten vijfde waren op het afgeschermde deel van het netwerk geheime sleutels aanwezig voor het aanmaken van zogenaamde certificaatherroepingslijsten.[38] De inbreker is erin geslaagd om deze sleutels te gebruiken om de vervalste certificaten die hij had gegenereerd te ondertekenen.

4.1.2 Vigerende regelgeving

DigiNotar leverde zowel standaard, gekwalificeerde en PKIoverheid-certificaten. Op deze drie typen certificaten zijn verschillende regels van toepassing. Ten aanzien van PKIoverheid-certificaten vloeien deze regels voort uit de overeenkomst tussen het bedrijf en de Staat der Nederlanden (zie paragraaf 5.2.4). Op zowel de levering van gekwalificeerde als PKIoverheid-certificaten zijn onder meer de bepalingen uit de ETSI-norm TS 101 456 van toepassing.

Deze ETSI-norm stelt onder meer eisen aan de veiligheid van de computersystemen en netwerken waarvan de processen voor certificaatdienstverlening gebruik maken. Twee bepalingen zijn relevant in het licht van de hierboven geconstateerde feiten. Ten eerste moet de certificaatdienstverlener ervoor zorgen dat computersystemen voor certificaatdienstverlening veilig zijn en juist bediend worden, met een minimaal risico op falen. Ten tweede moet hij ervoor zorgen dat toegang tot de computersystemen voor certificaatdienstverlening beperkt is tot op ordentelijke wijze geautoriseerde personen.[39]

De ETSI-norm bepaalt tevens dat de certificaatdienstverlener een risico-inventarisatie en –evaluatie opstelt als basis voor zijn beveiligingsbeleid, en deze periodiek herziet.[40] Betrokkenen verklaren dat hierin middels verschillende documenten was voorzien.

4.1.3 Periodiek onderzoek, toezicht en handhaving

DigiNotar beschikte over een geldige TTP.NL-verklaring (zie Hoofdstuk 5). Om deze verklaring te verkrijgen en te behouden, werd het bedrijf periodiek onderzocht door een ter zake geaccrediteerde auditerende instelling. Het laatste onderzoek in het kader van TTP.NL vond plaats in november 2010. Tijdens deze audit werden geen afwijkingen geconstateerd die aanleiding waren om de certificering te beëindigen.

Hetzelfde geldt voor de audits die DigiNotar liet uitvoeren in het kader van de WebTrust-certificering, een kwaliteitswaarborg voor leveranciers van SSL-certificaten waarover het bedrijf beschikte. Ook bij deze audits zijn geen afwijkingen aan het licht gekomen die aanleiding waren om de certificering te beëindigen.

OPTA fungeert als publieke toezichthouder op de levering van gekwalificeerde certificaten, en was in die hoedanigheid bij DigiNotar betrokken. OPTA vulde dit toezicht in door zich op de hoogte te stellen van de uitkomsten van de audits die DigiNotar zelf liet uitvoeren, en door zelf aanvullend onderzoek te doen als hiertoe op grond van deze auditrapporten aanleiding bestond. Dat is bij DigiNotar niet het geval geweest.

---

38 Certificaatherroepingslijsten worden uitgegeven door certificaatdienstverleners. Zij bevatten de gegevens van alle certificaten die, om wat voor reden ook, niet langer geldig zijn. De lijsten worden automatisch gecontroleerd door de software van degene die een certificaat gebruikt. Zo wordt voorkomen dat ongeldige certificaten door eindgebruikers worden gebruikt.

39 ETSI TS 101 456, artikelen 7.4.5 en 7.4.6.

40 ETSI TS 101 456, artikel 7.4.1.

Voor het leveren van PKIoverheid-certificaten moest DigiNotar voldoen aan de voorwaarden die het ministerie van Binnenlandse Zaken en Koninkrijksrelaties daaraan stelt. Het ministerie, in casu Logius, zag toe op naleving van de met haar gesloten overeenkomst. Logius baseerde dit toezicht in eerste instantie eveneens op de uitkomsten van audits die het bedrijf liet uitvoeren, en op informatie over incidenten. Van toezichtsactiviteiten op eigen initiatief was geen sprake.[41]

Naast de externe audits bestond binnen het bedrijf een systeem van interne audits, waarbij een externe deskundige betrokken was. Ook liet het bedrijf, overeenkomstig bepalingen in de eerder genoemde ETSI-norm, zijn computersystemen periodiek door een extern bedrijf controleren, dat onder andere zogeheten penetratietests uitvoerde.[42] Bij deze controles zijn voor zover bekend nooit bijzonderheden aangetroffen die hebben geleid tot het voor langere tijd stilleggen van de uitgifte van certificaten.

Tot slot is DigiNotar, voorafgaand aan de overname, onderworpen aan een onderzoek door Vasco. Uit dit onderzoek zijn geen bijzonderheden gebleken die een overname door Vasco in de weg zouden staan.

4.1.4 Analyse van constateringen

De eerder genoemde constateringen leiden tot het volgende beeld. Het bedrijf DigiNotar deed, onder meer naar het oordeel van de auditerende instelling, wat nodig was om zijn certificaat-dienstverlening zo veilig mogelijk te doen plaatsvinden. Geen van de partijen aan wie DigiNotar verantwoording verschuldigd was, of die anderszins toezicht hielden op de bedrijfsvoering of deze toetsten aan de vigerende regelgeving, signaleerde afwijkingen in de bedrijfsvoering die aanleiding waren tot zorg over de staat van de beveiliging van het bedrijf.

Toch kon zich een grootschalige inbraak voordoen met ingrijpende gevolgen voor de betrouwbaarheid van de door DigiNotar uitgegeven digitale certificaten. De computersystemen bestemd voor de gekwalificeerde certificaatdienstverlening waren kennelijk niet afdoende veilig. Ze waren niet op zodanige wijze ingericht dat alleen geautoriseerde personen er toegang toe hadden; de inbreker is er immers in geslaagd om zich toegang te verschaffen tot systemen voor certificaatdienstverlening en daarop certificaten te genereren. Bovendien zijn één of meerdere geheime sleutels die DigiNotar gebruikte om certificaten mee te ondertekenen toegankelijk geweest voor niet-geautoriseerde partijen, getuige het feit dat met deze sleutels ondertekende certificaten in omloop zijn gebracht.

Ten aanzien van de beveiliging van het bedrijfsnetwerk constateert de Onderzoeksraad dat DigiNotar de voor het bedrijf geldende regels niet volledig heeft nageleefd; hij wijst hier in het bijzonder op het gebruik van verouderde software en de instelling van de *firewall* zoals eerder beschreven, evenals het gebruik van niet-gerandomiseerde wachtwoorden. Als deze aspecten van de beveiliging anders waren ingevuld, had de inbreker wellicht niet of althans moeilijker kunnen doordringen tot de systemen voor certificaatdienstverlening. Gezien het bovenstaande ligt de vraag voor hoe het heeft kunnen gebeuren dat niemand deze tekortkomingen voorafgaand aan de inbraak heeft opgemerkt.[43]

De Onderzoeksraad heeft niet kunnen vaststellen welke omstandigheden ertoe hebben bijgedragen dat in de beveiliging van het bedrijfsnetwerk de hierboven genoemde zwakke plekken konden ontstaan. Mogelijk houdt de overname van DigiNotar door Vasco hiermee verband. Het onderzoek laat zien dat in 2011, het jaar van overname, het Nederlandse en het Amerikaanse management er verschillende veronderstellingen op nahielden wie verantwoordelijk was voor de dagelijkse gang van zaken bij DigiNotar, waaronder de beveiliging.

41 Sinds het DigiNotarincident heeft Logius zijn werkwijze veranderd. Het agentschap voert nu bijvoorbeeld op eigen initiatief bedrijfsbezoeken bij certificaatdienstverleners uit.

42 Een penetratietest (of pentest) is een poging om de beveiliging van een netwerk te doorbreken.

43 De Onderzoeksraad onthoudt zich van een oordeel over de vraag of DigiNotar de regels die zien op de inrichting van systemen voor certificaatdienstverlening al dan niet heeft nageleefd. Wel merkt hij op dat verschillende van de betrokken partijen, evenals experts die hij in zijn onderzoek heeft geraadpleegd, de wijze waarop de inbreker erin is geslaagd certificaten te genereren en te ondertekenen als zeer geavanceerd kwalificeren.

Ook zijn er aanwijzingen dat de gekozen overnameconstructie heeft geleid tot een verschuiving van de focus van het Nederlandse management van operationele naar commerciële resultaten. Hoewel van een directe causale relatie geen sprake is, acht de Onderzoeksraad het niettemin mogelijk dat dergelijke omstandigheden hebben bijgedragen tot een verminderde sturing op veiligheid.

Uit het onderzoek van de Onderzoeksraad blijkt dat de leiding van DigiNotar, in ieder geval in de periode voorafgaand aan de overname door Vasco, van mening was dat het bedrijf zijn verantwoordelijkheid voor een veilige certificaatdienstverlening goed invulde. Ook de eerder genoemde auditrapporten en technische onderzoeken hebben het management geen aanleiding gegeven om te vermoeden dat de bedrijfsvoering een veiligheidsrisico vertegenwoordigde. Bovendien had het Nederlandse management een lange staat van dienst op het gebied van certificaatdienstverlening en had het voor deze activiteiten ter zake kundig personeel in dienst.

Ten aanzien van het toezicht op een certificaatdienstverlener is een belangrijke rol weggelegd voor de auditerende instelling die het bedrijf onderzoekt. Voor certificaatdienstverleners die actief zijn onder PKIoverheid, zoals DigiNotar, worden twee onderzoeken verricht, waarvan één plaats vindt aan de hand van het certificeringsschema TTP.NL. Deze audit richt zich op het managementsysteem van de certificaatdienstverlener. Aan een verklaring die op grond van deze audit is afgegeven, kan een gerechtvaardigd vertrouwen (*justified confidence*) worden ontleend dat deze zijn diensten in overeenstemming met de vigerende regels verleent. OPTA en Logius, aan wie DigiNotar als certificaatdienstverlener onder PKIoverheid verantwoording verschuldigd was, baseren hun eigen toezicht voor een belangrijk deel op deze verklaring.

Volgens de interpretatie die de auditor in het geval van DigiNotar aan dit certificeringsschema gaf, stelde het managementsysteem het bedrijf voldoende in staat om te voldoen aan de wet- en regelgeving. Het schema schrijft niet gedetailleerd voor welke stappen de auditor moet doorlopen om te komen tot een dergelijk oordeel. Evenmin verplicht het de auditor om de overwegingen waarop hij een positief oordeel baseert, in het auditrapport kenbaar te maken.[44] Hierdoor kunnen externe partijen zoals OPTA en Logius niet vaststellen of en in hoeverre zij het oordeel van de auditor delen. In feite kunnen zij daardoor niet bepalen of hun vertrouwen in de TTP.NL-verklaring gerechtvaardigd is.

Niettemin gebruikten deze partijen de TTP.NL-verklaring wel als de belangrijkste leidraad voor hun toezicht. Zij controleerden niet zelf of en hoe het bedrijf invulling gaf aan de open normen in wet- en regelgeving. OPTA, als toezichthouder voor het leveren van gekwalificeerde certificaten, voerde geen overleg met de bij haar geregistreerde certificaatdienstverleners over de vraag welke interpretatie hiervan zij acceptabel achtte. In plaats daarvan vertrouwde zij erop, overeenkomstig de bedoeling van de wetgever, dat de betrouwbaarheid van de certificaatdienstverlening afdoende was gewaarborgd wanneer de certificaatdienstverlener beschikt over een geldige TTP.NL-verklaring. Hetzelfde gold voor Logius/het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, met wie DigiNotar een overeenkomst had voor het leveren van PKIoverheid-certificaten.[45]

4.1.5 Conclusie

Naleving van open normen veronderstelt dat de betrokken partijen zelf aan deze normen nader invulling geven, bijvoorbeeld door veiligheidsmanagement toe te passen. Voor het management van een organisatie betekent dit een voortdurende, actieve betrokkenheid bij het uitvoeren en aansturen van de veiligheidsaanpak en het systematisch monitoren van de effectiviteit ervan. Hierin hebben zowel de partij waarop de normen van toepassing zijn, als de partijen die een belang hebben bij naleving van deze normen, een rol.

44 Wel bepaalt het certificeringsschema dat de werkwijze van de auditor / auditerende instelling aan een aantal ISO-normen moet voldoen. Hierover verklaart NOREA, de beroepsorganisatie van IT-auditors: "Aan de formele vereisten is derhalve door [auditerende instelling] voldaan. Of de beoordeling en certificering ook in materieel opzicht adequaat is geweest vergt nader inhoudelijk onderzoek" (NOREA, *Voorlopige bevindingen en aanbevelingen n.a.v. DigiNotar-inbraak*. 2 december 2011). De Onderzoeksraad heeft dit niet nader onderzocht.

45 Logius heeft bij inzage aangegeven dat nieuwe bepalingen in het Programma van Eisen PKIoverheid ter becommentariëring aan de aangesloten certificaatdienstverleners worden voorgelegd.

DigiNotar was van mening dat het bedrijf aan deze normen zo goed mogelijk invulling had gegeven. Waardoor de zwakke plekken hebben kunnen ontstaan in de beveiliging van het bedrijfsnetwerk en de omgang met de systemen voor certificaatdienstverlening, heeft de Onderzoeksraad niet met zekerheid kunnen vaststellen. Hij acht het mogelijk dat de overname van het bedrijf door Vasco hierin een rol heeft gespeeld, aangezien deze lijkt te hebben geleid tot een overgangssituatie waarin minder aandacht bestond voor het geven van sturing aan de veiligheidsaanpak.

De auditor die DigiNotar geregeld onderzocht, zag geen reden om het bedrijf certificering volgens het certificeringsschema TTP.NL te onthouden. Een TTP.NL-verklaring impliceert echter slechts een gerechtvaardigd vertrouwen dat de certificaatdienstverlener de vigerende wet- en regelgeving naleeft, gebaseerd op onderzoek of zijn managementsysteem voldoet aan de ETSI-norm TS 101 456. De auditor toetst dan ook niet uitputtend of de certificaatdienstverlener alle regels feitelijk naleeft die van toepassing zijn op certificaatdienstverlening. Daarbij is de wijze waarop de auditor tot zijn oordeel moet komen in het certificeringsschema nauwelijks nader gespecificeerd, en verplicht het schema hem evenmin om de overwegingen te expliciteren waarop hij de beslissing baseert om een verklaring af te geven.

Hierdoor is het voor partijen zoals Logius en OPTA moeilijk om te beoordelen wat precies de waarde van de TTP.NL-verklaring is, en of deze naar hun maatstaven voldoende waarborgt dat de certificaatdienstverlener de voor hem geldende regels naleeft. Het certificeringsschema TTP.NL op grond waarvan de verklaring wordt afgegeven, schiet naar het oordeel van de Onderzoeksraad dan ook tekort voor het doel waarvoor Logius en OPTA het gebruiken.

Het schema biedt namelijk niet de mate van zekerheid dat een certificaatdienstverlener de regels naleeft die deze partijen, gezien hun rol in het stelsel, nodig hebben. De Onderzoeksraad is van oordeel dat vooral Logius, gezien het belang dat de rijksoverheid hecht aan PKIoverheid, als opdrachtgever een hoge mate van zekerheid dient te hebben dat de aangesloten certificaatdienstverleners zich houden aan de geldende eisen. Niettemin baseerden Logius en OPTA hun eigen toezicht op DigiNotar grotendeels op de TTP.NL-verklaring, in plaats van zelf systematisch te verifiëren of ook zij van mening waren dat het bedrijf op een goede wijze invulling gaf aan de wet- en regelgeving. Hiermee wordt in feite afgegaan op één aspect van de betrouwbaarheid van de dienstverlener, namelijk diens managementsysteem. Dit maakt het stelsel kwetsbaar voor inschattingsfouten.

De Onderzoeksraad merkt op dat, ten aanzien van gekwalificeerde certificaten, de Telecommunicatiewet uitdrukkelijk de mogelijkheid biedt dat het voldoen aan wettelijke bepalingen wordt aangenomen op basis van een TTP.NL-verklaring. Daarmee heeft de wetgever het toezicht op invulling en naleving van open normen in feite gedelegeerd aan de certificaatdienstverlener zelf. De overheid vertrouwt dus op certificaatdienstverleners, maar onthoudt zichzelf de instrumenten om te verifiëren of de betrouwbaarheid van hun bedrijfsvoering dat vertrouwen rechtvaardigt. Dit is een bewuste keuze van de wetgever geweest. Gezien de veiligheidskritische functie van digitale certificaten vindt de Onderzoeksraad deze constructie niet verantwoord.

4.2 Ontdekking van de inbraak en melding

Uit het technisch onderzoek blijkt dat de inbraak in verschillende fases is uitgevoerd, over een aaneengesloten periode van enkele weken. De eerste verkennende activiteiten op het netwerk vonden begin juni 2011 plaats, terwijl pas rond 1 juli 2011 de inbraak plaatsvond in het afgeschermde gedeelte van het netwerk. De eerste aangetroffen sporen van vervalste certificaten die succesvol gegenereerd zijn dateren van 10 juli 2011. De laatst bekende datum voor het genereren van ondertekende vervalste certificaten is 20 juli 2011. Hieruit kan afgeleid worden dat de inbreker uitgebreid de tijd heeft genomen en gekregen om vertrouwd te raken met het bedrijfsnetwerk van DigiNotar.

4.2.1 Ontdekking vervalste certificaten

DigiNotar hield onder meer toezicht op het certificaatuitgifteproces door gegevens van uitgegeven certificaten dagelijks te vergelijken met de administratie van certificaataanvragen. Het programma dat deze vergelijking uitvoerde had door onbekende oorzaak enige tijd niet gewerkt; omdat niet voorzien was in vervangende maatregelen had DigiNotar gedurende die periode geen zicht op de eventuele aanmaak van vervalste certificaten. Na herstel van het programma op 19 juli 2011 detecteerde het dat 128 SSL-certificaten waren gegenereerd die niet herleid konden worden tot aanvraaggegevens. DigiNotar heeft de toen geïdentificeerde vervalste certificaten onmiddellijk ingetrokken.

Op 20 juli 2011 werden op dezelfde manier nog eens 129 vervalste SSL-certificaten ontdekt. Ook deze trok het bedrijf in. Tevens riep DigiNotar de hulp van een ICT-beveiligingsbedrijf in, om eventuele ongewenste toegangen tot het netwerk te identificeren en af te sluiten.

De Onderzoeksraad is van oordeel dat DigiNotar voor wat betreft het intrekken van de vervalste certificaten op 19 en 20 juli en het inroepen van externe hulp gereageerd heeft zoals van het bedrijf verwacht had mogen worden.

4.2.2 Melding inbraak door DigiNotar

Toen op 19 juli 2011 aan het licht kwam dat vervalste certificaten in omloop waren gebracht, heeft DigiNotar zich direct de vraag gesteld of en aan wie hiervan melding moest worden gemaakt. Op DigiNotar rustte namelijk een drievoudige meldplicht in geval van incidenten en andere bijzonderheden.

DigiNotar was als leverancier van gekwalificeerde certificaten geregistreerd bij OPTA. Uit deze registratie vloeide de verplichting voort om alle wijzigingen te melden die op de registratie van invloed zijn.[46] Bovendien was DigiNotar als leverancier van PKIoverheid-certificaten verplicht om, krachtens de overeenkomst die het gesloten had, Logius onverwijld op de hoogte te stellen van een eventuele compromittering van zijn private sleutel(s) en van andere relevante incidenten. Relevante incidenten waren in ieder geval gebeurtenissen die afbreuk doen aan de betrouwbaarheid van de dienstverlening.[47] Ten derde was DigiNotar, als voorwaarde om zijn TTP.NL-verklaring te kunnen behouden, verplicht om melding te maken aan de auditerende instelling van ingrijpende wijzigingen die van invloed kunnen zijn op de certificering van het bedrijf.[48]

De formulering van de meldplicht in respectievelijk de Telecommunicatiewet en de beide overeenkomsten laat ruimte voor een eigen afweging door de partij op wie de meldplicht rust. In een overleg met de directie van Vasco op 21 juli 2011 heeft DigiNotar verslag gedaan van de inbraak. DigiNotar concludeerde, na juridisch advies te hebben ingewonnen, dat de meldplicht jegens geen van de drie hierboven genoemde organisaties betrekking had op de gebeurtenissen tot dan toe. De uitgifte van gekwalificeerde noch PKIoverheid-certificaten leek op dat moment gecompromitteerd te zijn, waardoor van een formele meldingsplicht jegens OPTA of Logius geen sprake was. Bovendien waren de aangetroffen vervalste certificaten onmiddellijk ingetrokken, en was de oorzaak van het probleem naar inschatting van DigiNotar weggenomen. Op dat moment leek de ernst van de inbraak mee te vallen.

De directie van Vasco nam dit voorstel om niet te melden over. Wel hadden zij hierbij aarzelingen, mede door de in maart van 2011 bekend geworden ernstige RSA-breach die ook voor Vasco aanleiding was geweest voor het nemen van maatregelen op het gebied van digitale beveiliging.[49] Vasco bleef op afstand de verdere ontwikkelingen bij DigiNotar volgen, maar liet de feitelijke afwikkeling van het incident over aan DigiNotar. Reden voor een niet meer directe rol van de Vasco-directie kwam voort uit een gebrek aan inhoudelijke kennis van de werking en risico's van het onbetrouwbaar zijn van digitale certificaten en vertrouwen in de reeds in gang gezette acties door DigiNotar.

46 Art. 2.3, vijfde lid Telecommunicatiewet.
47 Art. 4, derde lid Overeenkomst tussen de Staat der Nederlanden en DigiNotar B.V.
48 Art. 4, derde lid Algemene Voorwaarden Certificatieovereenkomst, tussen DigiNotar en auditerende instelling.
49 In maart 2011 werd bekend dat het bedrijf onderwerp was geweest van een *advanced persistent attack* waarbij digitaal informatie was gestolen over de gehanteerde SecurID-authenticatietechnologie.

Voor wat betreft het besluit van DigiNotar om de incidenten van 19 en 20 juli niet te melden, merkt de Onderzoeksraad het volgende op. Het bedrijf ging er op het moment dat het incident zich voordeed vanuit dat de PKIoverheid-certificaten niet getroffen waren. Hierdoor achtte het bedrijf het incident – formeel juridisch geredeneerd – niet meldingsplichtig. Bovendien verkeerde het bedrijf in de veronderstelling dat de problemen op dat moment opgelost waren. Ook dit speelde mee in de gemaakte afweging om niet te melden.

De Onderzoeksraad treedt niet in de vraag of in de onderhavige situatie melden vanuit juridisch oogpunt verplicht was. Vanuit het grote belang van veilige certificaatdienstverlening bezien, acht de Onderzoeksraad het echter noodzakelijk dat certificaatdienstverleners een eventuele meldplicht ruimhartig interpreteren en andere partijen ook op de hoogte stellen wanneer daartoe geen formele plicht bestaat, maar een melding voor hen mogelijk wel van belang is. Een dergelijke onderlinge omgang vergroot de kans dat veiligheidsrisico's in het stelsel vroegtijdig worden ontdekt, stelt partijen in de gelegenheid om in gezamenlijkheid passende maatregelen te nemen en maakt het voor de sector als geheel mogelijk van incidenten te leren. Het lering trekken uit de gebeurtenissen bij DigiNotar door de sector, had voor het bedrijf aanleiding moeten zijn het incident te melden. De inmiddels bestaande kennis over de ernst en impact van de inbraak en de situatie waartoe deze heeft geleid, maken des te meer duidelijk dat het goed was geweest als DigiNotar destijds anders besloten had.

4.3 Escalatie en crisisbeheersing

Tussen 20 juli en 29 augustus 2011 was er ogenschijnlijk niets aan de hand. DigiNotar en Vasco verkeerden in de veronderstelling dat alle vervalste certificaten waren ingetrokken en onvolkomenheden in de netwerkbeveiliging waren opgelost.

Op maandag 29 augustus 2011 meldde CERT-Bund, het *computer emergency response team* van de Duitse federale overheid, aan haar Nederlandse evenknie GovCert dat een Iraanse gebruiker van e-mailprovider Gmail een vervalst certificaat had aangetroffen dat afkomstig was van DigiNotar. Nog diezelfde dag nam GovCert hierover contact op met DigiNotar en het Nationaal Crisiscentrum (NCC). In overeenstemming met zijn rol als computer emergency response team heeft GovCert vervolgens de coördinatie op zich genomen over de afhandeling van het incident.

Nog dezelfde avond stelde GovCert ook Logius van de gebeurtenis op de hoogte, omdat DigiNotar tevens PKIoverheid-certificaten leverde. Behalve DigiNotar en Logius informeerde GovCert ook de softwarefabrikanten over het feit dat vervalste certificaten afkomstig van DigiNotar in omloop waren.[50] De softwarefabrikanten bleken al op de hoogte te zijn.

Na intern overleg sommeerde Logius het management van DigiNotar op dinsdag 30 augustus 2011 om een nieuwe audit te laten uitvoeren, waaruit moest blijken dat een soortgelijk incident niet meer kon voorkomen.[51] Bovendien eiste Logius een garantie van DigiNotar dat alle PKIoverheid-certificaten conform de vigerende regels waren uitgegeven, en dat "hetgeen onder de DigiNotar Root CA heeft plaatsgevonden niet kan plaatsvinden onder de DigiNotar PKIoverheid CA's". DigiNotar liet hierop nog diezelfde dag weten dat het geen aanleiding had om aan te nemen "dat deze bewuste hack nog kan plaats vinden voor de PKIoverheid CA's". Bovendien gaf DigiNotar aan dat het een gespecialiseerd bedrijf onderzoek liet doen, en dat tot dan toe geen bewijs gevonden was "dat de PKIoverheid omgeving gecompromitteerd is". Ten slotte verklaarde DigiNotar dat alle PKIoverheid certificaten conform de regels van PKIoverheid zijn uitgegeven, en dat deze certificaten "op geen enkele wijze gecompromitteerd" zijn.[52]

50 Het betreft hier fabrikanten van software waarin certificaten gebruikt worden, in het bijzonder internetbrowsers.

51 Door de wijze waarop het incident zich na 30 augustus 2011 ontwikkelde tot een crisis die onder meer uitmondde in het faillissement van DigiNotar, heeft DigiNotar niet aan de auditerende instelling om een nieuwe audit kunnen vragen. De auditor heeft aan de Onderzoeksraad verklaard dat het incident niet zonder meer aanleiding zou zijn geweest om de certificering van DigiNotar te beëindigen. Maatgevend zou zijn geweest hoe DigiNotar op het incident reageerde.

52 Briefwisseling tussen Logius en DigiNotar, d.d. 30 augustus 2011. Met "CA" (*certificate authority*) worden de systemen bedoeld die worden gebruikt voor het aanmaken en uitgeven van certificaten.

4.3.1 Een mogelijke crisis tekent zich af

Het onderzoek bij DigiNotar startte vrijwel direct, maar nam enige tijd in beslag. Op vrijdagmiddag 2 september 2011 zou uiteindelijk een eerste versie van de bevindingen worden opgeleverd. GovCert hield zich tussentijds van de vorderingen van het onderzoek op de hoogte.

De rijksoverheid, in casu Logius, stelde zich aanvankelijk op het standpunt dat de inbraak eerst en vooral het probleem was van een privaat bedrijf, waarover zij afgezien van de PKIoverheid-certificaten geen enkele zeggenschap had. Haar enige belang op dat moment was dat de betrouwbaarheid van PKIoverheid-certificaten niet onder druk zou komen te staan. Het scenario dat Logius hiervoor onderhield, was overzichtelijk: als Logius door het incident zijn vertrouwen in de betrouwbaarheid van DigiNotar zou verliezen, zou het agentschap het bedrijf verwijderen uit PKIoverheid. Als gevolg hiervan zouden alle PKIoverheid-certificaten die DigiNotar had uitstaan, ongeldig worden. De houders van deze certificaten zouden dan vervangende PKIoverheid-certificaten moeten inzetten, af te nemen van één van de resterende certificaatdienstverleners die onder PKIoverheid opereren.

