Universität Koblenz

Seminar: Berühmt berüchtigte Softwarefehler

Bernhard Beckert

AT&T - Ausfall des Telefonnetzes in den USA

Jörg Sesterhenn

SS03

Zusammenfassung

In diesem Seminar wurden Softwarefehler in verschiedenen Projekten analysiert. Dabei ging es unter anderem darum, wie es zu diesen Fehlern kommen konnte, welche Folgen sich ergaben und ob der Fehler hätte verhindert werden können. Ferner haben wir uns die Frage nach den Verantwortlichen gestellet und versuchten Schlüsse daraus zu ziehen.

Im Folgenden wird der durch einen Softwarefehler hervorgerufene Ausfall des Telefonnetzes in den USA im Jahr 1990 betrachtet. Die Ereignisse und deren Folgen werden geschildert und analysiert.

Inhaltsverzeichnis

1 Wer ist die AT&T?

Um den Zusammenhang zwischen AT&T (American Telephone and Telegraph Corporation) und dem Telefonnetz der USA zu klären, werde ich an dieser Stelle einen kurzen Abriss über die Geschichte von AT&T geben.

Die AT&T übernahm 1899 Bell Systems und begann den Aufbau des Telefonnetzes. 1913 wurde AT&T verpflichtet sein Telefonnetz den Mitbewerbern zu öffnen.

Nicht nur in Sachen Telekommunikation war die AT&T Pionier. Auch auf anderen Gebieten der Technologie führten sie Innovationen ein, bei denen heute nicht mehr jeder sofort an die AT&T denkt. So entwickelten sie 1950 die Solarzelle, 1969 die Programmiersprache C und das Betriebssystem Unix. 1983 folgte die erste Version von C++ [1]. Bereits 1974 hatte AT&T weltweit 300 Millionen Telefone installiert [ATT03].

[1] C++ wurde von Bjarne Stroustrup bei AT&T entwickelt.

2 Was ist passiert?

Das AT&T-Telefonsystem bestand 1990 aus einer Zentralstelle in New Jersey und 114 vernetzten regionalen Schaltzentralen. Am 15. Januar 1990 kam es zu einer Fehlfunktion in einer Schaltzentrale in Manhattan. Dies führte zu einer Kettenreaktion, in deren Folge 70 Mio. von 138 Mio. Ferngesprächen innerhalb der USA über 9 Stunden lang nicht vermittelt werden konnten.

Die Schaltzentrale in New York setzte sich nach einer Fehlfunktion in den Reset-Modus. Dieser bestand aus mehreren Schritten, die nacheinander ausgeführt wurden:

1. Eine Ausfall-Meldung wurde an alle anderen Schaltzentralen gesendet.
2. Die internen Routing-Tabellen der Schaltzentrale wurden zurückgesetzt (Reset).
3. Eine OK-Meldung ging an alle anderen Schaltzentralen.
4. Neu ankommende Ferngespräche wurden weitergeleitet.
5. Alle Schaltzentralen aktualisierten ihre Tabellen.

Während dieser Prozedur trat nun der eigentliche Fehler auf:

Bei drei Schaltzentralen kamen kurz nach der OK-Meldung neue Gespräche an. Die Verarbeitung der OK-Meldung und der neuen Gespräche führten zum Rechnerausfall, so dass auch diese Schaltzentrale in den Reset-Modus ging. Im Schneeball-System wurden so 9 Stunden lang fast alle Zentralen lahm gelegt. Als Notlösung wurde die Nachrichtenlast kurzzeitig reduziert und eine alte stabile Version der Schaltzentralen-Software wurde eingespielt [NEU90].

Der durch den Systemausfall entstandene Schaden hatte ganz unterschiedliche Formen. Der finanzielle Schaden belief sich auf 75 Millionen US $ bei AT&T und den Tochtergesellschaften und mehreren 100 Millionen US $ bei den Kunden (Versandhandel, Transportunternehmen, Reisebüros usw.), ohne die Folgeschäden durch entfallene Aufträge.

Darüber hinaus wurde das Firmen-Image empfindlich geschädigt. Bei den Kunden kam es zu einem Vertrauensverlust gegenüber AT&T, aber auch gegenüber der Technik im Allgemeinen.

Dieser Systemausfall hatte aber neben den naheliegenden Konsequenzen auch weitreichende Folgen. Der Verdacht auf einen Hackerangriff führte zur Novellierung der Gesetze zur Computerkriminalität in den USA [BRU92].

3 Was waren die Ursachen?

Als Ursache für den Ausfall könnte man den ständig wachsenden Grad der Automatisierung technischer Systeme nennen. Im Zuge der technischen Revolution wurden Systeme immer komplexer und undurchsichtiger, was eine manuelle Wartung unmöglich machte. Man versuchte automatische Sicherheitsroutinen gegen Pannenszenarien zu entwickeln, und sah die damit zusammenhängenden Risiken erst viel zu spät.

