

IM ZEITALTER DER PHISHING-EXPEDITIONS

Sicherheitskultur bewahrt Reputation

ADAM SCHMID

DER RICHTIGE UMGANG MIT DATEN UND INFORMATIONEN WILL GELERNT SEIN. DIES GILT BESONDERS FÜR DIE MITARBEITER VON BANKEN UND VERSICHERUNGEN. VORSCHRIFTEN UND TECHNISCHE VORKEHRUNGEN SIND ZWEIFELLOS NÖTIG. ABER SIE ALLEIN GENÜGEN NICHT. «ERST MIT DER ENTWICKLUNG EINER EIGENTLICHEN SICHERHEITSKULTUR KANN DEM DATENKLAU PRÄVENTIV BEGEGNET WERDEN», BETONT MARCO MARCESI, CEO VON ISPIN AG.



Marco Marcesi, CEO ISPIN AG:
«Fraud Management und Compliance sind die grossen Themen.»

Finanzdienstleister mögen punkto Informationssicherheitsbranchenmässig am besten aufgestellt sein. Dennoch

hört man immer wieder von Problemen mit Kundendaten, Phishing-Fällen und anderem. Könnten Finanzdienstleister die Sicherheit ihrer Daten noch verbessern?

Marco Marcesi: Sie haben Recht. Die Finanzbranche ist grundsätzlich sehr weit in Sachen IT-Security. In den Bereichen der «Information» sieht es allerdings anders aus. Die Banken sind wegen der heiklen Daten und Informationen besonders gefährdet. Gerade in schwierigen Zeiten gilt es, Risiken, und dazu zählen wir die Sicherheit und Vertraulichkeit der Information, wirksam und erfolgreich zu managen. In der unternehmensweiten Informationssicherheit gibt es noch entsprechendes Optimierungspotenzial.

Welche Sicherheitsprobleme werden die Finanzdienstleister kurz- und mittelfristig in technischer und praktischer Hinsicht am meisten beschäftigen?

Die grossen Themen sind oder wären: Compliance, DLP, IAM, Fraud Management und Awareness. Zum Teil sind diese bereits auf den Projektportfolios in unterschiedlichen Fortschritten fixiert. Aber hier braucht es noch viel Aufklärungsarbeit. Es ist für uns kaum begreiflich, weshalb die Informationen nicht

vermehrt direkt an der Quelle geschützt werden. Allseits bekannte Vorfälle in verschiedensten Banken und Ländern hätten so relativ einfach präventiv vermieden werden können. Auch sollte die Sensibilisierung im Umgang mit Informationen mehr eingeübt und geschult werden. Mit erlebbaren Awareness-Trainings erhöhen wir die Informationssicherheit massiv. Auf diese Weise wird eine eigentliche Sicherheitskultur geschaffen.

Welches sind aus Ihrer Sicht die momentan interessantesten Projekte im Finanzdienstleistungsbereich?

Interessant ist alles, was die Sicherheit für die Kundschaft erhöht. Das schafft und festigt das Vertrauen. Letztlich entscheiden unsere Kunden über ihre Prioritäten. «Nachholprojekte» im Fraud Management, DLP und IAM gehören ebenso dazu wie die teilweise Neuauslegungen der gesamten Security-Architekturen. Im Fokus dieser Projekte steht die Informations- und IT-Sicherheit in allen Geschäftsprozessen. Egal ob im Zahlungsverkehr, bei Anlagen oder bei Finanzierungen, in der Vermögensberatung oder in Retail-, Privat- und Firmenkundengeschäft; in all diesen Prozessen schleichen sich Mängel im Umgang mit Sicherheit und Risiken ein.

Die Finanz- und Wirtschaftskrise hinterlässt deutliche Spuren. Aber können es sich die Finanzdienstleister überhaupt erlauben, bei der Sicherheit zu sparen?


Wir alle wissen, dass sich in wirtschaftlich schwierigen Zeiten die Computerkriminalität erhöht. Und dass deshalb die Finanzbranche besonders im Fokus steht. Wer an der Sicherheit spart, der nagt mittel- bis langfristig an seiner Reputation, deshalb gehören die Banken oft zu den fortschrittlichen Unternehmen. Sie sind und waren für die Anliegen der Sicherheit im Grundsatz immer sehr offen. Vielerorts sind demnach die Sicherheitssysteme und -prozesse auf gutem Niveau. Allerdings verändern sich die technologischen Möglichkeiten laufend. Darauf werden sich die Investitionen in Zukunft konzentrieren. Dabei geht es um den Unterhalt und die Weiterentwicklung bestehender Lösungen.

