Online-Sicherheit: **Hardware**-Lösungen sind **unattraktiv**

Von Ralf Bloß

Welche Rolle die Netbank im Sparkassenverbund auch künftig spielen wird: als „Testlabor" für das Online-Banking taugt die reine Internetbank schon heute. So auch beim Thema Sicherheit. Hier hat die Netbank eine elegante Lösung zum Schutz vor Trojanern entwickelt: Um sicherzustellen, dass er sich auf der echten Website der Bank befindet, wird dem Kunden sein Geburtsdatum angezeigt. Dieses muss beim Onlinebanking nicht eingegeben werden, kann also nicht abgefangen worden sein. Hardware-basierte Sicherheitslösungen, die ein Zusatzgerät benötigen, stuft man dagegen als unattraktiv ein. Red.

Sicherheit ist ein menschliches Grundbedürfnis. Das gilt im wahren Leben wie für die Parallelwelt Internet, die heute über 60 Prozent der Menschen in Deutschland nutzt. Getrübt wird die Internetnutzung durch immer neue Betrügermaschen. Wer einmal einen Schaden davongetragen hat, misstraut dem Medium Internet möglicherweise ganz. Deshalb ist es für eine Online-Bank besonders wichtig, dass sie und ihre Kunden sich mit dem Thema Sicherheit beschäftigen.

Von jeher gehört das Thema Sicherheit zum Bankwesen, denn es geht ums Geld. Neue Ideen der Betrügerseite erfordern neue Schutzmechanismen auf Seiten der Bank. Besser noch, wenn die Bank nicht nur auf einen Schaden reagiert, sondern einen Schritt voraus ist. Das verlangt nach Innovationskraft und einer hohen Fachkompetenz.

Ob der Einsatz von Panzerglas an der Kasse, die Entwicklung neuer Safeschlösser oder Vorkehrungen am Geldautomaten – die konstante Weiterentwicklung von Sicherheitsmaßnahmen setzt sich auch bei der jüngsten Form des Bankings via Internet fort. Dabei sind die Gefahren im Internet nicht größer als in der realen Welt, sondern sie sehen schlichtweg anders aus.

Betrüger entlocken den Nutzern vertrauliche Daten

Phishing, Pharming, Trojaner und Finanzagententum heißen die derzeit gängigsten Gefahrenquellen im Internet. Massenhaft verbreitete Phishing-Mails sollen Nutzern vertrauliche Daten entlocken. Das gleiche wird mit gefälschten Websites (Pharming) versucht. Spionageprogramme (Trojaner) setzen sich unbemerkt auf ungeschützten Rechnern fest und erschleichen sich Tastatureingaben wie zum Beispiel Passwörter. Es vergeht kein Tag, an dem nicht jemand von außen „an die Tür klopft", um Zutritt zu persönlichen Daten auf dem Rechner zu erhalten. Seit einiger Zeit suchen Betrüger per E-Mail-Stellenanzeige nach „Finanzagenten", die gegen eine Provision gestohlenes Geld waschen.

Zum Autor

Ralf Bloß ist Vorstandsmitglied der netbank AG, Hamburg.

Kunden erhalten Informationen zu den Grundregeln für sicheres Onlinebanking

Die Netbank ist durch ihre Spezialisierung auf das Onlinebanking-Geschäft auf solche Risiken eingestellt und hat für ihre Kunden ein mehrstufiges Modell entwickelt.

- Zur Basis gehören ausführliche Informationen in der Rubrik „Sicherheit" auf www.Netbank.de. Hier kann sich der Nutzer über die Grundregeln für sicheres Onlinebanking, über technische Sicherheitsmaßnahmen und aktuelle Gefahren erkundigen. Und der Kunde erfährt, was er selbst zu seinem Schutz tun muss: Die Einrichtung einer Firewall sowie regelmäßige Updates eines Virenscanners gehören auf jeden internetfähigen Rechner.

- Auf der nächsten Stufe unterstützt die Bank ihre Kunden mit vergünstigter Sicherheits-Software.

- Die dritte Stufe steht für sofortige und kompetente Hilfe im Case of Emergency. Wer glaubt, gerade bestohlen worden zu

sein, muss schnell den Kontakt zu seiner Bank herstellen können. Hier helfen eine klare Strukturierung und eine intuitive Navigation der Bank-Homepage.

Auch wenn Sicherheit beim Onlinebanking ein komplexes Thema ist – der Kunde sollte sich nicht um zu viele Details kümmern müssen. Bei vielen Vorkehrungen spielt daher neben der Sicherheit auch der Service eine Rolle. Die mobile TAN beispielsweise steht für sicheres und flexibles Banking zugleich. Der SMS-Kontoservice ermöglicht eine regelmäßige Kontrolle über Ein- und Ausgänge auf dem Konto. Für diese Features ist keine spezielle Hardware nötig, sondern nur ein mobiles Telefon, das heute fast jeder dabei hat. Über 80 Prozent der Privathaushalte in Deutschland besitzt mindestens ein Mobiltelefon. Darüber hinaus erleichtern Sicherheitszertifikate und E-Mail-Signaturen der Bank das schnelle Erkennen der Echtheit.