Of PKIoverheid-certificaten door eindgebruikers worden vertrouwd, hangt in laatste instantie af van het vertrouwen dat softwarefabrikanten stellen in de Nederlandse rijksoverheid, waaraan PKIoverheid-certificaten hun betrouwbaarheid ontlenen. Om te voorkomen dat deze vertrouwensrelatie onder druk zou komen te staan, stelde Logius de softwarefabrikanten op de hoogte van het incident bij DigiNotar, omdat het bedrijf hen zelf had geïnformeerd. Als eerder gesteld waren de softwarefabrikanten echter reeds op de hoogte en druk bezig te onderzoeken wat de gevolgen van de problemen bij DigiNotar zouden kunnen zijn voor Nederland, voor de rest van de wereld en voor de positie van de softwarefabrikanten zelf.

Vertrouwen cruciaal

De techniek voor het beveiligen van elektronisch gegevensverkeer is afhankelijk van cryptografische technieken en van vertrouwensrelaties tussen verschillende partijen.

Wie zijn gegevensverkeer met een ander wil beveiligen, vertrouwt erop dat de sleutel die de ander hem hiervoor aanbiedt werkelijk aan hem toebehoort. Het digitale certificaat geeft een waarborg voor het vertrouwen dat een communicerende partij in de sleutel van een ander stelt.

Echter, de waarde van het certificaat is op zijn beurt afhankelijk van de mate waarin de beoogde gebruiker ervan vertrouwen heeft in de certificaatdienstverlener die het heeft uitgegeven.

Deze gebruiker laat een oordeel of vertrouwen bestaat in deze certificaatdienstverlener doorgaans over aan de computersoftware die hij gebruikt, zoals een internetbrowser. Die geeft een melding of een certificaat al dan niet is uitgegeven door een certificaatdienstverlener waarin de softwarefabrikant vertrouwen heeft. Het ‘slotje’ in de browser Internet Explorer is een voorbeeld van zo’n melding. Overigens kan een gebruiker ook besluiten om het oordeel over de (on)betrouwbaarheid van een digitaal certificaat dat zijn software geeft, te negeren.

Ingeval van PKIoverheid is geen sprake van direct vertrouwen tussen een softwarefabrikant en een certificaatdienstverlener. In plaats daarvan vertrouwt de softwarefabrikant het stamcertificaat Staat der Nederlanden, waaraan het vertrouwen in PKIoverheid-certificaten uiteindelijk wordt ontleend. De Staat der Nederlanden vertrouwt op zijn beurt de certificaatdienstverleners die PKIoverheid-certificaten uitgeven, zoals DigiNotar.[53]

53 Deze configuratie is niet uniek voor PKIoverheid. Ook voor andere certificaten is vaak sprake van een hiërarchische vertrouwensketen, waardoor softwarefabrikanten slechts een klein aantal partijen hoeven te vertrouwen.

Sommige fabrikanten overwogen hun vertrouwen in DigiNotar op te zeggen, omdat het bedrijf niet onmiddellijk een overzicht van vervalste certificaten kon overleggen.[54] Als zij dat zouden doen, zouden op eigen titel door DigiNotar uitgegeven certificaten door hun software als onbetrouwbaar gemarkeerd worden. Logius nam dit voor kennisgeving aan; hij beschouwde dit als een privaat probleem tussen private partijen, waarin de overheid geen enkel mandaat tot ingrijpen had.

Wat wel een zorg van Logius was, was dat sommige softwarefabrikanten dreigden om vanwege de inbraak bij DigiNotar hun vertrouwen in de Staat der Nederlanden als uiteindelijke 'bron' van PKIoverheid-certificaten op te zeggen. Als dit zou gebeuren, zou geen enkel PKIoverheid-certificaat nog door hun software als betrouwbaar worden aangemerkt, ook niet exemplaren die waren uitgegeven door andere certificaatdienstverleners. Een gevolg hiervan zou onder meer zijn, vreesde Logius, dat het authenticatiesysteem DigiD zou ophouden te functioneren.

Het dreigend onbruikbaar worden van het gehele PKIoverheid-stelsel legde een extra druk op het onderzoek bij DigiNotar. Immers, met de uitkomsten van dit onderzoek zou Logius de softwarefabrikanten kunnen overtuigen van het feit dat hun vertrouwen in de Staat der Nederlanden gehandhaafd kon blijven, omdat het uitgeven van PKIoverheid-certificaten door de inbraak bij DigiNotar niet was gecompromitteerd. Als de uitkomst van het onderzoek negatief was, kon naar de inschatting van Logius alleen een onmiddellijke verwijdering van DigiNotar uit PKIoverheid er nog toe leiden dat de softwarefabrikanten hun vertrouwen in het stelsel zouden behouden.

Anticiperend op vragen van certificaathouders over de betrouwbaarheid van door DigiNotar uitgegeven PKIoverheid-certificaten stelde Logius op 1 september 2011 gebruikers van Logius-producten op de hoogte van de problemen. Logius adviseerde hun om te inventariseren of zij gebruik maakten van door DigiNotar uitgegeven certificaten, en zich voor te bereiden op een mogelijke noodzaak tot vervanging daarvan.

4.3.2 Het onderzoek bij DigiNotar

Het onderzoek naar de inbraak dat DigiNotar liet uitvoeren, kwam in concept op vrijdagmiddag 2 september 2011 beschikbaar. Het wees uit dat de inbreker diverse registraties in het bedrijfsnetwerk van DigiNotar had gemanipuleerd, waardoor de methode die het bedrijf gebruikte om vervalste certificaten te detecteren en in te trekken geen volledige zekerheid meer bood. Daardoor was het niet alleen moeilijker om vast te stellen of en hoeveel vervalste certificaten waren aangemaakt, maar konden eenmaal geïdentificeerde vervalste certificaten niet alle worden ingetrokken.

Bovendien bleek in het onderzoek dat de registratie van computersysteemgebeurtenissen op het bedrijfsnetwerk van DigiNotar zodanig was afgesteld dat de inbreker zijn sporen deels kon wissen en manipuleren. Deze omstandigheid heeft de zekerheid waarmee uit het onderzoek conclusies konden worden getrokken, ernstig belemmerd.

Door verschillende registratiebestanden op het netwerk met elkaar te vergelijken, kwam naar voren dat in elk geval 531 certificaten op het bedrijfsnetwerk voorkwamen die niet gecombineerd konden worden met aanvraaggegevens. Daarvan konden er 333 worden ingetrokken. Van de overige 198 kon echter geen serienummer worden achterhaald, waardoor die niet konden worden ingetrokken. DigiNotar heeft andere maatregelen getroffen om deze 198 certificaten toch onbruikbaar te maken.[55]

54 Dit kwam omdat de inbreker kans had gezien om registratiebestanden in het bedrijfsnetwerk te manipuleren en gegevens te wissen (zie ook 4.3.2).

55 DigiNotar maakte na de inbraak onder meer gebruik van het zogenaamde *OCSP whitelisting*. Veel software toetst de geldigheid van een aangeboden certificaat aan een server van de certificaatdienstverlener die normaliter informatie geeft of een certificaat al dan niet ongeldig is (*blacklisting*). Door gebruik te maken van *OCSP whitelisting* wordt dit procedé omgedraaid, en krijgt de software informatie over de geldigheid van een te toetsen certificaat. DigiNotar had alle certificaten die het bedrijf zelf nog vertrouwde op deze *whitelist* geplaatst. Alle andere certificaten, waaronder de 198 exemplaren waarvan geen serienummer bekend was, zouden daardoor bij toetsing door de software van de eindgebruiker vanzelf als ongeldig worden beoordeeld.

Onbekend is hoeveel vervalste certificaten de inbreker daadwerkelijk in omloop heeft gebracht. Negen certificaten zijn herkend als vervalst bij toetsing van hun geldigheid door eindgebruikers, en vervolgens ingetrokken. Van één vervalst certificaat staat vast dat het daadwerkelijk door eindgebruikers is gebruikt, hetgeen de weg effent voor oneigenlijke toegang tot de gegevens die ermee worden beveiligd. Dit betreft het eerder genoemde certificaat dat is aangetroffen in Iran.

Op de server die DigiNotar gebruikte voor het genereren van gekwalificeerde en PKIoverheid–certificaten werden tijdens het onderzoek twee serienummers van certificaten aangetroffen die niet gecombineerd konden worden met aanvraaggegevens. Het onderzoek dat DigiNotar liet doen, heeft niet kunnen uitwijzen wat de precieze herkomst van deze serienummers is. Het is mogelijk dat deze geen enkel verband houden met de inbraak. Het is echter evenzeer mogelijk dat het bestaan van deze serienummers erop wijst dat de inbreker ook handelingen op deze server heeft uitgevoerd.

Daarbij komt dat het onderzoek niet met zekerheid heeft kunnen uitwijzen dat de geheime sleutel die nodig is om PKIoverheid-certificaten te ondertekenen, tijdens de inbraak ontoegankelijk was. Als dat het geval was geweest, had de inbreker sowieso geen bruikbare vervalsingen in omloop kunnen brengen; deze waren dan zonder meer, vanwege het ontbreken van een ondertekening, door alle software als ongeldig aangemerkt. Overigens is evenmin vastgesteld dat de bedoelde geheime sleutel wél door de inbreker is gebruikt.

Beide feiten gecombineerd leidden het bedrijf dat het onderzoek uitvoerde ertoe, te concluderen dat niet met zekerheid kon worden vastgesteld dat de systemen voor het verstrekken van PKIoverheid-certificaten *niet* waren gecompromitteerd. Anderzijds is evenmin met zekerheid vastgesteld dat de PKIoverheid-omgeving wel getroffen is door de inbraak.

Echter, of al dan niet sprake was van een werkelijk risico, en of de certificaatdienstverlening door DigiNotar werkelijk onbetrouwbaar was geworden, deed op dat moment niet langer ter zake. Logius had het vertrouwen in DigiNotar als certificaatdienstverlener verloren, omdat hij de eerder aangehaalde brief van 30 augustus 2011 van het bedrijf beschouwde als een garantie dat levering van PKIoverheid-certificaten niet gecompromitteerd was, terwijl de onderzoekers dit in hun rapportage van 2 september niet bleken te kunnen bevestigen. Op 2 september 2011 besloot Logius daarom om DigiNotar te verwijderen uit PKIoverheid. DigiNotar aan de andere kant verkeerde tot dat moment in de veronderstelling dat het bedrijf constructief meewerkte aan herstel van een betrouwbare certificaatdienstverlening. De Onderzoeksraad constateert dan ook, dat Logius en DigiNotar kennelijk een heel verschillend beeld hadden van hun eigen optreden en dat van de ander in het oplossen van de ontstane situatie.

Hoe dan ook, een snelle verwijdering van het bedrijf uit PKIoverheid was, naar inschatting van Logius en andere betrokkenen binnen de rijksoverheid, de enige mogelijkheid om het vertrouwen van de softwarefabrikanten in PKIoverheid als geheel te behouden. Het Programma van Eisen PKIoverheid bood hiervoor ook voldoende aanleiding, gezien het oordeel van de onderzoekers dat niet kon worden uitgesloten dat de levering van PKIoverheid-certificaten door DigiNotar niet gecompromitteerd was geraakt.

4.3.3 Een onvoorziene complicatie

Op donderdag 1 september 2011 had de plaatsvervangend directeur van Logius contact gehad met enkele leden van de programmaraad Logius, waaronder de Belastingdienst. De programmaraad Logius is het orgaan waarin alle rijksuitvoeringsdiensten zitting hebben die van Logius-producten gebruik maken. Deze waren op de hoogte gesteld van de inbraak bij DigiNotar, teneinde gezamenlijk in kaart te brengen welke problemen zouden kunnen ontstaan bij een noodzakelijke vervanging van door DigiNotar uitgegeven PKIoverheid-certificaten. Op vrijdag 2 september 2011 kwam de programmaraad Logius in een ingelaste bijeenkomst bijeen.

Aanleiding hiervoor was onder meer dat een inventarisatie bij de Belastingdienst een onvoorzien probleem aan het licht had gebracht. De Belastingdienst maakte geen gebruik van PKIoverheid-certificaten, maar wel van de zogenaamde BAPI-certificaten die DigiNotar voor de dienst leverde. Wanneer de softwarefabrikanten het vertrouwen in DigiNotar zouden opzeggen, zouden naar inschatting van de Belastingdienst al deze certificaten mogelijk in één keer onbruikbaar worden.

De Belastingdienst zou dan geen aangiften meer kunnen verwerken. De dagelijkse inkomstenstroom van de overheid via de rijksbelastingheffing zou dan in gevaar komen. Vergelijkbare problemen bleken zich ook te kunnen voordoen in de werk- en inkomensketen, waarin door DigiNotar uitgegeven certificaten eveneens een belangrijke rol speelden.

Deze problemen bleken niet snel op te lossen. De BAPI- en andere certificaten waar het om ging, waren geïntegreerd in de toepassingen die zij beveiligden waardoor een vlotte vervanging van de certificaten niet aan de orde was. De grote gegevensverwerkende instanties moesten eerst uitzoeken of, waarvoor en op welke schaal zij gebruik maakten van door DigiNotar uitgegeven certificaten. Tot zij daarmee klaar waren, was het van groot belang dat de softwarefabrikanten het vertrouwen in DigiNotar niet zouden opzeggen.[56]

De eenvoudige operatie die Logius voor ogen stond door DigiNotar te verwijderen uit PKIoverheid, bleek dus een ingreep die nog veel grotere complicaties zou opleveren dan de situatie waarvoor het een oplossing beoogde te zijn. Op het laatste moment zag Logius er daarom vanaf om DigiNotar uit PKIoverheid te verwijderen.

De Onderzoeksraad constateert dat de rijksoverheid zich liet verrassen door het feit dat de door DigiNotar uitgegeven certificaten niet op stel en sprong vervangen konden worden, en niet had geanticipeerd op de implicaties van deze onmogelijkheid.

In het licht van de nieuwe situatie besloot het crisisteam dat inmiddels was geformeerd om de continuïteit van het elektronisch gegevensverkeer te laten prevaleren boven de veiligheid ervan. Zelfs al hadden de op rijksniveau betrokken partijen inmiddels het vertrouwen in DigiNotar als betrouwbare certificaatdienstverlener verloren, toch spanden zij zich in om te zorgen dat door DigiNotar uitgegeven certificaten niet geweigerd zouden worden door softwaretoepassingen. Het crisisteam beoordeelde de risico's van deze handelwijze als acceptabel.

Uiteindelijk resulteerde deze strategie van het crisisteam erin dat de minister van Binnenlandse Zaken en Koninkrijksrelaties het bewind over DigiNotar aan zich trok, en de softwarefabrikanten het besluit om hun vertrouwen in DigiNotar op te zeggen nog enige tijd uitstelden.[57] Dit gaf de houders van door DigiNotar uitgegeven certificaten de gelegenheid om deze certificaten te vervangen door certificaten van een andere certificaatdienstverlener. Een meer gedetailleerde evaluatie van het optreden van de rijksoverheidspartijen rondom en na de overname van DigiNotar valt buiten het bestek van dit onderzoek. Dit is onderzocht door de Inspectie Veiligheid en Justitie.

4.4 Conclusie

Het verloop van de gebeurtenissen rond DigiNotar laat een plotselinge vertrouwensomslag zien. Het vertrouwen dat partijen als Logius en OPTA in DigiNotar stelden voor het incident was onvoldoende geborgd door feitelijke toetsing. OPTA en Logius kenden een grotere waarde toe aan de auditverklaring dan gerechtvaardigd was. Noch Logius, noch OPTA voerde hiernaast zelf toezichthoudende taken bij het bedrijf zelf uit. Hierdoor konden zij moeilijk inschatten of hun vertrouwen in DigiNotar feitelijk gerechtvaardigd was.

DigiNotar besloot om de incidenten van 19 en 20 juli niet te melden. Toen op 29 augustus 2011 aan het licht kwam dat de eerdere inbraak bij DigiNotar veel verstrekkender gevolgen had gehad dan tot dan toe was aangenomen, kwam het vertrouwen in het bedrijf snel onder druk te staan. Het niet melden van de incidenten op 19 en 20 juli 2011 werd door Logius in de context van de nieuwe feiten geïnterpreteerd als een blijk van onbetrouwbaarheid.

56 De Onderzoeksraad merkt op dat de betrokken overheidspartijen de veronderstellingen en scenario's die zij ten aanzien van de BAPI-certificaten ontwikkelden, niet deelden met DigiNotar zelf. Daardoor bleef relevante kennis op het gebied van BAPI-certificaten onbenut.

57 In het geval van softwarefabrikant Microsoft werd bijvoorbeeld een verplichte update die voor 6 september 2011 gepland stond omgezet in een optionele update, waarvan de gebruiker zelf kon kiezen of deze geïnstalleerd werd.

De sterk verschillende wijze waarop DigiNotar en Logius hun onderlinge briefwisseling van 30 augustus 2011 hebben geïnterpreteerd, versterkt dit beeld. Dat DigiNotar diverse maatregelen nam om de gevolgen van de inbraak te beperken om zo weer een betrouwbare certificaatdienstverlening te kunnen laten plaatsvinden, mocht toen al niet meer baten.

De Onderzoeksraad is van oordeel dat Logius en OPTA zich voorafgaand aan het incident meer betrokken hadden moeten tonen bij het bedrijf, en zich werkelijk hadden moeten overtuigen van de betrouwbaarheid van diens dienstverlening en de risico's die er waren. Als zij zelf goed zicht hadden gehad op de feitelijke situatie bij DigiNotar hadden zij de gebeurtenissen beter kunnen beoordelen en zouden ze minder overvallen zijn geweest. Voor wat betreft OPTA merkt de Onderzoeksraad overigens op dat zij haar toezichthoudende rol heeft uitgevoerd zoals die door de wetgever is bepaald.[58] Niettemin is de Onderzoeksraad van mening dat OPTA zich te gemakkelijk in deze marginale rol schikt. Van een publieke toezichthouder mag worden verwacht dat deze aan de bel trekt wanneer de wet- en regelgeving een effectieve taakuitoefening onmogelijk maakt, en ook dat deze de grenzen van zijn bevoegdheden opzoekt.

Toen de inbraak op 19 en 20 juli 2011 werd ontdekt, reageerde DigiNotar voor wat betreft het intrekken van de vervalste certificaten en het inroepen van externe hulp zoals van het bedrijf verwacht mocht worden. Toen het interne controlesysteem vervalste certificaten aantrof, nam het bedrijf immers zowel repressieve als remediërende maatregelen, door de vervalste certificaten direct in te trekken en de illegale toegangsmogelijkheden tot het netwerk af te sluiten. Bovendien liet het een extern onderzoek doen. Deze handelingen waren in lijn met het beoordelingskader voor veiligheidsmanagement dat de Onderzoeksraad hanteert.

De Onderzoeksraad treedt niet in de vraag of in de onderhavige situatie melden vanuit juridisch oogpunt verplicht was. Vanuit het grote belang van veilige certificaatdienstverlening bezien, acht de Onderzoeksraad het echter noodzakelijk dat bedrijven in een dergelijke situatie incidenten aan relevante partijen melden. Dit geldt ook in de situatie dat het bedrijf in de veronderstelling vekeerde dat de problemen waren opgelost. Alleen als dergelijke incidenten gemeld worden, kan immers door de sector van incidenten geleerd worden. Het lering trekken uit de gebeurtenissen bij DigiNotar door de sector had voor DigiNotar reden moeten zijn het incident te melden. De inmiddels bestaande kennis over de ernst en gevolgen van de inbraak en de situatie waartoe deze heeft geleid, maken des te duidelijker dat het goed was geweest als DigiNotar destijds besloten had om wel te melden.

Ten slotte concludeert de Onderzoeksraad dat geen van de betrokken partijen had voorzien dat certificaten van een gecompromitteerde certificaatdienstverlener in de praktijk niet zonder gevolgen ongeldig verklaard kunnen worden. In deze context is het des te belangrijker dat partijen zich werkelijk overtuigen van diens betrouwbaarheid enerzijds en anderzijds zijn voorbereid op de situatie dat zich toch een calamiteit voordoet. Het hebben van back-up certificaten van een andere leverancier, die terstond kunnen worden ingezet ter vervanging van gecompromitteerde certificaten is van groot belang gebleken. Hier was men zich onvoldoende van bewust.

58 Deze taak blijkt onder meer uit een nota van toenmalig minister Korthals van Economische Zaken, die onderdeel uitmaakt van de ontstaansgeschiedenis van de Wet elektronische handtekeningen. Zie kamerstuk TK 27743-6.

5 VEILIGHEID VAN DIGITALE CERTIFICATEN

In het voorgaande hoofdstuk werd beschreven hoe de inbraak bij certificaatdienstverlener DigiNotar kon leiden tot een situatie waarin de continuïteit van een veilige gegevensuitwisseling met en tussen overheidsorganisaties onder druk kwam te staan.

Digitale certificaten spelen een cruciale rol in het beveiligen van elektronisch gegevensverkeer. Het is daarom van groot belang dat deze certificaten betrouwbaar zijn. De betrouwbaarheid van een digitaal certificaat wordt primair bepaald door de certificaatdienstverlener die het uitgeeft. Naarmate deze het aanvragen, aanmaken, uitreiken en intrekken van certificaten met meer waarborgen omgeeft, neemt de betrouwbaarheid van het certificaat toe. In tweede instantie wordt de betrouwbaarheid van een digitaal certificaat bepaald door het stelsel van afspraken en partijen waarin een certificaatdienstverlener opereert, en de wijze waarop dit stelsel functioneert. Dit hoofdstuk gaat in op de vraag welke waarborgen zijn voorzien opdat certificaatdienstverleners betrouwbaar opereren. Ook bespreekt het hoofdstuk wat in de praktijk de waarde van deze waarborgen is. De Onderzoeksraad neemt hierbij de beginselen voor veiligheidsmanagement, zoals geformuleerd in hoofdstuk 3, als uitgangspunt.

5.1 De gebruikers van certificaten

Het gebruik van certificaten is een middel is om de veiligheid van digitale gegevens te waarborgen tijdens de overdracht van deze gegevens.

Overheidsorganisatie die burgers en bedrijven verplichten gegevens met hen te delen moeten er voor zorgen dat zij de overdracht van die gegevens zo goed mogelijk beschermen. Hiervoor maken zij gebruik van onder meer digitale certificaten. Overheidsorganisaties moeten een middel kiezen dat een niveau van bescherming biedt dat in verhouding staat tot het belang van de te beschermen gegevens. Hiervoor moet de organisatie een afweging maken. Voor sommige informatie is beveiliging middels een certificaat misschien niet eens nodig, terwijl voor andere een hoog niveau van beveiliging middels een zeer veilig certificaat nodig is. Ook burgers en bedrijven zouden zich ervan moeten vergewissen dat de overheidsorganisatie met wie zij gegevens uitwisselen daarvoor een geldig certificaat beschikbaar stelt.[59]

De Onderzoeksraad is weliswaar van oordeel dat overheidsorganisaties de verantwoordelijkheid hebben om passende beveiligingsmiddelen te kiezen om digitale veiligheid te waarborgen, maar vindt ook dat van hen niet verwacht kan worden dat zij zelf in staat zijn de feitelijke betrouwbaarheid van het certificaat te controleren. Juist daarom is effectieve zelfregulering of overheidsregulering van belang.

59 Veel computerprogramma's, zoals de meeste internetbrowsers, bieden de eindgebruiker hierbij ondersteuning, door een waarschuwing te geven of zelfs de verbinding met een website te blokkeren wanneer deze niet door een geldig certificaat wordt beschermd.

Soorten digitale certificaten
DigiNotar gaf verschillende soorten digitale certificaten uit. Voor dit onderzoek worden certificaten ingedeeld in drie categorieën, waarop verschillende regels van toepassing zijn.

Standaardcertificaten
Dit zijn alle soorten certificaten waarop geen wettelijke eisen van toepassing zijn. Voor uitgifte van standaardcertificaten gelden hetzij de voorwaarden die de certificaatdienstverlener eenzijdig formuleert, hetzij specifieke voorwaarden die hij overeenkomt met (groepen van) beoogde afnemers. Zo leverde DigiNotar onder meer het BAPI-certificaat, specifiek bedoeld voor het beveiligen van gegevensuitwisseling met de Belastingdienst. Ook leverde DigiNotar specifieke certificaten aan de Nederlandse Orde van Advocaten en diverse andere beroepsgroepen.

DigiNotar verstrekte standaardcertificaten aan zowel private partijen als overheidsorganisaties, voor verschillende beveiligingsdoeleinden: het identificeren van individuen of functionarissen, het identificeren van internetdomeinnamen (SSL-certificaten) en het beveiligen van gegevensuitwisseling tussen zelfstandig communicerende apparaten. Op 16 september 2011 had het bedrijf ca. 50775 geldige standaardcertificaten uitstaan.

Gekwalificeerde certificaten
Dit zijn certificaten waarmee een rechtsgeldige elektronische handtekening kan worden gezet. Gekwalificeerde certificaten, alsook hun wijze van uitgifte, moeten voldoen aan bij of krachtens de Telecommunicatiewet geldende vereisten.

DigiNotar verstrekte gekwalificeerde certificaten aan zowel private partijen als overheidsorganisaties. Gekwalificeerde certificaten zijn in beginsel alleen bestemd voor het identificeren van natuurlijke personen. Op 16 september 2011 had het bedrijf ca. 3950 geldige gekwalificeerde certificaten uitstaan.

PKIoverheid-certificaten
Dit zijn certificaten voor de betrouwbaarheid waarvan de Staat der Nederlanden in laatste instantie instaat. PKIoverheid-certificaten, alsook hun wijze van uitgifte, moeten voldoen aan regels die worden vastgesteld door de minister van Binnenlandse Zaken en Koninkrijksrelaties. Certificaatdienstverleners die PKIoverheid-certificaten willen uitgeven, zijn contractueel gebonden aan naleving van deze regels.

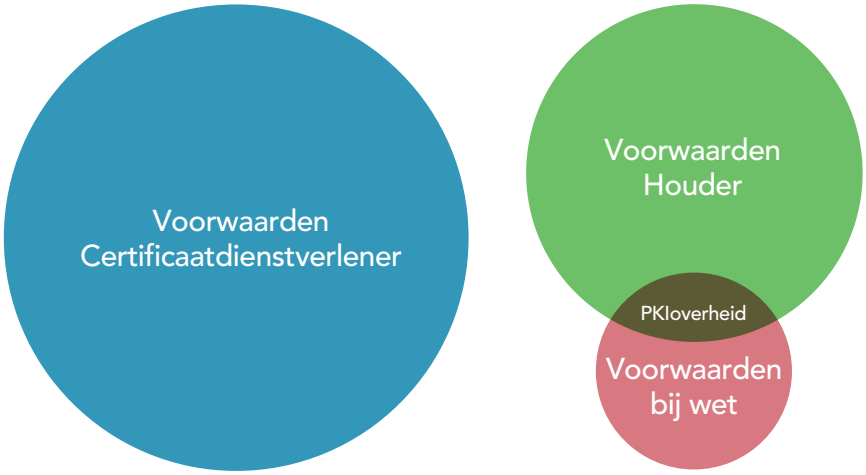
DigiNotar verstrekte PKIoverheid-certificaten aan zowel private partijen als overheidsorganisaties, voor alle eerder genoemde beveiligingsdoeleinden. Op 16 september 2011 had het bedrijf ca. 3200 geldige PKIoverheid-certificaten uitstaan. Het overgrote deel daarvan was verstrekt aan (functionarissen bij) overheidsorganisaties.

