Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.rijksoverheid.nl

Ons kenmerk
1088340-160727-OBP

Bijlagen
1

Uw brief
11 januari 2017

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

Datum 15 februari 2017
Betreft Kamervragen

Geachte voorzitter,

Hierbij zend ik u mede namens de staatssecretaris van Veiligheid en Justitie de antwoorden op de vragen van het Kamerlid Oosenbrug (PvdA) over slechte beveiliging van ziekenhuiswebsites (2017Z00213).

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

mw. drs. E.I. Schippers

Antwoorden op kamervragen van het Kamerlid Oosenbrug (PvdA) over slechte beveiliging van ziekenhuiswebsites.
(2017Z00213)

1
Bent u bekend met de berichten "Ziekenhuizen beveiligen hun sites niet goed" 1) en "Deel websites ziekenhuizen slecht beveiligd"? 2)

Ja

2
Deelt u de mening dat het zeer zorgelijk is dat 35% van de ziekenhuizen uit het onderzoek van Women in Cybersecurity geen beveiligde internetverbinding hebben, nog eens een kwart van de ziekenhuizen een verouderdere internetverbinding heeft en patiëntgegevens hierdoor gemakkelijk in verkeerde handen kunnen vallen?

Antwoord op vragen 2, 4, 5
Ik herken het beeld dat Women in Cybersecurity schetst, namelijk dat er verbetering nodig is op het terrein van informatiebeveiliging in de zorg. Het bewustzijn in ziekenhuizen over de omgang en verwerking van privacygevoelige gegevens is de afgelopen jaren toegenomen, zo concludeert het onderzoek van PBLQ[1], dat ik in december aan uw Kamer stuurde. Tegelijkertijd lijkt het bewustzijn nog niet bij iedereen in dezelfde mate aanwezig en dat is onwenselijk. De vertrouwelijkheid van medische informatie en de vertrouwelijke omgang met persoonsgegevens in de gezondheidszorg is essentieel en is een kernwaarde voor zowel patiënten als zorgaanbieders. De Wet bescherming persoonsgegevens (Wbp) verplicht het nemen van passende technische en organisatorische maatregelen waarbij het beveiligingsniveau passend moet zijn bij de aard van de te beschermen gegevens. In de gezondheidszorg zijn de NEN 7510, NEN 7512 en NEN 7513 de normen om dit beveiligingsniveau te bereiken.
De Autoriteit Persoonsgegevens (AP) ziet hierop toe en kan zo nodig handhavend optreden. Ook de Inspectie voor de Gezondheidszorg (IGZ) ziet toe op de naleving van relevante wet- en regelgeving op het gebied van informatiebeveiliging in de zorg, voor zover die raakt aan kwaliteit en veiligheid van zorg.

Informatiebeveiliging en privacybescherming zijn in de eerste plaats de verantwoordelijkheid van de zorgaanbieder zelf. Op grond van de Wbp is degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt, verantwoordelijk voor de verwerking. Dat betekent dat ziekenhuizen zelf zorg dienen te dragen voor passende technische en organisatorische maatregelen op hun websites. Het versleutelen van het informatieverkeer via een beveiligde (https-) verbinding is een voorbeeld van een dergelijke maatregel. De verplichte NEN-normen voor informatiebeveiliging besteden ook aandacht aan dit type passende maatregelen en het uitvoeren van een risicoanalyse. Voor iedere website en dienst zal de verantwoordelijke organisatie een risicoafweging moeten maken om te bepalen of een beveiligde verbinding nodig is. De AP ziet hierop toe.

[1] Kamerbrief Onderzoek PBLQ naar beveiliging van patiëntgegevens, 15 december 2016, kenmerk 1066048-159331-CZ

Ik heb naar aanleiding van onder meer het PBLQ-onderzoek toegezegd dat ik ernaar streef dit voorjaar samen met de sector met een 'Actieplan (informatie)beveiliging patiëntgegevens' te komen om de privacybescherming en informatiebeveiliging in het ziekenhuis en GGZ-domein te verbeteren. Ik zal het uitwisselen van patiëntgegevens via onbeveiligde verbindingen en websites en de awareness daarover, daarin als aandachtspunt meenemen.

3
Zijn bij u gevallen van datalekken bij ziekenhuizen bekend met als oorzaak het versturen van gegevens via een onbeveiligde internetverbinding? Zo ja, om hoeveel datalekken gaat het?

Meldingen worden bij de AP gedaan. Het is mij niet bekend of hierover meldingen zijn gedaan.

4
Deelt u de mening dat de reacties van ziekenhuizen op het onderzoek van Women in Cybersecurity (zoals "we hadden nog geen versleuteling toen onze site ontstond" en "bij de nieuwe site die binnenkort 'live' gaat, is dit probleem opgelost") in schril contrast staan tot de verplichting om te zorgen voor goede beveiliging van websites als bezoekers gevraagd wordt om bijzondere persoonlijke gegevens, zoals iemands gezondheid?

