Sicherheit bei der Einführung von Standardsoftware

Was verbirgt sich eigentlich hinter dem Begriff Sicherheit? Ganz allgemein kann man damit das Recht auf die Vertraulichkeit und Unversehrtheit seiner Daten bezeichnen.

Was ist Sicherheit?

Informationen in DV-Anlagen können geändert, zerstört oder gestohlen werden. Dies kann explizit durch Menschen aber auch implizit und unerkannt durch Software geschehen. Dabei gibt es erwünschte Modifikationen wie das Neuberechnen eines Excel-Arbeitsblatts oder den Eintrag eines Kunden in eine Datenbank, aber auch unerwünschte Aktionen, etwa durch einen Software-Fehler (Bug). Grundsätzlich müssen drei primären Sicherheitsaspekte berücksichtigt werden:

- Datenzugänglichkeit (Datenverfügbarkeit)
  Alle Arbeitsplätze im Netz müssen ständig Zugang zu ihren Daten haben. Zur Aufrechterhaltung der Zugänglichkeit ist es notwendig, Hardware, Arbeitsstationen, Software, Datenkommunikationsleitungen, Stromversorgung, Gebäude u. a. zu sichern.
- Datenqualität
  Datenqualität (Datenintegrität) bezeichnet den Umstand, daß die gespeicherten Daten die Realität exakt widerspiegeln sollen. Es dürfen daher weder Unfälle noch Eingriffe von außen Unstimmigkeiten zwischen den gespeicherten Daten und der Realität hervorrufen.
- Datenvertraulichkeit
  Die Daten des Systems können nur von den Personen gelesen und benutzt werden, die dazu berechtigt sind. Die Wahrung des Datengeheimnisses ist für die Konkurrenzfähigkeit des Unternehmens von Bedeutung, aber auch in Bezug auf externe Umstände, wie z. B. die Gesetzgebung.

Mangelnde Datenzugänglichkeit, Datenqualität (-integrität) und mangelndes Datengeheimnis können schwerwiegende Folgen haben:

- Geldverlust
- Imageverlust
- Verletzung gesetzlicher Vorschriften
- Gestiegene Betriebskosten
- Verlorene Geschäftsmöglichkeiten
- Nachteile gegenüber der Konkurrenz
- Irreführende Bilanzen

Wo einer oder mehrere der drei Sicherheitsaspekte verletzt werden, müssen nicht zwangsläufig von Sabotage herrühren. Es kann sich beispielsweise auch um unverschuldete Unfälle, wie Benutzerfehler, Brand- oder Wasserschaden handeln. Die Konsequenzen können jedoch für das betroffene Unternehmen genauso schädlich sein. Daraus ergibt sich als wichtigstes Fazit:
Als erste Maßnahme zu einem guten Sicherheitskonzept gehört ein vernünftiges und regelmäßiges Backup. Nach der Erstinstallation eines PCs oder einer Workstation fertigt man ein Backup der Stunde Null an. Das ist für Notfälle der letzte Rettungsanker,denn was nützt einem ein zwei Wochen altes Backup, wenn das System bereits vor acht Monaten mit einem Virus verseucht wurde. Danach sollte man regelmäßige Backups durchführen, siehe später.

Sicherheit ist Chefsache

Alle Unternehmen, die EDV benutzen, sollten ein entsprechend hohes Sicherheitsniveau haben, um Gefahren oder geringer Qualität der Datenverarbeitung begegnen zu können. Ein entsprechendes Sicherheitsniveau ist erreicht, wenn sich die geschäftlichen Konsequenzen der Unsicherheitsfaktoren mit den Kosten für das entsprechende Sicherheitsniveau die Waage halten. Das sicherste System ist unbrauchbar, und das benutzerfreundlichste System besitzt keine Sicherheit.
Die Sicherheitsarbeit sollte ihren Ausgangspunkt in einer gründlichen Analyse der gegenwärtigen Situation nehmen. Die Analyse umfaßt eine Prüfung der IT-Ressourcen als auch die Abhängigkeit von diesen, sowie die Umstände, die mit einer gewissen Wahrscheinlichkeit diese Ressourcen bedrohen können. Das Bild der gegenwärtigen Situation muß die Grundlage für die Formulierung der Sicherheitspolitik bilden. Das Ziel dieser Arbeit ist ein Handlungsplan mit Richtlinien zur Einrichtung des gewünschten Sicherheitsniveaus über einen gegebenen Zeitraum und zur Festlegung grundlegender, laufender Sicherheitsmaßnahmen sowie Termine für die erneute Einschätzung der Sicherheit. Begonnen wird mit einer Analyse, die u. a. eine Beschreibung der LAN-Ressourcen und eine Beschreibung der Gefahren und Schwächen des lokalen Netzes enthält. Die Beschreibungen münden in einen Sicherheitsbericht, der die Grundlage der Führung für die Steuerungsprozesse ist:

- Gewichtung von Ressourcen
- Design und Implementierung der Sicherheitspolitik
- Bewertung und Feinabstimmung

Schuld an den meisten Problemen sind ungeschickte oder unkundige Anwender. Anwenderfehler können unterschiedliche Folgen haben, z. B. unerwünschtes Löschen von Daten, Überschreiben von Daten und Verschwinden von Daten (verborgen und/oder vergessen). Ungeschickte Anwender zerstören oder löschen Dateien, mit denen Sie selbst arbeiten, und wenn beispielsweise der Fileserver keinen genügend restriktive Zugriffsschutz bietet, kann der Betreffende durch ein Mißgeschick gemeinsame Programme oder Daten löschen. Weitere Beispiele menschlicher Fehler sind Fehlbedienung und verkehrte Installation von Programmen aber auch Fehlbedienung bei der Hardware (z. B. Verwechseln von ISDN- und Netzwerkbuchse, die beide gleiche Bauart besitzen). Kritisch ist es auch, wenn nur wenige Mitarbeiter des Unternehmens bestimmte Informationen haben. Bei Abwesenheit eines solchen "Informationsträgers" können unter Umständen ganze Bereiche der Firma lahmgelegt werden.. Andere Gefahren stelltdas unrechtmäßige Kopieren von Daten und Software oder die Infektion mit sogenannten Computer-Viren dar. Das Eindringen in den Rechner via Modem- oder Internet-Anschluß ist ebenfalls eine steigende Bedrohung offener Systeme. Hinzu kommen Diebstahl von Hardware, Zerstörung von EDV-Material und Sachbeschädigung aller Art. Schließlich gibt es bewußten kriminelle Handlungen, wie beispielsweise Unterschlagung, Spionage und Sabotage.

