Virusaanval op zorginstellingen onvermijdbaar

Volgens schattingen van het ministerie van Veiligheid en Justitie zal **iedere zorginstelling** minimaal een keer per jaar geconfronteerd worden met een **virusaanval** en het verzoek om losgeld. Het overkwam Henk Methorst, nu hoofd informatie- en communicatietechnologie bij Revalidatie Friesland.

AUTEUR SUZANNE BREMMERS **BEELD** FOTOLIA

14 MEI 2015, 11.00 UUR De helpdesk van een vvt-instelling in het midden van Nederland krijgt een telefoontje van een medewerker dat ze haar Word-document kwijt is. Niet lang daarna komt eenzelfde melding van een andere medewerker binnen. In de loop van de dag wordt de helpdesk nog meerdere keren gebeld met dezelfde meldingen.

14.00 UUR Er zijn zoveel soortgelijke telefoontjes binnengekomen dat er geen sprake meer kan zijn van onoplettendheid. De helpdesk raadpleegt een systeembeheerder. Die heeft twee uur nodig om tot het vermoeden te komen dat een virus actief is. Hij licht hoofd automatisering Henk Methorst in. Aan het eind van de dag besluit Methorst alle systemen uit te schakelen. Methorst springt in de rol van crisismanager. Hij informeert de raad van bestuur op zeer regelmatige basis.

15 MEI, 9.00 UUR Methorst zoekt contact met de applicatieleverancier, want inmiddels is duidelijk dat onderdelen van de registratieapplicatie besmet zijn. De leverancier kan niet veel betekenen voor Methorst. Daarom zoekt hij contact met de eigen IT-leverancier. Het gaat inderdaad om een virus en ook het type virus wordt vastgesteld. Methorst vindt bestanden waarin staat dat hij 20.000 euro aan bitcoins (digitaal geld) moet betalen als hij wil dat de bestanden worden vrijgegeven. Methorst informeert de communicatieafdeling omdat ook bestanden met belangrijke aantekeningen over cliënten zijn besmet. Gelukkig werkt de zorginstelling nog niet met een elektronisch cliëntendossier.

12.00 UUR Methorst belt met cyberbeveiligingsbedrijf Fox IT. Het bedrijf kan misschien helpen doordat ze voor een specifiek virus in het bezit zijn van een lijst met 'sleu-

CEO-FRAUDE

Op het gebied van cybercriminaliteit komt ransomware het meest voor, maar het meeste geld gaat om in CEO-fraude, een nieuw fenomeen. Financiële afdelingen of managers worden, als de bestuursvoorzitter op reis is, uit naam van de bestuurder gevraagd met spoed geld over te maken. Het gaat vaak om grote bedragen, denk aan minimaal 100.000 euro. De schade wordt niet vergoed door de bank of verzekeraar. Ook hierbij is bewustwording belangrijk. Iedereen binnen een zorginstelling zou op de hoogte moeten zijn van het bestaan van deze vorm van fraude.

tels' waarmee je de bestanden kunt ontcijferen zonder losgeld te betalen. Het virus waarmee Methorst te maken heeft, zit daar helaas niet tussen. De analisten adviseren het losgeld niet te betalen. Digitaal forensisch onderzoeker Kevin Jonkers van Fox IT weet dat als zorginstellingen geen goede back-up hebben ze vaak bereid zijn losgeld te betalen. Hij adviseert altijd om het niet te doen omdat de bestanden soms alsnog niet worden teruggegeven. 'De criminele groep bedankt de zorginstelling dan hartelijk, maar vraagt vervolgens om nog meer geld.' De enige oplossing die Methorst nu nog heeft, is teruggaan naar de back-up. Als hij de back-up van eergisteren terugzet, is er feitelijk niets aan de hand, behalve dat medewerkers die gisteren bestanden hebben bewerkt een dag werk kwijt zijn.

16.00 UUR Dan openbaart zich het volgende probleem. De back-ups blijken niet in orde. Delen van cliëntengegevens worden opgeslagen op de systeemschijf en niet zoals gebruikelijk op de dataschijf, en van die systeemschijf zijn al maanden geen back-ups gemaakt. Bestanden over cliënten, over de intake en wachtlijsten zijn dus verloren. De onvolledige back-up wordt teruggezet. De computersystemen worden weer opgestart. Het verlies van de cliëntgegevens wordt genomen.

VAN DE SYSTEEMSCHIJF ZIJN AL MAANDEN GEEN BACK-UPS GEMAAKT

EEN MAAND LATER Het is duidelijk hoe het virus is binnengekomen. Iemand van het managementteam kreeg per mail een factuur van KPN, een vertrouwde afzender, en heeft de bijlage geopend. Eigenlijk zou het virus alleen de bestanden van deze medewerker kunnen besmetten, maar door een lek in de beveiliging kreeg het virus ook toegang tot de cliëntgegevens in de applicatieomgeving.

