

PC-Tipp – Computernetze in der Allgemeinpraxis

Heinz Bhend

Wiederholt wurde ich in Gesprächen mit Netzwerkproblemen in der Arztpraxis konfrontiert. Im folgenden möchte ich meine eigenen Erfahrungen weitergeben – in der Hoffnung, dass der eine oder andere Kollege davon profitieren kann. Ein weiteres Ziel ist auch, die Abhängigkeit – respektive das Gefühl des Ausgeliefertseins – von Hard- und Softwarelieferanten etwas zu reduzieren oder deren Angebote zu hinterfragen.

Einleitung

Der Trend nach Mehrplatzsystemen hat auch die Praxen längst erreicht. Obwohl die Mehrheit der Kollegen noch ein Einplatzsystem haben, kommt schnell einmal der Wunsch auf, auf die Daten zugreifen zu können. Prompt ist nun die MPA gerade daran, einen Bericht zu schreiben.

Die Vernetzung von zwei oder mehreren Computern ist in der Tat keine Hexerei mehr und kann mit etwas Geduld von jedem normalen User bewerkstelligt werden.

Wireless oder RJ-45-Leitung

Obwohl die Möglichkeiten des drahtlosen Datenaustausches erstaunlich sind und auch die Geschwindigkeit zugenommen hat, gilt grundsätzlich immer noch, wenn irgendwie möglich, eine feste Verkabelung vorzunehmen. Diese ist stabiler, viel schneller und weniger anfällig u.a. auch auf Sicherheitslücken.

Bei vielen Praxen stellt sich das Problem, dass für eine Vernetzung zusätzliche Leitungen gelegt werden müssten. Die Computernetzkabel lassen sich dabei in das gleiche Installationsrohr einlegen wie zum Beispiel die Telefonleitung.

Als elegante Lösung hat sich bei mir das Umstellen des Telefons auf ein Funksystem bewährt. Somit stehen die Telephonleitungen respektive deren Installationsrohre für die Computervernetzung zur Verfügung.

Zu jedem Arbeitsplatz muss ein achtadriges Twisted-Pair-Kabel verlegt werden mit RJ-45-Anschluss. Die Zeiten von Koax-Kabeln mit Abschlusswiderständen sind glücklicherweise definitiv vorbei. Durch diese Ver-

kabelung kann ein Datentransfer von bis zu 100 MB pro Sekunde erreicht werden. Diese Geschwindigkeit ist bei weitem genügend für den Datenaustausch in einer Arztpraxis.

Grundsätzlich können zwei einzelne Rechner durch ein «gekreuzt gepoltes» Kabel direkt verbunden werden. Eleganter und ausbaufähiger ist die Verbindung via Switch, eine kleine Box (Preis ca. 60 Franken), welche mehrere RJ-45-Ports hat und den Datenaustausch respektive Datenverkehr zwischen verschiedenen Rechnern überwacht und ermöglicht. Die alten Hubs gibt es praktisch nicht mehr, die Switches sind nicht teurer, ermöglichen aber die volle Bandbreite für alle angeschlossenen PC. Durch ein sogenanntes Uplink können mehrere Switches miteinander verbunden werden – und das System ist beinahe beliebig erweiterbar.

Die neueste Variante, Netzwerk via Stromnetz (Powerline) ist sehr einfach zu installieren und hat einen Datendurchsatz von 14 Mbps. Eine Powerline-Bridge (ca. 170 Franken) stellt die Verbindung zum Modem/Internet oder LAN her. Mittels eines speziellen (USB-)Adapters kann jeder Rechner im gleichen Stromkreis ans Internet/Intranet angeschlossen werden. – Sie kommt allenfalls in Frage, wenn Aufwendungen für eine Verkabelung unverhältnismässig wären.

Server oder Peer-to-peer

Grundsätzlich kann auch ein kleines Peer-to-peer-Netzwerk problemlos funktionieren, wenn die Architektur geregelt ist. Bei mehr als drei Rechnern empfiehlt es sich aber, ein serverbasiertes System einzuführen. «Serverbasiert» heisst (für mich!) lediglich, dass ein Rechner als Server (Diener, Zulieferer) dient und gewissermassen die Daten zur Verfügung stellt, sonst aber möglichst nicht als Arbeitsstation gebraucht wird.

Nach meinen Erfahrungen reicht ein Server, welcher als Betriebssystem «Windows 2000 Professional» installiert hat. Obwohl von den Softwarefirmen immer wieder gewünscht und empfohlen oder sogar befohlen, ist eine Windows-2000-Serversoftware nicht unbedingt nötig, zu dem sehr teuer und bereitet oft Probleme mit gewissen Geräten. Ferner fallen zusätzliche Kosten an für spezielle (servertaugliche) Software an (Bsp. Virensoftware). Persönlich hatte ich über ein Jahr ein Server-Betriebssystem installiert, dann aber wieder auf «Windows 2000 Pro-

Korrespondenz:
Dr. med. Heinz Bhend
Alte Zofingerstrasse 62
CH-4663 Aarburg
h.bhend@gmx.ch

fessional» gewechselt und damit Kosten für z.B. Viren-Software gespart.

