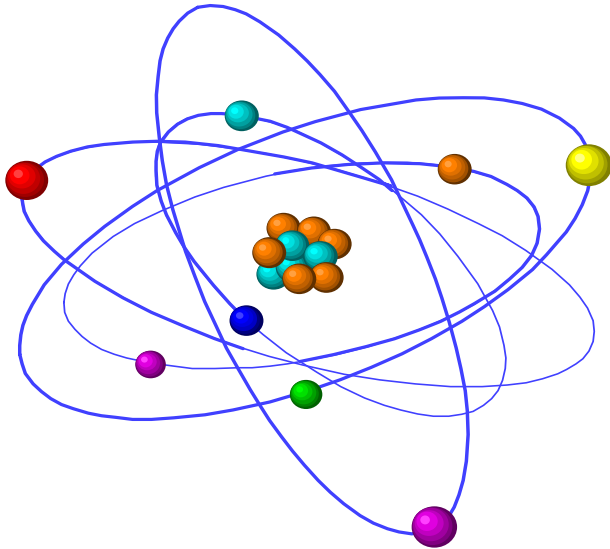


# Computer-Sicherheit gerät ins Schleudern



Schwer abschätzbare Zuverlässigkeit von Gesamtsystemen, zunehmende Komplexität der Software und Datennetze, Hacker die weltweit wühlen und neue Viren erfordern ein Umdenken der Computersicherheit

Von Max Kleiner

Computer werden immer leistungsfähiger. Ob sie auch sicherer werden, ist allerdings zweifelhaft. Zwar lässt sich die Funktionstüchtigkeit der Hardware gut abschätzen und den Bedürfnissen anpassen. Schwieriger ist die Beurteilung der Zuverlässigkeit von Software. Win95 birgt in dieser Hinsicht neue Gefahren. Und noch komplizierter ist es, die Betriebssicherheit von Gesamtsystemen zu evaluieren, welche zusätzlich durch Hacker und Viren bedroht ist.

Wer einen Computer kauft, nimmt als selbstverständlich an, dass dieser auch einwandfrei funktioniert. Um so grösser ist der Ärger, wenn dies nicht zutrifft. Den Schaden trägt aber nicht nur der enttäuschte Kunde, sondern letztlich auch der Hersteller, denn schlechte Nachrichten machen rasch die Runde und verunsichern potentielle Käufer. Dass Qualität zum Geschäftserfolg eines Unternehmens beiträgt, haben zumindest die Hardwarefabrikanten im Laufe der Jahre gelernt. Hingegen scheinen viele Softwarehersteller diese einfache Regel immer noch nicht zu kennen.

Was aber letztlich zählt, ist die Zuverlässigkeit des ganzen Systems, intern und extern betrachtet. Fachleute verstehen darunter die Wahrscheinlichkeit, dass dieses im Betrieb während einer bestimmten Zeit nicht versagt und auch nicht bedroht ist.

Das sollte nicht etwa eine Frage banger Hoffens sein, sondern auf gesichertem Wissen beruhen. Als Mass für die Zuverlässigkeit dient entweder die Anzahl Fehler oder Attacken, die pro Zeiteinheit durchschnittlich auftreten, oder die statistisch errechnete Zeitspanne, in der kein Zwischenfall auftreten wird.

## Risikofaktor Software

Für die Hardware kann man solche Werte relativ einfach ermitteln. Die Ausfallrate elektronischer Bauteile sollte jedem seriösen Hersteller bekannt sein. Wenn er zum Beispiel weiss, dass ein gewisser Kondensator durchschnittlich einmal in 1000 Stunden ausfällt, wird er wahrscheinlich zwei dieser Bauteile für die gleiche Funktion einbauen, womit an dieser Stelle des Systems eine nach Wahrscheinlichkeitsrechnung pannenfreie Betriebsdauer von einer Million Stunden gewährleistet ist (1000 mal 1000 Betriebsstunden). Allerdings darf man die Bauteile eines Systems nicht isoliert betrachten, sondern muss damit rechnen, dass defekte Komponenten andere Komponenten negativ beeinflussen. Mit dem Bereitstellen zusätzlicher Redundanz sollte aber auch dieses Problem lösbar sein. Damit lässt sich praktisch jede gewünschte Hardware-Zuverlässigkeit erreichen.

