user MAGAZIN

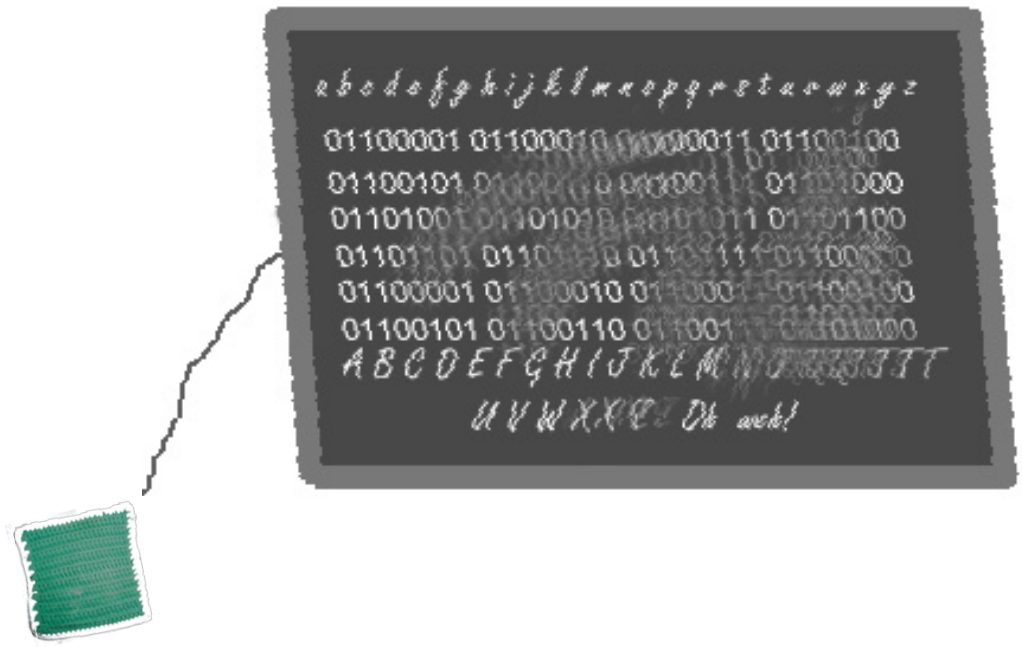
- Spezial -

Datensicherheit

zur

user Konferenz 2002

am 06. April 2002
in Köln



AUGE e.V. Wielandstraße 41 • 60318 Frankfurt • www.auge.de

AUGE e.V.

Der Verein der Computeranwender

lädt ein zur

user KONFERENZ

zum Thema ***D a t e n s i c h e r h e i t***

am Samstag, den 06. April 2002, ab 14.00 Uhr

Ort :OT St. Bartholomäus / Nonni • Helmholzplatz 11 • 50825 Köln-Ehrenfeld

Die Teilnahme ist kostenfrei

P r o g r a m m f o l g e

Florian Delonge **Begrüßung**
Vorsitzender des AUGE e.V.

Heinz Rothkegel **Datensicherheit - Allgemeine Einführung**
AUGE e.V. RG Köln

George Purrio **Haltbarkeit von Daten auf Datenträgern**
imation Leiter des Europäischen Labors

Micheal Schäl **Viren, 0190-Dialer und andere "Malware"**
AUGE e.V. RG Stuttgart

Wolf Müglich / Ralph Dürr **Firewalling**
AUGE e.V. RG Stuttgart/RG Ostalb

Klaus Görgens **Firewalling - Workshop**

Thomas Enke **Verschlüsselung von Daten**
AUGE e.V. RG Köln

Impressum

user - Das Anwendermagazin des AUGE e.V.
Sonderausgabe zur USER KONFERENZ am 06.04.2002 in Köln.
Das USER MAGAZIN ist eine Publikation des AUGE e.V. und dient der Kommunikation und dem Informationsaustausch innerhalb des Vereins sowie der Erfüllung der Ziele des Vereins. Mitteilungen des Vereins an die Mitglieder, die im USER MAGAZIN veröffentlicht werden, gelten als ordnungsgemäß zugestellt im Sinne der Satzung (unter Wahrung der jeweils geltenden Fristen). Dies gilt auch im Falle einer elektronischen Publikation.

Herausgeber:
AUGE e.V. – Der Verein für Computeranwender
Wielandstraße 41, 60318 Frankfurt/Main
Tel. 069/59795813, Fax 069/552004
E-Mail buero@auge.de, Web http://www.auge.de

Der AUGE e.V. wird durch seinen Vorstand vertreten. (E-Mail vorstand@auge.de). Namentlich gekennzeichnete Beiträge - soweit es sich nicht um Mitteilungen eines Vereinsorgans handelt - geben stets die Meinung des Autors wieder, nicht die des Vereins; eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes, Warennamen und –zeichen werden ohne Gewährleistung einer freien Verwendung benutzt.

Redaktion:
Redaktion USER MAGAZIN c/o AUGE e.V.
Wielandstraße 41, 60318 Frankfurt/Main
Tel. 069/59795813, Fax 069/552004 E-Mail redaktion@auge.de

Gertrud (M6274) und Leo Gehrt (Textbearbeitung, Layout)
Heinz Rothkegel (M2374) (Koordination, Anzeigen)

Mit Übergabe der Manuskripte, Abbildungen, Programmlistings etc. an die Redaktion erklärt der Autor, dass er mit einer Veröffentlichung in den Publikationen des AUGE e.V. einverstanden ist und dass sämtliche Materialien frei von Rechten Dritter sind. Der Autor wird insbesondere den Herausgeber von allen Ansprüchen Dritter aus Urheberrechtsverletzungen freihalten, sofern kein eindeutiges Verschulden des Herausgebers vorliegt. Für unverlangt eingesandtes Material wird keine Haftung übernommen. Die Redaktion behält sich das Recht vor, Beiträge zu kürzen, sie auf mehrere Ausgaben zu verteilen oder ggf. auch ganz abzulehnen. Ein Recht der Mitglieder auf Veröffentlichung ihrer Beiträge besteht nicht. Es gilt die jeweils aktuelle Honorarregelung des Herausgebers. Die Richtlinien für Autoren sind unbedingt einzuhalten.

Erscheinungsweise und Redaktionsschluss:
Das USER MAGAZIN erscheint in unregelmäßigen Abständen, je nach Erfordernis. Die Publikation kann entweder durch Versand einer gedruckten/vervielfältigten Ausgabe auf Papier erfolgen oder durch ein elektronisches Medium (Versand einer CD-ROM, Bereitstellung einer Datei zum Download im Web, Versand einer E-Mail). Redaktionsschluss ist in der Regel zwei Wochen vor dem geplanten Erscheinungstermin.

Anzeigen:
Anzeigen in den Publikationen des AUGE e.V. werden nur akzeptiert, soweit sie die Unabhängigkeit des Vereins, seine Ziele und den Grundsatz der Gemeinnützigkeit nicht berühren. Kleinanzeigen von Mitgliedern des AUGE e.V. werden kostenlos veröffentlicht.

Druck:
Kleikamp-Druck GmbH, Zülpicher Straße 205, 50937 Köln-Sülz

Inhaltsverzeichnis

Wir danken folgenden Firmen für ihre freundliche Unterstützung:

American Power Conversion (APC), München
Focus Magazin Verlag, München
IMATION, Neuss
Kleikamp Druck, Köln
Lindy Elektronik, Mannheim
Media-Point Ehgartner, Pulheim
Omega SEE, München
perComp Verlag, Hamburg
Rothkegel & Rolf, Köln
Symantec, Ratingen
Tandberg Data, Dortmund

Herzlich willkommen

zur ersten **uyer KONFERENZ** des AUGE e.V.!

Mit dieser Veranstaltung und dem vorliegenden Sonderheft der Vereinszeitschrift **uyer MAGAZIN** wird der Verein der Computeranwender einmal mehr dem Anspruch gerecht, den er in seiner Satzung an sich selbst stellt: einen Beitrag zu leisten zur "Förderung der Bildung durch Vermittlung von Kenntnissen in der elektronischen Datenverarbeitung".

Natürlich hat sich diese Aufgabe im Laufe der mehr als 20 Jahre seit der Vereinsgründung im Jahre 1979 sehr stark gewandelt. In den Anfangszeiten stand zunächst noch die reine Beschaffung von Informationen im Vordergrund, in aller Regel aus den USA, denn während dort der Siegeszug der Mikrocomputer bereits unaufhaltsam in vollem Gange war, stand Europa in dieser Beziehung doch noch sehr am Anfang. Im Laufe der weiteren Jahre wurde dann das Angebot reichhaltiger, immer mehr Hard- und Software wurde verfügbar und zahlreiche Computer-Zeitschriften kamen auf den Markt. Der stolze Computerbesitzer war nun nicht mehr damit zufrieden, überhaupt ein funktionsfähiges System zu haben, das "Hello, world!" (oder ähnlich) auf den Bildschirm schreiben konnte, sondern er wollte nun etwas Sinnvolles mit dem Gerät anstellen – der Computerbastler wandelte sich damit zum Computeranwender. In der heutigen Zeit ist nun der Computer endgültig zum Alltags-Gebrauchsgegenstand geworden, fast so selbstverständlich wie Telefon oder Fernseher. Der Siegeszug des Internet hat dazu nicht wenig beigetragen und darüber hinaus neue Kommunikationsformen und Wege der Informationsbeschaffung eröffnet.

Wozu also brauchen Computeranwender denn dann noch einen Verein, könnte man nun fragen. Die Antwort fällt uns leicht: Um Themen anzuschneiden, die in der verkaufsfördernden Atmosphäre der Computershops und in der schönen heilen Hochglanzwelt der so genannten Fachzeitschriften manchmal zu kurz kommen, um Alternativen aufzuzeigen und das Bewusstsein zu schaffen auch für die – teilweise unangenehmen – Randerscheinungen und Nebenwirkungen der Computeranwendung. Denn wo viel Licht ist (und sei es nur der Schein des Computermonitors), dort ist eben auch viel Schatten. Das Thema dieses Sonderheftes und der **uyer** KONFERENZ soll dies verdeutlichen ...

Ihr

Florian Delonge (M6285)
Vorsitzender des AUGE e.V.
E-Mail: florian.delonge@auge.de

Datensicherheit

Heinz Rothkegel (M2374), Regionalleiter Köln (RG500)

"In Amerika gibt es jetzt so genannte Microcomputer. Die sind so klein wie eine Schreibmaschine. Das wird eine Revolution in der Bürowelt auslösen. In 10-20 Jahren wird solch ein Teil auf jedem Schreibtisch stehen."
Solche Meldungen hörte man mit großem, fast ungläubigem Erstaunen im Herbst 1976. Das ist gerade mal 25 Jahre her. Wenn damals jemand auch nur ansatzweise prognostiziert hätte, wo wir heute stehen, wie rasant sich diese Technik entwickeln würde, man hätte ihn für gänzlich verrückt erklärt.
Aus 1 MHz Taktfrequenz sind 2000 MHz geworden, aus 8 Bit Datenbreite des Prozessors sind 64 Bit geworden, aus Datenträgern mit wenigen 100 KB Kapazität sind solche mit Kapazitäten von Giga- und Tera-Byte geworden. Diese Aufzählung ließe sich fast beliebig fortsetzen. Wenn man versucht, sich diese Dinge bildlich vorzustellen, kann einem richtig schummrig werden. Viele Dinge, in die man seinerzeit viel Arbeitszeit investieren musste, sind heute mit einem Bruchteil der Arbeitskräfte in einem Bruchteil der Zeit zu bewältigen. Brauchte ein technischer Zeichner damals für eine Bauzeichnung am Reißbrett zwei Wochen, so entwirft er die gleiche Zeichnung heute innerhalb weniger Stunden. Musste man damals Rechnungen mühevoll Buchstabe für Buchstabe mit der Schreibmaschine zu Papier bringen, so nutzt man heute Faktura-Programme oder Warenwirtschafts-Systeme, mit denen man innerhalb von Minuten erledigt, was früher Stunden dauerte. Und nicht nur das, automatisch werden Lagerbewegungen erfasst, Bestellvorschläge gemacht etc.

"Wundervolle Technik", will man meinen, "man drückt auf den sprichwörtlichen Knopf, und alles geht von alleine!" Ja, das wäre schön, wenn´s denn so einfach wäre. Nur leider hat jedes Ding zwei Seiten. Die Leistungsfähigkeit dieser "wundervollen Technik" ist so viel größer als die klassische Arbeitsweise, dass kein Betrieb daran vorbei kommt. Das wiederum schafft Abhängigkeiten. Und da jeder zunächst nur die Vorteile sieht, gibt es oftmals ein böses Erwachen, wenn mal etwas schief läuft. Denn je größer der Rationalisierungseffekt durch die EDV und je schnelllebiger das Geschäft, das man betreibt, desto größer ist auch der mögliche Schaden, wenn die Technik einmal ausfällt. Im Extremfall droht gar der wirtschaftliche Ruin.
Und die Gefahren sind vielfältig. Sie reichen von problematischer oder defekter Technik über Fremdeinwirkung bis zu Datenklau und Datenmanipulation, auch durch betriebseigene Mitarbeiter.
Der Oberbegriff, unter dem sich alle Aspekte dieser Thematik zusammenfassen lassen, heißt **Datensicherheit**. Wir haben ihn zum Thema unserer User-Konferenz gemacht, um ein wenig zu sensibilisieren für eine Sache, die oft erst dann Beachtung findet, wenn das Kind bereits im Brunnen liegt.
Wie wertvoll Daten sind, ist kaum jemandem bewusst. Ich habe einmal in einem Prospekt zum Thema Datensicherung folgendes Beispiel gelesen:
"Man stelle sich vor, die Festplatte geht kaputt und man hat keinerlei Zugriff mehr darauf. Eine Sicherung auf Band oder CD existiert nicht. Aber man war gewissenhaft und hat alles auf Papier in diversen Ordnern archiviert. Nun braucht man "nur" noch die Ordner zu greifen und alles wieder einzutippen. (Dieser Fall ist als extrem günstig anzusehen. Meist weiß man noch nicht einmal, was alles fehlt, geschweige denn, dass man es sofort zur Hand hätte. Aber gehen wir für unser Rechenbeispiel mal von dem "Glücksfall" aus, dass die Daten greifbar sind.) Um die Sache rationell zu gestalten, engagiert man eine Schreibkraft. Die Dame ist Profi ihres Fachs und schafft 300 Anschläge pro Minute. Dafür bekommt sie einen angemessenen Lohn in Höhe von 18 EUR / Std. (Man mag einwenden, dies sei ein hoher Satz für eine Schreibkraft. Die Dame ist allerdings, wie gesagt, auch recht flink. Aber das macht sowieso nichts. Die Kollegin, die nur 150 Anschläge pro Minute schafft und dafür 9 EUR stündlich bekommt, ist letztlich auch nicht billiger.) 300 Anschläge pro Minute sind 18.000 pro Stunde. Bei 18 EUR macht das 1 EUR pro 1.000 Anschläge, also ca. 1.000,00 EUR pro MegaByte! Das ist weniger als auf eine Diskette passt!"

Um die Vielfalt des Themas Datensicherheit zu erläutern, hier einige Unterpunkte:
- Datensicherung
  - Plattenspiegelung, Serverspiegelung, RAID-Systeme, Sicherung auf Band (Streamer) oder anderen geeigneten Medien, externe Lagerung von Datenbeständen
- Archivierung
  - Haltbarkeit von Daten auf unterschiedlichen Datenträgern
- Schutz vor Viren, Würmern und sonstiger "Malware"
  - "Gebührenfalle" Internet
- Schutz vor Hackerzugriffen
- Firewall, verschlüsselte Datenübertragung (Kryptographie)
- Sicherung vor Blitzschlag und anderen Störungen aus dem Stromnetz
- Zugriffsrechte auf Programme und Daten
  - Datenschutz
- ...

Während der Vorbereitungsphase wurde uns erst bewusst, wie vielfältig das Thema eigentlich ist. Wir hätten statt einer halbtägigen wohl auch eine ganzwöchige Veranstaltung organisieren und statt des vorliegenden Heftes auch ein 1000-seitiges Buch herausgeben können. Wahrscheinlich hätten wir trotzdem nur einige Teilbereiche erfassen können.

So haben wir beispielhaft einige Punkte herausgegriffen, die wir auf unserer User-Konferenz beleuchten wollen. Wir haben den Zeitplan bewusst so ausgelegt, dass dies keine einseitige Vortragsveranstaltung zu werden braucht. Vielmehr sollen die jeweiligen Vorträge die Grundlage bieten für eine sich anschließende, hoffentlich rege Diskussion. Dabei ist es uns wichtig, auch und gerade den Computer-Anfänger anzusprechen, denn der steht im Fall des Falles besonders hilflos da. Fortgeschrittene und Profis sind natürlich ebenso willkommen. In diesem Sinne wünschen wir Ihnen und uns ein paar schöne Stunden mit interessanten Vorträgen und anregenden Diskussionen.

.... und was bleibt denn eigentlich von uns ?

George Purrio, Technischer Leiter IMATION Datenspeicherlabor Europa

... wir schreiben das Jahr 4001, der Jahrtausendwechsel ist gerade 2 Tage vorüber. Der Schädel brummt noch leicht von der üppigen Sylvesterparty in Shuttle Xtra, dennoch gibt Transfer X nicht auf. Transfer X ist Archäologe vom Planeten Zetabyte und wühlt bereits seit Tagen in einem Areal von 20 x 30 Meter. Vermutlich eine ehemals von fremden Wesen besiedelte Lagerstätte. Aber so sehr er auch sucht und wühlt, er findet nichts, was auf eine Aufzeichnung, Schrift oder ähnliches der plötzlich verschwundenen Kultur des 3. Jahrtausends hinweist. Dabei hat man doch wesentlich ältere Aufzeichnungen auf Steintafeln gefunden!
Waren die Wesen des 3. Jahrtausends etwa von niedriger Intelligenz und der Aufzeichnung, Übertragung, Verteilung und Speicherung von Informationen nicht mächtig?
Speicherung von Informationen ... nicht mächtig ... Speicherung ... Daten ... Verlust?
Schweißgebadet wache ich auf, nichts mehr mit dem 5. Jahrtausend, die Wirklichkeit hat mich wieder: Januar 2002. Aber was war das? Nichts ist mehr da von unserer hochtechnisierten Informationsgesellschaft, nichts bleibt erhalten? Haben wir nicht alles digital gespeichert und gesichert?

So oder ähnlich geht es vielleicht vielen von uns. Alles für die Katz? Nichts bleibt von uns, weil Datenträger nur eine begrenzte Haltbarkeit haben? Die Antwort aus meiner Sicht: "Ja, aber nicht für die Katz." Wir müssen uns damit abfinden, dass Datenträger gleich welcher Art, digital oder analog, aus Stein oder Kunststoff, nur eine begrenzte Lebensdauer haben. Digitale Speichermedien haben eine geringere Lebensdauer als Stein, dafür aber enorme Speicherkapazitäten.

Langsam weicht mein Erschrecken der Logik und der Feststellung: "Nein, für die Ewigkeit brauchen wir die Speicherung von Zahlen, Bildern und Schriften unserer Informationsgesellschaft nicht, sondern für die überschaubare, nahe Zukunft." Der Vorteil der digitalen Information liegt nicht im "Erhalt auf ewig", sondern in der Möglichkeit, Informationen über einen überschaubaren Zeitraum zuverlässig speichern zu können und zu jeder Zeit an jedem Ort der Welt verfügbar zu haben..

Dabei bleiben die Fragen, was ein überschaubarer Zeitraum ist, und ob die heutigen Datenträger, besonders die magnetischen, diese Anforderungen erfüllen.

Lebensdauerdefinition und die Messmethode

Ich ertappe mich dabei, wie ich hungrig Informationen zur Lebensdauer von Datenträgern sammle. Das Erste, worauf ich treffe, ist eine für mich neue, teilweise schwer begreifliche Zahl von Kürzeln und Namensgebungen. Ich lese von Reliability, Block Error Rate, Expected Life, Mean Life, Mean Bytes between Error, MTBF (Mean Time Between Failures) ... Ich bin verwirrt, was ist denn nun die richtige Bezeichnung? Es dauert ein wenig, aber endlich gelange ich an Informationen von Tandberg Data und IMATION. Dort steht es klar und deutlich:

Lebensdauer = Zeitraum, über den Daten sicher

- **geschrieben,**
- **gespeichert und**
- **rückgelesen werden können.**

So einfach, so logisch. Das kritische Maß für die Lebensdauer von Daten ist also das Rücklesen.

Der Mensch 2078 Jahre alt, mathematisch kein Problem

Ich bin neugierig geworden und möchte jetzt verstehen, wie ich diese Lebensdauer denn messen kann. Wie kann ich die Lebensdauer von etwas bestimmen, was sein Ende noch gar nicht erreicht hat? Die digitale magnetische Speicherung ist ja gerade erst 50 Jahre alt, die optische sogar erst 25. Ich benötige also einen zuverlässigen Blick in die Zukunft. Ich denke über die menschliche Lebenserwartung nach. Was, wenn mir nur die ersten zwanzig Jahre der Statistik bekannt wären, ich aber gerne etwas über den gesamten Verlauf erfahren möchte?

Ich nehme mir eine Studie zum Lebensalter von 1000 Personen

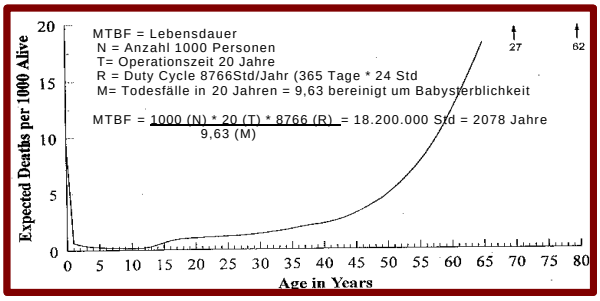


Bild 1 (ältere Studie Lebensdauer Modell Mensch auf der Basis von US 1000 Bürgern)

vor. Im ersten Lebensjahr finde ich einige Fälle von Säuglingssterblichkeit. Man mag mir den Vergleich verzeihen, aber die kenne ich auch aus der Hardware, man nennt dies "Infant Mortality Fehler" und sortiert diese Fälle durch Burn-In-Tests aus. Danach folgt eine relativ stabile Phase, ab und zu ein Ausfall, Unfall o.ä., und erst viel später, mir in meiner Annahme jedoch unbekannt, im Alter der mehr oder minder schnelle Anstieg der Sterblichkeitskurve, das Ende der Lebensdauer. Ich mache mich also daran, das zu erwartende Lebensalter des Menschen mathematisch und nur auf der Basis von zwanzig Jahren Erfahrung zu berechnen. Also Frühausfälle aussortiert, danach 9,63 Ausfälle in den ersten zwanzig Lebensjahren berücksichtigt und

hinein in die Berechnung des MTBF. Das Resultat, die zu erwartende Lebensdauer des Menschen, beträgt 2078 Jahre. Interessant und mathematisch korrekt, nur habe ich noch niemanden getroffen, der dieses Alter auch nur annähernd erreicht hat! Dies kann also sicherlich nicht die geeignete Methode zur Berechnung der Lebensdauer von Datenträgern sein. Mein erster Versuch ist damit jämmerlich gescheitert.

Arrhenius bietet Hilfe $k = A\, e^{-E_a/RT}$ (***Arrheniussche Gleichung***)

Ich begebe mich wieder auf die Suche und stolpere über einen interessanten Namen: Arrhenius, schwedischer Wissenschaftler. Er hat bereits vor über hundert Jahren in umfangreichen Studien einen Zusammenhang zwischen Temperatur und chemischen Reaktionsgeschwindigkeiten festgestellt. Dieser Methode bedient man sich bis heute als einer wichtigen Vorhersagemöglichkeit bei Langzeitprognosen. So testet man beispielsweise optische Medien bei 80^0C und 80% Feuchte über 750 Stunden und setzt das Testresultat gleich mit dem Ergebnis eines Tests bei Raumtemperatur über 100 Jahre. Habe ich nicht erst kürzlich etwas von 1.000.000, 2.000.000 oder sogar mehr Schreibzyklen gehört? Ich rechne nach, 2.000.000 bei einer Anzahl von 400 Datenspuren bei 8 parallelen Schreibkanälen ergibt 50 logische Spuren. 2.000.000 geteilt durch 50 macht 40.000, also 40.000 mal eine Kassette voll schreiben. Einmal schreiben dauert 2 Stunden, 2 Stunden mal 40.000 gleich 80.000 Stunden, also 9 Jahre Testzeit. Der Test soll 1991 begonnen haben. Und das soll eine neue Technologie sein? Ich werde skeptisch und betrachte große Zahlen ab sofort mit einigem Abstand.

Jetzt will ich mehr wissen. Was beeinflusst denn nun eigentlich die Lebensdauer eines Speichermediums? Glücklicherweise treffe ich auf die Experten von Datenspeichermarktführer IMATION und erfahre: Magnetische Datenträger sind, wie andere Datenträger, zuverlässig - sehr zuverlässig sogar - aber es sind Informationsspeicher auf Zeit. Die Haltbarkeit, d.h. Lesbarkeit ist, wie bei anderen Datenträgern auch, durch chemische und physikalische Eigenheiten begrenzt.

Was die Lebensdauer gespeicherter Daten beeinflusst

- Hardware- und Datenträgerverfügbarkeit
- Anwendung
  - z.B. Archivierung = chemische Stabilität gegen Umgebungsbedingungen
  - z.B. Backup oder HSM = mechanische Stabilität der Beschichtung und Komponenten
- Fertigungsqualität der Materialien, Prozesse und Qualitätsmaßnahmen
- Datenträgerverschleiß durch Laufwerksführung, Anzahl der Schreib- und Lesezyklen
- Verschmutzung durch Abrieb, Umgebungsbedingung, Handhabung durch Anwender

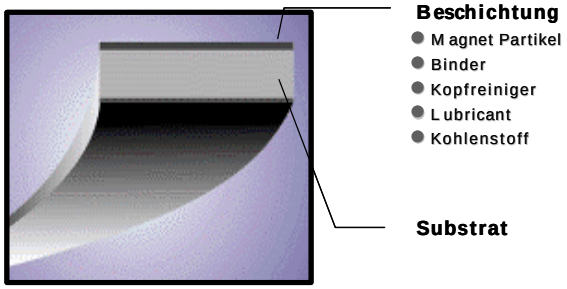
Also auch der Mensch, denke ich und erinnere mich an meinen letzten Arztbesuch. “Was glauben Sie, wie lange werde ich leben?” frage ich den Arzt. Er antwortet: “Wie wirst Du leben?” Jetzt verstehe ich, was er meinte.

