EDV-SICHERHEIT IN DER ARZTPRAXIS

Noch immer sind viele Ordinationsinhaber Einzelkämpfer, was im besonderen für die Installation von EDV-Anlagen gilt. Warum aber müssen (leidvolle) Erfahrungen immer selbst gemacht werden? Aus den Erfahrungen anderer lernen: Dr. Florian Mittermayer hat sich das zu Herzen genommen und seine Erlebnisse niedergeschrieben. Er berichtet von den ersten Anfängen der EDV-Anlage bis hin zum sicherheitstechnisch ausgereiften Ordinations-EDV-System. Der Weg dahin war nicht ohne Stolpersteine.


Dr. Peter Bitzan


Dr. Florian Mittermayer

Lesen Sie danach, was zwei EDV-Experten zu diesem Thema zu sagen haben.

Dr. Peter Bitzan und ich eröffneten am 15. Juli 2001 unsere Gruppenpraxis für Orthopädie im 10. Wiener Gemeindebezirk. In unserer Praxis arbeiten insgesamt 13 Personen, davon zwei Ärzte, eine diplomierte Physiotherapeutin, eine diplomierte Ergotherapeutin, eine Masseurin und sieben weitere Mitarbeiter. Unsere Praxis ist auf Rheumaorthopädie und Sportmedizin spezialisiert.

Um den Anforderungen einer modernen Praxis zu entsprechen, haben wir uns ein EDV-System angeschafft, um damit Arzt- und Behandlungstermine, Patientenstammdaten inklusive Diagnose und Behandlungen, Abrechnungen mit den Krankenkassen und unseren Internetauftritt abzuwickeln. Im Internet werden unsere Dienstleistungen, die Praxiszeiten, der Anfahrtsplan sowie die Kontakte (Telefon, Fax, E-Mail) dargestellt.

Wir schafften uns acht PCs, die in einem Netzwerk miteinander verbunden sind, sechs Drucker und die dazu erforderlichen Programme an. Die Installation von Hard- und Software sowie die laufende Wartung wurden von einem auf Ärzte spezialisierten EDV-Unternehmen durchgeführt.

Alle Mitarbeiter der Praxis sind berechtigt, alle Anwendungen zu benutzen. Aufgrund unserer Arbeitsprozesse ist es erforderlich, dass jeder Mitarbeiter auf jedem der acht PCs jederzeit arbeiten und auch auf alle Daten und Programme zugreifen kann. Mit dieser Lösung können wir sehr effizient unsere Praxis führen.

Bezüglich der EDV-Sicherheit haben wir uns für eine Firewall und das tägliche Abspeichern aller Daten auf ein Band, das außerhalb der Praxis gelagert wird, entschieden und fühlten uns mit diesen Maßnahmen sicher.

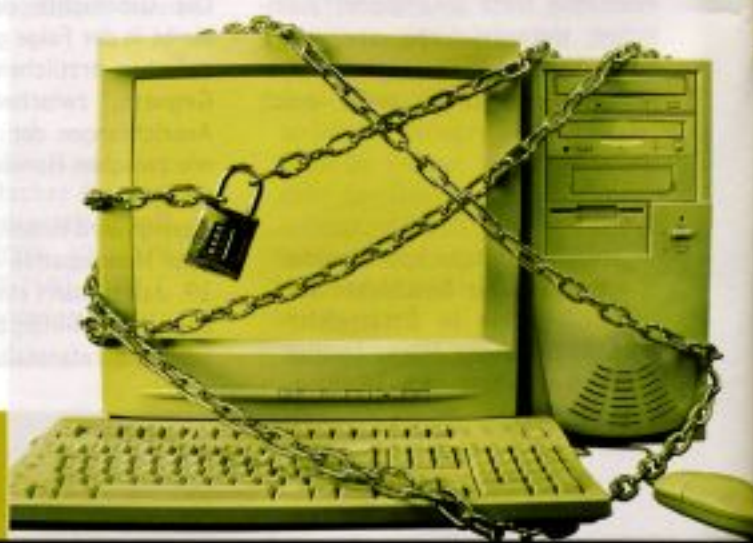
Einbruch in der Praxis

Im August 2001 wurde in unsere Praxis eingebrochen. Alle PCs wurden gestohlen. Die Einbrecher stiegen über den Balkon ein und hatten über die Balkontüre offensichtlich ein leichtes Spiel, in die Praxisräume einzudringen.

