Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directoraat Generaal Bestuur enKoninkrijksrelaties

Turfmarkt 147
Den Haag
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2014-0000593934

Uw kenmerk

Datum 7 november 2014
Betreft Beantwoording Kamervragen "inzake veiligheid DigiD n.a.v. tv-uitzending Opgelicht"

In antwoord op uw brief van 31 oktober 2014 deel ik u mede dat de schriftelijke vragen van de vaste commissie voor Binnenlandse Zaken worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk

Bijlage: antwoorden op vragen vaste commissie voor Binnenlandse Zaken inzake veiligheid van DigiD
Kenmerk: 2014Z19101/2014D39353

1 Wat was / is er volgens u feitelijk, en in chronologische volgorde, gebeurd ?

Op 25 september van dit jaar is bij Logius door een softwareleverancier melding gemaakt van een kwetsbaarheid in 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.

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 betrokken gemeenten geïnformeerd.

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.

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.

2 Bij welke gemeenten (volgens het programma Opgelicht 12 gemeenten) is, of was er geen goede beveiliging naar de DigiD-inlogpagina, een zogenoemd 'lek'?

In totaal zijn 12 gemeenten getroffen door de kwetsbaarheid in hun CMS systeem. 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. Er was geen lek in de beveiliging van DigiD zelf.

3 Hoelang heeft dit lek bestaan?

De softwareleverancier heeft in een gesprek op vrijdag 26 september jl. aan vertegenwoordigers van Logius aangegeven dat de betreffende kwetsbare versie van het CMS in totaal 14 maanden aanwezig is geweest.

4 Waarom is dit lek niet eerder geconstateerd?

Dit was een tot dan toe onbekende kwetsbaarheid. Overigens is de betreffende kwetsbaarheid door een beveiligingsaudit ontdekt. Dit onderschrijft het nut en de noodzaak voor het uitvoeren van audits.

5 Waarom is dit lek niet eerder naar buiten gebracht?

Zie antwoord vraag 4

6 Was er het plan om het lek helemaal niet naar buiten te brengen?

Op basis van een risicoafweging is besloten dat er geen aanleiding was om naar buiten te treden over deze kwetsbaarheid. De kwetsbaarheid kwam namelijk voor bij een beperkt aantal gemeenten en is zeer snel verholpen. Op 25 september is Logius door de softwareleverancier op de hoogte gesteld over de kwetsbaarheid in hun ContentManagementSysteem (CMS) en dat deze kwetsbaarheid binnen 24 uur na ontdekking (18 september) is opgelost. De softwareleverancier heeft de gemeenten daarover ook geïnformeerd.

Logius heeft op 8 oktober, naar aanleiding van het persbericht over deze kwetsbaarheid van beveiligingsbureau DeltaISIS, een persverklaring afgegeven. Hierin heeft Logius de kwetsbaarheid bevestigd en verklaard dat na onderzoek was gebleken dat bij 12 gemeenten de koppeling van het betreffende CMS met DigiD zodanig is 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.

7 Welke maatregelen worden genomen om lekken in het DigiD-systeem eerder te constateren?

De kwetsbaarheid had betrekking op het CMS dat door de betreffende gemeenten wordt gebruikt. Er was geen lek in de beveiliging van DigiD zelf. De beveiliging van DigiD heeft de permanente aandacht van Logius. DigiD wordt regelmatig onderworpen aan zware penetratietesten. De laatste testreeks is enkele weken geleden uitgevoerd. Afnemers van DigiD dienen ook jaarlijks een ICT-beveiligingsassessment naar de veiligheid van hun aan DigiD gekoppelde webomgeving uit te laten voeren en een auditrapport in te dienen. Als er een acuut beveiligingsrisico wordt geconstateerd, gaat Logius altijd over tot afsluiting van DigiD aansluitingen.

8 Is er misbruik gemaakt van dit lek? Zijn er aanwijzingen dat van de geconstateerde zwakheden in de digitale infrastructuur gebruik gemaakt is?

Nee, er zijn geen aanwijzingen dat er misbruik is gemaakt van de kwetsbaarheid. 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.

Logius heeft zelf ook onderzoek gedaan naar mogelijke, aan deze kwetsbaarheid te relateren, onregelmatigheden in het gebruik van DigiD bij de getroffen gemeenten. Ook daar is geen reden gevonden te vrezen dat DigiD gegevens in handen van derden zijn gevallen.

Omdat er geen enkele concrete aanwijzing was van exploitatie van deze kwetsbaarheid is op basis van risicoafweging besloten van nader onderzoek af te zien.

9 Indien er geen sprake van misbruik is geweest, hoe zeker weet u dit? Hoe is hier onderzoek naar uitgevoerd?

Zie antwoord op vraag 8. Over de werkwijze bij onderzoeken / maatregelen die de informatieveiligheid aangaan kunnen om redenen van veiligheid geen nadere mededelingen worden gedaan.

10 Waarom zijn de burgers die het betreft niet achteraf op de hoogte gesteld van het lek?

Het is aan de betrokken organisaties zelf om daar wel of geen mededelingen over te doen. Het betrof immers een kwetsbaarheid in een CMS dat door die organisaties wordt gebruikt. Betrokken organisaties zijn zelf verantwoordelijk voor hun informatieveiligheid.

