Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011

32 500 VII Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2011

Nr. 110

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 juni 2011

In de procedurevergadering van de vaste commissie voor Binnenlandse Zaken van 31 maart 2011 is gesproken over mijn brief van 24 maart 2011 (kamerstuk 32 500 VII, nr. 91) inzake het op afstand afluisteren van mobiele telefoons bij de overheid. De commissie heeft besloten mij een aantal vragen te stellen. Het antwoord hierop treft u in deze brief aan.

De commissie heeft besloten u te verzoeken de Kamer zo spoedig mogelijk te informeren over de resultaten van het onderzoek dat in gang is gezet, en over de maatregelen die reeds genomen zijn of waartoe de onderzoeksresultaten aanleiding geven.
In mijn brief van 24 maart heb ik als vervolg op dit incident laten onderzoeken of er misbruik is gemaakt van de tijdelijke kwetsbaarheden in het voicemailsysteem van Vodafone. Het misbruik is beperkt tot de zakelijke mobiele telefoonnummers van twee bewindslieden, dat te zien is geweest in de uitzending van Eén Vandaag. Dit onderzoek geeft geen aanleiding nader te onderzoeken in hoeverre staatsveiligheid in het geding is geweest.

Naar aanleiding van het incident hebben alle intranetredacties en interne communicatieadviseurs ten behoeve van plaatsing op de departementale intranetten een tekst met advies voor veiliger bellen gekregen.

De commissie ontvangt voorts graag een overzicht van de huidige maatregelen met betrekking tot de beveiliging van data bij de overheid (bijv. e-mailverkeer, data-opslag etc.).
Op het terrein van informatiebeveiliging heeft de Rijksdienst een aantal regelingen. Het fundament wordt gevormd door het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR2007). De grondgedachte is dat informatiebeveiliging op meerdere manieren tot stand kan komen, zolang dit maar door middel van bewuste keuzes gebeurt op basis van risicoma-

kst-32500-VII-110
ISSN 0921 - 7371
's-Gravenhage 2011

nagement. Informatiebeveiliging vormt een integraal onderdeel van de bedrijfsvoering en is daarmee een managementverantwoordelijkheid. Voor elk informatiesysteem[1] wordt door het betreffende lijnmanagement op basis van een risicoafweging bepaald welke specifieke beveiligingsmaatregelen de organisatie treft.

Alle ministeries hebben ervoor gekozen een (of meer) gemeenschappelijk stelsels van betrouwbaarheidseisen, normen en/of maatregelen af te spreken (informatiebeveilingsbaseline, hierna «baseline» genoemd). Het vertrouwelijkheidsniveau van veel baselines wordt ingegeven door het feit dat er in de organisaties persoonsgegevens worden verwerkt. Deze baselines bevatten ook maatregelen met betrekking tot e-mailverkeer en opslag van data. Voor e-mailverkeer tussen ministeries wordt gebruik gemaakt van een eigen netwerk: de Haagse Ring.

De rijksdienst werkt aan de totstandkoming van een rijksbrede baseline waardoor de interoperabiliteit binnen de rijksdienst wordt vergroot en een groot aantal baselines bij departementen en zelfstandige onderdelen van de rijksdienst overbodig worden. Ook bestaande interdepartementale baselines zoals voor mobiele informatiedragers zullen in deze rijksbrede baseline worden opgenomen.

Voor informatie waarvoor een verhoogde mate van vertrouwelijkheid (waaronder staatsgeheime informatie) is vereist, geldt een aanvullende regeling: het Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (Vir-bi). Het Vir-bi bevat regels en maatregelen, gericht op de bescherming van de vertrouwelijkheid. Het is een aanvulling op VIR waarin beveiliging van informatie in het algemeen binnen de rijksdienst is geregeld. Het Vir-bi wordt thans herzien om de aansluiting met het uitgangspunt van risicomanagement van het VIR2007 beter te maken.