Ich melde mich bei IMATION an, um mehr über Aufbau und Einflussparameter von Datenträgern zu erfahren. Sehr zuvorkommend werde ich ins Datenspeicherlabor Neuss eingeladen. Man führt mich in einen gediegenen Präsentationsraum. Frau Dr. Zinseg, Fachbereich Oberflächentechnologie bei Speichermedien, betritt den Raum, um meine Fragen zu beantworten.

Drei Dinge braucht das Band

“Das Magnetband ....,” ich höre, dass das Band aus drei wesentlichen Komponenten besteht. “Das wichtigste sind die Partikel, früher Chromdioxyd heute eher Metallpartikel (MP), feinste kleine Magnete. Etwa 10.000 dieser Partikel werden benötigt, um ein einzelnes Bit darzustellen. Sehr robust sind die Partikel und sehr beständig gegen Temperaturen bis zu 10.000^0C, gegen Feuchte und Bestrahlung. Weder elektronische Flughafenkontrollen noch Beta- oder Röntgenbestrahlung können ihnen etwas anhaben. Aber dennoch, erhöhte Temperatur etwa $40\text{-}50^0$ C, über einen Zeitraum von etwa 15-20 Jahren, können zu einem leichten Verlust des aufgezeichneten Signals führen (5-10 %). "Dabei ist der Signalverlust sehr abhängig von der Partikel- und Prozessqualität," erläutert Dr. Zinseg.

Ich erfahre weiter, dass dies nichts Überkritisches ist, da selbst ein Restsignal nach 85-90% Verlust noch sicher gelesen werden kann. Die Temperatur bei Lagerung und Einsatz ist allerdings ein wichtiger Parameter, der beachtet werden will. Auf der Basis der IMATION-Studien erfahre ich, dass für deren Metallpartikelbänder eine Lebensdauer von mindestens 15 - 30 Jahren kein Problem ist.



Ich erfahre weiterhin, dass der Binder (Polyester-Polyurethan-Basis) die Partikel zuverlässig und dauerhaft mit dem Bandträgermaterial verbindet. Dabei handelt es sich um eine chemische Struktur von größter Wichtigkeit, in die IMATION be-

reits vor vielen Jahren eine Menge Entwicklungsarbeit steckte, die durch mehrere Patente gesichert wurde. Ich bin erleichtert, auf IMATION zu treffen, erinnere ich mich doch an einen Fall vor einigen Jahren, wo ein anderes Unternehmen Millionen Kassetten zurückrufen musste. Der Binder war in seinen Eigenschaften mangelhaft, und ein Magnetpartikelchen nach dem anderen ging auf Wanderschaft. (“Bitte ein Bit, und noch ein Bit...,” geht es mir durch den Kopf.)

Ich erfahre, dass der Binder, wenn ordentlich konstruiert, sehr zuverlässig ist, aber gerne Feuchtigkeit aufnimmt, die dann die Polyesterketten angreift und zerstören kann. Stimmt die Formulierung und hält man die Feuchte unter Kontrolle, so zeigen auch hier IMATION Analysen, dass der Binder für mindestens 30 Jahre stabil bleibt. Feuchte unter Kontrolle halten, das tue ich gerne. Und noch etwas höre ich: “Keine Panik, wenn die Titanic ... [sprich ein Band] einmal unter Wasser geht." Auf keinen Fall sofort versuchen, das Band ins Laufwerk zu legen, um Daten zu retten. Gemach und erst mal backen, lautet die Empfehlung. Ich lerne, dass selbst dann, wenn ein Band Tage und Wochen im Wasser gelegen hat, erst einmal Ruhe angesagt ist. Man nimmt das feuchte Band und trocknet, backt es bei ca. 50^0C für zwei bis drei Tage. Das Band wird stabilisiert, und die Daten können jetzt in Ruhe und sicher auf einen neuen Datenträger übertragen werden.

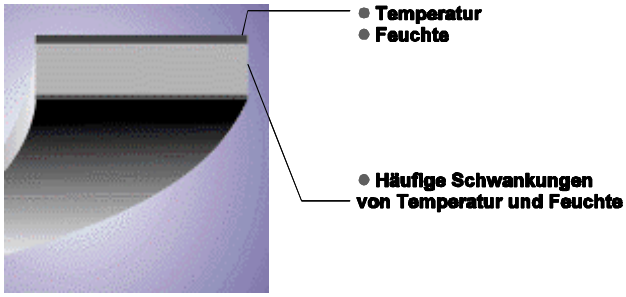
“Zum Dritten ..” - ich sehe mich mehlbestäubt eine Kassette nach der anderen in die Röhre schieben - “zum Dritten” - die Wirklichkeit hat mich wieder - “das Filmträgermaterial, ein Polyester Band PET bzw. PEN, neuerdings auch Aramide -” Ich lerne, dass dies eine wichtige Komponente ist, die als Trägerfilm das Datenträgermaterial gleichmäßig und fest fixiert, sicher über Umlenkrollen und Führungen lenkt, und all das bei höchsten Schreib-, Lese- und Suchgeschwindigkeiten. Das Trägermaterial, so höre ich, hat weniger Probleme mit Feuchte oder Temperatur, als vielmehr mit häufigen Temperatur- und Feuchteschwankungen. Das Kritische sind die Bewegungen der Bandlagen zueinander durch wiederholtes Ausdehnen und Zusammenziehen des Bandes bei häufigen Temperatur- und Feuchtewechseln.

Man lässt das Band “in Ruhe”, verstehe ich, bis man es wirklich benötigt, dann einmal das Band konditionieren, d.h. umspulen. Danach sind die Daten auch bei der Langzeitspeicherung zuverlässig rücklesbar. Ständiges unnötiges Umspulen verstärkt nur Bandstress (Zug- und Druckkräfte), der die Lebensdauer verkürzt.

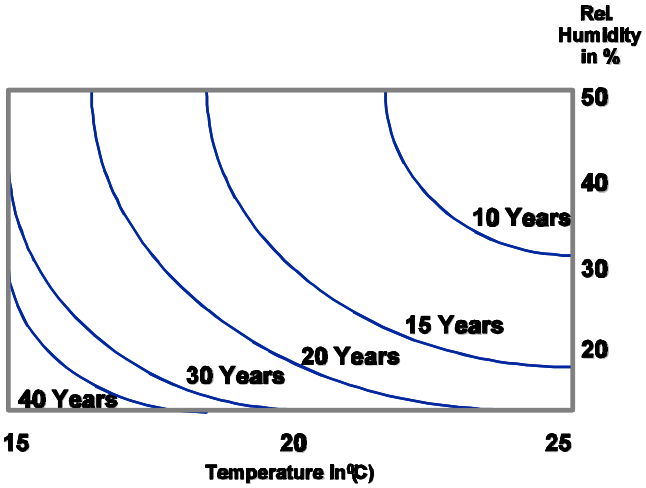
Die Umgebungsbedingungen, ein wichtiges Kriterium für die Haltbarkeit von Daten

Also fasse ich noch einmal zusammen:

- Partikel - erhöhte Temperatur
- Bindemittel – Feuchte
- Trägermaterial – Schwankungen



Ich bin überrascht, das ist sehr logisch und verständlich. Ich male mir bereits aus, wie ich Flüsse und Feuchtgebiete meiner Umgebung umlenken bzw. austrocknen lasse. Blaumilchkanal und Kishon kommen mir in den Sinn.
Es ist wieder Frau Dr. Zinseg, die mich in die Realität zurückholt und meinen bereits geplanten massiven Baumaßnahmen die Basis entzieht. “Sage mir, wie Du lebst - und ich sage Dir, wie lange Du lebst”, der Spruch meines Arztes fällt mir ein, als Dr. Zinseg mir eine Grafik zeigt. Die Grafik veranschaulicht die Abhängigkeit zwischen Archivierungszeit, Umgebung und Umgebungsbedingungen:
Temperatur und Feuchte runter, Archivierungszeit rauf.



Ich verstehe jetzt, dass eine Lebensdauer von 30 - 40 Jahren unter kontrollierten Bedingungen für magnetische Datenträger nicht unrealistisch ist. 8”-Disketten, sowie bereits 30 Jahre alte 3480-Bänder, bestätigen das Vorgetragene. Dabei fällt mir ein, ... wo habe ich eigentlich mein 8”- Diskettenlaufwerk? Ich schaue nach. Nein, im Laptop ist es nicht. Oder hab' ich vielleicht gar keins mehr? Je länger ich überlege, um so schwächer wird meine Erinnerung an ein Laufwerk 35 x 30 x 25 cm und 2,5 kg schwer. Traurig gleitet mein Blick auf eine vor mir liegende 8”-Diskette, zu gerne hätte ich sie wenigstens einmal gelesen.

Kleine Klimakunde für magnetische Speichermedien

- Medien kühl und trocken lagern
- Vor Einsatz, speziell nach Transporten, 24 Stunden an die Umgebung gewöhnen lassen

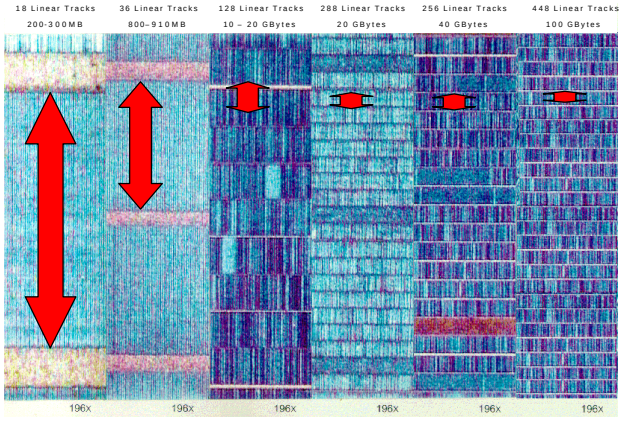
Ideale Archivierungsbedingungen für magnetische Speichermedien nach SMPTE (RP-103)

Operating < 10 Jahre	17EC bis 25EC		30% to 70%	±5%
Storage < years (med.term)	15EC bis 23EC	±2EC	40% to 55%	±5%
Storage < 10 years (long term)	17EC	±2EC	30%	±5%
ANSI/AES Medium Term	23EC max	±2EC	20% to 50%	±10%
Extended Term	20EC max	±2EC	20% to 30%	±5%
	15EC max	±2EC	20% to 40%	±5%
	10EC max	±2EC	20% to 50%	±5%

"Sie wollen also etwas über die Robustheit von Komponenten und Mechanik erfahren ... ?"

Ich schaue auf und bemerke, dass ein Herr um die 40, klein aber robust, den Raum betreten hat. Hans Kuma stellt sich vor, verantwortlich für Test und Prozesstechnik. "Schauen Sie sich dies an," beginnt er und zeigt auf ein Photo, auf dem Giancarlo Fisichella mit seinem Jordan-Rennwagen mit etwa 320 kmh die Ziellinie des Nürburgrings überquert. "Bemerken Sie etwas?" fragt mich Herr Kuma. Ich strenge mich an, kann aber nichts Besonderes finden. OK, das Bild ist ein wenig unscharf, das IMATION-Logo auf dem Wagen ein bisschen klein, aber sonst? "Schauen Sie genauer hin, da links und rechts vom Wagen, nichts, gar nichts, jede Menge Platz, und das bei diesem läppischen Tempo!" Ich bin geschockt, 320 Stundenkilometer und läppisch, mein Fiesta macht gerade mal 110.

"Verstehen Sie", fährt Herr Kuma fort, "hätten unsere Datenträger die Dimension eines Formel-1-Rennwagens, so betrüge unsere Geschwindigkeit über 100.000 km/h, und links und rechts blieben gerade einmal 3 Zentimeter Platz zum Nachbarn. Und wie die Straße aussieht! Nichts mit geradeaus, Richtungswechsel alle 3 Meter. Vor wenigen Jahren hatten wir Datenspuren so breit wie die Startbahn Eins auf dem Frankfurter Flughafen. Da waren es aber auch nur 18 Spuren je Zoll Bandbreite. Heute sind es bei der SLR Technologie 566 Spuren je Zoll Bandbreite und bei der neuen SDLT sogar 896. Früher betrug die Speicherkapazität schlappe 150 MB, heute bis zu 100.000 MB in einer Kassette, die wollen erst einmal geschützt werden. Was heute jeder wissen muss: Ein Datenträger mag ein Kunststoffgehäuse haben, ist aber kein Stück Plastik, sondern ein Präzisionsinstrument.." - Stolz schwillt Herrn Kumas Brust.



Entwicklung der Spurendichten bei der ½" Technologie

Ich lerne weiter, dass alle Gehäuseteile aus hochwertigen Kunststoffen gefertigt sind und selbst einem Fall aus einem Meter Höhe ohne Probleme für die Daten widerstehen. Ein höchstmöglicher Schutz vor Kantenbeschädigung, was sehr wichtig ist, da sich die Datenspuren auch immer mehr den Bandkanten nähern.

Ein Buch, 646 eng beschriebene Seiten Papier, 276.746 Wörter, 2.075598 Byte

Herr Kuma gibt mir anhand eines Buches mit 646 eng beschriebenen Seiten ein beeindruckendes Beispiel für die Fortschritte der Datenspeicherentwicklung bei IMATION.

Band Type	Kapazität(MB)	Bücher je Band	Band je Buch	Lesezeit je Buch
300A	2,9	1,4	65459 mm	23 s
Magnus	1350	649	357 mm	3,5 s
SLR24	12000	5800	59 mm	1,7 s
SLR 100	50000	24084	19 mm	0,4 s

"Vor wenigen Jahren benötigte man 65 Meter Band, um dieses Buch digital aufzuzeichnen, heute gerade mal 19 Millimeter," höre ich. "Und die Leute glauben immer noch, dass das Band nur deshalb glänzt, damit man hier seinen Fingerabdruck hinterlassen kann!"

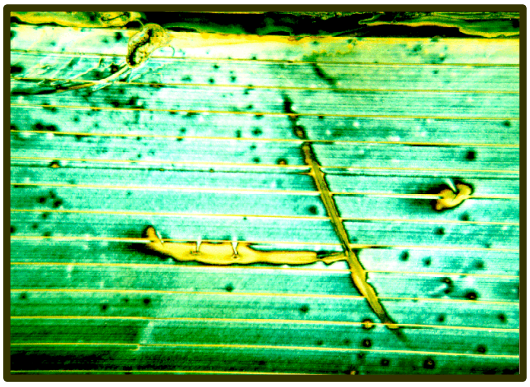
19 mm, fast 650 Seiten Buch! Wie breit ist ein Daumen? Ich rechne nach - und werde sehr nachdenklich.

Herr Kuma weist darauf hin, dass die IMATION in der Fertigung alles tut, um über patentierte Schnittverfahren, Spritzgusstechnologien usw. die Möglichkeit von fertigungsbedingter Verschmutzung zu vermeiden.

So oder ähnlich könnte sie beschrieben werden, die Wanderung durch die Realitäten der Haltbarkeit digitaler Daten. Sicher ist: Wir leben im digitalen Zeitalter und werden die Zeit weder anhalten noch zurückdrehen können. Wir werden uns daran gewöhnen müssen, dass die digitale Speicherung, optische wie magnetische, eine sehr zuverlässige Speicherung ist, aber eben nur eine Speicherung auf Zeit.

Sicher ist aber auch, dass die Haltbarkeit von Daten nichts mit den Versprechungen riesiger Zahlen zu tun hat. Wer glaubt, dass fünfzig, hundert oder sogar dreihundert Jahre Haltbarkeit Sicherheit bedeuten, wird sehr rasch und ziemlich barsch auf den Boden der Tatsachen zurückgeholt.

In unserer innovativen Zeit mit riesigen, immer neuen Technologieschüben ist die Lebensdauer von Technologie sehr häufig wichtiger als die Lebensdauer der von ihr benutzten Speichermedien. Informations- oder Datenmanagement ist heute wichtiger als je zuvor. 8”-und 5,25”-Disketten sind längst überholte Technologien. Und sie wurden gerade einmal zwanzig Jahre alt. War die Magneto-Optische Technologie aus den 90er Jahren lange Zeit führend, so ist sie inzwischen längst durch die Phase Change Technologie überholt worden. Hochkapazitive Bandtechnologien, heute auf der Basis von Servospurverfahren mit bis zu hunderttausend Megabyte Kapazität, haben nur noch wenig gemein mit Megabyte Lösungen der frühen 90er Jahre. Glück hat, wer z.B. auf die Tandberg und IMATION SLR Technologie gesetzt hat, die wie kaum eine andere den Weg der Rückwärtskompatibilität bei gleichzeitig enormer technischer Weiterentwicklung beschritt.



Daumenabdruck schädigt 10 Datenspuren

Die IMATION hat bereits sehr früh vieles getan, um die Speichermedien Schritt für Schritt auf zukünftige Aufgaben der Datenaufzeichnung vorzubereiten. Heutige Metallpartikelbänder (MP) sind sehr robust gegen Umwelteinflüsse. Bei 1800 Oerstedt müssen schon sehr starke, externe Magnetfelder mit den Medien in Berührung kommen, um einen negativen Einfluss ausüben zu können. Es ist aber auch der Anwender selbst (erinnern Sie sich daran, was mein Arzt sagte), der einen wesentlichen Einfluss auf die Langlebigkeit von Datenträgern hat. Sauberkeit am Arbeitsplatz ist sicherlich das erste Gebot. Staubpartikel oder ein Haar sind beispielsweise um ein Vielfaches dicker als eine Datenspur.

Datenaufzeichnung hat viel zu tun mit der Qualität des aufgezeichneten digitalen Signals. In der magnetischen Aufzeichnung wird daher ein sehr genau definierter Kontakt zwischen Medium und Schreib/Lesekopf gewünscht. Kontakt bedeutet aber auch Verschleiß und Abrieb. Wir haben darum bei der Entwicklung des Bandes immer großen Wert auf eine enge Zusammenarbeit mit den führenden Hardware-Herstellern wie Tandberg Data, IBM, Siemens, Seagate, HP, Quantum, um nur einige zu nennen, gelegt. Diese intensive Zusammenarbeit ermöglicht uns eine stetige Optimierung und genaue Balance zwischen Band und Schreiblesekopf bei größter Langlebigkeit, d.h. maximaler Anzahl von Überschreibzyklen. Viele unserer neueren Bandtechnologien, wie unsere 9840-Entwicklung mit Storagetek, verwenden bereits Luftlager sowohl im Laufwerk wie in der Kassette, eine weitere richtungsweisende Entwicklung für zukünftige Herausforderungen an die Lebensdauer.

Unser Ziel ist es, die Daten des Anwenders zu schützen. Aus diesem Grunde sind unsere Spezifikationen stets Werte, die unter statistischen Gesichtpunkten ermittelt die Mindestanforderungen an unsere Produkte repräsentieren. Dies ist vergleichbar dem Verfallsdatum bei Lebensmitteln, von dem wir auch wissen, dass es nicht den Zeitpunkt der Ungenießbarkeit angibt, sondern sicherstellt, dass mindestens bis zu diesem Datum absolut einwandfreie Qualität ohne jegliche Qualitätseinbußen sichergestellt ist.

Bei der SLR100-Technologie garantieren wir eine Lebensdauer von mindestens 15 Jahren und mindestens 10.000 Schreibzyklen, d.h. bei 192 Spuren und 4 Schreib/Lesekanälen mindestens 210 Schreib- und Lesezyklen über die gesamte Länge des Bandes. Dies ist gleichbedeutend mit einem permanenten Überschreiben einer 50 GB-Kassette (ohne Komprimierung) mit einem Datenvolumen von 21 Terabyte. Die Garantie umfasst alle mechanischen Komponenten, d.h. Band wie auch alle Antriebselemente der Kassette. Die mechanische Festigkeit des Bandes spezifiziert ein Dauertest über 40.000 permanente Schreibzyklen auf einer Bandlänge von ca. einem Meter ohne permanente Fehler. Unter Gesichtspunkten des täglichen Bedarfs sicher eine enorme Zahl.

65-70 % der Lebensdauer werden durch Fertigungs- und Prozessqualität des Herstellers, sowie die Handhabung durch den Anwender beeinflusst. Intensive Qualifizierungen stellen seitens IMATION sicher, dass die Anforderungen erfüllt und die Speichermedien über viele Jahre zuverlässig beschrieben und zurückgelesen werden können.

Wohin mit Ihren Daten?

Volker Langer (TANDBERG DATA)

Die Frage nach dem geeigneten Backup-Medium für Entry Level- und Midrange-Umgebungen stellt sich immer wieder. Eine Fülle von vermeintlichen Alternativen stellt den Anwender innerhalb einer professionellen Umgebung vor die schwierige Aufgabe, die für seine Zwecke sinnvolle Datensicherung herauszufinden. Unter Berücksichtigung der Anforderungen an ein Backup-System, sowie der Nutzung der gespeicherten Daten lässt sich die Auswahl erheblich einschränken.

Welche Ansprüche werden generell an ein geeignetes Backup-System gestellt?

Ein Backup-System muss austauschbare Medien nutzen, damit die Kopien der Daten / Informationen auch außerhalb des Gebäudes aufbewahrt werden können. Erst dann ist der Schutz vor unautorisiertem Zugriff oder vor Zerstörung bei bspw. einem Brand oder Wasserschaden im eigenen Gebäude gewährleistet. Auch können die Medien dann gegen Diebstahl oder Sabotage an einem sicheren Ort verwahrt werden. Dies können ausschließlich wechselbare Datenträger wie Magnetbänder, optische Platten, magnetische Platten oder auswechselbare Festplattenlaufwerke leisten.

Welche Anforderungen werden an diese austauschbaren Medien gestellt?

- Die Medien sollten klein und handlich sein, um einen geringen Platzbedarf zu beanspruchen und eine einfache Transportierbarkeit zu gewährleisten. Dadurch ist die räumliche Auslagerung für eine brand- und diebstahlsichere Aufbewahrung möglich.
- Um möglichst viele Daten speichern zu können, muss das Medium hohe Speicherkapazitäten bereitstellen.
- Damit auch in kleinen Zeitfenstern eine vollständige Datensicherung durchgeführt werden kann, müssen hohe Datentransferraten für einen schnellen Datenaustausch sorgen.
- Eine hohe Zuverlässigkeit sowie Haltbarkeit der gespeicherten Daten sind Grundvoraussetzungen, um Daten über einen langen Zeitraum archivieren zu können.
- Je nach Bedarf sollte das Medium häufig überschreibbar oder nur einmal beschreibbar sein. Überschreibbare Medien sollten strapazierfähig und zuverlässig sein, um eine möglichst hohe Anzahl an Nutzungen gewährleisten zu können. Medien, die nur einmalig genutzt werden sollen, um eine nachträgliche Veränderung der Daten zu verhindern, müssen einen Schutz gegen Manipulation bieten.
- Die weitreichende Verfügbarkeit muss gewährleistet sein, um jederzeit auf weitere Datenträger an verschiedenen Orten Zugriff haben zu können. Am besten kann dies ein gängiger de facto Standard leisten, der weltweit durch unterschiedliche Kanäle vertrieben wird.
- All diese Merkmale sollten jedoch auch zu einem vernünftigen Preis-Leistungsverhältnis erhältlich sein.

Was können Magnetbandgeräte hiervon erfüllen?

Magnetbänder eignen sich als Backup-Medium ideal, da diese austauschbaren und handlichen Medien die höchsten Kapazitäten pro Volumeneinheit, einen sehr schnellen Datentransfer, höchste Zuverlässigkeit durch Fehlerkorrekturen, geringe Kosten pro GByte, eine Vielzahl von Nutzungen durch häufiges Wiederbeschreiben und eine lange Lebensdauer der Daten für 20 bis 30 Jahre bieten.

SLR-Streamer

Die Nachteile der Magnetbänder liegen in einer relativ langen Zugriffszeit zu speziellen Daten der Aufzeichnung, wobei auf diese Sicherheitskopien in der Regel auch nicht häufig zugegriffen werden muss, in der Wiederbeschreibbarkeit (sofern man diese nicht wünscht) sowie in unterschiedlichen, nicht miteinander kompatiblen Formaten.

Was können andere Speichersysteme leisten?

Viele der vermeintlichen Alternativen eignen sich eher als Primär- oder Sekundärspeicher, denn als Backupsystem.

1. Festplatten

Zwar lässt sich durch den Einsatz von Diskarrays die Verfügbarkeit von Rechnersystemen deutlich erhöhen. Ein Allheilmittel gegen Datenverluste stellt RAID allerdings nicht dar. Um eine Ausfallsicherheit nahe 100 Prozent zu erreichen, müssen alle Komponenten des Speichersubsystems inklusive Controller, Netzteil und Lüftern redundant ausgelegt werden. Solche Lösungen bietet die Storage-Industrie zwar an, preiswert fallen sie aber nicht gerade aus.

Zudem ereignen sich Ausfälle von Laufwerken und anderen Komponenten nicht immer unabhängig voneinander. In der Praxis treten gelegentlich Situationen ein, durch die sich die Ausfallwahrscheinlichkeit des gesamten Arrays schlagartig erhöht. Dazu zählen etwa durch Blitzschlag verursachte Überspannungen, Überschwemmungen oder Brände. Auch Viren und Würmer befallen RAID-Systeme ebenso gern wie Einzellaufwerke.

Schließlich kann selbst das zuverlässigste Array den Risikofaktor Nummer 1 nicht ausschalten - den Menschen. Den weitaus größ-

ten Teil irreparabler Datenverluste verursacht nicht etwa versagende Technik, sondern Fehlbedienung durch den Benutzer. Gelöschte Dateien sind auch auf RAID-Systemen verloren. Selbst für das ausgefeilteste RAID-System gilt deshalb: den einzig wirklich zuverlässigen Schutz gegen Datenverluste bietet ein konsequent geplantes und vorgenommenes Backup mittels wechselbarer Medien.
Festplatten eignen sich als Datensicherung also nur dann, wenn sie per Wechselvorrichtung entnehmbar und portabel sind, damit sich das Backup-Medium nicht im laufenden System befindet, sondern an einem sicheren Ort aufbewahrt werden kann. Ansonsten können im Katastrophenfall auch beide Platten Verluste erleiden. Problematisch sind allerdings nach wie vor die mechanische Verarbeitung gängiger Wechselrahmen sowie die ruckartigen Beschleunigungen beim Hineinschieben und Entnehmen der Platte. Auch der Neustart beim Auswechseln der Festplatten ist eine unangenehme Begleiterscheinung.
Zudem bedarf es zweier Festplatten als Backup-Medium, die abwechselnd eingesetzt werden. Bei Verwendung von nur einer Backup-Platte erleidet diese im Falle eines Stromausfalls das gleiche Schicksal wie die eigentliche Festplatte, so dass kein Backup mehr vorhanden ist.
Festplatten sollten daher ausschließlich als Primärspeicher eingesetzt werden. Die notwendige Sicherung der Daten im laufenden Betrieb über redundante oder gespiegelte Speichersysteme kann nicht die Datensicherung über entfernbare Medien ersetzen.

