

Systemrelevante Spezialisten

Schießen Sie nicht auf den Programmierer!

Kay Behrmann über IT-Abhängigkeit

Kürzlich gab der Finanzminister bekannt, wie viele Banken er in Deutschland für systemrelevant hält. Es sind 36. Leider wird nicht verraten, welche das im Einzelnen sind. Zu gruselig die Szenarios von Schlangen wechselwilliger Kunden, die Ihr Geld zu staatlich anerkannten Relevanzinstituten transferieren wollen.

Aber die Mitarbeiter der betroffenen Häuser müssten es merken. Und auch wir Techniker, die externen Berater eingeschlossen, sollten erhöhte Aktivität bei aufsichtsrelevanten Projekten feststellen. Überhaupt hat der Finanzminister das Thema „Ausfallsicherheit“ ja eigentlich von uns geklaut. Instabile Großbanken mögen etwas neues sein, instabile IT-Systeme aber nicht. Backup, Ersatzserver und Failover-Prozeduren gehören zum Projektalltag, denn einen Systemabsturz hat jeder PC-Nutzer schon erlebt. Auch der Projektmanager der Fachabteilung, der das Budget für den Ersatzserver abzeichnen muss.

In einem – zugegeben extremen – Fall durfte ich Bekanntschaft mit einer Einkaufsrichtlinie machen, die bei der Beschaffung neuer Server immer den Kauf vier baugleicher Geräte vorschrieb. Eines für Entwicklung, eines für Tests, eines als Ausfallgerät und eines für den produktiven Betrieb. Gängig sind heutzutage zumindest Ersatzsysteme, die im einfachsten Fall als „cold standby“ und bei risikobewussten (und budgetgesegneten) Anwendern als „hot standby“ auf den Ernstfall warten, je nach Wärmegrad mehr oder weniger einsatzbereit.

Bei Prüfern stehen die technischen Sicherungsmaßnahmen meist auch auf der Checkliste. Nach meiner Erfahrung wird in der Praxis grundsätzlich die Dokumentation geprüft, gelegentlich wird nach Protokollen der Testläufe gefragt. Bemerkenswert selten fragen Prüfer nach technischen



Kay Behrmann ist selbständiger IT-Berater
www.vv.de

Details oder einer Demonstration. Wenn die Doku stimmt, würden viele Prüfer auch einen Schuhkarton als Ersatzserver akzeptieren. Das ist in der Praxis nicht tragisch, weil die IT-Abteilung ausreichend Eigeninteresse an einer funktionierenden Einrichtung hat.

Der folgende Text ist nicht für Terroristen geeignet. Lesen Sie nicht weiter, wenn Sie systemrelevanten Schaden anrichten möchten. Denn neben Abhängigkeit von der Technik hat praktisch jede Bank auch Abhängigkeiten zu Technikern mit Spezialwissen entwickelt. Vor einigen Wochen erfuhr ich von einem Fall einer Frankfurter Bank, die einen „Over-Night-Job“ zur Verteilung von Abwicklungsdaten für Zahlungsverkehr und Wertpapierhandel installiert hat. Das Programm ist klein, aber wichtig, und es gibt nur drei Menschen, die es beherrschen. Einer davon ist ein externer Berater (der Glückliche). Die anderen beiden waren kürzlich gleichzeitig krank, da fiel die Abhängigkeit auf. Das ist nicht ungewöhnlich. Ich würde persönlich eine Wette eingehen, dass es reichen würde, eine kleine Anzahl von (vielleicht zehn) Technikern der Frankfurter Bankenwelt zu entführen, um wesentliche Teile des Finanzsystems lahmzulegen. Es müssten nur die richtigen sein.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinem „Grundschutz-Katalog“ auch Vertretungsregelungen thematisiert. Unter anderem wird sogar der Einsatz „externer Kräfte“ angeregt. Was übrigens zu einer beliebten Strategie führen kann: Mit Outsourcing kann auch die Personalabhängigkeit ausgelagert werden. In dem Fall mit dem „Over-Night-Job“ werden nun größere Teile der technischen Abwicklung an einen Dienstleister ausgelagert, das Vertretungsproblem ist in der Bank kein Thema mehr. Bei dem Dienstleister gibt es übrigens zwei Programmierer, die dort den Job bedienen können.