Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

De voorzitter van de Onderzoeksraad voor de Veiligheid,
Dhr. Mr. T. Joustra
Postbus 95404
2509 CK Den Haag

DGBK | B&I
Informatie

Schedeldoekshaven 200
2511 EZ Den Haag

Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Kenmerk
2012-0000630589

Datum 12 november 2012
Betreft Reactie op het onderzoeksrapport van de Onderzoeksraad voor de Veiligheid inzake "Het DigiNotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt".

Geachte voorzitter van de Onderzoeksraad voor de Veiligheid,

Hierbij doe ik U, mede namens de Minister van V&J, mijn reactie toekomen op het onderzoeksrapport van de Onderzoeksraad voor de Veiligheid inzake "Het DigiNotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt".

Allereerst wil ik de Onderzoeksraad voor de Veiligheid (OVV) danken voor haar gedegen rapport over deze complexe materie. Het karakter van het DigiNotar incident geeft aan hoe indringend de invloed van informatie- en communicatietechnologie op de samenleving geworden is; elektronische certificaten, technisch hoogwaardig beveiligingsmiddelen, die een decennium geleden nog nauwelijks gebruikt werden, gebaseerd op een zogenaamde Public Key Infrastructure, blijken inmiddels onmisbaar voor onze dagelijkse werkprocessen. Digitale informatie en informatievoorziening zijn doorgedrongen in de haarvaten van onze maatschappij, en dus ook in die van de overheid. Voor de informatievoorziening binnen de overheid heb ik als Minister van BZK, sinds de jaren tachtig, een coördinerende rol. Deze rol is primair zichtbaar bij de Chief Information Officer (CIO)-Rijk in het Directoraat-generaal Organisatie en Bedrijfsvoering Rijk, die voor de Rijksoverheid samen met de CIO's van de departementen werkt aan stroomlijning en coördinatie van informatievoorziening. Daarnaast word ik door de Tweede Kamer aangesproken op de informatiebeveiliging bij de medeoverheden. De medeoverheden zijn en blijven echter zelf verantwoordelijk voor hun informatiebeveiliging. Dit geldt tevens voor de overige onderdelen van de publieke sector, die onder de coördinerende verantwoordelijkheid van de desbetreffende vakdepartementen vallen, en waarvoor ik uiteraard niet aanspreekbaar ben en kan zijn.
De grote afhankelijkheid van digitale informatie en informatievoorziening maakt het belang van een goede informatiebeveiliging en de daarbij horende noodprocedures des te pregnanter. Het DigiNotar incident is dan ook een "wake-up call" geweest. En de ervaringen met Lektober vorig jaar hebben voor extra commitment gezorgd waar het gaat om informatiebeveiliging, zowel bij de Rijksoverheid als bij de medeoverheden.

Ik zal in mijn reactie ingaan op de drie hoofdaanbevelingen (telkens bestaande uit twee punten) die de OVV doet zonder daarbij onrecht te willen doen aan de vele detailconclusies die ook in het rapport vermeld zijn. Het is mijn stellige overtuiging dat er, waar het gaat om de geconstateerde tekortkomingen bij het toezicht op de PKI stelsels, nu voortvarend wordt doorgepakt om deze tekortkomingen te adresseren en op te lossen. Zoals mijn ambtsvoorganger ook in mijn brief van 14 maart 2012 aan de Tweede Kamer heeft gemeld[1] over de drie andere onderzoeken die uitgevoerd werden naar aanleiding van het DigiNotar incident, zijn en worden er reeds vele maatregelen genomen. In die zin zie ik het rapport van de OVV dan ook als de bevestiging van de noodzakelijke aanpassingen voor een betere en robuustere infrastructuur.

Aanbevelingen uit het rapport en reactie minister(s):

De OVV vraagt de Rijksoverheid actiever gebruik te maken van haar regelgevende bevoegdheid ten aanzien van de stelselverantwoordelijkheid informatiebeveiliging voor de gehele overheid.