2. Sekundärspeicher / Near-Line-Speicher

VS80-Streamer

Von dieser Art der Speicherung spricht man, wenn Daten auf Off-Line-Datenträgern abgelegt sind, diese jedoch auf Anforderung mittels direktem Zugriff erreichbar sind. Als Sekundärspeicher werden in der Regel Laufwerke eingesetzt, die einen direkten Zugriff auf einzelne Dateien ermöglichen (wie optische oder magneto-optische). Aufgrund geringer Kapazitäten werden diese Technologien nur bedingt zur Datensicherung eingesetzt, eher zur Speicherung einzelner Projekte oder Dateien und zum Datenaustausch.

2.1 CD-Laufwerke:
Als optische Speichermedien eignen sich CDs mit Kapazitäten bis zu 700 MB ideal für den Datenaustausch, da die Datenträger mit vielen Systemen lesbar sind. Sie sind für mittel- bis langfristige Archivierung oder Austausch einzelner Dateien oder Projekte geeignet. Aufgrund der geringen Speicherkapazität sind sie als Speichermedium in einem professionellen Umfeld nicht geeignet. Die Haltbarkeit von mehrmals beschreibbaren Medien liegt bei ca. einem Drittel der nur einmal beschreibbaren. CD-Rs bieten eine relativ gute Datensicherheit, sind aber empfindlich gegen Kratzer, Wärme, UV-Licht und hohe Luftfeuchtigkeit.

2.2 DVD-Laufwerke:
Die DVD-Technologie wird herkömmliche CDs in naher Zukunft ersetzen, zumal diese von DVD-Laufwerken gelesen werden können. Es gibt sehr unterschiedliche Formate der DVD-Technologie, wobei die Kapazitäten bei nur lesbaren Medien bis zu 17 GB (DVD-ROM) liegen, wenn beide Seiten in zwei Schichten bespielt werden (bei einmal beschreibbaren Medien DVD-R liegen die Kapazitäten bei bis zu 5,2 GB). Durch die fehlende Standardisierung der Formate (gerade bei wiederbeschreibbaren DVDs) ist die Marktdurchdringung noch etwas problematisch. Das Format DVD+RW bietet beliebige Wiederbeschreibbarkeit und damit Einsatzmöglichkeiten ähnlich einer magnetischen Festplatte – mit dem Vorteil der auswechselbaren Datenträger. Ein weiterer Ansatz heißt DVD-RAM. Auch mit diesem Format ist der wahlfreie Zugriff auf die gespeicherten Daten möglich, auch hier lassen sich die Datenträger nach erfolgter Speicherung ganz oder teilweise wieder löschen und anderweitig verwenden. Die Kapazitäten dieser optischen Datenträger variieren leicht – je nachdem, welches Datenformat zum Einsatz kommt und ob die Medien einseitig oder doppelseitig beschrieben werden.

2.3 Magnetische Wechselspeicher:
Mit geringen Kapazitäten bieten sich Wechselspeicherlaufwerke wie ZIP, JAZ oder Superdisks vorwiegend für den Datenaustausch bzw. für den Transport von Daten oder zum vorübergehenden Speichern von unterschiedlichen Versionsständen, Testdaten oder Projektdateien an.

Welche Technologie also für das Backup?
Für das Backup kompletter Datenbestände von Workstations oder Servern kommt in der Regel ausschließlich das Medium Band in Betracht, da nur diese Technologie ausreichende Kapazitäten und sehr geringe Kosten pro GByte bieten kann. Für geringe Kapazitätsansprüche im privaten Umfeld finden CD-R/RW oder DVD-R/RW als Datensicherungstechnologien ihren angestammten Platz. Im professionellen Umfeld hingegen sind Bandlaufwerke nach wie vor die beste Wahl. Exponentiell wachsende Datenmengen lassen sich nur mit Tape-Backup-Systemen sicher, zeitgerecht und kostengünstig sichern. Aktuelle, auf dem Markt erhältliche Bandlaufwerke können bis zu 110 GB unkomprimiert auf einem Tape sichern (z.B. der Tandberg SDLT220). Mit diesen Kapazitäten ist auch der Einsatz eines Backup-Laufwerks im Netzwerkserver sinnvoll, auf welchem die Daten aller lokalen Rechner zentral gesichert werden können. Für sehr große Netze und Datenbestände eignen sich automatisierte Backup-Systeme mit Wechslern. Dies können Autoloader mit einem Laufwerk und mehreren Cartridges oder auch Libraries mit mehreren Laufwerken sein.

SLR Autoloader

Alleine am Computer?

Lieber Kontakte schließen,
Informationen austauschen
und gemeinsam Projekte
realisieren im AUGE e.V., dem
Verein der Computeranwender!

Besuchen Sie unsere
Webseiten im Internet
unter

http://www.auge.de/

AUGE e.V. - Bessere Ideen.

Festplatten mit Windows richtig einrichten

Das "unkaputtbare" Windows

Jochen Poßberg (M7152), RG Frankfurt/Main

Die Wartung von Windows-Systemen ist auch heute noch nicht immer einfach: kurz einen Treiber installiert, eine CD-ROM angeschaut (natürlich mit einem eigenen Viewer, der sich unaufgefordert installiert), oder etwas aus dem Internet heruntergeladen, und schon läuft Windows nicht mehr oder nicht mehr richtig. Bis es dann wieder wie vorher arbeitet und auch alle vorangegangenen Installationen und Einstellungen einwandfrei wieder hergestellt sind, vergeht mitunter viel Zeit. Windows 2000 und besonders XP haben hier durchaus einige Verbesserungen gebracht, aber auch diese Systeme sind noch nicht perfekt. Mit einer durchdachten Aufteilung der Festplatte und entsprechender Vorsorge in Form von Systembackups kann man sich einige Leiden ersparen.

Was läßt sich mit einer durchdachten Partitionierung erreichen?

Zunächst einmal erreichen wir eine saubere Trennung von Betriebssystem, Programmen und Daten dadurch, dass wir ihnen jeweils eigene Partitionen spendieren. Dadurch verringert sich auch die Größe der Betriebssystempartition um den Platzbedarf der "ausgelagerten" Dateien, was uns sehr entgegenkommt, denn dadurch verkleinert sich auch das Systembackup.

Standardmäßig packt Windows alles auf seine Startpartition und lässt den Anwender auch seine Programme und Daten hierauf ablegen. Dies bläht die Betriebssystempartition stark auf, und mit einer Neuinstallation sind dann entweder auch die Daten weg oder es bleibt Müll aus der letzten Installation zurück.
Eine vernünftige Trennung sieht so aus, dass neben Windows für die Programme, die Daten und für die Auslagerungs(Swap-)Datei jeweils eigene Partitionen angelegt werden. Falls man einen gemeinsamen Datenbestand unter zwei verschiedenen Betriebssystemen nutzen will (etwa Win 98 und XP), ist diese Trennung sogar die einzige Möglichkeit.

Außerdem sind die Daten vom Betriebssystem sauber getrennt, so dass die Betriebssystempartition überschrieben werden kann, ohne dass die Anwenderdaten verloren gehen und umgekehrt die Datenpartition wieder hergestellt werden kann, ohne das Betriebssystem in Mitleidenschaft zu ziehen.

Weiterhin ist es möglich, verschiedene Windows-Installationen auf einem System bereitzuhalten; etwa eine für die Arbeit und eine zum Spielen. Hierfür braucht man zusätzlich einen Bootmanager. Der in Partition Magic enthaltene eignet sich nur für relativ seltene Betriebssystemwechsel; es gibt aber einige Shareware-Bootmanager, z.B. den WWBMU von www.lab1.de

An diesem Punkt endet allerdings die Theorie, und die nicht so ideale Praxis beginnt. Einige (Microsoft-)Programme wie z.B. Outlook (Express) speichern ihre Daten, bei Outlook Express sind es die Mail-Datenbank und das Windows-Adressbuch, automatisch auf C:\
Indem man diese Dateien sucht und die dazugehörigen Registry-Einträge auf ein anderes Laufwerk "umbiegt", lässt sich auch hier Abhilfe schaffen. Die Bookmarks des Internetbrowsers sollte man sowieso in die regelmäßige Datensicherung einbeziehen.

Das Handwerkszeug

Mit den Bordmitteln von Windows kommt man allerdings nicht zum gewünschten Ziel. Erforderlich ist ein Partitionierungswerkzeug wie Partition Magic von PowerQuest (aktuelle Version ist 7.0 (etwa 70 EUR) oder Part.exe (Shareware); außerdem ein Programm zur Erzeugung von Partitionsabbildern, ein so genannter Disk Imager wie Drive Image (aktuelle Version 5.0; ebenfalls von PowerQuest) oder Norton Ghost.
Man sollte sich vor ihrem Einsatz unbedingt mit der Bedienung dieser Programme vertraut machen und auch wirklich die Handbücher lesen, denn bei falscher Handhabung droht Datenverlust!
Nützlich ist ein Werkzeug wie killmbr (nomen est omen!) [http://www.heisenews.de/ct/ftp/ctsi.shtml], das erlaubt, die Partitionstabelle zu löschen. Das kann die letzte Rettung sein für Festplatten mit falschen Partitionseinträgen, bei denen sowohl Fdisk als auch Partition Magic nur noch merkwürdige Fehlermeldungen liefern. Dieses Programm löscht den ersten Sektor der angegebenen Festplatte und damit Partitionstabelle und Master Boot Record. Das Partitionierungsprogramm findet anschließend eine "unberührte" Festplatte vor und kann wieder ganz normal damit umgehen.
Ein Tool namens btcheck zum Sichern und Wiederherstellen des MBR mit der Partitionstabelle gibt es an gleicher Stelle. Disketten-Images zur Erstellung verschiedener Bootdisketten findet man unter http://www.bootdisk.com

Notwendige Vorkenntnisse und Vorbereitungen

Vor der Anwendung der hier beschriebenen Methoden sollte man sicherstellen, über grundlegende Kenntnisse den Aufbau eines PCs betreffend zu verfügen und bereits mindestens eine Komplettinstallation eines Windows-Systems (ab Win 95) selbstständig vorgenommen zu haben, sowie in der Lage sein, sich bei auftretenden Schwierigkeiten selbst zu helfen. Die Aufteilung einer Festplatte in mehrere Partitionen sollte zumindest vom Prinzip her bekannt sein, unter dem Punkt "Partitionen B Festplatte in handlichen Häppchen" folgt eine sehr knappe Beschreibung der wichtigsten Begriffe um die

Partitionierung. Man sollte sich bewusst sein, dass solche grundlegenden Arbeiten wie die hier beschriebenen immer die Gefahr eines Datenverlustes in sich bergen, obwohl dieser bei richtigem Vorgehen sehr selten ist (aber ein Stromausfall zur "falschen" Zeit kann ungläubig erstaunte Gesichter hervorrufen!)

Weitere Vorbereitungen:

- Eine DOS-Startdiskette, angefertigt am besten mit dem zu installierenden Betriebssystem, mit angepassten Einträgen der Startdateien, siehe Anhang.
- Programmdisketten der Partitionier- und Image-Software; diese muss man zumindest im Fall der PowerQuest-Produkte Partition Magic und Drive Image erst auf der Platte installieren, um dann die Programmdisketten für die DOS-Version anfertigen zu können.

Für Anwender, die mit Windows begonnen haben und kein DOS kennen, gibt es eine gute Einführung bei http://www.knowware.de/dos.htm .
Hefte dieses Verlages sind auch für andere Themen erhältlich und sehr zu empfehlen. Sie kosten nur etwa 4 EUR und vermitteln Wissen in sehr kompakter Form. Der Inhalt ausverkaufter Hefte kann von der Webseite als PDF-Datei kostenlos heruntergeladen werden. Welcher andere Verlag bietet einen solchen Service?

Das Prinzip

Der Grundgedanke bei unserem Vorgehen ist der, dass das gesamte Betriebssystem (hier also Windows), alle Treiber, alle Einstellungen, alle Systemprogramme, alle Daten in ausgeschaltetem Zustand des PC sämtlich als Daten in einer Partition auf der Festplatte liegen. Dies ist bei Windows normalerweise die Partition mit dem Laufwerksbuchstaben C, Win NT/2000/XP machen hier eine Ausnahme, aber auch hierbei müssen die Startdateien auf C:\ liegen. Wenn man jetzt vor und nach Installationen und anderen Veränderungen des Systems von dieser Partition ein bitgetreues Abbild erzeugt und bei Problemen ein funktionsfähiges Abbild wieder zurückspielt, hat man im Prinzip schon ein "Unkaputtbares Windows". Das nennt man dann auch "Disaster Recovery" (wörtlich übersetzt: "stellt das letzte Desaster wieder her" ;-). Aber Scherz beiseite, zum vollständigen "Disaster Recovery" gehört noch die Wiederherstellung des "Master Boot Record", den man von einer zusammen mit der Sicherung der Festplatte hergestellten Bootdiskette durchführt. Diese Bootdiskette muss mit dem System hergestellt werden, das man auf der Platte hat (DOS/Win95/Win98). Die Erstellung des "Master Boot Records" erfolgt nach dem Starten von dieser Diskette mit dem Aufruf FDISK /MBR. Oder, besser, man verwendet ein Tool, das den MBR mitsamt Partitionstabelle sichern und wieder herstellen kann (Quelle siehe unter "Das Handwerkszeug"). Windows-NT-Anwender sollten außerdem unbedingt die "Hotline" in der c`t 3/99 lesen (S. 196, auch online verfügbar unter www.heise.de/ct/).

Das hört sich zwar alles gut an, allerdings sind in der Praxis einige wichtige Details zu berücksichtigen, damit es *wirklich* funktioniert. Eins dieser Details besteht darin, dass man keine Partition sichern kann, von der ein Betriebssystem gestartet wurde, denn dieses hält Dateien offen. Das Programm, das die Sicherung (und auch das Restore) durchführt, muss also von einer anderen Partition aus gestartet werden, aber ebenso natürlich auch das Betriebssystem. Da das gar nicht so einfach ist, sollte man sich zur Regel machen, Kopier-, Sicherungs- und Restore-Arbeiten an Partitionen immer unter reinem DOS durchzuführen, das von einer Bootdiskette gestartet wurde oder, alternativ, sich genau zu überlegen, von welcher Partition man Partition Magic starten muss (eine Mehrfachinstallation auf verschiedenen Partitionen ist empfehlenswert).

Für die Sicherung der Betriebssystempartition gibt es mehrere Möglichkeiten; sie kann erfolgen:

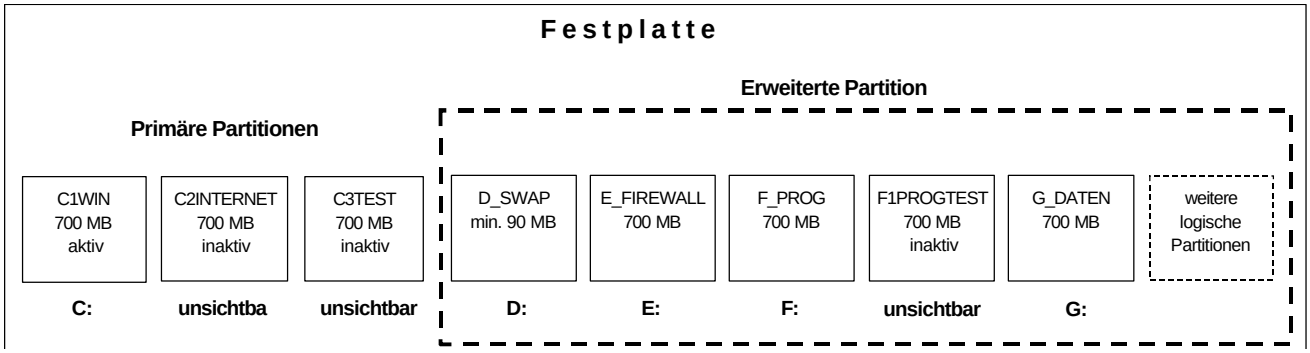
- auf der gleichen oder einer anderen Festplatte desselben Rechners
- auf einem Wechselplattenlaufwerk (MO; CD-R/W)

Im ersten Fall hat man den Vorteil, dass der Vorgang sehr flott vonstatten geht, die begrenzte Plattenkapazität kann jedoch schnell eine Grenze setzen, und es kann nicht von Datensicherung gesprochen werden, denn wenn die Platte den Geist aufgibt, sind auch die Images weg.

Im zweiten Fall ist die Speicherkapazität durch Wechselmedien im Prinzip beliebig erweiterbar. Das Werkzeug hierfür ist wie besprochen z.B. Drive Image oder Ghost. Heutzutage ist wohl in den meisten Fällen ein CD-R(W)-Laufwerk das Mittel der Wahl. Drive Image (und soviel mir bekannt, auch Ghost) kann unter DOS direkt über einen eigenen Packet-Treiber auf die CD schreiben. Der Autor hat das allerdings noch nicht ausprobiert, er verwendet weiterhin sein geliebtes SCSI-MO-Laufwerk.

Partitionen: Festplatte in handlichen Häppchen

Als notwendiges Grundwissen ganz kurz die wichtigsten Dinge rund um die PC-Partitionseinteilung: Eine Festplatte kann max. 4 Partitionen enthalten, diese werden auch primäre Partitionen genannt. *Eine* davon kann eine "erweiterte" Partition sein, die dann in eine oder mehrere sogenannte "logische Partitionen" aufgeteilt wird. Diese werden in der Literatur meist "logische Laufwerke" genannt, wir bleiben der Klarheit wegen aber bei dem Begriff "logische Partitionen".
Von den primären Partitionen darf unter Win 9x nur jeweils *eine* aktiv (d.h. sichtbar) sein, die anderen müssen inaktiv oder "versteckt" sein; auf diese kann in dieser Konfiguration dann nicht zugegriffen werden. Lediglich die erweiterte Partition mit ihren logischen Partitionen ist ebenfalls sichtbar. Hat man eine zweite (oder weitere) Platte im System, empfiehlt es sich, auf dieser ausschließlich eine erweiterte Partition anzulegen, die dann in logische Partitionen eingeteilt wird. Man vermeidet so den berüchtigten "Laufwerksbuchstabensalat", der dadurch entsteht, dass die Laufwerksbuchstaben nach einem eigenwilligen Abzählreim vergeben werden: zuerst kommen die primären Partitionen *aller* Platten, dann die erweiterten mit den darin befindlichen logischen Partitionen. Laufwerksbuchstaben verteilt übrigens das Betriebssystem, die von Partition Magic



angegebenen sollte man nicht unbedingt "ernst nehmen".

Für weitere Einzelheiten zu Partitionen, logischen Laufwerken und Verwandtem sei hier auf das (im übrigen sehr gute) Handbuch von Partition Magic verwiesen, dessen Lektüre an dieser Stelle dringend empfohlen wird.

Sonderfall Windows 2000/XP

Windows 2000/XP kann mit mehreren primären Partitionen umgehen und erlaubt auch die freie Wahl der Laufwerksbuchstaben. Mit dem unter Win 9x nötigen Verfahren macht man allerdings auch unter 2000/XP nichts falsch. Außerdem bietet es mit dem Konzept der "dynamischen Datenträger" eine andere, flexiblere und zu dem herkömmlichen und hier beschriebenen Verfahren der Partitionierung inkompatible Art der Aufteilung von Festplatten, worauf an dieser Stelle nicht weiter eingegangen werden kann. Details hierzu findet man in dem sehr ausführlichen und gut strukturierten Werk von Uwe Bünning / Jörg Krause: Windows XP Professional, Hanser-Verlag 2002; 50 EUR.
Allerdings hat die Sache auch einen Haken: Start- und Systemdatenträger (die Bedeutung dieser beiden Begriffe in Verbindung mit Win 2000 /XP entnimmt man am besten dem o.a. Werk) müssen auch unter diesen Betriebssystemen "normale" Partitionen sein. Das hier Gesagte verliert also auch dort nicht seine Bedeutung.

Ein praktisches Beispiel

Im Folgenden wird eine Neuinstallation unter Zugrundelegung der obigen Prinzipien beschrieben. Für die Partitionierung der Platte verwenden wir Partition Magic, für die Sicherung der Partitionsabbilder (Images) Drive Image. Es besteht zwar auch mit Partition Magic die Möglichkeit, Partitionen zu kopieren, aber das geht nur auf und zwischen Festplatten, ist also keine wirkliche Sicherung.

Das einzurichtende Betriebssystem soll Windows 9x sein, die einzige Festplatte sei ein EIDE-Gerät mit der Kapazität >10 GB. Das ist sozusagen die Pflicht. Die Kür ist wie beim Sport prinzipiell beliebig zu gestalten; mehrere Festplatten; SCSI-; Firewire- und USB-Systeme, alternative Betriebssysteme etc. Für Rückmeldungen über geglückte Doppelaxel und Rittberger dieser Art haben wir ein offenes Ohr bzw. AUGE ....

Los geht´s !

Getartet von der DOS-Bootdiskette legen wir mit der DOS-Version von Partition Magic auf der leeren Platte folgende Partitionen an:

- C Eine primäre Partition mit einer Größe von 700 MB mit dem "alten" FAT; nicht FAT 32 (so kann man auch unter reinem DOS - von einer Bootdiskette gestartet - noch auf die Dateien darin zugreifen). Wir geben ihr den Namen (die Datenträgerbezeichnung) C1WIN.
- C Eine weitere primäre Partition gleicher Größe (die wir verstecken bzw. inaktivieren); Name: C2INTERNET- Partition Magic lässt standardmäßig nur eine aktive primäre Partition pro Platte zu. Wird eine andere aktiviert, versteckt bzw. inaktiviert es automatisch die augenblicklich aktive.
- C Eine dritte primäre Partition, ebenfalls mit der gleichen Größe, auch inaktiv; Name: C3TEST
- C Eine erweiterte Partition mit dem Rest des Plattenplatzes, die wir in logische Partitionen (Laufwerksbuchstaben verteilt erst das Betriebssystem bei seinem Start) einteilen.
- **S** Die erste logische Partition erhält die doppelte Größe des installierten Hauptspeichers, mindestens jedoch 90 MB, sie ist reserviert für die Windows-Auslagerungsdatei; Name: D_SWAP.
- **S** Die zweite errichten wir wieder mit einer Größe von etwa 700 MB; Name: E_FIREWALL, ergibt unsere "Firewall"
- **S** Die dritte: Größe 700 MB; Name: F_PROGRAMME; auf ihr werden später alle Programme installiert, mit Ausnahme der Internet-Software.
- **S** Die vierte: Größe 700 MB; Name: F1PROGTEST; dient für Testinstallationen; sie wird versteckt!
- **S** Die fünfte: Größe 700 MB; Name: G_DATEN, ist für unsere Daten bestimmt, wieder mit Ausnahme der Daten der Internetprogramme.

Der Rest der Platte steht uns zur freien Verfügung. In dieser Beschreibung gehen wir generell davon aus, dass Partitionsbackups mit Drive Image oder Ghost angelegt werden; die versteckten Partitionen mit dem schönen Namen "LAURINx" aus der ersten Version des Artikels im User Magazin 1/99 werden also nicht benötigt. Die Platte sollte jetzt so aussehen, wie in der Abbildung oben dargestellt.

Auf die Plätze, fertig, Windows !

Jetzt kommt die Windows-Installation. Zuerst folgen wir dem Tipp im Kasten und weisen dem CD-ROM-Laufwerk in der AUTOEXEC.BAT einen festen Laufwerksbuchstaben in der zweiten Hälfte des Alphabets zu, damit genügend Platz für die Laufwerksbuchstaben der Partitionen bleibt; booten von Diskette und installieren ganz normal Windows. (Ist die erste primäre Partition auch aktiv geschaltet und die beiden anderen inaktiv?) Windows kann nur die primäre Partition für sich verwenden, vergibt allerdings für alle gefundenen Partitionen außer den versteckten die Laufwerksbuchstaben. Die *sichtbaren* logischen Partitionen in der erweiterten Partition haben also jetzt alle Laufwerksbuchstaben erhalten, und wir könnten demzufolge auch, wie in der PC-Welt üblich, von logischen Laufwerken sprechen, bleiben aber der Klarheit wegen bei dem bisher benutzten Begriff.

Tipp: Wenn man bereits dem CD-ROM-Treiber in der Autoexec.bat den Laufwerksbuchstaben vorschreibt (mit MSCDEX ... /L:Buchstabe) und nach der Installation von Windows diesen sofort im entsprechenden Teil der Systemsteuerung (System/ Gerätemanager/CD-Laufwerk/Eigenschaften gleichlautend festlegt, vermeidet man ein späteres Chaos dergestalt, dass Windows (oder andere Programme) sein/ihr Installationslaufwerk nicht mehr findet, wenn etwa eine logische Partition gelöscht oder neu angelegt wurde. (Wir empfehlen als Laufwerksbuchstaben O:, weil das erstens *fast so schön rund wie eine CD* aussieht und weil zweitens noch genügend Reserve sowohl für Plattenpartitionen als auch für Netzlaufwerke bleibt (die ja bekanntlich "von hinten her" belegt werden sollten).

Als Nächstes werden die benötigten Treiber und systemnahen Programme installiert; nur ausgereifte Versionen, kein Testkram! Die fertige Installation soll die solide Basis für den weiteren Aufbau des Systems sein. Partition Magic und Drive Image sollten ebenfalls bereits zu diesem Zeitpunkt installiert werden, damit sie komfortabel von der Platte gestartet werden können.