Dem offiziellen Bericht von AT&T ist zu entnehmen, dass der Fehler nicht auf eine Überlast im System zurückzuführen war ("calling volume was not unusual"), sondern auf eine Serie unglücklicher Zufälle, die nie zuvor aufgetreten war ("a series of events that had never occurred before") [GOO90].

Der eigentliche Fehler war eine falsch eingesetzte Break-Anweisung in der Fehlerbehandlungsroutine, die durch ein Softwareupdate vier Wochen zuvor ins System aufgenommen wurde. Seit diesem Zeitpunkt war der Fehler latent im System, hätte also auch durch weiteres Testen bemerkt werden können. Der Fehler war beim Testen der neuen Version jedoch nicht gefunden worden, da die Break-Anweisung innerhalb einer If-Anweisung ausgeführt werden sollte, deren Bedingung während des Testens jedoch nie erfüllt war. Die Testroutine deckte also nicht alle möglichen Fälle ab.

Folgender Pseudocode diene der Verdeutlichung des Fehlers:

```
switch expression {
[...]
case (value):
if (logical) { //dieser Fall trat beim Testen nie auf !
<statements>
break;
} else {
<statements>
}
<statements>
[...]
}
```

Das Ausmaß des Systemausfalls ist auf einen zweiten Fehler zurückzuführen:

Das Update wurde direkt im gesamten System durchgeführt. Das ist ein deutliches Zeichen für die Technikgläubigkeit der damaligen Zeit - man vertraute auf die Robustheit des Systems und der Fehlerbehandlungsroutinen. Dieser Mangel an Fehlerbewusstsein und der Glaube an die Unverwundbarkeit des Systems sind die größten Fehler die man AT&T vorwerfen kann [ACM90, NW90] zitiert nach [SOF03].

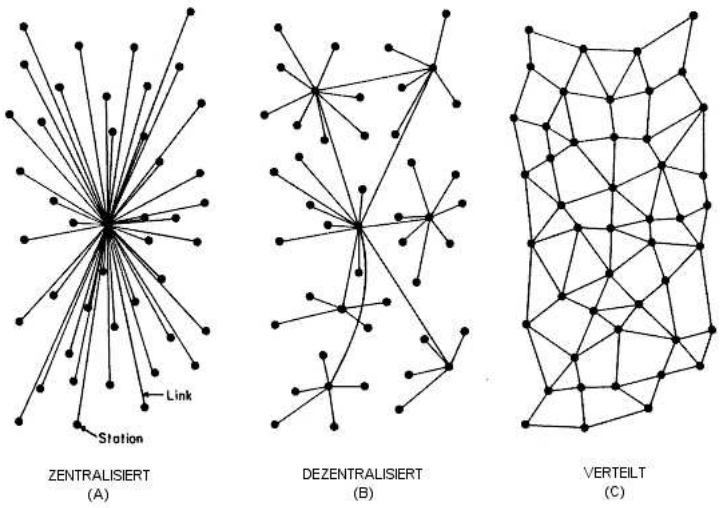

Abbildung 1: Netzwerke im Vergleich

4 Wie hätte der Fehler verhindert werden können?

Bis in die 20er Jahre musste man eine Vermittlungsstelle anrufen um ein Ferngespräch führen zu können. Hier wurden die notwendigen Daten aufgenommen und der Anrufer konnte wieder auflegen. Die Vermittlungsstelle leitete die Informationen zur Zentrale weiter, die ihrerseits die beste Route nachschlagen musste um sich nacheinander mit allen Vermittlungsstellen entlang dieser Route verbinden zu lassen. Wenn der Angerufene dann das Gespräch angenommen hatte, wurde der Anrufer zurückgerufen. Das dauerte damals im Durchschnitt 7 Minuten.

Ende der 40er wurde es durch neue technische Möglichkeiten und eine Hierarchisierung der Vermittlungsstellen ermöglicht, dass zum Verbinden des Gesprächs nur noch eine Vermittlungsstelle kontaktiert werden musste, was durchschnittlich 30 Sekunden dauerte.

Das hierarchische System wurde erst in den 80er Jahren zu einem dynamischen System umgestellt. Mit der landesweiten Installation digitaler vollautomatischer Schaltzentralen (AT&T 4ESS) wurde es möglich, die Vermittlungszeit auf eine Sekunde zu reduzieren, um so ca. 300 Mio. Anrufe am Tag zu vermitteln.

Das neue System war in der Lage, sich selbst den besten Weg für eine Verbindung zu suchen.

Die Entwicklung vom zentralen (Abb.1a) zum hierarchischen (Abb.1b) und letztendlich zum verteilten System (Abb.1c) hatte nicht nur den Vorteil, Zeit und damit Geld zu sparen, sondern erhöht auch die Ausfallsicherheit des Systems, da es gegen Ausfälle einzelner Schaltzentralen unempfindlicher wird.

