

Geheimzinnigheid ministerie is volgens kenners een veeg teken

Beveiliging EPD blijft schimmig

Heleen Croonen

Het ministerie van VWS geeft weinig prijs over de beveiliging van het landelijk elektronisch patiëntendossier. Dat is niet geruststellend, zeggen kenners. Want een beveiligingssysteem is pas echt goed als geheimzinnigheid erover onnodig is.



beeld: Corbis

‘Als er een mogelijkheid is om te hacken, wordt die gevonden’

Helemaal waterdicht kun je het niet maken, maar de beveiliging van het landelijk elektronisch patiëntendossier (EPD) is zo goed als maar kan, zegt het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Het ministerie heeft zoveel vertrouwen in de beveiliging omdat die jaarlijks door onafhankelijke derden wordt getest door middel van audits en ‘indringerstesten’, testen die moeten vaststellen hoe makkelijk het voor hackers is om in te breken. Bovendien is er een zogenaamde ‘intelligente logging’, aldus het ministerie, waarmee de toezichthouders kunnen controleren of er ongeoorloofde inzage is in medische dossiers. Dat maakt nieuwsgierig. Wat voor indringerstesten zijn dat en hoe werkt die intelligente logging? Het ministerie geeft uit zichzelf echter weinig prijs over de technische kanten van de beveiliging.

Kerckhoffs principe

Dat wekt verwondering. In de ICT-beveiliging is het gebruikelijk om informatie over beveiliging te delen. Dat vloeit voort uit het principe van Kerckhoff. Volgens dat principe is een systeem veilig als alles erover bekend is – behalve de sleutel – en het toch niet kan worden gekraakt. Als de maker probeert details over

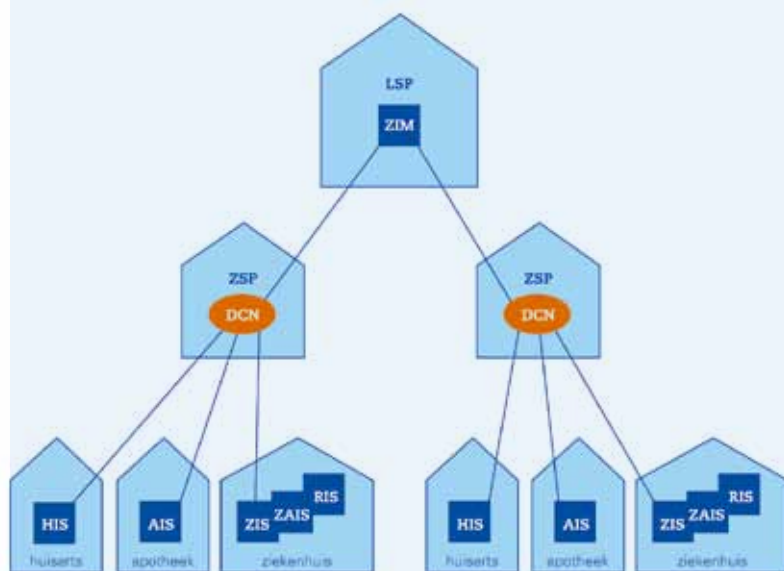
het beveiligingssysteem geheim te houden, is dat systeem onbetrouwbaar, aldus het principe. ‘Als er een mogelijkheid is om te hacken, kun je ervan uitgaan dat die wordt gevonden’, zegt Guido van ’t Noordende, onderzoeker gespecialiseerd in beveiliging en privacy van de Universiteit van Amsterdam, en adviseur van de Eerste Kamer over het EPD. Mysterieus doen over je beveiligingssysteem heeft dus geen enkele zin. Het is dan ook de vraag waarom het ministerie daar toch voor kiest. Reden genoeg voor Medisch Contact om samen met Brenno de Winter, journalist en expert op het gebied van de Wet openbaarheid van bestuur (Wob), een Wob-verzoek in te dienen bij het ministerie, bedoeld om relevante documenten over de beveiliging alsnog in de openbaarheid te brengen. In reactie op het verzoek presenteerde het ministerie een lijst met 45 documenten, waarvan er 43 (gedeeltelijk) werden vrijgegeven.

Risicoanalyse

Het ministerie diepte uit de archieven vijftien documenten op over risicoanalyse. Hieruit blijkt dat niet alleen is gekeken naar veiligheidsrisico's zoals ongenode gasten, maar ook naar andere risico's. Zo concentreert een aantal rapporten zich op de mogelijkheid van achterblijvende implementatie en financiering. Ook technische risico's zoals onjuiste koppelingen, netwerkstoringen en verkeerd gebruik bij de eindgebruikers komen aan bod.