Vorsicht: Das Starten in den DOS-Modus erfolgt unter Win 9x durch Umbenennung der Startdateien CONFIG.SYS und AUTOEXEC.BAT. Stürzt der PC dann zum falschen Zeitpunkt ab, ist er unter Umständen nicht mehr startfähig und muss mit Hilfe einer DOS - Startdiskette durch manuelles Umbenennen der Startdateien wieder in den bootfähigen Zustand zurückversetzt werden. Gut, wenn die Systempartition mit FAT16 und nicht mit FAT32 eingerichtet ist; die Struktur der FAT32-Startdiskette ist wesentlich schwerer zu verstehen. (Ich habe es leider noch nicht geschafft, allerdings bestand auch noch keine Veranlassung dazu.) Sicherer, wenn auch umständlicher, ist es auf jeden Fall, für Systemarbeiten unter DOS immer von Diskette zu starten. Gut, dass auch die modernen PCs immer noch über ein Diskettenlaufwerk verfügen.

Die Windows-Auslagerungsdatei verlegen wir nach D_SWAP (Unter Systemsteuerung/System/Leistungsmerkmale/Virtueller Arbeitsspeicher); minimale und maximale Größe sollten den gleichen Wert erhalten (s.o.), damit Windows die dynamische Verwaltung des virtuellen Arbeitsspeichers erspart bleibt, was nur Performance kosten würde.

Es sollte jetzt ein funktionsfähiges eingerichtetes Windows-System vor uns stehen, mit komplett und korrekt eingebundenen Treibern. Nach einigen Tests auf Lauffähigkeit ist jetzt der Zeitpunkt gekommen, den erreichten Stand zu sichern, damit er nicht mehr verloren geht.

Tipp: Als sehr wertvoll hat sich bei uns die Führung eines Installationslogs erwiesen, in das alle Änderungen am System eingetragen werden sowie auch die einzelnen Installationsschritte (sofern nicht "im Schlaf" geläufig) und auch alle Konfigurationsänderungen. Das kann und sollte ruhig recht ausführlich ausfallen. Dieses Log führt man am besten auf Papier oder, so vorhanden, auf einem zweiten PC. (Zu dumm, wenn es auf dem PC liegt, zu dem es gehört und man es braucht, weil er nicht läuft, man aber genau aus diesem Grund nicht herankommt ...)

Als nächstes wird von der DOS-Startdiskette gebootet und anschließend Drive Image (oder Ghost) gestartet. Wir erstellen ein Image der C1WIN auf einem externen Datenträger, also z.B. CD-R(W) oder MO; ersatzweise auf einer der ´großen´ logischen Partitionen, die wir eben angelegt haben. Außerdem kopieren wir mit Partition Magic die C1WIN:-Partition mit dem frisch installierten Windows in die versteckte/inaktive zweite primäre Partition, also C2INTERNET und auch in die dritte primäre Partition, also C3TEST. Jede der 3 primären Partitionen enthält jetzt also das Basis-Windows und ist nach Aktivschalten bootfähig.

Windows-Crash mutwillig ...

Jetzt ist der spannende Moment ... für einige Tests gekommen: Erneut von DOS-Diskette starten, Partition Magic aufrufen; C1WIN verstecken und dafür C3 aktivieren. Anschließend die Diskette entnehmen und neu starten.

Das Windows sollte jetzt starten, als ob nichts gewesen wäre. In Wirklichkeit startet aber nicht unser `eigentliches´ Windows, sondern dessen Kopie auf der Partition C3, die hiermit ihre Funktionsfähigkeit bewiesen hat.

Erneuter Start von Diskette, C1Win aktivieren und darauf das komplette Windows-Verzeichnis löschen.
Neustart ohne Diskette; Windows kann nicht starten; es ist defekt.

Jetzt booten wir erneut von Diskette und stellen aus unserem Image die Partition C1WIN wieder her. Dafür verlangt Drive Image, dass wir sie zuerst löschen.

Nach dem nächsten Neustart ohne Diskette ist der Beweis erbracht, dass das zurückgespielte Image funktionsfähig ist. Klappt das nicht, kopieren wir unter Partition Magic die Partition C3 zurück auf die C1Win.

Bitte probieren Sie das unbedingt *an dieser Stelle* aus, damit Sie sichergehen können, dass das auf *Ihrem* System einwandfrei funktioniert, denn es ist die Grundlage für alles weitere Vorgehen.
Wenn es klappt, dürfte sich eigentlich ein gewisser AHA-Effekt einstellen.

Tipp: Wenn das System viele und "schwierige" Hardwarekomponenten enthält, empfiehlt es sich, zuerst nur das Grundsystem einzurichten und dann bereits die 1. Sicherung der C1WIN mit Drive Image (Ghost) auf einem externen Datenträger durchzuführen. Das gleiche gilt für entsprechend "haarige" Software-Installationen. Denken Sie auch an die Dokumentation, damit Sie hinterher noch wissen, welche Windows-Version mit welchem Entwicklungsstand auf welchem Image gesichert ist. Uns ist es mehrmals passiert, dass wir es nicht mehr wussten. Am besten legt man sich für jeden PC einen Aktenordner an. In den kommt auch das oben beschriebene `Papier-Log´.

Windows-Einrichtung: Ein Mehr-Stufen-Plan

Als nächstes richten wir uns unser Windows (immer noch C1WIN) "häuslich ein", installieren die bevorzugte Software (allesamt auf "E:"; als Arbeitsverzeichnis immer ein Verzeichnis in "G:" angeben!) und arbeiten eine Weile mit den Programmen, setzen benötigte Einstellungen etc. Währenddessen haben sich die Anwendungsprogramme auch ausreichend in der Registry verewigt. Wenn alles zur Zufriedenheit läuft, erstellen wir ein weiteres Image. Wichtig: Gut und aussagekräftig beschriften! Es sollte aus der Beschriftung zu ersehen sein, von welchem PC (falls man mehrere betreut) das Image stammt; vor oder nach welcher Installation, also aus welchem Anlass es erstellt wurde und natürlich das Datum und ggf. die Uhrzeit.
Falls Windows nach einer der Installationen crasht, wird das lt. Installationslog letzte Image zurückgespielt, und alles sollte wieder in Butter sein.

Zur Erinnerung: wir sichern jeweils nur die aktive primäre Partition, also die Partition, die aktuell den Buchstaben C: erhalten hat und die aktuelle Windows-Konfiguration enthält. Die *Daten* , also Word-; Excel-; Audio ...- und andere Dateien, werden wie üblich auf externe Medien gesichert. Die Programmpartition braucht nur nach jeder Programminstallation gesichert zu werden.

Leider gibt es Programme, die Daten in ihre Installation- und deren Unterverzeichnisse schreiben. Mit einer Dateisuche im Explorer (Laufwerk E:\; alle Dateien (*.*); nicht älter als 1 Tag nach der letzten Installation) lassen sich diese Dateien aber schnell finden und ggf. in den Sicherungslauf mit einbinden.

Internet - aber sicher !

Für den Sicherheitsfanatiker kommt jetzt die Kür, mit dem Ziel, für die Internet-Arbeit ein eigenes Windows zur Verfügung zu haben. Breitet sich hierin ein Virus oder Wurm aus, so bleibt er zunächst auf das `Internet-Windows´ beschränkt. Natürlich kann der Grund, ein zweites Windows zur Verfügung zu haben, auch ein anderer sein; etwa der häufiger Programmtests mit Beta-Software.

Nach dem Start von der Bootdiskette verstecken wir die bis jetzt aktive Partition C1WIN und aktivieren C2INTERNET (Damit findet auch Name seine Erklärung). Nach einem Neustart von Platte richten wir den Internet-Zugang und evtl. die benötigte Internet-Software ein. Diese wird ausnahmsweise nicht auf E:, sondern auf der Betriebssystempartition selbst installiert. (Mit der üblichen Vorgabe C:\Programme). Hier kann man sogar auf gewisse Hardware verzichten (die Treiber für die TV-Karte etwa braucht man auch nicht, während man im Internet unterwegs ist.)
Die anschließende Sicherung ist nun schon halbwegs Routine. Nicht vergessen zu notieren, welche Sicherung welchen Installationsstand widerspiegelt, und zwar im Papier-Installationslog.

Rekapitulieren wir, was haben wir bis jetzt? Auf drei primären Partitionen (C1WIN, C2INTERNET und C3TEST) stehen komplette Windows-Installationen, mit den entsprechenden Partitions-Images auf externem Datenträger gesichert, außerdem ein oder mehrere Images der Windows-Grundinstallation in verschiedenen Stadien. Weiterhin ist die Festplatte so organisiert, dass sich auf F: die Programme, auf G: die Daten befinden und auf E: die Internet-Daten. Die Bezeichnung `Firewall´ für E: wird gleich klar werden.

Für das weitere Vorgehen wird ein Bootmanager benötigt, der in Abhängigkeit von der Auswahl des zu startenden Betriebssystems jeweils logische Partitionen verstecken oder sichtbar machen kann; etwa Vamos (Shareware) oder System Commander. Die Installation und die Arbeit damit wird hier nicht näher beschrieben. Es lässt sich auch der in Partition Magic integrierte Bootmanager verwenden, allerdings ist dieser nicht sonderlich komfortabel.
Es sollen für die verschiedenen Aktivitäten 3 unterschiedliche Windows-Versionen gestartet werden können:

- Für die normale Arbeit C1WIN
- Zum Surfen C2INTERNET
- Für Testinstallationen C3TEST

Das versetzt uns in die Lage, den in letzter Zeit zunehmend raffinierteren Online-Attacken und Sicherheitsproblemen durch die Internet-Nutzung sehr wirksam zu begegnen. Nach Testinstallationen wird C3TEST durch sein Sicherungsimage überschrieben, so dass es wieder komplett `sauber´ ist.

Da die Auswahl der Bootpartition über die Sichtbarkeit gesteuert wird (zur Erinnerung: es darf nur immer eine primäre Partition sichtbar sein, von der dann auch gebootet wird), müssen für den Wechsel des Betriebssystems die gewünschte Partition sichtbar und die anderen versteckt geschaltet werden.

Das Prinzip ist wie folgt: Es werden nur die jeweils für eine der beiden Konfigurationen benötigten Partitionen sichtbar geschaltet, die gerade erforderlich sind,

- Für die normale Arbeit sichtbar sind:
  C1WIN; E_FIREWALL; F:PROGRAMM; G_DATEN
- Für das Surfen im Internet:
  C2INTERNET; E_FIREWALL
- Für Testinstallationen:
  C3TEST;

Die beiden anderen, F_PROGRAMM und G_DATEN, setzen wir im "Internetbetrieb" unsichtbar. Da sie hinter E_FIREWALL liegen, bleibt dieser der gleiche Laufwerksbuchstabe zugeordnet, was ansonsten nicht der Fall wäre. Das ist auch der Grund, weshalb die Partitionen genau in dieser Art angelegt und verwendet werden mussten.

Der Clou hierbei ist, dass alle Attacken aus dem Internet, sei es in der Form von Trojanischen Pferden, Passwortspionen, Viren etc. ihren Einfluss nur auf die sichtbaren Partitionen ausüben können, keinesfalls jedoch auf unser "normales Arbeits-Windows" (in C1WIN) und ebenfalls nicht auf unsere Programminstallationen (in F_PROGRAMME) oder unsere Daten (in G_DATEN). Alle Daten aus dem Internet werden auf E_FIREWALL abgelegt, sind damit auch in der normalen Arbeitskonfiguration zugänglich und können mit entsprechenden (Antiviren- etc.)-Programmen unter die Lupe genommen werden. Allerdings ist uns das Internet-Windows (auf C2INTERNET) während der Arbeit mit der normalen Arbeitskonfiguration verschlossen, da immer nur eine primäre Partition sichtbar sein darf. Wollen wir hier dran, etwa für Virenscans in "inaktivem Zustand" (natürlich kann man auch auf dem Internet-Windows einen Virenscanner installieren, für gewöhnlich dürfte das auch ausreichen) so müssen wir diese Partition erst in eine der logischen Partitionen hinter G_DATEN hineinkopieren, diese sichtbar machen, und nach einem Neustart von Windows haben wir dann Zugriff darauf. Ein wenig umständlich ist das schon, aber eben auch sehr sicher.

Der Bootmanager muss jetzt so konfiguriert werden, dass für die verschiedenen Einsatzzwecke die oben aufgelisteten Partitionen sichtbar und jeweils alle anderen versteckt sind. Alternativ kann man auch Partition Magic dazu verwenden, aber das ist bei häufigem Wechsel der Arbeitsumgebung recht unkomfortabel.

Programminstallationen oder der Einbau neuer Hardware laufen jetzt nach folgendem Schema ab:
Alle Änderungen, die wir an Windows und der Konfiguration vornehmen, werden notiert. Wenn wir jetzt eine neue Software installieren wollen, gehen wir so vor, dass wir zunächst die letzte Sicherung wieder einspielen. Anschließend werden alle Konfigurationsänderungen, die nach dieser Sicherung am System vorgenommen wurden, nachgetragen. (Das hat den Sinn, die sonstigen, von den Programmen inzwischen vorgenommenen Änderungen [aufgeblähte Registry] nicht mit zu übernehmen). Den nunmehr auf der Basis einer "sauberen" Konfiguration erreichten neuen Zwischenstand sichern wir jetzt wiederum.

Danach installieren wir das zu testende Programm und testen es. Ist alles o.k., wird die letzte Prozedur wiederholt, also letzten Zwischenstand einspielen, Programm neu installieren (damit der "Müll" draußen bleibt) und erneut Zwischenzustand sichern; übrigens in einem neuen Image, nicht das alte überschreiben, das wird eventuell noch gebraucht, wenn sich das neu in das System eingeführte Programm doch nicht als so ideal herausstellt und man es gerne wieder loswerden möchte.
Gleichermaßen ist erkennbar, dass die Arbeit an den Windows-Konfigurationen nunmehr einer gewissen Planung und Überlegung bedarf. Das hört sich alles nach Arbeit an; ist es auch, es lohnt sich aber, denn, oh Wunder:

Der Windows-GAU hat seine Schrecken verloren

Denn was machen wir dann? Der lt. Installationslog (darum!) letzte Zwischenstand wird zurückgespielt; die Windows-Partition also wie oben geprobt aus dem Image wieder hergestellt, und das war es; das System funktioniert, als wäre nichts gewesen. Oftmals ausprobiert (gezwungenermaßen), immer wieder gestaunt, dass es wirklich so ist.

Also kann uns jetzt überhaupt nichts mehr passieren mit unserem Windows?
So einfach ist das natürlich nicht. Wir haben uns jetzt abgesichert gegen die typischen Windows-Ausfälle. Aber es kann ja auch etwas anderes ausfallen: zum Beispiel die Festplatte. Und Daten-Backups vergisst man ja gerne ... Übrigens: Wer braucht schon Backups? Eigentlich braucht man im Falle eines Falles nur ein Restore ...

Hier noch ein ketzerischer Gedanke für alle Anwender, die glauben, mit einer Sicherung auf eine zweite Festplatte hätten sie das große Los der Datensicherung gezogen:
Stellen Sie sich einmal vor, das Netzteil Ihres PC spielt verrückt und gibt etwa mal 12 Volt auf die 5-Volt-Leitung. Dann ist natürlich einiges hinüber; unter anderem vermutlich auch *beide* Festplatten und damit alle Ihre Datensicherungen. Oder man stößt in der Hektik der Examens- oder sonstigen Arbeit gegen den Tower, und der fällt unsanft auf seine Seitenfläche. Das kann im Betrieb durchaus reichen, um den Festplatten den Garaus zu machen. **Merke:** Ein richtiges Backup wird *immer* auf einen externen Datenträger durchgeführt.

Wir sind jetzt in der Lage, dem "ganz normalen Windows-Alltags-Wahnsinn" ein ganzes Stück gelassener entgegenzusehen. Halbtägige Neuinstallations-Marathons gehören ab sofort der Vergangenheit an (es sei denn, Sie verwirbeln gehörig Ihre Hardware oder sonst etwas Größeres passiert).

Kein Vorteil ohne Nachteile, alles hat seine Grenzen

Die Grenzen unseres Verfahrens liegen dort, wo nicht einzelne große, sondern viele kleine Änderungen rückgängig gemacht werden müssen. Für diesen Zweck wäre es nötig, nach jeder Änderung eine Sicherung anzulegen, was zu einer Unzahl von Sicherungen mit entsprechendem Platzbedarf führen würde. Für diesen Zweck eignen sich gute Deinstallationstools besser; geht

mal wirklich etwas daneben, arbeitet man ja noch mit "Netz und doppeltem Boden".

Auch ersetzt dieses Verfahren nicht die Sorgfalt, die man bezüglich Viren, Trojanischen Pferden, Internet-Attacken und sonstigem Ungemach an den Tag legen sollte. Ein, besser zwei gute und aktuell gehaltene Virenscanner, sowie eine gute Firewall, etwa Zone Alarm oder die Norton Firewall, gehören heutigentags zu einem PC einfach dazu.

Spielen und Testen ohne Nebenwirkungen

Mit Nebenwirkung meinen wir natürlich solche auf andere Partitionen; Nebenwirkungen exzessiver Spielsucht auf den Menschen sind nicht Gegenteil unserer Betrachtung ...Wir können ohne weiteres neben der Arbeits- und der Internetkonfiguration noch eine für Spiele oder Tests anlegen. Es ist ja noch eine primäre Partition frei (C3TEST), die sich hierfür benutzen lässt. Als Programmpartition verwenden wir F1PROGTEST. Wie immer werden die unbenutzten Partitionen versteckt. Sowohl die Arbeits- als auch die Internetkonfiguration sind daher nicht zugänglich und können durch den "Spielbetrieb" auch nicht gestört werden.

Tipp: Wenn man mehrere Versionen von Windows auf einem System fährt (etwa 95 und NT; auch dazu eignet sich dieses Verfahren ja ausgezeichnet), wird man es lästig finden, dass man jedes Mal alle Anwendungsprogramme neu installieren muss und diese dann den doppelten Platz auf der Platte belegen. Um die doppelte Installation kommt man zwar nicht herum, aber den doppelten Platz kann man sparen, indem man die Programme beim zweiten Mal in die gleichen Verzeichnisse wie zuvor installiert. Die Registry und das Systemverzeichnis werden aktualisiert, aber die Programmdaten überschreiben die bereits vorhandenen und belegen so keinen doppelten Platz. Wichtig ist, dass man jeweils genau die gleichen Programmkonfigurationen und -Optionen installiert.

Anhang:

Beispiel für den Aufbau der Startdateien CONFIG.SYS und AUTOEXEC.BAT einer Bootdiskette (zugrundeliegendes System Win 95 C). Die entsprechenden Programmdateien müssen natürlich auf der Startdiskette vorhanden sein, für den DOS-Editor außerdem EDIT.COM und QBASIC.EXE.
Aus Platzgründen (DOS kann ja nur 640 KB benutzen und EMM386 (s. Kommentar) wird es schnell eng im Speicher) werden keine FAT32-Treiber geladen. Partiton Magic und Drive Image macht das nichts aus; sie haben ihre eigenen Routinen im Zugriff auf die verschiedenen Dateisysteme, aber man kann natürlich mit dem geladenen DOS nicht auf FAT32-Partitionen zugreifen.

Config.sys:

```
DEVICE=HIMEM.SYS
rem Drive Image und Partition Magic mögen nicht
gerne EMM386;
rem sagt das Handbuch, deshalb ohne starten.
rem device=EMM386.EXE noems  novcpi verbose
DOS=HIGH,UMB

REM Treiber für IDE-CD-ROM; Universaltreiber
von WIN-95-CD
device=sample.sys /d:CD1

REM ggf. Treiber für SCSI-Controller hier
einfügen

REM ggf. Treiber für SCSI-CD-ROM hier einfügen
rem ggf. weitere Treiber, etwa für MO-Laufwerke
rem Tastaturtreiber
country=049,437,country.sys

files=20
buffers=30
lastdrive=w
break on
stacks=9,256
```

Autoexec.bat

```
@ECHO OFF
PROMPT $P$G

REM Smartdrive beschleunigt u.U. das Erstellen
von Images unter
REM Drive Image erheblich; ausprobieren.
REM Nicht verwendete Laufwerksbuchstaben weg-
lassen
LH smartdrv.exe a+ c+ d+ e+ f+ g+ h+ i+ j+  /V
4096 4096
LH keyb gr,,keyboard.sys
REM Erlaubt die komfortable Editierung der
Kommandozeile
LOADHIGH DOSKEY /INSERT
loadhigh \mscdex /D:CD1 /L:O
PATH=A:\
set dircmd=/p /o:gn
BREAK ON
VERIFY ON
REM Möglichst kleinen Maustreiber verwenden
MOUSE
REM Das ist der Packet-CD-Treiber von Drive
Image
PQPACKET
```

Alleine am Computer?

Lieber Kontakte schließen,
Informationen austauschen
und gemeinsam Projekte
realisieren im AUGE e.V., dem
Verein der Computeranwender!

Besuchen Sie unsere
Webseiten im Internet
unter

http://www.auge.de/

AUGE e.V. - Bessere Ideen.

Strom aus der Steckdose – oder woher sonst?

Hintergründe zu möglichen Störungen aus dem Stromnetz und wie man ihnen begegnet

Auszug aus einer Broschüre der Rotronic AG, ein Partner der Firma APC

Qualität der Stromversorgung

Das elektronische Zeitalter hat uns zwei unangenehme Wahrheiten gelehrt:

• Die Versorgungsunternehmen können den sauberen, gleichmäßigen Strom nicht liefern, den die empfindlichen elektronischen Geräte verlangen.

• Im Endeffekt ist der Kunde für den sicheren Betrieb seiner Geräte selbst verantwortlich.

Was besagt die Norm über die Netzqualität?

In der VDE-Norm 0558 Teil 5 sind die Grenzwerte für Spannung und Strom des öffentlichen Stromnetzes festgelegt. Jedoch gibt es keine Angaben bezüglich Art und Zahl zulässiger Störungen. Eine qualitativ hochwertige Stromversorgung weist nur eine sehr geringe Anzahl von Netzstörungen mit nur geringen Auswirkungen auf die Funktionen der angeschlossenen Verbraucher auf.

Wie sieht es international aus und wie sehen die Bedürfnisse an den Stromlieferanten aus?

Die Qualität der Stromversorgung ist im internationalen Vergleich in Mitteleuropa recht gut. Doch gibt es national große Unterschiede. Die zunehmende Anzahl Verbraucher mit geringer Toleranz gegenüber Netzstörungen und mit teilweiser großer Rückwirkung auf das Netz nehmen stetig zu, was zur Verschärfung der Anforderungen an die Stromqualität führt.

Was sagen die Elektrizitätswerke bezüglich Netzqualität und Verfügbarkeit?

Das Elektrizitätswerk liefert die Energie in der Regel ununterbrochen, innerhalb der üblichen Toleranzen für Spannung und Frequenz gemäss der Schweizer Norm (Regeln für genormte Werte der Spannungen, Ströme und Frequenzen); vorbehalten bleiben Ausnahmebestimmungen wie Einwirkung von Dritten sowie höhere Gewalt. Die Kunden haben von sich aus alle nötigen Vorkehrungen zu treffen, um in ihren Anlagen Schäden oder Unfälle zu verhüten, die durch Energieunterbruch, Wiedereinschaltung, den Betrieb von Rundsteueranlagen sowie aus Spannungs- und Frequenzschwankungen und Oberwellengehalt im Netz entstehen können.

Und wie sieht es in Zukunft aus um unsere Stromversorgung?

Es ist damit zu rechnen, dass bei uns die Qualität des Produktes Energie verringert wird, um mit Anbietern aus anderen Versorgungsgebieten erfolgreich konkurrieren zu können. Stromversorger in deregulierten Märkten haben bereits begonnen, Stromqualitäten den individuellen Bedürfnissen des Kunden entsprechend anzubieten. Es ist damit zu rechnen, dass die heutige Versorgungssicherheit für den Normalverbraucher nicht gehalten werden kann.

Wo und wie häufig treten Fehler in der Stromversorgung auf?

• Die Zuverlässigkeit im Mittelspannungsnetz ist um eine Größenordnung besser als im Niederspannungsnetz.

• Die meisten Fehler treten mit einer Dauer unter 3 Sek. auf.

• Nur wenige Fehler liegen im Zeitraum zwischen 3 Sekunden und 15 Minuten.

Untersuchungen, die im Auftrag des National Power Laboratory in den USA durchgeführt wurden, kommen zu ähnlichen Ergebnissen.

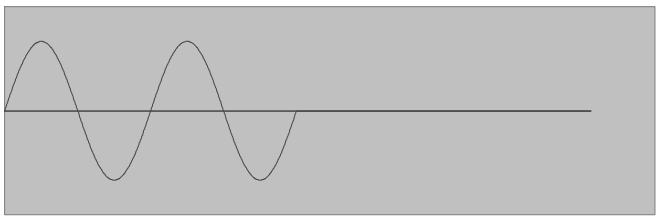
Was für Fehler treten am meisten auf?

Stromausfall/Überspannung: 45,3 %
Sturmschäden: 9,4 %
Brand oder Explosion: 8,2 %
Hardware-/Softwarefehler: 8,2 %
Überschwemmungen/Wasserschäden: 6,7 %
Erdbeben: 5,5 %
Netzwerkausfall: 5,5 %
Menschliches Versagen/Sabotage: 3,2 %
Ausfall von Hochspannungsleitungen: 2,3 %
Andere Ursachen: 6,7 %
Quelle: National Power Laboratory, USA

Störungsarten und deren Auswirkungen

Stromausfall (Power Failure & Momentary Interruption)

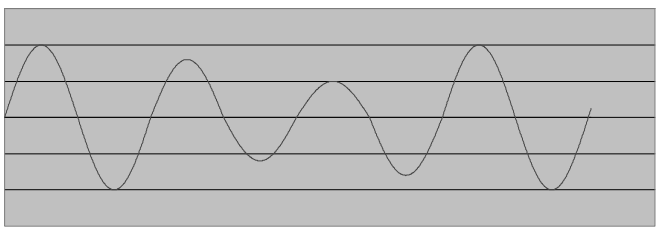
Netzunterbrüche werden in zwei Klassen eingeteilt. Lang- und kurzfristiger Spannungsverlust für mehr als 5 Min. oder kleiner als 5 Min. jedoch größer als wenige Millisekunden. Verursacht durch Unwetter, Schalthandlungen im Netz, Kurzschlüsse. Angeschlossene Verbraucher werden unkon-



trolliert abgeschaltet. Es können hohe wirtschaftliche Kosten entstehen. Menschen können verletzt werden, Umweltschäden entstehen, Sachanlagen beschädigt oder gänzlich zerstört werden.