Am nächsten Arbeitstag und in den darauf folgenden vier Wochen mussten wir ohne EDV-Anlage und vor allem ohne bereits vorgemerkte Arzt- und Behandlungstermine, ohne Patientenstammdaten inklusive Diagnose und Behandlungen und ohne der Möglichkeit der elektronischen Abrechnung mit den Krankenkassen auskommen. Komplett ohne Patientendaten mussten wir zusätzliche Rückfragen stellen, handschriftliche Notizen machen und behelfsmäßig ablegen. Trotz bester Improvisation und etlicher Mehrstunden aller Praxismitarbeiter mussten Patienten viel länger warten als üblich. Die Abrechnung mit den Krankenkassen stellte einen weiteren zusätzlichen Aufwand dar.

Vier Wochen danach hatten wir wieder eine neue EDV-Anlage. Wir mussten alle Patientendaten händisch nachtragen. Die Versicherung zahlte den Ersatz der Hardware. Den zeitlichen Mehraufwand durch den EDV-Ausfall (längere Ordinationszeiten, händisches Nachführen der Daten, Zeitaufwand für Versicherung, EDV-Firma, et cetera) haben wir für das gesamte Team auf etwa 250 Stunden geschätzt, was bei einem Stundenlohn von 50 Euro einer Schadenssumme von 12.500 Euro entspricht. Dieser Betrag wird nicht von den Versicherungen bezahlt.

Monate später hatten wir abermals Pech. Über unsere Internetanwendung kam ein Virus in unser EDV-System. Unsere EDV-Anlage war diesmal für sieben Tage nicht in Betrieb und ein nahezu identes Szenario wie vor Monaten spielte sich wieder ab: keine Patientendaten, keine Patien-



tentermine, ... Die Schadenbehebung kostete uns diesmal ungefähr 8000 Euro.

EDV-Check gegen offene Sicherheitslücken

Im April 2003 ließen wir einen umfassenden EDV-Sicherheitscheck von Moore Stephens Austria, einem unabhängigen Prüfungs- und Beratungsunternehmen, durchführen. Dieser umfassende Check, welcher speziell für Arztpraxen und Kleinkliniken entwickelt wurde, durchleuchtete unser EDV-System in den Bereichen:

- Hard- & Software
- Datenschutz & Verschwiegenheit
- Netzwerk & Internet
- Berechtigungssysteme & Passwörter
- Firewall & Virenschutz
- Backup & Recovery
- Organisation & Personal
- Serviceverträge

Der Bericht beinhaltete eine umfassende Information für EDV-Spezialisten, welche wir an unsere EDV-Betreuungsfirma weitergeleitet haben, sowie eine Kurzversion für Ärzte und Pflegepersonal in einer einfachen verständlichen Form. Mit Hilfe dieser Prüfung konnten einige wichtige Schwachstellen in unserem Sicherheitsnetz aufgedeckt werden. Andererseits erhielten wir aber auch eine Bestätigung für jene Bereiche, die bereits gut abgesichert waren. Gleichzeitig wurden wir und unsere Mitarbeiter über die verschiedenen Risiken im Umgang mit der EDV aufgeklärt und erhielten viele wertvolle Vorschläge zur Verbesserung unserer Sicherheit.

Im Anschluss an das Audit haben wir eine Reihe von Maßnahmen ergriffen, um noch offene Sicherheitslücken zu schließen. Neben einigen technischen Maßnahmen, wie beispielsweise Software-Updates und Konfigurationseinstellungen, betraf dies vor allem den richtigen Umgang mit Benutzerberechtigungen und Passwörtern sowie eine grundlegende Sensibilisierung des Personals für diese Problematik.

Damit können wir uns wieder sicher fühlen und uns beruhigt auf unsere EDV verlassen. Um mit den kommenden Entwicklungen Schritt zu halten, planen wir, im nächste Jahr erneut eine Überprüfung unserer Anlagen durchführen zu lassen.