5.2 Stelsels voor certificaatdienstverlening

Het aanmaken, verstrekken en intrekken van digitale certificaten gebeurt in een stelsel van partijen en afspraken waarvan certificaatdienstverleners zoals DigiNotar de spil vormen.Figuur 3: Deelmarkten voor certificaatdienstverlening[60] Figuur 3 onderscheidt vier typen van dergelijke stelsels, die verschillen in de wijze waarop de voorwaarden tot stand komen waaraan de certificaatdienstverlening moet voldoen, en de wijze waarop wordt toegezien op naleving van deze voorwaarden. De grootte van de vlakken geeft een impressie hoe de omvang van deze deelmarkten zich tot elkaar verhoudt.[61]

60 Sommige grote bedrijven en organisaties geven voor intern gebruik hun eigen digitale certificaten uit. Deze vorm van certificaatdienstverlening, waarbij de certificaten binnen één organisatie worden uitgegeven en gebruikt, blijft in dit onderzoek buiten beschouwing.

61 Dit is nadrukkelijk niet meer dan een impressie, gebasserd op uitspraken die zijn gedaan in de gesprekken die de Onderzoeksraad heeft gevoerd. Het aantal uitstaande certificaten wordt, behalve voor de gekwalificeerde certificaten, niet geregistreerd.



Figuur 3: Deelmarkten voor certificaatdienstverlening

5.2.1 Certificaatdienstverlening op voorwaarden certificaatdienstverlener

Certificaatdienstverlening is in beginsel niet gereguleerd. De aanvraag, productie en uitgifte van deze certificaten kan de certificaatdienstverlener omgeven met veiligheidsvoorzieningen zoals het hem goeddunkt. Als de gebruikers van de certificaten vertrouwen in zijn diensten hebben, zullen zij deze digitale certificaten afnemen. Het is onbekend hoe groot de deelmarkt voor ongereguleerde certificaatdienstverlening in Nederland precies is. Wereldwijd zijn circa 650 certificaatdienstverleners actief. Nederlandse bedrijven en organisaties kunnen bij elk van deze partijen hun certificaten betrekken, en zijn niet gebonden aan in Nederland gevestigde dienstverleners. Veel overheidsorganisaties beveiligen (delen van) hun gegevensverkeer door gebruik te maken van ongereguleerde certificaten.[62]

5.2.2 Certificaatdienstverlening op voorwaarden certificaathouder

In een kleiner gedeelte van de markt voor certificaatdienstverlening worden de voorwaarden waaraan het certificaat en de wijze van verstrekking moeten voldoen bepaald in overleg tussen de certificaatdienstverlener en de partij die deze certificaten als beveiligingsmiddel beschikbaar stelt. Het betrouwbaarheidsniveau van de certificaten kan zo worden afgestemd op de specifieke beveiligingsbehoeften van de certificaathouder. Een voorbeeld van deze vorm van certificaatdienstverlening zijn de zogenaamde BAPI-certificaten die de Belastingdienst gebruikt voor het beveiligen van zijn elektronische gegevensverkeer met bedrijven en intermediairs. Behalve voor de Belastingdienst maakt bijvoorbeeld ook de Orde van Advocaten van dit soort certificaten gebruik. Ook de omvang van deze deelmarkt van certificaatdienstverlening is onbekend.

5.2.3 Bij wet gereguleerde certificaatdienstverlening

Een klein gedeelte van certificaatdienstverlening wordt gereguleerd door de Telecommunicatiewet.[63] Dit betreft de levering van zogenaamde gekwalificeerde certificaten. Hiermee kan een rechtsgeldige elektronische handtekening gezet worden. De wetgever heeft bepaald dat deze certificaten aan specifieke betrouwbaarheidseisen moeten voldoen. Hiermee is beoogd dat zij een zeer hoog niveau van betrouwbaarheid bieden. Een certificaatdienstverlener die gekwalificeerde certificaten wil uitgeven, moet zich laten registreren bij OPTA. De markt voor gekwalificeerde certificaatdienstverlening is altijd tamelijk klein gebleven. Momenteel staan zeven organisaties geregistreerd bij OPTA als leverancier van gekwalificeerde certificaten. Zij hebben gezamenlijk ongeveer 130.000 gekwalificeerde certificaten uitstaan.

62 Voor de meeste ICT-diensten die Logius aanbiedt aan overheidsorganisaties (zoals de authenticatievoorziening DigiD) is echter het gebruik van PKIoverheid-certificaten verplicht.

63 Op grond van artikel 18.15 Telecommunicatiewet. Dit is de Nederlandse implementatie van de Europese Richtlijn 99/93/EG, betreffende een gemeenschappelijk kader voor elektronische handtekeningen.

De bij wet gereguleerde certificaatdienstverlening voor gekwalificeerde certificaten is niet noodzakelijkerwijs veiliger dan de deelmarkten waar partijen zelf de regels vaststellen, al dan niet met gebruikmaking van zelfregulering (zie hieronder). Certificaatdienstverleners zelf, dan wel de partijen in wier opdracht of met wier goedkeuring zij hun diensten verlenen, kunnen voorwaarden overeenkomen voor de uitgifte van certificaten die net zo strikt of zelfs strikter zijn dan de wettelijke vereisten die gelden voor gekwalificeerde certificaten.

5.2.4 PKIoverheid-certificaten

PKIoverheid-certificaten behoren tot de certificaten waarvoor de voorwaarden in overleg tussen de partijen zijn vastgesteld (zie paragra5.2.2af 5.2.2). PKIoverheid-certificaten beogen te voorzien in de specifieke beveiligingsbehoefte van hun doelgroep: overheidsorganisaties die onderling of met burgers en bedrijven elektronisch gegevens uitwisselen. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties beoogt met de PKIoverheid-certificaten aanvullende waarborgen te bieden ten opzichte van de andere certificaten. Het beleid en de voorwaarden voor het leveren van PKIoverheid-certificaten is opgesteld door de minister van Binnenlandse Zaken en Koninkrijksrelaties. Deze voorwaarden zijn onderdeel van een overeenkomst tussen het Ministerie en de onder PKIoverheid opererende certificaatdienstverleners, die een contractuele relatie met elkaar hebben. In paragraaf 5.3 wordt de inrichting van PKIoverheid in meer detail besproken.

De markt voor PKIoverheid-certificaten is kleiner dan de andere deelmarkten die eerder zijn genoemd. Nadat DigiNotar de levering van PKIoverheid-certificaten moest beëindigen, resteren nog zeven certificaatdienstverleners die PKIoverheid certificaten uitgeven. Het aantal certificaathouders is beperkt. PKIoverheid-certificaten zijn in eerste instantie bedoeld voor overheidsorganisaties.

5.2.5 De rol van zelfregulering

Zelfregulering speelt een belangrijke rol in de markt van certificaatdienstverlening. Er bestaan diverse keurmerken die als kwaliteitswaarborg dienen voor het leveren van certificaatdiensten. Sommige van deze keurmerken baseren zich op internationale of sectorspecifieke standaarden voor certificaatdienstverlening.[64] Deze keurmerken hebben ten doel zekerheid te bieden aan afnemers van digitale certificaten, zoals overheidsorganisaties, die zelf niet in staat zijn de betrouwbaarheid van een certificaatdienstverlener te beoordelen.

Het beleid van de Nederlandse rijksoverheid wil zelfregulering door certificaatdienstverleners zoveel mogelijk stimuleren. De rijksoverheid stimuleert dit door certificaatdienstverleners die beschikken over een TTP.NL-verklaring eenvoudiger toe te laten tot de levering van gekwalificeerde certificaten. Ditzelfde keurmerk is verplicht voor partijen die opereren onder PKIoverheid.

5.3 Inrichting van PKIoverheid

De nu volgende paragrafen gaan in op de inrichting van het stelsel van partijen en afspraken dat is gericht op het aanmaken, uitgeven en intrekken van PKIoverheid-certificaten. Er zijn twee redenen om dit stelsel nader te beschrijven. Ten eerste is PKIoverheid door de rijksoverheid in het leven geroepen met het specifieke doel om overheidsorganisaties een zo goed mogelijke bescherming van hun elektronisch gegevensverkeer te bieden. Gezien de bijzondere verantwoordelijkheid die overheidsorganisaties hebben om de digitale veiligheid van dit gegevensverkeer te waarborgen, is het van extra groot belang dat de middelen die de rijksoverheid daartoe aanbiedt, de veronderstelde mate van bescherming bieden. Dit geldt des te sterker aangezien de rijksoverheid PKIoverheid nadrukkelijk positioneert als een veiliger alternatief voor andere digitale certificaten.

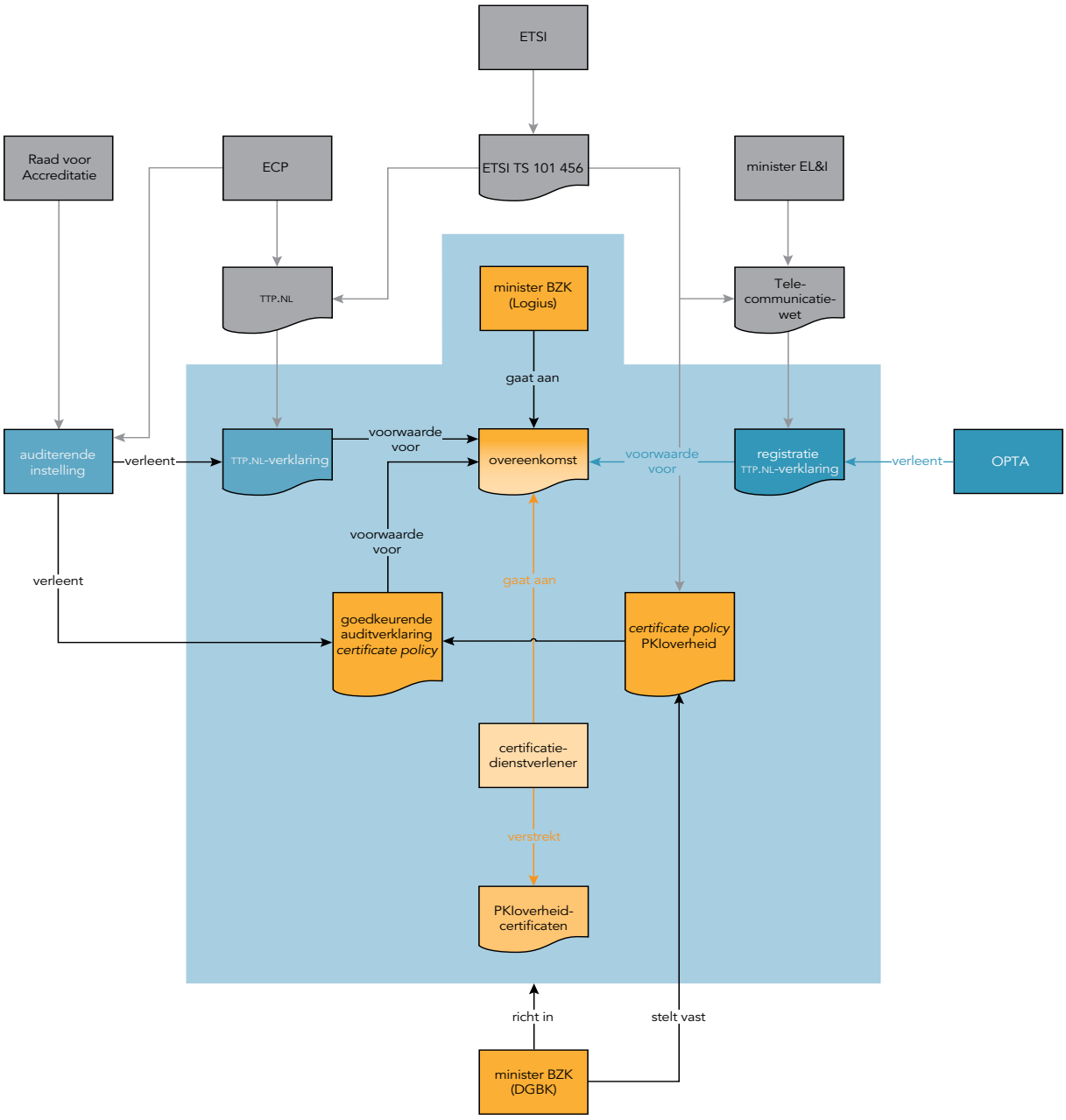
64 Voorbeelden van bekende normen en standaarden zijn de Europese ETSI TS 102 042, *Policy requirements for certification authorities issuing public key certificates* (ETSI, 2002) en de internationale RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* (IETF, 2003). Een bekend keurmerk voor certificaatdienstverlening is het Canadees/Amerikaanse WebTrust, dat onder meer refereert aan RFC 3647.

Ten tweede geeft het functioneren van PKIoverheid ook inzicht in het functioneren van andere stelsels voor certificaatdienstverlening; de regels en waarborgen die PKIoverheid omgeven, gelden immers in meer of mindere mate ook voor deze andere stelsels.

Figuur 4 geeft een schematische weergave van de inrichting van PKIoverheid. De figuur laat zien dat vier partijen een centrale rol in het stelsel hebben. De minister van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor de inrichting en het beheer van het stelsel, en voor de toelating van certificaatdienstverleners.

OPTA is verantwoordelijk voor de registratie van leveranciers van gekwalificeerde certificaten en voor het toezicht op werkzaamheden van bij haar geregistreerde certificaatdienstverleners, voor zover die betrekking hebben op het leveren van gekwalificeerde certificaten. Registratie bij OPTA is een vereiste om te kunnen toetreden tot PKIoverheid. Ten derde is er natuurlijk de certificaat-dienstverlener zelf, die de verantwoordelijkheid heeft om zijn bedrijfsprocessen zo in te richten dat hij voldoet aan de vereisten die gelden binnen PKIoverheid en die hem in staat stellen betrouwbare certificaten te leveren. Ten vierde spelen de auditerende instellingen een belangrijke rol. Zij toetsen in opdracht van de certificaatdienstverlener conform het TTP.NL-schema, of deze voldoet aan de voorwaarden die gelden voor het leveren van certificaten onder PKIoverheid.

Meer op afstand (in grijs weergegeven) spelen nog enkele partijen een rol. Deze hebben geen directe bemoeienis met het stelsel PKIoverheid, maar hebben wel invloed op het handelen van de partijen die in dit stelsel een rol spelen.



Figuur 4: Inrichting PKIoverheid

5.3.1 Rol minister Binnenlandse Zaken en Koninkrijksrelaties

De minister van Binnenlandse zaken en Koninkrijksrelaties heeft PKIoverheid opgezet om overheidsorganisaties een middel te bieden om hun gegevensverkeer te beveiligen. De minister van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor de inrichting van PKIoverheid en fungeert tevens als de beheerder van het stelsel. Hij laat certificaatdienstverleners tot het stelsel toe door met hen een overeenkomst te sluiten.

Het ambtelijk opdrachtgeverschap voor PKIoverheid berust bij het Directoraat-generaal Bestuur en Koninkrijksrelaties en daarbinnen de Directie Burgerschap en Informatiebeleid. Het tactisch beheer over PKIoverheid berust bij het agentschap Logius. Het operationeel beheer van PKIoverheid, zoals de inrichting en het beheer van de technologische omgeving, heeft Logius uitbesteed aan marktpartijen. Logius is belast met de toetreding van certificaatdienstverleners tot PKIoverheid en met controle en toezicht op hun werkzaamheden na toelating. Hiertoe behoort onder meer het sluiten en ontbinden van overeenkomsten met certificaatdienstverleners en het houden van toezicht op naleving van de voorwaarden die zijn opgenomen in de overeenkomst en het Programma van Eisen PKIoverheid.

Een andere taak van Logius is bijdragen aan de ontwikkeling en het beheer van het normenkader dat aan de PKIoverheid ten grondslag ligt, het zogeheten Programma van Eisen PKIoverheid.

Tot aan het incident met DigiNotar heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties niet geëvalueerd of PKIoverheid in de praktijk werkt zoals werd beoogd en of het stelsel in de praktijk functioneert conform de gestelde eisen. Ook heeft de minister geen risico-inventarisaties laten maken die in kaart brengen hoe de certificaatdienstverlening onder PKIoverheid in gevaar kan komen en op welke manier aan dergelijke scenario's dan het hoofd geboden kan worden.

5.3.2 Programma van Eisen PKIoverheid

De inrichting van PKIoverheid ligt vast in het Programma van Eisen PKIoverheid. Dit beschrijft de bevoegdheden en verantwoordelijkheden van de verschillende betrokken partijen en de voorwaarden waaronder certificaatdienstverleners aan PKIoverheid kunnen deelnemen.[65]

Het Programma van Eisen bepaalt dat een certificaatdienstverlener die actief is onder PKIoverheid aan drie belangrijke voorwaarden moet voldoen. Ten eerste moet hij de wettelijke vereisten naleven die gelden voor leveranciers van gekwalificeerde certificaten. Ten bewijze daarvan moet hij geregistreerd zijn bij OPTA. Ten tweede moet de certificaatdienstverlener de ETSI-norm TS 101 456 aantoonbaar naleven.[66] Hiertoe moet hij een TTP.NL-verklaring kunnen overleggen. Ten derde moet hij aantoonbaar voldoen aan de voorwaarden die zijn opgenomen in het Programma van Eisen PKIoverheid. Deze voorwaarden komen voor een groot deel overeen met de wettelijke vereisten die gelden voor leveranciers van gekwalificeerde certificaten, en met de eisen die zijn opgenomen in de eerder genoemde ETSI-norm TS 101 456. Wel zijn deze op enkele punten aangescherpt of nader ingevuld.[67]

Het Programma van Eisen regelt bovendien de wijze waarop Logius als wederpartij toeziet op naleving van de overeenkomst door certificaatdienstverleners binnen PKIoverheid. De certificaatdienstverlener moet jaarlijks een aantal documenten overleggen aan het agentschap, die bewijzen dat hij voldoet aan de hierboven genoemde eisen. Als OPTA zijn registratie beëindigt, of de auditerende instelling de TTP.NL-verklaring intrekt, moet hij daarvan direct melding maken. Uit de overeenkomst vloeit ook een plicht voort om relevante incidenten onverwijld bij Logius te melden.

5.3.3 Overeenkomst met certificaatdienstverleners

De toelatingsovereenkomst overweegt dat PKIoverheid voorziet in een werkbaar en betrouwbaar elektronisch communicatiekanaal voor en met overheidsorganisaties. De overeenkomst bepaalt dat de certificaatdienstverlener zich ertoe verbindt certificaatdiensten aan te bieden conform de door de minister van Binnenlandse Zaken en Koninkrijksrelaties gestelde eisen. Deze eisen zijn vastgelegd in de overeenkomst en het Programma van Eisen PKIoverheid. Ook stelt de overeenkomst dat het ministerie van Binnenlandse Zaken en Koninkrijksrelaties toeziet op de naleving van dit normenkader.

Enkele relevante bepalingen uit de overeenkomst zijn:

- De certificaatdienstverlener dient het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onverwijld op de hoogte te stellen van eventuele compromittering van zijn private sleutel(s) en van andere relevante incidenten. Relevante incidenten zijn in ieder geval incidenten die afbreuk doen aan de betrouwbaarheid van de dienstverlening (artikel 4, derde lid);
- het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is te allen tijde gerechtigd een audit te laten uitvoeren bij de certificaatdienstverlener om vast te stellen of hij voldoet aan de in de overeenkomst neergelegde eisen. De certificaatdienstverlener moet medewerking verlenen aan een dergelijk onderzoek (artikel 5, derde lid);

65 Dit laatste element van het Programma van Eisen wordt ook wel aangeduid als de *certificate policy* van PKIoverheid.

66 PKIoverheid kent ook enkele certificaatsoorten waarop andere ETSI-normen van toepassing zijn.

67 Het Programma van Eisen schrijft bijvoorbeeld een maximale termijn voor waarbinnen storingen aan sommige processen bij de certificaatdienstverlener moeten zijn verholpen, terwijl de ETSI-norm alleen bepaalt dat de certificaatdienstverlener hiervoor een maximale termijn moet stellen. Ook verplicht het Programma van Eisen tot vaststelling in persoon van de identiteit van de certificaathouder, terwijl een dergelijk stringente bepaling in de ETSI-norm niet is opgenomen.

- de minister van Binnenlandse Zaken en Koninkrijksrelaties is gerechtigd de overeenkomst met een certificaatdienstverlener eenzijdig te ontbinden als deze niet voldoet aan het Programma van Eisen PKIoverheid, of anderszins niet in staat geacht kan worden de verplichtingen uit de overeenkomst na te kunnen komen.

5.4 Toetreding tot PKIoverheid

In de vorige paragraaf werd gesteld dat certificaatdienstverleners onder PKIoverheid aan drie voorwaarden moeten voldoen. Bij hun toetreding tot het stelsel verifieert Logius namens de minister van Binnenlandse Zaken en Koninkrijksrelaties of dat het geval is.

5.4.1 Registratie bij OPTA

Certificaatdienstverleners die gekwalificeerde certificaten uitgeven moeten geregistreerd staan bij OPTA. Hiertoe moet de certificaatdienstverlener voldoen aan een aantal operationele en organisatorische eisen die zijn opgenomen in het Besluit elektronische handtekeningen.[68]

Doordat in de wetgeving uitsluitend een registratie- en geen vergunningsplicht is opgenomen om gekwalificeerde certificaten te mogen aanbieden, is de toegang tot de markt zeer laagdrempelig. De wetgever heeft deze mogelijkheid gecreëerd om zelfregulering door certificaatdienstverleners te stimuleren. Wel moeten certificaatdienstverleners die gekwalificeerde certificaten afgeven bij registratie aannemelijk maken dat ze aan de wettelijke eisen voldoen. Een bewijs van toetsing, afgegeven in het kader van een erkende certificatie en accreditatieregeling is hiervoor één mogelijkheid, een eigen verklaring met een ondersteunend informatiedossier is een andere.[69] OPTA voert, in lijn met de toelichting op de Wet elektronische handtekeningen, slechts een marginale toets uit op dat informatiedossier, tenzij er redelijke vermoedens bestaan dat er feitelijk niet aan de eisen wordt voldaan.

Een ttp.nl-verklaring (5.4.2.4.2) geldt als bewijs van toetsing. Een certificaatdienstverlener die deze verklaring kan overleggen, wordt zonder onderzoek door OPTA geregistreerd. Bovendien betaalt hij een lager registratietarief. De gekozen tariefstructuur, die wordt vastgesteld door de minister van Economische Zaken, Landbouw en Innovatie, stimuleert gebruikmaking van deze route. Als gevolg hiervan hebben tot nog toe alle certificaatdienstverleners gekozen voor de verkorte registratieroute via de ttp.nl-verklaring. OPTA registreert de certificaatdienstverlener na ontvangst van de ttp.nl-verklaring.

De onderliggende onderzoeksrapporten krijgt OPTA op dat moment niet te zien. Na controle van enkele aanvullende bedrijfsgegevens volgt registratie. Om de registratie te behouden, is de certificaatdienstverlener verplicht jaarlijks het rapport van de surveillance audit te overleggen.

5.4.2 Verkrijgen van een ttp.nl-verklaring

Om PKIoverheid-certificaten te mogen uitgeven, moet de certificaatdienstverlener de hiervoor genoemde ttp.nl-verklaring met rapportage van de auditor overleggen. Op grond van het Programma van Eisen PKIoverheid accepteert Logius deze verklaring als bewijs van het feit dat de certificaatdienstverlener voldoet aan de voorwaarden in de ETSI-norm TS 101 456. De verklaring wordt afgegeven op basis van een audit volgens het certificeringsschema ttp.nl. Dit schema bepaalt dat een certificaatdienstverlener aan de volgende eisen moet voldoen:

- Hij moet voldoen aan de ETSI-norm TS 101 456 en alle wettelijke vereisten voor leveranciers van gekwalificeerde certificaten;
- hij moet aantoonbaar beschikken over betrouwbare systemen;[70]
- hij moet periodiek onderzoeken c.q. toetsen of de eigen bedrijfsvoering nog voldoet aan de ETSI-norm TS 101 456;

68 Artikel 2 Besluit elektronische handtekeningen. Dit is een uitwerking van de bepalingen in bijlage II van de Europese richtlijn 1999/93 inzake elektronische handtekeningen.
69 Art. 18.16a, eerste lid Telecommunicatiewet.
70 Betrouwbare systemen (*trustworthy systems*) zijn ICT-systemen die aantoonbaar voldoen aan de vereisten van de Europese norm CWA 14167 voor de veiligheid van ICT-systemen voor certificaatdienstverlening, of een daarmee vergelijkbare standaard.

- hij moet waarborgen dat externe partijen aan wie werkzaamheden worden uitbesteed, handelen volgens de ETSI-norm TS 101 456;
- hij moet de auditors de voor certificering relevante documenten kunnen overleggen;
- hij moet na verkrijgen van het certificaat blijven voldoen aan de voor verkrijging geldende eisen.

Om een TTP.NL-verklaring te verkrijgen, moet de certificaatdienstverlener zich laten auditeren door een ter zake kundige auditor. De auditerende instellingen die TTP.NL-verklaringen mogen verstrekken worden ingevolge artikel 18.16 van de Telecommunicatiewet aangewezen door de minister van Economische Zaken, Landbouw en Innovatie. Een voorwaarde hiervoor is dat zij door de Raad voor Accreditatie zijn geaccrediteerd.[71] In Nederland zijn twee instellingen bevoegd om dergelijke audits uit te voeren. De auditerende instelling sluit voor het verrichten van de audit een overeenkomst met de certificaatdienstverlener.

De auditerende instelling onderzoekt de certificaatdienstverlener aan de hand van het certificeringsschema TTP.NL. Het schema beschrijft onder meer welke onderwerpen de audit omvat, hoe de audit wordt uitgevoerd, welke documenten de certificaatdienstverlener beschikbaar moet maken en aan welke kwalificaties de auditor moet voldoen. Ook bevat het schema richtlijnen voor het aantal manuren dat een audit ongeveer kost.

Het certificeringsschema schrijft voor dat de auditerende instelling zowel documentenonderzoek als een implementatie-audit verricht. Het certificeringsschema verbiedt de auditor een TTP.NL-verklaring af te geven wanneer de auditor zogenaamde major nonconformities constateert in de bedrijfsvoering van de certificaatdienstverlener. Deze tekortkomingen moet de certificaatdienstverlener eerst oplossen of verminderen. Hiertoe moet hij een actieplan opstellen, dat de auditerende instelling moet beoordelen. De auditerende instelling besluit in dit geval of een aanvullende audit of schriftelijke bewijsstukken nodig zijn om vast te stellen of het actieplan de geconstateerde tekortkomingen voldoende adresseert.

De TTP.NL-verklaring heeft een geldigheidsduur van drie jaar, waarbij de certificaatdienstverlener jaarlijks een eenvoudiger heronderzoek moet ondergaan (de zogenaamde surveillance audit). Wanneer de auditor daarbij een major nonconformity constateert, hoeft hij niet meteen de verklaring in te trekken. Hij verplicht de certificaatdienstverlener in dat geval tot het opstellen van een actieplan. Op basis van het actieplan beoordeelt de auditor of hij erop vertrouwt dat de tekortkoming wordt opgelost.