Viren und Würmer

Derzeit gibt es alleine im PC-Sektor mehrere tausend verschiedene Viren, und diese Zahl erhöht sich konstant. Virus-Designer entwickeln laufend neue Techniken und zugleich zirkulieren Entwicklungswerkzeuge, die es Personen ohne Programmierkenntnisse ermöglicht, Mutationen (strains) zu erzeugen. Viren beschränken sich dabei nicht mehr auf die "Infektion" ausführbarer Programme, sondern befallen alle Dateien, die in irgeneiner Weise ausführbare Teile enthalten, also auch Word-Dokumente, Excel-Tabellen, E-Mails, Webseiten, usw. Es ist deshalb notwendig, die Virengefahr ernst zu nehmen. Sieht man dies im Zusammenhang mit der Möglichkeit, eigene Datenträger mitzubringen und sie im LAN des Unternehmens zu verwenden, ist dies ein weiterer Grund zur Aufmerksamkeit. Es ist deshalb wichtig, eine

Antivirus-Politik zu formulieren. Die Antivirus-Politik des LAN hat primär das Ziel, eine Vireninfektion zu verhindern, Viren vor dem Ausbruch nachzuweisen sowie Bekämpfung und Wiederherstellung zu erleichtern, wenn das Unglück schon geschehen ist. Sie muß aber vor allem die Benutzer für die Gefahr sensibilisieren, so daß sie beispielsweise nicht auf jedes E-Mail-Attachment klicken (Man isst ja auch nicht jeden Pilz, den man im Wald findet.).

"Computervirus" wird oft als gemeinsame Bezeichnung für alle feindlichen und schädlichen Programmtypen verwendet. Prinzipiell gesehen sind Viren nur einer von mehreren schädlichen Programmtypen. Im folgenden werden kurz vier Kategorien feindlicher Programme skizziert.

- Viren
  Ein Virus ist ein Codefragment, das sich an ein Programm oder einen speziellen Bereich der Festplatte oder des RAM hängt. Es vermehrt sich, indem es sich in weitere Programmdateien einklinkt, und richtet oft Schaden an. Viren können im RAM, in Partitiontabellen, Bootsektoren oder Programmen operieren. Sie verbreiten sich von PC zu PC mit den Programmen, an die sie sich hängen, oder mit dem Bootsektor auf Disketten.
  Stealth-Viren verbergen sich im Arbeitsspeicher, im Master-Boot-Record oder im Bootsektor. Sie benutzen unter anderem falsche Meldungen an Antivirusprogramme, um einem Viruscheck zu entgehen.
  Polymorphe Viren sind imstande, sich zu verändern. Dieser Typ gehört zu der neuen Generation, die sich verschlüsselt und ihre Signatur verändert. Es ist klar, daß diese Eigenschaft sie sehr schwer nachweisbar und aufspürbar macht. Virusdesigner benutzen verschiedene "mutation engines" zum Generieren solcher Viren.
- Trojanische Pferde
  Ein trojanisches Pferd ist im Gegensatz zum Virus ein einzelnes Programm. Sie treten oft als unschuldige kleine Dienstprogramme auf, die leider ein Stück Kode enthalten, das Schäden anrichtet, wenn es ausgeführt wird.Ein besonderer Typ trojanisches Pferd wird entwickelt und installiert, um Benutzer-IDs und Paßwörter aufzuschnappen. Das Programm ahmt den Login-Bildschirm des betreffenden Systems nach und speichert die eingegebenen Benutzer-IDs und Paßwörter in einer Datei, deren Inhalt später gelesen und zum Versuch eines unrechtmäßigen Zugangs mißbraucht werden kann.
- Logische Bomben
  Eine logische Bombe ist ein destruktiver Kode, der in ein Programm in der ursprünglichen Entwicklungs- und Programmierungsphase eingebaut wird. Eine Quelle logischer Bomben sind oftmals unzufriedene oder frustrierte Entwickler in der EDV-Abteilung des Unternehmens. Sie fügen ihrem Programm eine Funktion hinzu, die eine bestimmte Operation zu einem gegebenen Zeitpunkt ausführt, oder wenn eine bestimmte Voraussetzung erfüllt ist. Beispielsweise kann der Programmierer eines Verwaltungsprogrammes eine Funktion einbauen, die in Abständen kontrolliert, ob der Betreffende immer noch auf der Gehaltsliste des Unternehmens steht. Ist dies nicht mehr der Fall, wird nach einer gewissen Wartezeit die logische Bombe gezündet, die z. B. alle Transaktionen des Zeitraums löscht.
- Würmer (Worms)
  Ein Wurm ist ein einzelnstehendes Programm mit einer schädlichen Funktion und der Fähigkeit sich zu vermehren - oft sogar über das Netz von Rechner zu Rechner. Außer sich zu vermehren, sich durch das System zu schlängeln und Systemressourcen wie RAM, Festplatte oder CPU in Beschlag zu nehmen, können Würmer andere schädliche Wirkungen haben. Das Programm unterscheidet sich dadurch von einem Virus, daß es ein einzelnstehendes Programm ist, im Gegensatz zu einem Codefragment, das andere Programme infiziert.

Ein zweckmäßiger Aufbau des lokalen Netzes ist eine Voraussetzung für einen hohen Grad an Sicherheit vor Virenangriffen. Eine konsequente Trennung von Daten- und ausführbaren Dateien hat große Bedeutung für die Sicherung vor Vireninfektionen und -ausbrüchen. Nur der Systemverwalter darf Schreibberechtigungen für Datenbereiche mit ausführbaren Dateien haben. Der Systemverwalter ist damit verantwortlich, die Software zu kontrollieren, ehe sie im LAN installiert wird. Datenbereiche mit Dateien, zu denen viele Benutzer Schreibberechtigungen haben, müssen von ausführbaren Dateien freigehalten werden. Das hilft zwar nicht gegen Makro-Viren in Datendateien, hält jedoch viele Viren fern. Der zweite Vorteil einer solchen Trennung ist die schnelle Wiederherstellung eines Client- oder Serverrechners. Da sich die Programmbereiche nicht ändern (sollten), kann ein solcher Bereich schnell durch Einspielen eines Backups oder, falls der älteste Backup auch schon verseucht sein sollte, durch Neuinstallation restauriert werden.
Alle Netzlaufwerke werden regelmäßig auf Viren gescannt (mindestens wöchentlich). Lokale Festplatten werden täglich gescannt. Die Benutzer sind verpflichtet, Disketten zu scannen, ehe sie in ihren PC eingelesen werden. Alle Benutzer werden in den Gebrauch von Antivirusprogrammen eingeführt, und es wird festgelegt, wann virusähnliche Probleme dem Systemverwalter überlassen werden. Es gilt der Grundsatz "lieber ein Virusverdacht zu viel als einer zu wenig", damit die Benutzer ermutigt werden, bei einem Versacht sofirt Alarm zu schlagen. Der Rechner des einzelnen Benutzers stellt einen Zugangsweg zum LAN dar und ist auch selbst verletzbar. Ein wichtiger Teil der vorbeugenden Arbeit ist die Benutzerdisziplin, die das Risiko von Vireninfektionen verringert. Programme unbekannter Herkunft und unbekannter Wirkung dürfen nicht ohne ein Virusscannen ausgeführt werden. Unbekannte Disketten müssen mit einem Antivirusprogramm kontrolliert werden, ehe sie ausgeführt oder auf Festplatte kopiert werden. Checken Sie regelmäßig Festplatten mit aktualisierten Antivirusprogrammen, und verwenden Sie ein residentes Antivirusprogramm, das den Rechner beim Start checkt.

