Datensicherheit: ein Leitfaden, um Geschäftsinformationen zu schützen

Autor(en): **Richter, Hans-J.**

Objekttyp: **Article**

Zeitschrift: **Schweizer Ingenieur und Architekt**

Band (Jahr): **106 (1988)**

Heft 43

PDF erstellt am: **22.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-85831

Datensicherheit

Ein Leitfaden, um Geschäftsinformationen zu schützen

Das wertvollste Geschäftskapital - Information - findet oft schon auf ein paar Daten-Disketten Platz. Die einfache Bedienungsweise der dezentralen Arbeitsplatzrechner erlaubt einer Vielzahl von Personen den praktisch nicht mehr kontrollierbaren Zugriff. Da Missbräuche enorme Schäden verursachen können, macht man sich zunehmend über die Datensicherheit Gedanken - zumal es hierfür auch juristische Vorschriften gibt und Versicherungen ohne den Nachweis bestimmter Massnahmen nur erheblich verteuerte Policen ausstellen. EDV-Beratungsunternehmen bieten teure Sicherheitskonzepte an, Seminarveranstalter und Sicherheits-Software verzeichnen einen Umsatz-Boom. Der vorliegende Beitrag versetzt in die Lage, mit bescheidenem Aufwand und in eigener Regie individuelle Sicherheitskonzepte zu erarbeiten.

VON HANS-J. RICHTER, FRANKFURT A.M.

Selbst kleinere Unternehmen kommen heute kaum noch ohne Computer, ohne aktuelle und zuverlässige Geschäftsdaten aus. Doch allzu sorgloser Umgang mit «Kollege Computer» kann teure Folgen haben: Im letzten Jahr entstanden allein der schweizerischen Wirtschaft nach Experten-Schätzungen Vermögensverluste in Milliardenhöhe - durch Ausspähung von computerverwalteten Betriebsgeheimnissen, Programmdiebstahl, Elementarschäden, aber auch einfach durch folgenreiche Fahrlässigkeit. Die Dunkelziffer in diesem Bereich gilt als hoch.

Personal Computer gelten in Sachen Sicherheit, da dezentral am Arbeitsplatz aufgestellt, als die problematischsten Systeme überhaupt. Immer mehr Unternehmen erarbeiten deshalb interne Sicherheitskonzepte, wie sie auch bereits von Beratungsunternehmen für fünfstellige Summen angeboten werden.

Das nachfolgende praxisnahe «Check-System Datensicherheit» ist ein Kompakt-Leitfaden mit dem wichtigsten Know-how zur Schadens-Verhütung oder zumindest -Begrenzung. Damit kann sofort - mit minimalem Aufwand und in eigener Regie - ein individuelles Datensicherungskonzept erstellt werden. Das Check-System ist speziell auf die Sicherheits-Schwachstellen von PCs und kleinen EDV-Systemen abgestimmt.

Bessere Datensicherung bei Arbeitsplatzcomputern wird nicht zuletzt auch durch den zunehmenden Trend zur Vernetzung von PCs immer notwendiger. Schon jetzt gilt jedoch: Zwei Drittel der Datensicherheit sind durch organisatorische Massnahmen, praktisch ohne grosse Zusatzinvestitionen zu erzielen. Das Check-System soll in komprimierter Form Entscheidungshilfen für die Risikoanalyse bieten. Für jeden der nachfolgend erläuterten Risiko-Bereiche folgen auch Informationen über praxiserprobte Sicherheitsstrategien. Was davon konkret realisiert werden muss oder sollte, entscheidet die Unternehmensführung dann individuell nach betrieblichen Gesichtspunkten.

Risiken

Diebstahl und Ausspähung von Daten und Programmen

Meist übersteigt der Wert betrieblicher Anwendungsprogramme und gespeicherter Daten etwaige Wiederbeschaffungskosten einer PC-Anlage um ein Vielfaches. Während die Technik oft binnen weniger Tage zu ersetzen ist, lassen sich «massgeschneiderte» Software und wertvolle Datenbanken bei mangelhafter Sicherung nur mit viel Aufwand rekonstruieren - wenn überhaupt.

Dazu kommt: Ohne Sicherheitsvorkehrungen ist das reine Ausspähen von Daten für einen Straftäter relativ risikolos. So lässt sich eine Daten-Diskette (Fassungsvermögen: bereits bis über eine Million Zeichen) binnen Minuten kopieren. Entsprechender Informationsabfluss wird in den meisten Fällen gar nicht bemerkt, weil ja scheinbar nichts «fehlt». Anderen können die Daten aber sehr nützlich sein, weshalb die Ausspähung von Geschäfts- und Betriebsgeheimnissen (falls von der Konkurrenz verwertet) juristisch auch unter dem Aspekt unlauteren Wettbewerbs relevant ist.

