

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
956677-149418-OBP

Bijlagen
1

Uw brief
30 maart 2016

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

Datum 11 mei 2016
Betreft Kamervragen

Geachte voorzitter,

Hierbij zend ik u mede namens de Staatssecretaris van Veiligheid en Justitie, de antwoorden op de vragen van de Kamerleden Dijkstra (D66) en Verhoeven (D66) over het bericht 'Noodtoestand in Amerikaans ziekenhuis wegens ransomware' (een chantagemethode op internet) (2016Z06407).

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

mw. drs. E.I. Schippers

Antwoorden op kamervragen van de Kamerleden Dijkstra (D66) en Verhoeven (D66) over het bericht 'Noodtoestand in Amerikaans ziekenhuis wegens ransomware' (een chantagemethode op internet) .
(2016Z06407)

1

Kent u het bericht 'Noodtoestand in Amerikaans ziekenhuis wegens ransomware'?

1)

Ja

2

Is een dergelijke situatie reeds in Nederland voorgekomen? Kunt u dit uitsluiten?
Zo nee, waarom niet?

3

Deelt u de mening dat deze situatie ook in Nederlandse ziekenhuizen mogelijk is?
Zo nee, waarom niet?

Antwoord op vraag 2 en 3

Een dergelijke situatie in de vorm van een noodtoestand binnen de Nederlandse gezondheidszorg is mij niet bekend. Het Nationaal Cyber Security Centrum (NCSC) is bekend met signalen dat in Nederland, ziekenhuizen, evenals andere sectoren, geconfronteerd worden met aanvallen op kantoorautomatisering door ransomware. Bij het NCSC zijn echter geen signalen bekend dat deze aanvallen hebben geresulteerd in grootschalige uitval of verstoring.

Melding van dit type incidenten bij de Autoriteit Persoonsgegevens (AP) is wettelijk verplicht indien er persoonsgegevens gecompromitteerd zijn. Per 1 januari 2016 geldt immers de wettelijke meldplicht datalekken. De Autoriteit Persoonsgegevens heeft beleidsregels over deze meldplicht opgesteld¹. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen. Of bij ransomware een datalek moet worden gemeld, hangt af van de ernst van het datalek. In het geval van ransomware moet de verantwoordelijke organisatie deze afweging niet beperken tot de gegevens op het gecompromitteerde apparaat. Hij moet het risico meewegen ten aanzien van alle soorten persoonsgegevens waarvan aangenomen kan worden dat die vanaf het randapparaat via een netwerkverbinding benaderd kunnen worden.

De IGZ heeft op 17 maart 2016 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 per brief gewezen op de meldplicht datalekken². Daarbij heeft de IGZ de koepels en hun leden ook opgeroepen een dergelijk incident vrijwillig te melden aan de IGZ.

¹ <https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken>

² <http://www.ggz-connect.nl/bericht/5619/igz-vraagt-aandacht-voor-informatiebeveiliging/document/downloaden/2750/brief%2BIGZ.pdf>

4

Kunt u aangeven wat voor voorzorgsmaatregelen er worden genomen om dergelijke situaties te voorkomen?

5

Zijn er bepaalde richtlijnen, bijvoorbeeld vanuit het Nationaal Cyber Security Centrum, met betrekking tot de inrichting van ICT-systemen van Nederlandse ziekenhuizen om data van patiënten te beschermen? Zo ja, kunt u aangeven welke richtlijnen dit zijn?

Antwoord op vraag 4 en 5

Informatiebeveiliging is een eigen verantwoordelijkheid van ziekenhuis. Vanuit de sectorale verantwoordelijkheid voor de zorg bestaat thans reeds een uitvoerig wettelijk kader ter bescherming van gegevens.

De eisen voor informatiebeveiliging voor ziekenhuizen zijn te vinden in de NEN 7510³, NEN 7512 en NEN 7513 voor respectievelijk veilige omgang met informatie, gegevensuitwisseling en het vastleggen van acties op elektronische patiëntdossiers. IGZ gebruikt deze normen om te toetsen of ziekenhuizen qua informatiebeveiliging voldoende maatregelen hebben genomen om de continuïteit en kwaliteit van zorg te kunnen waarborgen. In een Algemene Maatregel van Bestuur (AMvB) behorend bij het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens, dat ter behandeling voorligt in de Eerste Kamer, worden op grond van artikel 26 Wet bescherming persoonsgegevens (Wbp) specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling en zorginformatiesystemen wettelijk verankerd door het voldoen aan de bovengenoemde NEN-normen verplicht te stellen.

