Cybercrime

Dat ICT een steeds grotere rol in ons leven inneemt, zal niemand ontgaan. Ook in de zorgsector zal het digitaliseringsproces zich voortzetten. Waar dat toe gaat leiden is niet helemaal duidelijk, want de toekomst is nu eenmaal per definitie in nevelen gehuld. De digitale samenleving van de toekomst is daarom bij uitstek een thema om de fantasie de vrije loop te laten. En dat gebeurt dan ook volop in woord, beeld en geschrift. Zo heb ik pas geleden nog een bevlogen presentatie mogen bijwonen over de digitale toekomst van de gezondheidszorg. Heel boeiend, hoewel er tussen futuristische voorspellingen en realiteit doorgaans nog wel wat 'kleinigheidjes' van technische, financiële, psychologische of sociale aard te overbruggen zijn, waardoor niet alles wat in beginsel technisch mogelijk is (of lijkt) ook daadwerkelijk de nieuwe maatschappelijke realiteit wordt. Maar dit laat onverlet dat het belangrijk is om innovaties te omarmen die de kwaliteit, toegankelijkheid en betaalbaarheid van de zorg ten goede komen. In elke strategische beleidsnota krijgt dit thema dan ook aandacht.

Er is echter een belangrijke 'maar' die naar mijn smaak vaak wat onderbelicht blijft bij de toekomstverkenningen. Als digitale technologie een meer centrale rol in ons leven krijgt, neemt per definitie onze afhankelijkheid daarvan toe. En daarmee ook onze kwetsbaarheid. Niet alleen voor de onbedoelde en onvermijdelijke calamiteiten als gevolg van technische mankementen of menselijk falen, maar ook voor doelbewuste inbreuken op de ICT-infrastructuur. Het is niet voor niets dat jaarlijks door het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie een rapport wordt uitgebracht ('Cybersecuritybeeld Nederland') over de ontwikkelingen en bedreigingen op dit gebied. Het NCSC onderscheidt de volgende categorieën actoren waar we wat van te duchten hebben: beroepscriminelen (motief: geldelijk gewin), statelijke actoren (zoals buitenlandse inlichtingendiensten), cybervandalen en 'scriptkiddies' (hacken 'omdat het kan', baldadigheid, et cetera.), 'hacktivisten' (met ideologische motieven), interne actoren (zoals wraak, geldelijk gewin), cyberonderzoekers (aantonen kwetsbaarheden, eigen profilering) en private organisaties (digitale spionage en diefstal van bedrijfsgeheimen). Zorginstellingen kunnen doelwit worden van meerdere van deze groepen, vooral omdat het algemene beeld is dat het helemaal niet best gesteld is met het beveiligingsniveau van zorginstellingen. Reden voor SP-kamerlid Leijten om hierover recentelijk vragen voor te leggen aan ministers Schippers en Steur. Haar zorgen zijn bepaald niet ongegrond. Zo was er in februari van dit jaar bijvoorbeeld het bericht van beveiliger Kapersky Lab dat cybercriminelen medische apparatuur in ziekenhuizen kunnen hacken en gegevens kunnen stelen of diagnoses kunnen aanpassen. Ook beveiliger Fox-it wees er een paar maanden geleden op dat ziekenhuizen en hun medische apparatuur steeds vaker doelwit zijn van hackers. Oktober vorig jaar liet het Belgische tv-programma 'Koppen' zien dat het weinig moeite kost om digitaal bij een groot Vlaams universitair ziekenhuis in te breken en in een handomdraai duizenden medische dossiers te stelen. Slechts een paar maanden daarvoor (augustus 2015) zag de Amerikaanse overheid zich genoodzaakt ziekenhuizen te waarschuwen voor beveiligingslekken in bepaalde infuussystemen, en de gevaren hiervan voor patiënten. Enzovoorts.

De organisatie die zichzelf in slaap zou willen sussen met het idee 'dat overkomt ons toch niet' (deze houding is overigens risicofactor nr. 1) raad ik verder aan om kennis te nemen van het onderzoek van Deloitte ('Cyber security van netwerk verbonden medische apparatuur in Nederland' - 2015), waaruit naar voren kwam dat meer dan de helft van de onderzochte ziekenhuizen een keer te maken heeft gehad met een virusinfectie op het netwerk. Of de mededeling van de directeur informatiebeveiliging van beveiliger Dearbytes, dat van de in totaal 421 virusmeldingen bij hen

WFZ
Waarborgfonds voor de Zorgsector

Herman Bellers, directeur WFZ

in het afgelopen jaar er 106 afkomstig waren van zorginstellingen.

