Zorgsector aantrekkelijk voor cybercriminelen

Informatieveiligheid vraagt om goed leiderschap

Cyberaanvallen zijn volop in het nieuws. Het veroorzaakt veel schade. Wereldwijd zijn er voorbeelden van organisaties, waaronder ziekenhuizen en huisartsenposten, die stil komen te liggen. Medische apparatuur is niet meer bruikbaar. Operaties worden uitgesteld. En ambulances kunnen niet meer goed worden aangestuurd. Het voelt een beetje als een ver-van-mijn-bedshow. Waarom zou jij je druk maken over digitale veiligheid? Tijdens het congres 'Cyber? Mij een zorg!' van SVDC en Turnaround Communicatie wordt dat meer dan duidelijk.

"Pas als je weet dat iets kan, ga je erover praten", zegt technologietrendwatcher Yori Kamphuis. Daarom neemt hij de zaal mee naar een toekomst waarin zorg en technologie één zijn. Een toekomst waarin een handdruk voldoende is voor het verzamelen van iemands dna, om dat vervolgens te verwerken tot een spermacel en na negen maanden een tegenstander te beschuldigen van vreemdgaan.

Aan het stuur van de toekomst

Via 3D-printtechnologie print een verpleegkundige voortaan de echo van een ongeboren baby, zodat een blinde vrouw haar kind kan 'zien' door te voelen. Maar ook een oor of neus kan geprint worden. Met behulp van stamcellen wordt dit 'levend' gemaakt en opgeplakt. Deep brain beïnvloeding is in staat de hersenpulsen van Parkinsonpatiënten te corrigeren. De hersensignalen van dwarslaesie-patiënten worden via een extern gecomputeriseerd zenuwstelsel vertaald, waardoor zij hun ledematen weer kunnen bewegen. En prothesen zullen signalen terug gaan geven aan de hersenen. Het lezen, analyseren en verwerken van hersengolven krijgt steeds meer toepassingen. Zo is het mogelijk hersenen aan te sluiten op een rat en via hersengolven zijn staart te laten bewegen. Op die manier wordt het ook mogelijk je hond voor rood licht te laten stoppen of je kind ergens van te weerhouden. Kamphuis: "Mens, machine, biologie en computercode komen steeds meer bij elkaar. Hoe gaan we daar als maatschappij en zorgsector mee om? Welke ethische vraagstukken doen zich voor? En hoe digitaal veilig is dit? Zorg voor technologiekennis, zodat je aan de hand daarvan binnen de zorgsector en binnen je eigen instelling gesprekken kan voeren de benodigde maatregelen kan nemen. We staan zelf aan het stuur van de toekomst en hebben invloed op deze ontwikkelingen."

Laat je als bestuurder zien

In contrast met het futuristische beeld dat Kamphuis schetst, grijpt Ruben Wenselaar, CEO Menzis, terug op de muur van Hadrianus. Deze muur, over de hele breedte van Groot-Brittannië, beschermde de Romeinse noordgrens tegen vijandelijke invallen. Voor de drie meter dikke muur liep een diepe gracht met puntige staken. Daarachter lag nog weer een aarden wal, een diepe gracht en opnieuw een aarden wal. Verder was de grens versterkt met torens die goed zicht hadden op de verdedigingslinie. De metafoor is helder. Wenselaar: "In het digitale landschap moet digitale veiligheid op de agenda staan van het bestuur. Daar is geen discussie over mogelijk." Bij Menzis gebruikt het bestuur een risicokaart om inzicht te krijgen in de bedrijfsdoelstellingen en bijbehorende risico's. Cybersecurity staat altijd in de top. Die toprisico's bespreekt het bestuur van de zorgverzekeraar met de Raad van Commissarissen. "Zorgbestuurders moeten hierover spreken met

hun Raad van Toezicht. Ook dienen zij meerdere verdedigingslinies op te trekken, waaronder organisatorische maatregelen, autorisatiemanagement, gegevensbescherming en loggen. En heel belangrijk: Geef zelf het goede voorbeeld. Laat je als bestuurder zien, doe mee met bewustwordingsprogramma's en stuur consequent op dit onderwerp."

