Probleme mit Electronic banking

Thema: **Zahlungsverkehr** Fallnummer: **2004/05**

> Der Kunde wird per E-Mail über Probleme mit dem Electronic banking «seiner» Bank informiert. Zur Behebung der Probleme wird er aufgefordert, seine persönlichen und für das Electronic banking notwendigen Identifikationsmerkmale (wie Vertragsnummer, persönlicher Code und Streichlistennummer) bekannt zu geben. Der Kunde kommt dieser Aufforderung nach und stellt später fest, dass jemand via Electronic banking über sein Bankguthaben verfügt hat.

Beim Electronic banking handelt es sich um eine sehr sichere Art der Abwicklung von Bankgeschäften. Damit der Kunde mit der Bank kommunizieren kann, muss er sich vorerst legitimieren. Dem Bankenombudsman sind keine Fälle bekannt, in welchen es gelungen wäre, ohne Kenntnis der Identifikationsmerkmale (Vertragsnummer, persönlicher Code und Streichlistennummer oder ähnliches Verfahren) ins System einzudringen. Wird ein Fehler moniert, liegt meistens Nachlässigkeit oder eine Mitwirkung des Kunden vor. So kann der Täter auf konventionellem Weg in den Besitz der relevanten Daten gelangen, indem er diese beispielsweise stiehlt oder kopiert. Auch Computeridentifikationsmittel sind deshalb sicher und voneinander getrennt aufzubewahren. Insbesondere darf der Code nie bei der Streichliste vermerkt sein.

Die «Mitwirkung» des Kunden kann aber auch darin liegen, dass es dem Betrüger gelingt, den Kunden zur Bekanntgabe seiner persönlichen Identifikationsmerkmale zu bewegen. Dies kann – wie im eingangs erwähnten Beispiel – dadurch geschehen, dass der Kunde diese freiwillig bekannt gibt, weil er der Meinung ist, mit seiner Bank zu kommunizieren. Es ist aber auch möglich, dass es der Täterschaft gelingt, auf den Computer des Kunden zuzugreifen und diesen so zu manipulieren, dass der Kunde meint, mit der Bank verbunden zu sein, in Tat und Wahrheit aber auf eine täuschend ähnlich gestaltete Seite des Betrügers gelangt.

Diese Gefahren können jedoch mit relativ einfachen Mitteln umschifft werden. So gilt als oberster Grundsatz, dass sich eine Bank nie nach den persönlichen Identifikationsmerkmalen eines Kunden erkundigen wird. Bei jeder derartigen Anfrage – und sei sie auch noch so raffiniert gestaltet – handelt es sich um eine Fälschung. Der Kunde sollte daher auf keinen Fall auf solche Anfragen reagieren. Weiter sollte ein Kunde seinen Computer mit einer aktuellen Firewall und einem neuen Virenschutzprogramm sichern und die generellen Empfehlungen (wie Vorsicht beim Öffnen von E-Mails unbekannter Herkunft; keine Installation von Software von nicht vertrauenswürdigen Anbietern etc.) beachten. Wichtig ist auch, dass sich der Kunde direkt auf der offiziellen Internetseite des Bankinstituts einloggt und die Internetsitzung mit der Bank mit der dafür vorgesehenen Programmfunktion «Logout» beendet und nicht einfach das Browserfenster schliesst. Anschliessend soll er den Cache des Browsers leeren, so dass bei einem Hackerangriff nicht nachvollzogen werden kann, welche Seiten der Benutzer kürzlich benützt hat. Ferner hilft die Überprüfung, ob die Aufträge richtig erfasst wurden (via «pendente Zahlungen/Aufträge »), in zweierlei Hinsicht: Einerseits erhält der Kunde die Gewissheit, dass alles seine Richtigkeit hat, denn die notwendigen Daten kann ja nur die Bank liefern. Andererseits dient dies der Bestätigung, dass der Auftrag auch tatsächlich registriert wurde und somit – sofern die üblichen Erfordernisse erfüllt sind – auch am Bestimmungstag ausgeführt werden wird.

Weitere Informationen sowie Tipps, Checklisten und Anleitungen zum Thema Computer- und Internetsicherheit finden sich auf der Internetseite der Melde- und Analysestelle Informationssicherung des Bundes (www.melani.admin.ch).