Aan een TTP.NL-verklaring mag volgens het TTP.NL-schema een gerechtvaardigd vertrouwen worden ontleend dat de certificaatdienstverlener aan de vereisten van de eerder genoemde ETSI-normen voldoet. Belangrijk is evenwel dat het schema bepaalt dat het hier een managementsysteemaudit betreft. Het audit-team onderzoekt of het managementsysteem van het bedrijf voldoet aan de ETSI-norm en vigerende wet- en regelgeving. Een TTP.NL-verklaring impliceert een gerechtvaardigd vertrouwen dat de certificaatdienstverlener de vigerende wet- en regelgeving naleeft, gebaseerd op onderzoek of zijn managementsysteem voldoet aan de ETSI-norm TS 101 456. De auditor toetst beperkt of de certificaatdienstverlener de regels feitelijk naleeft.

Het TTP.NL-schema schrijft niet gedetailleerd voor welke stappen de auditor moet doorlopen om te komen tot een oordeel. Op welke overwegingen dit oordeel is gebaseerd is evenmin zichtbaar, omdat het auditrapport alleen afwijkingen van de norm vermeldt.

5.4.3 Voldoen aan Programma van Eisen PKIoverheid

Ten derde is de certificaatdienstverlener verplicht te voldoen aan het Programma van Eisen PKIoverheid. Hij moet hiertoe een goedkeurende auditverklaring verkrijgen van een auditerende instelling die ook geaccrediteerd is om TTP.NL-verklaringen af te geven. Het onderzoek dat aan deze verklaring ten grondslag ligt, moet een vergelijkbare diepgang hebben als het onderzoek dat wordt uitgevoerd om een TTP.NL-verklaring te verkrijgen. De goedkeurende auditverklaring met rapportage moet de certificaatdienstverlener voor toetreding overleggen.

71 Besluit elektronische handtekeningen, artikel 3a, onder d.

In de meeste gevallen breidt de auditerende instelling hiertoe de TTP.NL-audit uit met vragen om vast te stellen of de certificaatdienstverlener voldoet aan het Programma van Eisen PKIoverheid, voor zover de bepalingen daarin afwijken van die in de ETSI-norm TS 101 456. Dit lijkt logisch, omdat deze eisen slechts in enkele opzichten van elkaar verschillen. Echter, aangezien de TTP.NL-audit, zoals eerder is opgemerkt, primair gericht is op het functioneren van het managementsysteem van de certificaatdienstverlener betekent dit in de praktijk dat feitelijke naleving van een groot gedeelte van de bepalingen in het Programma van Eisen niet wordt onderzocht.

Logius controleert voor toelating van een certificaatdienstverlener tot PKIoverheid, of aan de drie bovengenoemde voorwaarden wordt voldaan. Bovendien toetst Logius bij aansluiting het Certification Practice Statement, het document waarin de certificaatdienstverlener zijn procedures beschrijft.

5.5 Toezicht op functioneren PKIoverheid

Er zijn drie partijen die controleren of een certificaatdienstverlener zich aan de geldende eisen houdt. Dit betreft Logius als wederpartij in de overeenkomst, en OPTA als toezichthouder op de gekwalificeerde certificaten. De auditerende instellingen controleren middels een TTP.NL-audit of het managementsysteem van de certificaatdienstverlener voldoet aan de geldende normen. Deze audit is enerzijds een zelfreguleringinstrument en anderzijds speelt hij een centrale rol in het toezicht.

5.5.1 Informatieplicht door certificaatdienstverlener bij calamiteiten

Bij het toezicht speelt de informatieplicht die op de certificaatdienstverlener rust, een belangrijke rol. Een certificaatdienstverlener die PKIoverheid-certificaten uitgeeft, heeft een drieledige informatieplicht: jegens OPTA, Logius en de auditerende instelling.

1. De Telecommunicatiewet (artikel 2, derde lid onder 5) bepaalt dat een geregistreerd certificaatdienstverlener de plicht heeft om bij OPTA "onverwijld alle wijzigingen te melden die van invloed zijn op de registratie".
2. Het certificeringsschema TTP.NL bepaalt dat er een meldplicht bestaat van de certificaatdienstverlener jegens de auditerende instelling. Bepaald is dat: "*any change in organization, management, activities and/or management system during the validity of the certificate must be reported to the Certification Body without delay*".
3. De toetredingsovereenkomst tussen Staat der Nederlanden en de certificaatdienstverlener verplicht deze laatste om Logius onverwijld op de hoogte te stellen van een eventuele compromittering van zijn private sleutel(s) en van andere relevante incidenten. Relevante incidenten zijn in ieder geval gebeurtenissen die afbreuk doen aan de betrouwbaarheid van de dienstverlening.[72]

5.5.2 Toezicht door Logius

Logius is als tactisch beheerder van PKIoverheid belast met het houden van toezicht op de naleving door de certificaatdienstverleners van de voorwaarden in de toetredingsovereenkomst.

De basis voor het toezicht door Logius zijn de verklaringen van de auditor. Het Programma van Eisen geeft aan dat de certificaatdienstverlener deze direct ter beschikking van Logius stelt, zodra hij deze heeft ontvangen van de auditerende instelling. De volledige rapportages met gedetailleerde bevindingen hoeven niet te worden bijgesloten.[73] Wel moeten de belangrijkste bevindingen die door de auditerende instelling zijn gedaan, worden overgelegd aan Logius. De volledige rapportages dienen op elk gewenst moment door Logius te kunnen worden ingezien op de locatie van de certificaatdienstverlener. Ook kan het voorkomen dat Logius van derden een signaal krijgt dat er aanleiding is voor nader onderzoek. Logius heeft voor het tactisch beheer van het PKI-overheidstelsel en voor haar toezichthoudende taken 1,4 fte tot zijn beschikking. Logius kwalificeert zichzelf als derdelijnstoezichthouder voor wat betreft de gekwalificeerde certificaten en tweedelijns voor wat betreft de aanvullende eisen in het Programma van Eisen.

72 Art. 4, derde lid Overeenkomst tussen de Staat der Nederlanden en DigiNotar B.V.
73 Programma van Eisen PKIoverheid, deel 2, paragraaf 3.2.1

5.5.3 Toezicht door OPTA

OPTA ziet er op grond van de Telecommunicatiewet op toe dat bij haar geregistreerde certificaatdienstverleners voldoen aan de wettelijke bepalingen die van toepassing zijn op het leveren van gekwalificeerde certificaten. Als OPTA constateert dat een geregistreerde certificaatdienstverlener activiteiten of diensten verricht in strijd met het bepaalde bij of krachtens de Telecommunicatiewet, kan zij deze een last onder dwangsom opleggen.[74] In het uiterste geval kan OPTA de registratie van een certificaatdienstverlener beëindigen. Als OPTA besluit deze middelen in te zetten, moet zij handelen volgens de Algemene wet bestuursrecht en de algemene beginselen van behoorlijk bestuur in acht nemen.[75] OPTA is tweedelijnstoezichthouder voor de bij haar geregistreerde certificaatdienstverleners. Zij had ten tijde van het DigiNotarincident voor het toezicht op bij haar geregistreerde certificaatdienstverleners 0,3 fte aan toezichtcapaciteit.[76, 77]

OPTA vult haar toezicht op geregistreerde certificaatdienstverleners in door jaarlijks de rapporten te vorderen van de TTP.NL-audits die zij hebben laten uitvoeren. Deze systematiek van toezicht is omschreven in de memorie van toelichting bij de Wet elektronische handtekeningen.[78] Indien twijfels bestonden ten aanzien van door de auditor geconstateerde afwijkingen, of de wijze waarop deze zijn opgelost, stelde OPTA daarover vragen bij de certificaatdienstverlener. Eénmaal is bij een partij aangekondigd dat de registratie zou worden beëindigd als bepaalde non-conformiteiten niet binnen een bepaalde termijn zouden worden opgelost. Voor het overige vertrouwt OPTA – in lijn met haar formele opdracht – op de verklaring van de auditerende instelling en toetst de betrouwbaarheid van de certificaatdienstverlener niet zelf.

5.5.4 TTP.NL-verklaring als basis voor toezicht door Logius en OPTA

De TTP.NL-audit staat als zelfreguleringsinstrument primair ten dienste van een proces van continue verbetering door de certificaatdienstverlener zelf, zoals bijvoorbeeld blijkt uit de omgang met majeure afwijkingen die het schema voorschrijft. Die leiden niet tot onmiddellijke intrekking van het certificaat, maar dient het bedrijf aan te grijpen om zijn beheersing van zijn bedrijfsprocessen verder te verbeteren. Deze beheersing stelt hem, maar ook zijn opdrachtgever (in casu Logius) in staat om een goede inschatting te maken van de betrouwbaarheid van zijn dienstverlening. Dat wil echter niet zeggen dat de TTP.NL-verklaring een betrouwbare dienstverlening garandeert.

De Onderzoeksraad constateert dat partijen in het stelsel, in het bijzonder Logius en OPTA, aan de TTP.NL-verklaring een waarde toekennen die niet overeenkomt met het doel waartoe dit keurmerk is opgericht. Zij lijken ervan uit te gaan dat de TTP.NL-verklaring betekent dat de certificaatdienstverlener zijn bedrijfsvoering met zekerheid uitoefent conform de bepalingen van de ETSI-norm TS 101 456 en de Telecommunicatiewet. Dat is echter niet zonder meer het geval. Bij de audit wordt gecontroleerd of het managementsysteem van de certificaatdienstverlener een gerechtvaardigd vertrouwen (justified confidence) biedt dat deze aan de regels voldoet.[79] De feitelijke naleving daarvan wordt beperkt getoetst.

De Onderzoekraad constateert dat er een discrepantie bestaat tussen het eigenlijke doel van een audit zoals de TTP.NL-audit, en de waarde die Logius en OPTA eraan toekennen als instrument voor toezicht op en handhaving van naleving van de vigerende wet- en regelgeving.

74 OPTA kan hiertoe gebruik maken van de generieke handhavingsbevoegdheden die zij heeft ex art. 15 Telecommunicatiewet.

75 OPTA ziet alleen toe op werkzaamheden van bij haar geregistreerde certificaatdienstverleners, voor zover die geen betrekking hebben op het leveren van gekwalificeerde certificaten. Omdat niet alle PKIoverheid-certificaten gekwalificeerde certificaten zijn, strekt het toezicht door OPTA zich dus niet uit tot alle PKIoverheid-certificaten.

76 De capaciteit die OPTA voor het toezicht op de certificaatdienstverleners beschikbaar heeft, wordt bepaald door de vergoedingen voor het toezicht die jaarlijks worden vastgesteld in de Regeling Vergoedingen OPTA.

77 Inmiddels bedraagt de toezichtcapaciteit van OPTA door toegenomen taken, zoals de Vertrouwenslijst en intensivering van het toezicht door middel van bedrijfsbezoeken, 1,8 fte.

78 Kamerstuk TK 27743-3.

79 De rapportage evaluatie PKI (Logica, in opdracht van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, en Economische Zaken, Landbouw en Innovatie) wijst erop dat auditerende instellingen in hun TTP.NL-verklaringen niet eenduidig verwijzen naar de regelgeving waarop deze zijn gebaseerd, waardoor de waarde van de verklaring niet op het eerste gezicht duidelijk is.

Zij moeten in het kader van dit toezicht beoordelen of het verantwoord is de certificaatdienstverlener nog langer gekwalificeerde of PKIoverheid-certificaten te laten afgeven. Daartoe moet de feitelijke betrouwbaarheid van zijn dienstverlening bekend zijn. De Onderzoeksraad meent dat gezien het grote belang van veilige certificaatdienstverlening en het feit dat het toezicht in hoofdzaak gebaseerd is op audits, een zuivere managementsysteemaudit onvoldoende zicht geeft op de vraag in hoeverre de bedrijfsvoering van certificaatdienstverleners werkelijk voldoet aan de voorschriften die de rijksoverheid hieraan als opdrachtgever van PKIoverheid stelt.

Hier komt bij dat het certificeringsschema TTP.NL niet voorschrijft hoe een auditor tot zijn oordeel moet komen en hem niet verplicht om de overwegingen te expliciteren die leiden tot het toekennen van de TTP.NL-verklaring. Toezichthoudende partijen kunnen hierdoor in feite niet bepalen hoeveel vertrouwen zij kunnen stellen in een TTP.NL-verklaring en daarmee in de kwaliteit van de dienstverlening door de certificaatdienstverleners. De Onderzoeksraad kan zich voorstellen dat de auditerende instellingen aandacht voor deze problematiek hadden gevraagd op het moment dat zij zich realiseerden dat aan de door hun uitgevoerde audit een zekerheid werd toegekend, die hier niet aan kon worden toegekend.

Zowel in de interviews die de Onderzoeksraad voerde, als in het commentaar op het conceptrapport blijkt een verschil van verwachtingen te bestaan tussen partijen voor wat betreft de zekerheid die ontleend mag worden aan de audit die de auditerende instellingen uitvoeren volgens het TTP.NL-certificeringsschema. De vraag die de betrokken partijen zich, naar het oordeel van de Onderzoeksraad gezamenlijk zouden moeten stellen is wat voor zekerheid gewenst is en hoe deze zekerheid verkregen wordt. Aanvullende zekerheid kan worden verkregen door verscherping en verdieping van de audits of aanpassing van het TTP.NL-schema. De Onderzoeksraad merkt echter op dat aanvullende zekerheid ook verkregen wordt als het toezicht meer gedifferentieerd is waardoor de audit niet langer het centrale element is waarop het toezicht is gebaseerd.

5.6 Conclusie

Dit hoofdstuk richtte zich op de vraag in hoeverre de inrichting en het functioneren van stelsels voor certificaatdienstverlening de betrouwbaarheid van digitale certificaten waarborgen. In relatie tot de eerder genoemde uitgangspunten voor veiligheidsmanagement (Hoofdstuk 3) concludeert de Onderzoeksraad het volgende.

5.6.1 Zicht op de risico's niet geborgd

De basis voor effectief veiligheidsmanagement is het kennen van de risico's. Alleen dan is het mogelijk een goede veiligheidsaanpak op te stellen, deze uit te voeren en stelselmatig te verbeteren.

Ten aanzien van de stelsels voor gekwalificeerde certificaten en PKIoverheid concludeert de Onderzoeksraad dat bij de betrokken partijen onvoldoende zicht bestaat op de risico's die de betrouwbaarheid van digitale certificaten bedreigen. Geen van hen heeft zich voorafgaand aan het incident bij DigiNotar ingespannen om, denkend in scenario's, te doorgronden op welke manieren de veiligheid van digitale certificaten – en daarmee de beveiliging van het elektronisch gegevensverkeer – in gevaar kon komen. Dit geldt voor de betrokken certificaatdienstverleners, OPTA als toezichthouder en Logius als opdrachtgever binnen PKIoverheid. Evenzeer geldt dit voor de minister van Binnenlandse Zaken en Koninkrijksrelaties als stelselverantwoordelijke voor PKIoverheid en de minister van Economische Zaken, Landbouw en Innovatie als stelselverantwoordelijke voor de gekwalificeerde certificaten. Voor zover partijen nadenken over de risico's, betreft dit hoofdzakelijk hun eigen bedrijfsvoering.

Wat betreft de veiligheid van PKIoverheid-certificaten merkt de Onderzoeksraad op dat in het bijzonder Logius zich niet bewust lijkt te zijn van het feit dat hij als contractpartij/opdrachtgever een essentiële rol heeft. PKIoverheid beoogt zeer veilige certificaten uit te geven, veiliger dan de andere certificaten. Deze doelstelling brengt een vergaande verantwoordelijkheid met zich mee. Het is de kerntaak van Logius ervoor te zorgen dat het vertrouwen dat de Staat der Nederlanden stelt in de certificaatdienstverleners die PKIoverheid-certificaten uitgeven, gerechtvaardigd is.

Het veiligheidsmanagement van Logius zou zich dan ook naar deze organisatiedoelstelling moeten richten, en systematisch moeten verkennen welke de scenario's zijn waardoor deze doelstelling in gevaar kan komen. Vervolgens kan op basis daarvan worden besloten of en door toepassing van welke beheersmaatregelen die risico's voorkomen kunnen worden, of hoe de gevolgen ervan kunnen worden beperkt.

5.6.2 Veiligheidsaanpak niet integraal en deels onrealistisch

De Onderzoeksraad concludeert dat geen sprake is van een aantoonbare, samenhangende aanpak die de veiligheid van digitale certificaten – en daarmee veilig elektronisch gegevensverkeer met overheidsorganisaties – door toepassing van realistische maatregelen beheerst. Dit hangt samen met de hierboven geconstateerde versnippering, waarin partijen zich vooral richten op hun eigen organisatieprocessen. Het systeem als geheel werd te weinig in ogenschouw genomen.

Door het ontbreken van een integraal perspectief bleken geen realistische beheersmaatregelen te bestaan voor de situatie dat een certificaatdienstverlener gecompromitteerd raakt. Voorzien was om in dit geval het vertrouwen in de certificaatdienstverlener op te zeggen, waardoor al diens certificaten onbruikbaar zouden worden. Ook de softwarefabrikanten hadden deze oplossing voorzien. Echter, men had zich niet gerealiseerd dat deze maatregel – mede door het in de loop der jaren sterk toegenomen gebruik van certificaten – maatschappelijk ernstige gevolgen zou kunnen hebben. In het bijzonder lijkt geen van de betrokken partijen zich te hebben gerealiseerd dat de verschillende certificatenstelsels hecht verweven zijn doordat gekwalificeerde, standaard- en PKIoverheid-certificaten door één en dezelfde certificaatdienstverlener verstrekt kunnen worden. Dit heeft gevolgen voor de beheersbaarheid van ongewenste gebeurtenissen. De uitval van een certificaatdienstverlener bleek te kunnen leiden tot grote economische schade en maatschappelijke ontwrichting.

Een ander aandachtspunt in de veiligheidsaanpak bij PKIoverheid is dat de inspanningen van de stelselpartijen er te eenzijdig gericht op waren te voorkomen dat een certificaatdienstverlener gecompromitteerd raakt. Er lijkt niet werkelijk rekening te zijn gehouden met de onvermijdelijke situatie dat het toch mis kan gaan. In de wedloop tussen hackers en de organisaties die hun doelwit vormen is altijd de kans aanwezig dat de hacker erin slaagt om de getroffen beveiligingsmaatregelen, hoe goed ook, te omzeilen. Hier houdt een realistische veiligheidsaanpak rekening mee.

5.6.3 Handhaven veiligheidsaanpak nauwelijks geborgd

Voor effectief veiligheidsmanagement moet worden toegezien op de uitvoering dan wel naleving van de veiligheidsaanpak. De Onderzoeksraad heeft niet uitputtend onderzocht of en hoe certificaatdienstverleners en overheidsorganisaties die gebruik maken van digitale certificaten vorm geven aan hun eigen verantwoordelijkheid om erop toe te zien dat de veiligheidsaanpak die zij hebben geformuleerd, ook wordt nageleefd. De conclusies in deze paragraaf spitsen zich toe op het functioneren van toezicht door andere partijen op naleving van de veiligheidsaanpak.

Ten aanzien van PKIoverheid-certificaten concludeert de Onderzoeksraad dat het stelsel van afspraken weliswaar voorziet in toezicht door drie partijen – de auditerende instelling, OPTA voor de gekwalificeerde certificaten en Logius voor de PKIoverheid-certificaten – maar dat in de praktijk slechts één van die partijen, de auditerende instelling, daadwerkelijk de bedrijfsvoering van de certificaatdienstverlener onderzoekt. In feite zijn de functionarissen in het audit-team van de auditerende instelling de enigen die zich periodiek actief verdiepen in de bedrijfsuitvoering van de certificaatdienstverlener.[80] Dit onderzoek heeft bovendien een andersoortige waarde dan Logius en OPTA eraan toekennen; de managementsysteemaudit verifieert of een certificaatdienstverlener de gewenste professionaliteit heeft en controleert of het managementsysteem gericht is op de vigerende regels. De auditor toetst niet uitputtend of de certificaatdienstverlener alle regels voor certificaatdienstverlening feitelijk naleeft.

80 In het geval certificaatdienstverleners ook penetratietesten laten uitvoeren is er nog een extern bedrijf bij betrokken.

Toch speelt de TTP.NL-verklaring een allesbepalende rol in de toelating tot het stelsel PKIoverheid, alsook in het verkrijgen van een registratie bij OPTA. Op een deel van de veiligheidsaanpak wordt zo überhaupt geen toezicht gehouden. Dit leidt tot de conclusie dat noch OPTA, noch Logius in de praktijk zicht hebben op de vraag of de bedrijfsvoering van de certificaatdienstverlener daadwerkelijk aan de door hen gestelde eisen voldoet.

Daarbij is de Onderzoekraad van oordeel dat Logius een te bescheiden opvatting van zijn eigen rol heeft. Het agentschap is geen toezichthouder, in tweede noch derde linie. Zijn rol vloeit voort uit de toelatingsovereenkomst. Zijn status als contractpartij geeft Logius, naar het oordeel van de Onderzoeksraad, een sterke positie om ervoor te zorgen dat partijen de regels kennen en er actief op toe te zien dat partijen de regels naleven, temeer gezien het belang dat de rijksoverheid toekent aan deze certificaten voor de beveiliging van elektronisch gegevensverkeer. Dit eerste doet zij door middel van het uitdragen van het Programma van Eisen PKIoverheid. Het tweede doet zij slechts reactief, gebaseerd op auditverklaringen en signalen van anderen. De Onderzoeksraad is van oordeel dat, blijkens de wijze waarop het toezicht door Logius is ingericht en de eigen kwalificatie van derdelijns toezichthouder, Logius zich onvoldoende bewust is geweest van zijn rol als opdrachtgever. Logius heeft door zich bij het toezicht op de certificaatdienstverleners primair te verlaten op de auditverklaringen, een toezichtsinstrument gebruikt dat in relatie tot het belang dat de rijksoverheid hecht aan PKIoverheid onvoldoende waarborgen biedt dat de certificaatdienst-verlener daadwerkelijk voldoet aan de op hem van toepassing zijnde vereisten.

Iets vergelijkbaars geldt voor OPTA. De Onderzoeksraad constateert dat het overheidstoezicht door OPTA op geregistreerde certificaatdienstverleners geen toezicht op daadwerkelijke naleving van wettelijke bepalingen omvat. Het overheidstoezicht is zo vormgegeven dat het zelfregulering afdwingt, maar het voegt daaraan zelf weinig toe. De Onderzoeksraad is van oordeel dat de wetgever de toezichtrol van OPTA ten onrechte heeft gemarginaliseerd.

Wanneer de wetgever het noodzakelijk acht de markt voor certificaatdienstverlening gedeeltelijk te reguleren, moeten eindgebruikers van gekwalificeerde certificaten er immers op kunnen rekenen dat de rijksoverheid er zicht op heeft of de leverancier van een gekwalificeerd certificaat de regels werkelijk nakomt.

5.6.4 Leren en verbeteren niet geborgd

De bestaande meldplicht voor certificaatdienstverleners laat in alle gevallen ruimte voor een eigen afweging over hetgeen hij wel of niet meldt. Hierdoor komen niet alle incidenten naar buiten, waardoor deze ook niet kunnen worden aangegrepen om het stelsel te verbeteren.

De Onderzoekraad acht melden van incidenten een belangrijk onderdeel om een veilig functioneren van de certificaatdienstverlening te waarborgen. Van de andere partijen in het stelsel vergt dit dat zij op hun beurt zorgvuldig met een melding omgaan en deze in de eerste plaats aangrijpen om gezamenlijk een oplossing te zoeken waardoor de negatieve gevolgen van een incident zo beperkt mogelijk blijven. Vanzelfsprekend doet dit laatste niet af aan het feit dat na melding kan blijken dat er redenen zijn voor toezichthouder of opdrachtgever zijn, handhavend op te treden.

5.6.5 Risico's eindgebruiker blijven buiten beeld

De veiligheid van digitale certificaten is niet alleen afhankelijk van de certificaatdienstverlener. Ook de wijze waarop certificaathouders (de afzonderlijke overheidsorganisaties) deze toepassen, speelt een belangrijke rol. Zo heeft het incident bij DigiNotar bijvoorbeeld laten zien dat de snelheid waarmee houders van certificaten in staat zijn om hun certificaten voor andere om te wisselen, bepalend is voor het herstellend vermogen van een PKI wanneer een certificaatdienstverlener gecompromitteerd raakt.

Van houders van certificaten mag dan ook worden verwacht dat zij zich voorbereiden op de situatie dat een certificaatdienstverlener niet meer te vertrouwen is. Dan moeten zij, vanuit hun verantwoordelijkheid voor digitale veiligheid, een oplossing voorhanden hebben. Deze oplossing moet zich enerzijds richten op een zo snel mogelijk herstel van de beveiliging van het elektronisch gegevensverkeer, en anderzijds op het bieden van een oplossing aan de burgers of bedrijven wier belangen getroffen zijn.

Binnen dit krachtenveld is inzicht in de risico's van het gebruik van certificaten in eerste instantie een verantwoordelijkheid van de betrokken overheidsorganisatie. Ofschoon de Onderzoeksraad dit niet uitputtend heeft onderzocht, komt uit het onderzoek het beeld naar voren dat overheidsorganisaties dit inzicht niet hebben, en zich ook niet in staat achten het te verwerven. Zij leveren zich als 'klant' in feite over aan de certificaatdienstverlener en voelen zich niet in staat om te verifiëren of diens werkelijke betrouwbaarheid hun vertrouwen rechtvaardigt. Zelfreguleringstrajecten zoals WebTrust en TTP.NL bieden onvoldoende waarborgen om dit te compenseren.

Geen van de in dit onderzoek betrokken partijen lijkt zich momenteel verantwoordelijk te voelen voor dit aspect van digitale certificaten. De Onderzoeksraad ziet hier een taak voor de minister van Binnenlandse Zaken en Koninkrijksrelaties, die naar het oordeel van de Onderzoeksraad een stelselverantwoordelijkheid heeft om de voorwaarden te scheppen waaronder afzonderlijke overheidsorganisaties (op rijks- en lokaal niveau) in staat zijn om optimaal invulling te geven aan hun eigen verantwoordelijkheid voor digitale veiligheid.

6 VERKENNING: DIGITALE VEILIGHEID BIJ OVERHEIDSORGANISATIES

In de vorige twee hoofdstukken stond centraal hoe de betrouwbaarheid van digitale certificaten en certificaatdienstverlening wordt gewaarborgd. Digitale certificaten vormen een belangrijk instrument in het waarborgen van digitale veiligheid: voorkomen dat (persoons)gegevens van burgers en bedrijven gecompromitteerd raken doordat onbevoegden er kennis van kunnen nemen, ze manipuleren of ze misbruiken.

Dit hoofdstuk verkent hoe overheidsorganisaties omgaan met deze digitale veiligheid in bredere zin. Hoe brengen zij bedreigingen van digitale veiligheid in kaart, hoe kiezen en implementeren zij beheersmaatregelen die aan deze bedreigingen het hoofd bieden, hoe bereiden zij zich voor op incidenten en geven zij op ambtelijk en bestuurlijk niveau sturing aan het digitale veiligheidsbeleid?

Om hierin inzicht te verkrijgen heeft de Onderzoeksraad een verkennend onderzoek uitgevoerd. Deze verkenning is uitgevoerd bij de Sociale Verzekeringsbank (SVB), de Belastingdienst en bij een aantal gemeenten. Daarnaast zijn gesprekken gevoerd met een aantal banken over hoe zij als private partij digitale veiligheid borgen. Relevante inzichten uit deze gesprekken zijn in kaders weergegeven. De Onderzoeksraad benadrukt dat de in deze verkenning betrokken organisaties niet zijn geselecteerd op grond van enig vermoeden dat zij onvoldoende invulling geven aan hun verantwoordelijkheid voor informatieveiligheid. Meer informatie over de selectie van organisaties is opgenomen in de onderzoeksverantwoording.

