Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 328

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 oktober 2014

Op 6 augustus jl. hebben diverse media[1] bericht dat het Amerikaanse bedrijf Hold Security (hierna te noemen Hold) in het bezit zou zijn van 1,2 miljard inloggegevens en 500 miljoen e-mailadressen. In mijn antwoorden d.d. 3 september op vragen van de leden Verhoeven en Berndsen (Aanhangsel Handelingen II 2013/14, nr. 2947) heb ik aangegeven dat het Nationaal Cyber Security Centrum (NCSC) direct contact heeft gezocht met Hold, maar dat het daarbij nog geen gedetailleerde informatie had verworven. Daarbij is aangegeven dat het NCSC conform haar rol in nauw contact staat met internationale partners om alsnog aanvullende informatie te verkrijgen. Inmiddels is het NCSC erin geslaagd om het Nederlandse gedeelte van deze gegevens van Hold in bezit te krijgen. Met deze brief stel ik u op de hoogte van de resultaten van deze inspanningen en de bijbehorende ingezette respons-acties.

Verkregen gegevens en duiding van deze gegevens

De gegevens die het NCSC heeft verkregen zijn gegevens die als Nederlandse gegevens aan te merken zijn. Het NCSC heeft daarbij louter de voor de respons noodzakelijke gegevens in bezit en beschikt daarmee niet over de in de grotere dataset voorkomende wachtwoorden.

Het betreft hierbij de volgende gegevens:
1. een dataset van circa 5600 mogelijk nog kwetsbare websites binnen het.nl-domein en;
2. een dataset van circa 1,3 miljoen e-mailadressen met een.nl-extensie.

Het NCSC heeft de impact voor rijksoverheid en de vitale sectoren ingeschat aan de hand van bij het NCSC bekende gegevens over deze partijen. De impact wordt op basis van deze gegevens als beperkt ingeschat. De veiligheid van de websites die de rijksoverheid beheert met

[1] Zie o.a. Tweakers, 6 augustus 2014, http://tweakers.net/nieuws/97664/hackers-stelen-1-komma-2-miljard-inloggegevens-en-500-miljoen-e-mailadressen.html

kst-26643-328
ISSN 0921 - 7371
's-Gravenhage 2014

kritieke voorzieningen in het contact met burgers (zoals bijvoorbeeld de Belastingdienst en DigiD) zijn daarbij niet in het geding geweest. Ook de impact op vitale sectoren wordt vooralsnog als beperkt ingeschat.

Ingezette response-acties door het NCSC en haar partners

In de tweede helft van september is met een aantal respons-partners (Stichting Internet Domeinregistratie (SIDN), de Informatiebeveiligingsdienst voor Gemeenten (IBD), Surfnet, Defensie en Internet Service Providers (ISP's) gewerkt aan het vormgeven van de respons. De respons is gericht op het wegnemen van kwetsbaarheden in de betrokken websites en het zo veel als mogelijk informeren van eindgebruikers dat hun e-mailadressen in de dataset voorkomen.

Een gecoördineerde respons is noodzakelijk aangezien het een overheid enerzijds niet past om langer dan noodzakelijk te beschikken over gegevens over mogelijk kwetsbare websites en gegevens van consumenten en het anderzijds operationeel noodzakelijk is om gezamenlijk zorgvuldige voorbereidingen te treffen voor een omvangrijke responsactie. Deze is vormgegeven langs drie actielijnen:

1. Het informeren van eigenaren van mogelijk nog kwetsbare websites via Stichting Internet Domeinregistratie Nederland (SIDN) en de zogeheten registrars (de partijen die voor bedrijven of eindgebruikers domeinen bij SIDN registreren), ten einde de kwetsbaarheid te verhelpen. Gelijktijdig informeert de Informatiebeveiligingsdienst voor gemeenten (IBD) betrokken gemeenten, SURFnet de academische en onderzoeksinstellingen en het Ministerie van Defensie de aan hen gelieerde organisaties.
2. Het NCSC informeert conform de reguliere rol partijen binnen de rijksoverheid en de vitale sectoren op basis van eerder door deze partijen bij het NCSC aangeleverde gegevens over door hen gebruikte mailadressen en websites. Daar waar nog additionele gegevens worden aangereikt door partijen binnen de rijksoverheid en de vitale sectoren zullen deze zo spoedig mogelijk worden verwerkt.
3. Daarnaast zijn ook de Internet Service Providers in stelling gebracht om de eigenaren van betrokken mailadressen met een.nl-extensie actief te bereiken.

Met deze ingezette acties worden alle eigenaren van getroffen websites bereikt. Ook wordt het overgrote deel, zo'n viervijfde, van de getroffen Nederlandse gebruikers die gebruik maken van een mailadres met een.nl-extensie de komende dagen bereikt. Omdat zoals eerder aangegeven mailadressen met een extensie anders dan.nl (zoals bijvoorbeeld de.com-domeinen) niet door het NCSC zijn opgevraagd, is het niet mogelijk die groep gebruikers te informeren.

De Hold-casus maakt daarnaast evenwel duidelijk dat dergelijke omvangrijke datasets met getroffen gegevens, waaronder in belangrijke mate persoonsgegevens, in toenemende mate in handen zijn van kwaadwillenden of goedwillende derde (bijvoorbeeld commerciële) partijen, en ook bekend bij het NCSC. Daarom verkent het NCSC samen met alle mogelijke responspartners de komende periode hoe de ervaringen uit deze casus geborgd kunnen worden in een te ontwikkelen structurele voorziening met de daarbij benodigde juridische waarborgen.

De bovengenoemde acties sluiten aan op de tweede Nationale Cyber Security Strategie en het daarin genoemde streven naar een optimale balans tussen vrijheid, veiligheid en maatschappelijke groei.

Handelingsperspectief

Diefstal van inloggegevens komt helaas regelmatig voor. Naar aanleiding van deze specifieke casus heeft het NCSC een aantal adviezen voor zowel eindgebruikers als beheerders van websites op www.ncsc.nl geactualiseerd. Eindgebruikers wordt te allen tijde aangeraden om regelmatig van wachtwoord te wisselen en voor verschillende toepassingen ook verschillende wachtwoorden te gebruiken. Voor beheerders van websites heeft het NCSC, en haar voorganger govcert.nl, sinds 2008 een factsheet over de kwetsbaarheid voor SQL-injectie.

Slot

De geschetste kwetsbaarheden in websites en het voorkomen van e-mailadressen in omvangrijke datasets van gelekte gegevens illustreren het belang van de bewustheid en bekwaamheid (awareness) van eindgebruikers. Tijdens de campagne Alert Online die van 27 oktober tot 6 november voor de derde maal gehouden zal worden zal hier nogmaals aanvullende aandacht voor gevraagd worden.

De Minister van Veiligheid en Justitie,
I.W. Opstelten