IT-Grundschutz im Bankenumfeld

IT-Grundschutz Mit Sicherheit mehr Vertrauen
von MarKo Rogge (Lektorat, Ralf Schluricke, pr+co)

Wie das BSI (Bundesamt für Sicherheit in der Informationstechnik) in seinem aktuellen Jahrbuch schreibt, steht die IT-Sicherheit bei 83 Prozent der IT-Verantwortlichen in Deutschlands Wirtschaft und Verwaltung auf Platz eins oder zwei der Prioritätenliste. Damit ist Sicherheit eines der am heißesten diskutierten Themen in Deutschlands IT-Abteilungen. Weiter schreibt das BSI, dass rund 89 Prozent der IT-Manager die Wirtschaft durch mangelnde IT-Sicherheit gefährdet sehen. Die Verbreitung von Schadprogrammen stellt die eindeutig größte Gefahr dar. Einen besonders hohen Stellenwert in der Wahrnehmung der IT-Sicherheit nimmt darüber hinaus der Faktor Mensch ein - also Irrtum und Nachlässigkeit eigener Mitarbeiter.

Betroffen sind hiervon auch Banken. Weite Teile der Wertschöpfungskette sind durch IT abgebildet und so bieten auch Banken große Angriffsflächen: intern durch Datendiebstahl, Datenverlust oder Sabotage. Einbrecher gefährden Hard- und Software. Mit den Mitarbeiter wandern oft auch sensible Kundendaten ab. Oft ist das Personal nicht ausreichend geschult und so werden einfach zu knackende Passwörter vergeben. Schlechte Systemkonfigurationen, unzureichende Systempflege stellen weitere Schwachstellen in punkto IT-Sicherheit dar. So machen es Banken Wirtschaftsspionen und Angreifern oft leicht.

Gefährdet ist jedoch vor allem die Schnittstelle Bank – Kunde. Denn im Privatkundengeschäft hat sich das Web neben der Filiale als zweiter Vertriebskanal etabliert. Laut den Marktforschern von Steria Mummert Consulting wollen rund 90 Prozent der Kreditinstitute das Internetbanking auch in 2006 weiter ausbauen. Angesichts stark ansteigender Schadenfälle durch Angriffe auf die Systeme der Privatkunden stellt sich die Frage, ob Banken insgesamt ausreichende Sicherheitsvorkehrungen treffen.

Datenkriminalität: Mafia geht phishen

Besonders das sogenannte Phishing, bei dem über gefälschte E-Mails und Websites die Zugangsdaten für Online-Banking ausgespäht werden, stellt zur Zeit eine der größten Gefahren dar. Während das US-Marktforschungsunternehmen Gartner schätzt, dass durch Phishing allein in den USA im Jahre 2005 ein Schaden von rund 2,75 Milliarden Dollar verursacht wurde, meldet die Financial Times Deutschland, dass deutsche Banken durch Phishing-Angriffe im letzten Jahr rund 70 Millionen Euro verloren haben. Seit Mitte 2005 beobachten die Polizei in Baden-Würtemberg einen sprunghaften Anstieg von Phishing-Fällen. Während in 2004 nur wenige Einzelfälle registriert worden seien, wurden bis Ende 2005 bereits 270 Fälle mit einem Gesamtschaden von rund 1,3 Millionen Euro angezeigt. Die Berliner Polizei berichtet über Fälle, in denen Einzelschäden von bis zu 29.000 Euro entstanden sind.

Bislang standen große Organisationen wie Deutsche Bank und Postbank im Fokus der Täter, die aufgrund ihrer internationalen Strukturen eindeutig der organisieren Kriminalität zugerechnet werden. Als Konsequenz führten Postbank und Deutsche Bank das iTAN-Verfahren ein. Doch Hacker der Universität Bochum brauchten dem Handelsblatt zufolge nur einen Tag, um das neue Verfahren der Postbank zu knacken. Da die betroffenen großen Institute zudem auch aktiv ihre Kunden informierten, droht nun vor allem den Kunden kleinerer Banken und Finanzdienstleister Ungemach: Sicherheitsexperten von F-Secure gehen davon aus, dass zukünftig mit gezielten Angriffen auf kleinere Ziele zu rechnen ist, um Benutzer ausfindig zu machen, die immer noch

getäuscht werden können und auf eine Phishing-E-Mail reagieren.