Geburtsdatum als Trojanerschutz

Neben zahlreichen weiteren Sicherheitsmaßnahmen im Online-Portal der Netbank ist gerade ein neues Feature hinzugekommen: die Anzeige des Geburtsdatums. Sie wird als Maßnahme gegen Trojanerangriffe eingesetzt. Trojaner können den Internetnutzer auf gefälschte Seiten lenken, auch wenn er die richtige Adresse eingegeben hat. Die Anzeige des Geburtstags bestätigt dem Nutzer, dass er sich auf der Seite seiner Bank und nicht auf einer gefälschten Seite befindet.

Das funktioniert so: Im Anschluss an eine Transaktion im Online-Banking-Portal erhält der Kunde eine Transaktionsbestätigung, in der sein Geburtstag angezeigt wird. Dieses Datum kann eine gefälschte Seite nicht anzeigen, da diese lediglich eingegebene Daten reproduziert. Und da der Kunde nie das Geburtsdatum bei einer Online-Banking-Transaktion eingeben muss, können diese Daten auch nicht abgefangen werden. Auf einer Betrügerseite würde das Datum falsch oder gar nicht angezeigt. So wichtig neue Sicherheitslösungen sind, so gibt es Möglichkeiten, die den Komfort des Onlinebankings einschränken. Beispielsweise wenn es um das ständige Bereithalten eines Extrageräte geht. Daher sind zum jetzigen Zeitpunkt Hardware-basierte Lösungen wie HBCI oder TAN-Generatoren als Schlüsselanhänger für die Netbank unattraktiv.

No-Risk-Garantie für den Kunden

Neben der Kundeninformation, vergünstigter Software sowie modernen, serviceorientierten Sicherheitsfeatures geht die Bank sogar noch einen Schritt weiter – mit der No-Risk-Garantie. Diese garantiert, dass der Kunde, grobe Fahrlässigkeit ausgenommen, keinen Schaden durch unberechtigte Kontoverfügung erfährt. Bei unverschuldetem Missbrauch haftet die Bank.

Dabei liegt die Beweislast nicht wie bei vielen anderen Instituten beim Kunden, sondern bei der Bank. Dies bedeutet aber nicht, dass der Kunde aus seinen Mitwirkungspflichten entlassen wird. Grob fahrlässig wäre zum Beispiel, wenn der Kunde die „Computer-Tür" sperrangelweit offen stehen lässt. Bank und Kunde müssen beim Thema Sicherheit deshalb partnerschaftlich zusammenarbeiten. Zum Part des Kunden gehören die regelmäßigen Sicherheits-Updates sowie ein sorgfältiger Umgang mit PIN und TAN.

Professionelle Hacker als Tester

Neben den Sicherheitsaspekten, die für den Kunden sichtbar und erlebbar sind, laufen hinter den Kulissen einer Bank Prozesse ab, die im weiteren Sinne für ein reibungsloses Onlinebanking sorgen. Beispielsweise greift die Bank im Notfall auf ein eigenes Cert (Computer Emergency Response Team) zurück, das in der Lage ist, von Trojanern ausgespähte Kundendaten im Internet festzustellen, bevor es zum Missbrauch kommt. In solchen Fällen informiert sie ihre Kunden umgehend, was nicht selten zu verwunderten Reaktionen führt.
Des Weiteren testet die Netbank neue IT-Prozesse bei der Einführung von Produkten und Dienstleistungen auf Herz und Nieren. Dafür lässt sie sie von professionellen „Einbrechern" angreifen, die nach Sicherheitslücken suchen, um Schaden anzurichten. Zu den Sicherheitsvorkehrungen gehört auch das Durchlaufen von Angriffsszenarien in der Theorie und in Praxistests.

Vollbank muss stets operabel bleiben

Die praktischen Maßnahmen werden weder Mitarbeitern noch Dienstleistern im Vorhinein angekündigt. In diesem Fall setzt sich eine komplexe Sicherheitsmaschinerie in Gang, Mitarbeiter und das Rechenzentrum werden alarmiert. Zu dem Anspruch an eine Vollbank gehört, dass sie stets operabel bleibt. Egal, was im Hintergrund passiert: Der Kunde muss zu jeder Zeit die Internetseite des Instituts aufrufen und seine Bankgeschäfte erledigen können.

Die parallele Entwicklung von Betrügermaschen einerseits und neuen Schutzmaßnahmen andererseits wird sich weiter fortsetzen. Für die Sicherheit ihrer Kunden, zu ihrem eigenen Schutz und um glaubwürdig zu bleiben, müssen Kreditinstitute diese Herausforderung annehmen und in Sicherheitsstandards investieren. Es ist nicht im Sinne des Kunden, wenn Banken aus Kostengründen auf Sicherheitsvorkehrungen verzichten. Und auch für die Bank zahlt es sich auf längere Sicht nicht aus, wenn sich Schäden durch Missbrauch häufen.

Mit der zunehmenden Aufgeklärtheit und dem wachsenden Bewusstsein der Internetnutzer wird das Thema Sicherheit ein entscheidendes Kriterium im Bankenmarkt. Das gilt sowohl für Internetbanken als auch für Institute, für die der Online-Vertriebsweg einer unter mehreren ist. ■