Eva Nyst
e.nyst@medischcontact.nl
@medischcontact

Ziekenhuis gehackt: hoe nu verder?

Via een lek in de beveiliging van thuiswerksoftwarebedrijf Citrix drongen hackers binnen bij Medisch Centrum Leeuwarden. De roep om meer grip op cyberveiligheid in ziekenhuizen zwelt aan. 'We kunnen ons niet veroorloven dat grote ziekenhuizen en spoedeisendehulpafdelingen uitvallen omdat ICT-systemen niet werken.'

HOLLANDSE HOOGTE

Vanuit huis radiologische beelden en andere patiëntgegevens inzien en het spreekuur van de volgende dag voorbereiden. De software van het Amerikaanse bedrijf Citrix maakt zulke informatie van buitenaf toegankelijk. Superhandig, en veel bedrijven, de overheid en ook ziekenhuizen maken er gebruik van. Dat maakt dat de cybercrimewaakhond van het ministerie van Justitie en Veiligheid, het Nationaal Cyber Security Centrum (NCSC), in de hoogste boom zit als het bedrijf op 17 december 2019 een lek in de beveiliging van twee producten bekendmaakt: de ADC en de Gateway. Een paar weken later hebben hackers de 'exploitcode' klaar waarmee ze via het gat kunnen inbreken. Op 10 januari informeert het NCSC organisaties die zich met de 'vitale infrastructuur' bezighouden – nutsbedrijven, banken – over de dreiging. Alleen, ziekenhuizen behoren niet tot deze processen die zo essentieel zijn 'dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid'.

Is het misschien beter als ziekenhuizen wel als 'vitaal' worden gezien?

Als een journalist hem tijdens het vragenuurtje hiernaar vraagt, zegt premier Mark Rutte daar 'niet van op de hoogte' te zijn en verwijst hij naar zijn collega Grapperhaus van Justitie en Veiligheid. Bij Nieuwsuur zegt IT-expert Ralph Moonen over de vitale infrastructuur 'dat het wel tijd wordt dat we die definitie een beetje gaan oprekken'. SP-Kamerlid Maarten Hijink sluit zich daarbij aan: 'Een vitale infrastuctuur wil zeggen: werkt het ontwrichtend als zo'n structuur uitvalt? Ik denk dat dat voor grote delen van de zorg wel zo is. We kunnen ons niet veroorloven dat bijvoorbeeld grote ziekenhuizen en spoedeisendehulpafdelingen uitvallen omdat ICT-systemen niet werken.' Het Kamerlid heeft de minister voor Medische Zorg gevraagd welke maatregelen hij gaat nemen opdat zorginstellingen 'eerder, actiever en indringender worden bijgestaan bij het nemen van maatregelen om hun data te beschermen tegen hackers'.

Moet er niet een cyberveiligheidsinstantie voor de zorg komen?
Die bestaat al sinds 2018: cybersecurity-centrum in de zorg Z-CERT (Computer Emergency Response Team). En Z-CERT staat wel op het NCSC-lijstje van te waarschuwen instanties. Z-CERT gaf de waarschuwing voor het lek netjes aan haar leden door. Deze stichting is opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen, de Nederlandse Federatie van Universitair Medische Centra en GGZ Nederland. Vooral ziekenhuizen en ggz-instellingen zijn nu lid. Vrijwillig, maar wat minister Bruins betreft sluit de hele zorgsector zich verplicht aan, zo liet hij maart vorig jaar weten op Kamervragen over het datalek bij het OLVG, waardoor onbevoegde studenten medische dossiers hebben ingezien. Daarbij zou het NCSC de bevoegdheid moeten krijgen om instellingen te dwingen hun software op orde te houden.

