

IT-Sicherheit in der Wirtschaftskrise: Verunsicherte Mitarbeiter als Risikofaktor

von Philippe Welti

Als Folge der Wirtschaftskrise müssen die weltweit grössten Finanzinstitute mit steigenden Risiken bei der Informationssicherheit rechnen. Das geht aus der sechsten Ausgabe des Global Security Survey von Deloitte hervor.

Die weltweite Krise im Finanzdienstleistungssektor stellt auch für die Informationssicherheit der Unternehmen ein Risiko dar. Laut Global Security Survey 2008 dürften Fehler oder Verstösse von verunsicherten oder unzufriedenen Mitarbeitern in den kommenden Monaten einer der Hauptgründe für das Versagen von Sicherheitssystemen sein.

So bezeichneten 86% der Befragten menschliches Versagen als häufigste Ursache für Sicherheitslücken in Informationssystemen. Das Ergebnis zeigt, dass die Mitarbeiter zwar auf der einen Seite das wertvollste Gut eines Unternehmens sind, gleichzeitig aber auch ihr schwächstes Glied. Dies ist besonders im heutigen Wirtschaftsklima von Bedeutung, in dem schwindende Arbeitsplatzsicherheit und wachsender Stress bei Mitarbeitern miteinander zu unüblichem Verhalten führt.

Zwar ist die Zahl der internen und externen Sicherheitsverstösse im Finanzsektor in den vergangenen zwölf Monaten weltweit zurückgegangen, dennoch nehmen Unternehmen Fehlleistungen von Angestellten zunehmend als Problem wahr. Mehr als ein Drittel (36%) der Befragten gab an, interne Verfehlungen als das grössere Risiko zu betrachten, für lediglich 13% geben Angriffe von aussen mehr Anlass zur Sorge. Sechs von zehn Umfrageteilnehmer erklärten sich zudem als «nicht sehr» oder nur «mässig» zuversichtlich, ihre Organisation gegen interne Cyberattacken schützen zu können.

Die wachsende Beliebtheit von sozialen Netzwerken wie Facebook oder mySpace und die zunehmende Verbreitung von USB-Sticks, MP3-Playern und PDAs stellen zusätzliche Anforderungen an die interne und externe Sicherheit. Interessanter-

weise schränkt inzwischen mehr als die Hälfte der befragten Finanzunternehmen den Zugang zu sozialen Netzwerken (53%) und zum Instant Messaging (58%) ein, doch 90% erlauben ihren Angestellten den Gebrauch von mobilen Geräten, die es Hackern potenziell ermöglichen, auf Identitäten zuzugreifen und an vertrauliche Informationen heranzukommen.

Die Befragten nennen dabei am häufigsten Phishing und Pharming als grösste Gefahrenquellen, 22% der Befragten geben an, schon davon betroffen gewesen zu sein. Damit sind dies die beiden am meisten verbreiteten externen Angriffsmechanismen.

«Die Finanzinstitute kämpfen beim Schutz der Vermögenswerte und Daten ihrer Kunden an zwei Fronten: Zum einen ist die Online-Kriminalität immer besser organisiert und eine wachsende Bedrohung, zum anderen sind viele Mitarbeiter aufgrund der schwierigen Wirtschaftslage und dem drohenden Verlust ihres Arbeitsplatzes verunsichert. Auch die Zahl der entlassenen und entsprechend aufgebrauchten früheren Angestellten nimmt zu. Im gegenwärtigen Wirtschaftsklima ist es daher unerlässlich, dass Unternehmen den Schutz ihrer Daten mit höchster Wachsamkeit betreiben und Kontrollen und Massnahmen einführen, um die möglichen Folgen menschlicher Fehlleis-

Hinweise

Aussagekraft

Diese Umfrage, die auf Interviews mit Sicherheitsverantwortlichen aus den 100 weltweit grössten Finanzinstituten basiert, gilt in weiten Kreisen als globaler Massstab für den Stand der IT-Sicherheit und den Datenschutz im Finanzsektor.