Trotz ausgedehnter Sicherheitsmaßnahmen können Arbeitsstationen oder das lokale Netz von Viren angegriffen werden. In dem Maß wie LAN-Benutzer und -Verantwortliche sicherheitsbewußter werden, werden Viren fortschrittlicher. Identifizieren Sie Ursprung und Art der Infektion. Wenn der Ursprung nicht unmittelbar festgestellt werden kann, ist es ausreichend, die Art der Infektion festzustellen. Suchen Sie den Schaden im Netz und identifizieren sie die betroffenen Rechner. Isolieren Sie eventuelle Schäden und soweit möglich die Quelle der Infektion. Entfernen Sie sofort infizierte Rechner vom Netz. Nehmen Sie kein Logoff vor, sondern ziehen Sie das Netzwerkkabel ab. Ein reguläres Logoff kann zur weiteren Verbreitung beitragen. Nur 100% desinfizierte PCs werden an das Netz angeschlossen. Wenn die Infektion nicht isoliert werden kann, ist es notwendig, das ganze Netz herunterzufahren, und die Festplatten in den Servern und Arbeitsstationen mit zwei oder mehr verschiedenen Virusscannern zu scannen. Nachdem die feindlichen Programme entfernt worden sind, wird ein Restore der verlorenen oder beschädigten Daten und auch der Boot- und Master-Boot-Sektoren vorgenommen.

Sicherheitskriterien für Software

Einführung

Nachdem einige Sicherheitsprobleme betrachtet wurden, die von außerhalb kommen, nun ein kurzer Blick nach innen. Hier kommt die Bedrohung von Mitarbeitern, eingeschleppten Viren oder durch die Anwendungssoftware selbst. Die nachfolgende Aufstellung der Bedrohungen von innen macht deutlich, daß die größten Risiken z.B. durch die Nutzung nicht freigegebener oder genehmigter Software oftmals als Gefahrenpotential überhaupt nicht wahrgenommen wird. Umso wichtiger wird es sein, sich genau diesen Risiken deutlich intensiver zu widmen (Reihenfolge entspricht der Häufigkeit).

1. Nutzung nicht genehmigter Software
2. mitgebrachte und eingeschleppte Viren
3. Einsatz des IT-Equipment für unerwünschte Aktivitäten
4. Missbrauch von Netzzugangsrechten
5. Installation nicht genehmigter Hardware/Peripherie
6. Diebstahl oder Sabotage des IT-Equipment
7. Diebstahl oder Sabotage von Informationen

Es erscheint vielleicht etwas überraschend, daß die größten unternehmensinternen Bedrohungen durch die Installationen und Nutzung nicht genehmigter und großteils unerwünschter Software wie z.B. Spielen dargestellt werden. Solche Programme sind meistens weder auf Virenverseuchung noch auf die Kompatibilität oder Auswirkungen auf die gesamte IT Struktur getestet und untersucht. Sehr interessant erscheint in diesem Zusammenhang eine Online Umfrage des Anbieters von „Moorhuhn“. Auszugsweise ergab diese Befragung folgende Erkenntnisse:
„Für die Moorhuhnjagd im Büro riskieren mehr als 40 Prozent der Spiele-Fans ihren Job oder nehmen arbeitsrechtliche Konsequenzen in Kauf... 14 Prozent halten sich an das Spielverbot im Dienst. Bei weiteren 14 Prozent wird das gelegentliche Moorhuhnjagen im Büro toleriert.“
Aus dieser Umfrage wird eines klar: Das Ziel der Angriffe wird in zunehmendem Maße der einzelne Desktop Computer. Er ist im Vergleich zu den Serverdiensten meist weit weniger geschützt. Wir der Desktop Computer von einem Angreifer erst einmal unter Kontrolle gebracht, kann man ihn relativ einfach dazu benutzen, die vermeintlich sicheren Serverdienste von „innen“ anzugreifen.
Einen weiteren Punkt möchte ich hier noch streifen: Die Software-Piraterie. Laut Erhebungen der Buisness Software Alliance (BSA) belief sich der Schaden durch Software-Piraterie auf ca. 450 Millionen Euro. Abgesehen davon, daß solche Zahlen mit Vorsicht zu interpretieren sind (oftmals werden "Raubkopien" nur kurz ausprobiert, würde jemand das Produkt, das er illegal kopiert hat, jemals kaufen, usw.) stellt die professionelle Software-Piraterie Gefahren für den Anwender dar. An einer Raubkopie kann man kein Eigentum erwerben. Wer eine Fälschung kauft, muß gegebenenfalls nochmals in die Tasche greifen. Die Kopie kann zudem Fehler aufweisen. Wird im Unternehmen eine Lizenz mehrfach installiert, kann es jrechtliche Probleme geben, sofern diese Tatsache aufgedeckt wird. Wer wirklich sparen will oder muß, der sollte auf ältere Versionen der Software zurückgreifen, die von vielen Herstellern preiswerter angeboten wird. Eine weitere Möglichkeit ist es, ein Update zu überspringen, wenn man die neuen Features nicht wirklich braucht. Oder man verwendet Freeware oder Shareware (s. u.).