SICH DER RISIKEN BEWUSST WERDEN

Das Thema Sicherheit und Kontrolle von Informationssystemen ist angesichts der heute anzutreffenden umfassenden und vernetzten Anwendungen zu einer Aufgabe ersten Ranges für praktisch alle professionellen Anwender geworden. Auch der medizinische Bereich, wo vorwiegend Personen tätig sind, die über kein oder nur geringes Fachwissen im Bereich der Informationstechnologie verfügen, bildet hier keine Ausnahme. Eher das Gegenteil ist der Fall, da einerseits besondere Ansprüche an die Verschwiegenheit des Berufsstandes gestellt werden, andererseits Handlungen aufgrund falscher, weil manipulierter, Daten mitunter schwerwiegende Folgen für Leben und Gesundheit der Patienten haben können. Eine entsprechend umsichtige und regelmäßige Vorsorge kann dieses Risiko jedoch auf ein vertretbares Mindestmaß reduzieren und eine allfällige Haftung verhindern.

Mag. Gerhard Donner Mag. Karl Fischer

Mag. Gerhard Donner und **Mag. Karl Fischer** sind Experten für IT-Sicherheit. Für doktorinwien berichten sie über EDV-Sicherheitsaudits für Ärztinnen und Ärzte, Therapeuten und Praxisgemeinschaften.

Sicherheit von Informationssystemen - ist das ein Thema für Mediziner?

Informationstechnologie (IT) ist in fast alle Gesellschaftsbereiche vorgedrungen. Auch aus der Medizin sind Computer heute nicht mehr wegzudenken. Im Praxis- und Klinikbetrieb erleichtern sie zahlreiche Routineaufgaben, wie zum Beispiel Terminverwaltung und Patientenaufnahme, Patientenkartei und Dokumentation, Rezeptierung und Abrechnung. Die fortschreitende Vernetzung erlaubt darüber hinaus einen raschen und unkomplizierten Informationsaustausch sowohl innerhalb als auch zwischen den Institutionen.

Der Einsatz von Informations- und Kommunikationstechnologien birgt allerdings neben den zahlreichen positiven Effekten leider auch eine Reihe von Risiken in sich, derer sich jeder Anwender bewusst sein sollte.

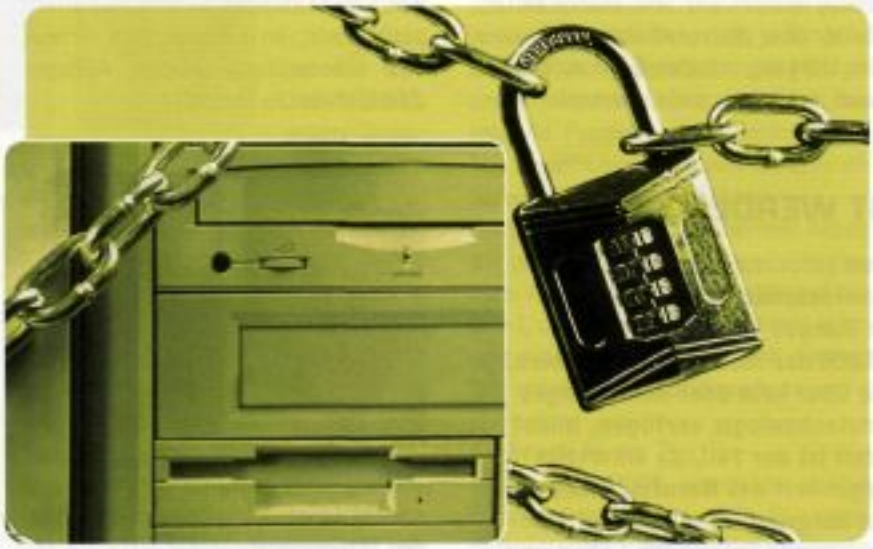
Welches Gefahrenpotenzial birgt der EDV-Einsatz in der Arztpraxis?