Aarzel niet en bel Z-CERT

Een van de verantwoordelijkheden van het bestuur is deelname aan Z-CERT. SG Gerritsen is heel stellig tijdens de opening in januari van dit computer emergency response team voor de zorg: "Bestuurders hebben echt wat uit te leggen als ze niets doen met dit onderwerp. Het gevaar is te groot." Directeur Nienke van den Berg vertelt dat Z-CERT een stichting is die alle zorgverleners tot haar doelgroep rekent. Deelname is niet gratis, "omdat we een bewust besluit van de boardroom willen hebben. Het bestuur moet namelijk zorgen dat digitale informatieveiligheid landt op alle niveaus in de organisatie." In 2017 is Z-CERT gestart met ziekenhuizen, categorale instellingen en GGZ-instellingen, in samenwerking met de Nederlandse Federatie van Universitaire Medische Centra (NFU), de Nederlandse Vereniging van Ziekenhuizen (NVZ) en GGZ Nederland. In 2018 vindt een pilot plaats met de langdurige zorg (Actiz), gehandicaptenzorg (VGN) en zelfstandige klinieken (ZKN). "Preventief sturen we in samenwerking met het Nationaal Cyber Security Centrum operationele alerts naar de aangesloten zorginstellingen. Ook verspreiden we diverse informatieproducten in het kader van het verhogen van de cyberweerbaarheid. Daarnaast geven we advies bij cyberincidenten. Aarzel niet en bel ons als zich iets voordoet. We helpen uw zorginstelling én we helpen anderen door ze te waarschuwen. Met elkaar maken we de zorg veiliger."

Leiders én managers gevraagd

Uit onderzoek van CGI in 2017 blijkt dat bestuurders data-analyse zien als prioriteit, om daarmee de zorg te verbeteren en de kosten te verlagen. Cybersecurity is de vijfde prioriteit, na bijvoorbeeld organisatieverandering en klantervaring. In 2015 was het helemaal geen prioriteit. Wat dat betreft neemt dit onderwerp steeds meer aan belang toe. Er is echter wel een gat met de IT-prioriteiten van de organisatie. Daar staat cybersecurity op nummer 2. "Bestuurders focussen op business optimalisatie", analyseert Eelco Stofbergen, directeur Cybersecurity bij CGI Nederland. "Denk in dat kader aan het invoeren van agile werken: in korte sprints van twee à drie weken worden nieuwe applicaties en functionaliteiten ontwikkeld. Er is geen tijd meer om wekenlang te pentesten, wat voorheen gebruikelijk was. Informatiebeveiliging moet op een andere manier in het IT-proces ingebed worden." Om dat voor elkaar te krijgen, is leiderschap nodig. Op het hoogste niveau moet iemand eigenaar zijn van het onderwerp 'informatiebeveiliging' en daarop sturen in lijn van de organisatiedoelstellingen, als toegevoegde waarde aan de business. Zo moet de IT-afdeling gericht zijn op het succesvol maken van de business, wetend waar de risico's zitten en security dient vroeg in het ontwikkel- of businessproces meegenomen te worden. Stofbergen: "Mensen gaan in de weerstand. De effectiviteit van de organisatie neemt af, om vervolgens weer toe te nemen. Dat proces moet goed begeleid worden, door leiders én door managers. Leiders ontwikkelen visie, krijgen mensen mee, motiveren en inspireren. Managers organiseren, regelen en plannen de praktische zaken. Beide heb je nodig om veranderingen voor elkaar te krijgen."

Integriteit en vertrouwelijkheid

De Algemene verordening gegevensbescherming (Avg) is een belangrijk onderwerp voor zorgorganisaties die informatieveiligheid serieus nemen. Op 25 mei 2018 moet heel Nederland aan