Wie sieht es bei Finanzdienstleistern aktuell speziell mit der Befindlichkeit der Web-Applikations-Sicherheit aus? Sind hier alle genügend gerüstet? Besteht Nachholbedarf? Was ist zu tun?

Die Banken haben es da nicht leicht. Der Markt fordert klare, einfache, schnelle, benutzerfreundliche und erst noch sichere Transaktionen rund um den Globus. Dies geht nicht ohne die relevanten Sicherheitsarchitekturen. Solchen technischen Herausforderungen begegnet man mit einheitlichen Standards für

Technologie sowie mit einem zentralen Management über alle Plattformen und Anwendungen hinweg. Solche Basisinfrastruktur und -systeme sind sicher vorhanden. Nachholbedarf besteht teilweise im strikten Einhalten der Sicherheitsrichtlinien. Dazu sind mehrstufige Konzepte und Plattformen notwendig. Systeme mit zentraler Zugriffskontrolle,

Anzeige



„Am Abend und an den Wochenenden herrscht auf unserer Internet-Plattform Hochbetrieb. Aspectra stellt sicher, dass unsere Systeme auch dann lückenlos für unsere Kunden bereitstehen.“

Peter Schwarzenbach, Leiter Informatik/Technik/Zahlungsverkehr
Schweizer Reisekasse REKA

Hosting - Monitoring - Business Continuity www.aspectra.ch

verschiedenen Zugriffsprüfungen sowie mehrstufiger Technologienutzung.

Im Bereich Awareness zeigten sich in den letzten Jahren Lücken? Haben die Finanzdienstleister mittlerweile ihre Hausaufgaben gemacht? Oder besteht noch Verbesserungspotenzial?

Dies lässt sich so nicht pauschal beantworten. Das steht uns auch nicht zu. Die Etablierung der Informationssicherheit in einem Unternehmen erfordert viel-

fältige organisatorische Massnahmen. Viele Unternehmen betreiben eine physische Sicherheitsausrüstung, sie schützen sich mit allen ihnen zur Verfügung stehenden Sicherheitswerkzeugen ab, reglementieren den Mitarbeitern den Netzzugang etc. Die direkte und persönliche Ansprache an den Mitarbeiter zu den Sicherheitsthemen erfolgt leider

mit niedriger Priorität und kommt dementsprechend viel zu kurz. Der Aufbau einer Informationssicherheitskultur kann nur dann erfolgreich sein, wenn die Führungskräfte im Unternehmen den Umgang mit sensiblen Daten und der IT gewissenhaft vorleben. Diese Vorbildfunktion ist ein entscheidender Punkt im Aufbau und in der Pflege der Informationssicherheit. Aktuell sind wir daran, dieses Thema für die Bankenwelt mehr zu sensibilisieren und stossen da auch offene Türen ein. ■

DATENVERLUST – VON KRIMINELL BIS UNWISSENHEIT

Daten gehen entweder absichtlich durch Diebstahl oder durch unbewusstes fahrlässiges Handeln, verloren. Gut geschulte, über Informationssicherheit aufgeklärte, zufriedene und loyale Mitarbeiter sind die besten Garanten für die Informations- und Datensicherheit. Nötig ist auch ein umfassendes und klares Regelwerk (Policies) sowie eine reibungslose und gut strukturierte Organisation der Prozesse und Geschäftsbereiche. Eine moderne IT-Infrastruktur stützt zudem die genannten Prozesse und formulierten Regelwerke in technischer Hinsicht.

Das Akronym DLP steht für Data Loss (oder Leakage) Prevention. Dabei geht es um das Verhindern von Datenverlust bzw. von Datenlecks. Das Kernziel ist es, Daten in den für sie vorgesehenen Räumen zu behalten. Die Räume sind eher virtueller Natur und bestehen beispielsweise aus Netzwerkgebieten, Servern und Applikationen. Eine breit angelegte Strategie integriert die organisatorische, technologische und menschliche Ebene und erhöht so die unternehmensweite Informationssicherheit.