De digitale afgrond

Vrijheid en onafhankelijkheid waren in de beginjaren de grote troeven van het world wide web. Communicatie was op onderling vertrouwen gebaseerd en daar werd weinig misbruik van gemaakt. Al gauw werden de mogelijkheden van dit netwerksysteem onderkend en nam het gebruik van internet met reuze sprongen toe. Ongeveer parallel hieraan verliep de ontwikkeling van de computer, de tablet en de mobiele telefoon. Gegevensopslag werd op grote schaal mogelijk, eenvoudig opvraagbaar en met anderen te delen. Slechts weinigen zullen hebben voorzien dat het internet binnen luttele jaren zou uitgroeien tot de ruggengraat van de hedendaagse maatschappij. Overheden, bedrijven, instellingen en burgers zijn in grote mate afhankelijk geworden van een goed functionerend internet.

De keerzijde van deze afhankelijkheid is dat men voor allerlei zaken alleen nog via een website kan communiceren, hetgeen voor ouderen een toenemend probleem is. Daarnaast is het vervelend dagelijks te worden bestookt met ongewenste advertenties, vreemde e-mails en verwijzingen naar websites met onbetrouwbare, misleidende informatie. Of dat bij een storing de pinautomaten in de winkels uitvallen. Deze ongemakken

vormen slechts het topje van de ijsberg. Op de achtergrond gebeurt er veel meer. Telkens wanneer men een browser start of een e-mail verzendt, wordt dit geregistreerd en in een database opgeslagen. De bekendste zoekmachine Google verdient miljarden met de verkoop van deze gegevens, waarmee marketeers advertenties voor bepaalde doelgroepen aan bedrijven kunnen leveren. Een socialmediaprogramma als Facebook doet hetzelfde aan de hand van berichten en foto's die de gebruikers versturen. Ook inlichtingsdiensten maken inbreuk op de privacy van burgers onder het motto "*het is in het belang van de veiligheid*". Kortom, gedrag en voorkeuren worden op allerlei manieren gevolgd, opgeslagen en kunnen voor veel doeleinden worden gebruik.

Een hacker die in pc's snuffelt, kan nog worden afgedaan als een 'nerd' die wil bewijzen dat hij slimmer is dan de beveiliging. Heel anders en veel ingrijpender wordt het als georganiseerde groepen criminele hackers op grote schaal zich in softwaresystemen nestelen, de communicatie monitoren en op zoek zijn naar fouten en lekken in de beveiliging. Daarmee krijgen ze inzage in gevoelige gegevens en kunnen dan grote materiële en immateriële schade toebrengen aan bijvoorbeeld banken, zorginstellingen, hi-tech-bedrijven en energie- en communicatieleveranciers.

De laatste tijd geven verontrustende berichten over de gevolgen van een aantal zeer ernstige cyberaanvallen reden om met het allerergste rekening te houden. Het is te hopen dat er ergens een 'plan B' achter de hand wordt gehouden om in elk geval de voor het dagelijks leven vitale systemen in stand te kunnen houden, maar het is te vrezen dat de ontwikkelingen zo snel zijn gegaan en de complexiteit zo groot is geworden dat het zelfs de experts boven het hoofd is gegroeid.

Om dichter bij huis te blijven kan men zich afvragen wat dit betekent voor een mondzorgpraktijk en kunnen er wel maatregelen genomen worden voor het geval het internet uitvalt. Ook hier zijn immers de opslag van patiëntengegevens, behandelingen, foto's, afspraken, verzekeringverificaties en de financiële administratie geïntegreerd in het praktijkautomatiseringssysteem, waarbij meerdere computers via een netwerk met elkaar zijn verbonden. Tegenwoordig worden zelfs opslag van bestanden en backups via externe servers in 'de cloud' verzorgd: handig en snel, maar daarmee ook gevoelig voor inbraak en diefstal van privacy gevoelige gegevens.

De *Wet bescherming persoonsgegevens* schrijft voor dat zorgverleners medische dossiers goed beveiligen. Zij moeten er bijvoorbeeld voor zorgen dat alleen bevoegde personen toegang hebben tot het dossier van een patiënt. Het College Bescherming Persoonsgegevens waakt over het naleven van deze wet. Wie privacybescherming van zijn patiënten serieus neemt, zal het hele proces van registratie, opslag en bewerking van de patiëntengegevens in zijn praktijk moeten analyseren en adequate maatregelen moeten nemen ter beveiliging.

In het verleden was het gebruik van een virusscanner en een firewall meestal voldoende, maar dat is heden ten dage absoluut onvoldoende. Men kan rustig stellen dat beveiligingsoplossingen die als gebruiksvriendelijk worden bestempeld in het algemeen ook nutteloos zijn. Wat wel een overweging waard is en een goed begin kan zijn, is bijvoorbeeld het praktijknetwerk waarin de patiëntenbehandelingen worden geregistreerd als gesloten systeem op te zetten zonder verbinding met internet en daarnaast aparte pc's te gebruiken voor de externe communicatie via internet. Beide systemen mogen natuurlijk geen verbinding met elkaar maken. Dat is niet eenvoudig, vergt een goed doordachte organisatie en een grote discipline, en in het begin bovenal veel tijd en moeite. Het is de moeite waard hierover na te denken, want men moet er toch niet aan denken dat zijn praktijksysteem wordt gehackt en alle gegevens met de privacy gevoelige patiëntenbestanden in onbevoegde handen terecht komen.