Special Innovation

Christoph Riesenfelder: „Das Internet ist schlicht und ergreifend ein Spiegel der Gesellschaft. Betrug findet dort genauso statt wie auch im normalen Leben. Und zwar auf eine äußerst gefinkelte Art und Weise“, erklärt der Security-Spezialist von IBM Österreich.

Internet ist Vertrauenssache

Sonja Gerstl

economy: ***Welche Entwicklungen stellt IBM in seinem Global-Business-Security-Index-Report in Sachen Internet-Kriminalität für 2007 in Aussicht? Mit welchen akuten Gefahren sehen sich Unternehmen konfrontiert?***

Christoph Riesenfelder: Zwei Themenbereiche stehen hier ganz deutlich im Vordergrund oder weisen ein erhöhtes Risikopotenzial auf. Der eine ist der Bankensektor – und hier ganz speziell die Sparte Online-Banking. Der andere Themenbereich betrifft Ebay und andere Online-Auktionshäuser. Sowohl Banken als auch Online-Auktionshäuser haben zunehmend damit zu kämpfen, dass ihre Kunden mitunter massiven Sicherheitsbedrohungen und perfiden Attacken organisierter Internet-Kriminalität ausgesetzt sind. Daraus resultieren enorme Image-Probleme.

Wer trägt die Verantwortung für diese Angriffe?

Um beim Online-Banking zu bleiben: Hier stehen wir zunehmend vor der Problematik, dass die Sicherheitsverfahren, die beim Online-Banking in Österreich eingesetzt werden, mitunter nicht mehr dem Stand der Technik entsprechen. Es gibt natürlich Banken, die diesbezüglich sehr weit sind – andere wiederum weniger. Grundsätzlich muss man jedoch sagen, dass in der Regel die zumeist ungenügend geschützten Endgeräte der Kunden, und nicht etwa der Bankenrechner, zunehmend Ziel von organisierter Internet-Kriminalität werden.

Natürlich sind auch Banken gefordert, damit derartige Attacken möglichst vermieden werden können. Aber Phishing *(der betrügerische Versuch, per E-Mail den Empfänger zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen, Anm.)* findet primär auf dem Privat-PC statt. Es gab eine Zeit, da haben Banken Schadenersatzforderungen von Kunden, die Internet-Betrügern aufgesessen sind, aus Kulanz heraus – und natürlich auch aus Angst vor Imageverlusten – Folge geleistet. Mittlerweile ist das nicht mehr der Fall.

Wie ist das nun bei Online-Auktionshäusern wie Ebay? Da sitzen ja quasi Anbieter und Kunden daheim vor dem Privat-PC.

Ebay ist ein interessanter Fall: Es operiert mit einem Geschäftsmodell, das darauf basiert, dass Kunden über diese Online-Plattform sicher und zuverlässig Auktionen tätigen können. Nun ist es aber so, dass das Vertrauen der Kunden in diese Plattform zunehmend abnimmt. Eben weil in letzter Zeit verstärkt schwere Mängel in Sachen Datensicherheit aufgetreten sind – etwa Attacken auf Kundenkonten. Kundenkonten wurden auch schon mehrfach erfolgreich geknackt. Auch die missbräuchliche Verwendung von Daten ist eine Gefahr, mit der sich Online-Auktionshäuser zunehmend konfrontiert sehen. Für Unternehmen, die ihr Business zu 100 Prozent via Internet tätigen, stellt das naturgemäß ein massives Problem dar. Diese Firmen riskieren, dass ihnen die Kundenbasis sukzessive abhanden kommt, wenn nicht massiv in die IT-Security investiert wird.

Naiv gefragt: Wie konnte es so weit kommen? Sind hier mittlerweile betrügerische Vollprofis am Werk, oder sind die Unternehmen in puncto Datensicherheit „schlampig“ geworden?