De eerste aanbeveling van de OVV:
1.1. De OVV vraagt om een programma te ontwikkelen om bestuurders te doordringen van het belang van digitale veiligheid en hen te voorzien van voldoende inzicht en vaardigheden.
1.2. De OVV vraagt om een door mij in te vullen verantwoordingsverplichting op het gebied van digitale veiligheid.

Ten aanzien van punt 1.1 wil ik graag het volgende opmerken. Ik onderschrijf het belang van digitale veiligheid en het besef van de noodzaak daarvan op bestuurlijk niveau. Het is van belang om hier een gerichte inhaalslag te maken. Ik zal dan ook een Taskforce instellen, voor een periode van twee jaar, die zich specifiek gaat richten op de bewustwording van bestuurders en hoger management, daar waar het gaat om nut en noodzaak van informatiebeveiliging.
Deze Taskforce zal zich gaan richten op het openbare bestuur, dus zowel Rijk- als medeoverheden. De Taskforce zal zich dus niet richten op andere organisaties binnen de publieke sector, daarvoor zijn de desbetreffende vakministers verantwoordelijk. De taak van de Taskforce zal zijn om bestuurders en hoger management te ondersteunen en handreikingen te bieden. Hierbij zal worden samengewerkt met het Nationaal Cyber Security Centrum (NCSC).
In de eerste plaats met het doel om bestuurders en hoger management bewust te maken van het belang van een betrouwbare en veilige informatiehuishouding. Maar ook om hen te wijzen op het belang van supervisie op en aansturing van de genomen en te nemen informatiebeveiligingsmaatregelen. Het is immers hun belang en hun taak om dit in de eigen organisatie adequaat te regelen. De Taskforce zal in zijn benadering aansluiten bij de werkelijkheid van bestuur en management van de deelnemende organisaties en op reeds bestaande activiteiten binnen het Rijk, zoals de ABD TopClass voor het hoogste managementniveau waarin ook informatiebeveiliging een belangrijke plaats heeft.
Mede aan de hand van de resultaten van de uit te voeren assessments op de informatiebeveiliging van organisaties die DigiD gebruiken, zal een gezamenlijke verkenning uitgevoerd worden naar de verschillende aspecten van digitale dienstverlening in het perspectief van digitale veiligheid. Ook de inrichting van de signalerings- en crisisbeheersingsfunctie zal daarbij aan de orde komen. De Taskforce zal daarbij de reeds aanwezige kennis en expertise in goed functionerende organisaties zo veel mogelijk betrekken.
Deze Taskforce zal snel aan de slag gaan. Dat toont de urgentie die ik aan dit onderwerp hecht. Ik wil niet wachten totdat er wet- en regelgeving tot stand is gekomen, wat altijd geruime tijd vergt. Bovendien acht ik het veel belangrijker dat er een omslag in het denken plaatsvindt, waarbij informatiebeveiliging standaard

[1] *Kamerstukken II 2011-2012, 22643 no. 230*

wordt meegenomen bij het inrichten en onderhouden van informatiesystemen. En die omslag wordt veel sneller en beter gerealiseerd door een Taskforce zoals nu wordt ingesteld, dan door het enkel opleggen van regels. Dat wil niet zeggen dat ik wet- en regelgeving uitsluit. De periode van twee jaar zal tevens gebruikt worden om een analyse te maken van bestaande en noodzakelijke wet- en regelgeving, inclusief de handhaving van al bestaande regels. Mocht bij de voorziene evaluatie van de Taskforce blijken dat het gewenste resultaat niet bereikt is, dan zal ik mij nader beraden over mogelijke wet- en regelgeving. Ik zal u deze evaluatie dan ook doen toekomen.