Nachfolgend die wichtigsten Varianten illegalen Zugriffs. Die meisten der in diesem Abschnitt genannten Sicherheitsstrategien sind auch auf andere Risiko-Bereiche übertragbar, auch wenn sie nicht mehr wiederholt werden.

Eindringen über Datenleitungen

Zahlreiche PCs sind anwählbar, also per Akustik-Koppler oder Datenleitungen auch über öffentliche Netze erreichbar - bei mangelhaftem Passwortschutz das klassische Schlupfloch für «Hacker» von aussen.

Empfang von Abstrahlung

Bestimmte Geräteteile wirken wie Sendeantennen. Deshalb können Wirtschafts-Spione heute mit entsprechendem Spezial-Gerät elektromagnetische Abstrahlungen von PC-Terminals bis zu einer Entfernung von mehreren hundert Metern (z.B. aus einem Nachbarhaus oder aus einem Pkw) drahtlos empfangen und sowohl die verarbeiteten Informationen als auch interne Passwörter rekonstruieren.

Computer-Kriminalität, Ausspähung von Geschäftsdaten, «Hacker»- Unwesen - immer häufiger kommen in letzter Zeit einschlägige Fälle mit zum Teil enormen Schadenssummen an die Öffentlichkeit. Das Thema EDV-Sicherheit war in vielen Unternehmen eben lange Zeit eine eher lästige - und deshalb vernachlässigte - Nebensache. Besonders bei kleineren Systemen steht nun einmal die konkrete Anwendung im Vordergrund des Interesses.

Nun wird «nachgerüstet». Angebote rund um die Datensicherheit verzeichnen derzeit hohe Zuwachsraten. Produkt- und Dienstleistungsangebote in diesem Bereich sind zu Umsatz-Rennern geworden. Deutlichster Trend: Vor allem PCs und kommerziell eingesetzte Mikrocomputer-Systeme werden jetzt verstärkt gesichert. Denn die einfache Bedienungsweise dieser dezentralen Arbeitsplatzrechner - z.T. im Netzwerk mit anderen PCs - erlaubt einer Vielzahl von Personen in den Unternehmen den praktisch nicht mehr kontrollierbaren Zugriff auf Daten und Programme.

Nur durch systematische Sicherheitsmassnahmen kann es gelingen, die spezifischen Risiken solcher «Miniatur-Rechenzentren» einzugrenzen und sensible Informationen zu schützen. Unser Check-System ist deshalb ganz auf die Datensicherungsprobleme kleiner Systeme ausgerichtet.

Unter «Datensicherung» verstehen wir die Summe aller technischen und organisatorischen Vorkehrungen zur Vermeidung von Schäden oder Missbräuchen im Bereich betrieblicher Computer-Anwendung. Dies schliesst die Belange des «Datenschutzes» ein, ein Begriff, der sich speziell auf die Sicherung personenbezogener Daten bezieht. Sicher ist: Ohne professionelle Datensicherung ist auch Datenschutz praktisch gar nicht möglich.

Absolute Sicherheit ist für das einzelne Unternehmen kaum je erreichbar. Unter betriebswirtschaftlichen Aspekten wird deshalb Verhältnismässigkeit auch bei der Datensicherung oberstes Prinzip sein. So verwundert es nicht, dass sich in den USA bereits zahlreiche Service-Unternehmen darauf spezialisiert haben, für gutes Geld grösstmögliche Sicherheit zu garantieren. Im New Yorker World Trade Center arbeitet ein solcher rund um die Uhr mit Kameras und Sicherheitspersonal bewachter «Daten-Speicher»: vollklimatisiert, vor Feuer durch eine Spezial-Sprinkleranlage geschützt, einbruch- und angeblich sogar bombensicher.

Auch bei uns ist der Aufwand für EDV-Sicherheitstechnik sowie Dienstleistungen in diesem Bereich in letzter Zeit sprunghaft angestiegen und betrug nach Branchenstudien im letzten Jahr europaweit insgesamt umgerechnet rund 1,5 Milliarden Franken. Jan Heidinger, Comptermissbrauch-Experte in einem Versicherungsunternehmen, sieht hier einen anhaltenden Trend: «Die Kosten für Sicherheits-Massnahmen im EDV-Bereich werden steigen. Wie zu Beginn der EDV-Entwicklung die Hardware die teuerste Komponente war und es zur Zeit die Software ist, werden es in der nächsten Zukunft die Sicherheitsmassnahmen sein.»

