men, d.h., Daten sind auf Betriebssystemebene unter Umgehung des Anwendungsprogrammes einsehbar.

Hinzu kommt ein teilweise nachlässiger Umgang mit Paßwörtern. Es werden häufig keine ausreichenden Vorkehrungen dahingehend getroffen, daß nur befugte Personen Kenntnis der Paßwörter erhalten, oft sind diese auch leicht zu erraten. Dies schafft die Möglichkeit des Zugriffs Unbefugter auf sensible personenbezogene Daten.

Diese Problemliste ließe sich unschwer verlängern, ohne daß sie dadurch vollständig würde. Allerdings gibt es einige Schwerpunkte, die sich als typisch und wichtig kennzeichnen lassen. Oft reichen relativ einfache und unkomplizierte Maßnahmen zur Lösung, wenn man die Probleme, ihre Ursachen und die Beseitigungsmöglichkeiten kennt. Viele Maßnahmen haben zudem den Vorteil, gleich mehrere Sicherheitsaufgaben zu lösen.

Folge 2 unserer Reihe „Medizin und Datenverarbeitung“ (Rheinisches Ärzteblatt Dezember) beschäftigt sich unter anderem mit den Fragen: Wie kann man Datenverlusten vorbeugen? Wie lassen sich Konflikte mit dem Datenschutz verhindern?

Anschrift für die Verfasser:
Nordrheinische Akademie für ärztliche
Fort- und Weiterbildung, Herrn Dr. med. Peter Lösche
Tersteegenstr. 29, 40474 Düsseldorf

Erste Hilfe bei Virenalarm

Mehrere tausend Computerviren treiben ihr Unwesen, hiervon verursachen jedoch nur einige hundert den größten Teil aller Infektionen. Grundsätzlich haben alle Viren das Ziel, sich zunächst unbemerkt auf viele Dateien über Festplatten und Disketten zu vermehren und bei Eintritt eines bestimmten Ereignisses (etwa ein bestimmtes Datum) Schäden anzurichten. Diese bestehen bspw. in Änderungen von Dateiinhalten, Löschen ganzer Verzeichnisse, Formatierung der Festplatte usw.

Die Viren sind selbst kleine Programme, die andere Programmdateien durch Einfügen ihrer Programmbefehle in deren Befehlsfolge infizieren. Um sich ausbreiten zu können, muß zunächst zwingend ein Datenaustausch zwischen infiziertem und noch nicht infiziertem Computer bzw. Datenträger stattfinden.

Eine günstige Gelegenheit zur epidemischen Vermehrung finden die Viren bei Infektion der zentralen Nervenbahnen des Computers. Aus diesem Grund dominieren rein zahlenmäßig Virenarten, die das Betriebssystem befallen. Diese Programme werden ja bei jeder Inbetriebnahme des Computers gestartet und haben u.a. die Aufgabe, andere Programme in den Hauptspeicher zu laden. Dies ist eine ideale Gelegenheit, zu überprüfen, ob diese Programme schon infiziert sind. Die ersten Datenbereiche auf einer Festplatte oder Diskette enthalten die zum Laden des Betriebssystems notwendigen Befehle. Sie werden demzufolge beim Starten des Computers zuerst gelesen und als Bootsektoren bezeichnet. Viren, die sich in diesen Sektoren festsetzen, werden analog als Bootsektorviren bezeichnet. Um sich zu schützen, sollte man seinen Computer also tunlichst nicht von Diskette starten und beim Starten keine Disketten im Laufwerk haben.

Werden Programme per Diskette weitergegeben und wird diese Diskette auf ihrem weiteren Weg einmal infiziert, kann sich ein Virus auf alle nachfolgenden Computer ausbreiten. Nach dem ersten Aufspielen sollte die Diskette also vor Weitergabe nochmals per Virenscanner überprüft und gegen weitere Schreibzugriffe durch Gebrauch des Schiebers in der oberen rechten Ecke der Diskette geschützt werden, so daß in der linken und rechten oberen Ecke ein Fenster entsteht.

Eine weitere Gelegenheit der Ausbreitung besteht für Viren über Datenfernübertragungsnetze. Wenn in einen Computer ein infiziertes Programm aus einer Mailbox geladen wird, werden alle übrigen an das lokale Netzwerk angeschlossenen Computer ebenfalls betroffen. Überspielte Programme sollten also immer mit einem Virensuchprogramm geprüft werden. im Idealfall nutzt man einen vom lokalen Netz abgekoppelten Rechner für Datenfernzugriffe.

Um eine effiziente Vorsorge zu betreiben, sollte man für den Fall der Fälle Virensuchprogramme bereithalten. Diese erkennen Viren durch Vergleich der dem einzelnen Virus typischen Codesequenz mit einer im Suchprogramm gespeicherten Signaturenliste. Verschiedene Schutzprogramme können einzelne Parasiten auch entfernen bzw. Programme bereinigen. Da einzelne Viren sich nicht nur an andere Programme anhängen, sondern auch die ursprünglichen Programmbefehle überschreiben, ist gerade hierbei der Erfolg nicht immer garantiert. Sicherungskopien aller Original-Programmdisketten sollten vorhanden sein, Programminstallationen nur von diesen Kopien angefertigt werden. Eine Alternative hierzu ist die Installation von einer CD-ROM-Version, diese Datenträger können nicht beschrieben werden.

Da veränderte Datenbestände sich nur schwer rekonstruieren lassen, helfen aktuelle Sicherungskopien der wichtigsten Daten, Panikgefühle zu vermeiden.

Den geläufigen Erkennungsverfahren versuchen moderne Virenarten durch ständige Änderung ihrer internen Struktur oder durch Verschlüsselungstechniken zu entgehen. Diese sogenannten polymorphen Plagegeister sind ebenso schwierig zu identifizieren wie Tarnkappenviren, die auf Überprüfung von Dateilängen oder Prüfsummenverfahren basierende Erkennungsmethoden austricksen können.

Als neueste Variante sind Makroviren hinzugekommen, die die in modernen Textverarbeitungs- , Kalkulations-, und Datenbankprogrammen integrierte Kommandosprache mißbrauchen. Damit werden erstmals nicht nur Programme, sondern auch Dokumente verseucht, und dies unabhängig vom Betriebssystem. Gerade das Internet ist für diese Virenart ein idealer Betätigungsort, das Laden einer einzigen Textdatei auf den eigenen PC kann genügen. Hinzu kommt, daß virulente Makros von vielen Schutzprogrammen noch immer kaum erkannt werden und schwer zu beseitigen sind.

Da ständig neue Viren auftauchen, müssen Virenschutzprogramme laufend aktualisiert werden. Diese sog. Updates sind bei vielen Produkten für einen gewissen Zeitraum kostenlos. Der Einsatz von mindestens zwei Antivirenprogrammen gibt allerdings größere Sicherheit.

Um einer Infektion vorzubeugen, empfiehlt sich zudem, die von einigen Programmen angebotene Option des speicherresidenten Schutzes zu nutzen. Diese Programme werden als erste in den Hauptspeicher geladen. Sie überprüfen danach quasi als digitale Türwächter vor jeder Ausführung andere Programmdateien auf Virenbefall. Zudem achten sie auf virentypische Aktionen wie z.B. Versuche einer Formatierung während der normalen Arbeit.

Dr. med. Peter Lösche