VASTGOED JOURNAAL

Informatiebeveiliging zorginstellingen achter op schema

30-01-2017 21:14

Bedrijven en instellingen zijn steeds meer afhankelijker van IT. Dat vergt extra waakzaamheid: niet in control zijn levert enorme risico's op. De steeds strengere wettelijke eisen aan informatiebeveiliging werken diep in de bedrijfsvoering van uw zorgstelling door. Dat vergt niet alleen kennis van informatietechnologie, maar vraagt ook om aanpassingen op strategisch, tactisch en operationeel niveau.

Achterstand bij woningcorporaties
Uit het brancheonderzoek in november 2016 bleek dat de meeste woningcorporaties hun informatiebeveiliging bij lange na niet op orde hebben. Het overgrote deel heeft geen concreet beveiligingsbeleid en heeft niet de juiste kennis in huis van bestaande en naderende privacywetgeving. Daarmee lopen woningcorporaties niet alleen achter bij andere (semi)publieke sectoren, maar zetten ze ook de privacy van huurders op het spel.

Voortuitgang bij zorginstellingen
Zorginstellingen gaan op alle vlakken vooruit met hun informatiebeveiliging, maar de vooruitgang gaat niet snel genoeg. Raden van bestuur trekken verantwoordelijkheid voor informatiebeveiliging vaker naar zich toe, de kennis van wetgeving groeit en steeds meer instellingen hebben informatiebeveiligingsbeleid. Ook de certificering van zorginstellingen is veel vaker op orde. Verdere verbetering is echter snel nodig met het oog op de Europese Privacy verordening, die al in 2018 ingaat. Veel zorginstellingen hebben daarvoor nog een flinke inhaalslag te maken.

Bestuurders van zorginstellingen moeten informatiebeveiliging hoog op de agenda houden en blijven werken aan het privacy bewustzijn en het gedrag van medewerkers op dat gebied. Bijna de helft (49%) van alle zorginstellingen heeft nog altijd geen beleid om de privacy van cliënten en patiënten te kunnen garanderen.

Wetgeving stimuleert actie
Uit het onderzoek blijkt dat wetgeving zorginstellingen op grote schaal in beweging zet, maar ogenschijnlijk pas zodra een nieuwe wet daadwerkelijk geldt. Zo zegt maar liefst 92% van de instellingen bekend te zijn met de Meldplicht Datalekken en heeft 85% maatregelen genomen om daar ook daadwerkelijk aan te voldoen. In 2015, toen de meldplicht nog niet gold, was 38% ermee bekend en had 28% maatregelen getroffen. Met de Europese Privacy verordening (EPV), die op 25 mei 2018 ingaat, is slechts de helft van de respondenten bekend. In 2015 was dat nog 40%.

"Ondanks de goede stappen die de sector maakt op het gebied van informatiebeveiliging is tien procent een verontrustend kleine vooruitgang voor een verordening die al over anderhalf jaar ingaat," zegt Chris van den Haak, partner BDO Audit & Assurance en voorzitter van de branchegroep Zorg. "Zorginstellingen beseffen vaak nog onvoldoende dat die EPV fors strengere eisen stelt. Zo moeten organisaties inzichtelijk maken hoe ze aan de wetgeving voldoen." Ook de sancties onder de EPV zijn van totaal andere proporties. Boetes bij overtreding kunnen voor grote organisaties oplopen tot 100 miljoen euro of vijf procent van de opbrengsten.

Bewustzijn trainen cruciaal
Meer dan een kwart (27%) van de zorginstellingen heeft inmiddels al eens met een privacy-incident te maken gehad. Een groeiend aantal; in 2015 was dit nog 18%. Terwijl privacy-incidenten in maar liefst zeven van de tien gevallen het gevolg zijn van menselijke fouten, heeft maar 27% van de zorginstellingen een zogenaamd security training- en awareness-programma uitgerold om medewerkers privacy bewustzijn bij te brengen. Dat is een stijging van slechts 5% ten opzichte van 2015.

Ook bij de implementatie van beleid boeken zorgorganisaties nog opvallend weinig vooruitgang. Iets meer dan

de helft van de instellingen (51%) heeft nu een informatiebeveiligingsbeleid, daar waar dat in 2015 nog 44% was. Een nog kleiner deel (35%) zegt te zijn ingericht conform de belangrijkste richtlijn voor privacy, NEN 7510. Dat is een vooruitgang van slechts 3% ten opzichte van 2015.

Bewustzijn is de basis voor gedragsverandering. Nieuw, state of the art beveiligingsbeleid zet nauwelijks zoden aan de dijk als je de mensen in je organisatie daar niet in meeneemt. Zolang het belang van je beleid niet echt tot de medewerkers doordringt, blijft het risico van data-incidenten onverminderd groot. Goede informatiebeveiliging draait niet alleen om het formuleren van beleid, maar vooral om het implementeren ervan.

Alert blijven
De grootste vooruitgang ten aanzien van informatiebeveiliging hebben zorginstellingen gemaakt op het hoogste niveau, bij de raden van bestuur. Steeds meer instellingen (59% nu tegen 49% in 2015) zeggen dat daar de (eind)verantwoordelijkheid voor informatiebeveiliging ligt – niet bij de IT-afdeling.

Conclusie
Raden van bestuur in de zorg zijn het afgelopen jaar merkbaar alerter geworden als het om informatiebeveiliging gaat. Wat daarbij helpt is dat ICT-afdelingen tegenwoordig assertiever zijn en bestuurders confronteren met hun verantwoordelijkheid. Nu is het zaak dat ze alert blijven en doorpakken. Er is nog veel werk aan de winkel.

Lees meer in het actuele brancheonderzoek HIER.

BDO branchegroep Zorg

Chris van den Haak RA, Partner Audit & Assurance
Robert van Vianen, Partner BDO Advisory (Cyber Security)