Met de Taskforce zal ik tevens aansluiten bij de initiatieven die binnen de Rijksoverheid, maar ook binnen de medeoverheden opstarten of gestart zijn waar het gaat om informatiebeveiliging. Binnen de Rijksoverheid wordt de invoering van de Baseline informatiebeveiliging Rijk op korte termijn voorzien. Deze algemene Baseline treedt in de plaats van een groot aantal bestaande baselines; het betreft departementale baselines en een aantal specifieke interdepartementale baselines. Hierdoor wordt het basisbeveiligingsniveau bij de Rijksdienst gelijkgetrokken en ontstaat eenduidigheid over dit basisniveau. Bij zowel de VNG als de Manifestpartijen zijn er initiatieven voor het instellen van informatiebeveiligings-steunpunten. Binnen de VNG/KING samenwerking bevindt de gemeentelijke Informatiebeveiligingsdienst (IBD) zich in de kwartiermakerfase. Vanuit BZK en V&J wordt de ontwikkeling van deze dienst actief verwelkomd. Met de IBD wordt invulling gegeven aan de eigen verantwoordelijkheid van gemeenten. Het ligt in lijn met het vanuit het NCSC geïnitieerde Programma Nationaal Response Netwerk. Het doel van dit programma is het vergroten van de weerbaarheid van de Nederlandse samenleving door het creëren en stimuleren van een netwerk van response-organisaties binnen Nederland. Hiermee wordt een belangrijke stap gezet in de landelijke ontwikkeling van sectorale capaciteiten op het gebied van ICT-response. Deze ontwikkeling geeft een impuls aan de verbintenis tussen het NCSC en partijen buiten de primaire doelgroep (Rijksoverheid en vitale sectoren) van het NCSC. Niet alleen kunnen langs deze weg verschillende sectoren binnen de eigen verantwoordelijkheid zelfstandig digitale weerbaarheid vergroten, ook wordt hiermee de uitrol van een effectief landelijk netwerk van sectorale informatiebeveiligingsdiensten gestimuleerd.
De Taskforce zal ook aansluiting zoeken bij bestaande, meer algemene, initiatieven, zoals het al genoemde ABD Topclass programma.

Ten aanzien van punt twee van de eerste aanbeveling, de verantwoordingsplicht bij mede overheden[2] zie ik deze verantwoordingsplicht als een normaal onderdeel van de bestuurlijke verantwoordelijkheid. Een maatregel die organisaties zelf kunnen nemen is bijvoorbeeld het aanvullend meenemen van het onderwerp informatiebeveiliging in de auditcycli die organisaties uitvoeren op basis van andere verplichtingen. Binnen de Taskforce zal dit meegenomen worden als belangrijk aandachtpunt voor bestuurders en hoger management. Immers als men supervisie voert over zijn informatiehuishouding dient men ook de juiste informatie te hebben voor de oordeelsvorming.

De tweede aanbeveling van de OVV (Gericht aan Min BZK en Min V&J)

De tweede aanbeveling vraagt om:

1. Zorg te dragen voor naleving van open standaarden ten aanzien van informatiebeveiliging, met een planning, en een aangewezen organisatie die overheidsorganisaties kan begeleiden.

[2] *(de Rijksoverheid verantwoordt zich in de slotwetten van de Ministeries en de Algemene Rekenkamer besteedt in haar beoordeling periodiek specifieke aandacht aan informatiebeveiliging)*

2. Aandacht voor voorbereiding op en herstel van schade bij digitale incidenten, inclusief het eenmalig melden van incidenten waarna adequate maatregelen getroffen worden door alle betrokken overheidsorganisaties.

