INTERNES KONTROLLSYSTEM: DAS BEISPIEL DER DATEN- BZW. INFORMATIONSSICHERHEIT AM ARBEITSPLATZ

Vorsicht Datenklau und Datenmissbrauch

MONIKA ROTH

DATENMISSBRAUCH IST ZU EINEM WICHTIGEN THEMA GEWORDEN, WEIL ES SICH GEZEIGT HAT, DASS DAS RISIKOBEWUSSTSEIN OFT NICHT GENÜGEND AUSGEPRÄGT IST UND ES DESHALB AN WIRKSAMEN SCHUTZ- UND KONTROLLMECHANISMEN MANGELT. ABER AUCH DANN, WENN DIESES BEWUSSTSEIN VORHANDEN IST, IST DAS RISIKOMANAGEMENT NICHT EINFACH.

Im ICT-Zeitalter erhält der Datenschutz eine neue Dimension.

Ein Grossteil der Datenmissbräuche geht auf demotivierte und/oder unehrliche und zu deliktischem Verhalten bereite Mitarbeitende zurück. Die Vorfälle um HSBC, CS und LGT haben bestätigt, dass Mitarbeitende ein wichtiges operationelles Risiko darstellen. Ein internes Kontrollsystem ist deshalb auch in diesem Zusammenhang von zentraler Bedeutung und erfordert die Identifikation von Schwachstellen, die Festlegung der Schnittstellen sowie Transparenz bei den Verfügungsrechten über Daten.

INTERNES KONTROLLSYSTEM (IKS)

Ein IKS stellt die Einhaltung von Gesetzen und Vorschriften sicher. Es dient dem Schutz des Geschäftsvermögens und leistet gleichzeitig bei der Verhinderung, Verminderung und Aufdeckung von Fehlern und Unregelmässigkeiten wichtige Beiträge. Ein internes Kontrollsystem wirkt sich zum direkten Nutzen der Kunden aus. Das zeigen wiederum die genannten Vorfälle: Hätten die Banken die Datensicherheit im Griff gehabt und ihre Mitarbeitenden besser eingeschätzt, so wären die Kundendaten geschützt geblieben. Der Kunde darf davon ausgehen, dass sich ein Unternehmen dadurch auszeichnet, dass es seine wichtigsten Risiken kennt und dokumentiert hat und sodann Steuerungs- und Kontrollmassnahmen vorsieht und umsetzt. Es gibt unerlässliche Aspekte für ein IKS, die vorliegen müssen:

- Das IKS muss dokumentiert sein.
- Es muss in Umfang und Ausprägung den Unternehmensrisiken entsprechen.
- Alle Mitarbeitenden müssen das IKS verstehen und ihre Aufgaben und Kompetenzen kennen.
- Das Management lebt seine Vorbildrolle.
- Es herrscht ein Kontrollbewusstsein: Jeder ist zugleich Objekt und Subjekt der Kontrollen in den betrieblichen Abläufen und versteht deren Bedeutung.

Das IKS umfasst sämtliche vom Verwaltungsrat (Aufsichtsrat) und von der Geschäftsleitung (Vorstand) angeordneten Vorgänge, Methoden und Massnahmen, die dazu dienen, einen ordnungsgemässen Ablauf des betrieblichen Geschehens sicherzustellen, das betriebliche Vermögen zu sichern, deliktische Handlungen und Fehler aufzudecken oder zu verhindern sowie die Richtigkeit und Vollständigkeit des Rechnungswesens und das rechtzeitige Erstellen verlässlicher Finanzinformationen zu gewährleisten. Vermögenssicherung und Vermeidung von Missbräuchen aller Art innerhalb des Unternehmens stehen im Vordergrund.

Kontrolle ermöglicht den Vergleich zwischen Soll- und Ist-Werten. Sie ist unentbehrliche Grundlage zur Erreichung der Unternehmensziele. Kontrolle unterstützt die Durchsetzung der Handlungserwartungen, die von der Unternehmung an alle Mitarbeitenden gestellt werden.