Insider-Kopien

Wenn Mitarbeiter Programm-Kopien zum persönlichen Gebrauch anfertigen, wird dies vielfach als «Kavaliersdelikt» gesehen, kann aber zu Schadenersatzforderungen von Software-Lizenzgebern führen. Kopierte Daten können in falsche Hände geraten. Und auch die Einsichtnahme von Firmeninterna (Gehaltsdaten, persönliche Verhältnisse einzelner Mitarbeiter usw.) ist – auch wenn kein direkter Schaden zu entstehen scheint – aus Gründen des Datenschutzes und betrieblicher Belange auszuschliessen.

Hardware-Diebstahl

Mikrocomputer stehen meist ungesichert auf den Schreibtischen. Mitunter sind zwar die Geräte selbst gesichert, nicht aber das durch einfaches Abschrauben des Gehäuses leicht zugängliche «Innenleben», z.B. wertvolle Graphik-Erweiterungskarten. Wird ein relativ leicht transportabler Kleincomputer entwendet, können – bei nicht gesicherten Festplattendaten – auch wichtige Informationen verloren sein.

Bewährte Sicherheits-Strategien gegen Diebstahl und Ausspähen

Passwort-Schutz:

Mit entsprechenden Zusatzeinrichtungen prüft der PC vor jedem Zugriff auf Daten (Änderungen, Programmanwendungen, Kopien usw.) die Benutzerberechtigung durch ein persönliches Passwort im Rahmen einer Anmeldeprozedur (log in). Manche Programme verfügen über integrierte Sicherheitscodes mit bis zu zwölf Stellen. Als Passworte beliebt, da leicht zu merken, sind Geburtsdaten, Vornamen oder gar Einzelzeichen (Sternchen) – allesamt leicht zu knacken, z.B. mit «password cracker»-Programmen.

Sinnvolle Vorschrift für die Gestaltung von Sicherheits-Codes: Sie sollten aus einer mindestens sechs- bis achtstelligen Kombination aus Buchstaben, Zahlen und Sonderzeichen bestehen, die in kürzeren Abständen geändert werden. Einen noch höheren Sicherheitsgrad kann durch die Kombination der Benutzer-Identifikation mit automatischen Benutzungsprotokollen erzielt werden, auch hierfür gibt es Zusatz-Software.

Organisierte Datenträgerverwaltung

Manche Firmen inventarisieren und numerieren prinzipiell alle betrieblichen Datenträger vor der (quittierten) Ausgabe an die Benutzer und schreiben Datenträgerkataloge für jeden einzelnen PC vor. Sinnvolle Ergänzungen dieses Systems: Verbot der Benutzung anderer, vor allem privater Datenträger. Und die Vorschrift, Programme und Datenträger nach Dienstende nur unter Verschluss aufzubewahren.

Mechanische Sicherung

An erster Stelle steht die Sicherung von Räumen mit Computer-Equipment durch Spezialtüren oder zumindest Sicherheitsschlösser. Für die Computer selbst werden auf dem Markt die unterschiedlichsten Spezial-Schlosssysteme für EDV-Anlagen und Zubehör angeboten. Eine Inbetriebnahme durch Unbefugte lässt sich durch Tastaturschlösser oder Schlüsselschalter an der Zentraleinheit verhindern. Auch mit kleineren Alarmanlagen ist Hardware zu sichern.

Elektronische Schlüssel-Module

Jüngste Entwicklung, müssen vor einem System-Start vom berechtigten Benutzer in eine PC-Schnittstelle eingesteckt werden. Ohne Modul keine Freigabe von Daten und Programmen.

Chiffrierung

Falls bei einer Datenfernübertragung über öffentliche Netze streng vertrauliche oder geheime Informationen übermittelt werden, ist eine Datenverschlüsselung mit speziellen Chiffrier-Chips oder -Software empfehlenswert. Gleiches gilt natürlich für den Fall, dass Datenträger per Post verschickt werden.

Abschirmung der Terminals

gegen Abstrahlung mit Metallfolien oder Spezialgehäusen oder Unterbringung der Computer in abgeschirmten Räumen.

Optimale Entsorgung

Vertrauliche Ausdrucke gehören nicht in den Papierkorb, sondern in den Reisswolf. Aktenvernichter werden heute für alle Sicherheitsstufen angeboten – auch für ausgemusterte Disketten und andere Datenträger.

Sonstige Computer-Kriminalität

Fiktive Transaktionen

Buchung von Waren oder Dienstleistungen, die in Wirklichkeit nie erbracht wurden. Neben Raubkopien häufigstes Delikt im Bereich der Computerkriminalität.

Datenveränderungen

Elektronische Verfälschung von Zahlungsaufträgen oder Liefermengen, Ausfertigung von Gutschriften, «Bezahlt»-Buchung offener Rechnungen, Änderung von Stammdaten (Provisionen, Rabattzusagen, Überstunden usw.).