De verkenning geeft een beeld van de mate waarin de onderzochte organisaties op bestuurlijk niveau de risico's voor digitale veiligheid onderkennen en welke maatregelen zij treffen ter voorkoming en beheersing van ongewenste gebeurtenissen op dit terrein.

6.1 Ontwikkeling e-dienstverlening door de overheid

De elektronische dienstverlening van overheidsorganisaties (e-dienstverlening) heeft het laatste decennium een snelle ontwikkeling doorgemaakt.[81] Steeds meer overheidsproducten en -diensten zijn via het internet beschikbaar. Aan de basis hiervan staat het rapport *Publieke dienstverlening, professionele gemeenten*, waarin de visie wordt geformuleerd dat de gemeente in 2015 hét loket van de overheid moet zijn.[82] Aan deze visie werd aanvankelijk uitvoering gegeven in het *Nationaal Uitvoeringsprogramma dienstverlening en e-overheid* (NUP). Voor partijen in de werk en inkomen keten was vooral het rapport *De burger bediend* de basis van veranderingen.[83]

Een belangrijk onderdeel van het NUP was de ontwikkeling van generieke bouwstenen voor e-dienstverlening, alsmede een aantal landelijke voorzieningen, waaronder DigiD.[84] In de opvolger van het NUP, de *Overheidsbrede implementatieagenda voor dienstverlening en e-overheid* (i-NUP), staat implementatie van deze bouwstenen centraal.[85] Onderdeel van het i-NUP is onder meer de beleidsafspraak dat DigiD dé authenticatievoorziening is waarmee burgers toegang krijgen tot e-dienstverlening door de overheid (zie kader).

81 Ook eerder zijn al aanzetten gegeven tot een verbetering van de dienstverlening door de overheid met behulp van ICT, bijvoorbeeld in het programma *Andere Overheid* (zie kamerstuk TK 29362-1, 2003).
82 VNG (2005). Publieke dienstverlening, professionele gemeenten – Visie 2015. Eindrapport Commissie Gemeentelijke Dienstverlening.
83 Expertcommissie informatievoorziening en elektronische dienstverlening SUWI (2005). De burger bediend. Rapport in opdracht van de minister van Sociale Zaken en Werkgelegenheid. Kamerstuk TK 26448-206.
84 Zie kamerstuk TK 29362-148, 2009.
85 Zie kamerstuk TK 26643-182, 2011.

Wat is DigiD?
DigiD is de centrale digitale authenticatievoorziening voor communicatie door burgers met de overheid en andere publieke dienstverleners. Burgers hoeven dankzij DigiD niet voor elke overheidsorganisatie aparte wachtwoorden en inlogcodes te gebruiken. DigiD is tot stand gekomen op initiatief van de Manifestgroep, een samenwerkingsverband tussen verschillende zelfstandige bestuursorganen. Logius beheert DigiD.

Verschillende overheidsorganisaties gebruiken DigiD in hun e-dienstverlening. Voorbeelden zijn de Belastingdienst die het gebruikt bij de jaarlijkse belastingaangifte en de Dienst Uitvoering Onderwijs (DUO) die DigiD gebruikt om studenten wijzigingen door te laten geven. Gemeenten gebruiken het om burgers online producten en diensten aan te laten vragen.

DigiD kent drie zekerheidsniveaus: basis, midden en hoog. Voor authenticatie op basisniveau identificeert de gebruiker van DigiD zich met zijn gebruikersnaam en wachtwoord. Voor authenticatie op middenniveau wordt hieraan een transactiecode toegevoegd, die verzonden wordt per sms. Zekerheidsniveau hoog is nog niet beschikbaar. Op dat niveau maakt de burger gebruik van een elektronische identiteitskaart met daarop een smartcard voor de authenticatie. Ook is gemachtigd gebruik van DigiD door derden mogelijk, zodat bijvoorbeeld een belastingconsulent namens een ander aangifte kan doen.

De gegevensuitwisseling die ten behoeve van authenticatie met DigiD plaats vindt, wordt beveiligd door PKIoverheid-certificaten.

Een randvoorwaarde voor e-dienstverlening is dat burgers er vertrouwen in hebben dat overheidsorganisaties de gegevensuitwisseling goed beveiligen. Een vermindering van het vertrouwen van burgers kan leiden tot een verminderde bereidheid gebruik te maken van e-dienstverlening. Daarnaast kan een tanend vertrouwen in de overheid op het gebied van e-dienstverlening leiden tot een afnemend vertrouwen in de overheid in het algemeen.

6.2 Digitale veiligheid bij de SVB en De Belastingdienst

Deze paragraaf schetst een beeld op hoofdlijnen van digitale veiligheid in relatie tot e-dienstverlening bij de Sociale Verzekeringsbank (SVB) en de Belastingdienst.

6.2.1 De SVB en Belastingdienst

De SVB is een zelfstandig bestuursorgaan en voert, op grond van de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI), de volksverzekeringen voor ruim 5 miljoen burgers uit, waaronder de AOW-uitkeringen.[86] De SVB doet dit in opdracht van het Ministerie van Sociale Zaken en Werkgelegenheid. De SVB voert daarnaast ook andere regelingen uit in opdracht van andere ministeries en organisaties.[87]

De primaire processen van de SVB bestaan uit beschikken en vaststellen van rechten van aanvragers van uitkeringen en/of toeslagen, en het doen van betalingen. Het online indienen van een aanvraag voor een van de uitkeringen of toeslagen door burgers vindt plaats via DigiD. De SVB betrekt gegevens uit bestaande authentieke bronnen, waaronder registraties die worden beheerd door andere instanties in en buiten de keten werk en inkomen, zoals de gemeentelijke basisadministratie. Verificatie van opgaves en mutaties door burgers vinden altijd plaats bij deze authentieke bronnen.

86 Naast de AOW, ook de nabestaandenuitkering Anw, Kinderbijslag, TOG Onderhoud gehandicapt kind, persoonsgebonden budget PGB, internationale detachering, AIO aanvulling en mantelzorgcomplement.
87 De niet-sociale verzekeringswetten en andere regelingen zijn onder andere de Asbestregeling, Regeling Bijstand Buitenland en het Pensioenregister. Andere opdrachtgevers zijn bijvoorbeeld het ministerie van Volksgezondheid, Welzijn en Sport, gemeenten, het UWV en het College voor Zorgverzekeringen (CvZ). Zie verder www.svb.nl

De gegevensuitwisseling met deze instanties verloopt volledig geautomatiseerd via een infrastructuur, Suwinet geheten, die wordt gereguleerd door de Wet SUWI.[88] Digitale verificatie van gegevens met behulp van de Suwinet-inkijkfunctie vindt alleen (aanvullend) plaats in uitzonderingssituaties, bijvoorbeeld als de SVB de gegevens niet rechtstreeks kan krijgen, of als de juistheid van de gegevens aangevochten wordt door een cliënt.

De Belastingdienst is onderdeel van het ministerie van Financiën, en is onder meer verantwoordelijk voor het innen van rijksbelastingen en premies, waaronder de loonbelasting. Daarnaast verstrekt de Belastingdienst enkele toeslagen en houdt hij toezicht op in- en uitgaande goederenstromen. Jaarlijks verwerkt de Belastingdienst de verschillende aangiften van ca. 6 miljoen particulieren en 1,1 miljoen ondernemers.

De primaire bedrijfsprocessen van de Belastingdienst bestaan op hoofdlijnen uit het verzamelen en verwerken van gegevens, en het doen ontvangen en doen uitkeren van betalingen. Ook de Belastingdienst wisselt op grote schaal digitaal gegevens uit met derden, zowel publieke als private partijen. Digitale gegevensuitwisseling tussen burgers en de Belastingdienst verloopt met behulp van DigiD.

6.2.2 Bestuurlijke inbedding digitaal veiligheidsbeleid bij SVB en Belastingdienst

Het informatiebeveiligingsbeleid van beide organisaties is gebaseerd op de code voor informatiebeveiliging (ISO 27002). Digitale veiligheid maakt onderdeel uit van dit beleid en is nauw verbonden met de bedrijfsdoelstellingen van de diensten. De Belastingdienst baseert zijn informatieveiligheidsbeleid bovendien op het Voorschrift Informatiebeveiliging Rijksdienst (VIR). Door toepassing van deze documenten volgt het informatiebeveiligingsbeleid van beide organisaties in grote lijnen de principes die de Onderzoeksraad ook in zijn beoordelingskader hanteert (zie hoofdstuk 3).

De SVB laat toepassing van de code in het eigen informatiebeveiligingsbeleid toetsen door middel van een EDP-audit door de eigen interne accountantsdienst.[89] Krachtens de Wet SUWI worden tevens eisen gesteld aan het informatiebeveiligingsbeleid van instellingen in de keten werk en inkomen. De Wet kent een streng regime van verantwoording, en voorziet in toezicht en handhaving door de Inspectie Werk en Inkomen (IWI) via een jaarlijkse review. Op grond van de Wet SUWI moet de SVB jaarlijks mededeling doen van de maatregelen die de continuïteit, de exclusiviteit en de betrouwbaarheid van de dienstverlening waarborgen. IWI beoordeelt deze maatregelen jaarlijks. Bovendien voorziet de Wet in een uitgebreide verslagleggingplicht voor SVB in de planning- en controlcyclus met betrekking tot de kwaliteit van de bedrijfsvoering, waarvan informatiebeveiliging onderdeel is. De verantwoording op ICT-gebied moet geschieden volgens de COBIT-norm, waardoor vergelijking met andere diensten mogelijk is.[90] Daar hoort ook certificering door een (externe) accountantsdienst bij.

Een ongestoorde uitvoering van de primaire processen heeft binnen de SVB de hoogste prioriteit. SVB ziet informatiebeveiliging als een wezenlijk onderdeel van excellente dienstverlening en verbindt dit met zijn missie.[91] Naast de code voor informatiebeveiliging is het informatiebeveiligingsbeleid gebaseerd op het normenkader Suwinet en nationaal en internationaal ontwikkelde richtlijnen voor beveiliging.[92] Het is ingebed in de primaire processen.

88 Deze infrastructuur, doorgaans aangeduid als Suwinet, wordt beheerd door het Bureau Keteninformatisering Werk en Inkomen. Alle partijen die onderdeel uitmaken van de keten werk en inkomen maken gebruik van Suwinet.

89 EDP staat voor *electronic data processing*. Dit type audit wordt ook vaak als IT-audit aangeduid.

90 Control Objectives for Information and related Technology (COBIT) is een standaard die in 1992 ontwikkeld is door het Information Systems Audit and Controls Association (ISACA) en het IT Governance Institute.

91 De missie luidt: De SVB wil een excellente en omgevingsbewuste uitvoerder zijn van persoonsgebonden financiële regelingen van de overheid. Bron: Beleid en organisatie van Informatiebeveiliging SVB, december 2010.

92 Het Suwinet-Normenkader is een set controleregels gebaseerd op Bijlage XIV bij de Regeling SUWI, de Code voor Informatiebeveiliging en de BS7799 / ISO17799.

De Belastingdienst wordt geauditeerd door de Auditdienst Rijk (tot 1 mei de Rijksauditdienst). Naast de wettelijk verplichte controle van de jaarrekening, voert de Auditdienst Rijk ook vraaggestuurde controles uit. Daaronder valt een jaarlijks bepaald auditprogramma voor informatiebeveiliging. Door de toenemende automatisering van de primaire processen schenken de audits van de Belastingdienst steeds meer geïntegreerd aandacht aan de samenhang tussen de controlemaatregelen aan de IT-kant en de gebruikersomgeving. Dit houdt in dat de uit te voeren controlewerkzaamheden in de gebruikersomgeving afhangen van de mate waarin de voortdurende werking van de ingebouwde applicatiecontrols (die in de IT-audits gecontroleerd worden) is gewaarborgd.

Behalve digitale veiligheid krijgen twee andere bedrijfsdoelstellingen, efficiency en klantgerichtheid, bij beide organisaties veel aandacht. Deze ontwikkelingen worden gestuurd door de vraag van de politiek en het publiek. Als gevolg hiervan wordt meer informatie uitgewisseld met cliënten dan vroeger het geval was, en kunnen cliënten in toenemende mate zelf gegevens aanvullen en wijzigen. Een voorbeeld hiervan is de vooringevulde aangifte van de Belastingdienst, waarin informatie van verschillende diensten en ook van banken bij elkaar wordt gevoegd en aan de cliënt wordt gepresenteerd. Een ander voorbeeld is dat in webomgevingen als 'Mijn SVB' de klant steeds meer mogelijkheden heeft mutaties zelf door te voeren. Ook wordt meer informatie uitgewisseld met andere partijen, om de kwaliteit en efficiency van de dienstverlening verder de verbeteren.

Uit de verkenning blijkt dat beide organisaties deze ontwikkelingen ook zien als een mogelijk risico. Het leidt er onder andere toe dat informatie van individuele burgers steeds verder wordt verweven. Tegelijkertijd neemt ook het risico van compromittering van elektronische gegevens van burgers en bedrijven toe, waardoor zij hun vertrouwen in overheidsdienstverlening kunnen verliezen. Dit is een uitdaging voor informatiebeveiliging, maar wordt ook als onontkoombaar ervaren. De Onderzoeksraad constateert dat deze ontwikkeling de wijze waarop beide partijen omgaan met digitale veiligheid sterk beïnvloedt. Beide organisaties zijn zich er scherp van bewust dat het vertrouwen van burgers en ketenpartners in hun informatiebeveiliging van steeds groter belang wordt voor het kunnen realiseren van hun organisatiedoelstellingen. Digitale veiligheid wordt zo een randvoorwaarde voor de continuïteit van de dienstverlening, die per definitie beheerst moet worden. In dat opzicht zijn zij vergelijkbaar met hoe andere transactieverwerkende organisaties als bijvoorbeeld banken het gegevensverkeer met derden beveiligen.

Hoe organiseren en borgen banken digitale veiligheid?
Banken hebben de afgelopen decennia de dienstverlening op grote schaal gedigitaliseerd. Het merendeel van de klanten maakt gebruik van internetbankieren. Dit heeft geleid tot een belangrijke verandering in de bedrijfsvoering: de ICT-intensiteit van banken is steeds groter geworden. Hierdoor hebben zij te maken met nieuwe risico's.

"Bankovervallen" vinden tegenwoordig in toenemende mate plaats op internet, via de computer van de klant. het internetverkeer met klanten wordt daarom intensief gemonitord op aanwijzingen van misbruik. Banken treden soms zelfs in contact met gebruikers als er sterke aanwijzingen zijn dat hun pc wordt misbruikt. Banken werken op dit gebied intensief met elkaar samen, en overleggen in het geval van ernstige criminele fraude ook met politie, justitie en AIVD.

Banken hebben de afgelopen jaren veel geïnvesteerd in de beveiliging van hun ICT-systemen. De meeste banken handelen klantencontacten op één centrale website (portal) af. Als bankfilialen lokale websites onderhouden worden die op een eenduidige en centraal vastgelegde wijze ingericht en onderhouden. Hierdoor wordt het inbraakrisico geminimaliseerd en kunnen snel en centraal wijzigingen worden doorgevoerd als blijkt dat er toch nog veiligheidsrisico's zijn.

Managementbetrokkenheid
Informatiebeveiliging bij banken is eveneens gebaseerd op het principe dat zij de risico's die zij en hun klanten op het internet lopen goed in kaart brengen; het is "core business" geworden. Steeds vaker is informatiebeveiliging daarom dan ook een onderwerp dat direct door de Raad van Bestuur en de Raad van Toezicht wordt behandeld.

Diverse aanvullende authenticatie-toepassingen voor klanten
Banken hebben op grote schaal voorzieningen getroffen om internetbankieren veilig te maken. Daarbij maken ook banken gebruik van digitale certificaten. Vanwege de inherente onveiligheid van het internet gaan banken ervan uit dat fraude en misbruik van persoonlijke gegevens gangbare praktijken zijn. Banken kiezen ervoor klanten via internet eenvoudig en snel toegang te geven tot hun gegevens. Om dit ook zo veilig mogelijk te laten plaatsvinden wordt de identiteit van de klant door een uitgebreide authenticatie vastgesteld. Dit gebeurt door aan de persoon afgegeven codelijsten, e.dentifiers, tokens etc. Met het introduceren van applicaties voor de smartphone wordt het zekerheidsniveau van de authenticatie iets meer losgelaten, maar aan deze applicaties zitten ook meer restricties.

Maatregelen voor herstel van vertrouwen
Net als overheidsorganisaties hechten banken grote waarde aan het vertrouwen dat klanten in hen stellen. Zij gaan ver om dit vertrouwen te behouden en te herstellen indien zich een incident voordoet. In de praktijk betekent dit vaak dat banken hun klanten bij de meeste vormen van fraude schadeloos stellen, behalve als de klant zelf aantoonbaar nalatig geweest is.

Van de overheid verwacht de burger dat hij er alles aan doet om de communicatie met burgers veilig te laten verlopen. Maar net als de banken is ook de overheid niet in staat volledige garantie te bieden dat deze communicatie niet verstoord raakt door een hack of een vorm van fraude. Een belangrijk verschil met de banken is dat de overheid tot dusver niet of nauwelijks aandacht besteedt aan de vraag waar gedupeerden van bijvoorbeeld identiteitsfraude terecht kunnen.

De SVB en de Belastingdienst monitoren doorlopend hun digitale gegevensverkeer. Hoewel de omvang van dat verkeer toeneemt – en daarmee het risico op verlies van gegevens of foutieve verwerking – neemt zo ook de kans toe op het vroegtijdig ontdekken van zulke gebeurtenissen. Zo kunnen tijdig passende maatregelen genomen worden om schade voor de organisatie of de betrokkene te beperken.

De Onderzoeksraad constateert dat digitale veiligheid zodanig onderdeel is van het primaire proces van de SVB en de Belastingdienst, dat de continuïteit van de dienstverlening er nauw mee is verbonden. De strakke wettelijke kaders, de eisen van de toezichthouders en het openbare verantwoordingsprotocol dat ook de niet-financiële informatie betreft, waar beide organisaties aan onderworpen zijn, versterken deze ontwikkeling. Het digitaal uitwisselen en verwerken van gegevens is niet meer weg te denken uit de primaire processen van beide organisaties. Digitale veiligheid is daarmee randvoorwaardelijk voor het invullen en behalen van de bedrijfsdoelstellingen. Dit laatste acht de Onderzoeksraad van groot belang, omdat daarmee vanuit de bedrijfsdoelstellingen inhoud wordt gegeven aan het werken volgens de principes van veiligheidsmanagement.

Kennen en beheersen van risico's
Beide organisaties inventariseren de risico's van hun eigen bedrijfsprocessen, waaronder de risico's voor digitale veiligheid. Zij beoordelen de risico's en nemen maatregelen om de risico's te verminderen. Geïnterviewden tot op het hoogste managementniveau gaven aan goed op de hoogte te zijn van en betrokken te zijn bij digitale veiligheid in relatie tot de continuïteit van de bedrijfsprocessen.

De SVB is voor zijn kernprocessen sterk afhankelijk van gegevens uit andere registraties, waaronder de Gemeentelijke basisadministratie persoonsgegevens (GBA). De SVB betrekt zoveel mogelijk gegevens uit authentieke bronnen, vult deze alvast in de aanvraag in (voorinvulling) en gebruikt deze gegevens rechtstreeks in de primaire processen. Hij kan deze zelf niet wijzigen, en moet er vanuit gaan dat deze gegevens juist zijn. Wanneer een aanvraag wordt gedaan, vindt digitale verificatie via Suwinet-inkijk alleen (aanvullend) plaats in uitzonderingssituaties, bijvoorbeeld als de gegevens niet rechtstreeks verkregen kunnen worden of als die gegevens aangevochten worden door de cliënt. Mocht Suwinet niet beschikbaar zijn, of aan de betrouwbaarheid van de getoonde gegevens worden getwijfeld, dan wordt informatie via andere kanalen (telefoon of post) of op een later moment geverifieerd.

De SVB registreert en muteert zelf, op verzoek van de cliënt, slechts één fraudegevoelig persoonsgegeven: het rekeningnummer waarop uitbetaling plaatsvindt. De burger kan via DigiD zelf dit gegeven digitaal wijzigen via een vooringevuld formulier. Dit is een gevoelig proces en het wijzigen van dit gegeven is daarom omgeven met vele inhoudelijke controles. De SVB wil voorkomen dat bijvoorbeeld het wijzigen van het bankrekeningnummer door onbevoegd gebruik (bijvoorbeeld een familielid) of misbruik (fraude door anderen) van diens DigiD-code door de cliënt onopgemerkt blijft. Sluitstuk van de flankerende maatregelen is dat de cliënt per post van een wijziging van het rekeningnummer op de hoogte wordt gesteld, op het laatst bekende GBA-adres. De SVB vertrouwt erop dat de cliënt bij een onjuiste mutatie zelf contact opneemt, omdat de cliënt zelf er direct belang bij heeft dat geen onjuist rekeningnummer bij SVB bekend is.

De SVB kan langs verschillende kanalen met zijn cliënten communiceren. Hoewel de SVB om redenen van efficiency communicatie via internet stimuleert, kunnen zij ook gebruik maken van telefoon of post, of een bezoek brengen aan een regiokantoor. Deze zogeheten multikanaalbenadering is primair ingericht om diverse doelgroepen te bedienen, maar functioneert ook als risicobeheersmaatregel. Als een van de kanalen uitvalt, zijn er genoeg alternatieven voor de cliënt om ervoor te zorgen dat de dienstverlening beschikbaar blijft.

De Raad van Bestuur geeft aan nauw betrokken te zijn bij de aansturing en uitvoering van het informatiebeveiligingsbeleid. Hij stelt het informatiebeveiligingsbeleid vast en voert de regie ervan door onder andere het Management Forum Informatiebeveiliging voor te zitten.[93] De Raad van Bestuur legt daarover in het jaarverslag verantwoording af en stelt op dit onderwerp 'in control' te zijn. Door informatiebeveiliging een integraal onderdeel van de bedrijfsvoering van de SVB te maken kunnen de verantwoordelijkheden daarvoor op alle (management-)niveaus binnen de organisatie belegd worden. Daardoor kan het management voortdurend op de hoogte en betrokken zijn bij het onderwerp.

Ook de Belastingdienst maakt op grote schaal gebruik van gegevens die worden verstrekt door derden. De gegevens afkomstig uit de GBA beschouwt de Belastingdienst als authentiek, conform de GBA-wet. De Belastingdienst treft eveneens zeer vele inhoudelijke controles en andere flankerende maatregelen bij het muteren van bankrekeningnummers waarop toeslagen en teruggaven worden uitgekeerd. Voor burgers kent de Belastingdienst net als de SVB verschillende communicatiekanalen, maar stimuleert de elektronische aangifte uit efficiency-overwegingen.

De Belastingdienst heeft een bedrijfsonderdeel dat zich richt op ontwikkeling en beheer van applicaties, maar werkt voor onderhoud en beheer aan ICT-systemen ook veel samen met externe partijen. Het DigiNotarincident en de gevolgen hiervan hebben de organisatie bewuster gemaakt van zijn afhankelijkheid van kennis van externe leveranciers. In de gevoerde gesprekken gaf men aan soms over te weinig eigen expertise te beschikken, omdat werknemers met inhoudelijke expertise veelal snel uitstromen naar de private sector.

De Belastingdienst ziet een vertrouwenscrisis als het grootste risico. De organisatie heeft in het verleden te kampen gehad met enkele incidenten die hebben geleid tot aanzienlijke imagoschade, zoals de aanloopproblemen bij het uitkeren van toeslagen. Het vertrouwen van het publiek in de dienst bleek moeilijker te herstellen dan de gemaakte fouten in de ICT-systemen of processen. De Belastingdienst geeft hierbij aan dat hoe minder een vertrouwenscrisis bij derden optreedt en hoe beperkter de gevolgen ervan kunnen worden gehouden, hoe beter de crisis beheerst kan worden.

De Belastingdienst ziet, net als de SVB, het waarborgen van digitale veiligheid en het beheersen van risico's die de informatieveiligheid bedreigen in de eerste plaats als een verantwoordelijkheid van het management en medewerkers van de 'uitvoering' (de primaire bedrijfsprocessen). Hiertoe moet het risicobewustzijn verankerd zijn in de organisatiecultuur.

93 Het Forum Informatiebeveiliging vergadert eenmaal per kwartaal en bestaat uit de Informatiebeveiligings-Domeindirecteuren, het lid Raad van Bestuur met portefeuille Dienstverlening en ICT, de Chief Information Security Officer, het hoofd EDP Audit en een directeur van een vestiging.

De organisatie onderkent eveneens de noodzaak van monitoring en registratie van verschillende parameters in de uitvoerende processen die informatie geven over de mate van digitale veiligheid, zodat de risicobeheersing daarop kan worden aangepast. Ook voor banken is risicobeheersing de basis voor digitale veiligheid (zie onderstaand kader).

Inzicht in risico's als basis voor digitale veiligheid
Ook banken werden verrast door wat er bij DigiNotar gebeurde. Niemand had rekening gehouden met dit scenario. De meeste banken hebben naar aanleiding van het incident de afspraken met hun certificaatdienstverlener nog een keer tegen het licht gehouden en een back-up voor de certificaten georganiseerd.

Ook voor banken is het de vraag in hoeverre het mogelijk was om voorbereid te zijn op een dergelijk incident. Geïnterviewden geven aan dat risicomanagement de sleutel is en dat digitale veiligheid meer is dan het gebruik van digitale certificaten. Het gaat om het geheel aan maatregelen: welke beveiligingsmaatregelen worden aan de voorkant getroffen, hoe wordt gecontroleerd of een gebruiker daadwerkelijk een klant is die gerechtigd is transacties te doen (authenticatie), hoe worden transacties gemonitord, wat wordt er gedaan met onregelmatigheden, wie houdt waarop toezicht en wat leert de organisatie van incidenten.

Net als bij de SVB, heeft de Onderzoeksraad de indruk gekregen dat de Belastingdienst de implementatie en naleving van het informatiebeveiligingsbeleid hoog op de bestuurlijke agenda heeft staan. Geïnterviewden bij beide organisaties zien in dat een belangrijk deel van het succes van informatiebeveiliging en digitale veiligheid is belegd in het gedrag van medewerkers. Uit de gesprekken bij de SVB lijken medewerkers zich bewust te zijn van de risico's van digitale gegevensuitwisseling met cliënten buiten de daarvoor goedgekeurde mogelijkheden. Sommige geïnterviewden gaven aan dat dit risicobewustzijn 'in de genen' van de organisatie zit.

Geïnterviewden bij de Belastingdienst geven aan dat medewerkers wel overtuigd zijn van het belang van informatiebeveiliging, maar dat zij zich niet altijd bewust lijken te zijn van gedragingen die de digitale veiligheid kunnen ondergraven, zoals ondoordacht gebruik van e-mail of gegevensdragers. Daarnaast lijken afdelingen vooral gericht op het eigen procesonderdeel en daarmee minder bewust van het feit dat hun handelen gevolgen kan hebben voor de digitale veiligheid van andere proces-onderdelen. Tenslotte wordt het veelvuldig gebruik van tijdelijke krachten ook door de Belastingdienst zelf gezien als aandachtspunt. Het vergt blijvende aandacht van het management en de eigen werknemers om ervoor te zorgen dat ook de tijdelijke krachten zich bewust zijn van het belang van digitale veiligheid en het daarvoor geldende beleid en de gedragsregels naleven. Door verschillende voorlichtingsactiviteiten, zoals het plaatsen van berichten over beveiliging op de Beeldkrant en gerichte awarenessprogramma's, wordt hieraan bij de Belastingdienst aandacht besteed.