Zie mijn antwoord op vraag 2.

5
Deelt u de mening dat ziekenhuizen zich onvoldoende bewust lijken van de risico's die het versturen van patiëntgegevens via een onbeveiligde internetverbinding met zich meebrengen?

Zie mijn antwoord op vraag 2.

6
Zijn alle ziekenhuizen actief geïnformeerd over deze risico's? Zo nee, bent u bereid de ziekenhuizen op zeer korte termijn te informeren over deze risico's? Zijn alle ziekenhuizen op de hoogte van de richtlijnen voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties, zoals de ICT-Beveiligingsrichtlijnen voor Webapplicaties van het Nationaal Cyber Security Centrum (NCSC)? 3) Zijn ziekenhuizen verplicht zich aan deze richtlijnen te houden? Zo nee, waarom niet en bent u bereid ziekenhuizen nogmaals op deze richtlijn te wijzen?

Zoals verwoord in mijn vorige antwoord zijn informatiebeveiliging en privacybescherming de verantwoordelijkheid van de zorgaanbieder zelf. Het wettelijk kader, de Wbp, stelt dat ziekenhuizen passende maatregelen moeten nemen daar waar sprake is van verwerkingen van persoonsgegevens. Voor de zorg gelden de NEN 7510, 7512, 7513 normen, die ook als passende normen voor informatiebeveiliging, waaronder netwerkbeveiliging, worden gezien. Zoals beschreven in het antwoord op vraag 2 zien de AP en de IGZ hierop toe.

Daarnaast kunnen ziekenhuizen kennis nemen van de door het NCSC publiekelijk gepubliceerde adviezen en kennisdocumenten, zoals de ICT-beveiligingsrichtlijnen

voor webapplicaties. Of de open standaarden voor beveiligde berichtuitwisseling op het web, die Forum Standaardisatie heeft opgenomen in de lijst met ´pas toe of leg uit´-standaarden. Er zijn afspraken gemaakt voor implementatie hiervan in het DigiD-domein en voor de rijksoverheid. Deze richtlijnen zijn niet verplicht voor de zorg, maar de zorg kan deze natuurlijk wel implementeren. Het aantoonbaar voldoen aan generieke richtlijnen kan een onderbouwing geven voor de vraag of al dan niet passende maatregelen zijn genomen.

Bij het opstellen van het 'Actieplan (informatie)beveiliging patiëntgegevens' om de privacybescherming en informatiebeveiliging in het ziekenhuis en GGZ-domein te verbeteren, zal ik het uitwisselen van gegevens via onbeveiligde verbindingen en websites en de awareness daarover als aandachtspunt meenemen.

7
Bent u voornemens aanvullende verplichte regels/richtlijnen op te stellen die ziekenhuizen moeten volgen, om zo dergelijke datalekken te voorkomen? Zo ja, door wie zal controle op deze regels/richtlijnen uitgevoerd worden? Hoort een onafhankelijke responsible disclosure daar ook bij?

Uit het onderzoek dat de ik onlangs heb laten uitvoeren komt geen indicatie naar voren dat verdere aanvulling van wet- en regelgeving voor informatiebeveiliging en privacybescherming in zorginstellingen noodzakelijk is. Uit de interviews en enquêtes bij het onderzoek blijkt wel dat er behoefte is aan het begrijpelijker maken van de huidige en komende wet- en regelgeving en het vertalen ervan naar concrete handvatten voor de praktijk.

Het inrichten van een responsible disclosure beleid is een eigen afweging van een zorginstelling. Het kabinet en in het bijzonder het ministerie van Veiligheid en Justitie stimuleren in den brede dat organisaties een responsible disclosure-beleid inrichten en uitvoeren. Wanneer een organisatie geen responsible disclosure beleid heeft ingericht of geen gehoor geeft aan de melding kunnen meldingen gedaan worden bij het NCSC[2]. Het NCSC zal met de betrokken partijen contact opnemen en indien nodig de rol van intermediair op zich nemen. Ook bij de AP kunnen meldingen gedaan worden wanneer partijen van mening zijn dat er sprake is van een inbreuk op de Wbp. In de nabije toekomst zullen meldingen van kwetsbaarheden in het kader van responsible disclosure ook gemeld kunnen worden bij het Computer Emergency en Response Team voor de zorg 'Z-cert', dat nu opgericht wordt en waaraan ik een financiële bijdrage lever om tegemoet te komen in de aanloopverliezen bij de start van de organisatie.

8
Hoe beoordeelt u de uitspraak van de Nederlandse Vereniging van Ziekenhuizen dat er aan een oplossing wordt gewerkt en dat het binnen vier jaar mogelijk is om veilig online gegevens in te zien en afspraken te maken? Deelt u de mening dat, zeker wanneer persoonlijke gegevens van patiënten op straat kunnen komen te liggen, datalekken zo snel mogelijk gedicht moeten worden en dat vier jaar een onredelijk lange termijn is om dit probleem op te lossen? Zo ja, hoe gaat u waarborgen dat de beveiliging van ziekenhuiswebsites zo snel mogelijk op orde is? Zo nee, waarom niet?