Auf der anderen Seite wächst der Aufwand Systeme zu warten, Fehler aufzufinden, Wechselwirkungen festzustellen mit dem Grad der Automatisierung und Dynamisierung der Systeme. Das bringt die Notwendigkeit von automatischen Fehlerbehandlungsroutinen und damit auch neue Probleme und Verantwortung mit sich.

Man hätte diesen Fehler vermeiden können, hätte man die Fehlerbehandlungsroutine hinreichend getestet. Da das System fast 4 Wochen lief, bevor der Fehler sich bemerkbar machte, kann hier auch nicht das Argument des Zeitmangels eingebracht werden.

Besonders da es sich hier um ein kritisches System handelt von dessen Stabilität vieles abhängig ist, wäre es notwendig und wichtig gewesen, das System anhand seiner Spezifikation zu verifizieren. Verifikation von verteilten parallelen Systemen ist zwar sehr aufwendig, kostspielig und nicht immer möglich, aber in diesem Fall hätte die Verifikation von Teilaspekten die fehlerhafte Break-Anweisung aufgedeckt.

Das Ausmaß des Absturzes hätte wesentlich verringert werden können, indem man das Sicherheits-Update nicht gleichzeitig auf allen Schaltzentralen eingespielt hätte. Stattdessen hätte man die neue Software in mehreren Schritten einführen können.

5 Was können wir daraus lernen?

Komplexe Systeme zu verifizieren ist schwierig bis unmöglich. Dennoch sollte insbesondere bei kritischen Systemen, wie etwa dem Telefonnetz, Verifikation zumindest für die Teilaspekte des Systems herangezogen werden, für die sie durchführbar ist.

Wir können Fehler in komplexen Systemen eindämmen aber nie ganz ausschließen. Softwareupdates können also instabile Systeme erzeugen. Daher ist es wichtig, in alle Überlegungen die Möglichkeit von Fehlern einzubeziehen. In diesem Fall hätte das bedeutet ein Systemupdate in mehreren Schritten durchzuführen.

Es gibt keine kleinen Fehler. Gerade solche Fehler, die in Standart-Szenarien nicht auftreten, können fatale Auswirkungen haben, wie in diesem Fall.

Wir sind heute von vielen komplexen Systemen abhängig (Telefon, Strom, Verkehr, Internet, ...). Wir sind auf das ständige Funktionieren dieser Systeme angewiesen. Wenn es um Änderungen an diesen Systemen geht, ist höchste Vorsicht geboten.

6 Weitere Softwarefehler im Bereich Telekommunikation

In den 90'er Jahren blieb dieser Softwarefehler kein Einzelfall im Bereich der Telekommunikation. Nachfolgend seien nur einige Beipiele genannt.

1. USA, Lokales Telefonnetz, Juni/Juli 1991:
   Das Telefonnetz war innerhalb einer Woche in Washington, Los Angeles und Pittsburgh stundenlang lahm gelegt. Ursache waren drei falsche Bits in einem 2 Millionen-Zeichen-Programm.

2. Notrufsystem England, März 1992:
   Programm der British Telecom, das Notrufe zur Ambulanz-Zentrale durchstellen und dort verteilen sollte, versagte. Den Hilfesuchenden wurde nur "Bitte warten" vorgespielt. Einige Anrufer verstarben während dieser Wartezeit.

3. AOL wählte bei der Einwahl ins Internet den Notruf:
   (9 für Amtsleitung, 1170 warten auf Freizeichen deaktivieren, Rufnummer)
   Beispiel: 911 70 12345689. Das führte zum Chaos in den Notrufzentralen.

4. Schnurloses Telefon Kanada, 1993:
   Das Mobiltelefon wählte selbst durch zufällig empfangene Frequenzen den Notruf 911.

Literatur

[SOF03] Software Research Inc.:'TCAT Application to AT&T Phone System Crash', http://www.soft.com/AppNotes/attcrash.html, 11.04.2003

[NW90] Newsweek: 'Can We Trust Our Software?', 29.01.1990

[ACM90] ACM SIGSOFT, Software Engineering Notes,Vol.15, No. 2, Page 11ff, April 1990

[NEU90] Neumann, Peter G.: 'Cause of AT&T network failure', The Risk Digest 26.01.1990, http://catless.ncl.ac.uk/Risks/9.62.html

[GOO90] Goodfellow, Geoff: 'AT&T Crash Statement: The Official Report', The Risk Digest 31.01.1990, http://catless.ncl.ac.uk/Risks/9.63.html

[BRU92] Sterling, Bruce : The Hacker Crackdown, 1992, http://www.mit.edu/hacker/hacker.html

[ATT03] History of the AT&T network, http://www.att.com/spotlight/nethistory/