Eigentlich sind es keine Sicherheitslücken in der IT, die für diese Entwicklung verantwortlich zeichnen. Das Internet ist ein Spiegel der Gesellschaft. Betrug findet dort genauso statt wie im normalen Leben auch. Und zwar auf eine äußerst gefinkelte Art und Weise. Grundsätzlich unterliegen Transaktionen, die über das Internet stattfinden, einer eigenen Dynamik. Man sitzt allein vor dem Computer – hört nichts, spürt nichts, riecht nichts, empfindet nichts. Man sieht nur ein Bild, und diesem Bild muss man vertrauen. Darauf basieren Internet-Handel und Internet-Dienstleistungen. Ist dieses Vertrauen nicht da, dann macht man das auch nicht.

www.ibm.at

Steckbrief

Christoph Riesenfelder ist Security-Spezialist bei IBM Österreich. Foto: IBM

Internet-Business ist Vertrauenssache. Absolute Datensicherheit bei geschäftlichen Transaktionen wird dabei von den Kunden vorausgesetzt. Foto: Bilderbox.com

In vier Schritten zur sicheren Firma

Maßgeschneiderte IT-Security-Lösungen schützen Unternehmensdaten und Firmennetzwerke vor Zugriffen.

Kommunikation über das Internet birgt Gefahren, die vielfach unterschätzt werden. Vor allem bei Unternehmen, die via Internet mit ihren Kunden in Kontakt treten beziehungsweise Geschäfte abwickeln, muss eine umfassende Daten- und Netzwerksicherheit gewährleistet sein. Beim Einstieg in das Thema Internet-Sicherheit tut sich jedoch sehr schnell eine verwirrende Vielfalt von Konzepten und Lösungsstrategien auf. Wer den Überblick behalten will, muss strukturiert vorgehen. Für die Auswahl der richtigen Security-Politik bedarf es einer nüchternen Bestandsanalyse, exakter Planung und einer kompetenten Durchführung des Konzepts.

Branchen-Profis wie IBM empfehlen folgende Vorgehensweise. Phase 1: Entwickeln der Sicherheitspolitik. Entscheidend für das Gelingen ist eine klare Zuteilung der Zuständigkeiten. Im Idealfall ist es ein Sicherheitsmanagement-Team, das in weiterer Folge gemeinsam Ziele formuliert und die individuelle Sicherheitspolitik und -strategie festlegt.

Step by Step

Phase 2: Erstellen eines Sicherheitskonzepts. Sind die Ziele klar vorgegeben, geht es nunmehr darum, zu identifizieren, welche Unternehmensbereiche geschützt werden sollen. Christoph Riesenfelder, IT-Spezialist bei IBM Österreich: „Vielen Unternehmen ist im Endeffekt nicht wirklich klar, was sie eigentlich schützen wollen.“

Ein Sicherheitsmanagement-Team sorgt für die Umsetzung der unternehmensinternen IT-Security. Foto: Bilderbox.com

Nach Festlegung der relevanten Bereiche, die künftig via IT-Security vor Zugriffen geschützt werden sollen, der Wahl der hierfür geeigneten Software und einer umfassenden Kosten-Nutzen-Analyse, kann Phase 3 – Umsetzen des Sicherheitskonzepts – eingeläutet werden. Diese erschöpft sich jedoch nicht nur in der Implementierung des Programms oder der Programme. Ein ganz wesentlicher Aspekt hierbei ist auch die umfassende Schulung und Sensibilisierung der Mitarbeiter mit der neuen IT-Security. Ohne IT-Sicherheitsbewusstsein bei den Mitarbeitern, ist man sich in Fachkreisen einig, sind die Wirkungen technischer Maßnahmen unzureichend. Phase 4: Aufrechterhaltung des Sicherheitsniveaus. Daten- und Netzwerksicherheit kommt nicht ohne permanente Kontrolle und konsequente Updates der implementierten Programme aus. Schließlich verursacht Nachlässigkeit in diesen Belangen mitunter irreparable Schäden fürs Business. *sog*