Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 218

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 december 2011

Bij de regeling van werkzaamheden van donderdag 8 december jl. hebben de leden El Fassed (GL) en Gesthuizen (SP) gevraagd om een brief over Diginotar 2 (Gemnet PKI Overheidscertificaten). Dit naar aanleiding van een tweetal berichten in de media:
1. inzake een hack bij de certificatenleverancier Gemnet;
2. inzake de intrekking van duizend certificaten door KPN.

Hierbij ontvangt u mijn reactie op deze berichtgeving.

1. Berichtgeving over de hack van KPN/Gemnet site

In de media is gemeld dat de website van KPN-Gemnet gehackt blijkt te zijn. KPN heeft dat zelf in een persbericht op 7 december bevestigd en heeft op 8 december twee updates uitgebracht.

Feitelijk heeft KPN-Gemnet twee verschillende sites:
– Een algemene publiekssite (www.gemnet.nl) met met name organisatorische informatie over Gemnet. Dit is de site die gehackt is.
– Een specifiekere site waarop PKIoverheidscertificaten aangevraagd kunnen worden (www.gemnetscp.nl). Deze site is niet gecompromitteerd.

Beide sites ondersteunen het aanvraagproces van overheidscertificaten. Specifieker: Gemnet is geen certificaatdienstverlener binnen PKIoverheid, maar slechts een verkoopkantoor van PKIoverheid certificaten, die overigens worden gemaakt door KPN/Getronics. De beide hierboven genoemde websites bevatten ten aanzien van het aanvraagproces alleen aanvraagformulieren voor het verkrijgen van PKIoverheid certificaten, die door de potentiële klant moeten worden gedownload, met de hand moeten worden ingevuld en per post moeten worden opgestuurd.

kst-26643-218
ISSN 0921 - 7371
's-Gravenhage 2011

Het aanvraagproces is dus niet gekoppeld aan het productieproces bij KPN/Getronics. Daarom is er geen enkele aanleiding te veronderstellen dat de hack bij de websites van Gemnet leidt tot compromittering van KPN/Getronics.

Over de mogelijkheden tot compromittering van de produktieomgeving, is de Kamer al geinformeerd op 9 november. De partij die destijds de penetratietest heeft uitgevoerd, heeft tevens nu een administratief onderzoek gedaan naar alle vanaf 1 maart 2011 uitgegeven PKIoverheid servicescertificaten (inclusief de via Gemnet aangevraagde certificaten). Hierbij is getoetst of er voor ál deze uitgegeven certificaten adequate administratieve vastlegging aanwezig is. Dat is het geval, dus ze zijn niet ten onrechte uitgegeven.

Bovengenoemde informatie kan ik u mede melden op grond van intensieve contacten die er de afgelopen dagen zijn geweest tussen mijn ministerie en KPN.

2. Nieuwsbericht over grote aantallen ingetrokken certificaten

Daarnaast is er op 8 december een tweede nieuwsbericht uitgebracht over de intrekking van duizend certificaten door KPN (Getronics).

Deze intrekking laat zich als volgt verklaren. Doordat de overheid het vertrouwen in Diginator heeft opgezegd, moesten de getroffen afnemers in grote aantallen omschakelen naar een andere certifcaatleverancier zoals KPN/Getronics. Dit leidde bij KPN/Getronics tot een additionele werklast, waarbij de productiecapaciteit zeer snel moest worden opgeschaald.

De voorgeschreven procedure houdt in dat alvorens tot daadwerkelijke uitgifte over te gaan van een aangevraagd certificaat, het certificaat door een auditor wordt gecontroleerd. Geconstateerde fouten leiden tot het blokkeren van de uitgifte. Het al aangemaakte certificaat wordt dan ingetrokken. De grootste uitval deed zich voor bij de productie van smartcards. Smartcards met zogenaamde persoonsgebonden certificaten bevatten vanwege de diverse functies drie certificaten. Een intrekking wordt als drie geteld.
Feitelijk is het aantal intrekkingen bij de versnelde omwisseling na Diginotar een goede indicatie dat de veiligheidsvoorschriften van PKIoverheid nauwgezet worden nageleefd. Overigens is informatie over de ingetrokken certificaten algemeen publiekelijk toegankelijk. Deze informatie staat dus los van de hack.

In de berichtgeving is de suggestie gedaan dat enkele organisaties niet handelde conform de aangescherpte beveiligingsbeleidslijn met betrekking tot de nieuwe generatie certificaten en dat daar geen toezicht op zou zijn. Dit is onjuist. Alle partijen hebben hun maatregelen getroffen om aan deze nieuwe standaard lijn te voldoen. De uitzonderingen zijn bewust na overleg verleend, bijvoorbeeld omdat de omschakeling automatiseringstechnisch gezien meer tijd vergt.

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