



> Retouradres Postbus 20011 2500 EA Den Haag

Aan college van burgemeester en wethouders van gemeenten

**Burgerschap en
Informatiebeleid**
Identiteit

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Kenmerk
2012-0000370801

Datum 26 juni 2012
Betreft ICT-beveiligingsassessments DigiD

Bijlagen
1

Geachte mevrouw, mijnheer,

Bij brief van 2 februari jongstleden aan de Tweede Kamer heb ik maatregelen aangekondigd om de kwaliteit van de ICT-beveiliging van DigiD-gebruikende organisaties een impuls te geven. De brief is bijgevoegd. Naar aanleiding hiervan vraag ik uw bijzondere aandacht voor deze maatregelen.

Aanleiding maatregelen

De aanleiding van de maatregelen is een aantal incidenten uit het najaar 2011. Zo heeft onder de noemer "Lekttober" (onder deze naam heeft de website webwereld.nl gepubliceerd) een aantal acties plaatsgevonden, waarbij er lekken zijn aangetoond in een aantal websites van overheidsorganisaties. Omdat deze incidenten een weerslag kregen op het vertrouwen van burgers in de digitale dienstverlening van de overheid en in het bijzonder in de dienstverlening van DigiD, heb ik verschillende maatregelen aangekondigd.

Inhoud maatregelen

De maatregelen houden in dat u, als DigiD gebruikende organisatie, jaarlijks een zogenaamde ICT-beveiligingsassessment (een soort audit) dient uit te laten voeren naar de veiligheid van uw ICT voor zover deze gekoppeld is aan DigiD.

Voor dit ICT-beveiligingsassessment dient u de *Norm ICT-beveiligingsassessments DigiD* te hanteren, die op de website www.logius.nl is gepubliceerd. Het assessment dient te worden uitgevoerd onder verantwoordelijkheid van een Register EDP-auditor. Organisaties die een Register EDP-auditor in dienst hebben, kunnen desgewenst een zogenaamde self-assessment uitvoeren. De bevindingen van het assessment dient u in de vorm van een rapportage aan Logius, de beheerorganisatie van DigiD, aan te bieden.

In dit verband heeft de Tweede Kamer na voornoemde brief een motie aangenomen waarin de regering wordt verzocht om te bewerkstelligen dat "alle DigiD-gebruikende organisaties (nader) werk maken van de veiligheid ervan en hiervoor eind 2012 een ICT-beveiligingsassessment laten uitvoeren".¹

¹ Kamerstukken II 2011/12, 26 643, nr. 238.

In bestuurlijk overleg van 18 april jongstleden heb ik met de vertegenwoordigers van mede-overheden gesproken over het belang van informatiebeveiliging en de veiligheid van websites, die gebruik maken van DigiD.

Datum
26 juni 2012
Kenmerk
2012-0000370801

Met betrekking tot gemeenten heeft de VNG haar leden al eerder in een ledenbrief over deze onderwerpen geïnformeerd.² Op dit moment voert KING samen met negen gemeenten, een impactanalyse uit om de gevolgen van de norm *ICT-beveiligingsassessment DigiD* in kaart te brengen en een zo efficiënt mogelijke aanpak te ontwikkelen. Uit de voorlopige bevindingen van het onderzoek blijkt, dat een volledige afronding van het proces in 2012 niet in alle gevallen mogelijk zal zijn, een forse niet voorziene inspanning vraagt en bovendien afhankelijk is van afspraken met leveranciers en auditors. Wel is duidelijk, dat een grote slag gemaakt zal kunnen worden indien nog dit jaar de (grote) leveranciers aan de genoemde audit onderworpen kunnen worden. De afzonderlijke gemeenten moeten in staat geacht worden nog dit jaar een substantieel deel van het onderzoek uit te voeren, conform het stappenplan van Logius. De afrondende audit zal in veel gevallen eerst in 2013 kunnen worden uitgevoerd. Het vorenstaande is vanzelfsprekend niet zonder meer op elke gemeente van toepassing. De situatie van gemeenten die de dienstverlening als service van een leverancier betrekken is per definitie anders dan die van een gemeente die zelfvoorzienend is. Ook de omvang van gemeenten en de optie om de ICT beveiligings assessment in eigen beheer uit te voeren speelt een rol. Zo verwachten de grote uitvoeringsorganisaties, die op DigiD zijn aangesloten wel de assessments voor het einde van 2012 te kunnen afronden.

VNG zal op basis van de definitieve uitkomsten van de impactanalyse u per ledenbrief informeren over de voorziene ondersteuningsaanpak op het gebied van informatiebeveiliging specifiek voor gemeenten.

Gelet op het grote belang van een betrouwbare communicatie met en dienstverlening aan burgers en bedrijven enerzijds en anderzijds de doorlooptijd van het assessment, het doorvoeren van mogelijke verbeteringen en de beschikbare capaciteit in de markt, verzoek ik u om op korte termijn te starten. Dit om een zo groot mogelijk deel van het stappenplan nog in 2012 te doorlopen.

Informatie en vragen

Op de website www.logius.nl/producten/toegang/digid/ict-beveiligingsassessments/ vindt u de norm, het stappenplan en alle overige informatie, documenten en veelgestelde vragen omtrent de ICT-beveiligingsassessments. Tevens is aangegeven bij welke organisatie u terecht kunt met specifieke vragen.

Met uw medewerking kunnen we een belangrijke impuls geven aan de kwaliteit van de ICT-beveiliging van de overheid. Om die reden reken ik op uw medewerking ten aanzien van de bovenstaande maatregelen.

²VNG, 7 februari 2012, *DigiD en ICT-beveiliging*, lbr 12/05, zie http://www.vng.nl/Documenten/actueel/brieven/ledenbrieven/2012/20120208_lbr12_015_Digi_CT.pdf

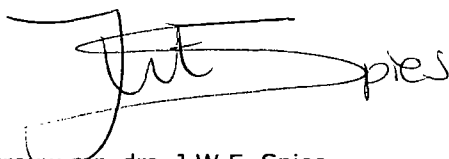
Eerder dit jaar is de contactpersoon DigiD van uw organisatie over het voorgaande geïnformeerd. Een afschrift van deze brief wordt tevens naar deze contactpersoon gestuurd.

Datum
26 juni 2012

Kenmerk
2012-0000370801

Aan het bestuur van provincies, waterschappen, uitvoeringsorganisaties en overige afnemers van DigiD is een soortgelijke brief verstuurd.

Hoogachtend,
De minister van Binnenlandse Zaken en Koninkrijksrelaties,

A handwritten signature in black ink, appearing to read 'J.W.E. Spies'. The signature is stylized with a large initial 'J' and a long horizontal stroke.

Mevrouw mr. drs. J.W.E. Spies