Structuur landelijk elektronisch patiëntendossier

Simpele weergave van de werking van het elektronisch patiëntendossier. Een arts vraagt vanuit zijn 'goed beheerd zorgsysteem' inzage in een medisch dossier van een andere arts. Het verzoek en de bijbehorende controles gaan via de zorgserviceproviders en het landelijk schakelpunt.



LSP: landelijk schakelpunt

ZSP: zorgserviceprovider

HIS: huisartsinformatiesysteem

ZIS: ziekenhuisinformatiesysteem

ZIM: zorginformatiemakelaar

DCN: datacommunicatienetwerk

(Z)AIS: (ziekenhuis)apothekinformatiesysteem

RIS: radiologieinformatiesysteem

Het wegvallen van het draagvlak door kritiek op het EPD wordt als een groter risico gezien dan een aanval van buitenaf, blijkt verder uit de documenten. En Interpay adviseert in een rapport een onafhankelijke risicoanalyse van de infrastructuur. Maar die analyse is niet vrijgegeven na het Wob-verzoek, terwijl naar alle risicoanalyses is gevraagd.

Een risicoanalyse waarin het gevaar van hackers 'hoog' wordt genoemd, is verder niet compleet geopenbaard. Het ministerie licht deze afwijzing toe in een brief: 'De passages

bevatten gevoelige informatie over de beveiliging van het EPD. Indien deze informatie zou worden geopenbaard, zou de veiligheid van het EPD niet kunnen worden gegarandeerd met alle risico's van ongewenste openbaarmaking van bijzondere persoonsgegevens van dien.' Dit druist in tegen het principe dat openbare beveiliging veiliger is dan geheime beveiliging.

Het is de vraag of de 'intelligente logging' wel bestaat

Hackerstest

In het Wob-verzoek is behalve naar risicoanalyses ook gevraagd naar de indringerstesten. Voor het landelijk elektronisch patiëntendossier is een grootschalige ketenbrede indringerstest (GKI) bedacht, die bestaat uit verschillende onderdelen. Zo stond er voor het tweede kwartaal van dit jaar een test gepland van de Sectorale Berichten Voorziening in de Zorg. Het Unieke Zorgverlener Identificatie Register (UZI-register) is eind 2009 getest, en dat wordt jaarlijks herhaald.

Het landelijk schakelpunt (LSP) is in juli 2009 aan een 'penetratietest' onderworpen, en daarbij zijn volgens het ministerie geen bevindingen van betekenis gedaan. De steekproeven in de goed beheerde zorgsystemen zijn eind 2009 begonnen en hebben evenmin iets bijzonders aan het licht gebracht. Ten slotte is er de EPD-keten Indringerstest op de Schakelconnecties (EIS), gericht op de verbindingen tussen de zorgverleners en de zorgserviceproviders. Die test laat de binnenkant van het schakelpunt echter ongemoeid, vermoedt onderzoeker Van 't Noordende. 'Dit betekent dat we geen informatie hebben over de beveiliging tegen aanvallen van binnenuit.'

Om vast te kunnen stellen in hoeverre de beveiliging van alle stappen van de aanvrager naar het dossier en terug worden gecheckt, is het nodig meer te weten over de EIS-test. Maar het ministerie weigert het stappenplan voor EIS te geven. Een tweede document met een programma van eisen is nog in de maak; ook de betrokkenen hebben nog geen kennis kunnen nemen van het concept.

Alles bij elkaar betekent dit dat de EPD-keten Indringerstest op de Schakelconnecties zich nog in een pril stadium bevindt. Het doel van EIS staat al wel in een brief: veilige en betrouwbare gegevensuitwisseling aantonen. Ook benadrukt het ministerie dat risico's ten aanzien van netwerken en informatiesystemen en de manipulatie van berichten door hackers worden meegenomen bij de uitvoering van EIS.

De resultaten van de andere onderdelen van de grootschalige ketenbrede indringerstest zijn niet genoemd of geleverd in antwoord op het Wob-verzoek. Een complete, ketenbrede test op hackers is er dus nog niet of wordt geheimgehouden, terwijl er al wel 2,5 miljoen dossiers worden gedeeld via het landelijk schakelpunt.

