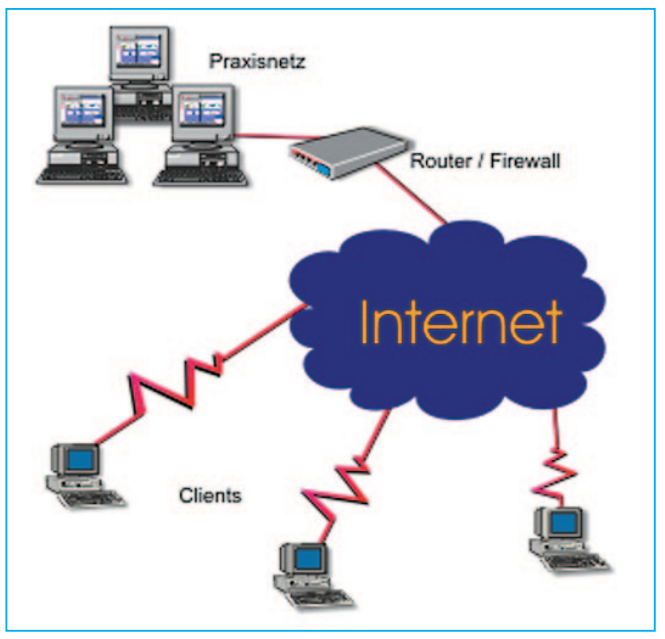
Mit Sicherheit mehr Schutz – Schutzmechanismen für das Internet (1):

Sicher ins World Wide Web

Der Countdown läuft. In 19 Monaten (Stichtag 1. Januar 2006) soll die elektronische Gesundheitskarte bundesweit eingeführt werden. Fernab möglicher Diskussionen sollten alle Zahnarztpraxen die Vorlaufzeit nutzen, um sich rechtzeitig über die technische Realisierung (Internet), aber auch über die damit möglicherweise verbundenen Risiken zu informieren. In diesem Zusammenhang stellt das Unternehmen Dampsoft, Damp, ein umfassendes Sicherheitskonzept vor, das wir in einem zweiteiligen Bericht näher erläutern werden.

Anfangs waren Computer nur mit Diskettenlaufwerken ausgestattet, wobei sich auf einem Laufwerk das Anwendungsprogramm befand und auf dem zweiten Laufwerk Daten gespeichert wurden. Durch relativ einfaches Kopieren konnten zügig Duplikate erstellt werden – somit war eine relativ hohe „Datensicherheit" gewährleistet.

Die weitere rasante Entwicklung im Hard- und Softwarebereich erweiterte ständig die technischen und inhaltlichen Anwendungsmöglichkeiten auf Benutzerseite. Nicht nur die wachsende Ausbaufähigkeit, sondern auch die Kommunikationsfähigkeit der einzelnen Computersysteme untereinander brachte den entscheidenden Durchbruch. Zunächst konnten über den lokalen Verbund einzelner Computersysteme zu Netzwerken die Mitarbeiter innerhalb einer Firma (in einem Gebäude) effizient Daten und Informationen austauschen beziehungsweise auf einzelne Daten zugreifen. Was ein einzelner Mitarbeiter erarbeitet hatte, konnte nun auch von anderen genutzt werden.



Dann kam die Möglichkeit hinzu, auch mit Computern zu kommunizieren, die sich außerhalb eines Firmen- oder Privatgebäudes befanden. Anfangs noch wenig ausgereift (BTX), kompliziert und langsam, wurden so doch die Weichen für eine globale Vernetzung gestellt – das Internet. Millionen von Computerbesitzern nutzen heute das kaum noch überschaubare Angebot des World Wide Web – neue technische Möglichkeiten scheinen keine Grenzen mehr zu kennen.

Die Euphorie über diese neuen Möglichkeiten stellte – zumindest anfangs – das Nachdenken über Sicherheits- und Schutzmaßnahmen in den Hintergrund.

Mittlerweile betrachten es manche Mitmenschen als ihre Lebensaufgabe, anderen via Internet oder E-Mail schaden zu wollen. Herrschte anfangs noch eine gewisse Fairness, indem sich Angreifer „Auge in Auge" dem Gegner stellten, ist dies mittlerweile Vergangenheit. Im Internet verbergen sie sich hinter Pseudonymen und werden nicht müde, den Gutgläubigen ihre zerstörerischen Machwerke in Form aggressiver Kleinprogramme aufzubürden. Die Motive sind mehr als fragwürdig, täglich werden wir über Medien vor neuen Internetattacken gewarnt – der Euphorie der Anfänge des Internet folgte die Angst vor Sicherheitslücken. Aus diesem Grund stehen Sicherheits- und Schutzmaßnahmen nicht nur bei vielen Unternehmen im Fokus der Computeranwendungen.

Die Gefahren im Internet sind vielfältig, fast jeder hat bereits Erfahrungen mit Computerviren oder auch so genannten Spam-Mails, die in nervenaufreibender Art und Weise den Mailboxspeicher belasten, gemacht, eventuell sogar schon mit Hackern. Sicherlich ist das Internet mit all seinen Möglichkeiten beruflich und privat interessant und – wenn man es beherrscht – auch komfortabel. Allerdings nur, solange man sich der Risiken bewusst ist und entsprechende Vorkehrungen trifft.