In de komende periode zal daarnaast de Netwerk- en InformatieBeveiligingsrichtlijn (NIB-richtlijn), waarover eind 2015 binnen de EU een politiek akkoord bereikt is, worden geïmplementeerd. Hierin is de zorg ook genoemd. Deze NIB-richtlijn bestaat onder andere uit een zorg- en meldplicht. Uw Kamer wordt door het ministerie van Veiligheid en Justitie reeds periodiek geïnformeerd over de voortgang van de NIB-richtlijn.

Daarnaast publiceert ook NCSC richtlijnen met betrekking tot de inrichting en beveiliging van ICT-systemen. Deze kunnen tevens worden gebruikt als handvat bij de implementatie van beveiligingsvereisten. Ook publiceert het NCSC algemene whitepapers, factsheets en best practices en dagelijks adviezen over nieuwe kwetsbaarheden in hard- en software die voor een ieder, ook buiten de doelgroep van Rijksoverheid en de vitale infrastructuur, te vinden zijn via de website www.ncsc.nl.

³ De norm NEN 7510 is een door het Nederlands Normalisatie-instituut ontwikkelde norm voor Informatiebeveiliging. De norm is gebaseerd op de Code voor Informatiebeveiliging. Dit de Nederlandse versie van de British Standards 7799, die later als internationale standaard voor informatiebeveiliging in organisaties is gepubliceerd. De Code voor Informatiebeveiliging bestaat uit twee delen: een norm (NEN-ISO/IEC 27001:2013+C11/2014 nl) en een 'code of practice' (NEN-ISO/IEC 27002:2013+C2:2015 nl).

In aanvulling hierop bestaat een door het NCSC in samenwerking met de sector opgezet Information Sharing and Analysis Centre (ISAC) voor de zorg. Een ISAC is een publiek-private sectoraal samenwerkingsverband, waarbinnen op tactisch niveau deelnemers van verschillende ziekenhuizen onderling (incident) informatie en ervaringen uitwisselen over cybersecurity en kwetsbaarheden in de sector ('situational awareness'). Door het delen van (incident) informatie en het opbouwen van een netwerk kunnen ziekenhuizen hun eigen informatiebeveiliging verbeteren.

Tot slot werken de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU) en GGZ Nederland, zoals ik in eerdere Kamervragen al aangaf, samen om in samenspraak met het NCSC, als verantwoordelijk Computer Emergency Response Team (CERT) voor de Rijksoverheid en de vitale infrastructuur specifiek, een CERT voor de zorg (Z-CERT) in te richten.

6

Krijgen artsen en medewerkers in ziekenhuizen 'cyberhygiëne'-training om dergelijke infecties van ransomware (of malware) te voorkomen? Zo nee, waarom niet? Deelt u de mening dat het wenselijk is als hier wel voor gekozen wordt om mogelijke risico's te verminderen?

Borgen van continuïteit van dossiers is een verplichting van zorgaanbieders. Als zodanig is cyber-awareness daarvan een onderdeel. Het is de verantwoordelijkheid van de instellingen om zijn personeel op te leiden in het (veilig) omgaan met software. Het geven van trainingen kan daar, naast bijvoorbeeld het treffen van technische maatregelen, deel van uitmaken. Door ziekenhuizen is de afgelopen jaren dan ook actief geparticipeerd binnen de landelijke awareness-campagne Alert Online.

7

Bent u bereid de ICT-systemen van Nederlandse ziekenhuizen te laten testen op het gebied van cybersecurity? Zo nee, waarom niet?

Zoals eerdere reeds aangegeven is het de eigen verantwoordelijkheid van ziekenhuizen om de informatiebeveiliging op orde te hebben. Ziekenhuizen kunnen hun informatiebeveiligingsbeleid en de beveiligingsmaatregelen periodiek laten auditen. De NEN 7510 heeft aan deze periodieke toetsing een specifiek hoofdstuk gewijd. Sinds februari 2016 kunnen zorginstellingen zich ook laten accrediteren in het kader van NEN 7510 en zich laten certificeren door een onafhankelijke accrediterende partij. De IGZ neemt, wanneer zij kijkt naar de informatiebeveiliging, de uitkomsten en inzet van dergelijke toetsing mee in haar oordeel over hoe de instelling met informatiebeveiliging omgaat.

1)

<https://www.security.nl/posting/465461/Noodtoestand+in+Amerikaans+ziekenhui+s+wegens+ransomware>