Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 267

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 februari 2013

Tijdens het vragenuur van 15 januari j.l. (Handelingen II, 2012/2013, nr. 39 mondelinge vragen van het lid Voortman over een ernstig beveiligingslek op de website van DigiD) heb ik u toegezegd de evaluatie van Logius over de calamiteit bij Ruby on Rails software waardoor DigiD op 9 januari tijdelijk uit de lucht is geweest, aan de Kamer toe te zenden. Bijgaand treft u het verslag van de evaluatie aan[1]. Het betreft een interne technische evaluatie van Logius zoals dat regulier gebeurt na een calamiteit, waarbij het verloop van de calamiteit en de opvolging die daarop plaatsvindt wordt vastgelegd en beoordeeld op leerpunten. Dat heeft ook deze keer plaatsgevonden.

Op 9 januari 2013 werd een risico gedetecteerd bij de open source software Ruby on Rails waar ook DigiD gebruik van maakt. In de uren die daarop volgden zijn er wereldwijd meer dan 1000 websites en diensten tijdelijk uit de lucht gehaald om het risico te repareren. DigiD was één van de diensten die tijdelijk werd uitgeschakeld om het mogelijk lekken van persoonsgegevens tegen te gaan.

Uit de evaluatie van de calamiteit van 9 januari komt naar voren dat er sprake was van een zodanige kwetsbaarheid in de onderliggende software van DigiD, het ontwerpplatform Ruby on Rails, dat het voor het handhaven van de integriteit van DigiD geboden was om direct maatregelen te nemen. Hieraan is – na overleg met het Nationaal Cyber Security Centrum (NCSC) – gevolg gegeven door DigiD uit de lucht te halen en aanpassingen in de software door te voeren, zodat de bedoelde kwetsbaarheid werd ondervangen. Dit is binnen de kortst mogelijke tijd gerealiseerd.

Belangrijk is de constatering dat, ook na het nader onderzoek, geen aanwijzingen zijn gevonden dat misbruik van de kwetsbaarheid in Ruby

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

kst-26643-267
ISSN 0921 - 7371
's-Gravenhage 2013

on Rails is gemaakt op DigiD en dat er dus geen persoonsgegevens van burgers in verkeerde handen terecht zijn gekomen.

Uit de evaluatie komt verder naar voren dat in dit geval direct gekozen is voor het publiceren van de maatregel om DigiD preventief uit de lucht te halen, hetgeen heeft geleid tot veel media-aandacht en vragen. Ondanks het beleid dat de belangrijkste dienstverleners die van DigiD gebruik maken snel door Logius moeten worden geïnformeerd, blijkt dat sommigen toch eerder via de media hebben vernomen dat de dienst tijdelijk uit de lucht was. Dat punt is onderkend en onderwerp van nader gesprek met de dienstverleners. Daarbij moet wel de kanttekening worden gemaakt dat onder omstandigheden zodanige spoed geboden kan zijn dat maatregelen onverwijld genomen dienen te worden. Dat past binnen de verantwoordelijkheden en het mandaat van de beheerorganisatie Logius. Mij hebben overigens geen signalen bereikt dat het afschakelen van DigiD bij uitvoeringsorganisaties of andere overheidsdienstverleners tot onoverkomelijke problemen heeft geleid.

Dit is de eerste keer in de geschiedenis van DigiD dat deze dienst gedurende 10 uur uit de lucht is geweest. DigiD kent een zeer hoog beschikbaarheidspercentage. In het afgelopen jaar betrof dat 99,83%.

Het voorgaande neemt niet weg dat er voortdurend waakzaamheid is geboden voor incidenten en dat het belangrijk is om de veiligheid en prestaties van het authenticatieproces op peil te houden. Zoals bekend vinden zowel bij DigiD als de afnemers van DigiD ICT-beveiligings-assessments plaats op de ICT-omgeving van de betrokken organisaties. Penetratietesten op de aangesloten applicaties maken daar onderdeel van uit. Hiernaast loopt het traject van de Taskforce ICT en veiligheid dat in het leven is geroepen om het bewustzijn van bestuurders en hoger management voor de noodzaak van informatiebeveiliging te bevorderen.

Ten aanzien van de suggestie van mevrouw Voortman om te overwegen om bankmiddelen in te zetten als authenticatiemiddel voor overheids-dienstverlening, kan ik u melden dat vorig jaar een ambtelijke verkenning is afgerond naar de ontwikkeling van een stelsel van elektronische identiteit, waarbij de inzet van particuliere instrumenten naast de bestaande overheidsmiddelen mogelijk wordt gemaakt. Reden voor de ontwikkeling van een stelsel van elektronische identiteit is overigens niet de onveiligheid van de bestaande overheidsvoorzieningen, maar de stimulering van de digitalisering van de dienstverlening, ook in Europees verband. Ook het vergoten van keuzemogelijkheden voor burgers en bedrijven en het wegnemen van het onderscheid in die gevallen (ZZP-ers) waarin dat onderscheid eigenlijk niet goed te maken is, zijn daarbij belangrijke uitgangspunten. Er heeft evenwel over de ontwikkeling van een stelsel van elektronische identiteit nog geen politieke besluitvorming plaatsgevonden.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk