COMPUTER

Würdevoller Verfall

Je komplexer die Programme werden, desto eher kommt es zum Absturz. Experten empfehlen daher einen intelligenteren Umgang mit dem Fehler.

Der amerikanische Transporthubschrauber „Osprey" gilt als einer der innovativsten der Welt. Trotzdem begann auf einem Übungsflug im US-Bundesstaat North Carolina vor gut drei Jahren eine der Maschinen plötzlich unkontrolliert zu schlingern. Hartnäckig verweigerte der Bordcomputer den Dienst. Verzweifelt drückte der Pilot den Reset-Knopf, um den Rechner neu hochzufahren – vergebens. Der Helikopter zerschellte, vier Besatzungsmitglieder starben.

Tragische Computerabstürze gehören zum Alltag von Peter Ladkin, Professor für Computersicherheit an der Universität Bielefeld. In Dutzenden Fachaufsätzen hat er immer wieder vor der Verletzlichkeit moderner Steuersysteme gewarnt, wie sie in Flugzeugen, Kraftwerken, Börsen oder Bankautomaten eingesetzt werden.

„Viele tausend Leute zerbrechen sich seit Jahren den Kopf, wie man Computerfehler ausmerzen kann, bislang ohne durchschlagenden Erfolg", berichtet Ladkin. „Moderne Systeme sind einfach zu komplex, um jede Fehlerquelle vorher zu erkennen."

Jeder Büroangestellte kennt das Grundproblem vom eigenen PC: Betriebssysteme werden immer umfangreicher, ständig werden sie erweitert durch Treiberprogramme für Drucker, Kameras, Scanner und allerlei Daten aus dem Netz. Unweigerlich steigt damit auch die Zahl möglicher Fehler.

Früher berechnete man die Zuverlässigkeit eines Programms in der Maßeinheit „Fehler pro 1000 Zeilen Programmcode". Im Endanwenderbereich liegt diese Quote bei bis zu fünf; in sicherheitsrelevanten Bereichen wie Medizin, Luftfahrt und Militär wird sie dank besonderer Sorgfalt bis auf etwa eins gedrückt. Die dann verbleibenden Fehler auch noch zu tilgen ist so gut wie nicht zu schaffen.

Das Problem ist nun: Moderne Betriebssysteme umfassen rund 40 Millionen Zeilen Programmcode, was ausgedruckt einem haushohen Papierstapel entsprechen würde. Die Fehlersammlung allein hätte Telefonbuchformat. Und sie wächst mit jedem Update weiter.

„Man wird wahnsinnig, wenn man sich vorstellt, was da alles schief gehen kann", sagt die kalifornische Programmiererin und Essayistin Ellen Ullman. Die wirtschaftlichen Schäden, die durch fehlerhafte Software verursacht werden, sind immens. Fast 60 Milliarden Dollar gehen jedes Jahr allein in den USA durch computerbedingte Produktionsausfälle und kostspielige Reparaturen verloren, schätzt George Candea von der kalifornischen Stanford University; in der Mobilfunkbranche dürften sich die Schäden auf immerhin acht Milliarden Dollar weltweit belaufen.

Als Gegenmittel schlägt Candeas Arbeitsgruppe jetzt ein grundlegendes Umdenken vor: „Da wir Computer- und Bedienungsfehler nicht ausmerzen können, sollten wir sie einfach als Tatsache akzeptieren und lernen, mit ihnen umzugehen." Technikkundige, die natürlich Bescheid wissen über die Verletzlichkeit von Systemen, hätten das häufig ohnehin längst eingesehen: „Die haben einen normalen Umgang mit dem Scheitern entwickelt, ein alltägliches Verhältnis zum Desaster."

Schadensbegrenzung statt Fehlervermeidung heißt das Prinzip neuartiger „absturzorientierter Programme" („Crash-only Software"). Der Trick dabei: Ein Programm wird in möglichst viele kleinteilige Ablaufkomponenten unterteilt, die gleichsam durch digitale Brandschutztüren voneinander getrennt sind. Tritt nun irgendwo ein Fehler auf, wird lediglich der kleine betroffene Programmteil neu gestartet – ohne gleich das ganze Programm mit in den Absturz zu reißen.

Fehler gelten folglich nicht mehr als katastrophale Ausnahme, sondern als hinnehmbare Regel. Und die Anwender bekommen vom ständigen Stolpern und Aufrappeln des Systems gar nichts mehr mit. In einem Testlauf für eine Satelliten-Bodenstation hat sich ein Programm der Absturzartisten bereits bestens bewährt. Auch in Deutschland werden inzwischen ähnliche Systeme entwickelt: Seit Anfang Februar zieht ein besonderer Sicherheitsrechner für das neue Gewinnspiel „Keno" von Lotto Hessen die Zahlen – mit einer Technik, die zuvor bereits in Satelliten erprobt wurde.

„Selbst wenn es alle paar Sekunden zu einer Störung käme, liefe die Ziehung ungestört weiter", berichtet Sergio Montenegro vom Fraunhofer-Institut für Rechnerarchitektur und Software-Technik in Berlin-Adlershof, das dieses System auch auf der Cebit vorgestellt hat.

„Graceful degradation" wird das neue Prinzip im Fachjargon genannt. Ein solcher „würdevoller Verfall" hätte der Besatzung des „Osprey"-Hubschraubers möglicherweise das Leben retten können, glaubt der Bielefelder Professor Ladkin. „Allerdings sind absturzfreundliche Systeme kein Allheilmittel", warnt er. „Grobe Programmierfehler kann selbst die sanfteste Absturzmethode nicht kaschieren."

HILMAR SCHMUNDT

DOUG BENC / AP

JEFF TOPPING / REUTERS / E LANCE MEDIA

„Osprey"-Helikopter, Absturzstelle: *Schon die Fehlersammlung eines modernen Betriebssystems hätte Telefonbuchformat*