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

2690

Vragen van de leden **Pia Dijkstra** en **Verhoeven** (beiden D66) aan de Minister van Volksgezondheid, Welzijn en Sport over *het bericht dat meerderheid van de zorgsites onbeveiligd is* (ingezonden 21 augustus 2017).

Antwoord van Minister **Schippers** (Volksgezondheid, Welzijn en Sport) (ontvangen 12 september 2017).

Vraag 1
Bent u bekend met het bericht «Meerderheid zorgsites onbeveiligd, privacy autoriteit dreigt met boetes»?[1]

Antwoord 1
Ja.

Vraag 2, 5, 6
Wat is uw eerste reactie op het feit dat twee op de drie websites van zorginstellingen geen gebruik maken van een veilige verbinding?
Deelt u de mening dat het onwenselijk is als informatie onderschept wordt via onbeveiligde websites? Zo ja, welke mogelijkheden ziet u om dit aan te pakken? Zo nee, waarom niet?
Deelt u de mening dat het van groot belang is dat de veiligheid van gegevens wordt beschermd en dat de zorgsector voldoende geëquipeerd moet zijn om zich te kunnen wapenen tegen kwaadwillende meelezers?

Antwoord 2, 5, 6
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. Ik vind het van belang dat zorgaanbieders hun verantwoordelijkheid moeten en kunnen nemen ten aanzien van informatiebeveiliging.
Zoals aangegeven in mijn eerdere reactie op vraag 2, 4 en 5 van Kamerlid Oosenburg (PvdA) over de beveiliging van ziekenhuiswebsites (Aanhangsel Handelingen, vergaderjaar 2016–2017, nr. 1216) zijn informatiebeveiliging en privacybescherming in de eerste plaats verantwoordelijkheden van de zorgaanbieder zelf. De Wet bescherming persoonsgegevens (Wbp) verplicht

[1] https://nos.nl/artikel/2188492-meerderheid-zorgsites-onbeveiligd-privacy-autoriteit-dreigt-met-boetes.html

ah-tk-20162017-2690
ISSN 0921 - 7398
's-Gravenhage 2017

de verantwoordelijke 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. Het versleutelen van het informatieverkeer via een beveiligde (https-) verbinding is een voorbeeld van een maatregel, die uit die norm kan voortkomen. Voor iedere website en dienst zal de verantwoordelijke organisatie moeten bepalen of een beveiligde verbinding nodig is.
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.
Om zorgaanbieders nog beter toe te rusten om hun verantwoordelijkheden ten aan zien van informatiebeveiliging te nemen heb ik aanvullend hierop met branchepartijen het «Actieplan (informatie-) beveiliging patiëntgegevens» opgesteld. Hierover heb ik u geïnformeerd in mijn brief van 20 juni jl. (Kamerstuk 31 765, nr. 275). Het «Actieplan (informatie-) beveiliging patiëntgegevens» benoemt in de praktijk bewezen «good practices». Deze «good practices» hebben betrekking op de cultuur, structuur en compliance aan bestaande regelgeving van zorgaanbieders. Ik ben voornemens het «Actieplan (informatie-) beveiliging patiëntgegevens» uit te breiden naar andere sectoren (zoals bijvoorbeeld apothekers en huisartsen) ter verhoging van informatieveiligheid en de privacybescherming. De NVZ-campagne ZEKER is mijns inziens een mooi voorbeeld van het oppakken van de eigen verantwoordelijkheid door de zorgsector om de bewustwording op informatiebeveiliging en privacybescherming te verhogen.
Ik wil tot slot benadrukken dat patiënten er op moeten kunnen vertrouwen dat de bescherming van medische gegevens goed is geregeld. Dit is noodzakelijk voor de vertrouwensrelatie met de zorgverlener. Beveiliging van patiëntgegevens is een doorlopend punt van aandacht en zal altijd een onderwerp blijven waar alle partijen zich voor moeten hardmaken. Met het «Actieplan (informatie)beveiliging patiëntgegevens» heeft de sector een belangrijke stap gezet om de bescherming van medische gegevens verder te verbeteren. De Autoriteit Persoonsgegevens kan ook handhavend optreden als een aanbieder de beveiliging desondanks niet op orde heeft.

Vraag 3, 4
Heeft u een verklaring waarom minder dan een kwart van de websites van de geestelijke gezondheidszorg, verloskundigen, thuiszorg en fysiotherapie een veilige verbinding afdwingt? Zo ja, wat is deze verklaring? Zo nee, kunt u dit laten uitzoeken?
Hoe komt het dat ziekenhuizen en huisartsen het relatief gezien goed doen? Is er een «best practice» te destilleren die door andere professionals overgenomen kan worden?

Antwoord 3, 4
Ik heb niet een specifieke verklaring waarom de ene zorgsector een hoger percentage beveiligde verbindingen heeft dan de andere zorgsector. Een mogelijke verklaring kan gevonden worden in een conclusie van PBLQ-rapport «Onderzoek naar de beveiliging van patiëntgegevens» (Kamerstuk 31 765, nr. 259). Daarin staat dat er groeiende bewustwording is bij zorgaanbieders als het gaat om informatiebeveiliging en privacybescherming. Dat leidt tot het nemen van maatregelen en beschikbaar stellen van capaciteit door zorgaanbieders op dat terrein. Het bewustwordingsproces is dus gaande, maar nog niet voltooid. In het nieuwsbericht van de NOS van 17 augustus jl. wordt bewustwording ook als verklaring genoemd. Ik wil door middel van de verbreding van het «Actieplan (informatie-) beveiliging patiëntgegevens» bijdragen aan een vergroting van de bewustwording en daarmee betere beveiliging, maar dat is niet een vrijblijvende keuze. Iedere zorgaanbieder zal dit op orde moeten hebben.