deze wet voldoen, dus ook de zorgsector. Leonie Gerding, juridisch adviseur bij Verdonck Klooster & Associaties, merkt in de praktijk dat sommige zorgorganisaties de Avg implementeren omdat ze bang zijn voor een boete. “Dat is zonde. Vanuit goed leiderschap zouden de beginselen van de Avg – integriteit en vertrouwelijkheid – centraal moeten staan. Die sluiten namelijk uitstekend aan bij de relatie tussen zorgverlener en patiënt. Vertel daarom heel transparant aan jouw doelgroep wat je doet met de verzamelde gegevens. Dat kan gewoon met vijf icoontjes of vijf beloften. En als je het echt belangrijk vindt, dan bespreek je dit aan het begin van een nieuwe cliëntrelatie.” Daarnaast vraagt de Avg volgens Gerding om goede gesprekken met ketenpartners, zoals leveranciers en andere aangesloten zorgorganisaties. “Iedere partij heeft andere belangen. Die moeten expliciet gemaakt worden. Daardoor kom je tot een betere gegevensbescherming.” Neem bijvoorbeeld beroepsethiek. Dat betekent voor een zorginstelling wat anders dan voor een app-ontwikkelaar. Het risico bestaat dat de app daardoor data deelt met anderen dan alleen de eigen arts. Of neem het belang van datalekken. Een leverancier brengt zijn software graag snel naar de markt, terwijl een zorginstelling het graag van tevoren getest wil hebben. “Doe dit niet alleen bij nieuwe leveranciers, maar ook bij bestaande leveranciers. En houd je eigen dienstverlening tegen het licht. Heb ik écht alle gegevens nodig die ik verzamel?”

Interne governance

Voor informatiebeveiliging in de zorgpraktijk biedt de NEN7510 goede handvatten. Dennis Verschuuren, Information Security Officer Maasstad Ziekenhuis en lid van de NEN7510 Normcommissie, komt in het implementatietraject echter een aantal hobbels tegen. Een daarvan is gebruiksgemak voor zorgpersoneel en patiënt. “Zodra je DigiD met SMS authenticatie verplicht stelt, daalt het gebruik van de betreffende website of app spectaculair.” Ook schort het aan bewustwording. “Nog steeds zijn er veel mensen die altijd dezelfde wachtwoorden gebruiken. De digitale bekwaamheid van de zorgprofessional is momenteel niet afdoende om de moderne zorg bij te kunnen houden.” Verder constateert hij dat informatiebeveiliging soms gevangen zit een vicieuze cirkel van privacy versus zorgverlening versus veiligheid versus performance. Zo blijkt privacy-by-design bijvoorbeeld lastig toe te passen, omdat de leverancier medische en persoonsgegevens niet van elkaar kan scheiden. Ook het vragen van toestemming aan patiënten om gegevens te mogen verwerken, stuit op problemen. Vanwege de vele verschillende situaties moet de software 144 verschillende aanvinkmogelijkheden aanbieden. Om deze en andere hobbels het hoofd te bieden en de implementatie te laten slagen, heeft Verschuuren een security dashboard ontwikkeld dat inzicht geeft in alle normen, achterliggende documenten, beheersmaatregelen, contracten en hobbels. Ook de interne governance is een belangrijke randvoorwaarde. Deze is georganiseerd over alle lagen in de organisatie. Aandacht voor en implementatie van informatiebeveiliging verloopt top down vanaf de Raad van Bestuur en bottom up vanuit de preventieteams. In deze teams zitten medewerkers die aansluiting hebben bij de verschillende operationele en stafafdelingen, en die informatiebeveiliging onder de aandacht brengen. “Uiteindelijk wil ik dat iedereen een ‘security mens’ is.”

Samenwerking regionale politie

Theo van der Plas, programmadirecteur Digitalisering en Cybercrime van de politie, wil samen met zorginstellingen strijden tegen cybercriminelen. “We moeten met elkaar voorkomen dat ziekenhuizen of andere zorginstellingen stil komen te liggen als gevolg van ransomware, malware, phishing of digitale inbraken. Dat is namelijk niet alleen een crisis voor uw organisatie, maar ook voor de samenleving. Zorg er daarom voor dat u zo’n klap flexibel op kunt vangen en de continuïteit snel

weer kunt herstellen.” Ook roept Van der Plas op om informatie uit te wisselen met de cybercrime-eenheid van de regionale politie. “Hoe meer data u verzamelt en hoe afhankelijker u daarvan wordt, hoe aantrekkelijker u bent voor cybercriminelen. Meldt daarom verdachte zaken. Dan kunnen wij actie ondernemen, proberen de criminelen voor te zijn en ze opsporen.” Er zijn voorbeelden genoeg van zorginstellingen die te maken hebben gehad met cybercrime. Zo werd de salarisadministratie van een organisatie gehackt en de salarissen naar een andere rekening overgemaakt. Andere organisaties hadden last van ransomware en leden financiële schade door het stilleggen van afdelingen en het terugzetten van back-ups. “Bent u slachtoffer geworden, doe dan altijd aangifte bij de politie en overhandig voor zover mogelijk bewijs. Licht instanties als de Autoriteit Persoonsgegevens en Z-CERT in en communiceer intern en extern over het incident.” Van der Plas sluit uit met de volgende opmerking: ‘never waste a good crisis’. Ga gelijk met het bestuur aan tafel om budget te krijgen voor een betere cybersecurity en informatiebeveiliging.