Zudem steht den Banken eine neue Bedrohung aus dem Lager der Cyber-Kriminellen bevor. Beim sogenannten „Pharming“ werden die technischen Abläufe beim Aufrufen einer Webseite so verändert, dass der Nutzer unbemerkt auf eine gefälschte Webseite geleitet wird. Selbst umsichtige Internetnutzer können so Opfer eines Angriffs werden.

Ein weiteres Problem der Datenkriminalität: Kreditkartendaten werden von Servern gestohlen. So teilte der Deutsche Sparkassen- und Giroverband (DSGV) Juni 2005 mit, dass es Angreifern gelungen sei rund 50.000 Kreditkarten- und Kundendaten zu kopieren. Betroffen waren Kunden mit Visa- und Mastercard. Der teilweise leichtfertige Umgang mit Kreditkartendaten zeigt sich auch in einer Meldung des DSW Shoe Warenhauses wider: Hier wurden 1,4 Millionen Kundendaten gestohlen.

Banken und Finanzdienstleister dürfen sich angesichts der Vielzahl interner und externer Bedrohungsszenarien nicht auf den aktuellen Sicherheitsstandards ausruhen. Denn es geht nicht nur um Image und Reputation sowie die Zukunft eines Vertriebskanals. Mangelnde Sicherheit kostet auch bares Geld. Zum einen bindet die Bearbeitung von Schaden- und Missbrauchfälle erhebliche Kapazitäten. Zum anderen handelt es sich um operationelle Risiken im Sinne von Basel II, also um die Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten. Derartige Risiken müssen nach Basel II mit Eigenkapital unterlegt werden, aber auch das Kreditwesengesetz (KWG), die Solvabilitätsverordnung (SolvV) und die Mindestanforderungen an das Risikomanagement (MaRisk) befassen sich mit der Behandlung dieser Risiko-Klasse.

IT-Grundschutz: die Säulen der IT-Sicherheit

Um den derzeitigen Bedrohungen fachlich entgegen zu wirken und einen hohen Grad an Sicherheit für Bank und Kunden zu verwirklichen, sollte als Mindestanforderung IT-Grundschutz aktiv umgesetzt und stetig gelebt werden. Das Bundesamt für Informationssicherheit (BSI) hat dazu einen Leitfaden für IT-Sicherheit und deren Umsetzung entwickelt. Dieser Leitfaden trägt den Namen Grundschutzhandbuch (GSHB) und hat sich als Vorlage zur Realisierung von Sicherheitsstandards in Unternehmen durchgesetzt. Basierend auf der Sicherheitsvorlage der ISO 17799/BS 7799 stellt dieser Leitfaden auch für Banken einen ausreichenden Grundschutz dar. Das Grundschutzhandbuch soll Sicherheitsverantwortlichen in Verwaltung und Wirtschaft bei der Umsetzung von IT-Sicherheitskonzepten helfen. Es enthält dazu Standardmaßnahmen, Umsetzungshinweise und Hilfsmittel für zahlreiche IT-Konfigurationen. Auf internationaler Ebene haben sich die Common Criteria sowie ISO 17799/BS 7799 zur Prüfung und Bewertung der Sicherheit von IT etabliert. Sie sind für die Bewertung der Sicherheitseigenschaften praktisch aller informationstechnischen Produkte und Systeme geeignet.

