Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 331

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 31 oktober 2014

In de uitzending van het programma Opgelicht van 28 oktober jl. kwam een kwetsbaarheid bij websites van o.a. 12 gemeenten aan de orde. Hackers zouden deze kwetsbaarheid hebben kunnen misbruiken om kwaadaardige software te plaatsen. In de uitzending werd met name ingegaan op de mogelijkheid om gegevens van DigiD gebruikers af te vangen. Verder kwamen enkele slachtoffers van fraude via DigiD aan het woord. Deze fraudegevallen staan overigens los van de betreffende kwetsbaarheid.

Kwetsbaarheid in het ContentManagementSysteem

In september van dit jaar is bij Logius door een softwareleverancier melding gemaakt van een kwetsbaarheid in hun ContentManagement-Systeem (CMS) bij 12 gemeenten. Deze kwetsbaarheid is volgens de softwareleverancier van dit CMS binnen 24 uur na ontdekking gedicht. Uit onderzoek van een gerenommeerd beveiligingsbureau en de softwareleverancier zelf, bleek dat er geen aanleiding was om aan te nemen dat er gegevens in verkeerde handen zijn gevallen. Dat wil niet zeggen dat dit signaal vervolgens niet zeer serieus genomen is. Logius heeft het Nationaal Cyber Security Center (NCSC), de informatiebeveiligingsdienst voor gemeenten (IBD) en het Ministerie van BZK geïnformeerd over de kwetsbaarheid en de gekozen oplossing. De betreffende gemeenten zijn ook onverwijld geïnformeerd door hun leverancier en door Logius. De namen van de betrokken gemeenten en andere organisaties zijn niet bekend gemaakt. Er wordt uit veiligheidsoverwegingen nooit met derden gecommuniceerd over welke organisaties te maken hebben met welke beveiligingsrisico's. Het al dan niet informeren van burgers is een verantwoordelijkheid van organisaties zelf.

kst-26643-331
ISSN 0921 - 7371
's-Gravenhage 2014

De kwaliteit van de maatregelen

Hetzelfde gespecialiseerde beveiligingsbureau heeft in opdracht van Logius de kwaliteit van de oplossing van de kwetsbaarheid onderzocht alsook de toepassing op de systemen. Daarbij is vastgesteld dat de kwetsbaarheid door middel van de oplossing is verholpen en niet meer op de getroffen systemen aanwezig is. Afrondend is ook onderzoek gedaan naar mogelijke aan deze kwetsbaarheid te relateren onregelmatigheden bij DigiD gebruik. Ook daar is geen reden gevonden te vrezen dat DigiD gegevens in handen van derden zijn gevallen. Dit onderzoek is bij alle 12 gemeenten gedaan. Omdat er in dit geval geen enkele concrete aanwijzing was van exploitatie van deze kwetsbaarheid is van nader onderzoek verder afgezien.

Assessments

Gemeenten zijn, net als alle afnemers van DigiD, gehouden te voldoen aan een DigiD beveiligingsassessment. Bij dit beveiligingsassessment worden de relevante beveiligingsnormen van het National Cyber Security Center door gecertificeerde auditors getoetst. Dat is ook gedaan bij de betrokken organisaties. Deze kwetsbaarheid is niet gebleken in het assessment traject. Logius onderzoekt dit nader en er zullen op basis daarvan maatregelen worden genomen.

Certificaten

In de uitzending werd ook gesteld dat DigiD gebruik zou maken van een certificaat die niet zou voldoen aan de moderne beveiligingseisen. Dat is niet juist. De in de uitzending getoonde cryptografie maakt geen onderdeel uit van het certificaat. De cryptografie waarmee DigiD wordt beveiligd staat in het certificaat zelf onder het tabblad bij het veld «handtekening hash-algoritme». Het certificaat van DigiD maakt gebruik van het moderne en veilige algoritme SHA256 en niet zoals in de uitzending werd gesuggereerd het minder veilige SHA1 algoritme.

Fraude met DigiD

In dezelfde uitzending kwamen ook slachtoffers van fraude met DigiD aan het woord. Die gevallen waren geen gevolg van een fout of lek in het DigiD-systeem, maar bijvoorbeeld van gebruik/misbruik van een DigiD-account door een (ex-) partner of als gevolg van phishing. Uit de voorbeelden bleek hoe groot het risico is als inlogcodes in verkeerde handen vallen. Het is van groot belang dat mensen zorgvuldig met hun inloggegevens omgaan, geen phishing mails beantwoorden en zorgdragen voor een adequate virusscanner. Aan dit belang wordt momenteel ook veel aandacht besteed in de Alert Online-campagne, waarin onder meer de website www.veiliginternetten.nl is gelanceerd. Als mensen toch slachtoffer zijn geworden van fraude is adequate begeleiding uitermate belangrijk. De inzet van de overheid is slachtoffers snel te helpen en schadeloos te (doen) stellen. Slachtoffers van identiteitsfraude kunnen ook altijd bij het Centraal Meldpunt Identiteitsfraude terecht. Bij vastgestelde fraude wordt altijd aangifte gedaan. Wel blijkt zorgvuldig onderzoek van groot belang omdat helaas blijkt dat niet altijd op voorhand eenvoudig vast te stellen is wat er precies gebeurd is en daders en slachtoffers niet altijd eenduidig te onderscheiden zijn. De zaken van de in uitzending aan het woord gekomen slachtoffers worden nader onderzocht.

Het belang van voortdurende aandacht voor veiligheid

De uitzending laat andermaal het belang zien van een goede beveiliging van ICT systemen. Ook toont de uitzending de complexiteit die er is als die systemen in ketens worden gebruikt en welke gezamenlijke verantwoordelijkheid dit voor ketenpartners met zich meebrengt om te kunnen voldoen aan de steeds hogere eisen die door nieuwe bedreigingen ontstaan. Het is duidelijk dat dit werk nooit klaar zal zijn.

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