De SVB geeft aan schriftelijke afspraken te maken met aanleverende partijen over de informatiebeveiliging en de privacy. De Belastingdienst stelt eveneens eisen aan de wijze waarop gegevens door de voorgaande schakel in de keten worden aangeleverd (bijvoorbeeld van gemeenten of intermediairs), maar diepgaande controles in hoeverre deze aangeleverde gegevens authentiek zijn vinden niet plaats. De risico's voor de eigen processen en continuïteit van de dienstverlening, die voortkomen uit de handelwijze en de producten van de voorgaande schakel, zijn naar wat de Onderzoeksraad er van heeft gezien, bij de SVB meer in beeld dan bij de Belastingdienst. Dat is begrijpelijk gezien het grote aantal (private) partijen waar de Belastingdienst via e-dienstverlening digitaal mee communiceert.

De Onderzoeksraad constateert dat zowel de SVB als de Belastingdienst onderdeel zijn van een complexe keten, waarin veel en intensief gegevens tussen instanties worden uitgewisseld die daardoor een sterke onderlinge afhankelijkheid kennen. Deze ketenafhankelijkheid brengt risico's met zich mee die de afzonderlijke ketenpartijen niet kunnen beheersen, en waarvoor samenwerking of een sterke ketenregisseur noodzakelijk is. De SVB en de Belastingdienst maken met hun ketenpartners weliswaar afspraken over de wijze waarop gegevens worden aangeleverd, maar moeten zich begrijpelijkerwijs verlaten op de juistheid van hetgeen zij aangeleverd krijgen.

Zij kunnen de digitale veiligheid van de processen die hun 'schakel' in de keten vormen, zo goed mogelijk beheersen, maar blijven afhankelijk van de mate waarin de andere schakels op hun beurt digitale veiligheid waarborgen.

6.2.3 Gevolgen van het DigiNotarincident bij de SVB en de Belastingdienst

Deze paragraaf beschrijft de impact van het DigiNotarincident op beide organisaties en welke lessen zij daaruit getrokken hebben voor hun eigen rol in het waarborgen van de digitale veiligheid.

De gevolgen voor de SVB van het onbetrouwbaar worden van de door DigiNotar uitgegeven certificaten waren minimaal. Al snel bleek dat de organisatie zelf zo goed als geen gebruik hiervan maakte. Wel maakte men zich zorgen over een mogelijke uitval van de verbinding met Suwinet. Hierdoor zouden medewerkers van de SVB niet meer de gegevens van aanvragers, indien noodzakelijk, digitaal kunnen controleren, en moeten terugvallen op andere kanalen of op controle achteraf. Uiteindelijk bleken dergelijke maatregelen niet nodig, omdat de verbinding van de SVB met Suwinet ongestoord en veilig bleef functioneren.

Een ander punt van zorg was het mogelijk verlies van vertrouwen van burgers in DigiD. Heel belangrijk voor de SVB en voor het functioneren van digitale gegevensuitwisseling is het vertrouwen van de klant in de betrouwbaarheid van DigiD. Maar ondanks mediaberichten over onveiligheid van DigiD, heeft de SVB zelf op basis van het inlogverkeer met burgers vastgesteld dat dit vertrouwen niet of nauwelijks aangetast was. De SVB constateerde geen significante vermindering van het inloggen met DigiD door cliënten bij de SVB toen het incident in de publiciteit kwam.

Voor de Belastingdienst had de inbraak bij DigiNotar veel grotere gevolgen. Na bekendwording van het incident werd een crisisteam ingericht op het niveau van de Belastingdienst en op het niveau van de Rijksoverheid. In het crisisteam van de Belastingdienst waren zowel mensen op politiek niveau als op uitvoeringsniveau vertegenwoordigd. Het uitvoeringsniveau was leidend. Volgens betrokkenen was dit laatste één van de succesfactoren van het managen van het DigiNotarincident.

De Belastingdienst maakte op grote schaal gebruik van door DigiNotar uitgegeven BAPI-certificaten. Deze bleken moeilijk te vervangen, omdat zij 'ingebouwd' waren in de applicaties die de Belastingdienst gebruikt. Om die redenen was de vervanging van de certificaten veel complexer en tijdrovender dan gedacht. De Belastingdienst heeft niet alleen in de eigen organisatie maatregelen genomen, maar wist ook externe partijen ertoe te bewegen maatregelen te nemen om digitale communicatie met bedrijven en andere partijen te laten doorgaan. Door het stilvallen van de dagelijkse gegevensuitwisseling met derden en de goederenstroom bij de douane dreigde het economisch verkeer te worden aangetast met ernstige daadwerkelijke economische schade tot gevolg. Dit heeft zich uiteindelijk niet voorgedaan.

Lessons learned door de SVB en de Belastingdienst

Geïnterviewden van beide organisaties hebben aangegeven welke lessen zij hebben geleerd uit het DigiNotarincident. Deze worden hieronder op hoofdlijnen weergegeven.

De inbraak bij DigiNotar heeft beide organisaties bewust gemaakt van hun afhankelijkheid van externe partijen, zoals één enkele leverancier van digitale certificaten. Ook is geconstateerd dat overheidsorganisaties in algemene zin erg afhankelijk zijn van externe ICT-kennis. Dit wordt door de betrokkenen gezien als een groot risico. Mensen met deze kennis die zich intern ontwikkelen worden 'weggekocht'. Dit geldt niet alleen voor de Belastingdienst, maar wordt door betrokkenen gezien als een overheidsbreed probleem, zoals ook uit de verkenning bij gemeenten naar voren is gekomen (zie ook paragraaf 6.3.2).

De gebeurtenissen bij DigiNotar hebben de SVB en Belastingdienst bovendien bewust gemaakt van het belang van terugvalscenario's waardoor de continuïteit, integriteit en vertrouwelijkheid van het gegevensverkeer niet in gevaar komen als een communicatiekanaal of beveiligingsmechanisme uitvalt. De noodzaak voor dergelijke redundantie geldt voor de dienstverlening van beide diensten maar ook voor de ketenpartners van wie zij afhankelijk zijn. Voor het inloggen met DigiD bij overheidsorganisaties, zouden bijvoorbeeld verschillende mogelijkheden moeten zijn, zoals internetbetalingen via Ideal, Paypal of met creditcard kunnen worden gedaan.

Beide organisaties geven aan dat de multikanaalbenadering bij dit soort incidenten ook als een vorm van meervoudig uitgevoerde beheersmaatregel (redundantie) of back-up systeem kan fungeren, hoewel niet zo bedoeld. De Onderzoeksraad tekent daarbij aan dat, hoewel de multikanaalbenadering onderdeel is van de dienstverlening van beide organisaties, de tendens lijkt te zijn dat deze 'fysieke' kanalen als post en kantoren worden uitgefaseerd omdat alles wordt gedigitaliseerd. Wellicht worden in de toekomst ook digitale multikanaal benaderingen mogelijk.

Betrokkenen bij beide organisaties zijn bijna zonder uitzondering tevreden over de aanpak van het DigiNotarincident in eigen huis en door anderen. De uitvoeringsinstanties werden al snel in een coördinerende rol betrokken bij het crisisoverleg en de situatie is volgens hen adequaat aangepakt. Zij hebben er veel vertrouwen in dat dit bij een volgend incident weer zo zal gaan. De Onderzoeksraad plaatst hierbij echter vraagtekens. Bij de succesvolle beheersing van de gevolgen van de inbraak bij DigiNotar speelde een grote rol dat de functionarissen met de juiste kennis elkaar snel vonden. Of er bij een volgend incident op het gebied van digitale veiligheid weer op een vergelijkbare manier kan worden opgetreden is afhankelijk van wie de leiding neemt, of dat door de anderen wordt geaccepteerd en welke belangen er spelen, aangezien een specifiek draaiboek voor het bestrijden van crises in het digitale domein ontbreekt. Begint een volgend incident bijvoorbeeld bij een organisatie buiten het publieke domein waarmee de overheid geen regulier contact onderhoudt, dan is het maar de vraag of snel genoeg zal kunnen worden ingegrepen als daarvoor geen structuur is ingericht.

6.2.4 Door geïnterviewden aangegeven verbetermogelijkheden

In het verlengde van het hierboven genoemde, zien de geïnterviewden bij de SVB en de Belastingdienst verschillende mogelijkheden voor verbetering. Zij geven als aandachtspunt hierbij aan dat zij deze mogelijkheden veelal niet zelfstandig kunnen realiseren, maar daarvoor hun ketenpartners of de rijksoverheid als ketenregisseur nodig hebben.

Een aantal geïnterviewden is van mening dat het verder uniformeren van GBA persoonsgegevenssystemen van gemeenten en het omgaan daarmee, kan leiden tot een verbetering van de dienstverlening aan burgers en meer digitale veiligheid in de keten. Sommigen plaatsen deze observatie in breder perspectief, en dringen aan op meer centrale regie op het gebied van ICT-infrastructuur en informatieveiligheidsbeleid bij rijksoverheidsorganisaties en lokaal bestuur.

Ten tweede zijn geïnterviewden bij beide organisaties van mening dat de landelijke authenticatievoorziening DigiD toe is aan modernisering. De huidige beveiligingsniveaus zijn naar hun oordeel onvoldoende om ook in de toekomst en bij de toenemende dreigingen voor digitale veiligheid, veilige en betrouwbare verbindingen te garanderen.

Ten derde geeft een aantal geïnterviewden aan dat het, gezien de snelheid van de ontwikkelingen op ICT-gebied, een illusie is te denken dat overheidsinstanties voor zullen blijven lopen op partijen met minder goede bedoelingen. Zij zijn allen van mening dat zich in de toekomst continue incidenten op het gebied van digitale veiligheid zullen voordoen, en benadrukken het belang van investeren in flexibele, veerkrachtige organisaties die goed in staat zijn optredende crises te beheersen. Bij het omgaan met dergelijke crises hoort ook snelle, eenduidige en juiste crisiscommunicatie met burgers en bedrijven.

Ten vierde signaleren de geïnterviewden dat overheidsorganisaties meer moeten investeren in communicatie aan burgers en bedrijven over de risico's voor digitale veiligheid en dienen te voorzien in maatregelen die de schade voor individuele burgers als gevolg van een digitaal veiligheidsincident beperken. Dit helpt het vertrouwen van burgers en bedrijven in de overheid vast te houden. Deze maatregelen dienen te voorzien in het melden van zaken als identiteitsdiefstal en –fraude en het bieden van hulp bij het beperken van de nadelige gevolgen hiervan.

Ten vijfde plaatst een deel van de geïnterviewden vraagtekens bij de vraag in hoeverre de lessen die zijn getrokken uit het DigiNotarincident werkelijk zullen beklijven. Immers, niemand heeft aan den lijve ondervonden wat er fout had kunnen gaan. De aandacht voor de betrouwbaarheid en continuïteit van de ICT-systemen is daarmee mogelijk in slaap gesust. Ook als er weinig lijkt te gebeuren, dienen organisaties continu alert te zijn en digitale veiligheid op de radar te houden.

Ten slotte ziet een aantal geïnterviewden dat de onderlinge verwevenheid van processen, diensten en organisaties in de complexe keten grote afhankelijkheden veroorzaakt. Dat behoeft naar hun inzicht aandacht van de rijksoverheid. Eén partij moet het initiatief nemen om de onderlinge afhankelijkheid en de risico's waartoe dat leidt in kaart te brengen, zodat eventueel maatregelen genomen kunnen worden.

6.3 Digitale veiligheid bij gemeenten

Deze paragraaf schetst een beeld op hoofdlijnen van digitale veiligheid in relatie tot e-dienstverlening bij de gemeenten.

6.3.1 Het bestuur en de ambtelijke organisatie van gemeenten

Het lokaal bestuur bestaat in Nederland uit ongeveer 420 gemeenten van verschillende grootte, die worden bestuurd door een gemeenteraad en een college van burgemeester en wethouders. Gemeenten hebben een eigenstandige beleidsbevoegdheid op allerlei terreinen, en zijn daarnaast een belangrijke uitvoerder van door de rijksoverheid vastgesteld beleid. Het college van burgemeester en wethouders is verantwoordelijk voor de ontwikkeling en uitvoering van beleid door de gemeente, en daarmee ook voor de bedrijfsvoering waarvan een goed beveiligingsbeleid en het waarborgen van digitale veiligheid onderdeel uitmaken. De gemeentelijke organisatie, onder leiding van de gemeentesecretaris, staat het college hierin bij. De gemeenteraad stelt het beleid op hoofdlijnen vast, en controleert de uitvoering hiervan door het college.

De gemeentelijke organisatie is, afhankelijk van grootte en opdeling van taken en werkzaamheden, verdeeld in diensten en/of afdelingen, veelal aangestuurd door een directeur. De afdelingen voeren taken uit als vergunningverlening, bouw- en woningtoezicht, burgerzaken, innen van belastingen, onderwijszaken, etc. Gemeenten maken veel werk van het verbeteren van dienstverlening. Zo startten zij Klant Contact Centra (KCC's) en bieden zij diensten aan via de website, de e-dienstverlening. Bovendien krijgen gemeenten meer taken toebedeeld door het rijk. Bijvoorbeeld via de decentralisaties van de Jeugdzorg, de Wet Werken Naar Vermogen en de Wet Maatschappelijke ondersteuning. Mede door programma's als het i-NUP staat een goede dienstverlening bij de meeste gemeenten prominent op de agenda.

Door hun brede werkterrein zijn gemeenten betrokken bij een grote verscheidenheid aan digitale gegevensstromen waarvan zij de veiligheid moeten waarborgen. Deze toename van de ketenautomatisering is veelal verplicht opgelegd door de landelijke overheid. Van bijzonder belang hierbij is dat gemeenten als beheerder fungeren van enkele basisregistraties, waaronder de Gemeentelijke basisadministratie persoonsgegevens (zie onderstaand kader). Zij moeten hiervoor voldoen aan wettelijk vastgelegde standaarden. Deze standaarden hebben een bepalende invloed op de informatiearchitectuur van de gemeentelijke organisatie. Tegelijkertijd wordt van gemeenten, onder meer naar aanleiding van het al eerder genoemde i-NUP programma, steeds meer verwacht op het gebied van digitale dienstverlening aan burgers. Gemeenten moeten hét loket voor de overheid worden.

Wat is de GBA?
De Gemeentelijke basisadministratie persoonsgegevens (GBA) is de registratie die enkele kerngegevens bevat van iedereen die in Nederland woont of gewoond heeft. Gegevens uit de GBA worden gebruikt door verschillende bestuursorganen en organisaties in de semi-publieke sector. De GBA is gekoppeld met diverse andere registraties.

De GBA wordt beheerd door de gemeenten, die verantwoordelijk zijn voor de juistheid van de gegevens. Wanneer een instantie die GBA-gegevens gebruikt op een onjuistheid stuit, is zij verplicht deze bij de gemeente te melden. Deze neemt de melding in onderzoek en past, indien nodig, de GBA aan. Iedere gemeente beschikt over een eigen GBA en registreert daarin de persoonsgegevens van haar inwoners.

Het GBA is een van de zogeheten basisregistraties, die de overheid gebruikt voor het uitvoeren van haar kerntaken. Voorbeelden van andere basisregistraties zijn de Basisregistratie Adressen en Gebouwen (BAG), het Nationaal Handelsregister (NHR) waar de Kamer van Koophandel alle bedrijfsgegevens registreert en de Registratie Niet-Ingezetenen (RNI). De GBA zal op termijn met de RNI opgaan in de Basisregistratie personen (BRP).

6.3.2 Bestuurlijke inbedding digitaal veiligheidsbeleid bij gemeenten

Deze paragraaf schetst een beeld van de wijze waarop de aan de verkenning deelgenomen gemeenten invulling geven aan hun verantwoordelijkheid voor digitale veiligheid. Uit de verkenning blijkt een tweedeling in het gemeentelijk digitaal veiligheidsbeleid tussen processen die worden beheerst door hogere wet- en regelgeving, zoals de omgang met de GBA persoonsgegevens en processen in de werk- en inkomensketen, en gegevensverwerkende processen waarvoor dat niet het geval is.

Ten aanzien van hun omgang met de GBA persoonsgegevens moeten gemeenten bijvoorbeeld voldoen aan stringente eisen op het gebied van beveiliging, waaronder het opstellen van een risicoanalyse en een informatiebeveiligingsplan waarin verantwoordelijkheden en procedures worden benoemd.[94] Deze eisen zijn enerzijds inhoudelijk en gericht op de kwaliteit en consistentie van de GBA-gegevens; anderzijds zijn deze gericht op de processen rond privacy en technische beveiliging en beschikbaarheid van de GBA-gegevens. Eens per drie jaar wordt elke gemeente onderworpen aan een GBA-audit, waarin een onafhankelijke instantie namens het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzoekt of de gemeente aan de gestelde eisen voldoet.

Voor veel gemeentelijke gegevensverwerkende processen die hier buiten vallen bestaan evenwel geen landelijke eisen. Gemeenten moeten hiervoor zelf invulling geven aan hun verantwoordelijkheid voor digitale veiligheid, maar doen dat slechts in beperkte mate. Buiten het domein van de GBA persoonsgegevens ontbreken risicoanalyses veelal, en ook het informatiebeveiligingsplan strekt zich vaak niet tot deze processen uit. Slechts enkele gemeenten hanteren een integraal beveiligingsplan voor al hun processen. De ISO-normen 27001 en 27002 voor informatiebeveiliging, die als open standaard gelden voor de gehele overheid en waarvan ook gemeenten alleen gemotiveerd mogen afwijken, worden slechts spaarzaam toegepast. Gebleken is dat pas na de incidenten in 2011 informatiebeveiliging bij gemeenten landelijk op de agenda is gekomen, onder andere vanuit VNG en KING. Activiteiten die hierop betrekking hebben, zoals bijvoorbeeld de in dit jaar uit te voeren audits op informatiebeveiligingsprocessen rondom Suwinet en DigiD en de beveiliging van webapplicaties kennen weinig landelijke coördinatie of afstemming. Het normenkader voor deze audits komt evenwel grotendeels overeen.

Ontwikkeling en uitvoering van beleid voor digitale veiligheid

Uit de verkenning blijkt dat de beleidsontwikkeling ten aanzien van digitale veiligheid over het algemeen een onderdeel is van het informatiebeveiligingsbeleid en is belegd bij de ICT- en facilitaire afdelingen in de gemeentelijke organisatie.[95] In teams, aangestuurd door operationele en tactische managers, wordt door een of enkele medewerkers het informatiebeveiligingsbeleid voor de gehele gemeente ontwikkeld. In een enkel geval vindt de beleidsontwikkeling plaats in een team met taken op het gebied van informatiemanagement. De managers bespreken het beleid met hun directeur. Vervolgens stelt de directie het beleid vast. Dit wordt slechts in enkele gevallen bekrachtigd door het college van burgemeester en wethouders, behoudens het beleid ten aanzien van de GBA persoonsgegevens waar de wet dit expliciet vereist.

94 Vergelijkbare verplichtingen gelden voor de taken van de gemeente in de werk- en inkomensketen (art. 6.4 Regeling SUWI). Uit onderzoek van de Inspectie Werk en Inkomen blijkt dat vrijwel alle gemeenten beschikken over een informatiebeveiligingsplan voor hun processen in dit domein.

95 Informatiebeveiligingsbeleid richt zich verder op de fysieke en logische beveiliging van systemen en gegevensbestanden tegen onbevoegde toegang. Ook is het gericht op waarborgen van de continuïteit van de dienstverlening bij een onverhoopte uitval van computers als gevolg van bijvoorbeeld een technisch defect of bij brand. De invulling ervan verschilt per gemeente.

Op basis van de verkenning blijkt dat veelal de wethouder met dienstverlening in zijn portefeuille de bestuurlijke verantwoordelijkheid draagt voor digitale veiligheid. Een enkele keer is het ondergebracht in de portefeuille ICT. Digitale veiligheid is in alle gevallen een klein onderdeel van de taken in die portefeuilles. De ambtelijke eindverantwoordelijkheid is belegd bij de directeur of manager die de ICT-afdeling binnen zijn sector heeft. Digitale veiligheid is op bestuurlijk niveau noch op directieniveau een onderwerp dat regelmatig aandacht krijgt. Uitzondering hierop zijn de verplichte formele GBA-stukken, die overigens vrijwel altijd hamerstukken zijn.

Het afdelingshoofd van de ICT- of facilitaire afdeling heeft de dagelijkse verantwoordelijkheid voor digitale veiligheid. Een van zijn hoofdtaken is het bewaken van de digitale veiligheid, waaronder in een aantal gevallen ook het beheer (bestellen en/of verlengen) van certificaten valt. Binnen deze afdelingen bevinden zich de medewerkers die belast zijn met het uitvoeren van het technische deel van het informatiebeveiligingsbeleid. Hieronder vallen onder meer: het uitvoeren van analyses op internet- en netwerkverkeer, logging van toegang tot gegevens, verstrekken en beheren van autorisaties, begeleiden van hackerstests of penetratietests (enkel bij sommige gemeenten), het werken aan bewustwording bij gemeentepersoneel, beleidsvoorbereiding, etc. Bij een aantal gemeenten is een 'security officer' benoemd. Deze rol omvat niet alleen de technische realisatie van digitale veiligheid, maar juist ook het vergroten van het bewustzijn van informatiebeveiliging binnen de organisatie.

Kennen van risico's
Uit de verkenning komt een drietal risico's naar voren ten aanzien van het digitaal veiligheidsbeleid bij gemeenten.

Ten eerste maken veel gemeenten in hun digitaal veiligheidsbeleid gebruik van diensten die zij inkopen bij externe partijen, zoals bijvoorbeeld het beheer van specifieke applicaties en data-opslag. Het uitbesteden van zaken waarvoor externe expertise benodigd is, introduceert echter ook nieuwe risico's. Een back-up van vertrouwelijke gegevens kan gecompromitteerd raken en een extern applicatiebeheerder is een extra schakel die toegang heeft tot de vertrouwelijke gegevens. De ICT-medewerkers van gemeenten zijn zich meestal wel bewust van dergelijke risico's, maar deze worden niet op een systematische wijze beheerst. Dat geldt ook ten aanzien van certificaat-dienstverleners, zoals DigiNotar.

Gemeenten achten zichzelf onvoldoende in staat om de betrouwbaarheid van de certificaten en de dienstverlening van deze organisaties zelf te controleren. Zij zien de certificaatdienstverlener als een organisatie die deskundig is op een zeer specialistisch terrein en dat zij erop mogen vertrouwen dat de veiligheid bij dergelijke partijen gegarandeerd is. Zij zien hierin ook geen keus: er is intern geen kennis aanwezig om dit te kunnen uitvoeren. Daarvoor zijn andere partijen, de auditerende instantie, die de certicaatdienstverlener controleert.

Ook in de gegevensuitwisseling met andere overheidsorganisaties zijn risico's te identificeren. Het DigiNotarincident is hiervan een voorbeeld. Diverse gemeenten hadden verschillende door DigiNotar geleverde certificaten in gebruik voor hun digitale dienstverlening. Toen de certificaten van DigiNotar werden ingetrokken, moesten sommige gemeenten bepaalde digitale diensten zelfs staken bij gebrek aan andere certificaten. Gebleken is dat de deelnemende gemeenten zich nauwelijks bewust zijn van dergelijke risico's.

Een derde punt van zorg betreft de mate waarin het bestuur en hoger management, maar ook de medewerkers die betrokken zijn bij de primaire dienstverleningsprocessen van de gemeente, doordrongen zijn van het belang van digitale veiligheid en hun eigen rol daarin. Over het algemeen hebben de functionarissen met kennis van zaken op het gebied van digitale veiligheid een hoge mate van risicobewustzijn. Het risicobewustzijn beperkt zich echter tot deze inhoudelijk deskundigen en is nauwelijks aanwezig bij het bestuur en hoger management. Dit kan ertoe leiden dat het veiligheidsbeleid in de praktijk niet of onjuist wordt uitgevoerd, waardoor de beoogde mate van digitale veiligheid niet kan worden geboden.

Over het algemeen geldt dat gemeenten de risico's voor digitale veiligheid goed in beeld hebben wanneer deze de GBA persoonsgegevens betreffen. Daarbuiten is dat minder het geval, in weerwil van de beschikbare ISO-norm die ook hierop toegepast kan worden. Slechts enkele (grotere) gemeenten tonen zich in staat te handelen naar de herkende risico's door bijvoorbeeld in gesprek te gaan met externe leveranciers. Andere (kleinere) gemeenten zijn in de veronderstelling dat zij hier geen invloed op uit kunnen oefenen, maar moeten vertrouwen op diens veilige dienstverlening. De risico's van het gecompromitteerd raken of uitvallen van gegevensuitwisseling met andere overheidsdiensten zijn niet overal in beeld.

De Onderzoeksraad wijst op een vierde risico, dat door geen van de in het onderzoek betrokken gemeenten is genoemd. Het valt de Onderzoeksraad op dat sprake is van geringe verbondenheid tussen digitaal veiligheidsbeleid en de primaire processen waarop dit van toepassing is. Zoals in hoofdstuk 3 is gesteld, is een duidelijke grondslag voor veiligheid in het primaire proces van de organisatie een voorwaarde voor adequaat veiligheidsbeleid. Dit vereist dat digitaal veiligheidsbeleid tot stand komt door intensieve samenwerking tussen degenen die verantwoordelijkheid dragen voor de primaire processen, en degenen die de voorwaarden kunnen scheppen om deze processen veilig te doen plaatsvinden. Uit de verkenning blijkt dat digitale veiligheid veelal aan die laatsten wordt overgelaten. Meer betrokkenheid bij en actieve aansturing door interne opdrachtgevers (de verschillende directies en diensten binnen de gemeente) aan de interne opdrachtnemers (de ICT-afdelingen) acht de Onderzoeksraad dan ook wenselijk.

De Onderzoeksraad constateert dat de digitale veiligheid van GBA-gerelateerde processen in gemeenten begrijperlijkerwijs de meeste aandacht krijgt. Aandacht voor de digitale veiligheid vanuit sectoren, waar de overige dienstverlening aan derden is belegd, heeft de Onderzoeksraad in veel mindere mate aangetroffen. Er worden vanuit die diensten geen eisen gesteld aan de kwaliteit en veiligheid van de informatie(-uitwisseling); dat gebeurt door de afdeling die verantwoordelijk is voor het voldoen aan de kwaliteitseisen. Het valt op dat een functiescheiding tussen opstellen, uitvoeren en controleren van het digitaal veiligheidsbeleid niet altijd aanwezig is. Ook valt op dat bestuur en hoger management eerder passief en reactief dan initiërend en sturend bij informatie-beveiliging betrokken lijken, terwijl zij tegelijkertijd aangeven informatiebeveiliging wel belangrijk te vinden. Gemeenten geven hiermee ten dele uitvoering aan de borging van het informatie-beveiligingsbeleid.

Evalueren van informatiebeveiligingsbeleid
Vanwege de in dat domein geldende verplichtingen onderzoeken gemeenten actief of het digitaal veiligheidsbeleid ten aanzien van GBA-gerelateerde processen goed wordt nageleefd. Dit leidt tot rapportages aan het management. Alle gemeenten hebben hiertoe een (wettelijk verplichte) beveiligingsbeheerder of security officer aangesteld, die het beleid onderzoekt en evalueert. Verder worden periodiek risicoanalyses en afhankelijkheids- en kwetsbaarheidsanalyses uitgevoerd. Dit alles leidt tot een voortdurende evaluatie van het beleid en de uitvoering ervan. Zonodig vindt bijsturing plaats.

Ten aanzien van andere systemen dan de GBA persoonsgegevens vindt, enkele uitzonderingen daargelaten, evaluatie in veel mindere mate gestructureerd plaats. Door het management wordt impliciet aangenomen dat, als de situatie ten aanzien van de GBA persoonsgegevens in orde is, dit ook geldt voor andere ICT-systemen.[96] Met betrekking tot systemen die zich buiten het gezichtsveld van een gemeente bevinden is helemaal geen sprake van onderzoek of evaluatie door de gemeenten. Gemeenten nemen kennis van het feit dat een organisatie of een werkwijze kennelijk door andere instanties wordt gecontroleerd en dat hierin voor de gemeente geen rol is weggelegd. In het verlengde daarvan wordt dit ook niet door hen geëvalueerd.

