Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

Aanhangsel van de Handelingen

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

849

Vragen van de leden **Oosenbrug** en **Bouwmeester** (beiden PvdA) aan de Ministers van Veiligheid en Justitie en van Volksgezondheid, Welzijn en Sport over *datalekken bij ziekenhuizen* (ingezonden 25 november 2016).

Antwoord van Minister **Van der Steur** (Veiligheid en Justitie) mede namens de Minister van Volksgezondheid, Welzijn en Sport (ontvangen 23 december 2016). Zie ook Aanhangsel Handelingen, vergaderjaar 2016–2017, nr. 821.

Vraag 1
Kent u het bericht «Ziekenhuizen melden elke dag datalek»?[1]

Antwoord 1
Ja.

Vraag 2
Is het waar dat de genoemde datalekken vaak voortkomen uit het gebruik van onbeveiligde verbindingen en door menselijke fouten? Zo nee, waarom doen de datalekken zich dan wel voor?

Antwoord 2
De Autoriteit Persoonsgegevens (AP) ziet in het algemeen, en dus niet alleen bij ziekenhuizen, tot op heden vooral de volgende soorten datalekken:
– Een brief met persoonsgegevens komt niet aan bij de ontvanger of komt geopend terug;
– Een klant ziet in een klantportaal de gegevens van iemand anders;
– Een e-mail met persoonsgegevens komt bij de verkeerde ontvanger terecht;
– Iemand raakt een USB-stick kwijt waarop persoonsgegevens staan;
– Een laptop waarop persoonsgegevens staan wordt gestolen.
Er zijn verschillende potentiële oorzaken te benoemen voor het ontstaan van datalekken. Het gebruik van onbeveiligde verbindingen en menselijke fouten zijn er hier twee van.

[1] http://www.trouw.nl/tr/nl/39683/nbsp/article/detail/4421103/2016/11/24/Ziekenhuizen-melden-elke-dag-datalek.dhtml

ah-tk-20162017-849
ISSN 0921 - 7398
's-Gravenhage 2016

Vraag 3
Hoe komt het dat van het totaal aantal meldingen van datalekken tot nu toe er een kwart uit de zorgsector kwam? Is de zorgsector daarmee relatief oververtegenwoordigd? Zo ja, waarom is
daar sprake van?

Antwoord 3
Eerder dit jaar hebben de AP en de Inspectie voor de Gezondheidszorg (IGZ) per brief gewezen op de meldplicht datalekken[2] bij de brancheorganisaties Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU), Zelfstandige Klinieken Nederland (ZKN), GGZ Nederland en Revalidatie Nederland (RN) en hun leden. In mei heeft de AP daarnaast een presentatie gehouden voor de koepels van zorginstellingen om hen te informeren over de meldplicht en deze uitgebreid toe te lichten. In reactie daarop hebben de koepels ook acties in gang gezet om de awareness te vergroten.
De Zeker-campagne van de NVZ[3] dit najaar was gericht op het vergroten van het bewustzijn over informatiebeveiliging en specifiek datalekken. Daardoor is de alertheid bij ziekenhuizen en de bereidheid om te melden mogelijk extra groot en mogelijk verklaart dit mede ook het aantal meldingen, waarover AP rapporteert. Omdat de meldplicht nieuw is, is het niet mogelijk goed te duiden hoe de meldingen uit de zorg zich verhouden tot de meldingen in andere sectoren.

Vraag 4
Deelt u de mening dat zeker in het geval er persoonlijke gegevens van patiënten op straat kunnen komen te liggen datalekken zo snel mogelijk gedicht moeten worden? Zo ja, hoe kunt u waarborgen dat de gemelde lekken worden gedicht? Zo nee, waarom niet?

Antwoord 4
Indien er sprake is van een datalek, waarbij persoonsgegevens zijn gelekt, is het zaak dat het lek zo snel mogelijk gedicht wordt. Bij melding aan de AP wordt de melder ook gevraagd om verbeteracties te benoemen.

Vraag 5
Zijn er door een van de gemelde datalekken patiëntgegevens gelekt? Zo ja, zijn deze patiënten daarvan op de hoogte gesteld en wat is er gedaan om de gevolgen van het lek te beperken?

Antwoord 5
Het is mij niet bekend of er bij de gemelde datalekken sprake was van zodanige lekken van patiëntgegevens dat de betrokkenen hierover geïnformeerd dienden te worden. De AP heeft beleidsregels gepubliceerd met daarin informatie over de meldplicht datalekken en handvatten om te beoordelen wanneer betrokkenen geïnformeerd moeten worden over een lek.[4] Wanneer patiënten geïnformeerd behoorden te worden, dan maakt dit onderdeel uit van het opvolgingsplan van het datalek, waarop de AP kan toetsen.