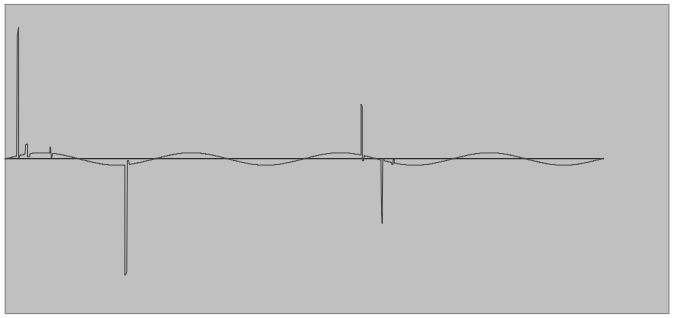
Spannungseinbruch (Power Sag)

Spannung unterhalb der zulässigen Grenzen für einen Teil einer Periode bis zu einer Dauer von mehreren Perioden oder Sekunden. Verursacht durch Überbelastung des Netzes. Eine kurze Absenkung der Netzspannung führt in den meisten Fällen zu keinen Problemen. Eine länger andauernde

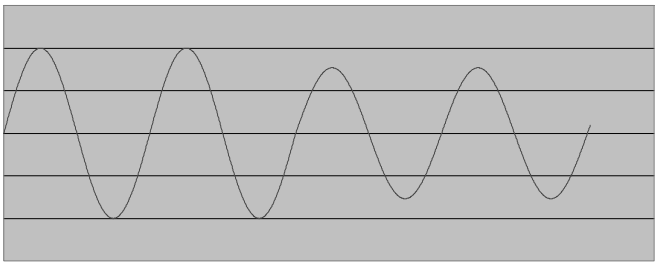


Unterspannung führt bei Verbrauchern mit konstantem Leistungsbedarf zu erhöhter Stromaufnahme und dadurch möglicherweise zu unzulässiger Erwärmung.

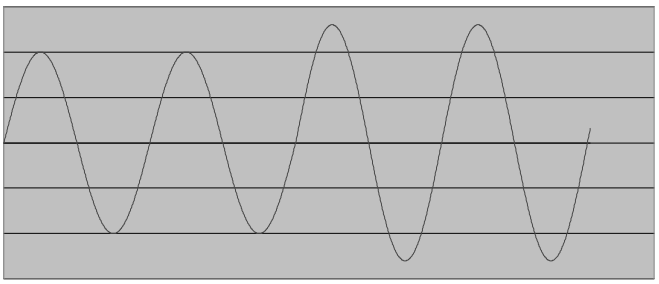
Spannungsstösse (Power Surge incl. Spike)
Spannungspulse sehr kurzer Dauer (Millisekunden) bis zu einigen 100 V über Nominalwert. Verursacht durch Blitzeinschläge im Freileitungsnetz, Gleich- und Wechselrichter, Kurzschlüsse oder Abschalten sehr großer Lasten (Motoren etc.). Hochspannungsspitzen führen zur Zerstörung von Elektronik-Komponenten oder zu unkontrollierbaren Arbeitsprozessabläufen.



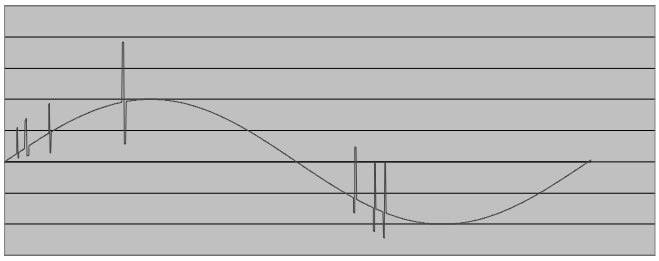
Unterspannung (Undervoltage / Brownout)
Spannung unterhalb der zulässigen Grenzen für einen Teil einer Periode bis zu einer Dauer von mehreren Perioden oder Sekunden. Verursacht durch Überbelastung des Netzes. Eine kurze Absenkung der Netzspannung führt in den meisten Fällen zu keinen Problemen. Eine länger andauernde Unterspannung führt bei Verbrauchern mit konstantem Leistungsbedarf zu erhöhter Stromaufnahme und dadurch möglicherweise zu unzulässiger Erwärmung.



Überspannung (Overvoltage)
Erhöhung der Spannung über den zulässigen Grenzwert für einige Sekunden oder länger beziehungsweise dauernd. Verursacht durch Unterbelastung des Netzes. Überspannung verursacht eine Sättigung bei magnetischen Bauelementen. Die nichtlineare Charakteristik führt zu drastisch erhöhter Stromaufnahme und bei längerer Dauer zu Überhitzung, teilweise bis zur Zerstörung.

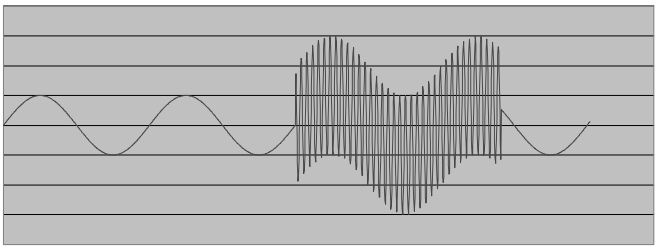


Schaltspitzen (Switching Transients Notch)
Spannungspulse sehr kurzer Dauer (Millisekunden) und Spannungsspitzen und -einbrüche. Verursacht durch Laständerungen (z.B. Anlaufen eines Fahrstuhls).Transienten führen zu einer Belastung eventuell Zerstörung von Komponenten, elektronische Steuerungen können in einen



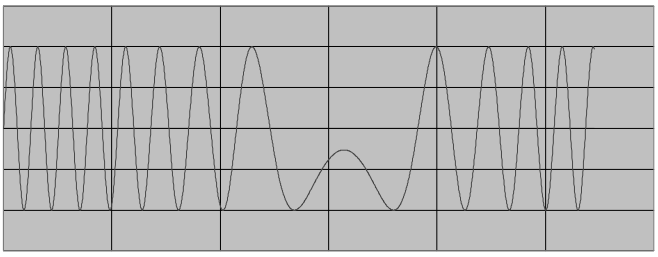
unkontrollierten Zustand kommen, Rechner blockieren, Netzwerke sowie Signalübertragungskreise können beeinträchtigt werden.

Störspannungen (Line Noise)
Unregelmäßige (stochastische) Veränderungen von Spannung und Strom mit kleiner Amplitude. Verursacht durch schlechte

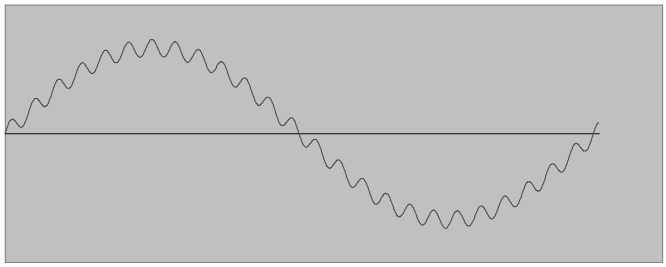


Steckverbindungen und HF-Einstreuungen durch die Luft (Radio- & Fernsehsender). Rauschen kann EDV-Netze beeinträchtigen. Datensätze können nicht richtig gelesen oder wiedergeben werden.

Frequenzschwankungen (Frequency Variations)
Abweichungen der Frequenz um mehr als das zulässige Mass. Verursacht durch den Einsatz von Netzersatzanlagen, z.B. Generatoren. Frequenzschwankungen führen zu Problemen mit netzfrequenzabhängigen Geräten. Netzteile oder Geräte können zu Fehlfunktionen und oder Überhitzung führen.

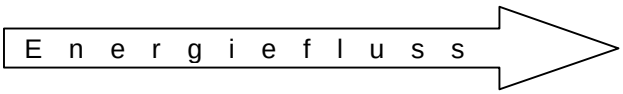


Harmonische Oberwellen (Harmonic Distortion)
Andauernde periodische Spannungsveränderungen unabhängig von der Netzfrequenz, normalerweise ein Mehrfaches der Netzfrequenz. Verursacht durch Gleich- und Wechselrichter, getaktete Netzteile. Oberwellen können elektrische



und elektronische Geräte beeinträchtigen, die Lebensdauer von Motoren kann sich infolge Überhitzung wesentlich verkürzen.

Klassische USV - Technologien



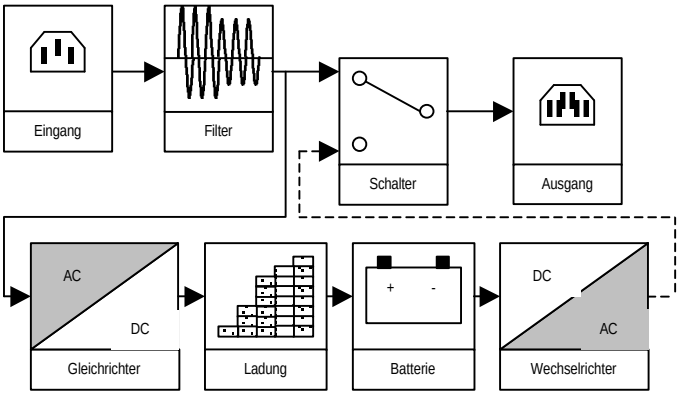
Off - Line USV

Geräte dieser Kategorie sind immer 1-phasig und werden bis zu einer Leistung von ca. 1 kVA gebaut.

Netzversorgungs-Betrieb
Der Eingang wird direkt, das heißt nur über Entstör- und Überspannungsfiltern, mit dem Ausgang verbunden. Gleichzeitig werden die Batterien über ein Ladeteil geladen.

Batterieversorgungs-Betrieb
Ist die Netzversorgung nicht mehr vorhanden oder ist sie außerhalb der Toleranz, wird der Ausgang via Wechselrichter von einer Batterie versorgt. Die Umschaltzeit zwischen Netzversorgungs- und Batterie-Betrieb beträgt in der Regel 4–10 ms. Die Ausgangsspannungs-Kurvenform entspricht einem abgestuften Sinus.

Vorteil dieser Technologie
Klein, günstig, kompakt, hoher Wirkungsgrad, für einfachste Anwendungen einsetzbar, wo nur reiner Stromausfall gesichert werden soll und die relativ große Umschaltzeit keine Rolle spielt.



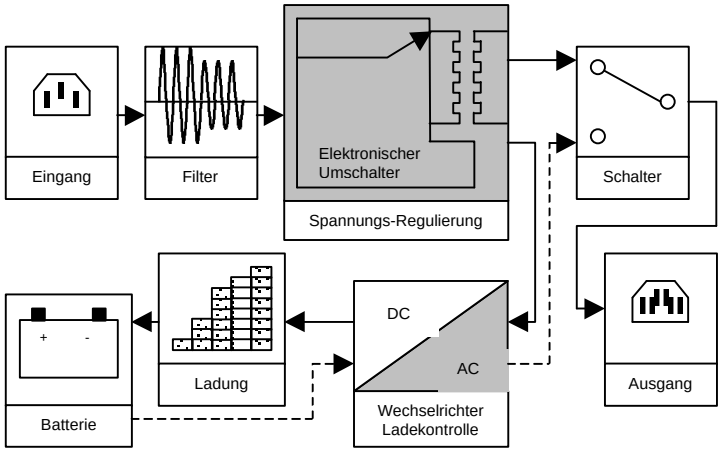
Line - Interactive USV

Geräte dieser Kategorie sind eigentlich im 1-phasigen Bereich. Sie werden bis zu einer Leistung von ca. 5 kVA gebaut.

Netzversorgungs-Betrieb
Der Eingang wird direkt, das heißt über Entstör- und Überspannungsfilter, einer Spannungsregulierungs-Einheit (Powerconditioning) mit dem Ausgang verbunden. Gleichzeitig werden die Batterien über den umgekehrt betriebenen Wechselrichter aufgeladen.

Batterieversorgungs-Betrieb
Ist die Netzversorgung nicht mehr vorhanden oder ist sie außerhalb der vom Gerätehersteller zulässigen Toleranz wird der Ausgang via Wechselrichter von einer Batterie versorgt. Die Umschaltzeit zwischen Netzversorgungs- und Batteriebetrieb beträgt in der Regel 2 – 4 ms. Die Ausgangsspannungs-Kurvenform kann je nach Produkt einem abgestuften Sinus oder einem reinen harmonischen Sinus entsprechen.

Vorteil dieser Technologie
Preiswert, kompakt, hoher Wirkungsgrad, für alle Anwendungen einsetzbar, wo kleinere Spannungsschwankungen sowie natürliche Frequenzschwankungen keine Rolle spielen.



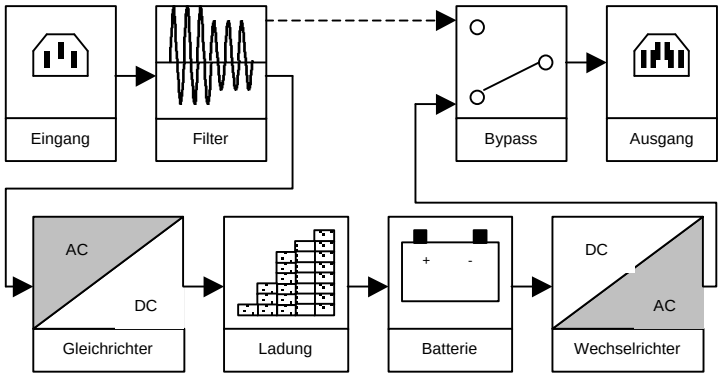
On - Line USV

Geräte dieser Kategorie sind 1-phasig und 3-phasig erhältlich und werden in der Regel ab ca. 500 VA gebaut.

Netzversorgungs-Betrieb
Der Eingang formt die Netzspannung in eine Gleichspannung für die Ladung der Batterie und für die Versorgung des Wechselrichters um, die Batterie steht im Bereitschaftsparallelbetrieb. Der Wechselrichter erzeugt aus der Gleichspannung eine sinusförmige Wechselspannung und führt diese dem Ausgang zu.

Batterieversorgungs-Betrieb
Ist die Netzversorgung nicht mehr vorhanden oder ist sie außerhalb der vom Gerätehersteller zulässigen Toleranz, wird der Ausgang via Wechselrichter von einer Batterie unterbrechungsfrei weiter versorgt.

Vorteil dieser Technologie
Keine Spannungs- und Frequenzschwankungen, für alle Anwendungen einsetzbar, wo dies verlangt wird.



Alleine am Computer?

Lieber Kontakte schließen,
Informationen austauschen
und gemeinsam Projekte
realisieren im AUGE e.V., dem
Verein der Computeranwender!

Besuchen Sie unsere
Webseiten im Internet
unter

http://www.auge.de/

AUGE e.V. - Bessere Ideen.

Sicherheit im Internet

Bericht vom RG Treffen in Stuttgart
Michael Schäl (M6115)

Thema des Abends war die Sicherheit im Internet. Speziell wollten wir uns mit der Absicherung des eigenen PC gegenüber anderen Benutzern im Internet befassen. Unsere einfachen Experimente sollten sich dabei weniger an IT-Sicherheitsexperten wenden, als vielmehr an den interessierten Computeranwender.

Wir wollten feststellen, wie schwer (oder einfach) es ist, fremde Rechner im Internet auszuspionieren. Um eine Demonstration der Möglichkeiten zu bieten, haben wir uns zunächst bewusst auf ganz primitive Methoden beschränkt. Wohl auch auf Grund seiner Verbreitung ist das Windows Betriebssystem mit allen seinen Varianten ein beliebtes Angriffsziel. Es gibt im Internet unzählige Tools, die es einem Angreifer erleichtern, sich Zugang zu fremden Rechnern zu verschaffen. Aber oft ist es gar nicht nötig, zu solchen Tools zu greifen. Durch die Ahnungslosigkeit der Benutzer stehen oft Tore und Türen offen. Und das kommt durchaus auch bei Mitgliedern unseres Vereins vor!

Die vielfältigen Möglichkeiten der modernen Computersoftware machen es fast unmöglich, genau zu wissen, was die eine oder andere Software auf dem Rechner tut. Deshalb ist es notwendig, sich die Vorgänge bei der Internet-Nutzung einmal klar zu machen. Das haben wir in einem einfachen Modell versucht.

Vernetzungsprinzip

Das Internet beruht auf einem gemeinsamen Netzwerkprotokoll, dem TCP/IP. Über dieses Protokoll werden alle Dienste abgewickelt. Dazu werden Verbindungen über verschiedene Medien aufgebaut. Beim normalen Heimcomputer ist das üblicherweise das Modem, aber auch eine ISDN-Verbindung oder DSL. Eine Anbindung über Ethernet ist eher im Profibereich üblich. Aber auch eine Kombination aus mehreren Verbindungen ist denkbar (z.B. ein eigener Router zum ISDN, der über Ethernet mit dem Rechner verbunden ist).

Man muss sich klar machen, dass es für eine Nutzung des Internet völlig unerheblich ist, wie die Anbindung erfolgt. Niemand kann auch genau sagen, wie die Daten zum Zielrechner gelangen. Es können auf der Strecke die unterschiedlichsten Übertragungswege genutzt werden. Funk- und Satellitenstrecken, Laser-Richtstrecken, Telefonstrecken, Glasfaserkabel, ATM, Ethernet, Token Ring, Frame-Relay und sonstige Datenkabel nach verschiedensten Normen. Allen gemeinsam ist nur eines: sie transportieren die Daten im TCP/IP.

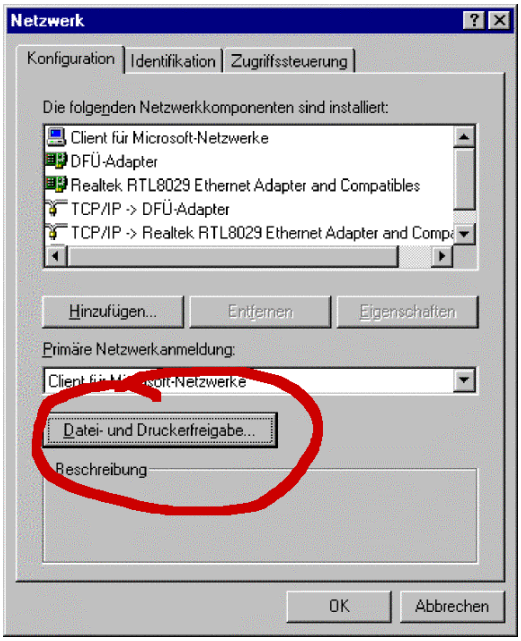
Musternetzwerk

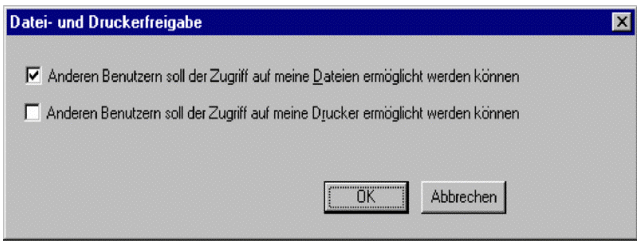
Um unsere einfachen Versuche durchzuführen, haben wir einige Rechner aufgebaut und mit Ethernet über einen Hub verbunden. Neben Windows hatten wir auch einen Macintosh (MacOS 9) und ein UNIX (Mac OS X = BSD UNIX) im Netz. Eine Internetverbindung stand uns leider nicht zur Verfügung. Das war aber auch nicht nötig. Denn eine Verbindung zwischen zwei PC auf dem heimischen Schreibtisch ist nichts anderes als die Verbindung zu einem Webserver wie www.auge.de.

Was kann man sehen?

Damit sind wir auch schon bei der ersten Sicherheitslücke. Selbst langjährige Computernutzer haben es sich oft nicht klar gemacht, dass ihr Computer beim Surfen im Internet in ein Netzwerk eingebunden ist. Wer nur über das Modem surft, denkt oft gar nicht an eine Vernetzung. Aber noch schlimmer sind Spieler und Kids, die ihre Rechner über eine Netzwerkkarte mit dem Rechner eines Freundes verbinden. Dazu werden Ressourcen der Computer (Verzeichnisse, Drucker) über das Netz freigegeben. Wird dieser Rechner dann mit dem Internet verbunden, stehen diese Ressourcen auch im Internet zur Verfügung.

Beispiel: Serverdienst bei einem Win9x System starten





Diese einfache Sicherheitslücke ist kein Fehler eines Betriebssystems (Microsoft), sondern einfach Unkenntnis der Technik beim Benutzer. Einzig die Tatsache, dass in manchen Windows Versionen bei der Einrichtung der DFÜ-Verbindung die Freigabe von Ressourcen nur mit einem Klick auf OK bestätigt werden muss, ist vielleicht zu bemängeln. Auch wenn hier ein Hinweis für den Benutzer erscheint, wird er meist überlesen oder nicht verstanden. (Wer hat sich denn schon die Nutzungsbedingungen seines Windows durchgelesen?)

Um diese leichtsinnig freigegebenen Rechner im Internet zu finden, sind nur geringe Fachkenntnisse nötig. Alle Funktionen dazu bietet das Windows Betriebssystem. Besser als Win9x sind die NT Varianten (NT, W2000, W XP) geeignet. In der Regel werden dazu Befehle über die Konsole (DOS-Fenster oder Eingabeaufforderung) eingegeben.

Wie kann ich fremde Rechner im Internet sehen?

Zunächst muss ich die Adresse eines Rechners herausbekommen. Jedes System im Internet hat eine eindeutige IP-Adresse. Meist wird diese Adresse bei der Einwahl dynamisch durch den Provider vergeben. Es ist also nicht ohne weiteres festzustellen, unter welcher IP ein bestimmter Nutzer heute arbeitet. Die Methoden, um das herauszufinden, haben uns zunächst nicht interessiert.

Es ist aber möglich, durch Probieren einen beliebigen Rechner zu finden. Ein gängiges Mittel dazu ist der *PING* Befehl. Mit einem Ping wird die Verbindung zwischen zwei IP-Adressen und damit in der Regel zwischen zwei Computern getestet. Von der einen Seite wird ein “Ping” an eine Adresse abgeschickt. Von der anderen Seite kommt ein “Pong” als Antwort. Mit verschiedenen Parametern kann man daraus Rückschlüsse über die Verbindung ziehen.

Beispiel: der Ping Befehl

```
C:\>ping 213.198.63.236

Ping wird ausgeführt für 213.198.63.236 mit
32 Bytes Daten:

Antwort von 213.198.63.236: Bytes=32
Zeit=110ms TTL=55
Antwort von 213.198.63.236: Bytes=32
Zeit=50ms TTL=55
Antwort von 213.198.63.236: Bytes=32
Zeit=130ms TTL=55
Antwort von 213.198.63.236: Bytes=32
Zeit=50ms TTL=55
```

Dieses System hat auf die 4 Versuche mit einer Zeit zwischen 50 und 130 Millisekunden geantwortet. Es ist also unter der Adresse erreichbar.

Allerdings wäre es mühsam, einfach zu probieren. Bei theoretisch 4 Milliarden Möglichkeiten (nicht alle Kombinationen davon ergeben zulässige Adressen) könnte das lange dauern. Aber wir wissen, dass alle Provider Subnetze nutzen, einen Bereich von IP-Nummern. Deshalb können wir z.B. einfach die eigenen IP nachschauen und Rückschlüsse auf den Adressbereich ziehen.

Beispiel: IP Konfiguration anzeigen

```
C:\>ipconfig

Windows NT IP-Konfiguration

Ethernet-Adapter CEM561:

      IP-Adresse ........: 198.162.145.191
      Subnet Mask....... : 255.255.255.0
      Standard-Gateway...: 198.162.145.1
```

Alle Nutzer bei diesem Provider haben also Adressen im Bereich 198.162.145.xxx. Gültig sind alle Adressen von 1 bis 254. Es kann auch sein, dass der Provider einen erweiterten Bereich nutzt. Dann sind auch im vorhergehenden Tripel (145) andere Zahlen möglich. Für Telekom DSL Anschlüsse ist z.B. die Adresse 80.138.163.67 typisch.

Nun kann ich systematisch den Adressbereich durchprobieren. Ein einfaches Batchprogramm erleichtert die Arbeit. Es gibt auch so genannte Scanner, die das erledigen.

Was kann ich über das Internet anstellen?

Wenn man nun eine IP Adresse gefunden hat, versucht man festzustellen, ob es sich um ein Windows-System handelt und ob freigegebene Platten vorhanden sind.

Beispiel: Netzressourcen anzeigen

```
C:\>net view \\80.138.163.67
Freigegebene Ressourcen auf \\80.138.163.67

Samba 2.2.0

Name         Typ     Lokal    Beschreibung

-------------------------------------------
HP-Laser     Drucker
CDROM        Platte           CD Laufwerk
musik        Platte           MP3 Sammlung
public       Platte           public Area

Der Befehl wurde erfolgreich ausgeführt.
```

In diesem Beispiel haben wir einen Linux Rechner mit Samba gefunden. Dieses System verhält sich im wesentlichen wie ein Windows Rechner. Die Anzeige unterscheidet sich nicht. Um jetzt eine Verbindung zu diesem Rechner aufzubauen, verbinden wir die Netzwerkressource mit einem Laufwerksbuchstaben. Auch das kann man wieder mit der Kommandozeile ausführen.

Beispiel: Laufwerk verbinden über das Netz

```
C:\>net use K: \\172.17.128.33\public
```

```
Der Befehl wurde erfolgreich ausgeführt.
C:\>dir K:Datenträger in Laufwerk K: ist .
Datenträgernummer: AF79-0882

Verzeichnis von K:\

08.01.02  21:27         <DIR>.
03.03.02  20:49         <DIR>..
26.10.01  23:13    4.948.640 wmencoder71.exe
29.10.01  14:38         <DIR>Terratec
29.10.01  14:38         <DIR>Logitech
29.10.01  14:39         <DIR>Philips
29.10.01  14:39     <DIR>QuickTimeCDInstaller
               7 Datei(en)    4.948.640 Bytes
                    1.190.264.832 Bytes frei
```

Und schon haben wir vollen Zugriff auf dieses Verzeichnis - zumindest zum Lesen der Daten. Ob wir auch schreiben dürfen, hängt von den erteilten Rechten ab. Ein Win9x System kann nicht so detailliert Rechte vergeben wie ein Windows NT.