Het rapport van de NCSC benadrukt de toenemende cyberrisico's voor de zorgsector. Vooral vanuit de categorie beroepscriminelen. De belangrijkste reden is dat er gewoon veel geld mee te verdienen is. Een indicatie hiervan: op de zwarte markt zijn medische gegevens - naar verluid - al vijftig keer meer waard dan een gestolen creditkaartnummer. De logica van de cyberwereld is immers: hoe meer je weet over iemand, hoe waardevoller het wordt. En een medisch dossier bevat nu eenmaal gedetailleerde en gevoelige informatie. Bovendien speelt de schaalgrootte een rol: met één geslaagde hack heb je meteen een groot volume te pakken. Die combinatie maakt digitale datadiefstal interessant. Niet alleen zorginstellingen en zorgverzekeraars lopen digitaal inbraakgevaar, maar in principe elke medische databank. Zo meldt directeur Eddes van het Dutch Institute for Clinical Auditing DICA (waar volgens zijn zeggen 'ongelofelijk veel gegevens in de kluis liggen', onder andere tot individuele ziekenhuizen herleidbare kwaliteitsregistraties van darmkanker, maagslokdarmkanker en borstkanker) in een interview (juni 2015) dat het DICA meerdere keren te maken heeft gehad met (mislukte) pogingen tot hacken.

Als meest belovende en sterkst groeiende 'businessmodel' voor cybercriminelen noemt de NCSC 'ransomware en cryptoware'. Kort gezegd gaat het hierbij om gijzelingspraktijken, waarbij de toegang tot systemen of bestanden door criminelen onmogelijk wordt gemaakt, en vervolgens tegen betaling van losgeld weer wordt vrijgegeven. De manieren waarop criminelen hun slachtoffers besmetten met deze 'malware' lopen uiteen. In veel gevallen reageren slachtoffers op mails uit naam van bekende bedrijven. Waarbij het aanklikken van een bijlage voldoende is om een schadelijk bestand te openen en de ellende te veroorzaken. Denk ook hier niet te snel: zoiets zal mij niet overkomen. Gebaseerd op ervaringen bij het WFZ kan ik u meedelen dat een vergissing helaas snel is gemaakt. Als je een email ontvangt van bijvoorbeeld het Kadaster of de Kamer van Koophandel - zoals zo vaak - en ook nog eens kort nadat je met die instantie telefonisch contact hebt gehad, dan is een moment van te weinig waakzaamheid niet altijd te vermijden. En ik moet zeggen dat de kwaliteit van de criminele nep-mails - excuses voor de woordkeuze - alle complimenten verdient. Zoals een beveiligingsexpert het verwoordde: "Dit zijn geen jochies van dertien, maar georganiseerde groepen criminelen die succesvolle zakenmannen zouden kunnen zijn."

Gelet op zijn rol en positie heeft het WFZ van oudsher veel aandacht voor beveiligingsaspecten, ook digitaal. Naar aanleiding van de ervaringen met cryptoware hebben we desondanks besloten om er nog een schepje bovenop te doen. Zo maken we bijvoorbeeld tegenwoordig twee keer per dag automatisch een back-up van al onze bestanden. Mocht het - ondanks alle andere ingebouwde systeembeveiligingen en onze eigen toegenomen alertheid op twijfelachtige mails - toch nog een keer misgaan met cryptoware, dan is onze maximale schade een halve dag (type)werk. Onze kwetsbaarheid voor losgeldclaims hebben we hiermee dus sterk verminderd. Maar dit is geen reden om zelfgenoegzaam achter over te leunen. De criminele creativiteit is namelijk groot, zoals het NCSC vaststelt. Als potentieel slachtoffer loop je dus eigenlijk voortdurend achter de nieuwe ontwikkelingen aan. Ik realiseer mij ook dat een organisatie als het WFZ - vanwege factoren als de van oudsher nadrukkelijk aanwezige 'risicocultuur', de beperkte personele omvang en de relatief afgesloten fysieke locatie - qua veiligheidsrisico's heel wat eenvoudiger te behappen is dan een gemiddelde zorginstelling. De veiligheidsrisico's voor bijvoorbeeld een groot algemeen ziekenhuis - met een gigantisch gebouw, een zeer omvangrijk personeelsbestand, en dagelijks in- en uitlopende mensenmassa's - zijn van een totaal andere orde. Deze conclusie stemt mij overigens verre van vrolijk. Als ik zie hoeveel tijd, geld en energie bij een kleine en overzichtelijke organisatie als het WFZ al wordt opgeslurpt door de digitale ontwikkelingen en de hieraan verbonden veiligheidsaspecten, wat mag men dan in redelijkheid verwachten van de gemiddelde zorginstelling? Organisaties met relatief beperkte ICT-deskundigheid en -budgetten, die ook nog eens volledig in beslag worden genomen door de hectiek en (transitie-) problemen van alledag?

Ik vrees dat er in de komende jaren alle aanleiding zal zijn voor meer Kamervragen. ///