INFORMATIONSSICHERHEIT

Eine Top-Management- Aufgabe

Der Missbrauch sensibler Bank-Kundendaten wie bei der LGT Bank oder bei der HSBC-Affäre führt zu grossen Reputationsschäden. Was zur Vorbeugung getan werden kann.

LUTZ M. KOLBE UND **MARCEL DREYER**

Im Laufe der letzten Jahre hat die Informationssicherheit im Finanzsektor enorm an Bedeutung gewonnen. Das liegt jedoch weniger daran, dass dieses Thema erst seit kurzem ernst genommen würde, sondern vielmehr an der Tatsache, dass die Banken durch die prominenten Kundendaten-Diebstähle bei der LTG Bank in Liechtenstein und bei der HSBC in Genf irritiert wurden. Denn sie wissen sehr genau, dass ihre Kunden darauf vertrauen, dass die Bankdaten «absolut sicher» sind.

Dabei stecken die Banken in einem klassischen Dilemma: Da es keine 100-prozentige Sicherheit gibt, müssen sie durch aktives Risikomanagement das Optimum finden aus Investitionen in Sicherheit und noch akzeptablem Schaden. Investieren sie zu wenig, sind die Schäden zu hoch, wird zu viel investiert, werden die Geschäftsprozesse eingeengt. Die Finanzinstitute scheinen hier einen Nachholbedarf zu haben. Die Problematik wird verschärft durch die zunehmende Komplexität aufgrund neuer Interaktionskanäle sowie durch steigende regulatorische Anforderungen.

Prof. Dr. Lutz M. Kolbe ist Inhaber der Professur für Informationsmanagement an der Georg-August-Universität in Göttingen.
Marcel Dreyer ist Senior Management Consultant bei der Comit AG.

IT-Sicherheit greift zu kurz

Die Digitalisierung der Wertschöpfungskette im Finanzsektor ist unter diesen Gesichtspunkten Segen und Fluch zugleich. Moderne Finanzprodukte sind ohne eine nahezu vollständige Digitalisierung, elektronische Speicherung und Übermittlung nicht denkbar. Die Kunden, vor allem die jüngere Generation, erwarten dies zunehmend. Sie erwarten aber auch, dass mit ihren Daten vertraulich umgegangen wird. Wird ein E-Mail, ein USB-Stick oder eine DVD fehlgeleitet oder gestohlen, kann dies das Sicherheitsdispositiv eines Finanzinstitutes unterlaufen und enormen finanziellen und reputationsmässigen Schaden anrichten.

Massnahmen der IT-Sicherheit wie das Sperren von USB-Ports, das Einrichten von Firewalls oder das Filtern von E-Mails lassen sich relativ einfach umsetzen. Sie zielen aber oft an den eigentlichen Ursachen vorbei, denn dabei handelt es sich z.B. um mangelndes Sicherheitsbewusstsein der Mitarbeiter oder um Insider-Schäden. IT-Security heisst oft nur die Betrachtung technischer Massnahmen. Dabei kann jedoch eine ganzheitliche Sicht auf die Problematik Informationssicherheit verloren gehen.

Ganzheitlicher Ansatz ist unabdingbar

Der Schutz von Systemen an sich ist also nicht das Ziel der Informationssicherheit. Vielmehr muss das Ziel darin liegen, die Business and Client Information Security (BCIS) sicherzustellen: Also den Schutz von sensiblen Informationen. Die IT-Sicherheit ist dabei nach wie vor ein wichtiger Baustein der Sicherheitsarchitektur. Es wird jedoch deutlich, dass neben der technischen auch andere Dimensionen betrachtet werden müssen. Daher ist ein ganzheitlicher Ansatz auf der Basis des Business Engineering sinnvoll, welcher eine methodische Betrachtung der Dimensionen Strategie, Prozesse und Systeme ermöglicht. Neben den genannten Dimensionen muss zudem noch die Dimension «Mensch» im Zusammenhang mit der Informationssicherheit ergänzend berücksichtigt werden, wie die prominenten Beispiele von LGT und HSBC verdeutlichen. In beiden Fällen wurden Kundendaten in krimineller Absicht von Mitarbeitern gestohlen.

Modelle aus anderen Branchen taugen nicht

Der Finanzsektor zeichnet sich beim Thema Datensicherheit durch spezifische Eigenschaften aus, besonders wegen der laufend zunehmenden Regulierungsdichte und dem hohen Grad der Vernetzung zwischen den Partnern in der Wertschöpfungskette. Das Übertragen eines Modells aus einem anderen Wirtschaftssektor ist nicht sinnvoll und kann den Aufwand für die Informationssicherheit beträchtlich erhöhen.

