Cyberoorlog in de boardroom?

Security, hackers, pentesten, AVG, trojan, fishing, spamdefense, firewalls, NEN7510, general IT-controls, WannaCry, backup en restore, access & identity management: het lijkt wel of mijn collega's in de Raad van Toezicht water zien branden. Ja, de privacywet (AVG) scoort wel op de bingo-kaart van vergaderonderwerpen. Daar hebben we het in de Raad zeker en zelfs ook meerdere malen over gehad. Maar die andere aanduidingen lijken te leiden tot glazige blikken. Zijn dat onderwerpen voor de Raad van Toezicht? Waar hebben wij het dan toch in vredesnaam over?

Ik vertel over de WannaCry-gijzelsoftware die vorig jaar alleen al de Britse ziekenhuizen circa 100 miljoen euro aan schade heeft gekost, aldus een rapport over het vergroten van de digitale weerbaarheid van zorgorganisaties van het Britse Department of health & Social Care. Ja, dat doet even zeer…

De grote ICT-storingen in het IJsselland Ziekenhuis in juni van het afgelopen jaar en in het Radboudumc begin 2018 - en de impact ervan - zijn helaas enkele van nog veel meer Nederlandse voorbeelden van hoe afhankelijk zorgorganisaties van ICT geworden zijn. Waarbij meteen vragen rondom de waarborgen van patiëntveiligheid aan de orde zijn. Het is dan ook niet vreemd dat de Onderzoeksraad voor Veiligheid onderzoek instelt naar de digitale veiligheid van ziekenhuizen.

Meer aandacht voor informatiebeveiliging

Ook de Inspectie Gezondheidszorg en Jeugd (IGJ) heeft in 2018 aangekondigd dat er meer aandacht nodig is voor afspraken en informatiebeveiliging bij gebruik van e-health. Een eerste inspectie bij tien ziekenhuizen en andere zorgorganisaties liet zien dat slechts twee instellingen konden aantonen aan belangrijke normen voor informatiebeveiliging te voldoen. Dit ondanks het op zich goede actieplan 'Informatiebeveiliging in de medisch-specialistische zorg en GGZ'. Waarbij ik mij dan vervolgens afvraag: hoeveel toezichthouders hebben dit überhaupt gelezen? Daar gaat dus het vergrootglas de komende tijd nog nadrukkelijker op.

En boem! Hiermee wordt cybersecurity inderdaad ook een onderwerp voor de Raad van Toezicht: omdat cybercrime het hart van de zorg kan raken en in extreme gevallen zelfs levens kan kosten.

Voorkomen en beperken

De vraag die geagendeerd dient te worden, is dan ook hoe de zorgorganisatie en diens ketenpartners verstoring, uitval en misbruik van ICT proberen te voorkomen, én: in hoeverre zij voorbereid zijn om de gevolgen daarvan te beperken.
Staat dit onderwerp ook op de agenda van de Raad van Bestuur? Is er überhaupt een SIO (Security Information Officer) in onze organisatie die zich hier mee bezig houdt? Op welke wijze is informatieveiligheid in de organisatie geborgd?

Vaak is het handig daarbij een onderscheid te maken in drie categorieën:

- '**Papier**': opstellen van beleid, procedures, richtlijnen, workflows en handleidingen
- '**Mensen**': bewustwording van gevaren en waarde van informatie. Het werken conform hetgeen op "papier' is geformuleerd
- '**Techniek**': inrichting van de ICT-infrastructuur conform de beleidseisen en zorgdragen dat de gewenste werkwijze is 'ingebakken' in de techniek

Een andere driedelige bril van kijken of vragen, is onderscheid maken naar:

- **Basisniveau**: alle systemen en software geüpdatet naar meest recente versie, firewalls, redundantie/failover, spamfilters, toegangsbeveiliging, calamiteitenplannen, back-up & restore, etc.
- **Monitoring & verbetering**: logging, security scanning op kwetsbaarheden, training en bewustwording, monitoring-beveiligings-tools, NEN7510 nulmeting, en vooral ook oefenen.
- **Externe toetsing**: NEN7510 audit, pentesten (penetratietesten om de hackerveiligheid te testen), externe partij/tool voor analyse verkeer en patronen, etc.

Agendeer dit onderwerp

Het is dus absoluut zaak om als toezichthouder dit onderwerp te agenderen. Nodig de bestuurder uit om een presentatie over dit onderwerp te laten verzorgen door de betreffende verantwoordelijk functionaris. Laat de accountant nog nadrukkelijker in zijn interim-controle het onderwerp ICT beoordelen en dit opnemen in zijn management letter. Gebruik bovenstaande onderwerpen en vragen om je zelf te oriënteren en voor te bereiden. Uiteindelijk is een proactieve aanpak de beste defensie in deze potentiële cyberoorlog.

Henk van der Stelt is professioneel toezichthouder in de zorg met de portefeuilles financiën en ICT.