

Vergaderjaar 2011–2012

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 193

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 oktober 2011

Het Kabinet constateert dat digitale informatie-uitwisseling een essentieel onderdeel is geworden voor het functioneren van de Nederlandse samenleving. Betrouwbare digitale communicatie is van wezenlijk belang en behoeft voortdurende zorg. Uiteraard moet alles in het werk worden gesteld om dit te borgen. Bedreiging van het vertrouwen in, en de integriteit van, elektronische overheidsdienstverlening is voor het Kabinet niet acceptabel.

Uit de voorbeelden die Webwereld in het kader van hun actie «Lektobert» tot nu toe heeft gepresenteerd, blijkt evenwel dat ICT beveiliging bij overheidsorganisaties te kort schiet. Recent is bij enkele tientallen gemeenten geconstateerd dat hun ICT beveiliging onvoldoende was. Dat moet beter. Dat is in de eerste plaats een verantwoordelijkheid van de individuele overheidsorganisaties zelf. Maar dat alléén, is met de huidige vernetwerkte elektronische dienstverlening niet voldoende. Deze dienstverlening is vaak modulair en in ketens georganiseerd. De informatiebeveiliging van de keten als geheel, moet op orde zijn. De zwakste schakels in die ketens bepalen namelijk de veiligheid van de keten als geheel. Wanneer overheidsorganisaties die gebruik maken van DigiD hun ICT beveiliging onvoldoende op orde hebben, vormt dit een risico. Gegevens kunnen mogelijk worden onderschept en oneigenlijk gebruikt. Dat kan afbreuk doen aan het vertrouwen dat burgers hebben in het stelsel van DigiD.

Om de gebleken problemen met de beveiliging te ondervangen is een aantal korte termijn maatregelen genomen die direct van kracht worden, namelijk:

1. De beheerorganisatie Logius, onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, heeft van mij – vanaf dit moment – opdracht gekregen alle organisaties waarvan blijkt dat de ICT gecompromitteerd is (met mogelijke gevolgen voor DigiD) per direct af te koppelen van DigiD. Deze organisaties kunnen dus hun elektronische dienstverlening met gebruikmaking van DigiD niet meer

voortzetten. Dat is weliswaar verstorend voor de burger en kost deze organisaties geld omdat efficiënte digitale interactie met de burger niet langer mogelijk is, maar uiteindelijk verbetert dit het vertrouwen in het systeem als geheel.

2. Organisaties die zijn afgesloten van DigiD kunnen weer worden aangesloten nadat is vastgesteld dat hun ICT beveiliging (voor zover die DigiD kan raken) weer op orde is.
3. Voor de langere termijn geldt dat alle DigiD gebruikende organisatie uiterlijk voor het einde van het eerste kwartaal van 2012 hun ICT beveiliging getoetst dienen te hebben op basis van een ICT beveiligings-assessment.

Vanaf 2012 zal sprake zijn van een jaarlijkse herhaling van het ICT beveiligings-assessment door alle gebruikende organisaties. Ten slotte zal Logius in het stelsel van ICT beveiligings-assessments enkele betrouwbare marktpartijen vragen de ICT beveiliging van gebruikende organisaties te kraken. Daarmee kan getoetst worden of het ICT beveiligings-assessment voldoende stringent wordt toegepast. GOVCERT.nl zal de normstelling regelmatig actualiseren vanwege nieuwe bedreigingen die zich aandienen.

Het ICT beveiligings-assessment gaat uit van bekende bedreigingen. De (basis)norm voor de assessment zal worden vastgesteld door GOVCERT.nl, na overleg met VNG/KING. Logius selecteert een beperkt aantal marktpartijen met voldoende technische ICT beveiligingskennis, om het ICT beveiligings-assessment uit te voeren. De DigiD gebruikende organisaties dienen zelf deze marktpartijen opdracht te geven tot het uitvoeren van ICT beveiligings-assessments. Grote partijen met voldoende ICT kennis (ter beoordeling aan Logius) mogen ICT beveiligings-assessments in eigen beheer uitvoeren.

VNG en KING zijn momenteel samen met de bij de bovengenoemde Lektoker actie betrokken gemeenten en de betreffende leveranciers, in samenwerking met GOVCERT.nl en Logius, de beveiliging van de getroffen websites op orde aan het brengen.

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