Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 224

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 2 februari 2012

Het is van belang dat de ICT-beveiliging van overheidsorganisaties op orde is. Dat is in eerste instantie de verantwoordelijkheid van individuele organisaties zelf.
De afgelopen periode is het echter nodig gebleken om een verscherpte en duurzame landelijke ICT-beveiligingsrichtlijn op te stellen, en bij signalen van inbraak altijd onderzoek te doen. Daarnaast wordt bij geconstateerde inbraak overgegaan tot het onverwijld afsluiten van DigiD. Om een structurele en forse impuls te geven aan kwaliteitsverhoging van ICT-beveiliging zullen er ICT-beveiligingssassessments worden ingevoerd.

In deze brief ga ik in op de inzet van een aantal specifieke maatregelen zoals aangekondigd in de brief van 11 oktober 2011 met onderwerp: «Lekken in aantal gemeentelijke websites». Daarin is u gemeld dat organisaties die gebruik maken van DigiD jaarlijks hun ICT-beveiliging, voor zover deze DigiD raakt, dienen te toetsen op basis van een ICT-beveiligingassessment.

De norm voor ICT beveiliging
De ICT-beveiligingassessments worden uitgevoerd met de ICT-Beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC,voorheen GOVCERT.NL) als basis. Deze beveiligingsrichtlijnen bevatten maatregelen op het gebied van netwerkveiligheid, besturingssysteem, basisbeveiliging (virusscanner, firewall) en applicatiebeveiliging. Ook een «*hack*»-test ofwel een zogenaamde penetratietest maakt deel uit van de richtlijnen. De beveiligingsrichtlijnen zijn opgesteld in samenspraak met een aantal publieke en private partijen, waaronder beveiligingsexperts. De richtlijnen worden gepubliceerd op de website van het NCSC. Bij nieuwe dreigingen stelt het NCSC de beveiligingsrichtlijnen bij.
De normstelling voor de assessments wordt bepaald door de belangrijkste elementen van de bovengenoemde richtlijnen. Met deze normstelling

kst-26643-224
ISSN 0921 - 7371
's-Gravenhage 2012

wordt een forse impuls gegeven aan de verdere kwaliteitsverhoging van de ICT-beveiliging bij de overheid.

Uitvoeren ICT beveiligingassessments
Allereerst zullen de organisaties die DigiD gebruiken, geïnformeerd worden over de bovengenoemde normstelling. Op deze wijze kunnen de DigiD gebruikende organisaties de benodigde aanpassingen in hun organisaties treffen en zich adequaat voorbereiden op de ICT-beveiligingsassessments.

Daarnaast dienen zij de ICT-beveiligingassessments te laten uitvoeren onder verantwoordelijkheid van een Register EDP-auditor.[1] Deze auditors beschikken over de benodigde kennis en ervaring voor dergelijke onderzoeken. Organisaties die een Register EDP-auditor in dienst hebben, kunnen desgewenst een zogeheten *self-assessment* uitvoeren. Vervolgens dienen de conclusies van de ICT-beveiligingsassessments in de vorm van een rapportage door de gebruikende organisaties aan Logius[2] te worden opgeleverd.

De Register EDP-auditors die in het register van de NOREA zijn ingeschreven, zijn onderworpen aan internationale regelgeving op het terrein van audit en assurance, waaronder de «Code of Ethics» en de Richtlijn «Assurance Opdrachten».

Gefaseerde aanpak
In de brief van mijn voorganger van 11 oktober jl. is aangegeven dat alle organisaties voor 1 april 2012 de ICT-beveiligingsassessments moesten hebben doorlopen. Omdat het belangrijk is te komen tot een duurzame richtlijn heeft dit zijn tijd gekost. Verder heeft nader onderzoek laten zien dat de markt op deze termijn niet kan voldoen aan de benodigde expertise met betrekking tot de assessments en penetratietesten. Ook zijn er signalen van DigiD gebruikende organisaties, waaronder VNG en KING[3], dat de benodigde aanpassingen en de doorlooptijd niet onderschat moet worden. Naast de huidige aanpak waarbij ingeval van signalen altijd nader onderzoek plaatsvindt en ingeval van inbraak onverwijld wordt afgesloten van DigiD, heb ik gekozen voor een gefaseerde aanpak met betrekking tot de beveiligingsassessments. Daarbij wordt ingezet op prioriteiten als het gaat om type organisatie en het belang voor de burger. Grootgebruikers van DigiD dienen voor het eind van het jaar het ICT-beveiligingsassessment te hebben uitgevoerd. Overige organisaties dienen het assessment uiterlijk een jaar later uitgevoerd te hebben.