Methodik

Die Umfrage wurde durch die Global Financial Services Industry Group (GFSI) von DTT mittels persönlicher Interviews und Online-Fragebögen durchgeführt. Befragt wurden Führungskräfte im Bereich Informationstechnologie (Chief Security Officer, Chief Information Officer, Sicherheitsmanagementteam usw.) bei Banken, Versicherungsgesellschaften, Wertschriften- und Vermögensverwaltungsfirmen. Die Fragen konzentrierten sich auf Gebiete wie Governance, Investitionen in die Sicherheit, Risiken, Einsatz von Sicherheitstechnologien, Prozessqualität und Datenschutz. Die Befragten repräsentieren öffentliche und private Unternehmen aus 32 Ländern und fünf Grossregionen: Europa, Naher Osten und Afrika (EMEA), Japan, Asien-Pazifik (APAC), Nordamerika (NA) sowie Lateinamerika und Karibik (LACRO). Wegen der unterschiedlichen Ausrichtung der befragten Unternehmen und des qualitativen Formats der Studie sind möglicherweise nicht alle Ergebnisse zu 100% repräsentativ für die jeweilige Region.

IT-Sicherheitsmanagement

Über Deloitte AG

Deloitte LLP und seine Tochterfirmen sind führende Beratungsunternehmen mit über 12'000 bestausgewiesenen Mitarbeitern und Mitarbeiterinnen in Grossbritannien und der Schweiz, das Leistungen in den Bereichen Wirtschaftsprüfung, Steuerberatung, Consulting und Corporate Finance Services bietet. Das Unternehmen, das dank seinen innovativen HR-Programmen als erklärter Wunscharbeitgeber gilt, setzt sich dafür ein, dass seine Kunden und Mitarbeitenden Erfolg haben.

www.deloitte.ch

tungen gering zu halten», betont Anthony Walsh, Leiter Security & Privacy Services bei Deloitte Schweiz.

«Die Finanzinstitute müssen zudem die neuen Anforderungen an den Schutz und die Geheimhaltung ihrer Kundendaten meistern. Die Abschirmung und vertrau-

liche Behandlung von Daten ist längst zu einer der wichtigsten Sicherheitsfragen geworden», so Walsh.

Ein weiterer Risikofaktor für die Informationssicherheit ist der zunehmende Kostendruck, dem die Finanzinstitute ausgesetzt sind. Zwar geben 60% der Befragten an, sie hätten ihre Ausgaben für die Datensicherheit aufgestockt, doch die Erhöhungen halten nicht Schritt mit den heutigen Anforderungen und Bedürfnissen. Mehr als die Hälfte (56%) nennen Budgetbeschränkungen und Geldmangel als wichtigste Hindernisse für die Gewährleistung der Datensicherheit. Weiter räumt eine wachsende Zahl von Befragten (15% im Vergleich zu 13% im Vorjahr) ein, dass ihre Unternehmen mit den Aufwendungen für die Informationssicherheit in Rückstand geraten.

«Die Folgen der Finanzkrise werden immer einschneidender, und die Unternehmen könnten sich darum veranlasst sehen, ihre IT-Budgets zu kürzen und die Ausgaben für Sicherheitsprojekte herunterzufahren. Dabei ist es heute so schwierig wie nie zuvor, die Sicherheitsrisiken in den Griff zu bekommen, und die Auswirkungen eines Ver-

sagens können um ein Vielfaches gravierender ausfallen», meint Anthony Walsh.

Weitere Ergebnisse der Umfrage

- Die drei Top-Prioritäten der Finanzunternehmen im Bereich der Informationssicherheit lauten: 1. Einhaltung der Sicherheitsvorschriften, 2. Datenschutz und Informationslecks, 3. Zugriffs- und Identitätsmanagement
- Im vergangenen Jahr verzeichneten die Finanzinstitute weniger Verletzungen der Datensicherheit, sowohl von aussen (47% gegenüber 65% im Jahr 2007) als auch in ihren eigenen Reihen (27% gegenüber 30% im Vorjahr)
- Die Hauptbeweggründe für ihren Bemühungen um den Schutz der Kundendaten sind für die Finanzinstitute die gesetzlichen Datenschutzbestimmungen (79%), gefolgt von Reputations- und Markenüberlegungen (70%)

Die Umfrage Global Security Survey kann unter www.deloitte.ch heruntergeladen werden. ■