Wie sicher ist das Online-Banking?

Onlinebanking gilt als sicheres und praktisches System, um Bankgeschäfte über Internet zu erledigen. Voraussetzung ist allerdings, dass die Kunden sorgfältig mit den Legitimationsmitteln umgehen.

von Regula Heinzelmann

Anfang dieses Jahres versuchten Betrüger an Daten von Kunden der Zürcher Kantonalbank (ZKB) heranzukommen. Via E-Mail sollten diese auf gefälschte Login-Seiten der ZKB-Onlinebank gelockt werden. Gleichzeitig wurden sie zur Herausgabe von Vertragsnummer, Passwort und Streichcodes aufgefordert. Wäre ein Kunde auf diesen Trick hereingefallen, hätten die Täter frei über dessen Konto verfügen können. Bei einem Kunden wurde versucht, eine Zahlung an ein dubioses Konto auszulösen. Bei einem anderen sollte ein Börsenauftrag ausgelöst werden. Beide Betrugsversuche wurden frühzeitig erkannt und die Zahlung respektive der Auftrag storniert. Ein finanzieller Schaden für die Kunden entstand bisher nicht.

Warnung vor dubiosen Mails

Die ZKB reagierte rasch und warnte die Kunden vor den betreffenden E-Mails mit falschem Absender. Dabei wurde ausdrücklich darauf hingewiesen, dass die Bank persönliche Informationen und vertrauliche Daten wie Kontonummer, Passwort oder PIN niemals per E-Mail verlangt. Dasselbe gilt übrigens auch für andere Banken.
Die ZKB zog ihrerseits Konsequenzen, verschärfte ihre Sicherheitsvorkehrungen und führte zusätzliche Kontrollen für laufende Zahlungs- und Börsenaufträge ein. Bei Schaden müsste der Sachverhalt sorgfältig abgeklärt und geprüft werden, wer dafür haftet. Trotzdem legt man bei der ZKB Wert auf die Feststellung, dass solche Missbräuche nicht aufgrund eines Sicherheitslecks in der Telebanking-Lösung entstehen, sondern durch arglistiges Erschleichen der Sicherheitsmerkmale beim Kunden.
Dieses Beispiel zeigt aber auch, dass die Sicherheit von Online-Banking nicht nur von der Bank abhängt, sondern auch vom Verhalten der Kunden. Diese sollten mit ihren Legitimationsmitteln so sorgfältig umgehen wie mit einem Hausschlüssel.

Sicherheit hat bei Banken Tradition

Banken haben traditionellerweise sehr hohe Sicherheitsstandards, heisst es bei der UBS. Dies gilt sowohl für die IT-Sicherheit als auch für das chipkarten-basierte Sicherheitssystem. Bei der UBS sind keine Fälle von Missbrauch wie unbefugter Zugriff auf ein Konto oder Umbuchungen bei den E-Banking-Kunden bekannt.
Die UBS lehnt in ihren AGB die Haftung für Systeme des Kunden und Dritter ab, ausser für Fälle von grobem Verschulden. Ausserdem lehnt sie

SICHERHEITSMASSNAHMEN FÜR KUNDEN

- Passwörter und private Schlüssel geheim halten und regelmässig ändern
- PIN-Codes sollten nicht leicht zu ermitteln sein, also Geburtsdaten, Auto- und Telefonnummern besser nicht benutzen
- Eingegebenen Daten auf Vollständigkeit und Richtigkeit überprüfen
- Ein Virenschutzprogramm ist unerlässlich, damit nicht während der Verbindung zur Bank Unbefugte eindringen können
- Benutzt man das Telebanking im Ausland, sollte man sich über die dortigen Regelungen informieren. Vor allem können Import- und Exportbeschränkungen für die Verschlüsselungsalgorithmen bestehen.

INFO-WEBSITES

Internet-Banking in der Praxis:
www.thomannfischerlaw.ch/i-banking.pdf

Information der Credit Suisse:
https://entry.credit-suisse.ch/csfs/p/rb/de/online/banking/index.jsp

UBS-Sicherheitslösung:
www.ubs.com/g/ebanking/security.html

Zürcher Kantonalbank www.zkb.ch

die Gewährleistung ab für die absolute Fehlerfreiheit der von ihr gelieferten Software. Die Haftung wird wegbedungen soweit dies gesetzlich zulässig ist.
Bei der Credit Suisse sind ebenfalls keine Versuche von Online-Bankbetrug bekannt. Credit Suisse verfügt über ein von Sicherheitsspezialisten anerkanntes Sicherheitskonzept, das konstant überwacht und geprüft wird. Beim Online-Banking gehören unter anderem dazu: die mögliche Direkteinwahl, 128-Bit-SSL-Verschlüsselung der übermittelten Daten sowie Identifikation mittels Vertragsnummer, Passwort und Streichliste oder SecurID (60 Sekunden gültige Zufallszahl). Zudem können die Benutzerinnen und Benutzer die digitalen Zertifikate überprüfen.

Probleme durch Fahrlässigkeit

In der Praxis ist die technische Lösung nicht das eigentliche Problem, meint man bei der Credit Suisse: «Missbräuche finden einzig statt, wenn Nutzer grobfahrlässig mit den Sicherheitsmerkmalen umgehen und diese etwa offen zu Hause herumliegen lassen.»
Im Zusammenhang mit Internet-Banking-Applikationen und Transaktionen sind verschiedene technische Komponenten involviert. Dazu gehören beispielsweise der PC des Kunden, die technischen Einrichtungen des Access-Providers, die für den Internet-Zugang und die Internet-Nutzung erforderliche Software etc. Diese Bereiche und technischen Einrichtungen befinden sich ausserhalb des Kontrollbereiches der Bank.
In den allgemeinen Geschäftsbedingungen weist die Credit Suisse darauf hin, dass sie keine Verantwortung für ein fahrlässiges Verhalten übernehmen kann, das ausserhalb ihres Machtbereiches liegt. Bezüglich der unter die Verantwortung der Bank fallenden Systemteile (etwa Webserver und Applikationen) schliesst die CS ihre Haftung im geschäftsüblichen Rahmen aus. Damit sei aber nicht gemeint, dass restlos alle Verantwortung auf den Kunden abgewälzt wird. Jeder Fall werde einzeln geprüft und auch individuell behandelt.

Keine Delikte im Kanton Zürich

Nicht nur Bankfachleute bezeugen, dass Onlinebanking relativ sicher sei. Bernhard Schneider von Schneider Communications AG befasst sich als Kommunikationsberater mit IT-Fragen. Er meint dazu: «Telebanking gehört im Bankenumfeld zu den sichersten Methoden. Man muss immer mindestens eine Information eingeben, zu der niemand ausser den Berechtigten Zugriff hat. Das macht es für Hacker sehr schwierig.»

HOHE SORGFALTSPFLICHT FÜR BANKEN

Haftungsausschlüsse sind nach OR erlaubt. Die Banken sind allerdings konzessionierte Betriebe. Deswegen haften sie voll für die Beachtung der banküblichen Sorgfalt. Traditionell stellt man an die Banken sehr hohe Anforderungen bezüglich der Qualität und Sicherheit.
Ausserdem gilt für die Banken natürlich das Datenschutzgesetz und die dazu gehörige Verordnung, nach der die Datensicherung dem aktuellen Stand der Technik entsprechen muss. Die Verschlüsselung der Kundendaten sollte so sorgfältig sein, dass es grundsätzlich keinem Unberechtigten möglich ist, die vertraulichen Kundendaten einzusehen. Zusätzlich muss die Bank die korrekte Legitimation der Online-Zugriffe nachweisen.
Aufklärungs- und Sorgfaltspflichten hat die Bank vor allem gegenüber Privatpersonen, von denen kein besonderes Wissen über die spezifischen Risiken im Internet-Banking zu erwarten ist. Das Bankpersonal muss die Kunden über die richtige Verhaltensweise und über Risiken des Telebanking aufklären. Das geschieht häufig in den AGB und auf der Website der Bank. Zusätzlich werden die Sorgfaltspflichten für Kunden festgelegt.
Wenn es trotzdem Probleme gibt, entscheiden die Gerichte meistens zugunsten der Kunden, wenn diese nicht eindeutig ihre Sorgfaltspflichten verletzt haben. Sinnvoll ist, dass jede Partei für die Schäden einsteht, die sie verursacht hat. Wenn ein Schaden von keiner der beiden Parteien verursacht wurde, gilt die so genannte Sphärentheorie: Jeder übernimmt die Kosten für die Schäden, die in seinem Einflussbereich aufgetreten sind.

Bei der Bezirksanwaltschaft III für den Kanton Zürich, Abteilung Wirtschaftsdelikte und Computerkriminalität, wurden bisher keine das Online-Banking betreffenden Delikte bearbeitet. Auch der Bankenombudsmann Hanspeter Häni hatte bisher noch nie mit Fällen von Missbrauch des Onlinebanking zu tun. ◆

CONVERTER FÜR 340 BILDFORMATE

Die New Yorker Softwareschmiede ReaSoft hat einen Converter herausgebracht, der insgesamt 340 Bildformate unterstützt. Nach Aussagen des Unternehmens kann mit dem ReaConverter nahezu jedes Bild in ein anderes Format umgewandelt und dabei das Bild auch noch verändert werden.

SOFTWARE GEHT E-MAILS AUF DEN GRUND

Eine neue Software ermöglicht es herauszufinden, ob E-Mails tatsächlich gelesen werden oder nicht. Ausserdem liefert DidTheyReadIt Informationen über den Ort, wo das E-Mail gelesen wurde, sowie über die Dauer des Lesevorganges. Das Neue an DidTheyReadIt ist, dass der Empfänger nicht weiss, dass seine E-Mail derart überwacht wurde.

CA SETZT AUF OPEN SOURCE

Der Business-Softwarespezialist Computer Associates will sein Open-Source-Engagement weiter ausbauen. Das US-Unternehmen wird seine relationale Datenbank Ingres der Open-Source-Gemeinde unter einer hauseigenen Lizenzform zur Verfügung stellen, berichtet die Computerwelt.

HP WEITET OPEN-SOURCE-SUPPORT AUS

Hewlett-Packard (HP) hat einen verstärkten Support für Open-Source-Software angekündigt. Der US-Konzern wird künftig Software von MySQL und JBoss zertifizieren und unterstützen. Damit nimmt HP Programme in sein Angebot auf, die in Konkurrenz zu Software von Oracle und BEA Systems stehen, die der Konzern ebenfalls anbietet.

MACROMEDIA BREEZE IN DEUTSCHER VERSION

Die US-amerikanische Softwareschmiede Macromedia hat eine deutschsprachige Version der Kommunikations- und Rapid-E-Learning-Plattform «Breeze» vorgestellt. *(ICT/Agenturen)*