Wenn Image und Vertrauen leiden

Während IT-Security-Anbieter immer leistungsfähigere Produkte entwickeln und Firmen ihre technischen und organisatorischen Vorkehrungen verbessern, sind auch Cyberkriminelle nicht untätig. Sie agieren professioneller und organisierter als je zuvor, machen sich den technischen Fortschritt ebenfalls zunutze und sind dabei auch häufig allen anderen einen Schritt voraus Priska B. Roelli

Innovationen und moderne Technologien bedeuten für jeden von uns in irgendeiner Form einen Mehrwert. Bankkunden profitieren dank Social Media, Mobile Apps oder Cloud Computing von neuen Services und Dienstleistungen sowie von einer riesigen Informationsvielfalt, die transparent und ortsunabhängig rund um die Uhr verfügbar ist. Banken ihrerseits können ihre Bank-Kunden-Beziehung stärken und gewinnen an Nähe zur ihrer Klientel, die über Gewinner und Verlierer am Markt entscheiden kann. Die technologische Entwicklung hat aber auch ihre Schattenseiten, die sich unter anderem in der Sicherheit bemerkbar machen: Sie bieten Cyberkriminellen eine grössere Auswahl an Angriffsflächen, für die sie immer raffiniertere Angriffsmethoden entwickeln, um die bestehenden Sicherheitssysteme auszutricksen.

BILD: FOTOLIA

Hacker können die Reputation von Unternehmen massiv gefährden.

Sicherheitsvorfälle nehmen um 170 Prozent zu

Natürlich ziehen sich Angriffe aus dem Internet durch sämtliche Branchen und Unternehmensgrössen. Finanzinstitute sind jedoch besonders häufig davon betroffen und zählen Datendiebstahl und Datenabfluss zu den derzeit grössten Herausforderungen. Allein zwischen 2012 und 2013 haben Sicherheitsvorfälle bei Banken um 170 Prozent zugenommen. Dies geht aus dem «Global State of Information Security Survey 2014» der Wirtschaftsprüfungs- und Beratungsgesellschaft PwC hervor. Ein Grund dafür ist, dass es speziell in der Finanzbranche mehr lukrative Unternehmens- und Personendaten als anderswo gibt, die es lohnt zu stehlen und die zu einem hohen Preis verkauft werden können. Der Handel floriert, und es gibt praktisch keine Information, die sich nicht auf dem Schwarzmarkt oder auf Auftrag beschaffen und verkaufen lässt. Wie schnell und plötzlich solche Angriffe aus dem Internet die Branche erschüttern und offensichtliche Lücken aufdecken, haben die jüngsten Übergriffe wie die NSA-Affäre oder die Heartbleed-Sicherheitslücke eindrücklich gezeigt. Während ein finanzieller Verlust durch eine Cyberattacke für Banken noch zu verkraften ist, sind die Auswirkungen auf das Kundenvertrauen und auf die allgemeine Marktwahrnehmung weit bedeutender für die Reputation. Dieser Punkt, so die Studie «Cyberrisk in Banking» von Longitude Research, wiegt fast doppelt so schwer wie ein monetärer Verlust. Gar 54 Prozent der Umfrageteilnehmer aus dem Handels- und Bankenumfeld gaben an, dass die finanziellen Verluste nicht hoch genug sind, um eine Alarmglocke in der Chefetage auszulösen.

Die Kombination macht's

Dass ein hundertprozentiger Schutz nie möglich sein wird, dürfte jedem klar sein. Umso wichtiger ist es, die Relevanz der Kundenbindung und eines Imageschadens zu verstehen, sich widerstandsfähig gegenüber jeder Form von Bedrohungen und Angriffen aufzustellen, um auch bei unvorhersehbaren Vorfällen handlungsfähig zu bleiben. Neben eines stabil funktionierenden IT-Betriebs, der Verfügbarkeit der Unternehmensprozesse und einer professionellen Verwaltung der IT-Dienste ist ein Sicherheitsfundament, das als IT-Grundschutz solide im Unternehmen verankert sein muss, deshalb Pflicht. Und: Cybersecurity ist kein rein technologisches, sondern vor allem auch ein menschliches Problem. Deshalb sollten auch die folgenden Fragen[1)] geklärt werden:

- Kennen wir die Risiken und Schwachstellen unserer IT-Infrastruktur?
- Welchen Schaden kann eine Sicherheitslücke für die Firmenreputation und Marktwahrnehmung bedeuten?
- Sind unsere Mitarbeiter genügend geschult und sensibilisiert in Bezug auf den Umgang mit Daten und dem Internet?
- Sind unsere Sicherheitsweisungen vollständig, aktuell und verständlich?
- Verfügen wir über ein aktives Risikomanagement und über ein Notfallkonzept?

Das Management trägt am Ende des Tages immer die Verantwortung und steht in der Pflicht, eine noch aktivere Rolle beim Schutz der Daten und Informationen einzunehmen und sicherzustellen, dass technische Massnahmen zur Verbesserung der IT-Sicherheit immer mit den organisatorischen Massnahmen kombiniert werden.

[1)] Quelle: Sidler Information Security GmbH