[2] Melden kan via het e-mailadres: cert@ncsc.nl

Het nu al voldoen aan het wettelijk kader rondom privacybescherming en informatiebeveiliging staat los van de ambitie van ziekenhuizen, zoals afgesproken in het Informatieberaad, om over vier jaar meer zorggegevens voor patiënten online te kunnen ontsluiten of het voor de patiënt mogelijk te maken om bij meer zorgpartijen afspraken online te kunnen maken en wijzigen. Zowel nu als dan moeten zorgpartijen, op basis van de Wbp, er voor zorgen dat de privacybescherming en informatiebeveiliging op orde zijn. Zoals beschreven in het antwoord op vraag 2 zien de AP en de IGZ hierop toe.

9
Op welke termijn verwacht u dat alle ziekenhuizen de beveiliging van hun internetverbinding en de verzending van patiëntgegevens op orde hebben? Heeft dit tot gevolg dat patiëntgegevens tot die tijd onveilig worden verzonden? Zo ja, wat gaat u er in de tussentijd aan doen om datalekken van patiëntgegevens te voorkomen?

Ik verwacht dat ziekenhuizen met de uitvoering van het Actieplan (informatie)beveiliging patiëntgegevens de privacybescherming en informatiebeveiliging (waaronder beveiliging van de websites) verder zullen verbeteren. Uitzicht op de termijn waarbinnen deze maatregelen zijn geïmplementeerd is afhankelijk van de inzet van de ziekenhuizen zelf. Ik verwacht dat elk ziekenhuis daarin de eigen verantwoordelijkheid neemt.

Sinds 1 januari 2016 geldt de meldplicht datalekken, die organisaties verplicht om datalekken te melden. Het is aan de AP om vervolgens toe te zien dat in reactie op een datalek passende maatregelen worden genomen.

10
Deelt u de mening dat de 110 miljoen euro die beschikbaar is gesteld om de beveiliging van ziekenhuiswebsites te verbeteren een ICT-project betreft, getoetst dient te worden door het Bureau ICT Toetsing en op het Rijks ICT-dashboard geplaatst moet worden? Zo nee, waarom niet?

Ik heb voor de komende drie jaar € 35 mln. per jaar beschikbaar gesteld, zodat patiënten binnen drie jaar op een veilige en gestandaardiseerde manier over hun medische gegevens kunnen beschikken en deze kunnen inzetten voor zelfzorg of om met andere medische professionals te delen. Dit is vastgelegd in de subsidieregeling[3] 'Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional (VIPP)', waar ziekenhuizen resultaatsverplichtingen moeten halen om de subsidie te verkrijgen. Het VIPP-programma valt in die hoedanigheid buiten scope van het Bureau ICT-Toetsing en hoeft ook niet op het Rijks ICT-dashboard geplaatst te worden. Bij de resultaatsverplichtingen is opgenomen dat er bij het uitwisselen van persoonsgegevens gebruik gemaakt moet worden van veilige authenticatiemiddelen, van een adequaat hoog betrouwbaarheidsniveau. De digitale gegevensuitwisseling die gerealiseerd wordt moet vanzelfsprekend aan de wettelijke kaders rondom privacybescherming en gegevensuitwisseling voldoen.
11
Zijn er naar aanleiding van het eerdere onderzoek van het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) "ICT in de zorg" 4) al acties ondernomen om de

[3] De regeling is te vinden op: https://www.rijksoverheid.nl/onderwerpen/subsidies-vws/inhoud/beleidskader-subsidiering-versnellingsprogramma-informatie-uitwisseling-patient-en-professional.

beveiliging van patiëntgegevens bij ziekenhuizen in het algemeen te verbeteren? Zo ja, wanneer en welke acties zijn dit? Zo nee, waarom niet?

Ik heb u naar aanleiding van het rapport van PBLQ over beveiliging van patiëntgegevens en het rapport van RIVM (in opdracht van de IGZ) 'ICT in de zorg' toegezegd dit voorjaar met een 'Actieplan (informatie)beveiliging patiëntgegevens' te komen om de privacybescherming en informatiebeveiliging in het ziekenhuis en GGZ-domein te verbeteren.

1) http://nos.nl/artikel/2151664-ziekenhuizen-beveiligen-hun-sites-niet-goed.html
2) http://www.telegraaf.nl/digitaal/27375556/__Sites_zieken-_huis_slecht_beveiligd__.html
3) https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
4) http://www.rivm.nl/dsresource?objectid=76dc3891-1d87-4b36-bfb7-30545e4f163f&type=org&disposition=inline