Ten aanzien van het eerste deel van de tweede aanbeveling heb ik in het voorgaande al gemeld dat de VNG in samenwerking met KING is overgegaan tot het instellen van een informatiebeveiligingsdienst (IBD) ter ondersteuning van gemeenten, en dat het Uitvoeringsinstituut Werknemersverzekeringen (UWV) samen met ketenpartners het Centrum Informatiebeveiliging en Privacybescherming (CIP) heeft opgezet. Doel van dit centrum is het weerbaarheids-, herstel- en leervermogen van zelfstandige bestuursorganen (zbo's en uitvoeringsinstellingen van het Rijk) rond cyber security te versterken. Beide initiatieven zullen samenwerken met het NCSC. Aangezien de open standaarden voor informatiebeveiliging ISO 27001 en ISO 27002 al op de '"Comply or Explain""(Pas-toe-of-leg-uit')-lijst van het Forum Standaardisatie zijn opgenomen als verplichte standaarden voor de hele overheid, ligt het in de rede dat deze standaarden in voornoemde organisaties de belangrijke leidraad zullen zijn voor het handelen. Binnen de Rijksoverheid zijn deze standaarden uitgewerkt in de voorziene Baseline Informatiebeveiliging Rijk (BIR).
Tevens zal er dit jaar een baseline informatiebeveiliging voor gemeenten worden ontwikkeld, die aansluit bij de baseline van de Rijksoverheid.
Beide standaarden behelzen ook de noodzakelijke voorbereiding op en herstelplannen voor verstoringen en schade. Ten aanzien van dit laatste punt kan ik niet genoeg benadrukken hoe belangrijk het hebben van deze herstelplannen is. Een goede informatiebeveiliging behelst niet alleen het voorkomen van, maar ook het mitigeren van eventuele beveiligingsincidenten. Daarbij spelen risicoanalyses een belangrijke rol, want 100% beveiligen kan niet, maar voorbereid zijn op eventuele verstoringen kan wel. Recentelijk heeft het Dorifel-virus het belang hiervan opnieuw aangetoond. Ik zal dan ook extra aandacht laten schenken door de Taskforce aan bewustwording op dit gebied.
Binnen de werkzaamheden in het kader van de Taskforce zal het belang van de ISO-standaarden bij de bestuurders worden beklemtoond. Daarnaast voorziet het NCSC in (operationele) richtlijnen en beveiligingsadviezen om tot een gerichte aanpak te komen. Deze zijn breder beschikbaar gesteld. Deze activiteiten dragen eveneens bij aan de gewenste bewustwording.

Ten aanzien van meldplicht merk ik op dat door de Minister van V&J begin juli dit jaar een brief[3] is gestuurd aan de Tweede Kamer inzake Security Breach Notification met daarin een aangekondigde wettelijke regeling voor een meldplicht ICT-incidenten. In 2012 zal een wettelijke regeling worden opgesteld waarbij randvoorwaardelijke sectoren, alsook de financiële sector en de overheid ertoe verplicht zijn om binnen de scope van de meldplicht melding te doen aan de sectorale toezichthouder, dan wel het NCSC. Het NCSC zal de organisatie of de sector hulp en advies bieden om de inbreuk te dichten en effecten van de inbreuk, die ook elders kunnen plaatsvinden, in te dammen. Voor de burger is sinds 2009 het Centraal Meld- en Informatiepunt Identiteitsfraude en fouten actief. Dit meldpunt verricht mede een regisseursrol naar andere overheden indien fraude wordt geconstateerd.

De derde aanbeveling van de OVV (gericht aan Min BZK en Min EZ)

De derde aanbeveling gaat over digitale certificaten en vraagt om:

1. werkelijk toezicht op en handhaving door OPTA en Logius van de feitelijke naleving van vigerende regelgeving, en:
2. het bevorderen van een cultuuromslag ten aanzien van het melden van incidenten

[3] *Kamerstukken II 2011-2012, 26643 no. 247*

Op beide punten is reeds actie ondernomen.

