Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

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

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2016-0000164302

Uw kenmerk
2016Z05065

Datum 24 maart 2016

Betreft Beantwoording Kamervraag van de leden Veldman, De Caluwé en Oosenbrug over het bericht «beveiliging tientallen gemeentesites lek: persoonsgegevens niet veilig» (ingezonden

Hierbij bied ik u de antwoorden aan op de schriftelijke vragen die zijn gesteld door de leden Veldman en De Caluwé (beiden VVD) en Oosenbrug (PvdA) over het bericht *«beveiliging tientallen gemeentesites lek: persoonsgegevens niet veilig»*.

Deze vragen werden ingezonden op 10 maart 2016, met kenmerk 2016Z05065.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk

Datum
24 maart 2016

Kenmerk
2016-0000164302

2016Z05065

Vragen van de leden Veldman en De Caluwé (beiden VVD) en Oosenbrug (PvdA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over het bericht *«beveiliging tientallen gemeentesites lek: persoonsgegevens niet veilig»* (ingezonden 10 maart 2016).

1
Heeft u kennisgenomen van het bericht «beveiliging tientallen gemeentesites lek: persoonsgegevens niet veilig»? 1)

Antwoord:
Ja

2
Herinnert u zich de antwoorden op eerdere vragen over het onderwerp beveiliging van persoonsgegevens bij gemeenten? 2)

Antwoord:
Ja

3
Hoeveel gemeenten hebben de beveiliging van persoonsgegevens niet op orde?

Antwoord:
Op 1 maart heeft een groep onderzoekers de DROWN-aanvalstechnieken gepresenteerd. Met DROWN maakt een aanvaller misbruik van (web)servers die SSL 2.0 ondersteunen of die een verouderde versie van OpenSSL, een veel gebruikte oplossing om webservers te beveiligen, gebruiken. De onderzoekers hebben bekendgemaakt dat ongeveer een derde van alle webservers wereldwijd kwetsbaar is voor DROWN. De manier waarop gemeenten in samenwerking met hun toeleveranciers de kwetsbaarheid hebben opgelost kan niet tot de conclusie leiden dat gemeenten de beveiliging van persoonsgegevens niet op orde zouden hebben. Gemeenten nemen hun verantwoordelijkheid als het gaat om informatiebeveiliging en de bescherming van vertrouwelijke gegevens en hebben hiervoor een gemeenschappelijk normenkader in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Alle gemeenten implementeren momenteel de maatregelen en normen uit de BIG. Mij zijn dus geen gemeenten bekend die informatiebeveiliging in het algemeen of de beveiliging van persoonsgegevens in het bijzonder niet op orde zouden hebben.

4
Wat is uw reactie op het feit dat tientallen gemeentewebsites kunnen worden onderschept door een datalek in SSL? Bent u het er mee eens dat de overheid in alle gevallen de veiligheid van persoonsgegevens dient te waarborgen?

Antwoord:

De kwetsbaarheid die op 1 maart bekend werd doet zich voor zelfs als nieuwere versies van het protocol gebruikt worden, maar de oudere versies nog niet zijn uitgeschakeld. Op 2 maart publiceerde het NCSC hierover een factsheet, waarin het zijn advies herhaalde om de oudere versie uit te schakelen en servers uitsluitend op basis van het nieuwe protocol te configureren, alsmede om, indien gebruik gemaakt wordt van OpenSSL, deze bij te werken tot de meest recente versie.
De overheid is, net als alle andere verwerkers van persoonsgegevens, gehouden passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Overigens bestaat 100% veiligheid niet en zullen steeds nieuwe kwetsbaarheden worden ontdekt.

5
Welke stappen heeft u tot nog toe ondernomen om dit probleem op te lossen? Welke maatregelen treft u om de gemeenten ertoe te bewegen maatregelen te treffen om de beveiliging van persoonsgegevens op orde te brengen? Welke rol ziet u voor u zelf om de omgang met privacy door gemeenten te verbeteren?