Sicherheitshinweis:

Freigaben immer mit einem Passwort versehen

Die Sicherheit für diese Verzeichnisse erhöht sich um ein Vielfaches, wenn für den Zugriff auf diese Verzeichnisse ein Passwort vergeben wird. Damit würde beim net use Befehl eine Abfrage nach dem Benutzernamen und dem Passwort erscheinen. Der durchschnittliche Computernutzer ist damit nicht mehr in der Lage, an die Daten heran zu kommen. Wie gesagt, wir haben uns nur mit sehr einfachen Sicherheitsmaßnahmen befasst. Aber wenn die Türe offensteht, kann wirklich jeder herein. Das Lesen dieser Daten wird nicht einmal als strafbar gehandelt, weil sie ja offen im Internet angeboten werden.

Unsichtbare Shares

Ein weiteres Sicherheitsloch haben wir noch auf einem anderen System gefunden. Es gibt die Möglichkeit, die Freigaben (engl. Shares) wie public oder musik aus dem Beispiel zu verstecken. Wenn ich den Freigabenamen mit einem “$” am Ende schreibe, werden diese Freigaben nicht angezeigt. Jedenfalls nicht mit normalen Bordmitteln. Das erschwert natürlich den Zugang für einen Angreifer. Wer sich mit diesen Freigaben verbinden will, muss den Namen wissen.
Aber genau hier liegt ein Sicherheitsrisiko. Windows NT und seine Nachfolger legen beim Start des Serverdienstes so genannte Administrative Freigaben an. Das sind C$ für die Platte C: und entsprechend D$ usw. für weitere Platten. Diese Freigaben sind im Netz unsichtbar. Aber sie können benutzt werden. Bei einem entsprechenden System können wir uns so den Zugang zur Platte C: verschaffen.

```
C:\>net use K: \\172.17.128.33\C$
Der Befehl wurde erfolgreich ausgeführt.
```

Auch hier gilt wieder: durch ein Passwort lässt sich der Zugang verhindern. Bei einem NT System mit NTFS formatierter Platte lässt sich neben dem Benutzernamen und dem Passwort für die Freigabe auch noch eine Berechtigung für den Plattenzugriff einrichten. Auf der Platte C: und insbesondere im Windows Verzeichnis hat niemand etwas zu suchen.

Diese Sicherheitsrisiken sind so verblüffend einfach auszunutzen, dass man es kaum glauben will. Eine kurze Suche im Internet zeigt sofort jede Menge offener Rechner. Deshalb sollte man die folgenden Sicherheitshinweise immer beachten.

Sicherheitshinweis:

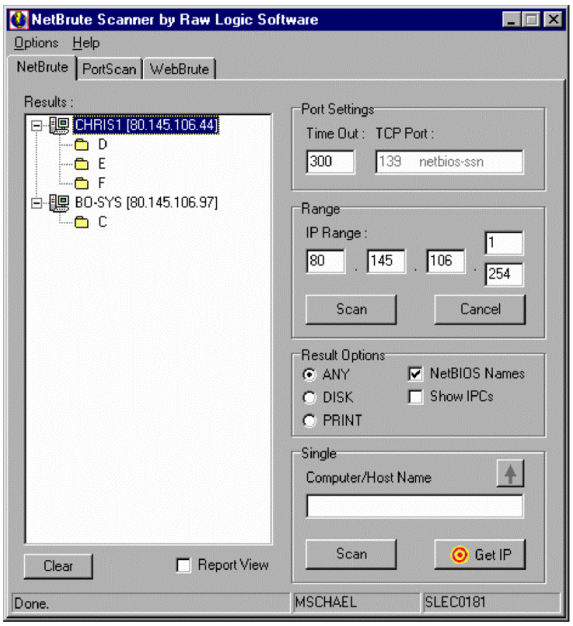
Wer ganz sicher gehen will, schaltet den Serverdienst ab, wenn er im Internet surft

Werkzeuge aus dem Internet

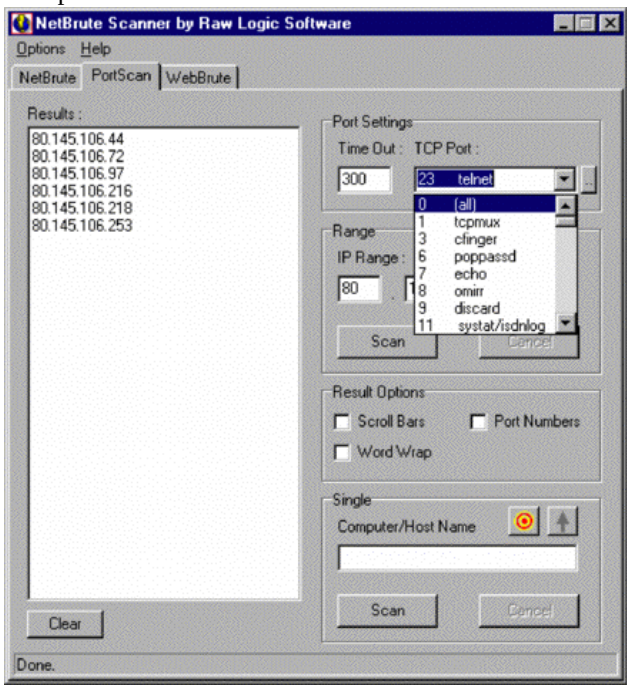
Richtige Hacker haben aber noch viel bessere Möglichkeiten. Inzwischen gibt es im Internet etliche Tools, um die verschiedensten Rechner auszuspionieren. Solche Werkzeuge kann man natürlich auch einsetzen, um das eigene System zu testen. Auf unserem Treffen haben wir zwei dieser Tools ausprobiert.

NetBrute ist ein so genannter Scanner. Das Programm kann ganze IP Bereiche nach Rechnern durchsuchen. Dabei benutzt es nicht nur den oben genannten Ping Befehl, auch als ICMP Test bezeichnet, sondern versucht mit einem Portscan herauszubekommen, welche Dienste auf einem Rechner laufen. Jeder Webserver kommuniziert unter seiner Webadresse über den Port 80 mit der Außenwelt. Weitere Ports werden von den Diensten wie FTP, DNS oder Telnet benutzt. Auch NetBIOS, das für das Windows Netzwerk Verwendung findet, benutzt solche Ports. Und so können auch im Internet Windows-Rechner entdeckt werden.

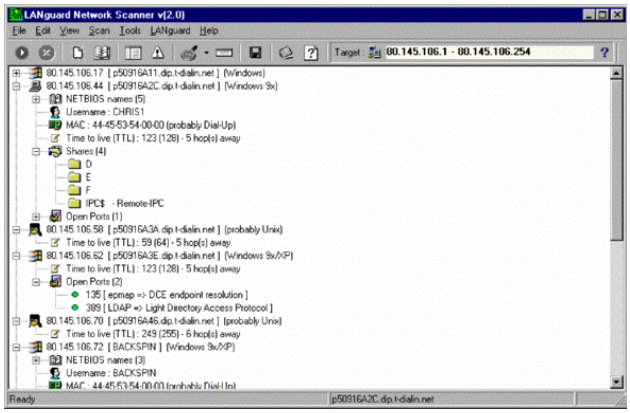
NetBrute scannt den angegebenen Bereich und zeigt alle gefundenen NetBIOS Rechner an. Dabei werden gleich alle freigegebenen Ressourcen mit angezeigt.



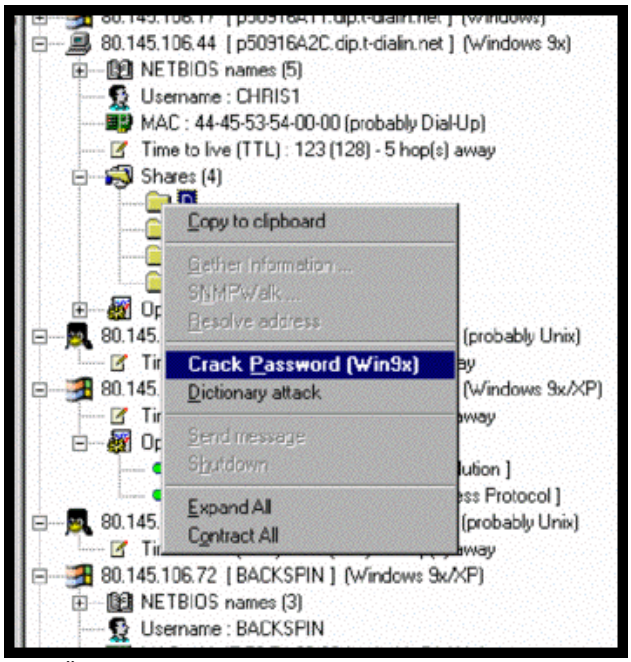
Alternativ lassen sich mit einem PortScan die offenen Ports anzeigen. Dabei kann entweder gezielt nach einem Dienst gesucht werden oder es können einfach alle bekannten Ports durchprobiert werden. Das dauert dann natürlich eine Weile.



Ein anderes Werkzeug ist der LANguard Network Scanner. Dieses Programm arbeitet ähnlich wie NetBrute, bringt aber noch mehr Informationen über die untersuchten Netzwerkrechner. LANguard testet in einem Lauf mit ICMP (Ping) und SNMP, sowie einem Portscan. Mit verschiedenen Tests versucht das Programm dann weitere Informationen über die gefundenen Rechner herauszufinden. Hier zeigen sich nach kurzer Zeit eine Menge Informationen. Sogar die versteckten Freigaben kann LANguard anzeigen.
LANguard erkennt das verwendete Betriebssystem auf dem Zielrechner. Dabei unterscheidet es sogar die verschiedenen Linux Distributionen. Allerdings verwechselt es schon mal ein SuSE Linux mit einem OpenNetBSD. Ein Mac OS 9 hält es grundsätzlich für “probably Unix”. Ein RedHat wurde korrekt erkannt. Ebenso ein Mac OS X als FreeBSD.



In der Regel ist auf den Unix Systemen nicht viel zu erkennen. Vermutlich haben die Linux Anwender ihr System besser abgedichtet. Für den Laien ist mit diesen Informationen auch nicht unbedingt viel anzufangen. Ein versierter Hacker sieht damit sicher einige Angriffsmöglichkeiten.



Eine Überraschung erlebten wir bei der Option “Crack Password”, die für Windows 9x Freigaben angeboten wird. Im lokalen Netzwerk konnten damit die kompliziertesten Passwörter in Sekundenschelle geknackt werden. Auch wenn die bisherigen Versuche im juristischen Sinne wohl in der Regel keine Einbrüche darstellen, begibt man sich hier auf dünnes Eis. Gegen das Ausspionieren von Daten gibt es gesetzliche Regelungen. Man sollte sich also gut überlegen, an wem man diese Option ausprobiert.

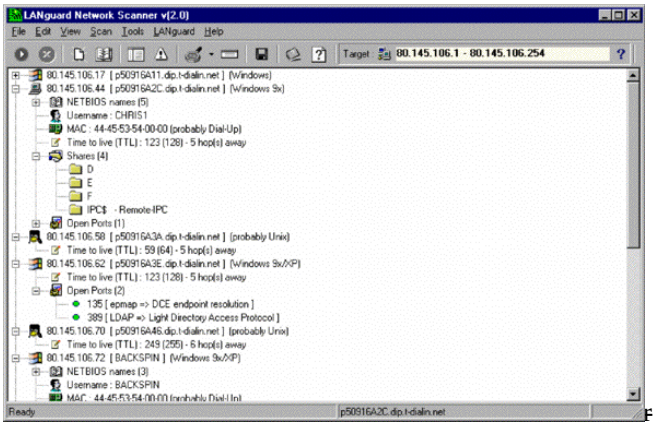
Das Programm weist in der Onlinehilfe auf dieses Problem hin. Es gibt von Microsoft für dieses Sicherheitsloch einen Patch für die Betriebssysteme Win 95, 98 und ME.

Sicherheitshinweis:

Für Windows 9x Sicherheitspatch einspielen

Sie finden den Patch unter
http://support.microsoft.com/support/kb/articles/Q273/9/91.ASP?LN=EN-US&SD=gn&FR=1

LANguard zeigt auch bei anderen Systemen Sicherheitsrisiken auf. Mit Alerts weist das Programm auf mögliche Schwachstellen hin. Meist gibt es Erläuterungen mit einem Link ins Internet dazu.



Es ist erstaunlich, welche Informationen sich über das Netz zusammentragen lassen. Besonders LANguard hilft dabei die Löcher aufzuzeigen. Es ist ein zweischneidiges Schwert, solche Werkzeuge zu verbreiten. Einerseits zeigen sie Schwachstellen auf, andererseits kann ein Angreifer diese Tools natürlich auch nutzen. Mittlerweile sind aber so viele Werkzeuge verfügbar, dass die Anwender nachrüsten sollten.

Wer selbst einmal etwas ausprobieren will, findet LANguard unter der Webadresse http://www.gfisoftware.com Das Programm ist für nicht kommerzielle Nutzung frei. NetBrute ist Freeware und in einschlägigen Free- und Shareware-Archiven zu finden, z.B. unter http://www.tucows.com

Wie man sich gegen die Attacken mit solchen Werkzeugen schützen kann, wollen wir uns auf einem der nächsten Treffen ansehen. Dazu werden wir über die Funktionen einer Firewall sprechen.

Auch das gibt es . . .

FOCUS berichtet in seiner Ausgabe 07/02 vom 9. Februar 2002 über Pharao-Ameisen (monomorium pharaonis),  die seit einiger Zeit auch in Europa vorkommen und sich schnell vermehren sollen. “Weil sie Wärme lieben, besiedeln die Tiere zudem  Computer, Küchenherde und medizinische Geräte. Verschmoren sie darin, können sie Kurzschlüsse verursachen - die Krabbler werden zum Sicherheitsrisiko.” 

Ein wirkungsvolles Gegenmittel wurde bisher noch nicht gefunden.

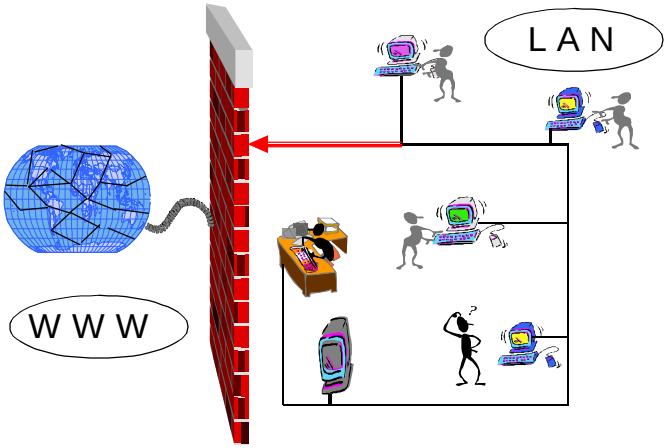
Mit freundlicher Genehmigung von Focus Magazin Verlag GmbH

Was ist denn eine Firewall?

Wolf Müglich, RG Stuttgart

Als "Firewall" bezeichnet man eine Einrichtung, die verschiedene Netzwerke voneinander abschotten soll **B** wie eine Brandwand in einem Gebäude. Bei einem Gebäude soll das Übergreifen des Feuers von einem Gebäudeteil in ein anderes verhindert werden. Die Firewall im Netz verhindert den Datenaustausch von einem Netz in das andere. Aber wie auch die Brandschutzwand eine Tür hat, um die Menschen vom einen in das andere Gebäude zu lassen, muss auch die Firewall bestimmte Datenströme durchlassen. Die einfachste Konstruktion einer Firewall zum Internet ist, den Verbindungsstecker heraus zu ziehen. Doch das ist nicht das gewünschte Ergebnis.

Die Firewall muss mit geeigneten Mitteln versuchen, genau die Daten herauszufiltern, die gebraucht werden. Dafür gibt es viele technische Ansätze. Es gibt keine genaue Beschreibung, was zu einer Firewall gehört. Meist besteht die Lösung sowohl aus Software als auch aus Hardware. Diese Komponenten werden in die Übertragungswege zwischen zwei Netzen eingebaut, von denen eines einen höheren Schutzbedarf hat. Dieses Netz wird durch die Firewall gesichert. Es ist möglich, aber nicht gebräuchlich, dass eine Firewall die Netze in beide Richtungen absichert.
So genannte "Personal Firewall" Lösungen, die auf dem lokalen Rechner installiert werden, enthalten Elemente einer Firewall, sind aber nicht Gegenstand dieses Artikels.



Gefährdungslage

Eine Firewall versucht, den unberechtigten Zugriff auf ein Netz zu verhindern. Dies ist notwendig, um die Vertraulichkeit von Daten zu gewährleisten und die internen Systeme vor Sabotage zu schützen. Eindringlinge könnten zunächst Merkmale wie IP-Nummern, Mailadressen, Rechner- und Benutzernamen des internen Netzes auslesen. Mit diesen Angaben können sie sich weiteren Zugang verschaffen.
Die vertraulichen Daten im Netz sind dadurch für Unbefugte erreichbar. Es besteht die Möglichkeit, Geheimnisse auszuspionieren, Transaktionen zu manipulieren (z.B. Banküberweisungen) oder auch nur Datenbestände zu zerstören. Auch ist es möglich, durch Manipulation an der installierten Software das ganze Rechnersystem lahm zu legen.

Wodurch können nun Gefahren entstehen?
Wie nicht anders zu erwarten, sind vor allem menschliche Fehlhandlungen mit die Hauptursache, dass Systeme "Löcher" bekommen. Fehlerhafte Administration des IT-Systems ist eine Ursache, Konfigurations- und Bedienungsfehler eine andere.
Weiterhin gibt es noch technisches Versagen. Oft hört man vom Bekanntwerden von Softwareschwachstellen oder Schwachstellen oder Fehlern in Standardsoftware. Wer weiß schon, wie ein System beim Überlaufen einer Festplatte reagiert? Und wie reagiert ein Programm auf unsinnige Eingaben? Solche Zustände können oft für ein Eindringen ausgenutzt werden.
Die "pressewirksamsten" Angriffe sind vorsätzliche Handlungen durch so genannte Hacker oder Cracker.

Als Beispiel seien hier einige Schwachstellen genannt:
Sollte ein Rechner direkt über ein Modem oder eine ISDN-Karte mit dem öffentlichen Wählnetz verbunden sein, kann auch über das Telefonnetz eingedrungen werden. Ankommende Verbindungen sollten unterbunden werden. Während einer direkten Verbindung des Rechners über die öffentliche Wählleitung sollte der LAN-Zugriff unterbrochen werden. Auf diese Art würde ansonsten die Absicherung durch eine Firewall umgangen!

Dictionary Attack, social Engineering

Auch systematisches Ausprobieren von Passwörtern kann eine Methode sein, sich Zugang zu verschaffen. Deshalb sollten Passwörter mit Bedacht gewählt werden - keine Namen von Angehörigen, keine auf- oder absteigenden Buchstaben- oder Zahlenkombinationen usw. Eine Dictionary Attack verwendet ein Wörterbuch zum Durchprobieren der Passwörter, während social Engineering die Erkundung im sozialen Umfeld der Benutzer bedeutet (Name von Frau, Kind, Hund, Katze etc.).

IP-Spoofing

ist eine Angriffsmethode, bei der falsche IP-Nummern verwendet werden, um dem angegriffenen IT-System eine falsche Identität vorzuspielen. Diese Methode führt fast immer zum Ziel, da auch eine Firewall dieser IP-Nummer vertraut!

Man-in-the-middle-Attack

Der Datenverkehr zwischen zwei Rechnern wird über ein drittes System (MitM) umgelenkt. Dieses zwischengeschaltete System kann alle Sicherheitsschranken ausschalten, da es von beiden Seiten für den rechtmäßigen Empfänger gehalten wird.

Portscan

Durch einen Portscan werden angebotene Dienste auf einem System festgestellt. Das ist an sich noch kein Problem. Oft ist der Scan aber die Grundlage für weitere Angriffe. Jeder offene Port ist eine Angriffsmöglichkeit.

Denial of Service ß Attack (DoS, DdoS)

Durch ständiges Anfordern eines Service (z.B. Webseite) wird ein System überlastet und eventuell ein Überlauf, wie schon oben beschrieben, herbeigeführt. Dabei wird meist mit manipulierten Datenpaketen gearbeitet. Durch diese Attacken wird ein System zumindest arbeitsunfähig. Eventuell können Folgefehler für einen Einbruch ausgenutzt werden.

Konzept der Netzkopplung mit Hilfe einer Firewall

Vor der Implementierung einer Firewall-Lösung muss man sich über einige Dinge klar werden. Die allgemeinen Sicherheitsziele müssen festgelegt werden. Eventuell muss auch eine Anpassung der Netzstruktur vorgenommen werden.
Die Sicherheitspolitik der Firewall sollte definiert werden, auch eine Auswahl der Kommunikationsanforderungen, besonders die Dienste-Auswahl.
Welche Dienste und Protokolle will ich zulassen?
IP, ARP, ICMP, Routing Protokolle, TCP, UDP, TELNET, FTP, SMTP, DNS, NNTP, HTTP o. a.?

Wenn die Vorbereitungen theoretischer Art abgeschlossen sind, kann die praktische Einrichtung der Firewall folgen:
Filterregeln wollen aufgestellt und implementiert werden. Filter-Proxy Anwendungen, z.B. zentrales Virenscanning muss eingerichtet werden. Allgemein sollte man die Randbedingungen für den sicheren Einsatz der einzelnen Protokolle und Dienste beachten. Einführende Literatur ist dabei sicherlich hilfreich.

Wenn eine erste Festlegung eingebracht wurde, sollte man die Firewall nicht nur vor sich hin arbeiten lassen, sondern auch während des laufenden Betriebs einiges beherzigen:
Eine regelmäßige allgemeine Kontrolle durchführen, die Protokolle der Firewall-Aktivitäten auswerten und eventuelle Datensicherungen durchführen. Vor allem eine regelmäßige Integritätsprüfung ist wichtig: verhält sich die Firewall so, wie ich es geplant habe?

Beim Betrieb der an der Firewall angeschlossenen Clients ist z.B. die Sicherheit von WWW-Browsern zu beachten, Virenscanner können zusätzlich eingesetzt und Sicherheitsupdates des verwendeten Betriebssystems und der Standardsoftware sollten regelmäßig eingespielt werden.

Ein kurzer Ausblick auf Systeme, die weitergehende Funktionalitäten bereitstellen:

Intrusion Detection und Intrusion Response Systeme = Eindringen erkennen und darauf "antworten".

Intrusion Detection Systeme lassen sich im wesentlichen in zwei Klassen einteilen: Signaturanalyse und Anomalie-Erkennung.

Bei der Signaturanalyse sollen bestimmte Muster im Datenstrom erkannt werden. Ein Beispiel ist das so genannte Portscanning, wobei die Ports (Eingangstore für die verschiedenen Dienste) daraufhin "abgeklopft" werden, ob ein Zugriff möglich ist. Aber auch ein DoS würde erkannt. Ein solcher Versuch wird von der Intrusion Detection erkannt und als Einbruchsversuch gemeldet.

Bei der Anomalie-Erkennung geht man andererseits davon aus, dass sich das normale Verhalten der Nutzer oder Rechner statistisch erfassen lässt und wertet Abweichungen hiervon als Angriff oder zumindest möglichen Angriff.

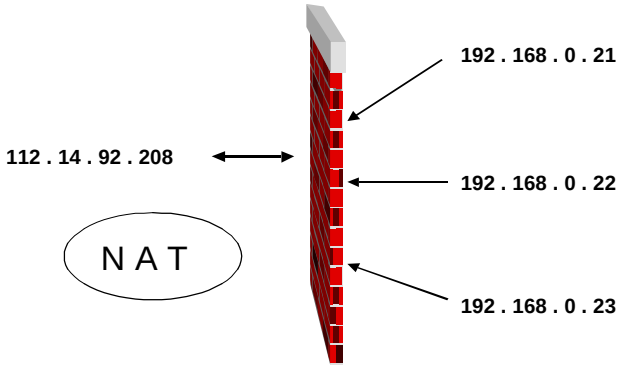
Wenn also eine bestimmte Art von Datenverkehr immer zwischen bestimmten Rechnern stattfindet, wird dies erfasst. Wenn diese Art des Verkehrs plötzlich auch noch zwischen ganz anderen Rechnern stattfindet, so wird dies (zumindest als Warnung) z.B. an den Administrator gemeldet.

Intrusion Response Systeme dagegen dienen dazu, automatisch Gegenmaßnahmen einzuleiten, sobald ein Angriff erkannt wurde. Dies geht bis zur temporären Trennung der Netzwerkverbindung nach außen. So könnte nach einem entdeckten Portscan die betreffende IP Adresse für eine bestimmte Zeit gesperrt werden.

Zur Zeit ist dies allerdings noch ein Gebiet, welches intensiv erforscht wird . . .

Adressumsetzung/NAT(Network Address Translation)

Einige Router und Paketfilter bieten die Möglichkeit einer Adressumsetzung ohne den Einsatz eines Proxys.
Eine Folge der dynamischen Adressumsetzung ist, dass ein Verbindungsaufbau zu einem internen Rechner aus dem Internet im Normalfall nicht möglich ist.
Um keine Informationen über die Struktur des eigenen Netzes nach außen bekannt zu machen, sollte eine Adressumsetzung am Internetgateway durchgeführt werden. Von außen gesehen hat jeder Rechner dann nur die öffentliche IP Adresse (in der Grafik die 112.14.92.208)
Von innen kann eine Verbindung aufgebaut werden. Dabei "merkt" sich der Router, von welchem Rechner (z.B. 192.168.0.22) die Anfrage kam und stellt diesem die Antwort wieder zu.



Application-Gateway

Dieses Gateway arbeitet auf Anwendungsebene, d.h. eine Bewertung des Inhalts wird möglich, anders als beim Paketfilter, der "nur" die Datenpakete an sich prüfen kann. Die auf dem Application-Gateway laufenden Filterprozesse werden als Proxy-Prozesse bezeichnet. Eine Filterung nach Inhalten sollte unterstützt werden, damit eine zentrale Virenprüfung und das Blockieren von aktiven Inhalten möglich ist.
Eine andere Anwendung ist ein "WWW"-Proxy, der angeforderte Seiten zum einen der anfordernden Maschine zustellt und andererseits speichert, um eine erneute Anfrage direkt aus dem Speicher beantworten zu können, ohne erneut im Internet anzufragen.