Zunächst muss man die möglichen Gefährdungen betrachten. Die wichtigsten Quellen sind:

- extern über Internet, Modem oder Datenträger von Personen mit unterschiedlichsten Interessen
- intern von Mitarbeitern, Patienten, Besuchern beziehungsweise Begleitpersonen, Lieferanten,

- Dienstleistern und sonstigen Personen, die Zugang zu Systemen haben beziehungsweise sich verschaffen können
- fehlerhafte HardVSoftwarekomponenten
- Umwelteinflüsse, Elementarereignisse, Einbruch/Diebstahl

Kommt es wirklich häufig vor, dass ein Patient oder Mitarbeiter vertrauliche Daten ausspioniert oder anderen Schaden anrichtet?
Hinsichtlich der von Personen ausgehenden Gefahren ist eine differenzierte Betrachtung angebracht. Zunächst kann man zwischen redlichen und unredlichen Personen unterscheiden. Auch redliche Personen können durch Unwissenheit oder Unachtsamkeit Handlungen vornehmen, dulden oder unterlassen, die dazu geeignet sind, Vertraulichkeit und/oder Integrität der Daten und Systeme zu gefährden. Unredliche Personen handeln hingegen mit dem Vorsatz, Systeme zu kompromittieren und so erlangte Informationen unter Umständen weiterzuverwenden, wobei die Motivation dafür ganz unterschiedlicher Natur sein kann. Während manche Menschen darin eine Art Freizeitbeschäftigung oder Wettkampf sehen, haben andere, beispielsweise aus wirtschaftlichen oder politischen Gründen, Interesse an der Krankengeschichte einer bestimmten Person. Leider zeigen die Statistiken, dass Fälle von Computerkriminalität oder eben auch nur die Fälle von wahllosem Hacken sehr hoch sind.



Welche Folgen sind damit verbunden?
Typische Folgen beim Eintreten solcher Vorkommnisse sind unter anderem:

- Offenlegung von vertraulichen Daten
- Löschung von Daten
- Veränderung von Daten
- Vornahme von Handlungen unter Vortäuschung einer falschen Identität
- Ausfall von Ressourcen
- Benutzung von Ressourcen für weitere Angriffe auf Dritte

Gerade im medizinischen Bereich können derartige Ereignisse aber schwere Konsequenzen nach sich ziehen. Sind bestimmte Daten oder ganze Systeme nicht mehr verfügbar, kann es zu empfindlichen Betriebsstörungen oder unvollständiger beziehungsweise verspäteter Leistungsverrechnung kommen. Ebenso sind aber auch eine Verletzung der Verschwiegenheitspflicht oder gar eine falsche oder gefälschte Rezeptierung/Therapie infolge manipulierter Informationssysteme denkbar.

Wie sieht die rechtliche Seite aus? Kann es zu einer Haftung des Arztes kommen?
Aus den genannten Bedrohungen können unmittelbare Vermögensschäden (zum Beispiel beschädigte Komponenten, Betriebsunterbrechung, Aufwand für das Wiederherstellen von Daten und Systemen), Vertrauensschäden (guter Ruf, Geschäftsentgang) und schließlich auch Folgeschäden für Dritte (zum Beispiel aufgrund falscher Medikation oder Verletzung der Verschwiegenheitspflicht) entstehen. Zur Minimierung dieser Risiken und der damit verbundenen möglichen berufs-, zivil- und strafrechtlichen Konsequenzen verlangt das Prinzip der allgemeinen und der besonderen Sorgfaltspflicht des Berufsstandes die Durchführung von dem aktuellen Stand der Technik entsprechenden und dem wirtschaftlichen und organisatorischen Rahmen angemessenen Präventivmaßnahmen zur Absicherung der verwendeten Informationssysteme und Datenbestände.

Unterbleiben derartige Sicherungs- und Kontrollmaßnahmen, muss damit gerechnet werden, dass die Rechtsprechung den Tatbestand der Fahrlässigkeit erkennt und dem Arzt oder der Klinik, die vielleicht selbst Opfer eines Angriffs waren, zumindest ein Mitverschulden anlastet.

Welche Gegenmaßnahmen und Abwehrstrategien sollten getroffen werden?
Prinzipiell sind alle medizinischen Einrichtungen, die Informationstechnik einsetzen, betroffen, von der

Arztpraxis über Diagnose- und Therapiezentren bis hin zu den großen Kliniken. Unterschiedlich ist jeweils nur die Komplexität der Organisation und der verwendeten Systeme, womit natürlich auch der Umfang der notwendigen Sicherungs- und Kontrollmaßnahmen variieren wird. Sinnvoll ist daher ein den individuellen Bedürfnissen und Gegebenheiten angepasstes Programm.

