Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

515

Vragen van de leden **Oosenbrug** en **Fokke** (beiden PvdA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *een lek in DigiD* (ingezonden 30 oktober 2014).

Antwoord van Minister **Plassterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 10 november 2014).

Vraag 1
Heeft u kennisgenomen van het item over beveiligingsproblemen bij Digid in de Uitzending van Opgelicht?[1]

Antwoord 1
Ja

Vraag 2
Is het waar dat er een lek in de beveiliging van Digid bij meerdere gemeenten en instanties is of was? Zo nee, hoeveel en welke gemeenten en andere organisaties waren gevoelig voor dit lek?

Antwoord 2
Nee, er was geen lek in de beveiliging van DigiD. In september van dit jaar is bij Logius door een softwareleverancier melding gemaakt van een kwetsbaarheid in een specifieke versie van hun ContentManagementSysteem (CMS). Na onderzoek van Logius bleek bij 12 gemeenten de koppeling van het betreffende CMS met DigiD zodanig te zijn opgebouwd dat er een potentieel risico bestond dat DigiD misbruikt kon worden.
Logius heeft de namen van de betrokken gemeenten en andere organisaties niet bekend gemaakt omdat het aan de betrokken organisaties zelf is om daar wel of geen mededelingen over te doen. Het betrof immers een kwetsbaarheid in een CMS dat door die organisaties wordt gebruikt.

Vraag 3
Kunt u uitleggen hoe het lek ontstaan is, op welke wijze er gebruik van gemaakt kon worden en welke informatie daarmee verkregen kon worden?

[1] Opgelicht, 28 oktober 2014, NPO1

ah-tk-20142015-515
ISSN 0921 - 7398
's-Gravenhage 2014

Antwoord 3
Het betrof een kwetsbaarheid in een specifieke versie van een ContentManagementSysteem. Hackers zouden deze kwetsbaarheid hebben kunnen misbruiken om kwaadaardige software te plaatsen en daarmee in theorie de mogelijkheid hebben om allerlei gegevens en handelingen van bezoekers aan betreffende gemeentesites af te vangen.

Vraag 4
Sinds wanneer zijn de betrokken gemeenten en Logius op de hoogte van het lek? Wat is in de tussentijd gedaan om het lek te dichten en te onderzoeken of er daadwerkelijk mensen slachtoffer zijn geworden van dit lek?

Antwoord 4
Op 25 september van dit jaar is bij Logius door een softwareleverancier melding gemaakt van een kwetsbaarheid in hun ContentManagementSysteem (CMS). De kwetsbaarheid was volgens de softwareleverancier van het CMS binnen 24 uur na ontdekking (18 september) gedicht. De softwareleverancier heeft een patch ontwikkeld en toegepast bij de getroffen gemeenten om de specifieke kwetsbaarheid te verhelpen. De softwareleverancier heeft de gemeenten daarover geïnformeerd.
Naar aanleiding van het onderzoek uitgevoerd door de softwareleverancier, met ondersteuning van een gerenommeerd beveiligingsbureau, zijn geen sporen aangetroffen die aannemelijk maken dat de systemen gecompromitteerd zijn.
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.
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 door Logius 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 uitgevoerd. Omdat er in dit geval geen enkele concrete aanwijzing was van exploitatie van deze kwetsbaarheid is van nader onderzoek verder afgezien.

Vraag 5
Zijn alle mensen waarvan de gegevens kwetsbaar geweest zijn door dit lek door de desbetreffende gemeenten en instanties geïnformeerd? Zo nee, waarom niet? Zo ja, wordt hun aangeraden om maatregelen te nemen naar aanleiding van dit lek?

Antwoord 5
Het al dan niet informeren van burgers is een verantwoordelijkheid van de organisaties zelf.
Naar aanleiding van het onderzoek uitgevoerd door de softwareleverancier, met ondersteuning van een gerenommeerd beveiligingsbureau, zijn geen sporen aangetroffen die aannemelijk maken dat de systemen gecompromitteerd zijn.
Afrondend is ook onderzoek gedaan door Logius 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.
Voor wat betreft wachtwoorden is het regelmatig wijzigen daarvan een standaardadvies dat Logius continu geeft, onder meer via de website www.digid.nl. Ook zijn de eisen voor DigiD-wachtwoorden sinds mei 2014 verscherpt, waardoor gebruikers met een zwak wachtwoord een nieuw – sterker – wachtwoord moeten aanmaken. Voor nieuwe aanvragen gold deze eis al langer. Deze casus is geen aanleiding geweest om daar gericht nog meer aandacht aan te geven dan al voortdurend wordt gedaan.