Softwarefehler /Bugs)

"There are no significant bugs in our released software that any significant number of users want fixed." Bill Gates
Das ist ein wahrhaft kühne Behauptung! Jede Standardsoftware hat mehr oder weniger viele Fehlfunktionen bereits "ab Werk". Bug Reports bei Hersteller führen meist zu der lapidaren Aussage, man möge doch auf die folgende Version "upgraden", die diesen Bug nicht mehr besitze (aber dafür andere). Es ist gut zu überlegen, ob man mit dem möglicherweie gefundenen "Workaround" besser leben kann als mit unbekannten Fehlern der Folgeversion. Manche Bugs sind nur lästig, wie z. B. der Neuumbruch eines Word-Dokuments,w enn man den Drucker wechselt, andere machen die Software nahezu unbenutzbar. Ein Beispiel aus der Raumfahrt: Am 4. Juni 1996 startete die ESA eine Ariane 5 mit vier Satelliten an Bord. 40 Sekunden nach dem Start explodierte die Rakete. Verlust ca. 500 Millionen Dollar für Rakete und Satelliten. Ursache für den Absturz: Der Bordcomputer stürzte 36.7 Sek. nach dem Start ab

als er versuchte, den Wert der horizont. Geschwindigkeit von 64-Bit-Gleitkommadarstellung in 16-Bit-Ganzzahldarstellung umzuwandeln. Die entsprechende Zahl war größer als 2^{15}=32768 und erzeugte einen Arithmetik-Überlauf. Das Lenksystem brach zusammen und die Selbstzerstörung wurde ausgelöst, da die Triebwerke abzubrechen drohten. Die Probleme liegen zwischen diesen beiden Extremen.
In offenbar kaum einem Unternehmen laufen die Computersysteme störungsfrei. Vor allem die Software erzeugt einer Untersuchung der LOT Consulting in Karlsruhe zufolge, die auf einer Befragung von 922 Firmen mit einem Umsatz von mehr als 20 Millionen Mark beruht, sehr häufig Schwierigkeiten. Sie sind gezwungen, mehr als ein Drittel ihrer IT-Budgets (35,9 Prozent) für die Beseitigung von Programmfehlern auszugeben. Daraus errechnet sich für die Mittelstands- und Großunternehmen ein Schaden von jährlich 28 Milliarden Mark. Um ein Fünffaches höher schlagen zusätzlich die Produktivitätsverluste aufgrund der Computerausfälle zu Buche. Nach den Angaben der befragten Firmen belaufen sie sich auf durchschnittlich 2,6 Prozent des Umsatzes und erreichen für die deutsche Wirtschaft ein Volumen von 137 Milliarden Mark pro Jahr. Damit summiert sich der Gesamtschaden durch Softwarefehler in den Unternehmen auf 165 Milliarden Mark jährlich. Oftmals ist es aber kein Bug, sondern ein Bedienfehler. Die Gründe hierfür können mannigfach sein, etwa mangelnde Kenntnis des Programms, schlechte Dokumentation oder auch unterschiedliche Denkweisen bei Anwender und Programmierer.

"Sichere" Programmierung

Man könnte es auch "defensive" Programmierung nennen. Es geht darum, schon bei der Konzeption (und später natürlich auch bei der Realisierung) der Software an mögliche Fehlerquellen außerhalb der eigenen Anwendung zu denken. Die häufigste Form des defensiven Programmierens ist die Nachfrage bei kritischen Operationen (z. B. "Wollen Sie die Datei wirklich löschen?"). Leider übertreiben einige Betriebssysteme die Fragerei so stark, daß der Anwender auf "O.K." klickt, ohne der Fragetext zu lesen. Oft wird auch die Frage so unklar gestellt, daß der Anwender sich eigentlich gar nicht klar über die Auswirkung seiner Aktionen sein kann. Man könnte dies testen, indem man die o.g. Frage durch "Datei *nicht* löschen?" ersetzt und die Benutzer-Reaktionen protokolliert. Software sollte also vor der unternehmensweiten Einführung auf Usability untersucht werden, beispielsweise durch Einsatz einer Muster-Installation.
Zur defensiven Programmierung gehört auch, daß die Auswirkungen anderer Fehler auf die Daten möglichst gering sind. Wenn beispielsweisse ein Buchhaltungsprogramm durch einen Stromausfall (oder den Absturz des Betriebssystems) unsanft beendet wird, sollte nur der aktuelle Buchungssatz betroffen sein und nicht die Integrität der gesamten Buchhaltungsdatenbank verletzt werden. Dazu auch ein einfaches Beispiel: Sie suchen eine Software zur Verwaltung von Adressen. Das erste Programm öffnet beim Start die Adreßdatenbank und liest sie in den Speicher, damit sie schneller zu verarbeiten sind. Sie können nun die Daten bearbeiten (ändern, ergänzen, etc.). Wenn Sie das Programm beenden, werden die Änderungen auf die Platte geschrieben und die Datenbank geschlossen. Das zweite Programm liest auch zu Beginn alle Daten in den Speicher und schließt dann die Datenbank. Bei jeder Änderung oder Neueingaben wird die Datenbank kurz geöffnet, der entsprechende Datensatz weggeschrieben und die Datenbank gleich wieder geschlossen. Dieses Programm ist natürlich wesentlich resistenter gegen Fehlereinwirkung von außen. Kein Mensch würde wissentlich die erste Variante kaufen – aber dazu muß man vor der Kaufentscheidung testen, was z. B. beim plötzlichen Ausschalten des Rechners mit den Daten passiert. Nebenbei: Haben Sie jemanls darüber nachgedacht, was passiert, wenn der Rechner abstürzt, während Sie mit Ihrer Textverarbeitung zu Gange sind?
Was macht eigentlich ein Programm mit offensichtlichen Fehleingaben? Akzeptiert es "zymryk" als Zahl und wandelt es diese Zeichenketten in den Zahlenwert

462239100256873636 um? Oder erhalten Sie die Fehlermeldung "Hier sind nur Zahlen erlaubt"? Akzeptiert es den 35.07.2002 als Datum? Sehr schlecht! Akzeptiert es den 29.02.2000 als Datum? Auch schlecht! Ein Programm sollte so geschrieben sein, daß es Benutzereingaben grndsätzlich mißtraut. Aber auch hier kann wieder defensiv gearbeitet werden. Ein weiterer Aspekt aus meiner eigenen Vergangenheit möge hier als Beispiel dienen. Als Computer noch nicht so geläufig waren, bekam ich die Beschwerde, daß eines meiner Programme Zahleneingaben nicht akzeptiert – und zwar immer dann, wenn eine Null in der Zahl enthalten war. Die Sekretärin, die das Programm bediente, war von ihrer alten Schreibmaschine gewöhnt den Großbuchstaben "O" anstelle der "0" einzugeben. Das Programm wurde dahingehend angepaßt, nun auch das "O" als "0" zu akzeptieren.

