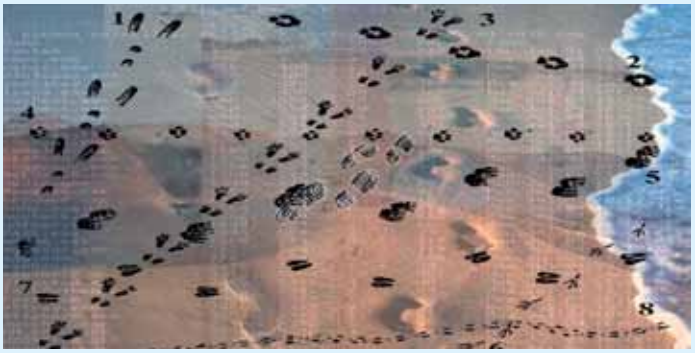
Der gläserne PC

Thomas Engel (Foto: zvg)

Wir hinterlassen immer mehr «Spuren». Nebst Kreditkarte, Cumulus und Supercard, Mobiltelefon oder Gesundheitskarte hinterlassen auch viele unserer Programme täglich digitale Daten. Was alles via WWW hin und her gesendet wird, wissen wir fast nie. Oft melden sich Programme bei jeder Benutzung bei ihrem Hersteller an und senden Registrations- und Versionenhinweise, manchmal noch vieles mehr.
Dazu kommen noch ungebetene «Gäste», welche getarnt als kleine Helfer ein besonderes Augenmerk auf Bankdaten, Passwörter und andere interessante Inhalte richten und ihren Hackern so viele weitere Daten frei Haus liefern. Solche «Gäste» sind etwa Trojaner oder Viren, welche leider immer zahlreicher, professioneller und «cleverer» werden.
Gerade all jene, die heikle Daten auf ihren Rechnern speichern oder Onlinebanking betreiben, sollten diesem Thema einen grossen Stellenwert geben. In den letzten Jahren haben immer mehr Zahnärzte ihre Praxis «digitalisiert» und verwalten Hunderte von Patientendaten auf ihren Servern und wickeln meist auch ihre Bankgeschäfte via Internet ab. Ein gefundenes Fressen für viele Internetgangster und der Graus jedes Datenschützers. Die Richtlinien sind sehr strikt und lassen kaum Spielraum für die Arbeit mit heiklen digitalen Daten. Vieles, was wir täglich machen, wäre laut Datenschutz zumindest fragwürdig, um nicht zu sagen illegal.



Was kann ich tun?

Am einfachsten und sichersten ist es, den Computer vom Internet zu trennen und ihn nie mehr anzuschliessen. Leider ist diese Variante heute kaum mehr praktikabel. Oft werden auch getrennte Systeme verwendet, ein PC für alle Internetaktivitäten, ein zweiter, vollständig getrennter Computer mit allen Patientendaten. Leider muss auch der getrennte PC ab und dann wieder ans WWW, etwa für Updates oder für Wartungsarbeiten (immer mehr Soft- und Hardware-Hersteller verlangen für ihren Support einen Internetzugang). Was kann also getan werden, um die Gefahren zu minimieren? Dazu gibt es mehrere Aspekte zu bedenken: Das Betriebssystem muss aktuell gehalten werden (Sicherheitsupdates!), ein zuverlässiges Antivirenprogramm muss vorhanden sein, der Browser muss aktuell sein und dessen Cache (Speicher) periodisch geleert werden, die Passwörter sollten regelmässig geändert werden und gewisse Anforderungen erfüllen: mindestens acht bis zehn Zeichen, Gross- und Kleinbuchstaben sowie Zahlen und Zeichen enthalten. Unter https://passwortcheck.datenschutz.ch/ kann ein entsprechendes Passwort (nicht das effektive!) geprüft werden. Ein weiteres wichtiges Element kommt zusätzlich zur Anwendung, informiert man sich etwa bei Microsoft, so erscheint folgender Text am Bildschirm: Nutzen Sie ab sofort eine Firewall. Internetverbindungen können bei mangelnder Vorsicht diverse Gefahren mit sich bringen. Durch eine Firewall können Sie das Risiko begrenzen.

Firewall

Was ist eine Firewall? Um dies zu erklären, möchte ich vereinfacht und verbildlicht den Internetverkehr kurz erläutern: Das WWW ist wie ein grosses Strassennetz, welches den verschiedenen Datenpaketen als Transportweg dient. Nun hat jeder PC mehrere Strassenanschlüsse, wo diese Datenpakete ein und aus können, etwa so, wie ein Land Strassenübergänge in ein anderes Land hat. Je nach Betriebssystem und Art des Computers hat dieser mehr als 65 000 solcher «Grenzübertritte», in der Informatik spricht man von Ports. In der Schweiz überwachen Zollbeamte die Grenzübertritte, bei einem PC überwacht niemand diese Übertritte, und die Datenpakete können ungehindert passieren. Eine Firewall ist also vereinfacht gesagt ein Zollbeamter für den PC, welcher all diese Ports überwacht. Es gibt nun verschiedene Firewall-Systeme, welche sich je nach Sicherheitsbedarf und Infrastruktur unterscheiden. Eine grobe Einteilung könnte etwa so aussehen: Hardware oder Software und extern oder intern. Um nicht zehn oder mehr Seiten zu schreiben, möchte ich nur auf die persönliche Software-Firewall etwas näher eingehen: Es gibt heute viele Anbieter solcher Firewall-Programme, von gratis bis sehr teuer, je nach Schutzbedarf und Grösse der Infrastruktur. Wer also seine Praxis mit einer Firewall sichern will, sollte sich an einen erfahrenen Informatiker wenden. Um den privaten PC sicherer zu machen, genügen meistens einfache Softwarelösungen wie etwa: Zone Alarm Pro, Kerio Firewall, Outpost Pro, Kaspersky Anti Hacker Firewall, McAfee Personal Firewall oder andere.
Erst wenn wir unsere Ports überwachen, stellen wir fest, wie viele Programme und wie oft diese Daten via Internet austauschen. Je nach Firewall können wir nun für jeden Port und für jedes Programm spezifische Durchgangsrechte festlegen, Programmen den Datenverkehr generell verweigern, nur nach Rücksprache oder immer erlauben, vertrauenswürdige Dienste festlegen, andere identifizieren und sperren.
Oft arbeiten Firewalls und Antivirenprogramme eng zusammen oder sind sogar im gleichen Programm integriert. Je nach Sicherheitsstufe der Firewall kann ein PC auch «arbeitsunfähig» gemacht werden und soweit eingeschränkt sein, dass jeder Internetverkehr unterbunden wird. Die richtige Programmwahl und Einstellung sind wie immer das A und O.

Fortsetzung folgt …