Digitale storm op komst: hoe niet te verzuipen in NIS2

De golven beuken tegen de digitale dijken van zorginstellingen. Cyberaanvallen, datalekken, het is aan de orde van de dag. En alsof de storm nog niet hevig genoeg was, rolt er een tsunami aan regelgeving op ons af: de NIS2-richtlijn. Een vloedgolf aan eisen die zorginstellingen moeten implementeren om de digitale patiëntgegevens veilig te stellen. En terwijl de IT-afdeling koortsachtig zandzakken vult, zit de Raad van Toezicht (RvT) vaak nog op het terras met een kop koffie en een gevulde koek. "Ach," denken ze, "die digitale rompslomp, dat lossen die techneuten van ICT wel op."

Fout! NIS2 is geen IT-dingetje, het is een bom die de hele organisatie op zijn grondvesten kan doen schudden. En de RvT, die club wijze dames en heren die geacht wordt boven de dagelijkse beslommeringen te staan, heeft een cruciale rol te spelen.

Nu vraag ik u, beste lezer, hoe moet een RvT in hemelsnaam navigeren in deze digitale storm? Moeten we plotsklaps allemaal cybersecurity-experts worden? De bits en bytes van de IT-infrastructuur tot in detail doorgronden?

Want laten we eerlijk zijn, cybersecurity is voor veel toezichthouders even grijpbaar als een nat zeepje. Ze denken bij een firewall aan een brandwerende muur in een serverruimte en bij phishing aan hengelen in een meer met verdacht veel e-mails. En dan die afkortingen! CISO, SOC, SIEM... het klinkt als een geheimtaal die alleen nerds beheersen.

Maar beste RvT-leden, wegkijken is geen optie meer. NIS2 eist dat jullie de digitale risico's begrijpen, de impact ervan op de organisatie kunnen inschatten en controleren of het bestuur wel de juiste maatregelen neemt.

Hoe dan?

Begrijpt de RvT de risico's? Is er een helder beleid? Wordt er geïnvesteerd in cybersecurity? Dat zijn de vragen die centraal staan. Hoe doe je dit dan? Simpel, door de juiste vragen te stellen. Niet: "Hebben we wel een goede firewall?", maar: "Hoe zorgen we ervoor dat onze kritieke systemen beschermd zijn tegen cyberaanvallen?" Niet: "Doen we wel aan phishing-training?", maar: "Hoe bewust zijn onze medewerkers van cybersecurityrisico's en hoe gaan ze daarmee om?"

En laten we vooral niet vergeten: cybersecurity is geen IT-probleem, het is een organisatiebreed probleem. Het gaat niet alleen over techniek, het gaat over mensen. Van de arts op de polikliniek tot de schoonmaker in de gang, iedereen heeft een rol te spelen. De RvT moet erop toezien dat dit besef doordringt tot in alle lagen van de organisatie. Zijn onze medewerkers getraind om een phishing-mail te herkennen? Weten ze wat ze moeten doen bij een ransomware-aanval? Een menselijke fout is vaak de zwakste schakel in de digitale verdediging.

Onwetendheid geen excuus

Natuurlijk, je hoeft geen hacker te worden om toezicht te houden op cybersecurity. Maar je moet wel snappen wat er speelt. Lees je in, volg een cursus, huur desnoods een externe expert in. Want onwetendheid is geen excuus meer.

Stel je voor: een grote cyberaanval legt je organisatie plat. Artsen en verpleegkundigen kunnen niet meer bij hun gegevens, systemen liggen eruit, de media smult van het drama. Wie wordt er dan aan de schandpaal genageld? Juist, de RvT. "Waar waren jullie?", zal de woedende menigte roepen. "Waarom hebben jullie dit niet zien aankomen?"

Tot slot, beste lezers, laten we realistisch zijn. We kunnen niet alle risico's uitsluiten. Zelfs de beste beveiliging is niet waterdicht. Maar door alert te zijn, kritisch te blijven en de juiste vragen te stellen, kunnen we de digitale storm trotseren en onze patiëntgegevens veilig houden.

Dus, beste toezichthouders, laat die koffie en gevulde koeken staan en duik in de digitale wereld. Want de storm komt eraan, en wie niet voorbereid is, wordt weggevaagd. En laten we eerlijk zijn, niemand zit te wachten op een datalek waarbij de medische dossiers van half Nederland op straat komen te liggen. Dat zou pas echt een hoofdpijndossier zijn! ■

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