Trügerische Sicherheit

Hier handelt es sich nicht um Bugs, sondern konzeptionelle Fehler in Standardsoftware. So gibt es Betriebssysteme, die Sicherheit nur vorgaukeln. Auch dazu zwei Beispiele. Bei Windows XP scheint die Verschlüsselung der Paßwörter auf den ersten Blick ausreichend sicher zu sein, bis man feststellt, daß die zur Verfügung stehende Anzahl von Schlüsselbits gar nicht vollständig verwendet wird.
Zweitens: Die Verschlüsselung von E-Mail in Firmennetzen läuft ins Leere, wenn sie in einer Umgebung mit Microsofts Exchange/Outlook 9x/200x stattfindet. Mit Krypto-Plug-ins verschlüsselte Dateianhänge werden zwischen dem Client und dem Server unverschlüsselt übertragen, selbst wenn im Plug-in die Verschlüsselung aktiviert ist. Das Problem besteht darin, dass ein Datei-Anhang über das RPC-Protokoll (Remote Procedure Call) sofort an den Server übertragen wird, sobald der Nutzer eine vertrauliche E-Mail erstellt und eine Datei angehängt hat - unabhängig davon, ob das Plug-In für die Verschlüsselung aktiviert ist. Auch die Option innerhalb des E-Mail-Programms Outlook "Save Drafts" hat darauf keinen Einfluß. Stellt der Nutzer die E-Mail fertig und drückt den Sende-Knopf, aktiviert Outlook zwar wunschgemäß das Plug-in und die Mail samt Anhang wird verschlüsselt. Doch zuvor wurde der unverschlüsselte Anhang bereits übermittelt. Die Aktivierung der RPC-Standardverschlüsselung wäre der einzige Schutz, doch diese beträgt bei manchen Versionen nur 40 Bit - diese gelten jedoch als unsicher. Abhilfe wird bisher nur durch Fremdprodukte geboten.
Das Fatale an den beiden Beispielen ist, daß nur wenige Benutzer überhaupt Kenntnis von diesem Problem haben und die meisten sich in trügerischer Sicherheit wiegen. Dabei beschränkt sich dieser Problemkreis nicht auf die beiden willkürlich gewählten Programme. Insbesondere der Paßwortschutz ist bei vielen Programmen äußerst schwach, auch bei Word, Excel oder Winzip läßt sich der Schutz recht schnell knacken. Inzwischen gibt es sogar passende Tools per Download aus dem Internet.

Verborgene Informationen

Nahezu jede Standardsoftware verwendt zum Speicherhn der Dateinein proprietäres Format. Neben dem eigentlichen Inhalt werden auch zusätzliche Informationen gespeichert, darunter Formatierungsinformationen, Autorenangaben, Erstellungs- und Änderungsdatum und viele nützliche Dinge mehr. Darunter können aber auch Geheimnisse sein, deren Weitergabe dem Autor unter Umständen gar nicht recht ist.
So kann es passieren, daß beim Einbinden einer Spalte von einer Excel-Tabelle in eine Powerpoint-Präsentation die gesamte Tabelle (verborgen) mit gespeichert wird und auch wieder herausgelöst werden kann. Dann hat der Kunde plötzlich nicht nur den Verkaufspreis, sondern auch den Einkaufspreis in der Hand. Bei Word kann man sich über mit dem Dokument gekoppelte Makros sogar Viren und Würmer einfangen.
Doch die Dateien geben noch weitere Geheimnisse preis. Laden Sie einfach mal eine ".doc"-Datei mit dem Primitiv-Editor von Windows, dem Notepad. Neben vielen unlesbaren

Steuerzeichen finden Sie auch den Inhalt des Löschpuffers – möglicherweise mit Resten des vorher bearbeiteten Dokuments. Bei jedem Speichern wird zusätzliche Information in die Datei geschrieben. So ist die gesamte Bearbeitungsgeschichte des Textes noch in der Datei enthalten Je nach Einstellung werden auch bei vielen Dateien die Fonts mit eingebunden, um die Darstellung auch dann sicherzustellen, wenn auf dem Zielrechner nicht alle Fonts vorliegen. Handelt es sich um einen für das Unternehmen lizensierten Font, kann die Weitergabe einer Datei sogar juristische Folgen haben.

Wissen Sie, was das "**ET-Syndrom**" ist? Das sind Programme mit "Heimweh", die immer versuchen, nach Hause zu telefonieren (Wie einst ET im Film). Ein Beispiel ist Microsofts Mediaplayer für Windows XP, der verrät, welcher Anwender welche Musikstücke und Videos abspielt. Zum einen identifiziert die Software zugleich mit dem Anmeldenamen des jeweiligen Windows-Benutzers die abgespielten Stücke und schreibt diese Informationen hinter dem Rücken des Anwenders in eine Logdatei auf die Festplatte. Nach Erkenntnissen von Richard M. Smith übermittelt nämlich der Media Player für Windows XP die Auskunft, was er gerade abspielt, brühwarm an Microsofts Datenbank, während er sich übers Internet von dort mit den Begleitinformationen über Tracktitel, Künstler und Sonstigem versorgt. Bei der gleichen Gelegenheit identifiziert sich das Programm bei seinem Schöpfer mit einer Seriennummer, die allerdings zunächst keine Auskunft über den Benutzer gibt und damit auch gegen keinerlei Privacy-Statement verstößt. Genau dieselbe Seriennummer wird zusammen mit Name und E-Mail-Adresse des Besitzers erneut versendet, sobald sich dieser etwa für Microsofts Windows Media Newsletter anmeldet. Ähnliches Verhalten zeigen der Real-Player und auch andere Programme, die sich damit als handfeste "Trojanische Pferde" erweisen. Kein Käufer von Standardsoftware kann sicher sein, daß keine solchen oder ähnliche "Features" in der Software enthalten sind. Andere Programme führen unbekannte Logdateien. WWW-Browser wie Netscape Navigator oder Internet-Explorer legen Cache-Verzeichnisse an, um den Web-Zugriff zu beschleunigen. Ein Cache erlaubt aber auch, später festzustellen, welche Websites ein Benutzer besucht hat (geben Sie mal beim Netscape "About:Cache" in der URL-Zeile ein). Von reinen Spionageprogrammen, die jede Aktion, egal ob Mausklick, Programmstart oder Tastendruck, protokollieren soll hier nicht weiter die Rede sein.

Dritter Problemkreis: Es kann nicht sichergestellt werden, ob die im Programm realisierten Algorithmen richtig implementiert sind und mit allen Daten korrekte Ergebnisse liefern. Das betrifft vor allem Programme, die komplexe Berechnungen durchführen, aber auch gerade Software, die der Sicherheit dient (z.B. Verschlüsselungssoftware). Ein Beispiel: Umrechnung von BEF in EURO. Der Konversionsfaktor ist 6-ziffrig: 1 EUR = 39.5225 BEF

Umrechnung:	0.01 EUR --> 0.395225 BEF ---> 0 BEF mit Fehler von 100% .
Totalisierungsfehler:	Dasselbe 100 mal. - Erst 100 mal, dann Umwandlung ergibt 39.52 BEF. - Erst Umwandlung, dann 100 mal ergibt 0 BEF.