Lessen geleerd

Methorst, inmiddels hoofd informatie- en communicatietechnologie bij Revalidatie Friesland, heeft meerdere lessen geleerd uit de aanval. De tijd waartussen het virus wordt ontdekt en de systemen worden stilgelegd, moet zo kort mogelijk zijn. 'Enerzijds omdat het virus steeds meer bestanden besmet, maar ook omdat je alle data kwijt bent die medewerkers in de tussentijd aan het bewerken zijn. In veel gevallen van ransomware moet je namelijk terug naar je back-up. >

RANSOMWARE

Via een bijlage in een mailtje komt software binnen die bestanden versleutelt door middel van encryptie. De bestanden zijn dan ontoegankelijk; je kunt nergens meer bij. Als je een bedrag in bitcoins overmaakt, het losgeld ('ransom'), krijg je een sleutel om de bestanden te bevrijden. Het advies van de politie is om niet te betalen omdat je daarmee criminaliteit in de hand werkt. Bovendien laat je zien dat je chantabel bent en geven criminelen misschien maar een deel van de bestanden terug. Op www.nomoreransom.org staan decryptie-tools voor een aantal ransomwarevarianten waarmee je bestanden kunt ontsleutelen zonder losgeld te betalen. Een goede back-up is de beste voorzorgmaatregel.

> Hoe langer het duurt, hoe meer je kwijt bent.' Dat is niet de enige les. 'Het netwerk moet goed ingedeeld zijn in verschillende onderdelen voor verschillende personen of afdelingen', zegt specialist informatiebeveiligingsbewustzijn in de zorg Martine van de Merwe van Privacylab. 'Als je dat niet goed hebt ingericht, wordt er steeds meer versleuteld. Het is dus van belang om je netwerk goed in te richten zodat een virus nooit veel schade kan veroorzaken.'

De laatste les is een goede back-up maken en die ook controleren. Met een goede back up is het namelijk niet nodig om losgeld te betalen. Je heb immers een kopie van alle bestanden. Wat is een goede back-up? Van de Merwe: 'Bij een goede back-up is nagedacht over wat een aanvaardbaar verlies van gegevens is. De meeste zorginstellingen maken iedere dag een back-up, maar een back-up van patiëntengegevens wordt soms vaker gedaan. Dit is pas stap 1. Een *restore* van een back-up, waarbij je controleert of alles wat je nodig hebt op de back-up staat, is net zo noodzakelijk als nadenken over de frequentie.'

Bewustwording

Snel reageren, een goede indeling van het netwerk en back-up zijn nog niet afdoende maatregelen tegen ransomware. Naast technische aspecten, is bewustwording van medewerkers net zo belangrijk, stelt Van de Merwe, en dat geldt ook voor de raad van bestuur. 'Het is belangrijk dat medewerkers op de hoogte zijn van het fenomeen ransomware en dat ze alert zijn op verdachte mailtjes. De raad van bestuur zou het goede voorbeeld moeten geven. Als zij geen aandacht besteden aan het voorkomen van virussen, doen medewerkers dat ook niet.'

Het bewustzijn van ransomware is nu nog niet erg hoog, laat ook recent onderzoek van Deloitte onder NVZ-leden zien. 17 procent van de 65.000 medewerkers van zorginstellingen die zonder dat ze het wisten meededen aan een onderzoek, klikte op een mailtje waarvan ze hadden kunnen zien dat de afzender onbetrouwbaar was.

Dat geringe bewustzijn is volgens Van de Merwe ook een van de redenen waarom de zorg een aantrekkelijke sector is voor cyberfraudeurs, terwijl de noodzaak om weer snel online te zijn groter wordt nu het gebruik van elektronische patiëntendossiers toeneemt.

'HET IS BELANGRIJK DAT MEDEWERKERS ALERT ZIJN OP VERDACHTE MAILTJES'

Steeds persoonlijker

Bijkomend probleem is dat herkenning van ransomware steeds lastiger is. Dat komt doordat de mails die criminelen versturen persoonlijker worden, dat heet *spear phishing*. Volgens het ministerie van Veiligheid en Justitie hebben beroepscriminelen zich ontwikkeld tot 'geavanceerde actoren' die 'hoogwaardige operaties' uitvoeren. De investeringen in en opbrengsten van hun campagnes zijn groter geworden. Van de Merwe kent verschillende voorbeelden van spear phishing in de zorgsector. 'Een bekende is een mail met een factuur van Verpleegkundigen & Verzorgenden Nederland (V&VN). De criminelen sturen de mail specifiek aan een persoon van de financiële afdeling. Niet zo gek dus, dat diegene zonder twee keer nadenken de bijlage opent.' ■