Antwoord:
Informatiebeveiliging van gemeenten is een lokale verantwoordelijkheid. De BIG biedt voldoende technische, organisatorische en fysieke handvatten om de beveiliging van persoonsgegevens te kunnen waarborgen.

6
Wat doet de Autoriteit Persoonsgegevens (AP) anders dan 'verscherpte aandacht hebben' voor het geconstateerde probleem?

Antwoord:
Naast 'verscherpte aandacht' adviseert de Autoriteit Persoonsgegevens in haar nieuwsbericht van 4 maart 2016 verwerkers van persoonsgegevens om, indien gebruik wordt gemaakt van de programmeerbibliotheek OpenSSL, deze bij te werken naar de laatste versie en zij waarschuwt dat indien de configuratie niet wordt aangepast mogelijk artikel 13 van de Wet bescherming persoonsgegevens (Wbp) wordt overtreden.

7
Deelt u de mening dat de AP de beveiliging van persoonsgegevens bij gemeenten tot hoogste prioriteit moet benoemen en daarnaar handelen? Zo nee, waarom niet? Zo ja, welke (aanvullende) rol kan het Nationaal Cyber Security Center (NCSC) spelen?

Antwoord:
De AP heeft het onderwerp beveiliging van persoonsgegevens en het onderwerp lokale overheden als twee van haar vijf prioritaire thema's vastgesteld in haar 'Agenda 2016' en beschouwt dit dus als prioriteit, net als vorige jaren. Zij heeft ook meermaals onderzoek gedaan naar de beveiliging van persoonsgegevens bij gemeenten. Daarnaast heeft zij gesprekken gevoerd met de VNG en heeft zij

onder meer richtsnoeren en beleidsregels over beveiliging van persoonsgegevens gepubliceerd op haar website.
Het NCSC adviseert beheerders van websites hoe deze de geconstateerde kwetsbaarheid kunnen verminderen.
Ook steunt de Informatiebeveiligingsdienst voor gemeenten (IBD) gemeenten bij het opheffen van de kwetsbaarheid.

8
Deelt u de mening dat beheerders van de gemeentewebsites de site moeten updaten, zodat oudere SSL-technologieën niet meer worden ondersteund? Wat is uw reactie op de uitspraak van de onderzoeker van het beveiligingsbedrijf Dear Bytes dat het 'verbazingwekkend is dat overheidsinstanties nog gebruikmaken van zulke verouderde technologieën, terwijl er al meer dan vijf jaar veilige alternatieven zijn'?

Antwoord:
Zoals ik in het antwoord op vraag 4 aangaf, doet de kwetsbaarheid zich ook voor als er wel degelijk van nieuwe technologieën gebruik wordt gemaakt, maar de configuratie het gebruik van het oude protocol nog toestaat. Daarom luidt het advies om niet alleen de servers op basis van het nieuwe protocol te configureren, maar ook om gelijktijdig de oudere versie uit te schakelen. Gemeenten moeten passende maatregelen nemen om vertrouwelijke gegevens te beveiligen en beveiligd te houden. Het gaat hierbij om technische maar ook organisatorische en fysieke maatregelen. Bij bekendwording van de DROWN-kwetsbaarheid hebben gemeenten maatregelen genomen.

9
Kunt u aangeven welke sanctie er staat op een datalek zoals bedoeld in de Wet meldplicht datalekken? Kunt u aangeven of de gemeentes conform hun plicht in de Wet meldplicht datalekken hun bewoners hebben geïnformeerd? Zo nee, wat gaat u hieraan doen?