Volgens het Beveiligingsvoorschrift Rijksdienst 2005 wijst de secretaris-generaal binnen ieder ministerie een beveiligingsambtenaar (BVA) aan die belast is met de integrale beveiliging van organisatie, medewerkers, materieel, informatiesystemen, gebouwen en overige objecten, alsmede het toezicht op de werking van de beveiligingsorganisatie en de informatiebeveiliging.

Vraagpunten van de Commissie

Monitoring van ICT-systemen binnen de overheid is van groot belang. Heeft de overheid zicht op wat er gebeurt op haar netwerken, waaronder mailsystemen, en kan ze tijdig ingrijpen als er sprake is van een onbewuste hiaat in de beveiliging of een doelbewuste inbreuk op de beveiliging?
Departementen beschikken over virusscanners en firewalls in hun ICT-infrastructuur, die standaard aanvallen kunnen weerstaan. Ten behoeve van het onderkennen van vreemde datastromen die lopen tussen het eigen netwerk en het internet, beschikken ze bovendien over een Intrusion Detection Systeem (IDS). Met networktools worden sinds begin dit jaar de websites van de overheid door GOVCERT gemonitord op het verspreiden van malware. GOVCERT heeft een actieve waakdienst om ICT-dreigingen te detecteren en identificeren die op overheden gericht kunnen zijn. GOVCERT informeert overheidspartijen hier proactief over om informatie te bieden hoe deze dreigingen te weerstaan. In geval van een incident is GOVCERT 24 uur per dag bereikbaar om ondersteuning te bieden bij de afhandeling ervan. Daartoe zet GOVCERT haar uitgebreide internationale kennisnetwerk en speciaal ontwikkelde, geavanceerde instrumenten in. Als er externe partijen zijn die merken dat er bij Nederlandse overheidsorganisaties een probleem met malware is, dan

[1] Een informatiesysteem is in de context van VIR2007 een samenhangende (logische) groepering van gegevensverwerkende processen en gegevensverzamelingen.

komt de melding hiervan bij GOVCERT.NL terecht en wordt de overheidsorganisatie geholpen met het oplossen. GOVCERT.NL is in staat om grote hoeveelheden van deze meldingen te filteren en relevante incidenten te signaleren.

Wordt een vreemde datastroom gesignaleerd, dan is er al sprake van een succesvolle aanval die niet door virusscanners is voorkomen. Om een dergelijke gerichte aanval op een eerder moment te kunnen onderkennen, wordt op meerdere sporen actie ondernomen. De rijksdienst heeft de ambitie het aantal koppelingen tussen de rijksdienst als geheel en internet sterk te reduceren en onder te brengen in een Rijks internetkoppeling als bouwsteen van de generieke ICT-infrastructuur, zoals is voorzien in het programma Compacte Rijksdienst. Hierdoor kan het aantal IDS systemen worden teruggebracht en komt er capaciteit vrij om ook in de toekomst beter weerstand kunnen bieden tegen toenemende cyberbedreigingen. Deze capaciteit zal centraal worden georganiseerd. Verder ondersteunt de AIVD, samen met GOVCERT, in een proef diverse ministeries bij het vroegtijdig detecteren van digitale aanvallen op hun netwerk, zodat de beveiliging van gevoelige informatie wordt gewaarborgd. Een geslaagde proef zal leiden tot verdere uitrol bij de rijksdienst. De AIVD helpt voorts bij het doen van analyses naar afwijkingen ten opzichte van het normale netwerkverkeer. Op die manier wordt de beveiliging van het ministerie in staat gesteld potentiële incidenten te onderzoeken en weerstandverhogende maatregelen te nemen.