Ziel des IKS ist es, die Risikolage im einzelnen Unternehmen transparent zu machen, allfällig bestehende Lücken in der Risikobeurteilung bzw. im Risikomanagement rechtzeitig aufzudecken, als Barometer für Veränderungen in der Risikolage zu dienen und die Schwachstellen gezielt auszumerzen. Im Fokus stehen Marktrisiken, Kreditrisiken und die operationellen Risiken. Eine der Kontrollkategorien ist Compliance. Compliance ist – wie die interne Revision – Bestandteil des internen Kontrollsystems. Die Prüfung durch die interne Revision erfolgt ungeachtet der konkreten Organisationsform von Compliance. Die Compliance als Funktion muss überwacht werden hinsichtlich Einhaltung der Vorgaben der Geschäftsleitung (Geschäftsführung) und hinsichtlich Änderungen der Normen, welche die Tätigkeit von Compliance beeinflussen können. Die Vorfälle betreffend Datenklau haben bestätigt, dass Mitarbeitende ein grosses operationelles Risiko darstellen. Die Berücksichtigung der Dimension «Mensch» ist essenziell. Dazu kommt im gegebenen Zusammenhang die Berücksichtigung finanzsektorspezifischer Besonderheiten: erhöhter Diskretionsbedarf, digitale Wertschöpfungskette, hoher Vernetzungsgrad, regulatorische Anforderungen.

OPERATIONELLE RISIKEN

- Kunden und Produkte
- Betrug
- Haftungsrisiken (Legal & Compliance)
- Verarbeitungsrisiken
- Personal
- System, physische Risiken

VERHINDERUNG DATENMISSBRAUCH

Klassische Massnahmen wie

- die Verwaltung der Rollen (Wer darf was?)
- die Verwaltung der Identitäten (Wer ist wer?)
- die Verwaltung der Datenzugriffe (Wer hat Zugriff?)
- die Verschlüsselung der Daten
- die Trennung der Aufgaben

sind zentral, aber je nach krimineller Energie eines Mitarbeitenden ungenügend. Heinrich Kieber, der ehemalige Angestellte der LGT Bank und Datendieb, beschreibt sein Vorgehen so: «Ich habe die (gemeint sind die Daten) nicht kopiert, ich habe ein DLT mitgehen lassen, das ist ein Magnetband, ein sogenanntes Tages-Backup-Band. Die Treuhand macht über Nacht eine Sicherungskopie auf einem handelsüblichen Magnetband. Das sieht aus wie so eine dicke, alte Kassette, ungefähr 12 mal 15 Zentimeter und 4 Zentimeter hoch. Der Ablauf bei der LGT war jeden Tag gleich. Ich habe gesehen, dass bei der alltäglichen Routine das Datenband für ein Weilchen bei der verantwortlichen Person auf dem Tisch lag, im Um-