Nun bestehen aber moderne Systeme nicht aus Hardware allein, sie hängen auch von Software ab. Wenn diese versagt, nützt das beste Gerät nichts mehr (Vorausgesetzt wir haben nicht noch einen Floating Point-Fehler à la Pentium). Die Hauptsorge des Systemlieferanten müsste also weniger der Ausfall physischer Bauelemente sein, sondern ein Versagen der Software.

Überraschenderweise denken aber viele Hersteller gar nicht an Programmfehler, wenn sie die Zuverlässigkeit eines Systems taxieren sollen. Weshalb? Ein Grund dafür könnte sein, dass die Software-Zuverlässigkeit oft nach sehr subjektiven Kriterien beurteilt wird - zum Beispiel dem schieren Glauben eines Programmentwicklers an die Korrektheit seines Codes. Zudem sind immer auch Rundungsfehler im Spiel.

Während also die Fehlerrate der Hardware statistisch berechenbar ist, tappt man bei der Bestimmung der Software-Ausfälle noch weitgehend im dunklen. Verschiedene Fachleute glauben zudem, dass nicht nur gewöhnliche Programmfehler zu einem Versagen führen, sondern dass manchmal auch der gesteuerte Zufall eine Rolle spielt. Der Grund: Software ist eben keine so logische, definierte und abstrakte Sache, wie man gemeinhin annimmt. Die Kombination z.B. eines Pentium133 mit Win95 im Netz und zusätzlicher Peripheriegeräte kann infolge hoher Komplexität Unsicherheit erzeugen.

## Im Betrieb ist alles anders

Viele Software-Fehler treten nur unter ganz bestimmten und meist ungewöhnlichen Umständen auf, zum Beispiel bei einer ganz speziellen Kombination von Input, Systemzustand und Ausführungspfad im Programm. Ich bezeichne diese Eventualität als „Magic Logic“. Schon bei relativ einfachen Aufgaben gibt es da so viele Möglichkeiten, dass niemand voraussehen kann, welche Kombinationen allenfalls zu einem Fehler führen könnten.

Trotz dieser Gefahr wird die Betriebstauglichkeit von Software auch heute noch mit ziemlich hölzernen Methoden eruiert: zum Beispiel, indem die Programmentwickler ihre Produkte mit standardisiertem Input füttern und dann messen, wie schnell und zuverlässig die Daten verarbeitet werden. Für die tägliche Praxis sind solche Tests leider nur bedingt aussagekräftig, weil die Betriebssicherheit eines Programms auch von den äusseren Umständen abhängt.

Mann müsste also das System in möglichst wirklichkeitsnahen Situationen testen. Bei einer so vielseitigen Maschine wie dem Computer kann man aber nur einen winzigen Bruchteil aller denkbaren Fälle ausprobieren. Fazit: Die Gewissheit, dass kein Software-Fehler auftreten wird, hat man nie. Wenn man in der Testphase der Software-Entwicklung Fehler entdeckt und ausmerzt, sollte die Zuverlässigkeit des Programms eigentlich zunehmen.

Man muss das tatsächlich so vorsichtig formulieren, denn die Voraussetzung dazu ist, dass sich durch die Korrekturen nicht wieder neue Fehler einschleichen, was leider, auch aus eigener Erfahrung, sehr häufig vorkommt.

## Crash statt Cash bei der EBS

Anfangs Mai 95 in den Handelsräumen der SBG: 40 Börsenhändler hatten nach Arbeitsschluss anzutreten, um einen umfangreichen Testlauf auf dem neuen Handelssystem der elektronischen Börse Schweiz zu absolvieren. Nun, nachdem insgesamt gegen 40 Minuten benötigt wurden, bis alle Geräte aufgestartet waren, dauerte es gerade ganze drei Minuten, bis das System zusammenbrach. Aus Händler- und Informatikerkreisen, die ins EBS-Projekt involviert sind, ist unter der Hand zu hören, dass die Funktionsfähigkeit des Systems noch weit hinter den Versprechungen hinterherhinkt, dementsprechend stellt man laufend Mängel fest. Die Lösung dieser Mängel kommt jedoch nicht so