Zeitdiebstahl

Die vielleicht unauffälligste Form von Computer-Missbrauch im Unternehmen. Die Palette aufgabenfremder Nutzung reicht vom (noch relativ harmlosen) Schachspielen auf dem Firmenrechner über die Verwaltung einer Vereinskasse bis zur Erledigung regelrechter Nebenjobs am PC. Werden in diesem Zusammenhang auch noch die Möglichkeiten der Daten-Fernübertragung genutzt, können zusätzliche Vermögensschäden durch hohe Postgebühren entstehen.

Bewährte Sicherheits-Strategien

Doppelte Buchführung

Bei einer Kombination elektronischer mit konventioneller Buchführung müsste ein potentieller Täter auch die Quellenbelege fälschen. Bei gleichzeitiger personeller Funktionstrennung der beiden Buchführungsarten ist dies nur sehr schwer möglich.

4-Augen-Prinzip

Für Warenausbuchungen, Ausdruck von Gutschriften und andere betrugsanfällige Vorgänge sollte das System über eine integrierte Ablaufsteuerung verfügen. Anwendungsbeispiel: Bestimmte Vorgänge können dann nur zwei Personen zusammen – mit ihren persönlichen Codes – entsprechend ausführen.

Planmässige Rückmeldungen

Durch konventionelle Kontrollmechanismen: So lassen sich beispielsweise durch den Vergleich von Dateien und Inventarlisten unerklärliche Differenzen in Lagerbeständen erkennen.

Personalauswahl

Bei der Personalauswahl im EDV-Bereich sind neben der Qualifikation auch Sicherheitsaspekte zu berücksichtigen, denn Insider können aufgrund ihres Know-hows in der Praxis viele Systemsperren umgehen. Obwohl Angestelltenverträge betriebsfremde Tätigkeiten während der Arbeitszeit meist ohnehin untersagen, lassen sich Interessenkonflikte, die dann z.B. zu Zeitdiebstahl führen, nie ganz ausschliessen. Vorbeugend wirken auf jeden Fall einige wichtige Grundregeln für die Sicherung von EDV-Systemen – siehe Kasten «Sieben Prinzipien».

Bedienungsfehler

Fahrlässigkeit ist laut Versicherungs-Statistiken der weitaus häufigste Grund für Schäden im EDV-Bereich. Gut drei Viertel aller Schadenfälle entfallen auf Bedienungsfehler und unsachgemässen Umgang mit sensibler Technik, insbesondere:

Löschung von Daten

Durch Unaufmerksamkeit oder Unwissenheit kommt es immer wieder einmal zur versehentlichen Löschung von Dateien. Dies kann – z.B. bei telefonischen Orders – zu Auftragsverlusten führen, wenn für die Tagesdaten noch keine Sicherheitskopien existieren. Solche Folgen falscher Befehle kommen umso häufiger vor, je öfter «schnell angelernte» Aushilfskräfte den PC bedienen. Aber auch, wenn Fachkräfte ein neues Programm noch nicht korrekt beherrschen und es dennoch mit «echten Daten» testen.

Fehlbuchungen

Fahrlässige Falscheingaben können die Produktivität des Betriebs erheblich beeinträchtigen. Der St. Galler EDV-Berater Rudolf Baer nennt aus seiner Praxis einen krassen, aber gar nicht so unwahrscheinlichen Fall: «Kaum zu glauben, aber wahr ist die Geschichte vom Benutzer, der fehlerhafte Auftragspapiere einfach zerriss und neue Aufträge erfasste. Es dauerte entsprechend lange, bis jemand auf die Idee kam, die Ursache für die laufend falschen Umsätze, Lagerbestände usw. bei ihm zu suchen.»

Siehe auch nächste Rubrik: «Technische Probleme».

Technische Probleme

Schadhafte Disketten

Unsachgemässe Lagerung und unvorsichtige Handhabung können Disketten unbrauchbar machen. Schon ein scheinbar harmloser Fingerabdruck verändert die magnetisierte Datenfläche, irritiert den Schreib-/Lesekopf des Diskettenlaufwerks und kann zu Datenverlusten und Programmfehlern führen. Hitze kann Bits und Bytes ab 50 °C zum Schmelzen bringen – da reichen unter Umständen schon Sonnenstrahlen durchs Bürofenster.

Stromschwankungen und -ausfälle

Zwei Drittel aller technisch bedingten Betriebsstörungen sind auf Stromschwankungen (Über- oder Unterspannung, z.B. durch Gewitter oder technische Störungen im Stromnetz) zurückzuführen. Auch hier drohen Datenverluste und die Fehlfunktion von Programmen. Im Extremfall: Totalausfall von Festplatten («head crash»).