Investeer in continuïteit

Een van de stellingen tijdens het paneldebat luidt: ‘Bij zorginstellingen valt niets te halen’. Marcel van Oirschot (Fox-IT), Melanie Rieback (Radically Open Security) en Eric Luiijf (zelfstandig cybersecurity consultant) gaan onder leiding van Elly van den Heuvel, secretaris Cyber Security Raad, het gesprek aan met de zaal. Het blijkt vooral interessant te zijn om ziekenhuizen plat te leggen met ransomware. Omdat zorginstellingen hun backups niet zo goed op orde hebben, is de kans aanwezig dat het geëiste losgeld wordt betaald. Dat is in sommige gevallen goedkoper dan alle schade herstellen. De politie raadt betalen af, omdat het onzeker is of criminelen daadwerkelijk de bestanden weer vrijgeven en omdat een criminele industrie op die manier in de lucht wordt gehouden. Van der Plas: “Investeer in backups en continuïteit, in plaats van geld besteden aan criminelen en hopen dat het goed komt.” Maar backups zijn niet zaligmakend. Het is ook interessant via een hack medische gegevens te veranderen. Als dat niet wordt opgemerkt, staat dat vervolgens vast in de backup. “Er zijn voorbeelden van pogingen tot moord op familieleden via verandering van medicijnuitgifte”, zegt Luiijf. Ook het chanteren van patiënten – zeker als ze beroemd zijn – met hun medische gegevens kan geld opleveren, stelt Rieback. “Digitale veiligheid in de zorg moet op een hoger niveau komen. Er is onderling nauwelijks concurrentie, dus de patiënt kan niet kiezen tussen een veilig en niet veilig ziekenhuis kiezen.”

Inzicht in eigen veiligheid

Een andere stelling poneert dat de privacywet (Avg) het topje van de ijsberg is van de veiligheidsrisico’s die zorginstellingen lopen. Al snel blijkt dat dat iedereen dit onderkent. Slagbomen bij het parkeerterrein, brandalarm, toegangscontrole, airco zijn voorbeelden van gebouwfuncties die vaak worden uitbesteed én die vaak online zijn. Wasstraten voor bedden bevatten veel technologie. En medische apparatuur draait op verouderde software en hangt slecht beveiligd aan het netwerk of het internet. Rieback brengt de discussie vervolgens op een ander spoor. Zij pleit voor maximale openheid en transparantie in informatievoorziening en informatiebeveiliging. Dat leidt tot een betere cybersecurity van zorginstellingen. “Als zorgsector zou je met elkaar een wiel moeten bouwen, in plaats van allemaal afzonderlijk het wiel uitvinden. Op het gebied van beveiliging zouden jullie geen concurrenten moeten zijn en volledig transparant informatie met elkaar moeten delen. Het is jullie tegen de buitenwereld, niet jullie tegen elkaar.” Uit de zaal komt naar voren dat leveranciers niet vooruitstrevend zijn in het delen van informatie en dat zij een obstakel vormen. Rieback biedt wel openheid aan haar leveranciers en het panel vindt dat zorginstellingen volwassener mogen optreden

naar hun leveranciers. Spreek ze aan. Vraag inzicht. Werk samen aan veiligheid. Het is onmogelijk om beveiliging over de schutting te gooien en het aan een leverancier over te laten. Als organisatie moet je daarbij betrokken zijn. Lukt dat niet, kies dan voor een andere leverancier. Functioneel of aanbestedingstechnisch is dat niet altijd makkelijk of mogelijk, maar het gaat het panel vooral om de mindset die moet veranderen. Zorginstellingen gaan over hun eigen veiligheid en moeten daar inzicht in hebben!"

***Turnaround Communicatie**: dé communicatiespecialist voor veiligheid, ICT, zorg en overheid. Bijvoorbeeld voor bewustwordingstrajecten digitale veiligheid en implementatie van systemen.*
***SVDC**: adviseur in crisisbeheersing. Bijvoorbeeld voor OTO-trajecten, crisismanagement en crisisoefeningen.*