Ten aanzien van het eerste punt: als opvolging van de eerdere onderzoeken heeft Logius, in haar rol als Policy Authority het programma van eisen bijgesteld. De samenwerking tussen OPTA, Logius en de auditor is verbeterd. In een tweemaandelijks overleg wordt de stand van zaken bij de certificatiedienstverleners besproken. Verder hebben OPTA en Logius een samenwerkingsconvenant ondertekend waardoor het toezicht wordt versterkt. Zo leggen Logius en OPTA samen bedrijfsbezoeken af.

OPTA heeft meer capaciteit gekregen om het toezicht op gekwalificeerde certificaten te intensiveren. OPTA maakt momenteel voor alle certificatiedienstverleners een risicoanalyse op grond waarvan gericht toezicht wordt gehouden op de onderdelen van dienstverlening waarvan de risico's het grootst zijn. OPTA gebruikt daarbij ook de auditrapporten. Dit levert een startpunt voor de bedrijfsbezoeken bij de certificatiedienstverleners, die minstens één keer per jaar plaatsvinden, en tussentijdse correspondentie. Daarnaast heeft OPTA alle certificatiedienstverleners een brief gestuurd waarin zij worden opgeroepen om beveiligingsincidenten te melden; deze boodschap is ook tijdens de bedrijfsbezoeken door OPTA afgegeven.

Nog te nemen maatregelen

- Logius PKIoverheid zal zelf als opdrachtgever voor de vanaf 1 januari 2012 verplichte jaarlijkse pentesten bij de PKIoverheid leveranciers gaan fungeren waardoor zij in deze als eerstelijns toezichthouder opereert en inzicht krijgt in de risico's en kwetsbaarheden van het onderzochte systemen bij de PKIoverheid certificatiedienstverleners;
- Er vindt thans een actie plaats om in het BIR het verplicht gebruik van PKI overheidscertificaten voor de Rijksoverheid vast te leggen;
- Ten slotte is PKIoverheid bezig met het opzetten van een gebruikersgroep waarin bijvoorbeeld de Belastingdienst vertegenwoordigd zal zijn. In deze groep worden ontwikkelingen binnen PKIoverheid toegelicht.

Ten aanzien van het tweede punt zal veilig melden op grond van een wettelijke Security Breach Notification, zoals hiervoor gemeld, bijdragen aan de nodige cultuuromslag. Binnen het PKI overheidsstelsel zal daarnaast nogmaals beklemtoond worden hoe belangrijk een tijdige melding is.

Tenslotte

De door de OVV gedane aanbevelingen neem ik ter harte. Veel is al gedaan, ook naar aanleiding van eerdere onderzoeken, maar ik onderschrijf het belang dat aan bewustwording voor informatiebeveiliging bij bestuurders moet worden toegekend. De uitwerking daarvan, zowel in ondersteuning van bestuurders als het aanreiken van instrumenten om aan de eigen verantwoordelijkheid invulling te geven, zal belegd worden bij de Taskforce Bewustwording informatiebeveiliging. Daarmee wordt een belangrijke impuls aan de medeoverheden en de Rijksoverheid zelf gegeven, om deze verantwoordelijkheid binnen de bekende "plan-do-check-act" cyclus zelf in te voeren. Wanneer deze impuls echter niet voldoende blijkt, kan alsnog worden overgegaan op meer dwingende maatregelen zoals wet- en regelgeving.
De overheid is zoals eerder gesteld in grote mate afhankelijk van digitale informatie. Daarom is goede informatiebeveiliging noodzakelijk, en hoewel 100 % veiligheid niet kan worden gegarandeerd, kan er wel nog een slag gemaakt worden langs de lijn die de OVV aangeeft. Daarom stelt het kabinet dan nu ook in deze tijd van schaarste geld beschikbaar voor de genoemde Taskforce. Een juiste afweging van risico's en te nemen maatregelen is en blijft de verantwoordelijkheid van de

bestuurder en het hogere management. Met de Taskforce wil ik deze verantwoordelijkheid ondersteunen en begeleiden.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

Dr. R.H.A. Plasterk