Wenn ausschließlich ein Paketfilter als Firewall eingesetzt wird, gibt es Vorteile:

- Der Packetfilter ist leicht realisierbar, da die Funktionalität von vielen Routern geliefert wird.
- Er ist leicht erweiterbar für neue Dienste.

aber auch Nachteile:

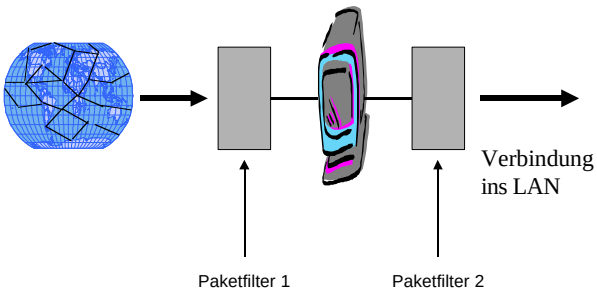
- IP-Spoofing ist u.U. möglich,
- alle Dienste, die gestattet werden sollen, müssen auf allen Rechnern, die erreicht werden können, sicher sein.
- Es müssen z.T. komplexe Filterregeln erstellt werden.
- Es gibt u.U. keine Testmöglichkeiten und es ist insbesondere nicht möglich, festzustellen ob die Filterregeln in ihrer Reihenfolge verändert werden, was bei einigen Routern geschieht um den Durchsatz zu steigern.
- Weiterhin gibt es keine ausreichende Protokollierungsmöglichkeit.

Diese Anordnung kann deshalb nur in kleinen Netzen eingesetzt werden, in denen alle Rechner gegen Angriffe abgesichert sind.

Dualhomed Gateway

Das Typische an einem solchen Gateway ist der Einsatz von zwei getrennten Interface-Karten sowie laut Empfehlung des BSI der Einsatz von zwei Paketfiltern nach außen bzw. nach innen.

Dualhomed Gateway (2 Netzwerkkarten)
laut Empfehlung vom BSI
(Bundesamt für Sicherheit im Informationswesen)



Vorteile:

- Eine umfangreiche Protokollierung ist möglich
- die interne Netzstruktur wird verdeckt.

Nachteile:

- Ein relativ hoher Preis (da ein leistungsfähiger Rechner mit zwei Netz-Interfaces benötigt wird).
- Es gibt Probleme beim Implementieren neuen Diensten, da immer auch die Software angepasst werden muss.
- Die Übernahme des Application-Gateways durch den Angreifer führt zu einem vollständigen Verlust der Sicherheit!

Ein zusätzlicher Schutz läßt sich durch den Einsatz eines Paket-Filters vor dem Gateway erreichen, wie z. B. durch einen vorhandenen Router. In diesem Fall müssten Router und Gateway durchbrochen werden, um Zugang zum zu schützenden Netz zu erhalten. Ein weiterer Paketfilter nach innen stellt eine weitere Hürde dar.

Allgemeine Grundsätze

Für die Konfiguration jeder Firewall sind zwei grundsätzliche Vorgehensweisen möglich:

1. Alle Dienste und Protokolle werden freigegeben. Nach und nach werden im Betrieb nicht benötigte und potentiell gefährliche Dienste gesperrt.

2. Alle Dienste und Protokolle werden gesperrt. Bei Bedarf wird nach Prüfung der Berechtigung und der Gefährdung ein Dienst freigegeben. Dabei werden für jeden Dienst geeignete Protokollierungs- und Zugangsmechanismen implementiert.

Dabei ist die zweite Methode bei weitem sicherer. Aber sie ist auch die aufwendigere und erfordert wesentlich mehr Arbeit in der Administration.

Für die beteiligten Rechner gilt, daß sie so eingerichtet werden müssen, dass nur die unbedingt notwendigen Programme auf ihnen laufen, diese richtig konfiguriert sind und alle bekannten Schwachstellen beseitigt werden.

Auch sollten die Anwender darauf hingewiesen werden, daß sie aus Sicherheitsgründen eventuell eingeschränkt werden. Dadurch kann ein gewisser "Unmut" vermieden werden, wenn die Gründe dafür hinreichend bekannt sind. Denn nicht nur außen gibt es Angreifer, sondern auch innen. Wenn man entsprechenden Berichten glauben will, ist dies gar nicht so selten der Fall.

Der Aufwand für die Einrichtung einer Firewall hängt immer von der Umgebung ab. Eine Lösung „Out of the Box“ ist nur die halbe Miete. Es ist immer eine Anpassung an die Gegebenheiten des Netzes notwendig. Das erfordert jedoch vom Administrator einiges an Wissen.

Namen sind Schall und Rauch ...

Günter Mußtopf, Hamburg
Geschäftsführer der perComp-Verlag GmbH

CodeRed II alias CodeRed.C alias IIS-Worm.CodeRed.C alias Trojan.Win32.VirtualRoot ... Wer als Anwender Informationen über einen Computerschädling sucht, muss manchmal ganz schön suchen, bis er bei verschiedenen Anti-Virus-Softwareherstellern fündig wird. Ein neuer Ansatz will den Namenswildwuchs entwirren.

Die Zahl der Computer-Viren, Würmer, Trojanischen Pferde, Backdoors und verwandter Sabotage-Software – kurz: Malware – wird in Bälde die Zahl von insgesamt 60 000 übersteigen. Vor vielen Jahren war die Zahl verwirrender Alias-Namen schon einmal beachtlich: so etwa 1987 mit Cascade alias Herbstlaub alias Falling_Letters alias Black_Jack. Damals verursachten zeitverzögerte Analysen und wenig Informationsaustausch zwischen den verschiedenen Anti-Virus-Labors diese Divergenzen. Dieses Problem ist heute weitgehend entschärft. Seit einigen Jahren sind wichtige Ergebnisse wesentlich schneller verfügbar. Nicht zuletzt hat sich auch die Kommunikation zwischen den Herstellern von Anti-Virus-Programmen, vor allem der Austausch neuer Malware zu Analysezwecken, entscheidend verbessert.

Ein Bestreben von Anti-Virus-Organisationen war, dass bereits der Name einer Malware im Prüfbericht eine grobe Aussage über die Art der Infektion liefern sollte. Zu diesem Zweck wurde eine ständig wachsende Zahl von Pre- und Postfixes für Malware-Namen definiert, beispielsweise: WM/... (Word Macro), X97M/... (Excel'97 Macro), Win32/..., Trojan/..., VBS/... oder als Postfix ...@mm (mass mailer), .corrupt (durch Infektion funktionsunfähig gewordene Dateien) oder .kit (mit Virenbaukasten erzeugt ## richtig?##).

Die Praxis dieser erstrebenswerten Absicht ist für die meisten PC-Anwender allerdings recht verwirrend, da die Schreibweise von Hersteller zu Hersteller recht unterschiedlich ist. Außerdem unterscheiden sich die Positionen (Pre- oder Postfix) und die Trennzeichen. Dies erschwert vielen PC-Anwendern die Suche nach Malware-Beschreibungen auf den Websites der Hersteller. Aufgrund einer ständig wachsenden Zahl von Malware, die zum Beispiel mehrere Typen enthält (etwa Viren und Würmer) oder die unter mehreren Plattformen funktionsfähig ist (wie NT und UNIX) missbrauchen viele Hersteller zudem Alias-Namen, um diese verschiedenen Aspekte zum Ausdruck zu bringen: so etwa mit IIS/ Sadmind, Worm/Sadmind, UNIX/Sadmind, Solaris/ Sadmind, ... Nicht zuletzt sind manche Prefixes, zum Beispiel O97M/ nicht eindeutig, da sie keine Aussage enthalten, ob zwei oder drei Office-Produkte als Plattform verwendet werden.

Mit Sicherheit werden noch weitere Pre- und Postfixes (etwa für PDAs) und neue Mixturen unterschiedlicher Malware-Eigenschaften hinzukommen. Eine einheitliche Namensgebung für Malware über die Herstellergrenzen hinweg ist schon heute angesichts der Anzahl bekannter Malware und dem rapiden Auftreten neuer Schädlinge nicht mehr durchsetzbar.
Während der Virus Bulletin Conference 2001 in Prag wurde dieses Problem in einer kleinen Gruppe diskutiert. Basis der Diskussion war eine Ausarbeitung "Identification of Malware from the User's Point of View". Darin schlugen die Autoren vor, in den Scanner-Berichten jeweils nur den Namen und die Variante der gefundenen Malware anzugeben. Der Benutzer könnte dann anschließend mit Hilfe eines Dienstprogramms detaillierte Informationen aus dem WWW erhalten, mindestens:

- Typ(en) der Malware: Boot-Virus, File-Virus, Makro-Virus, Wurm etc.
- Plattform(en): DOS, Win16, Win32, UNIX, Linux etc.
- Art der Distribution: fast infector, slow infector, mass-mailing usw.
- Schadfunktion(en): Löschen von Dateien, Formatieren von Platten usw.
- Entfernen der Malware, besonders Hinweise für Würmer, Trojaner und Backdoors, Regenerierung von Registry und INI-Dateien usw.

Diese Verweise auf externe – und zentral zu speichernde – Informationen würden dann die bisherigen Pre- und Postfixes ersetzen. Ein einfaches Beispiel könnte so aussehen:

Name:	CodeRed.C
Typ:	Wurm, Backdoor
Plattform:	NT, 2000, XP, IIS
Distribution:	automatisch
Schadfunktion:	Backdoor
Entfernen:	Patch

Der Vorteil dieses Verfahrens wäre, dass Informationen nach dem erstmaligen Auftreten einer neuen Malware schnell zentral bereitgestellt und zusammengeführt werden könnten. Für die Hersteller ist nur eine relativ geringfügige Erweiterung der Scanner erforderlich: ein Dienstprogramm, das den in ihrem Produkt verwendeten Namen in einen Standard-Namen konvertiert, unter dem die Informationen abrufbar sind.
Selbstverständlich ist in die *Strukturierung* genannten Informationen noch viel Arbeit zu investieren. Die Anzahl der Eigenschaften und ihre Definitionen müssen sorgfältig festgelegt werden. Diese Aufgabe soll eine Arbeitsgruppe leisten, in der Endanwender ebenso wie Mitarbeiter von Herstellern aktiv sind. Ziel ist es, die Benennung von Malware benutzerfreundlicher und vor allem weitgehend einheitlich zu gestalten.
Das in Prag diskutierte Arbeitspapier enthält viele Beispiele. Interessierte Leser können es per E-Mail von gm@percomp.de anfordern. Die jetzt konstituierte Arbeitsgruppe möchte zudem auch weitere aktive Teilnehmer für die Ausarbeitung dieses Vorschlags gewinnen; Interessierte sind zur Kontaktaufnahme über die genannte Mail-Adresse eingeladen.

(www.percomp.de).

Alleine am Computer?

Lieber Kontakte schließen,
Informationen austauschen
und gemeinsam Projekte
realisieren im AUGE e.V., dem
Verein der Computeranwender!

Besuchen Sie unsere
Webseiten im Internet
unter

http://www.auge.de/

AUGE e.V. - Bessere Ideen.

Alles ist zu knacken - oder etwa nicht?

Thomas Enke (M7062), RG Köln

1. Die Anfänge

Der theoretische Computerbau dieses Jahrhunderts wird im wesentlichen von zwei Mathematikern getragen, die beide in total gegensätzliche Richtungen operierten. Zum einen war dies der Engländer Alan Turing, zum anderen der Österreicher Kurt Gödel.

Alan Turing (1912 - 1954)

Alan Turing übersetzte 1936 die "Formalen Systeme" von Kurt Gödel in die Maschinensprache und entwarf das erste Papiermodell eines elektronischen Computers, so wie er anschließend von Johann von Neumann gebaut wurde. Während des zweiten Weltkrieges war Alan Turing maßgeblich an der Entschlüsselung der deutschen ENIGMA-Chiffriermaschine beteiligt. Heute bezeichnet man "herkömmliche" Computer, das heißt elektronisch arbeitende digitale Rechner, auch als Turing-Maschinen.

Kurt Goedel (1906 - 1976)

Kurt Gödel dachte in eine andere, mehr philosophische Richtung, und er dachte weiter, an andere nicht elektronische, nicht digitale Systeme. Daher nennt man diese Systeme, im besonderen den Quantenrechner, auch Gödel-Maschine.

Die theoretische Entwicklung heutiger Elektronenrechner geschah zu einer Zeit, als der Sprung von mechanischen Hollerith-Computern zu den mechanischen Wellenrechnern vollzogen wurde. Diese Wellenrechner wurden unter anderem von Alan Turing entworfen, um militärische Kodes zu knacken. Heute gilt es wieder, einen "sehr sicheren" Schlüssel zu entziffern, den RSA-Schlüssel, benannt nach den Mathematikern Ronald **R**ivest, Adi **S**hamir und Leonard **A**dleman.

Der RSA-Schlüssel wurde 1977 entwickelt und gilt heute als Standard bei der Übermittlung von Daten. Er wird hauptsächlich im Bereich des Internet-Banking und zur Übermittlung von sensiblen Daten und Unterschriften genutzt. Der Schlüssel basiert auf der mathematischen Tatsache, dass man zwei natürliche und sehr große Zahlen recht einfach miteinander multiplizieren kann. Aber der Weg zurück, die Zerlegung einer großen Zahl in die Primfaktoren ist fast immer zeitaufwendig, und hier liegt der Vorteil dieses Schlüssels.

2. Zur Theorie

Ein Quantenrechner arbeitet im Gegensatz zu einem "herkömmlichen" Elektronenrechner mit Hilfe von Quanten. Die Quantenphysik ist ein noch recht junger Zweig der Wissenschaften und wurde erst zu Anfang dieses Jahrhunderts entwickelt. Maßgeblich am Aufbau der Quantenphysik war Max Planck beteiligt, als er im Jahr 1899 die Licht- und Wärmestrahlung eines glühenden Eisenstückes erklären wollte. Es zeigte sich, dass dies nur dann zu erklären war, wenn die Energie in kleinen Mengen, Quanten, abgegeben wird.

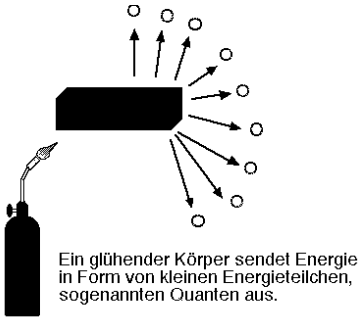


Bild 1

Albert Einstein vertiefte die Theorie und fügte 1905 den Quanten die Lichtquanten, oder auch Photonen, hinzu. Hierfür (und nicht für die Relativitätstheorie!) erhielt Einstein dann auch den Nobelpreis. Niels Bohr war der erste, der die Quantentheorie in die Atomphysik einbrachte, und mit der Entwicklung der Schrödinger-Gleichung erfolgte 1926 die erste theoretische Fassung der Quantenphysik. In der Schrödinger-Gleichung werden Position eines Teilchens und Zeitpunkt der Messung durch eine Wellengleichung W(x,t) ersetzt. Der Betrag |W2| gibt dann die Wahrscheinlichkeit an, ein Teilchen an einer bestimmten Position im Atom zu finden. Aber eine genaue Aussage zu der Position (x) eines Teilchens zu einer entsprechenden Zeit (t) ist so gut wie ausgeschlossen. Allerdings konnte Schrödinger ein Wasserstoff-Atom mit Hilfe dieser Gleichung in Formeln fassen und berechnen - bis dahin waren alle Ansätze gescheitert.

Zu dieser Gleichung entwickelte Schrödinger 1935 ein Gedankenexperiment, die so genannte "Schrödinger-Katze":

Bild 2

In einer geschlossenen Kiste befinden sich eine Katze, ein radioaktives Atom, eine Messapparatur und eine Flasche mit einer tödlichen Substanz. Wenn das radioaktive Atom zerfällt, wird dies von der Messapparatur erfasst, die dann die tödliche Substanz in der Flasche freisetzt und damit die Katze tötet. Die Quantentheorie besagt, dass die Katze gleichzeitig tot und lebendig ist, denn solange niemand die Kiste öffnet und nachschaut, ist der Zustand der Katze nicht bestimmbar. Erst das Öffnen der Kiste, was einer Messung des Zustandes der Katze gleichkäme, würde zeigen, ob die Katze noch lebt oder nicht.

Dieser neue, dritte Zustand "Superposition" zeichnet eine der Besonderheiten des Quantenrechners aus. Da der Quantenrechner mit Quanten rechnet, sind im Gegensatz zum Elektronenrechner nicht nur die Zustände "EIN" und "AUS", sondern auch der Zustand "UNGEWISS" möglich. In Unterscheidung zu den Bits des Elektronengehirns arbeitet daher ein Quantenrechner mit so genannten QuBits. Jahrelang galt diese "Superposition" als reine Theorie, da die Vorgänge im Atom in kurzen Zeiträumen und auf sehr kleinen Strecken ablaufen. Wenn man mit einer Masse von einem Gramm eine Superposition von zwei Ortszuständen im Abstand von 1 cm darstellen will, so hat man unter normalen Umständen genau 10-23 Sekunden Zeit, diesen Vorgang zu beobachten. Erst im Jahr 1995 gelang es, die langlebige Superposition eines Atoms unter Laborbedingungen herzustellen, das sich an "zwei verschiedenen Orten"gleichzeitig befindet.

Doch bevor es zu der Realisierung des Quantenrechners geht, müssen noch drei weitere Theorien kurz abgehandelt werden:
- die Heisenbergsche Unschärferelation,
- Bells Nichtlokalität und
- Everetts Viele Welten.

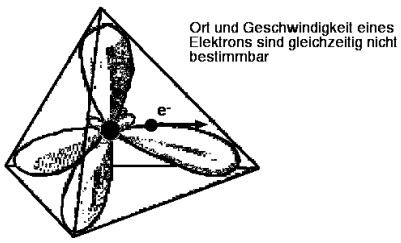


Bild 3

Heisenberg formulierte, dass es für kleine Teilchen nicht möglich ist, gleichzeitig sowohl den Ort x , als auch den Impuls p (und damit die Geschwindigkeit, da p = m * v) des Teilchens exakt zu bestimmen. Gemäß der Formel Æx * Æp => h/4o hat eine Messung immer ihre Grenzen. h entspricht in diesem Falle der Planckschen Konstante, h = 6,6256 * 10-34 Js. Damit wird noch einmal deutlich, dass es hier um Messungen von sehr kleinen Massen und Ortsverschiebungen geht. Übertragen auf die Ebene eines Atoms bedeutet die Heisenbergsche Unschärferelation, dass von einem Elektron auf seiner Flugbahn um einen Atomkern nicht immer alle "Flugdaten" gleichzeitig bekannt sein werden. Es bleibt immer eine gewisse Unsicherheit, wo sich nun das Elektron mit welcher Geschwindigkeit befindet.

Die Bellsche Ungleichung besagt, dass eine klassisch-lokale Theorie (z.B. die Newtonschen Gravitationsgesetze) die Nichtlokalität der Quantenmechanik nicht erklären kann. "Nicht-lokal" heißt eigentlich "überall" - aus Sicht der Quantenmechanik ist in dieser Welt alles miteinander verbunden, das heißt, jedes Teilchen ist mit jedem weiteren Teilchen verwoben und tritt mit diesem auch in eine Interaktion. Dazu ein Beispiel von Bell aus seinem Buch "Speakable and Unspeakable in Quantum Mechanics": "Es war bekannt, dass der Mathematiker Bertlmann immer eine grüne und eine rote Socke trägt. Sieht man die grüne Socke am linken Fuß, so weiß man mit einer in der Quantenmechanik tolerierten Genauigkeit, dass am anderen Fuß eine rote Socke sein muss. Dieses Ergebnis einer "Messung" am linken Fuß führt automatisch zu einer Erkenntnis über den rechten Fuß, ohne dass vom rechten Fuß eine Signalübertragung zur Messstelle stattgefunden hat." Das Theorem der Bellschen Ungleichung wurde angeblich 1997 im Versuch nachgewiesen - mit welchen Auswirkungen für die Grundpfeiler der Physik ist dabei noch nicht erfassbar. Zumindest im Bereich des Mikrokosmos wurden Begriffe wie Überlichtgeschwindigkeit und Raumkrümmung angefasst und neu definiert. Sollte es möglich sein, die Bellsche Ungleichung auch im Makrokosmos nachzuweisen, würden sich mehr als nur neue (Quanten-) Welten auftun.

Die vierte Formulierung ist noch weniger fassbar, wird aber im Laufe des Artikels noch eine große Rolle spielen: Everetts Theorie der vielen (Quanten-) Welten. Im Jahr 1957 stellte Hugh Everett die Behauptung auf, dass sich das Universum immer dann in eine Vielzahl neuer Welten aufspaltet, wenn eine entsprechende Vielzahl von Möglichkeiten zur Interaktion zwischen Teilchen entsteht. In jeder dieser neu entstandenen (Quanten-) Welten ist alles identisch - bis auf die entsprechend getroffene Auswahl. Dies führt zu einem Universum, das sich nach jeder sich bietenden Interaktion in weitere Unter-Universen aufspaltet, so dass eine gewaltige Zahl von (Quanten-) Welten nebeneinander existiert. Im ersten Augenblick vielleicht unfassbar, jedoch leicht erklärlich, weil sich die Quantenmechanik im kleinsten Bereich abspielt und sich in jedem Augenblick vielseitig verändert.

Vergleichbar ist dies am einfachsten mit einem großen Schwimmbecken, in dem eine Vielzahl von Personen die vorerst glatte Wasseroberfläche aufwühlen. Jede Wellenbewegung des Wassers entspricht einem Quant, das sich wellenförmig von der jeweiligen Person wegbewegt. Nach der Theorie des Dualismus ist jedes Energieteilchen auch gleichzeitig eine Welle - man denke an Lichtteilchen (Photonen) und Licht als Teilspektrum der elektromagnetischen Wellen. Treffen sich zwei Wellen, so treten sie in Interaktion zueinander, sie verstärken sich oder löschen sich aus. Es entstehen so neue Wellenformationen, die sich vom Punkt der Interaktion wegbewegen, dabei ggf. vom Rand reflektiert werden oder auf andere Wellen treffen. Für den Beobachter von außen sieht dies wie eine einzige brodelnde Oberfläche aus. Der Quantenphysiker untersucht aber in sehr kleinen Flächen des großen Schwimmbades einzelne Wellenbewegungen und

versucht, hier geordnete Strukturen zu erkennen.
Wichtig ist in diesem Zusammenhang, dass ein Beobachter, der sich einer einzelnen Wasser- oder auch Quanten-Welle in den Weg stellt (z. B. um ihre Höhe zu messen) ebenfalls in Interaktion mit dieser Welle tritt, ihre ursprüngliche Form verändert und damit ihre eigentliche Information zerstört.

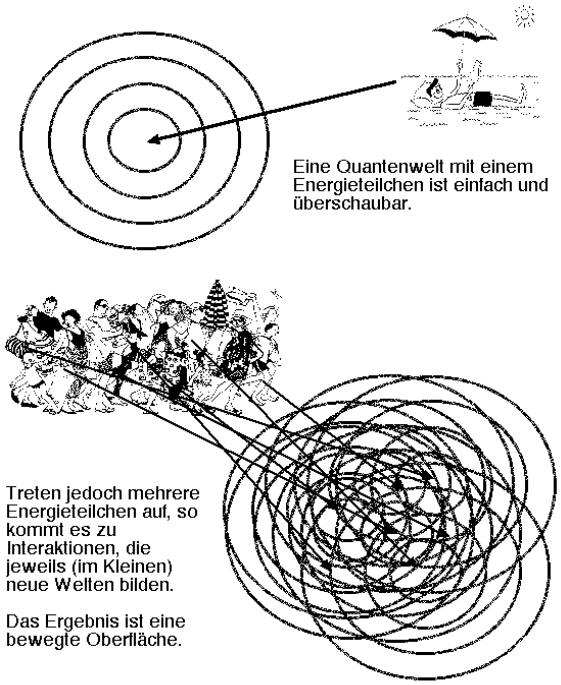


Bild 4

3. Das QuBit

Beim herkömmlichen Computer nutzt man feine Elektronenströme aus, die in Miniaturtransistoren entsprechende Schaltfunktionen auslösen. Das QuBit benötigt Schaltkreise, die sehr viel kleiner und sensibler ausgestattet sein müssen, da nur kleinste Systeme in atomarer Größenordnung der Quantenphysik unterliegen. Zusätzlich müssen diese Mikrocomputer von der Umwelt abgeschirmt sein, um die Superpositionszustände lange genug aufrecht zu erhalten und nicht durch Umwelteinflüsse zu stören. Durch Einflüsse von außen entstehen unerwünschte Wechselwirkungen, die die Superposition nicht nur verändern, sondern sogar vernichten.

Seit 1995 ist es möglich, QuBits mit Hilfe von Ionen herzustellen. Den Durchbruch dazu schafften die Physiker Cirac und Zoller. Dazu wurden die QuBits in einer so genannten Ionenfalle gespeichert, genauer gesagt, isoliert. Eine Ionenfalle besteht aus einem elektrischen Wechselfeld in einer luftleeren Kammer mit speziellen Elektroden. Dieses Speicherprinzip ist seit etwa 40 Jahren bekannt und wird hauptsächlich in der Kernforschung angewandt. Nun entzieht man dem Ion mit Hilfe eines Laserstahls solange kinetische Energie, bis dessen Temperatur nur noch knapp über dem absoluten Nullpunkt von -273,15°C (d.h. 0 K) liegt. In diesem Temperaturbereich schwingt das Ion nur noch geringfügig und kann zur Produktion eines QuBits genutzt werden. Die logische "0" ist dabei der Grundzustand des Ions, eine logische "1" entspricht einem Zustand höherer Energie in dem Ion. Mit Hilfe eines weiteren Laserstrahls, abgestimmt auf den Übergang von "0" nach "1", wird die Superposition der beiden Zustände erzeugt, und schon erhält man ein QuBit.

Da das QuBit drei Zustände ("0", "1" und "ungewiss") haben kann, ist es möglich, bei der Kommunikation zwischen zwei Datenstationen mehr Information in einer Zeiteinheit zu übertragen als dies mit Elektronen-Bits möglich ist. Genau genommen ist dies ein Informationszuwachs von log23 = 1,58, und damit genau ein "Trit". Somit könnte ein ASCII-Zeichen mit nur 5 QuBits (Trits) anstatt 8 Bits übertragen werden.