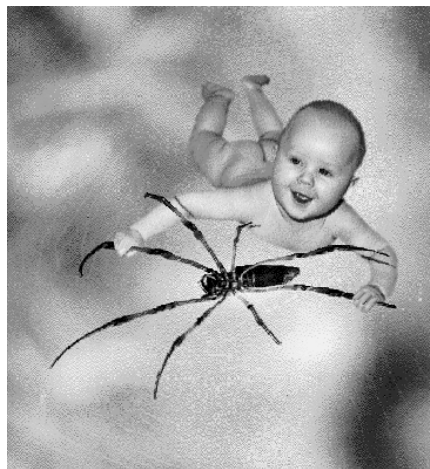
recht voran, denn die Probleme sind komplex und der Dämon liegt im Detail. EDV-Projekte dieser Größenordnung sind aufwendig und im Zeitaufwand unberechenbar, das ist heute eine allgemeine Erkenntnis. Jedoch die Erkenntnis mit zunehmender Komplexität auch vermehrt mit intertemporalen, nichtlogischen Zustandsänderungen (Magic Logic) rechnen zu müssen, ist für viele Projektleiter noch kein Thema.

## Wie die Spinne im Netz

Wie viele Fehler im System stecken, mag wohl eine interessante Zahl sein, aber isoliert betrachtet sagt sie wenig aus. Ein System mit vielen, selten auftretenden Fehlern kann nämlich durchaus zuverlässiger sein als eines mit wenigen Fehlern, die dafür umso häufiger vorkommen. Die Erfahrung zeigt, dass die erste Variante eher der Realität entspricht als die zweite: Selbst nach sprichwörtlich Tausenden von Betriebsjahren (man untersuchte gleichzeitig viele Geräte) fördern komplexe Systeme immer wieder neue Fehler zutage; dazwischen arbeiten sie zu voller Zufriedenheit der Anwender. Seit dem Internet-Boom und der zunehmenden Vernetzung droht jetzt auch noch Gefahr von aussen. Nicht nur die rasante Zunahme von Viren sondern Hacker.

Das Phänomen der Hacker ist so alt wie ein IBM AT. In Europa startete die Story mit dem Hamburger Chaos-Computer Club im Jahre 84. Vor einigen Wochen sorgte der Fall des Biochemie-Studenten Levin aus St. Petersburg für Schlagzeilen: Er hatte den Computer des USA-Bankkonzerns Citicorp geknackt und dabei rund 12 Millionen Dollar an Kundengeldern illegal auf fremde Bankkonten überweisen lassen.

Levin und etliche seiner Komplizen wurden zwar gefasst, doch nach den ersten Details vor einem New Yorker Gericht ist der Fall weitaus gefährlicher als angenommen. Denn Levin war es offenbar als erstem überhaupt gelungen, in eines der am besten geschützten Computersysteme einzudringen: ins vollelektronische Cash-Management der Bank, über das man jeden Tag ca. 500 Milliarden Dollar in alle Welt verschiebt - es hätte der grösste elektronische Bankraub der Geschichte werden können.



Im April 95 wird im Internet „SATAN“ (Security Administration Tool for Analyzing Network) veröffentlicht, ein Programm, das die Sicherheitslücken anderer Rechner aufzeigen soll. Einmal entdeckt, gibt es kein Entrinnen mehr, denn die Spinne ist überall. „SATAN“ löst eine weltweite Kontroverse aus.

Wie in allen Belangen der Sicherheit gilt auch hier: erkannte Risiken sind kalkulierbar. Eine hundertprozentige Sicherheit gibt es aber auch hier nicht; immer wieder entstehen neue Löcher, welche neue Abwehrmechanismen erfordern. Trotzdem kann eine überwachte und gewartete Firewall (elektronische Filter und Türhüter) das Risiko minimieren.

Übrigens, topaktuell im Kino ist der Film „The Net“, der in beklemmender Weise den Hacker-Dschungel schildert worauf Angela plötzlich zur Gejagten wird. Ihre Gegner benutzen nicht nur herkömmliche Waffen, sondern auch das Internet: Sie verpassen Angela im Regierungscomputer eine neue Identität. Plötzlich ist sie eine Frau, die wegen Drogendelikten und Prostitution gesucht wird.