96 Zie ook artikel 'Gemeenten slordig met privégegevens; beveiliging van vertrouwelijke en privacygevoelige informatie van burgers is onder de maat', NRC Handelsblad, 14 maart 2012.

Herstellen en leren van incidenten
Uit de verkenning blijkt dat gemeenten slechts in beperkte mate beleid hebben over het leren van incidenten op het gebied van digitale veiligheid. Zo vindt melden van incidenten op het gebied van digitale veiligheid niet op grote schaal plaats. Waar dat wel bestaat, is aangegeven bij wie medewerkers een melding kunnen doen. Ook is er in het beleid aandacht voor terugkoppeling met de melder over de afdoening van het incident. Het beleid voorziet veelal in een rapportagecyclus voor incidenten onder verantwoordelijkheid van een informatiemanager. Net als het kennen van de risico's en het treffen van maatregelen, geldt voor het leren van incidenten dat het aanwezige beleid gericht is op de GBA persoonsgegevens. Een integrale aanpak, om te leren van alle incidenten op het gebied van digitale veiligheid binnen een gemeentelijke organisatie, ontbreekt.

De verantwoordelijkheid voor het oplossen van ontstane incidenten ligt bij alle deelnemende gemeenten vrijwel geheel bij de ICT-afdeling. De ernst van het incident bepaalt of de informatiemanager de directie onmiddellijk of met enige vertraging op de hoogte stelt van de gebeurtenis. Het bestuur en de leden van de directie, die verantwoordelijk zijn voor de digitale veiligheid, zijn voor de informatiemanagers eenvoudig en snel bereikbaar (laagdrempeligheid). Het bestuur en de directie vertrouwen op de adviezen van de ICT-afdeling en laten zich daardoor leiden. Uit de gesprekken is niet inzichtelijk geworden in welke mate zulke adviezen van invloed zijn op de sturing van de organisatie en in welke mate gemeenten in het algemeen daarvan op structurele wijze leren.

Bestuurlijke betrokkenheid bij digitale veiligheid
Uit de gesprekken is gebleken dat bestuurders steeds meer het belang van digitale veiligheid zien en zich actief met het onderwerp willen bezig houden. Ook gemeentelijke directieteams geven aan dat zij informatiebeveiliging erg belangrijk vinden. Omdat de mogelijke risico's en de daarbij passende maatregelen echter vaak technisch van aard zijn, geven veel gemeenten aan dat noch de directie, noch het college van burgemeester en wethouders deze goed kunnen overzien. Daardoor is digitale veiligheid een onderwerp waarop in de praktijk vaak de computertechnici en de operationeel leidinggevenden van de ICT-afdelingen het beleid en de strategie bepalen. Slechts als er ernstige incidenten zijn is er een actieve rol voor de bestuurders en het hogere management. Zij moeten dan op grond van de bij hen aanwezige kennis beslissingen nemen tijdens een incident. Digitale veiligheid staat bij slechts enkele deelnemende gemeenten vast op de agenda van het bestuur of de gemeenteraad.

Door de hierboven beschreven 'kenniskloof' op het gebied van digitale veiligheid tussen de directie en het bestuur enerzijds en de uitvoerende afdelingen zoals ICT aan de andere kant, is binnen gemeentelijke organisaties veelal geen sprake van goed functionerend opdrachtgeverschap op dit terrein. Directie en bestuur erkennen het belang van digitale veiligheid, maar ervaren tegelijkertijd dat zij inhoudelijk onvoldoende geëquipeerd zijn om sturing te geven aan dit onderwerp. Directie en bestuur slagen er onvoldoende in deze schaarse functionarissen aan te trekken of te behouden. Hierdoor kunnen de directie en het bestuur vaak hun verantwoordelijkheid voor digitale veiligheid in onvoldoende mate gestalte geven. Dit baart de Onderzoeksraad zorgen.

6.3.3 De impact van het DigiNotarincident bij gemeenten

Sommige van de deelnemende gemeenten hadden nauwelijks certificaten van DigiNotar, andere gemeenten veel. De meeste gemeenten vernamen uit de media dat er problemen waren met deze certificaten. Toen de certificaten van DigiNotar werden ingetrokken, haalden gemeenten de getroffen digitale diensten en websites offline. Hoewel verschillende gemeenten meteen contact zochten met DigiNotar, Logius, de Vereniging Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING), kregen zij in de eerste dagen weinig tot geen ondersteuning. In de weken na het incident kwam meer informatie van VNG en KING beschikbaar en werden deze partijen ook beter bereikbaar voor de gemeenten.

Gemeenten zagen zich genoodzaakt zelf de DigiNotarcertificaten te vervangen. Een knelpunt was dat PKIoverheid-certificaten, waarvan sommige gemeenten gebruik maakten, maar door weinig leveranciers werden aangeboden. De gemeenten hebben veel energie gestoken in het vervangen van de certificaten. Door het incident hebben zij beter zicht gekregen op de digitale certificaten die zij in gebruik hadden, en de daaraan verbonden risico's.

Enkele gemeenten hebben vooral last gehad van de zogenaamde Lektober-actie, omdat deze hun dienstverlening op verschillende manieren raakte (zie onderstaand kader). Voor burgers betekende dit dat zij naar het gemeentehuis toe moesten of telefonisch contact op moesten nemen, met vertraging in de afhandeling tot gevolg.

Lektober
Lektober was een actie van de digitale ICT-nieuwssite Webwereld. Hierin werd o.a. naar aanleiding van het DigiNotarincident, de maand oktober 2011 uitgeroepen tot de maand 'lektober'. Elke werkdag van deze maand werd een ICT-privacylek in een website of overheidsdienst onthuld, zoals van particuliere – en vrijwilligersorganisaties, maar ook van ziekenhuizen en gemeenten.

Het doel van Webwereld met deze actie was om organisaties bewust te maken van het feit dat het beheer van privacygevoelige gegevens een grote verantwoordelijkheid met zich meebrengt. Zij stellen zich op het standpunt dat steeds weer op pijnlijke wijze blijkt dat organisaties, zowel in het publieke als het private domein, veel te weinig aandacht besteden aan het beveiligen van de privégegevens die ze beheren. Om dat onder de aandacht te brengen heeft Webwereld in samenwerking met freelance onderzoeksjournalist De Winter in oktober 2011 elke werkdag een privacylek openbaar gemaakt. De werkwijze was dat voordat de lekken in de openbaarheid werden gebracht, de bewuste organisatie op de hoogte gebracht werd van het lek (responsible disclosure). Zo kon die lekkende partij actie ondernemen voordat Webwereld het lek publiceerde. Daarnaast werd geen enkele database gedownload of geopenbaard

De onderzochte gemeenten geven aan dat het Diginotarincident en de Lektober-actie waardevolle leermomenten zijn geweest. Zij hadden geen crisisteams voorbereid voor dergelijke calamiteiten. Het oplossend vermogen van de ICT-afdelingen van de verschillende gemeenten speelde een grote rol bij de afhandeling van deze incidenten.

Ook wijzen de gemeenten erop dat de afhankelijkheid van een enkele leverancier (zoals van digitale certificaten) een belangrijke les is geweest. Voor zover die al niet bestonden, zijn adequate terugvalscenario's nog meer van belang. Wat hierbij opvalt, is dat, anders dan bij de SVB en de Belastingdienst, de ketenproblematiek en het daarbij behorende bewustzijn van de eigen kwetsbaarheid of afhankelijkheid van de andere ketenpartners bijna geheel aan de gemeenten voorbij lijkt te gaan. Gemeenten zijn niet alleen leverancier van GBA persoonsgegevens aan andere organisaties in de werk en inkomen keten, maar ook zelf opdrachtgever daarin, zoals van de SVB (zie ook paragraaf 6.2.1). De afhankelijkheid van andere partijen die wel sterk gevoeld wordt, is die van Logius als landelijk beheerder van DigiD en van private, externe leveranciers van ICT-diensten. Digitale veiligheid speelt slechts in beperkte mate een rol bij uitbesteding van diensten aan derde partijen. Gemeenten nemen soms specifieke eisen op dit terrein op in contracten en *service level agreements*, maar monitoren naleving daarvan slechts zelden.

Uit de verkenning is niet duidelijk geworden in hoeverre beide incidenten aanleiding hebben gegeven tot wijziging van het veiligheidsbeleid. Men realiseert zich ook dat na enige tijd de aandacht voor de gevolgen van een incident wegebt. Om het veiligheidsbewustzijn op een acceptabel niveau te brengen en te houden, zien informatiemanagers het belang van permanente voorlichting door het management.

6.4 Conclusies uit de verkenning

De verkenning heeft geleid tot een aantal observaties over de borging van digitale veiligheid bij overheidsorganisaties in het algemeen. Daarnaast heeft het een aantal specifieke inzichten opgeleverd over de wijze waarop en de mate waarin de verschillende overheidsorganisaties hun verantwoordelijkheid waarmaken. Deze worden hierna toegelicht.

Er bestaan grote verschillen in de wijze waarop de diverse overheidsorganisaties hun verantwoordelijkheid voor digitale veiligheid invullen en borgen. Zo lijken de grote, hooggeautomatiseerde uitvoeringsorganisaties met gestandaardiseerde werkprocessen daarin beter te slagen dan de veel kleinere overheidsorganisaties met een grote diversiteit aan processen en diensten en taken als gemeenten. Een ander inzicht is dat de ketenproblematiek en het daarbij behorende bewustzijn van de eigen kwetsbaarheid of afhankelijkheid van andere partners in de keten, heel verschillend wordt beleefd. Gemeenten lijken deze bijna niet te ervaren, in tegenstelling tot de SVB en de Belastingdienst. Als laatste valt op dat gemeenten er veel minder op gericht lijken om de knelpunten en uitdagingen waar zij zich bij digitale veiligheid voor gesteld zien gezamenlijk het hoofd te bieden, waar de uitvoeringsorganisaties op rijksniveau via zelfgeorganiseerde samenwerkingsverbanden als de Manifestgroep van elkaars kennis en expertise gebruik maken.

Er zijn ook overeenkomsten tussen de verschillende overheidsorganisaties: zo geven alle organisaties aan dat zij niet voorbereid waren op het DigiNotarincident en dat dit voor hen een echte 'wake up call' is geweest om het onderwerp hoog op de bestuurlijke agenda te krijgen en er werk van te maken. Ook zien zij in dat digitale veiligheid, meer nog dan door de techniek, bepaald wordt door het gedrag van medewerkers, hetgeen continue aandacht vereist.

Meer specifiek lijkt het zo te zijn dat organisaties het best in staat zijn invulling te geven aan hun verantwoordelijkheid voor digitale veiligheid wanneer deze zo veel mogelijk geïntegreerd is in hun primaire processen. Als gevolg daarvan kunnen de risico's bij organisaties waar digitale dienstverlening deel uitmaakt van het primaire bedrijfsproces beter worden beheerst. Dat heeft te maken met het feit dat digitale veiligheid in die organisaties veel directer gekoppeld is aan het behalen van de doelstellingen en van direct belang is voor de continuïteit van die dienstverlening die het bestaansrecht vormt van de organisatie. Het wekt in dat licht geen verbazing dat de uitvoerende organisaties, zoals de SVB, meer aantoonbaar grip lijken te hebben op digitale veiligheid dan gemeenten. Daarbij zijn niet alleen de omvang van de bedrijfsprocessen en de mate waarin de gegevensuitwisselingen geautomatiseerd uitgevoerd worden, bepalend. Dat deze organisaties digitale veiligheid zien als randvoorwaarde voor de continuïteit van hun dienstverlening en het vertrouwen van derden daarin maakt het verschil.

Diezelfde organisaties waarbij digitale veiligheid onderdeel uitmaakt van de bedrijfsprocessen en -doelstellingen hebben losgelaten dat honderd procent (digitale) veiligheid mogelijk is. Zij blijven hiernaar streven en richten zich vooral op het tijdig ontdekken en herstellen van onregelmatigheden en het ontwikkelen van een flexibele en weerbare organisatie die in staat is adequaat te reageren op optredende incidenten op dit terrein.[97] Een belangrijk hulpmiddel daarbij zien zij in het werken volgens de bestaande ISO 27000-normen, uitgebreide monitoring en logging van al het 'verkeer' in de digitale processen en ICT-systemen. Ook passen zij continu de criteria aan op basis waarvan de werkvloer en de ondersteunende ICT-afdelingen tijdig onregelmatigheden kunnen herkennen en afhandelen.

Toch zijn ook deze organisaties kwetsbaar voor digitale veiligheidsincidenten door onder andere de staat van digitale veiligheid van derde partijen waar zij digitaal mee communiceren én van het digitale veiligheidsbewustzijn van de eigen medewerkers. Zij onderkennen ook zelf deze aspecten als de zwakke schakels in de veiligheidsketen. Het niet snel kunnen overstappen op andere certificaten of een andere werkwijze, zoals naar aanleiding van het DigiNotarincident, is daarvan maar één voorbeeld. Afhankelijkheid van één internetprovider, één certificaatleverancier of één inlogsysteem (DigiD) voor gebruikers, zijn andere voorbeelden.[98] De huidige 'fysieke' multikanaalbenadering (post, telefoon en loket naast websites) is een effectieve, praktische oplossing gebleken voor het opvangen van gevolgen van digitale incidenten, maar waarschijnlijk op lange(re) termijn niet houdbaar.

97 High Reliability Organizations zijn organisaties die er in slagen om crises en grote incidenten te voorkomen of snel tot een goed eind te brengen in een omgeving die zich kenmerkt door hoge risico's en een hoge mate van complexiteit. Zie verder Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for High Reliability: Processes of Collective Mindfulness. In B. M. Staw & L. L. Cummings (Eds.), Research in Organizational Behavior (Vol. 21, pp. 81-123). Greenwich, CT: JAI Press, Inc.

98 DigiD is tot op heden het enige authenticatiemechanisme voor burgers voor het gebruik van overheidsdiensten. Zie ook kader in paragraaf 6.1

Als een vergelijkbare vorm van effectieve risicobeheersing kan in de toekomst naar een digitale multikanaalbenadering gezocht worden om de kwetsbaarheid van organisaties en hun klanten voor incidenten in digitale informatiestromen en gegevensuitwisselingen te verkleinen.[99]

Bij gemeenten is naar voren gekomen dat het politieke bestuur en de directie van de gemeentelijke organisatie doorgaans weinig betrokken zijn bij digitale veiligheid. Alleen in geval van een groot incident zoals DigiNotar of de Lektober-actie komt het onderwerp in beeld bij het bestuur. Digitale veiligheid is geen vast onderwerp op de agenda. Het management van de verschillende dienstverlenende organisatieonderdelen stelt doorgaans geen eisen aan de door andere partijen te realiseren mate van digitale veiligheid. Dit geldt zowel in hun rol als intern opdrachtgever van de eigen ICT-afdeling, als opdrachtgever van externe ICT-dienstverleners.

Op GBA-gerelateerde processen passen gemeenten over het algemeen een adequate vorm van veiligheidsmanagement toe. Ook is voorzien in controle op dit beleid, door periodiek zowel interne als externe audits uit te voeren. De digitale veiligheidsrisico's van informatie-uitwisseling buiten het GBA-domein worden echter veel minder systematisch beheerst. Van integrale risicobeheersing op het gebied van digitale veiligheid is geen sprake. Het gebrek aan integrale eisen op dit vlak draagt hier aan bij, terwijl de beschikbare ISO-norm op dit vlak niet expliciet wordt toegepast.

99 De Stuurgroep Compacte Rijksdienst is hier al mee bezig. De Stuurgroep heeft besloten tot het inrichten van een aantal expertisecentra waarin meerdere overheidsinstellingen de krachten gaan bundelen. Onder andere de SVB, het UWV en de Belastingdienst werken mee aan de ontwikkeling van een Centrum Informatiebeveiliging en Privacybescherming.

7 CONCLUSIES

Het onderzoek van de Onderzoeksraad voor Veiligheid naar digitale veiligheid naar aanleiding van het DigiNotarincident richt zich op overheidsorganisaties. Overheidsorganisaties zijn verantwoordelijk voor de gegevens die zij verwerken. Zij moeten hier zo zorgvuldig mogelijk mee omgaan. Ook wanneer overheidsorganisaties taken uitbesteden aan externe partijen ligt de uiteindelijke verantwoordelijkheid voor de veiligheid van hun gegevens nog steeds bij hen. Zij moeten ernaar streven zo veel mogelijk grip te hebben op de beveiliging van hun gegevens en de betrouwbaarheid van het elektronische gegevensverkeer. Dit uitgangspunt is de reden dat de conclusies en aanbevelingen in dit onderzoek zich richten op overheidsorganisaties.

De centrale vraag in dit onderzoek is hoe overheidsorganisaties in bestuurlijk en organisatorisch opzicht omgaan met digitale veiligheid, en welke knelpunten zich hierbij manifesteren. Om antwoord op deze vraag te geven, is onderzocht hoe de veiligheid van digitale certificaten in zijn algemeenheid wordt gewaarborgd. Daarnaast is bij een aantal overheidsorganisaties onderzocht hoe zij in algemene zin digitale veiligheid waarborgen. De Onderzoeksraad trekt, op basis van het onderzoek dat hij heeft uitgevoerd, de volgende conclusies.

7.1 DigiNotarincident

Voorafgaand aan de inbraak bij DigiNotar hadden de betrokken partijen onvoldoende zicht op de veiligheid van DigiNotar. Zowel toezichthouder OPTA als Logius, het agentschap waarmee DigiNotar een overeenkomst had voor het mogen leveren van PKIoverheid-certificaten, waren niet op de hoogte van de feitelijke betrouwbaarheid van de dienstverlening van DigiNotar. Beide organisaties gingen grotendeels af op de verklaring die wordt afgegeven door de auditerende instelling. Deze had, werkend volgens de voor haar geldende regels, aangegeven dat het managementsysteem van het bedrijf conform de daarvoor geldende normen was ingericht. Of de certificaatdienstverlening door DigiNotar feitelijk voldeed aan de regels die daarop van toepassing waren, werd slechts beperkt getoetst.

Geen van de betrokken partijen was voorbereid op het DigiNotarincident. Het risico, en de mogelijke gevolgen van het gecompromitteerd raken van alle certificaten en daarmee van de certificaatdienstverlener zelf, waren niet voorzien. Geen van de betrokken partijen had stilgestaan bij de mogelijkheid dat certificaten van een gecompromitteerde certificaatdienstverlener niet zonder gevolgen ongeldig verklaard kunnen worden. Niemand had zich gerealiseerd dat dit kon leiden tot het stilvallen van belangrijke gegevensstromen met en tussen overheidsorganisaties, met ingrijpende maatschappelijke gevolgen.

7.2 Veiligheid certificaatdienstverlening en omgang met certificaten

Goed gebruikte, betrouwbare digitale certificaten zijn essentieel voor de veiligheid van elektronisch gegevensverkeer. De Onderzoeksraad concludeert evenwel dat op beide terreinen – het goed gebruik van certificaten door overheidsorganisaties, en de geborgde betrouwbaarheid van certificaten – reden is tot zorg.

Overheidsorganisaties laten de aanschaf van digitale certificaten veelal over aan ICT-afdelingen, waardoor het risico ontstaat dat de aard van het te beschermen gegevensverkeer in deze keuze geen bepalende factor is. Daarbij blijken veel overheidsorganisaties zichzelf niet in staat te achten om een eigenstandige inschatting te maken van de betrouwbaarheid van de certificaten die zij aanschaffen. Zij verlaten zich daarom op het oordeel van anderen, zoals dat bijvoorbeeld tot uitdrukking komt in een keurmerk als WebTrust, of door gebruik te maken van PKIoverheid-certificaten die zijn ‘goedgekeurd’ door de rijksoverheid.

Deze situatie maakt het des te belangrijker dat het vertrouwen van overheidsorganisaties in keurmerken, of specifiek voor hen in stand gehouden stelsels als PKIoverheid, gerechtvaardigd is. De Onderzoeksraad concludeert echter dat dit momenteel slechts beperkt het geval is. PKIoverheid, evenals het stelsel voor gekwalificeerde certificaten, biedt niet de toegevoegde waarde die de rijksoverheid ermee beoogt, doordat geen adequaat toezicht plaats vindt op feitelijke naleving van de vigerende regels door de deelnemende certificaatdienstverleners.

Deels houdt dit verband met de structuur van het afsprakenstelsel op basis waarvan PKIoverheid functioneert. Daarnaast concludeert de Onderzoeksraad dat de betrokken overheidspartijen – in het bijzonder Logius, in mindere mate OPTA – zich onvoldoende inspannen om zicht te krijgen op de feitelijke betrouwbaarheid van certificaatdienstverleners, en hun oordeel in hoge mate baseren op onderzoek door een auditerende instelling. Dit onderzoek is er evenwel niet primair op gericht om vast te stellen of de certificaatdienstverlener aan de voor hem geldende regels voldoet.

De Onderzoeksraad concludeert dat PKIoverheid door de inrichting van het afsprakenstelsel en de wijze waarop de verschillende partijen daarbinnen opereren (zie onder), door een gebrek aan werkelijke grip momenteel niet de toegevoegde waarde biedt die de rijksoverheid ermee beoogde ten opzichte van andere digitale certificaten. Bovendien lijkt PKIoverheid vaak niet aan te sluiten bij de behoefte van overheidsorganisaties, die er daardoor maar beperkt gebruik van maken. Gezien de veiligheidskritische functie van digitale certificaten in het beveiligen van elektronisch gegevensverkeer met en tussen overheidsorganisaties, vindt de Onderzoeksraad dit niet toelaatbaar.[100]

7.2.1 Logius als beheerder van PKIoverheid

De Onderzoeksraad concludeert dat Logius zijn rol als beheerder van PKIoverheid niet zodanig invult dat de beoogde toegevoegde waarde van PKIoverheid-certificaten ten opzichte van andere digitale certificaten gerealiseerd wordt.

Dit betreft in het bijzonder de wijze waarop Logius toeziet op naleving van de contractvoorwaarden die de Staat der Nederland overeenkomt met certificaatdienstverleners die deelnemen aan PKIoverheid. Logius is namens de Staat der Nederlanden de wederpartij in deze overeenkomst, en zou daarom belang moeten hechten aan strikte naleving ervan. Echter, Logius controleert zelf slechts heel beperkt of de certificaatdienstverlener voldoet aan de voorwaarden die de overeenkomst hem oplegt. Het agentschap stelt zich op het standpunt dat het zijn toezicht kan baseren op de audits waartoe de overeenkomst de certificaatdienstverlener verplicht.

Logius marginaliseert zijn eigen rol door zich te kwalificeren als 'derdelijnstoezichthouder'. De Onderzoeksraad is van oordeel dat de organisatie hiermee tekort schiet. Juist omdat de toelating van certificaatdienstverleners tot PKIoverheid in essentie berust op een contractrelatie, heeft het agentschap als wederpartij in deze relatie een sterke positie om naleving van de contractvoorwaarden te bewerkstelligen. Gezien het belang dat de rijksoverheid hecht aan PKIoverheid kan voor Logius het oordeel van de auditor niet volstaan als voornaamste basis voor zijn optreden, maar moet het agentschap zich zelf actief vergewissen van een betrouwbare dienstverlening door de certificaatuitgever, conform de eisen die onder PKIoverheid van toepassing zijn.

7.2.2 OPTA als publieke toezichthouder op gekwalificeerde certificaatdienstverlening

OPTA fungeert als de publieke toezichthouder voor de markt van gekwalificeerde certificaten; daarnaast hanteert de rijksoverheid registratie van een certificaatdienstverlener bij OPTA als voorwaarde voor deelname aan PKIoverheid.

100 Dit onderzoek richt zich op de vraag hoe overheidsorganisaties de digitale veiligheid waarborgen. Ten aanzien van DigiNotar of certificaatdienstverleners in het algemeen trekt de Onderzoeksraad in dit hoofdstuk dan ook geen conclusies. Hetzelfde geldt voor de auditerende instellingen, die in opdracht van de certificaatdienstverleners werken en de kwaliteit van hun bedrijfsvoering certificeren.

De Onderzoeksraad concludeert dat OPTA haar mogelijkheden voor toezicht op en handhaving van de voorwaarden die gelden voor het leveren van gekwalificeerde certificaten als beperkt ervaart, en haar toezichthoudende rol daarom beperkt invult. De Telecommunicatiewet verplicht OPTA om op grond van een geldig bewijs van toetsing te veronderstellen dat een certificaatdienstverlener voldoet aan de wettelijke vereisten. Door dit 'rechtsvermoeden' in de Wet op te nemen, heeft de wetgever de rol van OPTA in het toezicht op certificaatdienstverleners beperkt.

Niettemin is de Onderzoeksraad van mening dat OPTA zich te gemakkelijk in een marginale rol schikt. De Onderzoeksraad verwacht van een publieke toezichthouder dat deze van zich laat horen wanneer de wet- en regelgeving een effectieve taakuitoefening onmogelijk maakt, en ook dat deze de grenzen van zijn bevoegdheden opzoekt als hij dat nodig acht voor een goed functioneren van de sector waarin hij opereert. Hij wijst er in dezen op dat het 'rechtsvermoeden' in de Telecommunicatiewet zijns inziens geen verbod inhoudt voor OPTA om waar nodig door eigen onderzoek vast te stellen of de bij haar geregistreerde certificaatdienstverleners werkelijk aan de wettelijke vereisten voldoen.

7.3 Overheidsorganisaties en digitale veiligheid

7.3.1 Waarborgen digitale veiligheid

De Onderzoeksraad heeft in zijn verkenning grote verschillen aangetroffen in de manier waarop overheidsorganisaties invulling geven aan hun verantwoordelijkheid om de veiligheid van digitale gegevens zo goed mogelijk te waarborgen. Het valt de Onderzoeksraad op dat twee factoren een systematische benadering van digitale veiligheid positief lijken te beïnvloeden. Ten eerste lijken organisaties waar gegevensverwerking wordt ervaren als een centraal onderdeel van het primaire proces de digitale veiligheid beter te waarborgen dan organisaties die gegevensverwerking beschouwen als een instrumentele voorwaarde voor het bereiken van andere organisatiedoelen. Dit geldt bijvoorbeeld voor de Sociale Verzekeringsbank en de Belastingdienst. Ten tweede lijkt de digitale veiligheid in processen en ketens waarop specifieke regelgeving van toepassing is – zoals de GBA of de keten werk en inkomen – beter te zijn gewaarborgd dan waar zulke regelgeving ontbreekt.

Toch pleit de Onderzoeksraad er niet voor om het verwerken van gegevens door overheidsorganisaties strikter te reguleren. Hij is van mening dat een dergelijke aanpak geen duurzaam perspectief op verbetering van de digitale veiligheid biedt, omdat die voorbij gaat aan de eigen verantwoordelijkheid die overheidsorganisaties hebben. De Onderzoeksraad vindt dat zij zelf een aanpak moeten formuleren om digitale veiligheid te waarborgen, die recht doet aan de specifieke context waarin zij opereren.

De Onderzoeksraad krijgt uit de verkenning de indruk dat veel overheidsorganisaties niet of niet systematisch in kaart hebben gebracht welke verschillende soorten gegevens zij verwerken, en welke mate van veiligheid daarvoor passend is. Evenmin lijken zij te inventariseren aan welke bedreigingen deze gegevens bloot staan. Beide zijn naar het oordeel van de Raad een voorwaarde om een beredeneerd besluit te kunnen nemen over de wijze waarop gegevens beveiligd moeten worden, en hoe deze beveiliging het beste kan worden ingericht.

