

Anzeige



Mit dem Executive MBA in
General Management besser da stehen.



NZZ Online

Dienstag, 23. März 2010, 16:57:01 Uhr, NZZ Online

Nachrichten > Digital

20. März 2010, Neue Zürcher Zeitung

Wie dem Diebstahl von Daten begegnen

Heikle Verwaltung von Kundeninformationen



Sind die Daten von Computern der Credit Suisse kopiert worden? (Bild: pd)

Der Diebstahl von Daten hat erhebliche Schäden für die betroffenen Unternehmen zur Folge. Oft werden wirksame Schutzmechanismen aus Unwissenheit oder mangelndem Risikobewusstsein nicht umgesetzt.

Didier Assandri

Die Nachrichtensendungen berichten zurzeit gehäuft von Datenmissbrauch – von vertraulichen Daten, die kopiert wurden und sich in Händen wiederfanden, für die sie nicht bestimmt waren. Diese Missbrauchsfälle machen deutlich, wie wichtig es ist, sich mit den Themen Informationssicherheit und Datenschutz zu befassen. In den meisten Fällen sind sich die Unternehmen der Risiken nicht bewusst, und wenn sie es sind, sind sie vielfach ohne wirksamen Schutz. Ein böses Erwachen gibt es im Schadenfall, bei dem es um hohe Summen gehen kann und der oftmals einen erheblichen Imageverlust zur Folge haben kann.

Aber wie können diese folgenschweren Datenlecks entstehen? Aus den bekannten Fällen kann man folgende Schlüsse ziehen: Der Grossteil der Datenverluste ist auf interne Quellen, also auf demotivierte oder unehrlche Mitarbeiter, zurückzuführen oder ist Folge von Nachlässigkeit. Die IT ist für viele Geschäftsführer, Verwaltungsräte und Manager eine hermetisch abgeschlossene und unbekannte Welt. Die Überwachung und Kontrolle des IT-Personals ist ein wichtiges Element des Risikomanagements in Unternehmen. Inzwischen können grosse Datenmengen auf einfachen USB-Schlüsseln oder Laptops gespeichert werden, was die Kontrolle des Datenflusses zusätzlich erschwert. Der Gesetzgeber hat 2009 die Rahmenbedingungen für die Vermeidung von Datenmissbrauch geschaffen (OR Art. 728), und zwar mit der Auflage, dass ein internes Kontrollsystem aufzubauen ist. Es gibt auch internationale Regeln, die eine solche Kontrolle verlangen (etwa Sarbanes-Oxley, Basel II), aber es bleibt noch viel Raum für Verbesserungen.

Die Corporate Governance von Informatikdaten in Finanzinstituten hat viele Schwachstellen, sei es wegen Unwissenheit oder aus Resignation: Ein einfacher IT-Administrator hat oftmals Zugriff zum gesamten Datenbestand. Eine solche Situation ist aus objektiver Sicht nicht nachvollziehbar. Ein IT-Administrator soll eine reibungslose Arbeit des IT-Systems sicherstellen und nicht den Inhalt kontrollieren. Um ein einfaches Beispiel zu nennen: Der Garagist braucht für die technische Überprüfung eines Autos keinen Zugang zum Inhalt des Kofferraums.

Geeignete Lösungen existieren und liegen in erster Linie in der Corporate Governance der Datenverarbeitung. Im Wesentlichen geht es um die Verwaltung der Rollen (Wer darf was?), der Identitäten (Wer ist wer?) und der Datenzugriffe (Wer hat Zugriff?), aber auch um die Verschlüsselung der Daten (wobei die Verschlüsselungscodierung der IT-Abteilung unbekannt sein sollte) und die Trennung der Aufgaben (der Auftraggeber darf einen Auftrag nicht gleichzeitig autorisieren und durchführen).

Hinzukommen sollte die direkte Einbindung des Verwaltungsrates, der seiner Kontrollfunktion auch im Bereich des intellektuellen Eigentums nachkommen muss (OR Art. 716a). Auch hier stellt sich die Frage: Wie kontrolliert man etwas, das man nicht im Griff hat? Wie viele Informatiker sitzen in den Verwaltungsräten? Wie stelle ich sicher, dass ein IT-Administrator nicht gleichzeitig für die IT-Sicherheit zuständig ist? Welche Möglichkeiten hat ein Abteilungsleiter, um in Echtzeit zu kontrollieren, wer Zugang zu den Daten seiner Abteilung hat? Und nicht zu vergessen: Welche Massnahmen zur Vermeidung interner Übergriffe wurden ergriffen, um die sensibelsten Bereiche einer Unternehmung, wie Finanzen, Recht, Vertrieb sowie Forschung und Entwicklung, zu schützen? Nur wenige Unternehmen sind in der Lage, auf diese Fragen klare Antworten zu geben.

Eine solcherart ausgestaltete Governance gewährleistet eine interne Risikokontrolle im IT-Bereich, da sie eine Aufgabenteilung im Unternehmen ermöglicht; sie trennt diejenigen Akteure, die die Sicherheitspolitik definieren, von denen, die sie umsetzen. Die wirtschaftlichen Risiken sind enorm,

da heutzutage fast alles numerisch vorhanden ist und so innerhalb weniger Sekunden kopiert, heruntergeladen werden kann und damit verfügbar ist.

Ob sich die Banken für die skizzierten Massnahmen entscheiden oder nicht: Klar ist, dass die Loyalität der Angestellten stets der Schwachpunkt in den Sicherheitsfragen einer Firma sein wird. Es ist unvermeidbar, dass ein Angestellter sich fünf Kundenadressen pro Tag merkt und sie abends zu Hause aufschreibt. Aber es ist die Pflicht der Unternehmen, die «Türe» zu ihren Systemen nicht offenzulassen, so dass ein unehrlicher Angestellter sich bedienen kann. Denn Gelegenheit macht bekanntlich Diebe. Unternehmen erfüllen somit erst dann ihre Sorgfaltspflicht, wenn sie solche Gelegenheiten durch den Einsatz effizienter Lösungen, die durchaus bereits verfügbar sind, erschweren.

Didier Assandri ist Geschäftsführer der Solvis Ltd.

Diesen Artikel finden Sie auf NZZ Online unter:

http://www.nzz.ch/nachrichten/digital/wie_dem_diebstahl_von_daten_begegnen_1.5253883.html

Copyright © Neue Zürcher Zeitung AG

Alle Rechte vorbehalten. Vervielfältigung oder Wiederveröffentlichung zu gewerblichen oder anderen Zwecken ohne vorherige ausdrückliche Erlaubnis von NZZ Online ist nicht gestattet.