Abnormaal gedrag

Blijft over de 'intelligente logging', waarmee toezichthouders onterechte inzage in medische

SAMENVATTING

- Volgens het ministerie van VWS tonen 'indringerstesten' aan dat de beveiliging van het landelijk EPD deugt.
- Met de 'intelligente logging' kunnen toezichthouders misbruik bovendien makkelijk traceren.
- Het ministerie houdt de technische details van de beveiliging echter geheim, wat volgens de principes van ICT-beveiliging een slecht teken is.
- Documenten die met een beroep op de Wob zijn verkregen, doen vrezen dat de beveiliging eigenlijk nog in de kinderschoenen staat.

dossiers kunnen zien, zonder voor de onmogelijke taak te staan om al het berichtenverkeer te bekijken. Onderzoeker Van 't Noordende is bang dat dit filter kleine, gerichte aanvallen zal missen. Daarnaast is de overdracht van de met intelligente logging verkregen gegevens aan de toezichthouders College Bescherming Persoonsgegevens en Inspectie voor de Gezondheidszorg een risicomoment.

Op het Wob-verzoek levert het ministerie onder meer een plan van aanpak van Nictiz uit 2009. Daarin staat: 'Voor het detecteren van zowel technische als functionele issues ontbreekt de nodige informatie.' Verder staat in het plan dat er een systeem moet komen dat 'abnormaal gedrag' herkent en rapporteert en duidelijk maakt wat dat voor gedrag is. September 2009 was de geplande einddatum, maar het ministerie kan geen eindrapport overhandigen. Het is daarmee de vraag of de 'intelligente logging', waar zo vaak mee wordt geschermd, al wel bestaat.

Kinderschoenen

Als de hackerstesten en intelligente logging nog in de kinderschoenen staan, zoals de vrijgegeven documenten suggereren, staat de beveiliging dat ook. Uitslagen van tests en technische gegevens over de beveiliging worden niet gedeeld, terwijl dat wel beter is voor de veiligheid.


In de laatste voortgangsrapportage is wel te lezen dat het ministerie inmiddels iets toeschietlijker reageert op de voorstellen van onderzoeker Van 't Noordende om de beveiliging



Een complete hackerstest is er nog niet, of wordt geheimgehouden.



Documenten, de analyse van Guido van 't Noordende en de correspondentie met het ministerie, voortgangsrapportages van het EPD en meer vindt u bij dit artikel op www.medischcontact.nl.

te verbeteren. Zijn advies werd aanvankelijk afgewezen, maar nu schrijft het ministerie: 'Het onderzoek van de UVA zal worden gebruikt bij de continue evaluatie van de beveiligingsmaatregelen. Wanneer hieruit nieuwe inzichten naar voren komen, zullen aangepaste of aanvullende beveiligingsmaatregelen worden genomen.' 

Reactie van het ministerie van VWS

Trainen zonder publiek

In het artikel wordt gesuggereerd dat het een uitzonderlijke situatie is dat niet alle beveiligingsmaatregelen van een infrastructuur bekend worden gemaakt. Dit is echter vrijwel bij alle infrastructuren het geval. Het Kerckhoffs principe is van toepassing op encryptie en gaat ervan uit dat de kracht daarvan niet alleen gebaseerd mag zijn op het geheimhouden van de werking. Veel beveiligingssystemen bevatten geheimen (zoals sleutels en wachtwoorden) maar volgens het Kerckhoffs principe mogen alleen die elementen geheim worden gehouden die snel kunnen worden aangepast. Geheimhouding van maatregelen mag niet als beveiligingsmaatregel op zichzelf worden gebruikt.

Zoals de beveiligingsexpert Jaap van der Wal aangeeft op de website Zorgvisie, is dat voor het landelijk EPD juist niet het ge-

val: 'De werking van het systeem is gepubliceerd zodat iedereen de zwakke plekken kan opsporen. Dat stelt Nictiz in de gelegenheid om de gaten weer te dichten. Wij noemen dat security by clarity.'

De in het artikel aangehaalde niet verstrekte informatie betrof niet de maatregelen zelf maar de uitkomsten of voorbereidingen voor deze maatregelen. Het Nederlands elftal traint ook wel eens zonder publiek.

Stephan Koole,
directeur Voorlichting en Communicatie, ministerie van VWS



Een link naar de opmerkingen van Jaap van der Wal op Zorgvisie staan bij dit artikel op www.medischcontact.nl.