

Datensicherheit ist ein Dauerbrenner

Datendiebstähle haben die Finanzbranche aufgeschreckt und die Sicherheitsmassnahmen verstärkt in den Fokus gerückt. Der IT-Branche verleiht dies aber keinen zusätzlichen Schub.

Von Matthias Hassler

Vaduz. – Kein Wunder, schrillten bei manchem Finanzdienstleister im Februar die Alarmglocken. Zuerst gab die Liechtensteinische Landesbank (LLB) bekannt, dass sie mit gestohlenen Kundendaten erpresst worden war. Wenige Tage später wurde öffentlich, dass bei der LGT Treuhand Daten entwendet und deutschen Behörden zugespielt wurden. Mit dem Diebesgut aus dem Hause LGT holte Deutschlands Regierung zum grossen Schlag gegen Steuerhinterzieher und die Steueroase Liechtenstein aus und trat die Steueraffäre los.

Nervosität machte sich in der Finanzbranche breit. Von peinlich genauen Sicherheitschecks war zu hören oder davon, dass Unternehmen die Kundendaten noch stärker vor unerlaubten Zugriffen geschützt verwalten wollen.

Temporärer Beschleuniger

Die Unruhe gab und gibt der IT-Branche tatsächlich einiges zu tun, lässt aber nicht goldene Zeiten anbrechen. «Viele Unternehmen überprüfen derzeit ihr Sicherheitsniveau oder lassen es überprüfen», sagt Christine Wohlwend von der Kyberna AG in Vaduz. Zum Kundenkreis der Firma zählen unter anderem Banken, Versicherungen oder Treuhandbüros. Zusätzliche Umsätze bringe die momentane Lage nicht, aber es sei «eine weit reichende Sensibilisierung» festzustellen. Laut Wohlwend zeigt sich seit Jahren die Tendenz, dass Unternehmen zunehmend in Sicherheitsmassnahmen investieren. Ein Vorfall wie die Steueraffäre sei nur ein «temporärer Beschleuniger» und werde den generellen Aufwärtstrend bei Daten- und Kommunikationssicherheit nicht beeinflussen.

Ganz ähnlich beurteilt Roland Herrmann, Geschäftsführer der Infor-Tele-Matik AG (ITM) in Eschen die Lage. Die ITM-Software hat im Bereich Gesellschaftswesen in Liechtenstein einen Marktanteil von mehr als 50 Prozent. Zwar habe der Wirbel um die Steueraffäre zu vielen Nachfragen seitens der Kunden geführt, sagt Herrmann, diese seien inzwischen aber wieder abgeflaut. Auf den Geschäftsgang habe sich die Aufregung nicht erheblich ausgewirkt.

Datenverschlüsselung gefragt

Die Kundenanfragen beziehen sich vorwiegend auf technische und organisatorische Sicherheitsaspekte. Dreh- und Angelpunkt sind laut Herrmann vielfach die Datenverschlüsselung und Zugriffsrechte. Dies beinhaltet, welche Datenbereiche für welche Benutzer zugänglich sein dürfen, wie sensible Daten in geschützte Bereiche abgelegt werden, wer wie oft auf welche Daten zugreifen kann etc. Das geht hin bis zur Verschlüsselung von Informationen einer Stiftung, indem z. B. der wirtschaftlich Berechtigte vermerkt ist. Entsprechend solcher hohen Anforderungen unterliegen auch die IT-Unternehmen selbst strengen Regeln. «Datenschutzbestimmungen oder Geheimhaltungspflichten entsprechend dem Bankgeheimnis oder dem Sorgfaltspflichtgesetz müssen von allen Mitarbeitern eingehalten werden», so Herrmann.

Nicht nur die IT-Firmen selbst müssen ihre Mitarbeiter dementsprechend auswählen, auch die Kunden prüfen genauestens, mit welchen Personen sie zusammenarbeiten. «Betreuungspersonen und Ansprechpartner werden sorgfältig ausgewählt und einer Risikoanalyse unterzogen. Zudem müssen in unserem Unternehmen Zuständigkeiten und Verantwortlichkeiten strikt geklärt sein», sagt Christine Wohlwend.