Vraag 6
Deelt u de mening dat zeer grondig onderzocht moet worden of er mensen slachtoffer zijn geworden van dit lek in DigiD? Zo ja, klopt het bericht van Fox-IT dat niet bij alle kwetsbare gemeenten en instanties onderzoek is gedaan naar misbruik van het lek? Wilt u alsnog opdracht geven om bij alle betrokken gemeenten en instanties onderzoek te doen naar misbruik van het lek, om een maximale inspanning te doen om alle slachtoffers te achterhalen?

Antwoord 6
Naar aanleiding van het onderzoek uitgevoerd door de softwareleverancier, met ondersteuning van een gerenommeerd beveiligingsbureau, zijn geen sporen aangetroffen die aannemelijk maken dat de systemen gecompromitteerd zijn. Dit onderzoek is onder een aantal gemeenten uitgevoerd.
Afrondend is ook onderzoek gedaan door Logius 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 uitgevoerd.
Omdat in beide onderzoeken geen enkele concrete aanwijzing is gevonden van exploitatie van deze kwetsbaarheid ben ik nog steeds van mening dat nader onderzoek niet nodig is.

Vraag 7
Is het waar dat DigiD gebruik maakt van certificaten die niet voldoen aan de moderne beveiligingseisen? Zo ja, wanneer wordt dit opgelost en waarom zijn deze certificaten niet eerder vervangen?

Antwoord 7
In de uitzending werd gesteld dat DigiD gebruik zou maken van een certificaat dat 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.

Vraag 8
Deelt u de mening dat het zorgelijk is dat gemeenten belangrijke onderdelen van de infrastructuur voor de digitale overheid zo slecht beheren? Is dit voor u reden om de decentrale infrastructuur, waarbij iedereen verantwoordelijk is voor de beveiliging van zijn eigen systemen, te heroverwegen en bijvoorbeeld een standaard (kern)website voor gemeenten te ontwikkelen?

Antwoord 8
Nee, ik deel deze mening niet. Er is geen sprake van een zorgelijke situatie. De gemeenten hebben juist een goed informatieveiligheidsbeleid opgezet. In november 2013 hebben gemeenten onderling goede afspraken gemaakt over informatieveiligheidsbeleid in de resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeenten. De in januari 2013 opgerichte gemeentelijke Informatiebeveiligingsdienst (IBD), ondersteunt gemeenten in bewustwording en met het op een hoger plan tillen van hun informatieveiligheidsbeleid. De IBD heeft, zoals het tot haar taak behoort, adequaat gereageerd op kwetsbaarheden, die er nu eenmaal kunnen zijn in ICT.
Het kwaliteitsinstituut voor Nederlandse Gemeenten (KING) onderzoekt momenteel de mogelijkheid om gemeenten gebruik te kunnen laten maken van een meer gestandaardiseerde (kern)website.

Vraag 9
Welke van de getroffen gemeenten en instanties heeft een positieve audit uit laten voeren op zijn DigiD-systemen? Wat zegt dit over de waarde en de betrouwbaarheid van de audits en welke conclusies verbindt u hieraan?

Antwoord 9
Gemeenten zijn, net als alle afnemers van DigiD, gehouden te voldoen aan een DigiD beveiligingsassessment. Bij dit beveiligingsassessment worden een selectie van beveiligingsnormen uit de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC, door gecertificeerde auditors getoetst. Dat is ook gedaan bij de betrokken organisaties. Deze kwetsbaarheid is niet gebleken in het assessment traject. Logius heeft inmiddels overleg gevoerd met NOREA, de beroepsorganisatie van IT-auditors. Naar aanleiding hiervan is NOREA gestart met een verkennend onderzoek. Overigens is de betreffende kwetsbaarheid door een beveiligingsaudit ontdekt. Dit onderschrijft het nut en de noodzaak voor het uitvoeren van audits.