Fehlfunktionen der Software

Fast jede neue Software auf dem Markt hat ihre «Kinderkrankheiten», auch scheinbar ausgereifte Produkte können aus unerfindlichen Gründen Datenmüll produzieren.

Defekte Hardware

Das Tückische an defekten Schaltelementen und Schaltkreisen in der Zentraleinheit, Diskettenstationen oder Festplatten: Datenschäden werden oft erst mit Verzögerung bemerkt.

Vier gewichtige Argumente pro Datensicherung:

Gesetzliche Bestimmungen: Ein demnächst auch in der Schweiz zu erwartendes Datenschutzgesetz wird – wie jetzt schon in Österreich und der BRD der Fall – zur Sicherung betrieblicher Daten vor Missbrauch verpflichten. Entsprechende Richtlinien gibt es bereits seit 1981 für die Bearbeitung von Personendaten in der schweizerischen Bundesverwaltung. Schon heute gilt auch für Privatunternehmen: Sollte es zur Verletzung von Persönlichkeitsrechten durch den mangelhaften Schutz personenbezogener Daten (wie sie praktisch in jedem Unternehmen, von der Personal- bis zur Verkaufsabteilung gespeichert werden) kommen, hat der Betrieb eine ungünstige Rechtsposition bei zivilrechtlichen Auseinandersetzungen.

Regresspflicht/Folgekosten: Informationsabfluss kann nicht nur das eigene Betriebsergebnis schmälern, auch Dritte könnten geschädigt werden und Regressansprüche anmelden – man denke etwa an Diebstahl und unberechtigte Verwertung von Lizenz-Know-how auf Datenträgern. Softwareverträge sehen häufig Konventionalstrafen bei vertragswidriger Nutzung vor. Die Einhaltung anerkannter Sicherheitsmassnahmen schliesst derartige Ansprüche von vornherein aus.

Vorbeugung: Gelegenheit macht bekanntlich Diebe. Vorbeugende Sicherungsmassnahmen erhöhen die Schwelle für rechtswidrige Manipulationen. Ohne sie sind Missbräuche (und damit Regressansprüche) zudem oft kaum nachweisbar. Wie sehr gerade Vorbeugung als entscheidende Deliktbarriere wirkt, hat Horst Abel, Datenschutz-Experte festgestellt: «Die Praxis hat gezeigt: wenn Sicherungsmittel mit dem Ziel eingesetzt werden, Tätern Hürden aufzubauen, sie zu überraschen oder zu erschrecken, nehmen viele Täter dann von ihrem Vorhaben Abstand.» Dies, so Abel, gilt insbesondere für kleine und mittlere Betriebe: «Für den Kleinanwender ist es ganz wichtig, bestimmte Mindest-Sicherheitsvorkehrungen zu treffen, da oft das gesamte Know-how, die Geschäftsbilanzen, Daten über Geschäftsbeziehungen u.ä. auf einem leistungsfähigen Personal Computer oder in einem Netz von Personal Computern gespeichert werden.»

Versicherungen: Manche Unternehmen versuchen, EDV-Risiken auch durch Versicherungspolicen zu mindern. Sichern kommt allerdings vor Versichern, denn Voraussetzung für eine ganze Reihe von Schadenersatzleistungen ist – wie aus dem «Kleingedruckten» entsprechender Verträge hervorgeht – die Einhaltung wichtiger Grundregeln der Datensicherung. Die Höhe der Beiträge für Elektronikversicherungen – wie Datenträger-, Mehrkosten- oder Betriebsunterbrechungsversicherungen – ist zudem in aller Regel von den firmeninternen Sicherheitsmassnahmen mit abhängig.

Bewährte Sicherheits-Strategien gegen Bedienungsfehler und technische Mängel

Wartung

Regelmässige Wartung mit Funktionsprüfung und Fehleraufzeichnung. So kann etwa der drohende Totalausfall einer Festplatte schon im vornhinein an einer erhöhten Fehleranfälligkeit erkannt werden. - Wichtig auch: Man sollte Hardware-Investitionsentscheidungen auch nach Lieferfähigkeit und Lieferzeit treffen, denn beim Totalausfall einer Systemkomponente (z.B. Laserdrucker) kommt es genau darauf an. Bei grosser Abhängigkeit des Geschäftsbetriebs von funktionsfähiger EDV sollte für einen Ausweichrechner gesorgt sein. Optimale, jedoch teuerste Lösung: Installation zweier identischer Systeme. Es gibt zwei Kompromissmöglichkeiten: Wartungsvertrag mit Geräte-Ersatzgarantie bei längeren Reparaturzeiten oder Zusammenarbeit mit einem externen Rechenzentrum.