Op een aantal punten wordt de preventie rijksbreed verbeterd. In mijn brief van 24 maart schreef ik dat ik laat onderzoeken op welke wijze de signaleringen van GOVCERT actiever opgepakt kunnen worden. De uitkomsten hiervan worden mede betrokken bij het inrichten van de ICT-beveiligingsorganisatie door de minister van V&J. Ten slotte heeft het kabinet in de Notitie privacybeleid van 29 april geschreven dat er een verplichting komt om in gevallen van verlies, diefstal of misbruik van persoonsgegevens melding te maken van dat voorval aan de toezichthouder, het College Bescherming Persoonsgegevens. Deze kan boetes opleggen indien de meldplicht niet wordt nageleefd.

Goed opdrachtgeverschap. In hoeverre vormt (informatie-)beveiliging een expliciet aandachtspunt bij een aanbesteding? Het grootste risico is dat in een aanbesteding beveiliging niet in de eisen wordt meegenomen.
Om te voldoen aan het VIR2007 wordt in het systeemontwikkelingtraject de vaststelling van betrouwbaarheidseisen zo vroeg mogelijk uitgevoerd, bij voorkeur tijdens de fase «definitiestudie», eventuele detailleringen passen in de fasen «basisontwerp» en «detailontwerp». Naast het ontwikkelen en implementeren kunnen informatiesystemen ook worden verworven en/of geëxploiteerd. In deze gevallen draagt de lijnmanager de zorg voor het betrouwbaar (laten) exploiteren van het informatiesysteem en de zorg voor het betrouwbaar (laten) verwerven van (componenten van) het informatiesysteem. De CIO's bij de rijksdienst zien op dit geheel toe. De eerder genoemde rijksbrede baseline informatiebeveiliging zal bij alle ICT-aanbestedingen en ICT-projecten de basis voor informatiebeveiliging zijn.

Ten slotte heeft GOVCERT enkele producten uitgebracht die overheden kunnen helpen bij het doen van juiste aanbestedingen. Zo zijn er de adviesdocumenten over securitytests, beveiliging van webapplicaties en smartcards

Het wordt steeds gebruikelijker om eigen apparatuur te mogen gebruiken op het zakelijke netwerk («bring your own device» beleid). Dit vergt een goede en veilige infrastructuur. Hoe is dit geregeld bij de overheid en hoe

verhoudt dit beleid zich tot het initiatief van enkele ministers om eigen toestellen te gebruiken tegen het advies van de departementale ICT-afdeling in?
ICT-apparatuur wordt doorgaans door de departementen ter beschikking gesteld aan de medewerker. Bij een aanzienlijk aantal departementen is het wel mogelijk voor het veilig telewerken gebruik te maken van eigen voorzieningen. Bij een dergelijke inzet hebben deze departementen een risicoafweging gemaakt en daarbij passende maatregelen genomen. Zoals het kabinet in de beantwoording van de kamervragen over iPhone (Vraagnummer: 2011Z08644) heeft geschreven, moet altijd een op de functie van het apparaat toegespitst beveiligingsniveau worden gerealiseerd. Over rijksbreed beleid ten aanzien van «bring your own device» zal ik terugkomen in de i-Strategie die ik in november 2011 naar uw Kamer zal sturen.

Om succesvol het nieuwe werken te kunnen invoeren in een organisatie is goede en veilige infrastructuur nodig. Hoe is dit geregeld bij de overheid?
Departementen hebben een eigen ICT-infrastructuur waarvan de beveiliging is gebonden aan regelgeving zoals het VIR en het VIR-BI en enkele interdepartementale beveiligingskaders. De rijksdienst beschikt op dit moment over een veilig interdepartementaal netwerk, de Haagse Ring en een interdepartementaal intranet, Rijksportaal. Op het niveau van de werkplekinrichting leidt het lopende project Digitale Werkomgeving Rijksdienst (DWR) tot standaardisatie. Binnen het uitvoeringsprogramma Compacte Rijksdienst wordt voorzien in de opzet van een gemeenschappelijke beheerorganisatie voor DWR.