Und wenn Sie glauben, das passiert nur dem Mittelständler, liegen Sie falsch. Bei der US Federal Reserve System (Zentralbank) überweist ein neues Computersystem nach Inbetriebnahme 28 Milliarden Dollar an falsche Banken. Zurück kamen nur 24 Milliarden! Die 1991 gebaute Ölplattform "Sleipner A" wurde vorher durchgerechnet mittels NASTRAN, einem verbreiteten und teueren Finite-Element-Programm. Aber die auftretenden Scherungskräfte wurden um 47% unterschätzt. Diese Liste läßt sich beliebig fortsetzen. Allgemein gilt in etwa:

- Normale Software: 25 Fehler pro 1000 Programmzeilen Quellcode.
- Gute Software: 2 Fehler pro 1000 Programmzeilen Quellcode
- Space-Shuttle-Software: < 1 Fehler pro 10000 Programmzeilen Quellcode

Windows-95 hat 10 Millionen Zeilen Quellcode. Das heißt bis zu 200 000 Fehler. Das Gesetz der Software-Industrie lautet "Bananen Software": *"Lass die Software beim Kunden reifen!"*

Investitionssicherung

Stellen Sie sich für jede wichtige Anwendung in Ihrem Unternehmen die Frage: "Kann ich in zwei Jahren meine heute erstellten Dateien noch bearbeiten?". Wie ist es in der Vergangenheit um die Aufwärtskompatibilität der Software bestellt gewesen. Ob Textverarbeitung, Kalkulation, CAD-Programm, Warenwirtschaft oder anderes – die Kompatibilität zu früheren Versionen lag keinem Softwarehersteller besonders am Herzen. Wenn es hoch kam, ließen sich Dateien im "alten" Format noch in das neue Format Konvertieren. Ein Weg zurück ist nicht vorgesehen. Das bedeutet, daß auf einen Schlag **alle** vorhandenen Versionen der Software aktualisiert werden müssen. Eine sanfte Migration klappt nicht. Heute ist nahezu jedes Unternehmen auf Gedeih und Verderb von einigen wenigen Softwareherstellen abhängig, da auch kein Dateiformat dokumentiert ist.
Geht es um Textverarbeitung und die Ausgabe von vielen Anwendungen, kann man sich überlegen, ob für die längerfristige Datenarchivierung nicht allgemeingültige Firmate Anwendung finden sollten:

- In vielen Fällen ist es überhauptnicht nötig, alle Formatierungen eines Textes weiterzugeben. Gerade bei E-Mail würde meist ein einfacher Text, direkt im E-Mail-Programm geschrieben oder über das Clipboard ("Zwischenablage") einkopiert, völlig genügen.
- Ebenfalls von Microsoft entwickelt, aber mit offengelegten Syntaxregeln und im Quelltext nachvollziehbar ist das **Rich Text Format (RTF)** zumindest das kleiner Übel. Es enthält alle Textformatierungen, wird von den meisten Textverarbeitungen unterstützt, kann keine Viren übertragen, ist für Word-User genauso unproblematisch in der Handhabung wie 'DOC'. RTF enthält keine Kompression für eingebundene Grafiken. Grafiklastige Dokumente werden deshalb deutlich grösser als im .DOC-Format. Dokumente, die nur Text enthalten, sind dafür kleiner.
- Das professionelle Standardformat zur Weitergabe von formatiertem Text in digitaler Form ist das **Portable Document Format (PDF)**. Es wurde von Adobe als Erweiterung der Seitenbeschreibungssprache PostScript (Standard zum Ansteuern professioneller Drucker) entwickelt. Der Acrobat Reader ist kostenlos und gehört zur Standard-Installation jedes PC. Die Vorteile sind Layout-Echtheit, Vielseitigkeit und Plattformunabhängigkeit. Mit einem verbreiteten PlugIn können PDF-Dokumente auch direkt aus dem Internet im Web-Browser betrachtet werden.
- Die **HyperText Markup Language (HTML)** ist die "lingua franca" des Internet. Da sich HTML-Dokumente ausschließlich auf den ASCII-Zeichensatz stützen, sind die Dokumente auch ohne beonderen Betrachter lesbar und platformübergreifend zu nutzen. Zudem wird die Struktur von Dokumenten klar dokumentiert. Mit der **Extensible Markup Language (XML)** lassen sich eigene Dokumentenstrukturen definieren und mit geeigneter Software verarbeiten.

OpenSource - ein Ausweg?

Mit "Open Source" wird Software bezeichnet, die mit Programmquelle weitergeben wird (kostenlos oder kostenpflichtig). Ursprünglich war die Weitergabe von Quellcode eine Notwendigkeit bei Systemen auf Basis des Betriebssystems UNIX. Da dieses Betriebssystem auf den unterschiedlichsten Harwareplattformen läuft, wurden viel Tools und Anwendungen