Sichere Verträge

Man sollte in Software-Verträgen Regelungen in eigenem Sinne durchsetzen und Geschäftsbedingungen ablehnen, die das Risiko einseitig auf die eigene Seite abwälzen. Ferner ist es von Vorteil, sich vom Lieferanten in einem Pflichtenheft die umgehende spesenfreie Nachbesserung im Falle von Programmfehlern garantieren zu lassen.

Stromversorgung

Zusatzaggregate zur unterbrechungsfreien Stromversorgung sind teurer als ein durchschnittlicher PC - meist genügt eine Pufferbatterie für kurzfristigen Stromausfall. Empfehlenswert sind auch Spezial-Steckdosen für den automatischen Stromausgleich bei Netzschwankungen, sog. «Interferenz-Filter».

Testläufe

Bei der Einführung neuer Programme sollte während der Testläufe nicht mit «echten» Daten gearbeitet werden, allenfalls mit Test-Kopien. Durch entsprechende Schulung und Einarbeitungszeit produzieren qualifizierte Mitarbeiter keine teuren «Daten-Flops». Ist doch einmal etwas passiert, keine Panik! Mit speziellen Hilfsprogrammen - sog. «Utilities» unterschiedlicher Anbieter - lassen sich gelöschte Daten notfalls elektronisch wiederbeleben («recovery»). Vorausgesetzt, der Fehler wird gleich bemerkt und der Datenträger nicht überschrieben.

Disketten sind in speziellen Boxen stehend zu lagern, nur an den Schutzflächen zu berühren, vor Temperaturschwankungen und anderen Beeinträchtigungen (Staub, manuelle Beschädigungen usw.) zu schützen.

Sabotage und Vandalismus

Vandalismus kommt häufig in Verbindung mit Einbrüchen vor - die Folgen mutwilliger Zerstörung von EDV-Inventar lassen sich in Grenzen halten, wenn wertvolle Datenträger prinzipiell unter Verschluss gehalten und die wichtigsten Datensicherungs-Prinzipien (siehe Kasten) beachtet werden. Gegen externe Täter wirken die üblichen Massnahmen der Objektsicherung.

Die Störung und Beschädigung von EDV-Anlagen erfolgt vor allem in zwei Varianten:

Mutwillige Beschädigung

Sabotage im EDV-Bereich, soweit von Angestellten begangen, ist häufig motiviert durch extreme Unzufriedenheit am Arbeitsplatz, schlechtes Betriebsklima, Rachegefühle gegenüber Chef oder Kollegen, reinen Mutwillen, verbunden mit fehlender sozialer Kontrolle. Man spricht auch von «Frust-Delikten». Cola in der Zentraleinheit, Kratzer in Programmdisketten, Datenlöschung durch Magneteinwirkung und weitere ähnliche Methoden sind aktenkundig geworden.

Computer-Viren

Als «Computer-Viren» bezeichnet man Manipulationsprogramme oder Zusatzbefehle, die Originaldaten und Programmabläufe unmerklich verändern können - bis zur vorprogrammierten «Selbstzerstörung» ganzer Dateien mit zeitlicher Verzögerung («digitale Zeitbombe»). Über scheinbar harmlose Programme («trojanische Pferde») ins System eingeschleuste Viren können z.B. auch den Passwortschutz zerstören. Sofern anwählbar, wird der PC für «Hacker» von aussen zugänglich.

Nach und nach können Viren sämtliche Datenbestände und Arbeitsprogramme «infizieren» und unbrauchbar machen. Ihre Herkunft lässt sich nachträglich meist nicht mehr rekonstruieren, der Saboteur ist somit kaum je einwandfrei zu ermitteln. Diese Gefahr darf nicht unterschätzt werden: Wird ein infiziertes Programm auf Festplatte übernommen, ist der komplette Datenbestand gefährdet. Im Rahmen eines Netzwerks wird früher oder später das ganze System «durchseucht» sein.

Bewährte Sicherheits-Strategien gegen Sabotage und Vandalismus

Software-Sicherung

Betriebliche Original-Software sollte unter Verschluss gehalten und Disketten mit Schreibschutz versehen werden, dies verhindert deren Infektion durch viröse Programme oder nachträgliche Manipulation. Software unsicherer Provenienz muss zuerst mit Probeläufen und Checkdaten getestet werden. Eine Dokumentation aller verwendeten Programme nach der «Prüfsummen-Methode» ermöglicht die Entdeckung nachträglicher Änderungen - denn auch Viren brauchen Speicherplatz. Firmen verwenden zwar in der Regel keine Software-Raubkopien. Nicht gerade selten kommt es allerdings vor, dass Mitarbeiter Spiele-Disketten im Firmenrechner «laufen lassen» oder mit aus Mailboxen abgerufenen Hilfsprogrammen arbeiten. Untersagen Sie den Start betriebsfremder Programme auf den Rechnern, denn nicht umsonst lautet ein gern zitierter «Hacker»-Spruch: «Häufiger Diskettentausch mit wechselnden Partnern birgt ein hohes Infektionsrisiko».