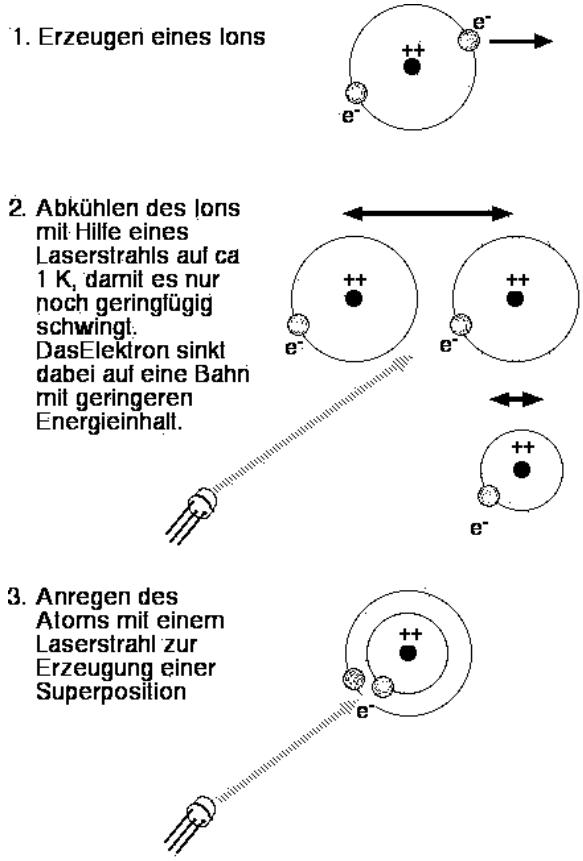


Bild 5

Die Superposition ist nun das eigentlich Interessante an dem QuBit. Wenn ein klassischer Elektronenrechner mit einer Basis von 8 Bit zur Berechnung von 256 Funktionswerten einer Funktion f(x) eingesetzt wird, so benötigt er 256 Eingaben und 256 Schleifendurchläufe zur Berechnung aller Werte. Ein Quantencomputer mit einer Basis von 8 Bit erzeugt erst einmal eine Superposition aller möglichen Zustände der Eingabe. Nach Everetts "Viele Welten"-Prinzip können so alle 256 möglichen Funktionswerte mit einem Rechendurchgang bearbeitet und im Speicher gehalten werden. Erst beim Auslesen aus dem Speicher erfolgt eine Auswahl des gewünschten Funktionswertes. Gleichzeitig wird aber durch Interaktion des Messinstruments mit den QuBits

im Speicher die Superposition zerstört, so dass weitere Messergebnisse (zur Zeit) noch nicht auslesbar sind.

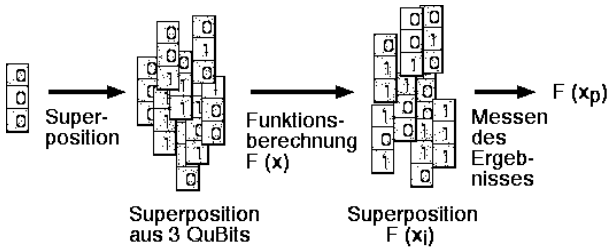


Bild 6

Damit hat man einen Parallelrechner erschaffen, der zwar auch nur ein Resultat als Ergebnis liefert, aber mittlerweile ist es möglich, dem Quantenrechner zumindest Eigenschaften aller Einzelresultate zu entlocken, so dass man, je nach Anwendung, schneller zu einer Lösung gelangt als mit einem Elektronenrechner.

4. Prinzipieller Aufbau eines Quantenrechners

Zum Verständnis: ein Quantenrechner ist nicht die weitere Miniaturisierung des elektronisch arbeitenden Computers mit immer kleiner werdenden Transistoren und integrierten Schaltungen. Elektronenrechner werden, gleichgültig wie klein ihre Bauteile in Zukunft werden, immer mit Bits arbeiteten, auch wenn ihre Bauteile bei genügender Miniaturisierung mehr und mehr den Gesetzen der Quantenphysik unterworfen werden.

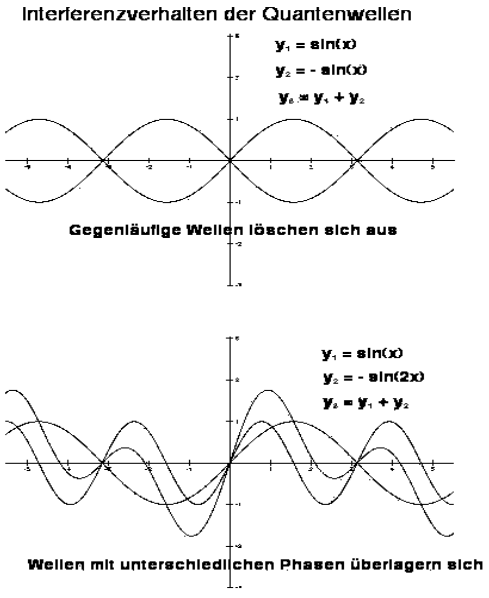


Bild 7

Zur Zeit werden zwei Bauausführungen von Quantenrechnern verfolgt. Dies ist zum einen der Bau eines Berechnungsnetzwerkes und zum anderen der "Zelluläre Automat". Wie auch beim herkömmlichen Computer werden logische Gatter aufgebaut, allerdings nicht aus elektronischen Schaltkreisen, sondern aus kleinsten Bauteilen der Kernforschung. Ein weiterer Gegensatz zum Elektronenrechner liegt in der Art der Gatter. Während beim elektronischen Schaltkreis eine fest vorgegebene Anzahl von Bit verarbeitet wird, treten bei den Quanten-Gattern Überlagerungen auf. Dies liegt an der Tatsache, dass Quanten sowohl Teilchen als auch Wellenform haben können. Wellen, die in Phase laufen, verstärken sich, gegenläufige Wellen löschen sich aus.

Die Programme der Quantenrechner machen sich dieses mathematische / quantenmechanische Verhalten zunutze. Richtige Antworten werden im Laufe des Programmablaufes verstärkt, falsche Antworten werden ausgelöscht. Wenn man mehrere parallele Messungen durchführt, erreicht man astronomisch hohe Rechengeschwindigkeiten. Fehlerkorrekturen aus mehreren Quantengattern und aus speziellen Rechenvorschriften sollen dabei für eine störungsfreie Berechnung sorgen.

5. Was läuft bisher?

Ein Quantengatter macht noch keinen Hochleistungscomputer. Zusätzlich zur Hardware muss eine völlig neue Software geschaffen werden.
Der erste Quantencomputer wurde bereits 1989 in Betrieb genommen. Er besteht aus einer Reihe von Ionenfallen, in denen Laserstrahlen auf das äußere Elektron eines Ions einwirken und so die benötigten QuBits erzeugen können. Die Lebensdauer eines QuBits beträgt zur Zeit etwa 0,1 Sekunden - lang genug für entsprechende Rechnungen, da die Rechenzeit im Mikrosekundenbereich liegt.
Seit 1990 beherrscht man das Problem der Datenübertragung. Allerdings waren die Distanzen mit ca. 50 cm zwischen Sender und Empfänger noch sehr klein. Eine Datenübertragung von QuBits über eine Entfernung von 30 km wurde 1997 erreicht. Dabei ist es mittlerweile möglich, herkömmliche Glasfaserkabel zu nutzen.
1995 wurde die Fehlerkorrektur als eigener Baustein dem Quantencomputer hinzugefügt. Damit wurde erreicht, einen einigermaßen störungsfreien Rechenbetrieb aufzunehmen und das Erreichen des richtigen Rechenergebnisses sicherer zu machen. Kleinste Einflüsse von außen, ein einzelnes unerwünschtes Photon kann das ganze Rechenergebnis verfälschen, gegebenenfalls sogar den Computer für einige Zeit unbrauchbar machen. Weiterhin unterliegt der Quantencomputer der Heisenbergschen Unschärferelation und gibt daher ein Rechenergebnis nur mit einer gewissen Wahrscheinlichkeit aus. Hier muss das Rechenergebnis unter Umständen mehrfach wiederholt werden, um daraus einen wahrscheinlich richtigen Mittelwert bilden zu können.
Ein weniger aufwendiger "Speicherbaustein" kam 1997 hinzu. Hier werden mikroskopisch kleine Bauteile aus dem Bereich der Kernspin-Resonanz genutzt, um QuBits zu speichern.

Die Softwareentwicklung polarisiert sich zur Zeit auf nur wenige Anwendungsgebiete, dies ist zum einen die Entwicklung von abhörsicherem Datentransfer und zum anderen auf

die Berechnung von Primfaktoren großer Zahlen. Hier gibt es seit etwa 1994 leistungsfähige und vor allem schnelle Algorithmen zur Zerlegung von sehr großen Zahlen. Weitere Anwendungsgebiete könnten die Sortierung von großen Datenmengen sein, da ein Parallelrechner eine um mehrere 10er-Potenzen höhere Verarbeitungsgeschwindigkeit erreicht.

6. Sichere Datenfernübertragung mit Hilfe von QuBits

Quantenkryptographie gilt zur Zeit als eine der sichersten DFÜ-Möglichkeiten. Da die Information der zu übertragenden Daten durch Quantentechnologie selbst gesichert ist, könnte so das Problem der Kodierung von Daten für einige Jahre gelöst werden.

Zur Übertragung der Daten werden Photonen genutzt, die entweder in der Polarisationsebene "waagerecht/senkrecht" linear oder "schräg links/rechts", das heißt zirkulär, schwingen. Der Sender kann beide Polarisationsebenen einstellen und senden, aber gemäß den Gesetzen der Quantenmechanik kann der Empfänger nur die eine oder andere Ebene messen. Hier kann nach der Heisenbergschen Unschärferelation zur gleichen Zeit nur die lineare Polarisation als horizontale oder vertikale Schwingung oder die zirkuläre Polarisation als Drehimpuls des Teilchens (hier ganz einfach als Polarisationsebene "schräg links/rechts" dargestellt) gemessen werden. Wenn nur ein Photon mit einer Polarisationsebene von "waagerecht/senkrecht" eine auf "waagerecht/ senkrecht" eingestellte Messapparatur durchläuft, wird auch der Messwert "waagerecht oder senkrecht" angezeigt. Sollte ein Photon mit der Polarisationsebene "schräg links/ rechts" diese Messapparatur passieren, ist der Messwert rein zufällig und kann "waagerecht" oder "senkrecht" ausfallen. Mehr kann in diesem Fall nicht gemessen werden.

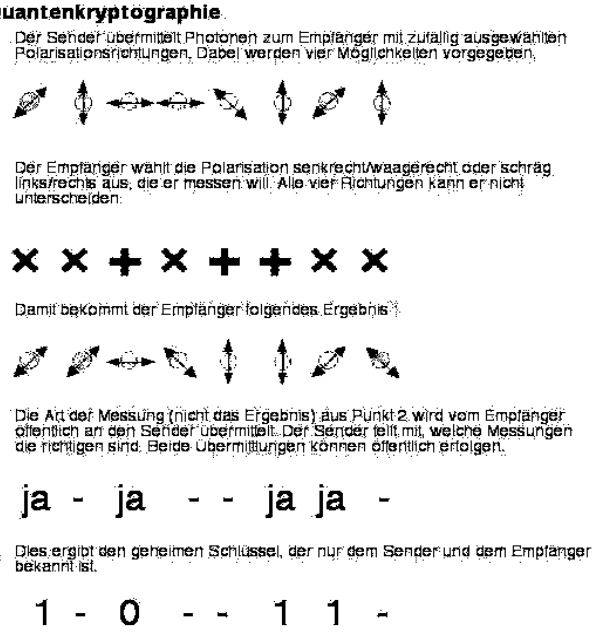


Bild 8

Der Empfänger übermittelt seine Messung öffentlich, d.h. unverschlüsselt an den Sender. Dieser teilt ihm, auch öffentlich, mit, bei welchen Einstellungen die vom Sender gewählte Polarisationsebene richtig gemessen wurde. Nur diese Einstellungen werden dann vom Sender und Empfänger als geheimer Schlüssel zur chiffrierten Übermittlung von Nachrichten genutzt. Ihr größter Vorteil liegt aber darin, dass ein Abhörversuch sofort von Sender und Empfänger bemerkt wird. Denn, wenn ein vermeintlicher Dritter in der Übertragungsstrecke Messungen vornimmt, verändert er automatisch auch die übertragenen Daten. Dies fällt spätestens bei der Überprüfung der empfangenen Daten auf, wenn nur noch ein Datensalat, aber keine sinnvollen Botschaften mehr empfangen werden. Dann können Sender und Empfänger zu entsprechenden Gegenmaßnahmen greifen, im einfachsten Fall wäre dies der Abbruch der Nachrichtenübermittlung. Daher ist es möglich, die Datenübertragung auf nicht geschützten Lichtwellenleitern aus Glasfaser zu übertragen.
Wenn Sender und Empfänger bei der Datenübertragung mit unterschiedlichen Polarisationsebenen arbeiten, ist die Verschlüsselung der Daten nach heutigen Kenntnissen perfekt. Diese zukunftsträchtige Kodier-Technik trägt den Namen "Quantum Public Key Distribution", abgekürzt QPKD und kann zur Zeit für die Datenübertragung auf Entfernungen bis etwa 30 km genutzt werden. Größere Entfernungen können zur Zeit nicht überbrückt werden, weil bisher keine Signalverstärkung möglich ist. Eine Signalverstärkung wiederum stellt einen Eingriff in das System dar und führt, wie auch eine unbefugte Messung, zu einem Datensalat. Aber, vor allem das Militär arbeitet an einer Lösung dieses Problems.
Wie kompliziert dabei die Vorgänge sind, soll folgendes Forschungsexperiment aus dem Jahr 1997 zeigen. Eine Innsbrucker Forschungsgruppe übertrug ein "Trit" an Informationen mit Hilfe eines Systems aus zwei Polarisationszuständen eines Photons. Dabei wurde mit einem Laserstrahl in einem Kristall ein Photonenpaar erzeugt, dessen Zustände gemäß der Quantentheorie nicht unabhängig voneinander sein können. Diese speziellen "EPR"-Photonen wurden in einem Gedankenexperiment von Einstein, Podolsky und Rosen erdacht, sie bilden ein zusammenhängendes Quantensystem, auch wenn beide Photonen sich in unterschiedliche Richtungen bewegen. Das heißt, eine Messung an einem Photon dieses Paares beeinflusst den Zustand des anderen Photons, ohne dass ein messbarer Informationsfluss stattfindet. Damit ist ein eindeutiger Nachweis der bereits oben angesprochenen Bellschen Ungleichung über die Nichtlokalität gelungen. Ob es auf diese Weise möglich ist, Informationen mit einer höheren Geschwindigkeit als der Lichtgeschwindigkeit zu übertragen, ist bisher noch nicht geklärt, da die Mess-Strecken im Versuchsaufbau und die Lebensdauer des Photons noch zu kurz waren.
Dieser Versuchsaufbau hat gezeigt, dass es möglich ist, von einem Sender zwei Photonen an einen Empfänger abzusenden. Ein Photon erreicht den Empfänger direkt, das zweite wird in der Polarisationsrichtung manipuliert. Der Empfänger ist nun in der Lage, durch gleichzeitige Messung drei verschiedene Zustände zu erkennen: ein "Trit" wurde übertragen.

7. Entschlüsseln von Nachrichten mit Hilfe des Quantencomputers

Eine weitere Hauptaufgabe des Quantencomputers liegt in der Dechiffrierung von Botschaften. Die meisten kryptographischen Schlüssel basieren auf der Tatsache, dass es sehr mühsam und vor allem zeitaufwendig ist, große Zahlen in ihre Faktoren zu zerlegen. Zahlen mit mehr als etwa 20 Stellen können praktisch nicht in einer vertretbaren Rechenzeit in ihre Faktoren zerlegt werden und wenn, dann ist beim heutigen Stand der elektronischen Computer die so entschlüsselte Botschaft mehrere Jahre alt und damit uninteressant. Daher gilt die RSA-Technologie eigentlich als recht sicher.
Peter Shor, der Pionier unter den Entwicklern der Quantencomputer, hat in den AT&T Bell Labs einen Algorithmus aufgebaut, der das Ende der RSA-Kryptologie bedeuten könnte. Sein Programmentwurf beruht auf einem Algorithmus von Euklid und arbeitet wie folgt:
Die Faktorzerlegung mit Hilfe eines Quantenrechners basiert auf der Periodizität der Funktion fN(x) = ax mod N. N stellt die zu zerlegende Zahl dar. Für steigende Potenzen von x wird die Funktion periodisch mit der Periode r. Damit genügt die Kenntnis von r, um die Primfaktoren von N zu berechnen. Die Primfaktoren sind in diesem Fall die größten gemeinsamen Teiler von N und ar/2 " 1. Wenn man nun einen genügend schnellen Rechner zur Verfügung hat, ist ein Schlüssel aus einer Zahl mit mehreren Dutzend Ziffern schnell geknackt. Dazu ein "einfaches" Beispiel:
Für die Faktorisierung der Zahl N = 15 wird die Funktion f15(x) mit a = 11 berechnet. Die Funktion hat ausschnittsweise folgende Wertetabelle:
Anhand der Wertetabelle sieht man, dass die Funktion perio-

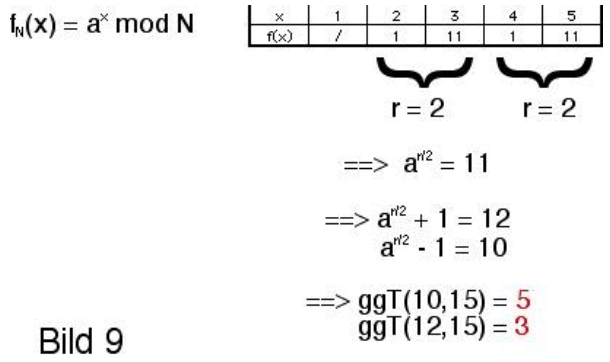


Bild 9

disch ist und die Werte 1 und 11 annimmt. Die Periodendauer hat den Wert 2. Nun berechnet man zwei Hilfszahlen nach der Formel H = ar/2 " 1 mit a = 11 und kommt so auf die Hilfszahlen 10 und 12. Der jeweils größte gemeinsame Teiler der Zahl N und der Hilfszahlen ergibt dann die gesuchten Faktoren. Der hier vorgestellte Algorithmus nutzt die Fähigkeit des Quantencomputers als Parallelrechner. Da der Quantencomputer aber immer nur ein Ergebnis pro Rechenoperation preisgibt, muss man den Umweg über die Periodizität der Funktionswerte gehen. Dieser ist auf einem Quantenrechner aber immer noch schneller als der herkömmliche Rechenweg auf einem Elektronencomputer. Die Rechendauer einer Zahl mit n Ziffern wächst auf einem Elektronenrechner exponential an, während sie auf einem Quantenrechner nur quadratisch anwächst. Schon bei einer Zahl mit nur 4 Ziffern gewinnt die Überlegenheit eines Quantenrechners. Deutlich ist der Vorsprung bei Zahlen mit mehr als 100 Ziffern, wie das folgende Bild zeigt.

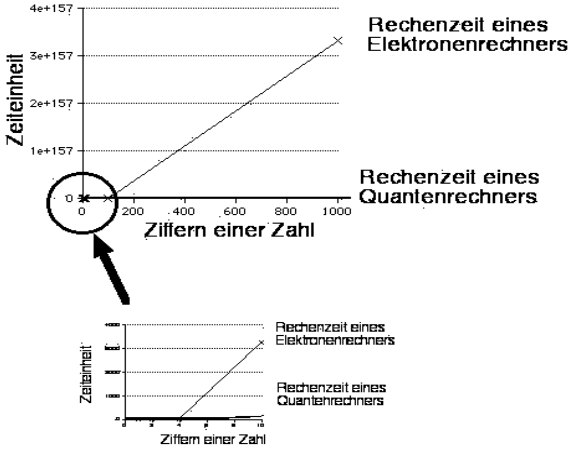


Bild 10

Mit dem Algorithmus von Peter Shor ist die Faktorisierung großer Zahlen genauso schnell möglich, wie das Multiplizieren. Für das Zerlegen einer 130-stelligen Zahl benötigt ein Quantencomputer 10 Millionen weniger Zeiteinheiten als ein

Peter Shor

herkömmliches Elektronengehirn.

8. Ausblick

Wie weit sind Forschung und Entwicklung fortgeschritten? Unbestritten steht die Wissenschaft erst am Anfang der Quantencomputertechnik. Mehr als unbeholfene Prototypen der Quantencomputer stehen sicherlich noch nicht in den Laboren. Man geht davon aus, und hier sind die Quellenangaben in einer Prognose sehr unterschiedlicher Meinung, dass in etwa einem Jahrzehnt die ersten Programme implementiert sind und ein Quantenrechner die ersten 2- bis 3-stelligen Zahlen in Primfaktoren zerlegen wird, bzw. die ersten leistungsfähigen Computer bei großen Instituten, Universitäten und natürlich dem Militär arbeiten werden. Wann der RSA-Schlüssel wirkungsvoll geknackt sein wird, darüber gibt es zur Zeit noch nicht einmal eine Prognose. Allerdings,

im Gegensatz zu den USA (Etat zur Zeit 20 Millionen US-$), arbeitet man in Europa nicht gerade mit Hochdruck in diesem Zweig der Technologie. Vielleicht aus gutem Grund, denn wer hat schon ein Interesse am Ende der RSA-Kryptographie?

Weiter ist man im Bereich der Quantenkryptologie. Schon jetzt arbeiten leistungsstarke Kryptosysteme auf Basis der Quantentechnologie, die Distanzen bis etwa 30 Kilometer überbrücken können. Das nächste Ziel ist die Satellitenübertragung von geheimen Daten.

Mittlerweile ist auch eine internationale Wissenschaftskooperation entstanden, die klären will, wie und wann der Quantencomputer für die Sicherheit der Kryptologie gefährlich werden kann. Dazu erklärte 1998 Prof. Thomas Beth vom Institut für Algorithmen und Kognitive Systeme der Universität Karlsruhe: "Eine Gefahr für die Datensicherheit von Banken und Internetbenutzern besteht zur Zeit noch nicht."

9. Quellenangabe

J.S. Bell: Speakable and Unspeakable in Quantum Mechanics, Cambridge 1987
D. Deutsch: The Fabric of Reality, New York 1997
O.E. Rössler: Das Flammenschwert, Bern 1996,
sowie verschiedene Internetadressen über Peter Shor, Kurt Gödel und Alan Turing.

Mitglied werden im AUGE e.V.

Der AUGE e.V. bietet u.a.:

- Die Vereinszeitschrift user Magazin mit den für Mitglieder kostenlosen Kleinanzeigen
- Den aktuellen Infobrief user Magazin Aktuell
- Regelmäßige Regionaltreffen in 20 Orten in Deutschland, die den Kontakt mit anderen Mitgliedern ermöglichen und dem Wissensaustausch dienen.
- Arbeitsgemeinschaften, die sich mit speziellen Themen befassen
- Web-Space und E-Mail Account mit zahlreichen Features
- Und ein Willkommensgeschenk: Kugelschreiber, Anstecker oder Tasse?

[ ] Aufnahmeantrag

[ ] Änderungsmitteilung (nur für Mitglieder) Mitgliedsnummer: .....

[ ] als Familienmitglied (nur bei Erteilung einer Lastschrifteinzugsermächtigung); Mitgliedsnummer des Vollzahlers: .....

Bitte verwenden Sie dieses Formular auch dann, wenn sich Ihre Anschrift oder Kontoverbindung geändert hat.

Bitte füllen Sie die folgenden Felder vollständig aus:

Name .....

Vorname .....

Firma (falls Firmenantrag) .....

Straße, Hausnummer .....

Nationalität ..... Postleitzahl ..... Ort .....

Geburtsdatum .....

Bitte füllen Sie diese Felder aus, wenn Sie per Lastschrift zahlen wollen (siehe nebenstehenden Text).

Kontonummer ..... Bankleitzahl .....

Geldinstitut, Ort .....

Kontoinhaber (falls vom Antragsteller abweichend) .....

Hiermit ermächtige ich/wir den Verein AUGE e.V. widerruflich, die von mir/uns zu entrichtenden Zahlungen bei Fälligkeit zu Lasten meines/unseres nebenstehend angegebenen Kontos mittels Lastschrift einzuziehen.Wenn das angegebene Konto die erforderliche Deckung nicht aufweist, besteht seitens des kontoführenden Geldinstituts keine Verpflichtung zur Einlösung. Teileinlösungen sind bei Lastschriften ausgeschlossen.

Freiwillige Angaben:

Beruf .....

Telefon (privat) ..... Telefax (privat, 24 Std.) .....

E-Mail-Adresse

Der Weitergabe meiner Anschrift an andere Mitglieder stimme ich zu [ ] stimme ich nicht zu [ ]

Hiermit beantrage ich die Aufnahme in den AUGE e.V. Die Satzung erkenne ich an.

Ort, Datum Unterschrift

.....

(bei Minderjährigen auch die Unterschrift des gesetzlichen Vertreters)

Der Mitgliedsbeitrag beträgt derzeit pro Jahr 60,- EUR für natürliche und 120,- EUR für juristische Personen. Für Schüler und Studenten gilt bis zum vollendeten 27. Lebensjahr gegen Nachweis ein ermäßigter Beitrag von 30,- EUR.

Die auf diesem Antrag gemachten Angaben werden elektronisch gespeichert und nach Beendigung der Mitgliedschaft gelöscht.

Bitte unterschrieben einsenden an:

AUGE e.V.
Wielandstr. 41
D-60318 Frankfurt a. M.

AUGE e.V.

Der Verein der Computeranwender
Regionalgruppe Köln ▯ RG 500

RG-Treffen: Wir treffen uns am 2.Samstag jeden Monats
zwischen 14:00 Uhr und 18:00 Uhr
zum **Erfahrungsaustausch** zwischen
Anfängern, Fortgeschrittenen und Profis

(Der Termin kann sich in Ausnahmefällen ändern,
deshalb bitte aktuell im Internet nachschauen
oder beim RG-Leiter telefonisch erfragen)

Treffpunkt: Günter Sprung (M360)
Mutzenrather Weg 5
50259 Pulheim-Sinnersdorf

RG-Leiter: Heinz Rothkegel (M2374)
Neuenbaumer Straße 4
50739 Köln-Longerich
Tel. 0221/541036 oder 0172/2001154
E-Mail: heinz.rothkegel@auge.de

Gäste sind herzlich willkommen!