11 Heeft, behalve bij een aantal gemeenten, op meerdere plekken de poort naar de DigiD-gegevens opengestaan? Zo ja, op welke plaatsen ? Zo nee, hoe is vastgesteld dat dit niet het geval is?

Nee, er zijn buiten de 12 gemeenten geen andere organisaties waarbij de mogelijkheid bestond dat DigiD gegevens misbruikt konden worden. Uit onderzoek van Logius is gebleken dat alleen de 12 gemeenten die deze specifieke versie van het contentmanagementsysteem in gebruik hebben en bij deze gemeenten de koppeling van het betreffende CMS met DigiD zodanig is opgebouwd dat er een potentieel risico bestond dat DigiD misbruikt kon worden.

12 Was uzelf op de hoogte van dit lek, en zo ja, vanaf welk moment ? Indien u op de hoogte was, waarom heeft u de Kamer hier niet over geïnformeerd? Indien u niet op de hoogte was, waarom was u niet op de hoogte?

Ik ben op de hoogte gesteld over de kwetsbaarheid op 8 oktober.
De kwetsbaarheid kwam voor bij een beperkt aantal gemeenten en is zeer snel na ontdekking verholpen. Indien er een acuut beveiligingsrisico was geconstateerd voor DigiD, was ik uiteraard gelijk overgegaan tot afsluiting van de betreffende DigiD aansluitingen en had ik de Kamer daarover geïnformeerd. Dit was echter niet aan de orde. Zie verder antwoord op vraag 6.

13 Is het lek nu op alle plekken gedicht? Is de beveiliging van DigiD op deze plekken weer op orde?

Ja, de kwetsbaarheid in het CMS van 12 gemeenten is verholpen. Voor de goede orde er was geen lek in de beveiliging van DigiD zelf.

14 Hoe is het mogelijk dat zoveel gemeenten hun ICT niet op orde hebben?

Het ontdekken van kwetsbaarheden is aan de orde van de dag. 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.

15 Zijn de ten behoeve van DigiD gebruikte certificaten van voldoende niveau naar hedendaagse maatstaven? Zo nee, wanneer zijn ze dit wel?

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.

16 Is het beveiligingsniveau van DigiD nu over de volle breedte weer op orde? Zo nee, wat moet hiervoor nog gebeuren?

Ja, het beveiligingsniveau binnen de keten van DigiD met betreffende gemeenten is weer op orde sinds de softwareleverancier de patch beschikbaar heeft gesteld en heeft doorgevoerd in de specifieke versie van haar contentmanagementsysteem.

17 Welke maatregelen zijn er voorzien voor de verdere verbetering van DigiD en wanneer zullen deze zijn geïmplementeerd?

Zoals eerder toegezegd wordt de Kamer per separate brief over de mogelijkheden tot versterking van DigiD geïnformeerd.

18 Welke matregelen gaat u treffen ten aanzien van gemeenten die de toegang vanuit hun website naar de inlog voor de DigiD-omgeving niet consequent goed beveiligd houden?

Afnemers van DigiD dienen jaarlijks een ICT-beveiligingsassessment naar de veiligheid van hun aan DigiD gekoppelde webomgeving uit te laten voeren en een auditrapport in te dienen. Als er een acuut beveiligingsrisico wordt geconstateerd, gaat Logius altijd over tot afsluiting van DigiD aansluitingen.

19 Welke maatregelen neemt u om te voorkomen dat mensen inloggen op een gespoofde DigiD-website?

Logius doet er alles aan om het gebruik van DigiD veilig te houden. Bij ontdekking van zogeheten gespoofde sites worden deze websites in samenwerking met de Belastingdienst en het Nationaal Cyber Security Center (NCSC) zo snel mogelijk uit de lucht gehaald. Dit jaar zijn er al 40 sites op deze manier uit de lucht gehaald.

Op de website van DigiD wordt door Logius advies gegeven over het veilig omgaan met DigiD. Daarbij wordt onder meer gewezen op het belang dat de gebruiker controleert dat hij/zij daadwerkelijk inlogt op de echte inlogpagina van DigiD. Ook wordt gewaarschuwd voor valse e-mails waarin wordt gevraagd om inloggegevens in te vullen. Bovendien wordt uitgelegd hoe de gebruiker misbruik van zijn account kan herkennen en welke actie hij kan ondernemen bij geconstateerd misbruik.

20 Wat gaat u doen om de slachtoffers te helpen die er nu al zijn in verband met ongeautoriseerde toegang tot DigiD?
21 Bent u voornemens een afdeling op te zetten die casus van benadeelden beoordeeld? Zo ja, hoe wordt die vormgegeven? Of ligt die bevoegdheid, of blijft die bevoegdheid liggen, bij respectievelijk Logius en de afnemers? Welk risico houdt dat in voor het afschuiven van problemen binnen de keten?
22 Vindt u het terecht dat mensen, die buiten hun eigen schuld slachtoffer worden van veiligheids-problemen rond DigiD, bijvoorbeeld door uit de brievenbus geviste brieven, geld, dat ze nooit hebben aangevraagd en nooit hebben ontvangen, moeten terugbetalen aan de overheid?

In de uitzending kwamen enkele slachtoffers van fraude via DigiD aan het woord. Deze fraudegevallen staan overigens los van de betreffende kwetsbaarheid.
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.