Einschränkungen und Kontrolle

Ebenso strikt verfahren z. B. die Banken mit ihren internen Massnahmen hinsichtlich der Datensicherheit, die laufend auf den neuesten Stand gebracht werden. «Möglichkeiten der Anonymisierung von Daten bilden dabei einen wichtigen Aspekt», sagt LGT-Sprecher Hans-Martin Uehlinger. Der Zugang zu Daten ist strikt limitiert; die Mitarbeiter haben nur Zugriff auf Informationen, die sie benötigen. Diese Devise gilt auch bei anderen Banken. «Sämtliche Berechtigungen für die verschiedenen Systeme werden nach einem strikten Need-to-know-Prinzip in einem systemgeschützten, mehrstufigen Bewilligungsverfahren vergeben», sagt LLB-Kommunikationschef Cyrill Sele. Datenzugriffe werden protokolliert, kontrolliert und streng überwacht.

Auch bei der VP Bank gelten klare Regeln. «Unsere Systeme sind so ausgelegt, dass Kundendaten grundsätzlich nicht einsehbar sind. Die Vergabe von Zugriffsrechten wird sehr restriktiv gehandhabt», sagt Geschäftsleitungsmitglied Gerhard Häring. Sämtliche angefragten Banken lassen ihre Massnahmen regelmässig von externen Experten prüfen und Tests unterziehen.

Schwachstelle Mensch

Trotzdem gibt es keine absolute Sicherheit, wie die Vorfälle bei der LGT oder der LLB zeigen. «Der Mensch ist das schwächste Glied in der Sicherheitskette», sagt Uehlinger. Auf kriminelle Weise wird auch versucht, diese Schwachstelle auszunutzen. Das sogenannte «Social Engineering» ist im Internetzeitalter in Mode gekommen. Dabei gibt z. B. ein Anrufer eine falsche Identität vor, mit dem Ziel, das Vertrauen des Gesprächspartners zu gewinnen und so an vertrauliche Informationen zu gelangen.

Dementsprechend stehen neben technischen Vorkehrungen die Angestellten im Mittelpunkt. «Wir arbeiten mit externen Spezialisten zusammen, die Gespräche mit Bewerbern und Mitarbeitenden führen, die Zugang zu sensiblen Daten haben. Die Spezialisten sind auch Ansprechpartner für Mitarbeitende, sollten diese in eine schwierige persönliche Situation gelangen», erklärt Uehlinger. «Wir unternehmen alles, um den höchstmöglichen Standard an

Datenvertraulichkeitsvorkehrungen zu erreichen», sagt Sele. «Dazu gehört auch die laufende Sensibilisierung und Schulung der Mitarbeitenden für Fragen der Datenvertraulichkeit.»

Bei der VP Bank werden Mitarbeitende und Führungskräfte ebenfalls regelmässig im Umgang mit sensiblen Daten geschult. Dazu gehört auch die sichere Handhabung von mobilen Geräten wie z. B. Notebooks.

Hohes Niveau

Die Bemühungen um die Datensicherheit sind gerade für Liechtenstein von immenser Bedeutung, da der Schutz der Privatsphäre ein Eckpfeiler des Finanzplatzes ist. Die Sicherheitsvorkehrungen bewegen sich nach Einschätzung der Finanzmarktaufsicht (FMA) auf hohem Niveau. «Die Finanzintermediäre verfügen über einen sehr hohen Sicherheitsstandard», sagt Mario Gassner, interimistischer FMA-Chef. Es gelte aber, diesem Punkt oberste Priorität beizumessen. «Gerade aufgrund der aktuellen Ereignisse wurden die Standards nochmals kritisch geprüft und gegebenenfalls angepasst.»