Um Risiken und Schutzbedarf exakt feststellen zu können, empfiehlt sich zu Beginn die Durchführung eines IT-Audits. Ein solches Audit identifiziert nicht nur vorhandene Schwachstellen, sondern liefert auch konkrete, an die jeweilige Situation angepasste, Maßnahmenvorschläge zur Mängelbehebung und zur Optimierung von Sicherheit, Ordnungsmäßigkeit und Kontrolle.

Sinnvoll ist es, nicht den eigenen IT-Betreuer, der die Hard- und Softwarekomponenten installiert und verwaltet, mit der Durchführung dieses Audits zu beauftragen, sondern einen unabhängigen und neutralen Prüfer, der frei von wirtschaftlicher Abhängigkeit, Betriebsblindheit und Befangenheit vorgehen kann. Weltweit anerkannte und geschützte Zertifizierungen wie der CISA (Certified Information Systems Auditor), die eine umfangreiche Ausbildung und praktische Erfahrung voraussetzen, helfen bei der Auswahl eines geeigneten Partners.

Auf der Grundlage des Audits kann im nächsten Schritt die Erstellung eines Sicherheitskonzepts erfolgen. Ein wesentliches Kriterium für das Sicherheitskonzept ist die ganzheitliche Betrachtungsweise. Vielfach werden IT-Risiken als ausschließlich technische Angelegenheit angesehen. Damit werden allerdings wesentliche Bereiche außer Acht gelassen. Für eine wirksame Absicherung sind organisatorische und personelle Aspekte mindestens genauso wichtig wie die technischen. Beispiele dafür sind etwa das Design von Berechtigungssystemen oder Systemen zur Datensicherung. Auch der wirtschaftliche Blickwinkel sollte dabei nicht zu kurz kommen, da sich die zu ergreifenden Maßnahmen auch in einem angemessenen finanziellen Rahmen bewegen sollen.

Die Implementierung des Sicherheitskonzepts umfasst (in der Reihenfolge) eine Kombination von Ausbildungs- und bewusstseinsbildenden Maßnahmen, die Installation und Konfiguration technischer Sicherheitseinrichtungen, wie zum Beispiel Firewalls, Virenscanner und ähnliches, sowie die Umsetzung verschiedener organisatorischer Regelungen. Wichtig ist dabei, alle beteiligten Personen, insbesondere jene, die keine IT-Spezialisten sind, umfassend aufzuklären und mit dem Umgang der Sicherheits- und Kontrolleinrichtungen vertraut zu machen.

Bedeutsam ist auch die Tatsache, dass die Absicherung der Informationssysteme kein einmaliges Ereignis bleiben darf. Angesichts der rasanten technologischen Entwicklung und dem daraus resultierenden Auftreten laufend neuer Gefährdungen ist vielmehr ein kontinuierlicher Entwicklungsprozess erforderlich. So ist eine regelmäßige Überprüfung in Abständen von ein bis zwei Jahren mit einer entsprechenden Anpassung der Sicherungs- und Kontrollmaßnahmen unbedingt zu empfehlen. Zusätzlich müssen verschiedene Softwarekomponenten laufend aktualisiert werden, um einen wirkungsvollen Schutz zu gewährleisten.

Diese Aufgabe kann durchaus in Form eines Servicevertrags an einen externen IT-Betreuer beziehungsweise ein darauf spezialisiertes Unternehmen ausgelagert werden. Wichtig sind auch hier Zuverlässigkeit, Qualität und Integrität des Dienstleisters.

Mag. Gerhard Donner, CISA, ist geschäftsführender Gesellschafter der Moore Stephens Austria Consulting GmbH und Experte für Sicherheit, Ordnungsmäßigkeit und Kontrolle von Informationssystemen und Anwendungen der Informationstechnik.
Mag. Karl Fischer ist Partner der Moore Stephens Austria Consulting GmbH und Experte für Customer Relationship Management und Projektmanager für Sicherheit, Ordnungsmäßigkeit und Kontrolle von Informationssystemen und Anwendung der Informationstechnik.