Soziale Kontrolle

Regressvereinbarungen in Arbeitsverträgen können mutwillige Beschädigungen von Insidern nicht mit letzter Sicherheit verhindern, zu erwartende Sanktionen erhöhen aber ganz sicher die «Deliktschwelle». In erster Linie jedoch sollte eine bewusst gepflegte Unternehmenskultur und eine funktionierende positive soziale Kontrolle derartige Auswüchse gar nicht erst aufkommen lassen.

Elementarschäden

Sicher wird nicht jedes prinzipielle Risiko dieser Kategorie - Sturmflut, Erdbeben oder andere Formen höherer Gewalt - zur konkreten Bedrohung. Wir beschränken uns hier deshalb abschliessend auf zwei Bereiche, die auf jeden Fall Vorkehrungen zur physischen Sicherung der Anlage erfordern:

Brände

Bereits einer kurzfristigen Hitzeeinwirkung zwischen 50 und 80 °C halten handelsübliche elektromagnetische Datenträger nicht mehr stand - von direkter Feuereinwirkung gar nicht zu reden. - Sicherheits-Strategien: Keine Aufbewahrung brennbarer Flüssigkeiten sowie Rauchverbot in Computerräumen und brandhemmende Isolatio-

Sieben Prinzipien
Die Grundregeln professioneller Datensicherung

Die Einhaltung der nachfolgend erläuterten Sicherheitsprinzipien mindert das Risiko in allen erwähnten Bereichen und sind dort deshalb auch nicht extra erläutert worden:

1. Bestandesaufnahme mit Risiko-Profil: Grundlage der Planung ist eine individuelle EDV-Bestandesaufnahme mit Risikoprofil. Check-Fragen in Zusammenarbeit mit Mitarbeitern aus den Fachabteilungen: In welchen Bereichen müsste der Schutz verbessert werden, um erwünschte Schutzziele zu erreichen? Mit welcher Wahrscheinlichkeit könnten prinzipielle Risiken zu konkreten Schäden führen und mit welchen Kosten wäre zu rechnen?

2. Sicherheitskonzept: Ein schriftlich fixiertes EDV-Sicherheitskonzept motiviert alle betroffenen Mitarbeiter zu verstärktem Sicherheitsbewusstsein. Um seine Akzeptanz zu gewährleisten, wird es von der Geschäftsführung initiiert und eingeführt. Es definiert genau die Schutzziele, legt eindeutig Kompetenzen und Zugangsbeschränkungen fest und dient in Zweifelsfällen als verbindliche, jederzeit nachschlagbare Richtlinie. Ein Kapitel unter dem Motto «Notorganisation» enthält für Problemfälle wie grössere Schäden eine Zusammenfassung der wichtigsten EDV-gestützten betrieblichen Abläufe mit Alternativmöglichkeiten.

Nicht fehlen sollten persönliche Funktionszuordnungen sowie ein Anschriften- und Telefonverzeichnis - vom Servicetechniker bis zur Feuerwehr, Privatnummern inklusive. - Last but not least: Wer soll als Projektleiter für Erarbeitung und Einführung des Sicherheitskonzepts verantwortlich zeichnen?

3. Systemdokumentation mit Rekonstruktionsplan: Die systematische und fortlaufende Dokumentation des Systems (mit kompletter Inventarisierung der Hard- und Software, Schnittstellen usw.) ermöglicht im Schadens- oder gar Katastrophenfall die schnellstmögliche Rekonstruktion der Anlage sowie eine Notorganisation für die Übergangszeit.

4. Sicherheits-Stufen und Benutzer-Hierarchie: Die zu schützenden Daten sind nach ihrer Bedeutung für das Unternehmen zu klassifizieren. Die Skala reicht von geheimen und absolut betriebsnotwendigen über vertrauliche bis zu geschäftsinternen, aber leicht rekonstruierbaren Unterlagen. Sobald die Sicherheits-Prioritäten ermittelt sind, können die Massnahmen sinnvoll auf die sensibelsten Bereiche konzentriert werden.

Bewährt hat sich ein «4-Stufen-Schema zum Schutz von EDV-Anlagen», entwickelt vom US-Verteidigungsministerium, aber auch von vielen Privatunternehmen entsprechend praktiziert:

- Stufe 1: nur minimaler Schutz notwendig;
- Stufe 2: benutzerbestimmbarer Schutz;
- Stufe 3: vorgeschriebener Schutz;
- Stufe 4: verifizierter, hierarchisch kontrollierter Schutz.