(primär aus dem Hochschul- und Forschungsbereich) als Programmquelle weitergegeben, die dann auf dem Zielsystem übersetzt und installiert wurde. Unter dem Dach der Free Software Foundation (FSF) wurden viele Programme weiterentwickelt und unter dem Acronym "GNU" ("GNU is not UNIX") zugänglich gemacht. Mit Aufkommen der UNIX-Variante "Linux" als Open-Source-Betriebssystem hat sich die Open-Source-Basis weiter verbreitert. Open Source heißt übrigens nicht, daß alles kostenlos ist – mit etlichen Open-Source-Produkten wird ordentlich Geld verdient. Noch weiter als reine Quelloffenheit geht das von der FSF entwickelte "GNU Public License Agreement (GPL)". Es besagt unter anderem, daß Entwicklungen auf Basis von Programmen, die unter der GPL weitergegben wurden, wieder quelloffen sein müssen. Das hat leider viele Unternehmen zu dem Irrtum geführt, bei Verwendung quelloffener Programme, alle "Betriebsgeheimnisse" weitergeben zu müssen – was natürlich nicht stimmt.
Die Vorteile von Open-Source-Lösungen lohnen aber auf jeden Fall weitere Überlegungen. Der Einsatz von OpenSource Lösungen bietet viele strategische und praktische Vorteile. Ganz wesentlich ist es, dass für Open-Source-Produkte keine Lizenzkosten anfallen und die Software beliebig oft installierbar ist. Damit sinken sowohl die Anfangsinvestitionen als auch die Folgekosten bei Erweiterung des Nutzerkreises und bei Updates. Nebenbei: Nachezu die Gesamte Software für das Internet stammt aus der Open-Source-Ecke. So haben z. B. der Webserver "Apache" oder das Mailserverprogramm "Sendmail" statistisch den höchsten Marktanteil. Bei Open-Source-Lösungen existiert für den Anwender keine zwangsweise Herstellerbindung. Damit kann sich der Anwender den für geeignetsten Dienstleister frei auswählen. Durch die freie Verfügbarkeit der Quelltexte kann Open-Source-Software an die eigenen Bedürfnisse angepaßt, individuell erweitert und in bestehende Softwarelandschaften integriert werden. Insbesondere in sicherheitsrelevanten Bereichen haben solche Lösungen den Vorteil, daß durch den offen liegenden Quellcode interne oder externe Sicherheitsaudits durchgeführt werden können und wenn nötig auch Anpassungen vorgenommen werden können. Verbreitete OpenSource Produkte werden durch die breite Entwicklerbasis sehr schnell weiter entwickelt. Auch die Fehlerbeseitigung erfolgt schnell, und im Notfall kann der Anwender einen beliebigen Dienstleister seines Vertrauens damit beauftragen, ohne von der "Gnade" eines Herstellers abhängig zu sein. Dabei profitieren alle Anwender gegenseitig von den Entwicklungen Anderer. Dadurch verkürzen sich die Entwicklungszeiten und der Aufwand für den Einzelnen sinkt. Die breite Entwicklerbasis und der offen liegende Quellcode ermöglichen darüber hinaus eine schnelle und kompetente Hilfe. Insgesamt hat OpenSource den Praxistest bestanden: Open-Source-Lösungen arbeiten stabil, zuverlässig, sicher und kostengünstig – und sie machen unabhängig.
Aber nicht nur die Freaks, sondern auch die Politik hat inzwischen die Bedeutung von Open-Source erkannt.Auf den Webseiten des Bundesministeriums für Wirtschaft und Technologie steht eine Broschüre zum Download bereit, die sich sachlich mit dem Thema "Open-Source-Software" auseinander setzt. Die Broschüre richtet sich an mittelständische Unternehmen und Verwaltungen. Sie ist ein Wegweiser für potenzielle Anwender und soll vor allem über die Vorteile und Chancen, aber auch über Nachteile und Risiken von Open-Source-Software aufklären. Der Autor der Broschüre stellt die Stärken, wie aber auch Schwächen von OpenSource im Einsatz in kleineren und mittleren Unternehmen (http://www.bmwi.de/Homepage/download/infogesellschaft/Open-Source-Software.pdf)

Hardware-Schutzmaßnahmen

Schutz von Servern

Der Server ist der Kern eines jeden lokalen Netzes, es ist deshalb erforderlich, daß besonders viele Ressourcen zu dessen Schutz bereitgestellt werden. Der Schutz des Servers sollte

Maßnahmen gegen unerwünschten physischen Zugang, Feuer, unregelmäßige Stromversorgung, Komponentenausfall (typischerweise in Speichermedien) und mangelhafte Kühlung umfassen. Der Server wird in einen abgesperrten Raum gestellt, zu dem der Zugang sehr begrenzt ist. Nur der Systemverwalter und eventuelle Superuser und der Hardwareservice haben Zugang hierzu. Es ist weiterhin zu empfehlen, für das Supervisor-Login nur einen bestimmten Arbeitsplätze zuzulassen. Sollte das Paßwort des Systemverwalters kompromittiert werden, so ist es weiterhin nur möglich, das Login von dieser Maschine vorzunehmen.
Bei der Installation des lokalen Netzes und auch bei dessen laufendem Ausbau sollte bedacht werden, ob im Anschluß an den Serverraum ausreichende Ventilations- und Kühlungskapazität vorhanden ist, um ein vernünftige Arbeitsbedingungen für die zentralen Komponenten des lokalen Netzes zu sichern.
Vorbeugende Maßnahmen bestehen in der Verwendung von feuerhemmenden oder feuerfestem Baumaterial. Der Serverraum sollte keine brennbaren Dinge enthalten, z. B. Druckerpapier, Handbücher, Verpackungen, Holzregale und -tische. Weiterhin wichtig sind Rauch- und Feuermelder, griffbereite Feuerlöscher und Training der Mitarbeiter für den Brandfall
Entscheidend für eine effektive Vorbeugung und Begrenzung von Wasserschäden ist, daß der Serverraum nicht unterhalb der Erdoberfläche eingerichtet wird. Der Serverraum darf auch nicht unter überführten Rohrleitungen, Abflüssen, Küchenbereichen und Badebereichen plaziert werden. Die Sicherung der Stromversorgung umfaßt Maßnahmen gegen Störungen und totalen Stromausfall. Ein Stromausfall kann durch unterbrochene Versorgungsleitungen, aber auch durch Ansprechen von Überlastsicherungen hervorgerufen werden. Um sich gegen Störungen oder Ausfall der Stromversorgung zu schützen, empfiehlt sich nachdrücklich die Anschaffung und Installation einer USV (unterbrechungsfreie Stromversorgung), die gerade mit diesen Verhältnissen fertig wird. Die USV muß eine Notstromversorgung (akkumulatorbasiert) in dem Umfang bieten können, wie es zur Durchführung eines kontrollierten Herunterfahrens des Servers erforderlich ist.

Sicherung von Netzdruckern

Berichte, Projekte und andere Dokumente, die im Unternehmen ausgearbeitet werden, liegen früher oder später über die Netzdrucker in schriftlicher Form vor. Die meisten Mitarbeiter haben wahrscheinlich schon vertrauliches Material im Druckerraum gesehen, wenn sie dort gewesen sind, um ihre eigenen Ausdrucke abzuholen. Die Möglichkeit, daß ausgedrucktes Material in die falschen Hände gerät, ist deshalb offensichtlich. Das Risiko eines unsachgemäßen Zugangs zu vertraulicher Information wird durch eine oder mehrere der folgenden Maßnahmen verringert: Schaffen Sie lokale oder persönliche Drucker für Mitarbeiter oder Arbeitsgruppen an, die sich mit vertraulichen Informationen beschäftigen. Ein oder mehrere Drucker können auch in einen Raum verlegt werden, wo ein Sicherheitsmitarbeiter für die Verteilung ausgedruckten Materials sorgt.
Bei der Industriespionage existiert der Begriff "trashing". Das läuft ganz einfach darauf hinaus, weggeworfenes schriftliches und elektronisches Material als Quelle zu Paßwörtern, Benutzer-IDs oder anderen wertvollen Informationen über das Unternehmens zu benutzen. Schriftliches Material können Ausdrucke, Handbücher, interne Memos, Berichte und anderes sein. Weggeworfene Disketten, CD-ROMS, Festplatten und Bänder können ebenfalls Daten enthalten, die nicht in die falschen Hände fallen sollten. Maßnahmen gegen trashing sind abgeschlossene Abfallbehälter und der Reißwolf sowie Zerstörung oder Überschreiben von ausgemusterten Datenträgern. Dazu gehören übrigens auch die Carbon-Farbbänder von Schreibmaschinen und die Transferfolien von Normalpapier-Faxgeräten und bestimmten Typen von Farbdruckern.