Antwoord:
Een datalek vormt op zichzelf niet direct aanleiding tot het opleggen van een sanctie. Indien een datalek ten onrechte niet bij de Autoriteit Persoonsgegevens gemeld wordt, kan de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen. Daarna kan de Autoriteit Persoonsgegevens eventueel een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 januari 2016 maximaal 820.000 euro. De boetebeleidsregels van de Autoriteit Persoonsgegevens die op haar website staan, geven hier een nadere invulling aan. Los van de boete kan de AP ook een last onder dwangsom opleggen. Tot slot heeft de AP de bevoegdheid om bij constateringen van overtreding van artikel 13 (over het vereiste om passende technische en organisatorische maatregelen te nemen ter beveiliging van persoonsgegevens) van de Wet bescherming persoonsgegevens een bindende aanwijzing, boete of last onder dwangsom op te leggen.

Of de DROWN-kwetsbaarheid bij gemeenten heeft geleid tot een datalek zullen deze gemeenten zelf vast moeten stellen. Een belangrijke vraag die de gemeente daarbij moet beantwoorden is of zij onrechtmatige verwerking redelijkerwijs kan uitsluiten. Of een eventueel datalek moet worden gemeld aan de toezichthouder, en eventueel aan de betrokkenen, hangt onder meer af van aard van de persoonsgegevens die het betreft. De Autoriteit Persoonsgegevens heeft beleidsregels meldplicht datalekken gepubliceerd op haar site. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en bij de betrokkenen.

10
Op welke wijze wordt binnen de GDI toegezien op het voorkomen van risico's voor burgers wanneer zij digitaal zaken doen met de overheid, nu in het kader van de Generieke Digitale Infrastructuur (GDI) afspraken worden gemaakt met decentrale overheden over digitale dienstverlening door de overheid ?

Antwoord:
Zoals ik in december 2015 aan uw Kamer meldde, bereid ik op dit moment, samen met de minister van Economische Zaken wetgeving voor ter ondersteuning van het voornemen uit het Regeerakkoord, dat burgers en bedrijven uiterlijk in 2017 zaken die ze met de overheid doen, digitaal kunnen afhandelen. Gestreefd wordt het wetsvoorstel voor de eerste tranche, met daarin de onderwerpen informatieveiligheid, de naleving daarvan en de inrichting van het toezicht daarop, eind 2016 bij de voorzitter van de Tweede Kamer aan te bieden.

11
Hoe beoordeelt u de problemen met de veiligheid van de persoonsgegevens in het licht van de afspraak uit het regeerakkoord dat uiterlijk in 2017 bedrijven en burgers zaken met de overheid digitaal kunnen afhandelen?

Antwoord:
Voor het zaken doen met de overheid is veiligheid en privacybescherming essentieel en randvoorwaardelijk. Zie ook het antwoord op vraag 10.

12
Kunt u aangeven of de problemen met de beveiliging van invloed zijn op Operatie BRP? Zo ja, op welke manier is dit van invloed?

Antwoord:
De geschetste problemen met de beveiliging van websites van gemeenten zijn niet van invloed op Operatie BRP. De BRP is, anders dan de gemeentelijke websites, immers niet publiekelijk benaderbaar.

13
Kunt u aangeven hoe het staat met de uitvoering van de motie Veldman en Oosenbrug (Kamerstuk 34 300-VII nr. 27) , waarin de regering wordt opgeroepen

om samen met de VNG tot een sluitende aanpak met betrekking tot bescherming van persoonsgegevens bij gemeenten te komen?

Antwoord:
Het ministerie van BZK is met de VNG en de directeuren sociaal domein aan het werk om te zorgen dat de aanpak van privacy zoals die afgelopen jaren is uitgewerkt ook structureel geborgd wordt bij gemeenten. Hiervoor worden onder andere best practices verzameld en werkbijeenkomsten belegd met directeuren sociaal domein. In samenwerking met VNG en GGZ Nederland wordt daarnaast gewerkt aan een programma om te zorgen dat ook de aansluiting bij instellingen gerealiseerd wordt. Dit zal worden afgesloten met een werkconferentie in juni.

1) http://www.rtlnieuws.nl/nieuws/binnenland/beveiliging-tientallen-gemeentesites-lek-persoonsgegevens-niet-veilig
2) Aanhangsel Handelingen, vergaderjaar 2015-2016, nr. 319 en nr. 1613