Grootgebruikers
Logius start per direct een samenwerkingstraject met de grootgebruikers van DigiD omdat deze cruciaal zijn voor de overheidsdienstverlening. Organisaties als de Belastingdienst, DUO en de UWV behoren daartoe. Het is ons streven om te komen tot een spoedige afronding van de assessments bij deze organisaties. Andere organisaties kunnen vanzelfsprekend daarop aansluiten. Logius biedt daarnaast ondersteuning aan organisaties (niet gemeenten) door voorlichting en het delen van *best practices.* Bij de vormgeving van het traject voor deze organisaties zal gebruik worden gemaakt van de ervaringen die bij de grootverbruikers zijn opgedaan, alsmede de impactanalyse bij een aantal gemeenten.

Gemeenten, Provincies en Unie van Waterschappen
VNG start, ondersteund door KING, per direct een samenwerkingstraject met een vertegenwoordiging van auditors en ICT-leveranciers van gemeenten over de aanpak van de ICT-beveiligingassessments bij gemeenten. Dit traject heeft als doel om een efficiënte uitvoering en eenduidige toepassing van de ICT-beveiligingsrichtlijnen bij gemeenten te

[1] Electronic Data Processing auditor.
[2] Logius is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
[3] Kwaliteits Instituut Nederlandse Gemeenten.

bewerkstellingen. Dit doel wordt versterkt door het feit dat bepaalde auditors en ICT-leveranciers in opdracht van meerdere gemeenten werken. In dit traject kunnen desgewenst ook het Interprovinciaal Overleg en de Unie van Waterschappen worden betrokken.

KING voert de eerste helft van dit jaar bij een aantal gemeenten, waaronder kleine, middelgrote en grote gemeenten, een impactanalyse uit. De uitkomsten hiervan bieden input voor een gestandaardiseerde aanpak voor het uitvoeren van de ICT-beveiligingassessment bij gemeenten. Dit mede met het oog op het beperken van de uitvoeringslasten.

Daarnaast onderzoeken VNG en KING hoe zij gemeenten structureel op het terrein van ICT-beveiliging kunnen ondersteunen. Afhankelijk van de uitkomsten van deze onderzoeken bepalen VNG en KING hoe zij gemeenten ondersteunen bij de assessments (te denken valt aan het inrichten van een helpdesk).

Tevens zal ik het onderwerp ICT-beveliging agenderen in mijn eerstvolgende overleg met de mede-overheden, en bezien of nadere bestuursafspraken nodig zijn.

Uitvoeren «hack»-testen
In het kader van de jaarlijkse ICT-beveiligingsassessments heeft Logius de mogelijkheid om enkele betrouwbare marktpartijen opdracht te geven tot het krakenvan de ICT-beveiliging van gebruikende organisaties. Deze mogelijkheid staat los van de *«hack»*-testen of zogenaamde penetratietesten die Logius zelf jaarlijks laat uitvoeren op DigiD.

Communicatie richting organisaties
In de afgelopen periode is het effectief gebleken de communicatie te stroomlijnen. Daarom zijn er afspraken gemaakt over wie de aanspreekpunten zullen zijn. Voor vragen over het proces, kunnen organisaties bij Logius terecht. VNG is aanspreekpunt voor gemeenten. NCSC levert informatie over de beveiligingsrichtlijn. EDP-auditors kunnen met vragen bij NOREA terecht.

Tot slot
Hoewel 100% veiligheid nooit te garanderen is, wordt met deze samenwerking een belangrijke en haalbare impuls gegeven aan de kwaliteitsverbetering van ICT-beveiliging bij de overheid. In het derde kwartaal van 2012 zal ik u informeren over de stand van zaken met betrekking tot de genomen kwaliteitsmaatregelen.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. W. E. Spies