Zugriffsberechtigungen zu den verschiedenen Schutzklassen können in Dienstanweisungen, aber auch in Stellenbeschreibungen festgelegt werden.

5. Archiv-Kopien: Regelmässiges Kopieren von Datenbeständen («Backup») auf separat zu archivierende Disketten ist die preisgünstigste Lösung, allerdings relativ zeitaufwendig. Mit Hilfsprogrammen lässt sich das Disketten-back up beschleunigen. Sind die Basis-Daten erst einmal komplett kopiert, kann die fortlaufende, tagesaktuelle und datierte Sicherung zur Routine werden («file by file»-back up). Im Rahmen von Netzwerken ist es auch möglich, einen reinen back up-PC zu installieren, der kontinuierlich die Daten aller angeschlossenen PCs abspeichert. Bei grösseren Datenmengen arbeitet man mit auswechselbaren Festplattenspeichern oder selbstladenden Magnetbandstationen.

6. Kontrolle: Nach dem Muster grösserer EDV-Anlagen lassen sich auch bei PCs mit Zusatzprogrammen Zeitpunkt, Urheber und Art jeder Benutzung automatisch protokollieren («logging»). Ein elektronisches Logbuch ermöglicht im Bedarfsfall z.B. den Nachweis unbefugten Kopierens von Dateien, nicht autorisierter Dateneingabe oder sonstiger Verstösse gegen interne Richtlinien. Check-Fragen: Wie sonst wird die Einhaltung der Sicherheitsvorschriften kontrolliert? Gibt es einen (nicht unbedingt hauptamtlichen) Sicherheitsbeauftragten? Welche Sanktionen sind bei Verstössen vorgesehen und sind diese bekannt?

7. Permanente Aktualisierung: Risiken und Schutzziele ändern sich in jedem Unternehmen ständig, z.B. durch neue Technik oder die Reorganisation einzelner Abteilungen. Wenn das Sicherheitskonzept von Anfang an in Ringbuchform als Loseblatt-Ordner, geführt wird, können jederzeit bequem die entsprechenden Ergänzungen vorgenommen werden. Zur permanenten Verbesserung des Sicherheitsstandards gehören natürlich auch die Schulung und Weiterbildung aller Mitarbeiter in den betroffenen Bereichen.

nen zur Vorbeugung. Installation von Feuerlöschern und evtl. automatischen Brandmelde- und Löschanlagen. Anschaffung feuersicherer Datensafes oder zumindest hitzebeständiger Spezialschränke. Relativ neu auf dem Markt sind Datenbunker aus Stahl, mit denen man nach dem Öltank-Prinzp ein unterirdisches Auslagerungsarchiv einrichten kann. Kostenfreie Massnahme: Lagerung von Daten-Duplikaten in anderen Brandabschnitten der Geschäftsräume.

Wasserschäden

Ob Rohrbrüche, Überschwemmungen, Eindringen von Regenwasser durch defekte Dächer oder Dachfenster - auch Wasser kann eine Anlage ruinieren. - Sicherheits-Strategien: Computer sowie Zubehör sollten möglichst in Räumen ohne direkte Wasserzuführung untergebracht werden, ferner muss für eine sichere Abdichtung der Leitungen gesorgt werden. Bei Kellerräumen Hochwassergefahr einkalkulieren. Evtl. Montage von Feuchtigkeitsmeldern.

Massnahmen

Die wichtigsten Schwachstellen und Sicherheits-Strategien bei der Anwendung PC-gestützter Datenverarbeitung können Schritt für Schritt in Kenntnis der individuellen Schutzkonzepte realisiert werden. Erster Schritt könnte sein: Studium dieses Leitfadens durch alle betroffenen Mitarbeiter. Schon diese Sofortmassnahme wird nicht nur das Sicherheitsbewusstsein im Betrieb erhöhen, sondern zu einer ganzen Reihe von Verbesserungsvorschlägen aus der Belegschaft führen.

Durch die offene Einbindung der Mitarbeiter wird von Anfang an verhindert, dass ein «Geist des Misstrauens» aufkommt. Die Transparenz der wirtschaftlichen Notwendigkeiten entsprechender Massnahmen ist Voraussetzung der Motivation zu bewusster Vorsorge.

Notwendigkeit entsprechender Massnahmen transparent machen. Sicherheit ist nicht gegen, sondern nur im Konsens mit der Belegschaft zu erreichen. Letztlich nützen Datenschutz und Datensicherheit allen Beteiligten, denn, wie es der amerikanische EDV-Berater Henry F. Sherwood einmal drastisch formulierte: «Ohne Daten sind die meisten Unternehmen in einer Woche pleite.»

Adresse des Verfassers: Dr. *Hans-J. Richter*, Wiener Str. 61, D-6000 Frankfurt a.M. 70.