De rijksdienst streeft ernaar de bestaande netwerkbeveiliging steeds meer gepaard te laten gaan met gegevensbeveiliging. Hogere eisen aan identificatie en autorisatie van gebruikers wordt gecombineerd met gegevensbeveiliging. Op die manier worden gegevens op maat beschikbaar gesteld aan hen die toegang moeten hebben en blijven afgeschermd voor diegenen die geen toegang moeten hebben. Zo wordt ook plaats- en tijdonafhankelijk werken beter gefaciliteerd.

Eigen verantwoordelijkheid. Gebruikers hebben een eigen verantwoordelijkheid bij het veilig gebruiken van communicatiemiddelen en ICT. Hoe wordt dit veilige gebruik binnen de overheid gestimuleerd?
De departementale BVA heeft onder andere als taak om het beveiligingsbewustzijn bij de medewerkers te bevorderen en de communicatie op het gebied van de integrale beveiliging te verzorgen. Onderdeel daarvan is ook het bevorderen van het bewustzijn van gebruikers ten aanzien van hun eigen verantwoordelijkheid bij het veilig gebruiken van communicatiemiddelen en ICT. Ook het lijnmanagement heeft een taak ten aanzien van het vergroten van het beveiligingsbewustzijn bij medewerkers. De naleving van de beveiligingsvoorschriften blijft immers mensenwerk en vereist voortdurende aandacht.

De rijksdienst streeft ernaar dat regels en veiligheidsmaatregelen helder en eenvoudig uit te leggen en na te volgen zijn en verantwoord gedrag bij medewerkers oproepen. Daarom streeft de rijksdienst naar maximale facilitering van gevraagde ICT-functionaliteit op een veilige manier. Immers, dit zorgt voor beveiliging van gegevens die dat nodig hebben, op een manier die uit te leggen is. In de i-Strategie zal dit streven worden geconcretiseerd.

Het GovCERT en het NBV hebben een taak om de overheid te adviseren en waarschuwen als er mogelijke beveiligingsrisico's zijn. Hebben zij ook een signalerende rol naar de leverancier van producten en diensten, waarin zij dit risico signaleren?

NBV en GOVCERT hebben geen structurele signalerende rol naar leveranciers van producten en diensten. Het Nationaal Bureau voor Verbindingsbeveiliging (NBV), onderdeel van de AIVD, bevordert de beveiliging van gevoelige informatie bij de rijksoverheid, zoals departementaal vertrouwelijke en staatsgeheime informatie. De AIVD geeft voor dit type informatie advies over informatiebeveiliging, beoordeelt beveiligingsproducten en ondersteunt bij de implementatie ervan. Ook kan de AIVD beveiligingsproducten ontwikkelen als er geen producten beschikbaar zijn die voldoen aan de beveiligingseisen.

Voor de Vodafone Voicemail kwetsbaarheid heeft GOVCERT na ontdekking in overleg met de contracteigenaar de leverancier geïnformeerd. GOVCERT vervult deze signalerende rol in dergelijke gevallen op ad-hoc basis. Een signalerende rol naar de leverancier van producten en diensten bij gevonden kwetsbaarheden in hun producten, is (inter)nationaal momenteel een bijzonder actueel onderwerp. Onderzoekers die lekken in software vinden en leveranciers die patches moeten uitbrengen voor die software hebben sterk verschillende belangen: voor de leveranciers het voorkomen van reputatieschade en voor de onderzoekers erkenning voor hun werk. Het streven naar goed georganiseerde verantwoorde openbaarmaking («responsible disclosure») van kwetsbaarheden in software aan producenten ligt tevens in het verlengde van het streven, zoals genoemd in de Nationale Cyber Security Strategie, om producenten nadrukkelijker te wijzen op hun verantwoordelijkheid voor de veiligheid van hun producten. Een meer structurele inrichting van een coördinerende rol voor GOVCERT daarin, past in dit streven.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. P. H. Donner