Um die komplexen Herausforderungen der Informationssicherheit im Finanzsektor zu lösen, ist ein zielgerichtetes Management unabdingbar. Eine Einstufung der gesamten Informationssicherheits-Problematik als Führungsaufgabe ist dabei für ein erfolgreiches Vorgehen unausweichlich. Neben der Anerkennung der Bedeutung dieses Problemfeldes durch die Unternehmensführung bedarf es aber auch einer zielgerichteten Methodik zur Erreichung der Sicherheitsziele.

Der Einsatz eines Referenzmodells für die Informationssicherheit im Finanzsektor, wie das Business and Client Information Security Model (BCIS) der Universität Göttingen, welches zurzeit in Kooperation mit einem Praxispartner und dem Direct Management Institute St. Gallen für Finanzdienstleister eingeführt und umgesetzt wird, ist daher notwendig. Auf Basis eines mehrstufigen, strukturierten Vorgehens ist dabei vor allem die erste Phase «Assessment», in welcher der aktuelle Stand der Informationssicherheit ermittelt wird, von Bedeutung.

Nur wenn ein Finanzdienstleister genau über seinen Sicherheitsstand informiert ist, können sinnvolle und gezielte Massnahmen zur Verbesserung des Sicherheitsniveaus umgesetzt werden. Ein ausführliches, unternehmensspezifisches Assessment bildet hierbei die Grundlage für die Identifikation und Umsetzung notwendiger Handlungsmassnahmen – unterstützt durch ein effizientes methodisches Vorgehen.

Dieses muss sich nach vorhandenen Normen, Standards und Best Practices richten. So kann auf die bereits vorhandene Wissensbasis zurückgegriffen werden, zudem ermöglichen bereits implementierte Standards eine effizientere Durchführung der Analyse. Als Grundlage eignet sich besonders die ISO-Normenfamilie 27 000. Sie enthält teilweise genau formulierte Prüfpunkte und beschäftigt sich im Kern mit der Informationssicherheit. Ergänzt durch Informationen aus Best-Practice-Sammlungen sowie aktuellen wissenschaftlichen Erkenntnissen lässt sich so ein umfassendes Bild über das Sicherheitsniveau eines Finanzdienstleisters ermitteln.

Datenklau und CD-Handel: Die moderne Bedrohungslage im Bereich Datensicherheit bei Banken verlangt nach umfassenden Lösungen.

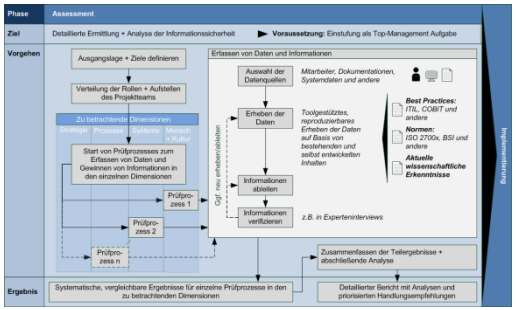
Das BCIS-Referenzmodell

Der heute häufig selektive und reaktive Ansatz der Finanzinstitute begegnet der komplexen Problematik der Informationssicherheit nur ungenügend. Der Einsatz eines durchgängigen Referenzmodells, welches die Besonderheiten eines Finanzinstitutes über alle relevanten Dimensionen hinaus berücksichtigt, muss daher folgende Eigenschaften besitzen:

- Analyse von strategischen, prozessualen und systemischen Aspekten
- Berücksichtigung der Dimension «Mensch»
- Einbindung finanzsektorspezifischer Besonderheiten (digitale Wertschöpfungskette, hoher Vernetzungsgrad, regulatorische Anforderungen)
- Verknüpfung von neuesten Erkenntnissen der Wissenschaft mit Anforderungen der Praxis

Eine erfolgreiche Analyse und Umsetzung bringt vielfachen Nutzen: Eine Identifikation von Schwachstellen, eine verbesserte Sicherheitslage im Unternehmen und an den «Schnittstellen nach aussen», sowie vor allem Transparenz der Verfügungsrechte über Daten. Damit wird das Unternehmen quasi automatisch zu dem optimalen Punkt zwischen Mitteleinsatz und Schadenserwartungen geführt.

Das Referenzmodell sollte kontinuierlich angewendet werden. So kann sich die Informationssicherheit einer Bank zum starken Verkaufsargument gegenüber Kunden, Regulatoren und Partnern entwickeln. «



Die Phase ‚Assessment' im BCIS-Referenzmodell