kreis von meinem Arbeitsplatz. Die einzige Möglichkeit, es zu entwenden, ohne dass es jemand merkt, war natürlich, es auszutauschen. Ich hätte das Band jeden Tag austauschen können, es war ja ein wiederkehrendes Ritual. Ich musste keine Statistiken erstellen oder wie in Kriminalfällen Pläne und Grundrisse studieren oder so. Ich war schon zwei Jahre bei der LGT, extra eingestellt, um die Kundenakten zu digitalisieren. Ich sass sozusagen an der Quelle. Ich war ein bisschen nervös. Ich hatte einen normalen Tag. Ich hab das Band nach dem Mittagessen eingesteckt, ein leeres Band auf den Tisch gelegt und weitergearbeitet. Es gab keine Kameras in den Büros. Das Band ist ja relativ klein und passt in die Jackentasche. Bei Feierabend hab ich es mitgenommen und bei mir zu Hause gut versteckt. Ich wusste, dass nichts passiert. Ich wusste, dass die verantwortliche Person das Band nicht ins Lesegerät steckt und nachschaut, ob da Daten drauf sind. Sie legt es einfach zu den anderen Backup-Tapes.»[1] Falls diese Schilderung zutrifft, reibt sich der Leser die Augen: In jedem mittleren Modegeschäft sind die Kleidungsstücke gesichert und es geht eine Alarmanlage los, wenn man das Geschäft mit nicht entsicherter Ware verlässt. Finanzinstitute müssen sich warm anziehen, da sich ausländische Staaten nicht zu schade waren, gestohlenen Daten zu kaufen, Zeugenschutzprogramme anzubieten, die man sonst von Mafiamitgliedern kennt, die das Gebot der Omertà gebrochen und mit den Ermittlungsbehörden zusammengearbeitet haben, und sich Deutschland überlegt, gesetzlich zu verankern, dass solche Daten vom Staat rechtmässig erworben werden dürfen. ■

1 Stern 32/2010 vom 05.08.2010, S. 55–65. Der abgetauchte Datendieb Heinrich Kieber plaudert in einem Interview mit dem Titel «Der Albtraum der Millionäre». Das Originalzitat stammt von S. 59 des Interviews. Kieber erhielt vom deutschen Bundesnachrichtendienst für die gestohlenen Daten 5 Mio. Euro und lebt mit neuer Identität in einem Zeugenschutzprogramm. Liechtenstein hat ihn international zur Fahndung ausgeschriebene und Kieber behauptet im Interview, dass auf einer Webseite aus dem Fürstentum Liechtenstein 7 Mio. Euro auf seinen Kopf ausgesetzt worden seien (S. 59).

DATENSICHERHEIT AM ARBEITSPLATZ: ALLGEMEINE MASSNAHMEN

Zutrittskontrolle	Zugangskontrolle	Zugriffskontrolle
Weitergabekontrolle	Eingabekontrolle	Auftragskontrolle
Verfügbarkeitskontrolle	Trennungskontrolle	Weitere Kontrolle

FIRMENREGISTER

2 InCore – Swiss Banking Services
5 SunGard – Ambit Mobile Banking
6 EMC, IPC Information Systems, New Value, SilentSoft, SVC (Investment-Plattform der Credit Suisse) Temenos, Swissquote Bank, SAP, SYBASE, Abraxas Informatik AG, Ringler Informatik AG
7 Korn/Ferry, Heidrick & Struggles, McKinsey, Credit Suisse, Oracle, Siemens Business Services, BT, Schweizerischer Verband für Strukturierte Produkte, B-Source, SAP, Hewlett-Packard
8 Valiant Bank
9 PricewaterhouseCoopers
10 Lombard Odier Darier Hentsch LODH, Finnova, Entris Banking, IBIS
11 Swisscom IT Systems
12 KOBIL Systems GmbH
14 Fachschule für Bankwirtschaft, Zürich
15 CNO Panel
16 Burson-Marsteller, Philips
17 HSBC Holding, Swiss Re
18 Consulting World AG
26 CRESOFT AG
28 Baring Point Management Technology Consultants
30 Marcus Evans
31 Institut für Finanzdienstleistungen, Zug, AXA Winterthur, UBS AG, Comparis, Blogwerk AG, PARX
32 Berner Kantonalbank, Thurgauer Kantonalbank, Nidwaldner Kantonalbank, Obwaldner Kantonalbank, Appenzeller Kantonalbank
36 SwissSign
37 PostFinance, Helvetia Versicherungen
38 Raiffeisen, Sipera, Swisscom, Google
39 CSC
40 UBS AG, SAS
43 SOWATEC, Bank Vontobel
45 Zürcher Kantonalbank
48 Fachhochschule Nordwestschweiz
49 Swisscom IT Services
50 Avaloq, Finnova, SAP, Incore Bank AG
55 UBS
56 Quarta