

2017Z00213

Vragen van het lid **Oosenbrug** (PvdA) aan de Ministers van Veiligheid en Justitie en van Volksgezondheid, Welzijn en Sport over *slechte beveiliging van ziekenhuiswebsites* (ingezonden 11 januari 2017).

Vraag 1

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

Vraag 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?

Vraag 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?

Vraag 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?

Vraag 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?

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

Vraag 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?

Vraag 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?

Vraag 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?

Vraag 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?

Vraag 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?

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

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>