



Informatiebeveiliging in de orthodontiepraktijk: inzichten en aanbevelingen uit recent onderzoek

In de eerste helft van 2025 voerde Techni Team een uniek onderzoek uit naar het informatiebeveiligingsniveau binnen de orthodontie. Middels een enquête beantwoordden orthodontisten vragen over dit onderwerp. Het doel: informatiebeveiliging op de agenda zetten, risico's verkleinen en bewustwording stimuleren.

Resultaten Onderzoek

Bewustzijn

De meeste respondenten erkennen het belang van informatiebeveiliging, maar hebben beperkt inzicht in de risico's van bijvoorbeeld datalekken of cyberaanvallen. Zo'n 70% besteedt ICT-diensten uit, vaak in de veronderstelling dat daarmee ook de beveiliging geregeld is — wat niet het geval is.

Kennis en vaardigheden

Basale maatregelen, zoals schermvergrendeling, worden goed toegepast. Bij complexere situaties, zoals phishing, weten medewerkers vaak niet goed wat te doen. 90% van de praktijken geeft aan dat de kennis over informatiebeveiliging onvoldoende is; slechts 40% biedt medewerkers trainingen aan.

Technische maatregelen

De meeste praktijken hebben basisvoorzieningen als firewalls en antivirussoftware. Maatregelen als encryptie van patiëntgegevens en beveiligde netwerken blijven echter achter.

Beleid en monitoring

Formeel beleid ontbreekt vaak. Slechts 33% heeft een Incident Response Plan, en 45% beheert toegangsrechten actief. Evaluaties en monitoring vinden in de meeste gevallen niet structureel plaats.

Cybercrime-ervaringen

Meer dan 75% heeft te maken gehad met phishing; ook malware, ransomware en ongeautoriseerde toegang kwamen voor. Ernstige gevolgen bleven vaak uit, maar het bewustzijn over de risico's is laag.



Verbeterpunten

Veel praktijken willen verbeteren, met name op het gebied van:

- Opstellen van beleid en protocollen.
- Regelmatige trainingen.
- Encryptie van patiëntgegevens.
- Security scans voor kwetsbaarheden.

Conclusies Onderzoek

Het onderzoek toont aan dat informatiebeveiliging wel aandacht krijgt, maar dat een structurele en professionele aanpak vaak ontbreekt. Basismaatregelen zijn doorgaans aanwezig, maar beleid, training en monitoring zijn zelden goed geborgd. Medewerkers missen vaak de kennis om moderne cyberdreigingen het hoofd te bieden. Er wordt te veel vertrouwd op ICT-dienstverleners, die niet verantwoordelijk zijn voor de volledige beveiliging. Die verantwoordelijkheid ligt namelijk bij de orthodontist. Dit vergroot de kans op kwetsbaarheden. Gerichte en structurele verbeteringen zijn daarom noodzakelijk.

Bewustzijn vergroten

Security Awareness Training verhoogt alertheid en maakt implementatie van beveiligingsmaatregelen eenvoudiger.

Beleid opstellen

Essentiële documenten:

- Incident Response Plan (IRP)
- Informatiebeveiligingsbeleid (IBB)
- Beleid privéapparatuur
- Toegangsbeheer

Technische verbeteringen

Naast basismaatregelen verdienen de volgende extra aandacht:

- Encryptie patiëntgegevens
- Beveiligde netwerken
- Sterk wachtwoordbeheer
- Kwetsbaarheidsscans
- Monitoring van digitale infrastructuur



Aandacht voor cybersecurity

Hoewel cybersecurity steeds vaker als belangrijk wordt erkend, krijgt het in de praktijk nog te weinig aandacht. Door de dagelijkse werkdruk zakt dit onderwerp vaak weg op de prioriteitenlijst.