Je bent slachtoffer of je wordt het...

Als lid van de Raad van Toezicht neem ik kennis van het recente jaarrapport van de Autoriteit Persoonsgegevens (AP) over datalekken. En wat blijkt? Cyberaanvallen met als doel persoonlijke gegevens te bemachtigen, spelen zich voor het grootste deel af in de sector zorg en welzijn! Wanneer heeft u voor het laatst over dit onderwerp als Raad van Toezicht gesproken met de Raad van Bestuur?

Vorig jaar was 23 procent van de aanvallen gericht tegen de sector zorg en welzijn. Zo werden bij cyberaanvallen op drie IT-leveranciers in de zorg de persoonsgegevens van maar liefst 900.000 patiënten geraakt en kwamen medische gegevens op straat te liggen. Van de datalekken vond 41 procent plaats in de zorgsector. Dennis Davrador, coördinator Team Datalekken bij AP geeft aan 'dat je er maar vanuit moet gaan dat je slachtoffer bent van een lek, of dat je het nog zult worden'.

De zorgsector is een sector waarin veel gevoelige informatie wordt verwerkt en opgeslagen. Het is dus van groot belang dat deze informatie goed beveiligd wordt. Helaas blijkt uit onderzoek dat de zorgsector ook nog steeds slecht beveiligd is tegen cyberaanvallen.

Ernstige gevolgen datalek

Dit is zeer zorgwekkend. De gevolgen van een datalek in de zorgsector kunnen zeer ernstig zijn voor zowel patiënten als zorginstellingen.

Voor patiënten:

- Identiteitsfraude, waarbij persoonlijke gegevens van patiënten worden gestolen en misbruikt. Uit Amerikaans onderzoek blijkt dat een compleet medisch dossier, met verzekeringsnummer, adres en BSN tussen de 50 en 500 dollar kan opbrengen. Dat is veel meer dan bijvoorbeeld een creditcardnummer, dat op de zwarte virtuele markt nog geen euro waard is. Niet vreemd, want een patiëntendossier bevat veel informatie die aantrekkelijk is voor fraude. Denk bijvoorbeeld aan verzekeringsfraude of het regelen van recepten voor bepaalde medicijnen. Dit kan leiden tot financiële schade en reputatieschade voor de betrokken patiënten.
- Medische fouten, omdat de vertrouwelijkheid van medische gegevens niet meer gewaarborgd is. Dit kan leiden tot verkeerde diagnoses en behandelingen.
- Emotionele schade, omdat patiënten zich niet meer veilig voelen bij de betreffende zorginstelling en/of zorgverlener.

Voor zorginstellingen:

- Reputatieschade, omdat het vertrouwen van patiënten en andere belanghebbenden geschaad kan worden.
- Financiële schade, bijvoorbeeld door boetes van de Autoriteit Persoonsgegevens en/of claims van patiënten.
- Juridische schade, omdat zorginstellingen wettelijk verplicht zijn om zorgvuldig om te gaan met privacygevoelige informatie van cliënten en patiënten.

Kennis van oorzaken

Het is dan ook belangrijk om kennis te hebben van de meest voorkomende oorzaken van datalekken in de zorg en hoe hiermee om te gaan.

De meest voorkomende datalekken zijn:

1. Het versturen van persoonsgegevens naar de verkeerde ontvanger (63% van de gemelde datalekken).
2. Inbreuk op de integriteit van gegevens, bijvoorbeeld als gegevens (onbedoeld) zijn aangepast of niet meer volledig zijn.
3. Hacking, malware (zoals ransomware) en phishing.
4. Diverse fouten, zoals het kwijtraken van informatiedragers en het verkeerd of onveilig versturen van (e-)mails.
5. Misbruik door insiders.

Kennis van maatregelen

Om de beveiliging van gevoelige informatie in de zorgsector te verbeteren, is er naast een breed in de organisatie gedragen inzicht in deze oorzaken ook kennis van mogelijke maatregelen essentieel.

Het is belangrijk om als Raad van Toezicht bevestigd te zien dat maatregelen de aandacht hebben, te beginnen bij de top van de organisatie. Het begint bij aandacht voor het op orde hebben en houden van de basis (denk onder meer aan het regelmatig uitvoeren van software-updates), een goede back-up strategie, het gebruik van sterke wachtwoorden en multi-factor authenticatie.

Daarnaast is het van belang dat zorginstellingen:

- Investeren in digitale expertise en cybersecurity-opleidingen voor hun medewerkers.
- Zich bewust zijn van de risico's van cyberaanvallen en datalekken en hierop anticiperen. Dit kan bijvoorbeeld door het uitvoeren van regelmatige risicoanalyses en het opstellen van een incident response plan.
- Zich houden aan de geldende wet- en regelgeving op het gebied van privacy en gegevensbescherming, zoals de Algemene Verordening Gegevensbescherming (AVG)

Kortom, de beveiliging van gevoelige informatie in de zorgsector is van groot belang om op de eerste plaats de privacy en veiligheid van patiënten te waarborgen. Immers: 'je bent slachtoffer van een datalek of je wordt het.' ■

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