

## Sicherheit im Sudhausturm

**Wer seine Bankgeschäfte online abwickelt,  
ist in Deutschland gut gegen Missbrauch geschützt**

■ Im alten Hofbrauhaus zu Coburg wird schon längst kein Bier mehr gebraut, doch der Betrieb ist emsiger denn je. Im einstigen Sudhausturm summt und brummt, schaltet und waltet Technik aus dem 21. Jahrhundert. In den Großrechnern der Firma Elaxy laufen Daten der virtuellen Finanzgemeinde zusammen. Elaxy, einer der führenden IT-

Finanzdienstleister, der für viele deutsche Banken arbeitet, stellt sicher, dass nur derjenige Zugang zu einem Konto bekommt, der dazu auch befugt ist.

Onlinebanking liegt im Trend. Dreißig Millionen Konten wurden 2003 in Deutschland bereits online geführt. Mehr als die Hälfte aller deutschen Internetnutzer wi-

ckelt derzeit Bankgeschäfte – zumindest teilweise – online ab. Der Bankenverband registriert seit Jahren zweistellige Zuwachsraten beim Onlinebanking.

„Von diesem Trend profitieren sowohl die Banken als auch die Kunden“, sagt Dr. Kerstin Altendorf, Sprecherin des Bundesverbands deutscher Banken. Die Onlinebank ist immer präsent, und wer sie nutzt, spart Zeit – und Geld: Die meisten Banken geben ihren Onlinekunden inzwischen Ge-

Von **Friederike Nagel**, Fotos **Rainer Kwiotek/Zeitungspiegel**



Spiegelsaal: IT-Operator Henry Hälbig im Rechenzentrum der Firma Elaxy

bührenachlässe. Dennoch gibt es noch immer eine große Zahl von Kunden, die es ablehnen, ihr Ersparnis per Mausklick auf die Reise durch den Cyberspace zu schicken. Sicherheitsbedenken stellen wohl die größte Zugangsbarriere für jene dar, die Onlinebanking noch nicht nutzen. Dies gab die Hälfte der Befragten im November 2003 bei einer Umfrage an. Die Furcht vor Datenmissbrauch hat vor allem mit dem schlechten Ruf des Internets zu tun, mit Meldungen über Würmer, Viren und anderes Ungeziefer, das sich durchs Netz frisst und Computer lahm legt – Heimcomputer ebenso wie Rechneranlagen von Unternehmen.

#### **Wie sicher kann im „Wilden Weiten Web“ das Onlinebanking sein?**

Viel sicherer als zum Beispiel das Bezahlen mit der Euroscheckkarte, sagen Experten. Trotz einer enormen Zunahme von Transaktionen liegt dem Bundeskriminalamt kein einziger Fall von krimineller Manipulation eines Onlinekontos vor, den der Nutzer nicht durch eigene Fahrlässigkeit erst möglich gemacht hätte. (Siehe auch die Tipps für sicheres Onlinebanking auf der nächsten Seite.) „Absolute Sicherheit wäre eine Illusion“, sagt Thorsten Gramlich, Projektleiter für Onlinebanking bei der DaimlerChrysler Bank in Stuttgart, „doch in Deutschland und bei den internationalen Großbanken hat das Internetbanking einen hohen Sicherheitsstandard.“

Das hat nicht zuletzt mit dem alten Brauereiturm in Coburg zu tun. Wer sich online Zugang zu seinem Konto verschaffen will, muss dem Elaxy-Rechner erst einmal beweisen, dass er das Recht dazu hat. Dazu werden die Daten durch ein komplexes Sicherheitssystem geschleust. Zuerst werden die Daten im Computer des Kunden verschlüsselt, bevor sie die Reise durch das ge-



fährliche Internet antreten. Die Bank verschlüsselt die Daten erneut und schickt sie in den Elaxy-Rechner, der den Zugangscode und das Kennwort entschlüsselt und mit den Daten vergleicht, die der Kunde bei der Kontoeröffnung hinterlegt hat. Stimmen sie überein, gibt Elaxy grünes Licht, der Kunde darf zum Konto.

Elaxy bietet für den Betrieb dieser Autorisierung ein Team von 25 Spezialisten auf, das im Schichtbetrieb mehr als zweihundert Serversysteme und Applikationen betreut. Jeder Mitarbeiter verfügt über definierte Zugriffsrechte in die Großrechner, per Protokoll lassen sich alle Eingriffe nachvollziehen. Im Zusammenspiel wird so eventuellem Missbrauch vorgebeugt. Die Verschlüsselung der Daten stellt außerdem sicher, dass nicht einmal die Mitarbeiter der Bank wissen, mit welchen Zugangsdaten

Schaltzentrale:  
Die Überwachung und  
das Management von  
Störungen in einer Hand

sich ihre Kunden anmelden. Auch die Hardware in Coburg kann sich sehen lassen. Die Stromversorgung gliedert sich in drei gesicherte Ebenen: eigene Trafostation plus unterbrechungsfreie Stromversorgung und Notstrom-Dieselaggregate. Beim Internetzugang garantieren mehrere Leitungsanbindungen einen verlässlichen Zugang zu den Servern. Elaxy nutzt dafür den „backbone“ des Telekomnetzes und zwei Anbindungen zu je 622 Mbit (fast tausendfach schneller als DSL). „Wir gewähren höchste Sicherheitsstandards“, versichert Andreas Bittner, Sprecher der Geschäftsführung.

