Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

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

2680

Vragen van het lid **Pia Dijkstra** (D66) aan de minister van Volksgezondheid, Welzijn en Sport over *het bericht dat honderden huisartsen gedwongen onveilige software gebruiken* (ingezonden 5 juni 2013).

Antwoord van minister **Schippers** (Volksgezondheid, Welzijn en Sport) (ontvangen 25 juni 2013).

Vraag 1
Wat is uw reactie op het bericht «Huisartsen gedwongen tot gebruik uiterst onveilige Java-versie»?[1]

Antwoord 1
Achtergrond van het artikel op Tweakers.net is de volgende. ICT-leverancier Promedico heeft een deel van haar klanten geadviseerd om nog even te wachten met de nieuwste update van Java. De reden hiervoor was dat deze nieuwste versie van Java een probleem opleverde bij het gebruik van de UZI-pas. Het advies betrof dan ook alleen Promedico-klanten die een UZI-pas gebruiken. Volgens Promedico zijn dat 134 praktijken. Promedico heeft aangegeven dat sinds maandagavond 3 juni een update voor de klanten beschikbaar is. De Promedico-klanten die gebruik maken van een UZI-pas hebben hun systeem inmiddels kunnen aanpassen.

Vraag 2
Deelt u de mening dat het dwingen tot uitstel van een securitypatch een veiligheidsrisico met zich meebrengt, omdat reeds bekende veiligheidsproblemen in de software niet verholpen worden?

Antwoord 2
Dat zou inderdaad onwenselijk zijn. Het is de verantwoordelijkheid van de zorgaanbieders en de leveranciers om informatiesystemen adequaat te beveiligen, zodat veilige en betrouwbare gegevensuitwisseling mogelijk is. Softwareleveranciers hanteren over het algemeen release-planningen zodat klanten niet te pas en te onpas met aanpassingen worden geconfronteerd. Voor wat betreft de situatie waarover het artikel handelt, geldt het volgende. Promedico heeft na de release van april het probleem geconstateerd.

[1] «Huisartsen gedwongen tot gebruik uiterst onveilige Java-versie», http://tweakers.net/nieuws/89440/huisartsen-gedwongen-tot-gebruik-uiterst-onveilige-java-versie.html, 3 juni 2013

ah-tk-20122013-2680
ISSN 0921 - 7398
's-Gravenhage 2013

Besloten is om de oplossing te prioriteren voor de eerstvolgende release. Deze release stond in de release-planning voor 6 juni. Promedico heeft dit onderdeel maandagavond 3 juni, in een aparte release aan haar klanten beschikbaar gesteld.

Vraag 3
Klopt het dat via deze veiligheidsproblemen computers in theorie overgenomen kunnen worden, en dat daardoor patiëntendossiers mogelijk door onbevoegden kunnen worden ingezien?

Antwoord 3
Het is Promedico niet bekend dat met de betreffende Java versie computers kunnen worden overgenomen. Echter in deze Java versie zaten wel de nodige security issues. De Java update heeft betrekking op de PC van de arts die met het centrale systeem Promedico-ASP werkt. Promedico heeft aangegeven dat bij Promedico-ASP de patiëntgegevens niet op het systeem van de arts staan, maar dat alle patiëntgegevens staan opgeslagen in beveiligde datacenters. Inloggen in de dossiers is beveiligd met middelen als Digi-pas en UZI pas. In de datacenters wordt gebruik gemaakt van firewalls om hacken te voorkomen. Alle gegevens worden versleuteld verzonden van datacenter naar de arts.

Vraag 4
Deelt u de mening dat bij het verwerken van medische gegevens een dergelijke situatie niet voor zou mogen komen, en dat hiermee niet wordt voldaan aan wettelijke eisen voor gegevensbescherming?

Antwoord 4
Dit is inderdaad geen wenselijke situatie. Het is aan het College Bescherming Persoonsgegevens (CBP) te beoordelen of in een dergelijke situatie wordt voldaan aan de wettelijke eisen voor gegevensbescherming.

Vraag 5
Kunt u toelichten waar de verantwoordelijkheid voor adequate gegevensbescherming in dergelijke situaties ligt? Ligt die verantwoordelijkheid bij de huisarts, of juist bij de leverancier?

Antwoord 5
De zorgaanbieder is op grond van de Wet bescherming persoonsgegevens verantwoordelijk voor een veilige verwerking van de gegevens van zijn patiënten. De noodzakelijke beveiligingseisen zouden in de afspraken (de zogenaamde bewerkersovereenkomst) tussen zorgaanbieders en ICT-leveranciers duidelijk vastgelegd moeten zijn.

Vraag 6
Hoe gaat u dergelijke situaties in de toekomst voorkomen?

Antwoord 6
ICT leveranciers moeten met de zorgaanbieders het beheer en onderhoud van hun systemen zo vormgeven, dat de kans op dergelijke situaties minimaal is. Het CBP ziet toe op het naleven van deze verantwoordelijkheden op basis van de Wet Bescherming Persoonsgegevens.
Specifiek voor de gezondheidszorg is de combinatie van bijzondere functionele eisen aan de informatievoorziening («een overal bereikbaar patiëntdossier») met bijzondere risico's (soms levensbedreigend, zeer privacygevoelig). Hiervoor is voor de informatiebeveiliging in de zorg een speciale norm opgesteld: NEN 7510. De NEN 7510 geeft aanwijzingen voor het organisatorisch en technisch inrichten van de informatiebeveiliging. NEN 7510 wordt verder ingevuld door NEN 7512 en NEN 7513, die respectievelijk handelen over de veiligheid van gegevensuitwisseling tussen partijen en logging. In de toelichting bij het wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens is aangegeven dat naar deze NEN-normen bij algemene maatregel van bestuur dwingend zal worden verwezen (Tweede Kamer, vergaderjaar 2012–2013, 33 509, nr. 3).