Nog steeds cyberoorlog in de bestuurskamer!

Op de agenda staat de eindrapportage van de externe adviseur inzake onze ICT- en informatieveiligheid. Ik kan het niet laten om toch even een diepe zucht te laten horen en moet denken aan mijn column alweer meerdere jaren geleden in dit blad. Die column had als titel 'Cyberwar in de boardroom'. Helaas moeten we vaststellen dat die oorlog nog steeds gaande is.

Oekraïne en de verhalen over de virtuele oorlog met vijandelijke hackers wakkeren dit vuurtje verder aan. De Raad van Toezicht die dit nog steeds niet heeft geagendeerd en besproken met zijn Raad van Bestuur, mag ernstig aan zijn functioneren gaan twijfelen. Dit is een onderwerp dat juist vanuit de bril van risicomanagement minimaal elk jaar behandeld dient te worden.

Praktische vragen

Daarom kom ik in deze column met een aantal praktische vragen die u kunt gebruiken in uw vergaderingen.

1. **Risicomanagement als basis**
   De aanpak van risicomanagement vormt de basis. Hier begint het dus mee en dit onderwerp hoort niet alleen thuis bij het audit-comité, maar in de voltallige Raad van Toezicht. Een risicogestuurde aanpak zorgt ook voor een effectiever gebruik van alle benodigde resources die per definitie al schaars en kostbaar zijn. Zeker op dit terrein.

   Hebben wij zicht op hoe de organisatie dit onderwerp heeft belegd? Op welke wijze is de Raad van Bestuur hierbij betrokken? Hoe volgen zij dit in de tijd? Immers, risicomanagement is absoluut chefsache.

2. **Niet alleen korte termijn**
   De verleiding is groot om alleen te kijken naar de kortetermijnmaatregelen om de gaten in de dijk te dichten. Maar dat is absoluut onvoldoende. Natuurlijk moet het grootste gat in de dijk eerst dicht, maar uiteindelijk gaat het om een structurele meerjarige continue beheersopgave.

   Is daar ook voldoende aandacht voor? Welke kosten en formatie vinden we hiervoor terug in de begroting van dit en volgend jaar? Niets? Dan is er nog het nodige huiswerk te doen om niet de continuïteit en kwaliteit van de zorg overmorgen wederom op het spel te zetten.

3. **Goed en integraal beleggen in de organisatie**
   Maar dit is nog niet voldoende. Hoe versla je dit veelkoppige monster in de organisatie? Bieden regelmatige maandelijkse rapportages een vinger aan de pols? Heeft het de juiste ophanging in de organisatie en wordt het een onderdeel van integrale managementverantwoordelijkheid op managementteam-niveau? Het moet zeker niet het feestje (nou ja, feestje…) van ICT sec worden. Is de bemensing adequaat? Hebben we echt mensen in huis die dit goed op de rit kunnen krijgen en houden? Hoe komt het terug in de overlegstructuur van afdelingen? Is er een meldingssysteem? Hebben we echt zicht?

   Hoe kun je dit integreren in de veiligheidscultuur waar ook dokters, verpleegkundigen en verzorgenden hun inbreng hebben? Mede om die reden is het niet alleen een onderwerp voor de auditcommissie, maar ook voor de commissie Kwaliteit en Veiligheid van de Raad van Toezicht.

   Is er voldoende zicht op de breedte van dit onderwerp? Het is immers een breed onderwerp dat niet alleen over de harde techniek van firewalls en pen(etratie) testen gaat, maar vooral ook om de zachtere cultuurelementen gaat.

Tot slot

Hoe voorkom je dat je dit in 'splendid isolation' doet en weer zelf het wiel denkt te moeten uitvinden? Zoek de samenwerking op met andere partijen en collega-organisaties. Tap kennis en ervaring af. Je kunt het bijna per definitie niet alleen stand alone als organisatie oplossen. Je zult ook een deel moeten uitbesteden aan externe leveranciers en dat stelt op zich weer hoge eisen aan hoe je dat doet en bewaakt.

Kortom, de cyberoorlog is nog lang niet gestreden en gewonnen. ■

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