#### **Mit Passwörtern und Zugangscodes sorgfältig umgehen**

Über den ohnehin hohen Standard von Online-Finanztransaktionen hinaus stellt die DaimlerChrysler Bank – Nutzerin der Elaxy-Technik – eine zusätzliche Barriere gegen Missbrauch auf. Abbuchungen vom Tagesgeldkonto der DaimlerChrysler Bank können nur auf das vorher vom Kunden festgelegte Referenzkonto transferiert werden. Um dieses Referenzkonto zu verändern, bedarf es eines schriftlich formulierten Antrags – keine Chancen für Onlinepiraten.

Es ist ein System, das eigentlich perfekt gegen Angriffe von außen gerüstet ist, wäre da nicht der Unsicherheitsfaktor Kunde, der Passwörter und Zugangscodes herumliegen lässt oder sich in Fallen locken lässt. Manche Betrüger verschicken E-Mails, in denen sie die Kunden bitten, ihre Zugangsdaten noch einmal einzugeben. „Banken verschicken keine E-Mails, in denen nach Passwörtern oder Zugangsdaten gefragt wird“, warnt Thorsten Gramlich von der DaimlerChrysler Bank, und rät: „Ignorieren!“ Denn auch ein gemauerter Brauereiturm ist bei offenem Tor kaum sicherer als ein Gartenhaus. Der umsichtige Kunde jedoch, der einige Grundregeln beachtet, ist beim Onlinebanking deutlich besser geschützt als bei anderen Arten elektronischer Datenübermittlung im Internet. <<<

#### **Tipps zum sicheren Onlinebanking:**

- Schützen Sie sensible Daten bei der Übertragung über offene Netze. Geben Sie Ihre PIN, Ihre TAN oder Ihr Auftragskennwort nur ein, wenn Sie sich auf einer geschützten Seite der Bank befinden und Sie eine verschlüsselte Verbindung haben. Zu erkennen am Schloss-Symbol, unten auf der rechten Bildschirmseite.
- Vergewissern Sie sich, mit wem Sie es zu tun haben. Für Können ist es vergleichsweise leicht, gefälschte E-Mails oder Web-Seiten zu verfassen. Eine „Zertifikatsprüfung“ einer Internetseite, ausgestellt durch eine unabhängige Instanz, kann deshalb sinnvoll sein. Zertifikat wird über den Doppelklick auf das Schloss-Symbol geprüft.
- Gehen Sie sorgfältig mit sensiblen Daten und Zugangsmedien um. Wichtige Daten (wie PINs, TANs, Kundennummern, Passwörter, Auftragskennwörter) nicht speichern, vor allem nicht auf der Festplatte.
- Wählen Sie ein sicheres Passwort. Vermeiden Sie Eigennamen, bekannte Begriffe, Wiederholungen einzelner Zeichen und Tastaturfolgen. Ein gutes Passwort umfasst sechs bis acht Stellen und setzt sich zusammen aus Groß- und Kleinbuchstaben sowie Ziffern.
- Nutzen Sie aktuelle Programmversionen. Denn nur die jeweils aktuellen Versionen der gängigen Internet-Software können gewährleisten, dass die bis dahin bekannt gewordenen Sicherheitslücken in diesem Programm geschlossen sind.
- Setzen Sie regelmäßig einen Virensch scanner und eine zusätzliche Sicherheitssoftware (Firewall) ein.
- Aktivieren Sie die Sicherheitseinstellungen Ihres Internet-Browsers. Wichtig ist vor allem, dass Sie die Zulassung von so genannten „aktiven Inhalten“ nur nach Rückfrage gestatten. Prüfen Sie, ob die Internetseite, auf der Sie sind, ein vertrauenswürdigen Unternehmen ist, und entscheiden Sie dann, ob Sie einen Zugriff zulassen möchten.
- Beenden Sie Ihr Internetbanking auf dem dafür vorgesehenen Weg. Wenn Sie zum Ausstieg nur den Browser schließen, wird das Banking auf dem Server erst nach einigen Minuten beendet. Zeit genug für einen Missbrauch durch Dritte.



Verschlussache: Die Sicherungsbänder werden in einem Tresor aufbewahrt