Sicherung von Workstations

Der Ausfall einer Workstation hat nicht den Einfluß auf das Gesamtsystem "Firma" wie der eines Servers, aber auch hier lohnt sich "vorsorgende" Wartung, so daß dem Ausfall von Komponenten vorgebeugt werden kann. Workstations sind aber oft ganz anderen Angriffen ausgesetzt, denn im Gegensatz zu Servern stehen sie in der Nähe von Kaffetassen, Getränkeflaschen und Aschenbechern (wer einmal den Teerschmier im Netzteil eines Computers gesehen hat, dessen Besitzer starker Raucher ist, der wundert sich höchstens, daß die Maschine so lange durchgehalten hat). Hinzu kommen Fehlbedienung oder gezielte Sabotage durch den Benutzer. Auch der Einbau zusätzlicher Hardware (z. B. Steckkarten) gehört nicht zu den Aufgaben des Mitarbeiters, der vor dem Computer sitzt, sondern in die Hände eines firmeninternen PC-Service. Dieser kann durchaus als Zusatzaufgabe einiger Mitarbeiter definiert werden. Zu berücksichtigen ist auch die Gefahr des Diebstahls unbewachter PCs oder Workstations. Gegen Dreistigkeit hilft oft nicht einmal gesundes Mißtrauen. Wenn eine Mensch im weißen Overall ins Büro kommt, strahlend verkündet, daß nun endlich neue Computer installiert werden, und er die alten Rechner wegräumen muß, um Platz für die neuen zu haben, merkt man erst nach Stunden, daß vielleicht irgend etwas faul ist. Es ist auch vorgekommen, daß Rechner regelrecht "ausgeschlachtet" wurden und nur das Gehäuse zurückblieb. Zum Klauen einer Festplatte braucht ein Profi weniger als fünf Minuten – das geht viel schneller, als die Platte zu kopieren. Deshalb gehören wichtige oder geheime Firmendaten nicht auf die Platte eines Arbeitsplatzes, sondern auf den Server.

Backup

Es wurde schon erwähnt, daß effektives Backup von Daten und Software das A und O zur Erreichung hoher Sicherheit im Netz ist. Backup ist die einzige Methode, sich vor Datenverlusten als Folge von Betriebsstörungen, Benutzerfehlern, Virusangriffen etc. zu schützen. Wenn das Unglück geschehen ist, gehen nur die Daten verloren, die sich seit dem letzten Backup geändert haben. Zweckmäßige Backup-Prinzipien und -Routinen sind entscheidend dafür, in welchem Maß das Unternehmen seine Daten wiederfinden kann. Unter den grundlegenden Richtlinien sollten folgende hervorgehoben werden:

- Konsequente Backup-Politik
- Zentralisierte Datenspeicherung und Backup
- Wahl der Backup-Strategie
- Sichere Aufbewahrung
- Einübung und Überprüfung von Restore-Routinen

Für das Backup-Medium im Zusammenhang mit professionellen LANs gibt es derzeit keine Alternative zu Magnetbändern, denn diese erlauben zuverlässiges, automatisches Kopieren großer Datenmengen. Lokale Backups könne auch auf andere Medien erfolgen, z. B. CD-ROM, CD-RW, MO-Platte, etc.

Auf Führungsebene muß dazu Stellung genommen werden, wie lange in die Vergangenheit der Bestand an Backupdaten reichen soll. Eine oftmals angewandte, effektive und in den meisten Fällen ausreichende Vorgangsweise ist, jeden Tag nach Ende der allgemeinen Arbeitszeit Backups von den Änderungen der Benutzerdaten vorzunehmen, und jede Woche ein komplettes Backup. Die täglichen Backups werden eine Woche aufbewahrt, wöchentliche Backups einen Monat, und die monatlichen Backups werden ein Jahr aufbewahrt. In diesem Zusammenhang ist auch an den Befall mit Computerviren zu denken, die nicht unbedingt sofort in Erscheinung treten. In solchen Fällen ist mitunter nur ein sehr "altes" Backup noch nicht verseucht.

Besonders kritische Dateien können auf ein alternatives Medium kopiert werden. Kritisch sind Dateien, die nicht von Originaldisketten rekonstruiert werden können. Zur Sicherheit vor versagenden Bandstationen werden diese auf eine lokale Festplatte, einen anderen Fileserver

oder eine andere Bandstation kopiert. Führen Sie ein "Meilenstein-Backup" vor und nach kritischen und wichtigen Begebenheiten durch, wie z. B. Abschluß der Jahresbilanz, Update des Betriebssystems oder Verlagerung von Geräten.
Bewahren Sie die Backup-Bänder in sicherer Umgebung auf: kühl und fern von direkter Sonneneinstrahlung, Wärme und kräftigen Magnetfeldern. Als Sicherung gegen Diebstahl oder Brand sollten Bänder isoliert von dem System, das sie repräsentieren, aufbewahrt werden.
Falls die Backup-Bänder im Serverraum oder in demselben Gebäude wie der Server aufbewahrt werden, hat das Backup im Falle von Brand, Wasserschaden, Verwüstung, Diebstahl u. a. geringe Wirkung. Stellen Sie deshalb zwei Sätze von Sicherheitskopien her, der eine Satz wird in einem feuerfesten Schrank aufbewahrt, während der zweite Satz extern aufbewahrt wird, z. B. beim Systemverwalter privat (mit dem Vorgesetzten absprechen). Seien Sie sorgfältig bei der Kennzeichnung von Sicherheitskopien, d. h. Quelle, Datum und Inhalt.
Das Backup ist nur die eine Seite der Backuparbeit. Wenn die Bänder unlesbar sind, z. B. aufgrund verschmutzter Schreib- oder Leseköpfe in der Bandstation oder unsachgemäßer Aufbewahrung, ist das Backup natürlich verschwendete Zeit. Kontrollieren Sie, ob das angelegte Backup wiederhergestellt werden kann. Wenn Dateien von den Bändern wiederhergestellt werden können, ist das System grundsätzlich in Ordnung.