Technisch gesehen ist eine Internetverbindung mit einer internen Netzwerkverbindung (etwa dem Zusammenschluss mehrerer lokaler Computer in einer Zahnarztpraxis) durchaus vergleichbar. Nach der Einwahl ins Internet befindet sich der „Surfer" unter Umständen auf einem unsicheren Terrain. Selbst bei vertrauenswürdigen Seitenbetreibern besteht die Gefahr, Viren auf das eigene Computersystem übertragen zu bekommen. Eine unbeabsichtigte Laufwerksfreigabe reicht schon aus, um jedem Fremden aus dem Internet Zugriff auf persönliche Daten zu geben, ohne dass dieser über spezielle „Hackerkenntnisse" verfügen muss.

Viele Unternehmer haben sich in den vergangenen Jahren im Gegensatz zu nur wenigen Privatpersonen verstärkt um Datensicherheit bemüht. Wichtige Betriebsdaten werden (hoffentlich) regelmäßig auf geeignete Zweitmedien kopiert. Hierzu gehören Disketten, Bandlaufwerke (Streamer) oder auch CDs. Ferner können Daten auf einen zweiten Computer kopiert werden oder durch Plattenspiegelung den Sicherungseffekt verstärken. Lokale Datensicherungen sind erforderlich, um betriebswichtige Daten vor Zerstörung zu bewahren. Hierbei können beispielsweise folgende Gründe bei Datenverlusten benannt werden:

- defekte Computerbauteile,
- Festplattenausfall,
- Stromstörungen (Ausfälle und Schwankungen),
- unsachgemäßer Umgang mit Programmen oder Daten,
- Wettereinflüsse (z. B. Gewitter und Blitzeinschläge),
- Systemüberhitzung,
- Vandalismus und Diebstahl und
- fehlerhafte Programminstallationen.

Jeder PC-Verantwortliche weiß, wie wichtig die regelmäßige Datensicherung und -pflege ist. Spätestens bei einem Datenverlust wird die Ernsthaftigkeit technischer Sicherungen jedem Anwender deutlich. Nicht anders ist es um die Sicherheit in Verbindung mit dem Internet bestellt. Hierbei muss jedoch der lokale Schutz um einen weiteren Bereich erweitert werden. Dieser dient dazu, einer „beabsichtigten Zerstörung" Einhalt zu gebieten. Hier ein Überblick geprüfter und bewährter Sicherungs- und „Abwehrmaßnahmen":

Personal Firewall

Durch den Einsatz der Personal Firewall erhält der Anwender der Kontrolle und Informationen, welche Programme Verbindungen aufbauen und welche Daten übertragen bzw. ausgetauscht werden. Durch den Einsatz einer Whitelist lässt sich dieses auch bereits auf Router-Ebene unterbinden. Empfehlung: DSL-Hardware-Router mit Firewall und Whitelist

Virenscanner

Eine Virenprüfung sollte regelmäßig durchgeführt werden. Das Antivirenprogramm sollte regelmäßig aktualisiert werden, um neue Viren eliminieren zu können.

Sicherheitsupdates/ Service-Packs

Das Betriebssystem sollte auf dem aktuellen Stand gehalten werden. Microsoft etwa veröffentlichen regelmäßig Sicherheitsupdates. Für Rechner ohne Routerfirewall empfehlen sich regelmäßige Updates.

Hardwarekonstellation

Die bestehende Hardware sollte mit einem (DSL-/ISDN-)Hardware-Router, Firewall und Whitelist ausgestattet sein. Durch entsprechende Organisation kann festgelegt werden, welcher Rechner aus dem Praxisnetz eine Verbindung ins Internet aufbauen darf.

Durch die Whitelist werden sogar bereits aktive Trojaner und Spyware sowie unvorsichtige Mitarbeiter blockiert. Eine weitere VPN-Erweiterung ermöglicht eine gesicherte, hoch verschlüsselte und kostengünstige Anbindung eines externen Computers (Home-Office) an den Hauptrechner (Server) in der Praxis. Gleichsam kann der VPN-Nutzer auf jeden einzelnen Netzwerkrechner zuzugreifen.

Software

Auf den Systemen sollte ein Schutz gegen Dialer nicht fehlen. Sicherheitseinstellungen von Browser und Mailclient sollten immer auf höchster Stufe stehen, Anhänge von E-Mails dürfen sich nicht bereits bei der Ansicht öffnen. Ein Virenscanner ist Pflicht auf jedem Rechner, der E-Mails abholt oder Dateien laden darf. Sicherer wäre es, E-Mails nur von einem separaten Rechner (nicht mit dem Server verbunden) herunterzuladen.

Mitarbeiterschulung

Regelmäßige Schulungen gewährleisten die notwendige Sensibilisierung und informieren über neueste Erkenntnisse und Verhaltensweisen. Auch die Kompetenzverteilung und die nötigen Zugriffsrechte sollten festgelegt werden.

Verfahrenshinweise

Wichtige betriebsinterne Daten, etwa Kreditkartennummern, Bankverbindungen etc. sollten nur über gesicherte und verschlüsselte Verbindungen, etwa https-Verbindungen, übertragen werden. Bei vielen Browsern wird dieses durch ein eigenes Symbol (geschlossenes Schloss) gekennzeichnet.

Datensicherung

Eine Datensicherung sollte nicht nur regelmäßig durchgeführt werden, sondern auch die verwendeten Speichermedien sollten gewechselt werden.

Abnutzung und andere Faktoren können diese Medien irgendwann unbrauchbar machen und senken damit die angestrebte „Sicherheit". Auch sollten die verwendeten Speichermedien zwingend an einem anderen Ort gelagert werden. Hierzu bieten sich Schließfächer oder geeignete private Räume beziehungsweise Verwahrungsstellen an.

Bernd Materzok, Tony Domin, Hamburg ■

(wird fortgesetzt)