Für die Bedürfnisse einer Praxis oder eines KMU ist ein Server, welcher «Windows 2000 Professional» installiert hat, bei weitem genügend. Ausnahmen (Bsp. VPN) bestätigen hier die Regel.

Jedenfalls gilt es zu berücksichtigen, dass der Servercomputer, wie schon erwähnt, möglichst nur als Zulieferstelle eingesetzt und nicht als Arbeitsstation benutzt wird. Dies ist meiner Erfahrung nach wichtiger, als die Wahl des Betriebssystems.

Internetanbindung

In diversen Offerten habe ich astronomische Zahlen gelesen über notwendige Hardware und Software, um eine sichere Anbindung ans Internet zu ermöglichen. In einer Arztpraxis brauchen wir jedoch kaum eine höhere Sicherheitsstufe als eine durchschnittliche Regionalbank!

Damit mehrere PC gleichzeitig ans Internet angeschlossen werden können, muss ein sogenannter Router im Netz eingeschaltet sein. Dieser wird via RJ-45-Kabel direkt am Switch angeschlossen.

Die neuen Modelle haben meist eine integrierte Firewall. Als kostengünstige Variante bietet sich zum Beispiel der Zyxel-652-Router (ADSL) an, welcher für ISDN und analoge Netze zum Preis von etwa 700 Franken zu haben ist.

In der Grundeinstellung sind sämtliche Ports geschlossen, so dass eine Attacke von aussen gar nicht möglich ist. Dieses Gerät bietet sogar die Möglichkeit einer VPN-Session («virtual private network»). Dies ist allenfalls für Kollegen interessant, welche von zu Hause aus (via Internet) auf ihre Praxisdaten zugreifen möchten. Mit spezieller Software ist dies von jedem PC mit Internetanschluss möglich – und falls auf der Gegenseite (Privathaus) ebenfalls ein Zyxel-652-Router installiert ist, braucht es nicht einmal eine spezielle Software. Allerdings ist die Konfiguration des Routers für eine VPN-Sitzung nichts für Anfänger.

Wenn ein Fachhändler dieses Gerät verkauft, sollte er auch die entsprechende Konfiguration vornehmen können.

Die meisten Internetanbieter beschränken die Anzahl der PC mit gleichzeitigem Internetzugriff nicht mehr. Cablecom hat eine

eigene Politik via Highspeed-TV-Internetanschluss. Dort sind drei IP schon zugewiesen, das heisst, es könnten theoretisch nur drei PC gleichzeitig eine Online-Verbindung haben. Wenn aber beim gelieferten Modem ein Switch dahintergeschaltet wird, können wiederum beliebig viele Rechner ans Netz angeschlossen werden.

Zu beachten ist, dass in allen Netzwerken mit Internetanbindung die zur Verfügung stehende Bandbreite durch die gleichzeitig angeschlossenen (surfenden) PC geteilt wird.

Funktionsprinzip einer Firewall

Die Verbindung zweier PC funktioniert über sogenannte Protokolle. Um überhaupt ins Internet gehen zu können, wird meist das sogenannte «http» («hyper text transfer»-Protokoll) verwendet. Theoretisch könnte ein Angriff erfolgen, wenn ich im Internet aktiv bin und via «http» Daten austausche. Die Firewall prüft nun, ob von einem internen Rechner eine Anfrage stattgefunden hat, wenn von aussen ein Datenpaket gesendet wird. Ist dies nicht der Fall, kann das Datenpaket nicht hinein. Die Firewall hat somit nichts anderes zu tun als ständig zu überwachen, dass «Antworten» nur auf entsprechende Anfragen eingehen. Alle weiteren Eingänge von aussen werden als Attacken angesehen und entsprechend abgewehrt.

Für ADSL-Kunden empfiehlt sich eine hardwaremässige Firewall, sei es in einem separatem Gerät oder kombiniert mit einem Router. Eine Software-Firewall ist nur zu empfehlen, wenn ein separater Rechner im Netz für den Internetzugang zuständig ist und alle Anfragen via diesen PC laufen. Man muss sich immer vorstellen, dass man eine allfällige Attacke möglichst an der Grenze und nicht im Zentrum eines Systems abwehren sollte.

Datensicherheit und Datensicherung

Die Sicherheit gegen aussen (Internet, Mailverkehr) kann mit entsprechenden Vorkehrungen (Firewall) bewerkstelligt werden. Dies betrifft aber nur die «Verteidigung der eigenen Stellung» und hat nichts mit dem Austausch von Daten zu tun.