Bei der Einführung von IT-Sicherheitskonzepten gilt es zunächst Antworten auf folgende Fragen zu definieren:
- Wie sicher ist die IT einer Institution?
- Welche IT-Sicherheitsmaßnahmen müssen ergriffen werden?
- Wie müssen diese Maßnahmen umgesetzt werden?
- Wie hält beziehungsweise verbessert eine Institution das erreichte Sicherheitsniveau?
- Wie sicher ist die IT relevanter Kooperationspartner?

Für IT-Sicherheitsbeauftragte gilt es, insbesondere folgende Punkte zu beachten:

- besonnen und systematisch an das Thema IT-Grundschutz herangehen
- Sicherheitsanalysen vornehmen, Notwendigkeiten von Maßnahmen erläutern
- Sicherheitsziele definieren und Regelungen festlegen
- IT-Sicherheit auf Schutzmechanismen aufbauen
- Durchsetzung der IT-Sicherheit und permanente Kontrolle

Ist die Entscheidung für einen ersten oder weiteren Vorabcheck gefallen, so baut dieser auf den drei Grundsäulen des IT-Grundschutzes auf, nämlich Verfügbarkeit, Vertraulichkeit sowie Integrität. Der Vorabcheck beschreibt die Grundsteinlegung zur Einführung oder zur Aktualisierung des IT-Grundschutzes nach den Kriterien des BSI (BS 7799) und Common Criteria. Sowohl das Sicherheitsbedürfnis als auch die notwendigen Maßnahmen unterliegen Veränderungen, da sie laufend den aktuellen Gegebenheiten angepasst werden müssen. Hacker, Datenschlepper und Passwort-Fänger werden auch weiterhin versuchen dem IT-Grundschutz mit immer neuen Methoden zu begegnen. Wie für den Banksafe gilt auch fürs Internet: Es gibt keine 100prozentige Sicherheit. Ob PIN/TAN- oder iTAN-Verfahren und SSL-verschlüsselte Websites, kein Verfahren bietet absoluten Schutz vor Cyber-Kriminalität. Neue Angriffsmethoden wie beispielsweise das Pharming werden auch zukünftig Opfer unter Bankkunden und Banken fordern – mit drastischen Konsequenzen für Vertrauen und Image des betroffenen Instituts. Darüber hinaus werden Angreifer auch weiterhin Versuchen Mitarbeiter zu bestechen, um Angriffe auf Banken und Finanzdienstleister effektiver durchzuführen. Fachleute rechnen damit, dass insbesondere Würmer und Trojanische Pferde weiterhin auf das aktive Ausspähen von Daten programmiert werden, um so an die Zugangsdaten für Online-Konten zu gelangen.

Kein Zutritt: Hacker, Datenschlepper und Passwortfänger

Hochsicherheit und Hochverfügbarkeit lautet deshalb das Credo für Banken und Finanzdienstleister. Aus Sicht des IT-Sicherheitsspezialisten sind dies die einzigen effizienten vertrauensbildenden Maßnahmen gegenüber Kunden und der eigenen Belegschaft. Outsourcing kann deshalb gerade unter Sicherheitsaspekten eine echte Alternative darstellen. Sicherheitskritische Prozesse lassen sich an spezialisierte Dienstleister auslagern und so der IT-Grundschutz umsetzen. Darüber hinaus umgehen Banken und Finanzdienstleister so auch das sensible Thema der Vertrauensfrage gegenüber den eigenen Mitarbeitern.

Beim Aufbau von IT-Grundschutz können externe IT-Sicherheitsberater helfen, eine objektive Entscheidung herbeizuführen. Eine fortlaufende Kontrolle der IT-Grundschutzmaßnahmen durch externe Beauftragte kann dem Erfolg der Sicherheitsmaßnahmen ebenfalls dienlich sein.

Doch letztlich gilt: IT-Grundschutz und die Umsetzung in IT-Sicherheitsrichtlinien ist und bleibt gesetzlich verankert Chefsache!

Erschienen in der IT-Finance 1/2006