IT-Sicherheit

# Datenschutz und Abhörskandal

## Kay Behrmann über Sicherheitslücken und Schutzmaßnahmen

Es ist über dreißig Jahre her, dass ich mit Familie über die innerdeutsche Grenze zu Tante Meta zum Kaffeetrinken fuhr. Als wir uns an ihrem Wohnzimmertisch niederließen, zog sie noch schnell das Telefonkabel aus der Buchse „... Ihr wisst schon.". Wir wussten nicht. Im Flüsterton klärte sie uns auf, das Hörermikrofon könne von der Stasi auch im aufgelegtem Zustand zum Abhören genutzt werden. Vor dem Kaffeeklatsch war es üblich, erst den Stecker zu ziehen.

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

Nachdem letztes Jahr die New York Times von Sicherheitslücken im Polycomm Konferenzsystem berichtete, war das Tante-Meta-Verhalten gelegentlich auch in Besprechungsräumen der Finanzwelt zu beobachten. Ein Hacker war über das Netzwerk in dutzende Firmen eingebrochen und konnte unberechtigt auf Kamera und Mikrofon zugreifen. Er verschaffte sich Zugriff auf Konferenzsysteme einer Rechtsanwaltskanzlei, einem Gericht und kam sogar bis in die Vorstandsetage von Goldman Sachs. Nach der Veröffentlichung seines Coups wurde der Polycomm-Anlage gelegentlich ebenfalls erst mal der Stecker gezogen.

Vielleicht werden künftig auch Laptops aus Konferenzen verbannt. Schon lange können bösartige Trojaner Mikrofon und Kamera unter Windows anzapfen. Neue Würze bringt das aktuelle Geständnis von Microsoft, auch Skype-Gespräche und -Chats in Kooperation mit der amerikanischen Sicherheitsbehörde NSA abzuhören. Aber auch Apple, Google, Facebook und Yahoo haben der NSA Zugriff auf Kommunikationsdaten ihrer Kunden gewährt.

Hierzulande werden Vermögensverwalter und BaFin-regulierte Family Offices einmal jährlich auf IT-Sicherheit hin geprüft. Sollten sie jedenfalls. Die Vorschriften im Kreditwesengesetz enthalten großen Auslegungsspielraum; das Wort „angemessen" kommt im relevanten §25a neun Mal vor. Auch die Gesetzesauslegung in der MaRisk-Verordnung ist nicht viel besser. Sie gibt zwar vor, „die Vertraulichkeit der Daten sicherzustellen", hat aber keinen Tipp parat, was dazu konkret zu tun wäre. Erfahrungsgemäß entwickeln Prüfer in diesem Thema kein großes Engagement zur Definition, was „angemessen" ist. Und nicht selten ist die IT-Prüfung nach wenigen Minuten erledigt, wenn Firewall und Berechtigungskonzept einen guten Eindruck machen.

Diejenigen Institute, die über die Pflichtprüfung hinaus einen Auftrag zur IT-Sicherheitsprüfung an entsprechende Spezialfirmen vergeben, dürfen dagegen Überraschungen erwarten. In den Fällen, die ich bisher begleiten konnte, gab es die ausnahmslos. Da war der Prüfer mit den coolen Hacker-Tools, der das Admin-Passwort der Bank in wenigen Minuten knacken konnte. Ein anderes Mal kam ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierter Auditor, zwar ohne Hacker-Tools (enttäuschte Gesichter bei den IT-Mitarbeitern), aber mit ausgefeilten Checklisten. Er stellte unter anderem fest, dass im Serverraum der Feuerlöscher fehlte.

Die IT-Grundschutzkataloge des BSI sind mittlerweile ca. 4000 Seiten stark und beschreiben detailliert mögliche Gefahren und Schutzvorkehrungen. Mit dem zugehörigen Standard ISO 27001 teilt dieses Werk das Schicksal, in der täglichen Praxis oft nicht anzukommen. Die Diskrepanz der vorgeschriebenen, aber unspezifischen „Vertraulichkeit der Daten" einerseits, und einer Unmenge an konkreten Bedrohungen und Gegenmaßnahmen andererseits, ist für Vermögensverwalter und Family Offices ein Problem. Übrigens ein Problem, das auch das amerikanische Verteidigungsministerium (DoD) beschäftigte. Auch dort störte diese Diskrepanz. Man erarbeitete deshalb eine Liste von 20 "Critical Security Controls" als Richtlinie für die Praxis. Die Liste wurde inzwischen veröffentlicht und wird auch in Banken eingesetzt, um die Maßnahmen zur IT-Sicherheit zu priorisieren. Die Entstehungsgeschichte der Liste enthält zudem ein interessantes Detail. Vom Weißen Haus kam nämlich die Vorgabe „offense must inform defense", also das Gebot zur Nutzung von Erfahrungen aus Angriffen zur Abwehrplanung. Das führte dazu, dass der erste Entwurf unter Federführung der für Cyber-Angriffe zuständigen Stelle geschrieben wurde: der NSA.