Is bekend hoeveel ziekenhuizen een lek in hun beveiliging hebben door Citrix?
Niet alle organisaties met Citrix hebben ook de software met het lek. Het Erasmus MC bijvoorbeeld heeft geen problemen gehad hoewel ze Citrix hebben. Dat umc maakt geen gebruik van de twee pakketten waar de kwetsbaarheid in zat. Thuiswerken kon daar dus nog gewoon. Maar dat was niet iedereen in de zorg gegund. Half januari meldt Z-CERT dat ruim honderd zorginstellingen de lekke software gebruiken. Echt mis gaat het op 14 januari bij Medisch Centrum Leeuwarden. Dat wordt digitaal van de buitenwereld afgesloten nadat een cyberaanval is vastgesteld. Later laat het ziekenhuis opgelucht weten dat de cyberaanval beperkt bleef tot 'de deurmat' en de hackers geen toegang hebben gehad tot vitale gegevens zoals patiënteninformatie. Ook de gemeente Zutphen en de provincie Gelderland zijn de klos. Bijna dertig organisaties melden bij de Autoriteit Persoonsgegevens (AP) dat ze een mogelijk datalek hebben. De AP geeft geen antwoord op de vraag hoeveel zorginstellingen daaronder zijn en benadrukt dat het gaat om meldingen 'uit voorzorg. De melders zijn nog aan het onderzoeken of er daadwerkelijk persoonsgegevens zijn gelekt'.

> 'Nederland was een specifiek target van aanvallen'

Is het Friese ziekenhuis de enige instelling in de zorg die is gehackt?
Dat lijkt er wel op. Met het nachtmerriescenario van de Universiteit Maastricht die hackers in de kerstvakantie mogelijk tonnen losgeld betaalde nog vers in het geheugen, adviseert VWS op voorspraak van de AIVD aan het eind van die week op 17 januari: zet de Citrix-systemen uit. Massaal gaan de systemen dat weekend uit de lucht. Ook het Diakonessenhuis in Utrecht doet dat, vertelt woordvoerder Trudy van den Oosten. 'We hadden steeds de updates van Citrix gevolgd, dus we wisten zeker dat het gat dicht was. Maar toen eind van de dag het ministerie van VWS met dit advies kwam, hebben we dat voor de zekerheid opgevolgd. Want als er toch iets mis zou gaan, is dat moeilijk uit te leggen.' Met de dienstdoende artsen wordt overlegd welke maatregelen hierdoor nodig zijn. 'Dat gold onder andere voor de radiologen die normaal vanuit huis werken. Zij moesten nu in huis komen. Maar het was ook lastig voor de specialisten die normaal op zondagavond vanuit huis hun spreekuur voorbereiden', aldus Van den Oosten. In het Diakonessenhuis konden patiënten wel inloggen in mijnDiak, dat draait niet op Citrix.

Was dat uitschakelen achteraf gezien echt nodig?
Het Financieele Dagblad (FD) concludeerde dit weekend dat in Nederland het NCSC strenger optrad dan elders. Volgens IT-expert Frank Groenewegen werd het advies om de Citrix-servers uit te zetten genomen doordat het bedrijf niet helder communiceerde, maar was die brede maatregel achteraf gezien 'niet nodig geweest' omdat de bug maar in één versie zat. Maar het NCSC baseerde zijn advies ook op informatie van de veiligheidsdienst AIVD, aldus de krant. 'Nederland was een specifiek target van aanvallen', zegt Steven Dondorp van beveiligingsbedrijf Northwave. Daarbij maakte de media-aandacht voor het lek vervolgens ook andere hackers wakker, schrijft het FD.

Komt de casus Citrix als een donderslag bij heldere hemel?
Nee, al langer spreken deskundigen hun uit zorgen over cyberveiligheid. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) concludeerde afgelopen september dat Nederland 'onvoldoende' is voorbereid op digitale ontwrichting. De WRR bracht twee eerdere crises in herinnering. Allebei betreffen die de zorg: 'Als gevolg van de besmetting van computers van de Britse National Health Service door de vermeende gijzelsoftware WannaCry (2016) moesten 19 duizend patiënt-afspraken worden geannuleerd. De NotPetya-aanval (2016) trof in Nederland de Rotterdamse haven, waardoor het containertransport via haven, snelweg en spoor deels kwam stil te liggen. In Oss werd bij deze aanval de vestiging van farmaceutisch bedrijf MSD getroffen, waardoor de medicijnproductie tot stilstand kwam en veel documentatie verloren ging.' ■

Gevraagd naar een terugblik op het Citrix-incident, laat het Medisch Centrum Leeuwarden weten er geen behoefte aan te hebben om hier met de pers op terug te kijken. 'De zorg liep probleemloos door, er waren alleen een paar lichte rimpelingen in het uitwisselen van beeldmateriaal met collega-ziekenhuizen zoals het UMCG. Maar die zijn inmiddels opgelost', laat een woordvoerder weten.

web
Meer over dit onderwerp vindt u onder dit artikel op medischcontact.nl/artikelen.