In het algemeen lijkt de tendens bij veel overheidsorganisaties om de digitale veiligheidszorg volledig over te laten aan ICT-deskundigen, binnen dan wel buiten de eigen organisatie. Het bestuurlijk en/of ambtelijk opdrachtgeverschap schiet in zulke gevallen veelal tekort. Bestuurders en hoger management zijn vaak niet in staat de goede vragen te stellen. Doordat zij onvoldoende kennis van en inzicht in de materie hebben om hieraan sturing te kunnen geven, slagen zij er onvoldoende in bestuurlijk-organisatorische waarborgen te realiseren voor digitale veiligheidszorg. De cruciale bestuurlijke beslissingen over digitaal veiligheidsbeleid en risicobeheersing worden nu veelal door de ICT-afdeling genomen en niet door de bestuurlijk verantwoordelijken. Bestuurlijk bestaat er dan ook niet altijd voldoende besef van en inzicht in de digitale veiligheidsrisico's.

Dit onvermogen tot het geven van bestuurlijke sturing aan digitale veiligheidszorg wordt scherper gevoeld nu recente gebeurtenissen zoals het DigiNotarincident de kwetsbaarheid van digitale veiligheid zichtbaar maken, maar veel overheidsorganisaties lijken nog geen manier gevonden te hebben om de gevoelde urgentie om te zetten in concreet handelingsperspectief. Verscheidene aanbevelingen bij dit rapport zien op deze problematiek.

De geldende wet- en regelgeving, branchenormen en contracten geven open normen voor digitale veiligheid. Open normen zijn noodzakelijk in de snel veranderende digitale wereld. Uit het onderzoek blijkt echter dat het voor overheidsorganisaties moeilijk is hieraan concreet invulling te geven. Bestuurlijke betrokkenheid, duidelijke aansturing, expliciete controle en toezicht en voldoende kennis is hiervoor vereist.

De sterk gedigitaliseerde overheid wordt gekenmerkt door een grote afhankelijkheid van het functioneren van ICT-systemen. De onderlinge verwevenheid van deze ICT-systemen maakt dat er weinig overzicht is en een gebrekkige regie. Het DigiNotarincident heeft laten zien dat de digitale overheid kwetsbaarheden kent. Enerzijds kwetsbaarheden voor burgers en bedrijven wier gegevens door de overheid verwerkt worden, anderzijds kwetsbaarheden voor de vitale infrastructuur als ICT-systemen uitvallen door verstoringen. Deze nieuwe kwetsbaarheden zijn van dien aard dat de overheid de regie moet nemen in het beheersen hiervan.

7.3.2 Rijksoverheid als stelselverantwoordelijke

De Onderzoeksraad is van mening dat de rijksoverheid een stelselverantwoordelijkheid heeft voor digitale veiligheid bij overheidsorganisaties. Deze verantwoordelijkheid houdt in dat zij de randvoorwaarden moet scheppen die het individuele overheidsorganisaties mogelijk maken hun verantwoordelijkheid te nemen voor digitale veiligheid. Deze stelselverantwoordelijkheid geldt naar de mening van de Onderzoeksraad voor de gehele publieke sector. Gesteld zou zelfs kunnen worden dat deze verantwoordelijkheid zich uitstrekt tot de samenleving als geheel, gezien de steeds verder toenemende maatschappelijke belangen die zijn gemoeid met digitale veiligheid, en het reële risico dat ook private partijen het maatschappelijk verkeer ernstig kunnen schaden wanneer zij de digitale veiligheid onvoldoende waarborgen.

De rijksoverheid vult haar stelselverantwoordelijkheid momenteel in door de minister van Binnenlandse Zaken en Koninkrijksrelaties een coördinerende bevoegdheid toe te kennen voor de informatievoorziening binnen de rijksdienst. Daarnaast acht de rijksoverheid het haar taak om ook buiten de rijksdienst de digitale veiligheid te stimuleren.

De Onderzoeksraad concludeert op grond van dit onderzoek dat een doortastender invulling door de rijksoverheid van haar stelselverantwoordelijkheid voor digitale veiligheid is gewenst. Door actiever gebruik te maken van haar regelgevende bevoegdheid en haar centrale positie in het openbaar bestuur kan de rijksoverheid verbetering van de digitale veiligheidszorg door alle overheidsorganisaties bevorderen, ook zonder te treden in de autonomie van mede-overheden en zelfstandige bestuursorganen. Diverse aanbevelingen bij dit rapport zien hierop.

8 AANBEVELINGEN

De Onderzoeksraad komt tot de volgende aanbevelingen.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties

1. **Zorg dat bestuurders van alle overheidsorganisaties hun verantwoordelijkheid nemen voor het beheersen van digitale veiligheid.**

   Daartoe moet u een programma ontwikkelen dat bestuurders van overheidsorganisaties doordringt van het belang van digitale veiligheid, en hen voorziet van voldoende inzicht en vaardigheden om hen in staat te stellen actief sturing te geven aan de beheersing van digitale veiligheid in hun organisatie.

   Ook moet u overheidsorganisaties verplichten om zich te verantwoorden over de wijze waarop zij digitale veiligheid waarborgen. Veranker daartoe een duidelijk omschreven openbare verantwoordingsplicht op het gebied van digitale veiligheid in de planning & controlcyclus van overheidsorganisaties, en laat bestuurders van overheidsorganisaties jaarlijks een 'in control statement' voor digitale veiligheid afgeven.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties; aan de minister van Veiligheid en Justitie

2. **Schep voorwaarden zodat overheidsorganisaties hun digitale veiligheid systematisch beheersen.**

   Hiertoe moet u ervoor zorgen dat alle overheidsorganisaties de open standaarden NEN-ISO/IEC 27001 en 27002 naleven, die gezamenlijk een kader voor systematische digitale veiligheidszorg bieden. Stel daarvoor een plan op waarin concrete doelen, maatregelen en een tijdspad worden benoemd. Wijs bovendien een organisatie aan die overheidsorganisaties kan begeleiden bij het tot stand brengen van adequate digitale veiligheidszorg.

   Als onderdeel van een dergelijke systematische aanpak moet vanuit gemeenten, veiligheidsregio's en het Rijk aandacht bestaan voor het voorbereid zijn op, en het herstellen van schade als gevolg van, digitale incidenten. Burgers en bedrijven wier gegevens door een digitaal veiligheidsincident zijn getroffen, moeten kunnen volstaan met dit één keer te melden waarna adequate maatregelen moeten worden getroffen door alle betrokken overheidsorganisaties.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties; aan de minister van Economische Zaken, Landbouw en Innovatie

3. Realiseer een veiliger uitgifte en gebruik van digitale certificaten.

Pas hiervoor de rol van OPTA en Logius zodanig aan, dat sprake is van werkelijk toezicht op en handhaving van de feitelijke naleving door certificaatdienstverleners van de vigerende regelgeving ten aanzien van gekwalificeerde en PKIoverheid-certificaten.

Bevorder daarnaast een cultuuromslag bij alle partijen die bij certificaatdienstverlening betrokken zijn, in het bijzonder ten aanzien van het melden en leren van incidenten. Maak daarbij gebruik van ervaringen met veilig melden uit andere sectoren.

Bestuursorganen aan wie een aanbeveling is gericht dienen een standpunt ten aanzien van de opvolging van deze aanbeveling binnen een half jaar na verschijning van deze rapportage aan de betrokken minister kenbaar te maken. Niet-bestuursorganen of personen aan wie een aanbeveling is gericht dienen hun standpunt ten aanzien van de opvolging van de aanbeveling binnen een jaar kenbaar te maken aan de betrokken minister. Een afschrift van deze reactie dient gelijktijdig aan de voorzitter van de Onderzoeksraad voor Veiligheid en de minister van Veiligheid en Justitie verstuurd te worden.

BIJLAGE 1: ONDERZOEKSVERANTWOORDING

Onderzoek door de Onderzoeksraad voor Veiligheid
De Onderzoeksraad voor Veiligheid doet onafhankelijk onderzoek naar de oorzaken van voorvallen, met als doel daarvan te leren. Het onderzoek van de Onderzoeksraad is niet alleen gericht op het identificeren van feitelijke oorzaken, maar vooral ook op het aan het licht brengen van achterliggende oorzaken en eventuele tekortkomingen op systeemniveau.

De Onderzoeksraad beslist zelf waarnaar hij onderzoek doet. In het geval van dit onderzoek was sprake van een verzoek in de zin van art. 43 van de Rijkswet Onderzoeksraad voor Veiligheid, gedaan door de minister van Binnenlandse Zaken en Koninkrijksrelaties mede namens de minister van Veiligheid en Justitie. Deze ministers verzochten de Onderzoeksraad "het DigiNotar en andere incidenten te onderzoeken, en in meer algemene zin het stelsel te beoordelen waarin betrokken partijen de digitale veiligheid waarborgen van (internet)communicatie tussen burgers en de overheid." De Onderzoeksraad heeft in dit verzoek bewilligd. De redenen hiervoor, evenals de centrale vraagstelling en de afbakening van het onderzoek, zijn aangegeven in Hoofdstuk 1 van dit rapport.

Dit onderzoek heeft ten doel een bijdrage te leveren aan het verhogen van bewustwording bij overheidsorganisaties en burgers omtrent digitale veiligheid, de daarbij optredende risico's en hun gevolgen. Anderzijds beoogt het onderzoek concreet bij te dragen aan het verbeteren van de staat van digitale veiligheid bij de overheid, private partijen en burgers.

Onderzoeksaanpak
Het onderzoek kende twee fasen: een oriënterende fase en een onderzoeksfase. In de oriënterende fase heeft het onderzoeksteam zich enerzijds gericht op het verkrijgen van nadere kennis van en inzicht in de relevante onderwerpen voor het onderzoek, waaronder de werking van bestaande methoden en technieken voor versleuteling van digitale gegevensuitwisseling en authenticatiemechanismen. Daarnaast heeft het team zich gericht op een brede oriëntatie van de relevante spelers en (overheids-)partijen op het gebied van digitale veiligheid in Nederland en de door hen gepercipieerde problemen, aandachtspunten en knelpunten daarbij. Deze fase heeft geresulteerd in het formuleren van de centrale onderzoeksvraag, het vaststellen van de reikwijdte van het onderzoek en het formuleren van een plan van aanpak voor de onderzoeksfase.

Tijdens de onderzoeksfase zijn drie deelonderzoeken uitgevoerd. De gevolgde werkwijze voor elk deelonderzoek wordt hieronder kort beschreven.

Het eerste deelonderzoek was gericht op een reconstructie van de gebeurtenissen die vooraf gingen aan en volgden op het bekend worden van de inbraak in de computersystemen van DigiNotar in september 2011, om te kunnen beoordelen hoe betrokken partijen omgingen met het risico op oneigenlijk gebruik van digitale certificaten. Als onderdeel van dit deelonderzoek is onder meer het verloop van de gebeurtenissen tijdens de casus in kaart gebracht. Ook is onderzocht hoe de verschillende betrokken partijen hebben gehandeld, wat deze handelwijze verklaart en hoe die zich verhoudt tot de verantwoordelijkheden die de partijen ten aanzien van certificaatdienstverlening hebben.

De Onderzoeksraad heeft geen eigen technisch onderzoek laten doen naar de inbraak bij DigiNotar. De exacte technische redenen waarom de inbreker zo diep in de bedrijfssystemen kon doordringen, zijn naar het oordeel van de Onderzoeksraad van minder belang dan de vraag hoe het kon gebeuren dat de beveiliging van het bedrijf kennelijk ontoereikend was om een dergelijke aanval te weerstaan, en waarom de partijen die toezagen op de certificaatdienstverlening door DigiNotar dit niet hebben opgemerkt. Kennis van de specifieke technische details van de inbraak is niet nodig om deze vragen te beantwoorden. Wel is gebruik gemaakt van technisch onderzoek waartoe DigiNotar zelf opdracht heeft gegeven, om een globaal beeld te krijgen van het verloop van de inbraak.

Het tweede deelonderzoek was gericht op de vraag in hoeverre de inrichting van PKI-stelsels, waarin certificaatdiensten worden geleverd, de digitale veiligheid waarborgt. Als onderdeel van dit deelonderzoek is onder meer onderzocht wat de historische achtergrond is van de verschillende 'regimes' voor certificaatdienstverlening, hoe deze zich tot elkaar verhouden, hoe deze stelsels zijn ingericht, welke typen digitale certificaten in gebruik zijn bij overheidsorganisaties, en of sprake is van zwakke plekken.

Ten derde heeft de Onderzoeksraad verkend hoe overheidsorganisaties digitale veiligheid bestuurlijk-organisatorisch vormgeven en borgen. In dit deelonderzoek is onder meer onderzocht hoe overheidsorganisaties omgaan met digitale veiligheid en deze borgen in hun organisaties, welke afwegingskaders en beheersmaatregelen worden gehanteerd, en of sprake is van knelpunten en verbetermogelijkheden voor de wijze waarop zij digitale veiligheid waarborgen.

Daartoe zijn vijf gemeenten en twee uitvoeringsorganisaties op rijksniveau, te weten de Sociale Verzekeringsbank (SVB) en de Belastingdienst, bereid gevonden mee te werken aan deze verkenning. De selectie van gemeenten is in overleg met de Vereniging Nederlandse Gemeenten (VNG) en het Kwaliteits Instituut Nederlandse gemeenten (KING) tot stand gekomen. De gemeenten waren bereid aan de verkenning deel te nemen op voorwaarde van anonimiteit. Bij de deelnemende organisaties zijn diverse functionarissen op verschillende bestuurlijke- en managementniveaus geïnterviewd en is relevante documentatie opgevraagd en bestudeerd. Er is ook een gemeentelijk samenwerkingsverband in de verkenning betrokken.

Alle organisaties werkten vrijwillig mee aan de verkenning. Er was bij geen van deze organisaties sprake van een incident als reden voor medewerking aan de verkenning. Wel hebben deze organisaties op verschillende manieren nadelige gevolgen ondervonden van het DigiNotarincident of de Lektober-actie, waardoor zij gemotiveerd waren om hun ervaringen en inzichten te delen met de Onderzoeksraad.

Om enig inzicht te verkrijgen in de omgang met digitale veiligheid door private partijen zijn bovendien gesprekken gevoerd met vertegenwoordigers van enkele Nederlandse banken.

Onderzoeksmethodiek
In het onderzoek is gebruik gemaakt van kwalitatieve onderzoeksmethoden, waaronder literatuurstudie, interviews en rondetafelgesprekken. De literatuurstudie bestond uit het bestuderen en analyseren van openbare informatie zoals (inter-)nationale wet- en regelgeving, normen, kaders en richtlijnen. Daarbij zijn ook relevante publicaties en studies van onderzoeks- en overheidsinstanties, artikelen in tijdschriften, websites en internetfora betrokken. Daarnaast is gebruik gemaakt van documentatie van de bij het onderzoek betrokken partijen, waaronder beleidsdocumenten over informatiebeveiliging, handboeken, interne rapportages, verslagen van verschillende soorten overleggen, auditrapporten en notities.

De interviews vonden plaats op basis van semigestructureerde vragenlijsten waarbij betrokkenen werden uitgenodigd te reflecteren op:

- De werking van de PKI-stelsels in het algemeen, de vigerende regelgeving en normen, de wijze van toezicht evenals de ervaren knelpunten en verbetermogelijkheden van deze aspecten;
- de achtergrond en relevante omstandigheden die tot het incident leidden;
- de impact en de wijze waarop binnen de organisaties is omgegaan met de gevolgen van het incident en de daaruit te trekken lessen;
- de wijze waarop de organisaties en de betrokken functionarissen informatiebeveiliging en risicomanagement vormgeven en uitvoeren, de ervaren knelpunten en verbetermogelijkheden die zij zien;
- hoe betrokken partijen aankijken tegen digitale veiligheid in het algemeen en de wijze waarop deze geborgd kan worden en welke rol partijen daarbij kunnen en moeten spelen in het bijzonder.

In het derde deelonderzoek zijn bovendien twee verdiepende rondetafelgesprekken georganiseerd met referentiegemeenten: één met enkele burgemeesters en wethouders en één met vertegenwoordigers van de ambtelijke organisaties, waaronder gemeentesecretarissen. Doel van deze bijeenkomsten was de terugkoppeling van de bevindingen uit de verkenning bij gemeenten te toetsen en te verbreden.

Overige onderzoeken en rapporten naar aanleiding van het DigiNotarincident
Naar aanleiding van de inbraak bij DigiNotar en de nasleep zijn door uiteenlopende organisaties onderzoeken en vanuit verschillende invalshoeken studies verricht. Een aantal van deze rapporten was vertrouwelijk. De bevindingen zijn door Onderzoeksraad in het onderzoek betrokken en verder geanalyseerd.

Afstemming met de Inspectie Veiligheid en Justitie
De Inspectie Veiligheid en Justitie is naar aanleiding van het DigiNotar incident in september 2011 een eigen onderzoek gestart. De Inspectie Veiligheid en Justitie is vrijwel direct na het incident door de minister Ministerie van Veiligheid en Justitie gevraagd om onderzoek te doen naar de structuur van de crisisopschaling. De onderzoeken van Inspectie Veiligheid en Justitie en de Onderzoeksraad richten zich op dezelfde casus, maar hebben een andere invalshoek en vraagstelling. De afspraak is gemaakt beide onderzoeken gelijktijdig te publiceren. De Inspectie Veiligheid en Justitie richt zich op de vraag hoe de crisis rondom de hack werd beheerst. De Onderzoeksraad richt zich op de vraag hoe deze gebeurtenissen konden ontstaan.

Begeleidingscommissie
De Onderzoeksraad heeft voor dit onderzoek een begeleidingscommissie in het leven geroepen. Deze commissie bestond uit externe leden met voor het onderzoek relevante deskundigheid onder voorzitterschap van twee leden van de Onderzoeksraad. De externe leden hadden op persoonlijke titel zitting in de begeleidingscommissie. Gedurende het onderzoek is de commissie drie keer bijeengekomen om met de raadsleden en het projectteam van gedachten te wisselen over de opzet en de resultaten van het onderzoek. De commissie vervulde een adviserende rol binnen het onderzoek. De eindverantwoordelijkheid voor het rapport en de aanbevelingen ligt bij de Onderzoeksraad. De commissie was als volgt samengesteld.

prof. mr. dr. E.R. Muller (voorzitter)	Onderzoeksraad voor Veiligheid
prof. dr. ing. F.J.H. Mertens (vice-voorzitter)	Onderzoeksraad voor Veiligheid
prof. dr. ir. E. Huizer	SURFnet / Universiteit Utrecht
prof. dr. B.P.F. Jacobs	Radboud Universiteit Nijmegen
drs. S.M. Roos	Lid Raad voor de rechtspraak
mr. B.B. Schneiders	Burgemeester Haarlem
prof. dr. W.Ph. Stol	NHL Hogeschool / Politieacademie / Open Universiteit
prof. dr. Y.H. Tan	TU Delft
drs. L.J. Wijngaarden	Commissaris SNS Reaal

Projectteam
Het onderzoek is uitgevoerd onder verantwoordelijkheid van mw. dr. A. Nelis, onderzoeksmanager van het cluster gezondheid, crisisbeheersing en onderzoek & ontwikkeling.

drs. W.J. van Helden	projectleider
R.J.H. Damstra	onderzoeker
drs. M.F. Jager, MSHE	onderzoeker
P.P. Lips	onderzoeker
H. Possel	onderzoeker
ing. T.T. van Prooijen	onderzoeker
dr. N. Smit	onderzoeker
drs. W.A.A. Verhoeff	onderzoeker
drs. H.J.A. Zieverink	onderzoeker
ing. P.A. Keur, MSc (Zenc)	onderzoeker
ing. A. van Nuil, RI (BMC)	onderzoeker

BIJLAGE 2: INZAGEREACTIES

Een conceptversie van dit rapport is, conform artikel 56 van de Rijkswet Onderzoeksraad voor veiligheid, voorgelegd aan de betrokken partijen. Deze partijen is gevraagd het rapport te controleren op feitelijke onjuistheden en eventuele omissies.

De meeste partijen hebben gebruik gemaakt van de gelegenheid te reageren. Het commentaar heeft in veel gevallen wel, maar in sommige gevallen niet geleid tot aanpassing van het rapport. De reacties die niet hebben geleid tot aanpassing van het rapport zijn opgenomen in een tabel, waarbij tevens is opgenomen waarom de reactie niet is verwerkt. Deze tabel is te vinden op de website van de Onderzoeksraad: www.onderzoeksraad.nl.

BIJLAGE 3: GERAADPLEEGDE LITERATUUR

In deze bijlage zijn alleen documenten opgenomen die openbaar toegankelijk zijn. Wetten, regels en normdocumenten zijn niet opgenomen.

Algemene Rekenkamer (2009). Weloverwogen toezicht. Analyse van departementale toezichtvisies. RWT-verkenningen deel 2.

Algemene Rekenkamer (2010). Rechtmatigheidsonderzoeken bij de departementale jaarverslagen 2010.

Baarsma, Barbara et al. (2003). Zelf doen? Inventarisatie van zelfreguleringinstrumenten. Onderzoek in opdracht van het ministerie van Economische Zaken. Amsterdam: SEO.

Broeders, Dennis, Colette Cuijpers en Corien Prins (2011). *De staat van informatie*. Verkenningen van de Wetenschappelijke Raad voor het Regeringsbeleid. Amsterdam: Amsterdam University Press.

CIO Platform Nederland (2007). Informatie Beveiliging in control.

Collis en HEC (2012). Eindrapport Onderzoek veiligheid diensten in de Digitale Agenda.nl. Onderzoek in opdracht van het ministerie van Economische Zaken, Landbouw en Innovatie. Kamerstuk TK 26643-230.

Commissie Gemeentelijke Dienstverlening (2005). Eindrapport Publieke dienstverlening, professionele gemeenten – Visie 2015. Rapport in opdracht van de Vereniging Nederlandse Gemeenten.

Commissie Postma/Wallage (2007). Het uur van de waarheid. Advies over regie en sturing van de elektronische overheid.

CP-ICT Inwonerszaken (2009). Informatiebeveiliging gemeenten. Handreiking beleid en organisatie Strategisch niveau.

Expertcommissie informatievoorziening en elektronische dienstverlening SUWI (2005). De burger bediend. Rapport in opdracht van de minister van Sociale Zaken en Werkgelegenheid. Kamerstuk TK 26448-206.

Forum Standaardisatie (2010). Expertadvies, PvE PKIoverheid deel 3a t/m 3d, versie 2.1.

Fox-IT B.V. (2011). DigiNotar Certificate Authority breach. Operation "Black Tulip". Interim-rapport d.d. 5 september 2011. In opdracht van DigiNotar B.V., later in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Bijlage bij Kamerstuk TK 26643-188.

Hert, Paul de (2011). Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting. In Broeders et al., pp. 33-96.

Hintzbergen, K., A. Smulders en H. Baars (2011). *Basiskennis beveiligen van informatie op basis van ISO27001 en ISO27002*. Zaltbommel: Van Haren Publishing.

IT Governance Institute (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management*. 2nd edition.

Logica Business Consulting (2012). Evaluatie PKI. Rapportage in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Economische Zaken, Landbouw en Innovatie. Kamerstuk TK 26643-230.

Logius (2012). Handreiking Betrouwbaarheidsniveaus voor elektronische overheidsdiensten.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2012). Brief aan de Tweede Kamer over onderzoeken naar aanleiding van DigiNotar, d.d. 14 maart 2012. Kamerstuk TK 26643-230.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2011). Informatiseringsstrategie rijksoverheid. Brief aan de Tweede Kamer d.d. 15 november 2011. Kamerstuk TK 26643-216.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2011). Kabinetsreactie op het rapport *iOverheid* van de Wetenschappelijke Raad voor het Regeringsbeleid. Kamerstuk TK 26643-211.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2011). Overheidsbrede implementatieagenda voor dienstverlening en e-overheid. Kamerstuk TK 26643-182.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2009). Modernisering van de overheid. Brief aan de Tweede Kamer over het Nationaal Uitvoeringsprogramma dienstverlening en e-overheid (NUP), d.d. 9 januari 2009. Kamerstuk TK 29362-148.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2008). Bestuursakkoord rijk en provincies 2008-2011. Aangeboden aan de Tweede Kamer op 26 november 2008. Kamerstuk TK 31700VII-44.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2007). Brief aan de Tweede Kamer inzake het kabinetsplan aanpak administratieve lasten, d.d. 25 juni 2007. Kamerstuk TK 29362-120.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2007). Samen aan de slag. Bestuursakkoord rijk en gemeenten 2007-2011. Aangeboden aan de Tweede Kamer op 5 juni 2007. Kamerstuk TK 30800B-17.

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2003). Actieprogramma andere overheid. Kamerstuk TK 29362-1.

Minister van Economische Zaken, Landbouw en Innovatie (2011). Digitale agenda.nl 2011-2015. Kamerstuk TK 29515-331.

Minister voor Grote Steden- en Integratiebeleid (2000). Actieprogramma Elektronische Overheid. Kamerstuk TK 26387-9.

Minister van Veiligheid en Justitie (2011). Nationale Cyber Security Strategie. Kamerstuk TK 26643-174.

Minister van Veiligheid en Justitie (2011). Cybersecuritybeeld Nederland December 2011. Kamerstuk TK 26643-220.

Minister van Veiligheid en Justitie (2010). Bevindingenrapportage Nationale Risicobeoordeling. Kamerstuk TK 30821-12.

Minister van Veiligheid en Justitie (2010). Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010. Kamerstuk TK 28684-292.

Ministers van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Financiën, Justitie, Onderwijs, Cultuur en Wetenschappen en Verkeer en Waterstaat (1999). De Digitale Delta: Nederland oNLine. Kamerstuk TK 26643-1.

Noordegraaf-Eelens, Liesbeth, Paul Frissen en Martijn van der Steen (2010). De crisis van het vertrouwen en het vertrouwen na de crisis. De risico's van het vertrouwen op vertrouwen. Verkenning in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 's-Gravenhage: Nederlandse School voor Openbaar Bestuur.

Oud, Ernst J. (2011). *Praktijkgids Code voor informatiebeveiliging*. 's-Gravenhage: Sdu Uitgevers.

Platform voor Informatiebeveiliging (2008). Basiskennis beveiligen van informatie.

Rijksauditdienst (2012). De zaak 'DigiNotar': handelde de overheid adequaat? Rapport naar de alertheid en adequaatheid van het handelen van de overheid ten tijde van de 'DigiNotar'-problematiek. In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Kamerstuk TK 26643-230.

Van Eeten, M. (2011). Gedijen bij onveiligheid, afwegingen rond de risico's van informatietechnologie. In Broeders et al., pp. 133-164.

VIAG (2005). Handboek Informatiebeveiliging.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for High Reliability: Processes of Collective Mindfulness. In B. M. Staw & L. L. Cummings (Eds.), *Research in Organizational Behavior*, pp. 81-123. Greenwich, CT: JAI Press, Inc.

Wetenschappelijke Raad voor het Regeringsbeleid (2011). iOverheid, rapport 89. 's-Gravenhage / Amsterdam: Amsterdam University Press.

Zouridis S. et al. (2004). Een open tunnelvisie. Evaluatie van het nationaal TTP-beleid, in opdracht van het ministerie van Economische Zaken. Kamerstuk TK 26581-3.

Onderzoeksraad voor Veiligheid

telefoon (070) 333 70 00 • **e-mail** info@onderzoeksraad.nl • **internet** www.onderzoeksraad.nl

bezoekadres Anna van Saksenlaan 50 • 2593 HT Den Haag • **postadres** Postbus 95404 • 2509 CK Den Haag