Vraag 6
Heeft de Autoriteit Persoonsgegevens (AP) al boetes aan zorginstellingen gegeven vanwege het niet tijdig melden van een datalek? Zo ja, hoe vaak is dat gebeurd en wat was de aard van de betreffende datalekken? Zo nee, betekent dat dat de datalekken steeds op tijd zijn gemeld?

Antwoord 6
De AP heeft tot op heden geen boetes opgelegd vanwege het niet tijdig melden van een datalek. Dit betekent niet automatisch dat datalekken steeds op tijd zijn gemeld. De AP heeft overigens meerdere instrumenten wat betreft

---

[2] http://www.ggz-connect.nl/bericht/5619/igz-vraagt-aandacht-voor-informatiebeveiliging/document/downloaden/2750/brief%2BIGZ.pdf
[3] https://www.zorgzekeren.nl/zekercheck/
[4] https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

het opleggen van sancties en maakt hierin als onafhankelijke toezichthouder zelf een keuze.

Vraag 7
Deelt u de conclusie van Women in Cybersecurity (WICS) dat ziekenhuizen onzorgvuldig met beveiliging omgaan, onder andere door slordig om te gaan met inloggegevens of het gebruik van verouderde software en apparatuur? Zo ja, hoe en door wie worden de desbetreffende ziekenhuizen daar op aangesproken en tot verbetering gemaand? Zo nee, waarom deelt u die conclusie niet?

Antwoord 7
De afgelopen maanden heeft de Minister van VWS een onderzoek laten uitvoeren door PBLQ naar de beveiliging van patiëntgegevens en heeft het RIVM in opdracht van de IGZ ook onderzoek gedaan naar de omgang met privacy en informatiebeveiliging in de curatieve zorg en GGZ. Het PBLQ-rapport en het RIVM-onderzoek zijn op 15 december jl. met een beleidsreactie aan uw Kamer gestuurd.[5] Ook in deze onderzoeken komen de voorbeelden die Women in Cybersecurity noemt naar voren. In de beleidsreactie op het PBLQ-rapport heeft de Minister van VWS aangekondigd om op basis van de aanbevelingen met het veld een «Actieplan (informatie)beveiliging patiëntgegevens» op te zetten. Hierbij zal een belangrijke rol zijn weggelegd voor de koepels van ziekenhuizen, zelfstandige klinieken, GGZ-instellingen en de Patiëntenfederatie, als ook voor VWS en de toezichthouders. Op korte termijn neemt de Minister van VWS het initiatief om met de genoemde organisaties te starten met het Actieplan. Daarbij zullen mogelijk op een later moment ook koepels uit de andere sectoren betrokken worden. De Minister van VWS streeft ernaar dat het Actieplan in het voorjaar van 2017 gereed is, waarna de implementatie direct kan starten voor zover dat nog niet is gebeurd. Naar verwachting zal het Actieplan een meerjarig karakter zal hebben.

Vraag 8
Bent u net zoals de in het bericht genoemde ethisch hacker bekend met het feit dat op online zwarte markten patiëntgegevens worden aangeboden? Zo ja, wat is de aard en de omvang van dit probleem en wat zouden kwaadwillenden met die gegevens kunnen doen? Zo ja, wat doet u om aan deze praktijken een einde te maken? Zo nee, waarom niet en acht u onderzoek hiernaar wenselijk?

Antwoord 8
Ik heb geen inzicht in de aard en omvang van het verhandelen van patiëntgegevens op online zwarte markten. Wel acht ik het in alle gevallen zeer onwenselijk dat persoonsgegevens, en in het bijzonder medische persoonsgegevens, verhandeld worden en voor commerciële doeleinden gebruikt worden met consequenties voor patiënten zonder dat deze daar weet van hebben. In het Cyber Security Beeld Nederland[6] (CSBN) wordt het risico genoemd dat bijvoorbeeld vanuit zorginstellingen of zorg-gerelateerde websites inloggegevens bemachtigd worden, die vervolgens misbruikt worden voor financieel gewin. Dat maakt ook dat ik het van groot belang vindt dat zorginstellingen preventieve maatregelen nemen op het terrein van informatiebeveiliging en privacybewustzijn om informatiebeveiligingsincidenten en datalekken te voorkomen. De eerste verantwoordelijkheid daarvoor ligt bij de instellingen zelf.

[5] Kamerbrief Onderzoek PBLQ naar beveiliging van patiëntgegevens, 15 december 2016, kenmerk 1066048–159331-CZ
[6] Tweede Kamer, Vergaderjaar 2015–2016, Kamerstuk 26 643 nr. 420.