Die grösste Sicherheitslücke ist aber wiederum intern, indem patientenrelevante Daten (zum Beispiel Worddateien von Über-

weisungsbriefen) meist ohne Passwortschutz von jedem Rechner im System eingesehen werden können.

Hier ist das Personal zu sensibilisieren und auch auf die entsprechenden Vorkehrungen und Strategien aufmerksam zu machen. Ein noch weit grösseres Problem ist jedoch die Datensicherheit beim Austausch mit Spitälern bzw. mit Kollegen.

Um hier eine genügende Sicherheit zu gewährleisten, braucht es eine sogenannte Verschlüsselungssoftware oder einen Tunnel. Allerdings nützt es wenig, wenn die Mails von Rechner A bis zum Beispiel zum HIN-Server verschlüsselt via ASAS-Tunnel und von dort aus unverschlüsselt zum Rechner B gelangen. Das HIN-System funktioniert nur, wenn beide daran angeschlossen sind und die Mails respektive Daten so austauschen. Unabhängig von einem speziellen System können Mails zum Beispiel mit PGP («pretty good privacy») ausgetauscht werden. Absender und Empfänger tauschen sich jeweils die entsprechenden Schlüssel aus. Die Mails werden mit diesem Schlüssel mit einer hohen Sicherheit verschlüsselt und können nur mit dem Gegenschlüssel wieder geöffnet werden. Dies hat den Vorteil, dass der Datenaustausch mit einem x-beliebigen Provider und Server möglich ist und die Schlüsselvergabe nur einmalig erfolgen muss. Weder Tunnel noch PGP-Schlüssel verhindern aber Virusattacken. Die Viren werden einfach auch verschlüsselt und wieder entschlüsselt und können so ihr Unwesen treiben.

Datensicherheit

Der Verlust von Daten erfolgt meist infolge Virusattacken, Softwareproblemen oder Manipulationsfehlern. Hardwareseitige Crashes sind möglich, aber immer seltener geworden. Ein Backupsystem ist unabdingbar, nützt allerdings nichts, wenn es nicht regelmässig durchgeführt wird. Solche Arbeiten sind entsprechend zu automatisieren oder zu institutionalisieren.

Nach jahrelangem Kampf mit Bändern und Tapes habe ich diese definitiv verbannt und arbeite nur noch mit CD-Brennern. Die «einmal-beschreibbaren» CD dazu kosten inzwischen unter 50 Rp. Ich beschreibe jeweils zwei pro Tag, was für die Datensicherung einen täglichen Aufwand von unter einem Franken ausmacht (nebst der Hardware =

CD-Brenner, welcher inzwischen schon für 60 Franken zu kaufen ist).

Raid

Von Hardware- und Softwareanbietern wird oft ein sogenanntes Raid empfohlen. Es ist ein System, welches die Harddisk spiegelt und somit garantiert, dass bei einem Hardware-, sprich Harddiskproblem, weitergearbeitet werden kann. Obwohl ich die Möglichkeit hätte, habe ich dies bisher nicht so konfiguriert. Glücklicherweise sind Hardware-, d.h. Harddiskcrashes, sehr selten geworden in den letzten Jahren. Für mich weit wichtiger ist es, einen zusätzlichen (billigen) Rechner zu haben, welcher im Bedarfsfall einfach hingestellt, angeschlossen und hochgefahren werden kann. Somit kann ich ohne grossen Aufwand weiterarbeiten. Eine weitere Möglichkeit bietet das früher einmal vorgestellte Drive-Image (siehe www.sgam.ch/tools). Dabei wird von einer Harddisk oder Partition eine identische Kopie in einer einzigen Datei abgespeichert und kann bei Bedarf wieder zurückkopiert werden.

Periodisch muss die Datensicherung überprüft werden, das heisst das Backup muss auf einen Rechner zurückgespielt werden. Nur so kann man kontrollieren, ob wirklich alle Daten wieder vorhanden sind.

Dies ist zum Beispiel möglich, in dem man das Rückspielen nicht mehr an den ursprünglichen Speicherort macht und dann die Daten mit dem ursprünglichen Standort vergleicht. Selbstverständlich übernimmt jede Softwarefirma gerne diese Prüfung gegen entsprechendes Entgelt.

Hardwareanforderungen

Für den Server-PC lohnt es sich allenfalls, eine etwas exklusivere Variante zu wählen. Dies sagt allerdings nichts aus über deren Lebensdauer, höchstens über den Preis. Auch hier kann mit einem entsprechenden Abonnement ein 24-Stunden-Vorortservice vereinbart werden. Wenn man aber zum Beispiel mit elektronischer KG arbeitet, sind 24 Stunden völlig unrealistisch. Somit bleibt nur die Autonomie und das Selfmanagement.

Ich hoffe mit diesen Zeilen diese etwas erhöht zu haben.