Sicheres Online-Banking

Von Heike Peters und André Grieger

Der „erste periodische Sicherheitsbericht“ des Innen- und Justizministeriums vom Juli 2001 hat es deutlich gemacht: „Indem sich gesellschaftliche Aktivitäten wie Kommunikation, Information und Handel zunehmend in das Internet verlagern, erweitern sich auch die Möglichkeiten, unter Nutzung des Internet Straftaten zu begehen. Die im Rahmen des polizeilichen Meldedienstes „Kriminalität in Verbindung mit Informations- und Kommunikationstechnik“ registrierte Internetkriminalität weist eine steigende Tendenz auf. Brauchbare Statistiken über das gesamte Ausmaß von Angriffen auf die Sicherheit, Zuverlässigkeit und Integrität von Daten über das Internet gibt es aber bislang nicht.“

Der wachsenden Bedeutung dieser Bedrohung sind sich auch die Sparda-Banken bewusst. Sie investieren viel Zeit und Geld, um ihre Systeme so sicher wie möglich zu machen. Und sie setzen auf Aufklärung. Denn die Angriffe finden fast ausschließlich auf die Computer der Banking-Nutzer statt und nicht auf die Rechner der Banken selbst.

Keine Chance für Phishing

Online-Banking bietet ohne Frage ein hohes Maß an Flexibilität, Bequemlichkeit und Geschwindigkeit. Generell finden die Vorzüge der virtuellen Bewegung im WorldWideWeb immer mehr Anhänger. Beim Shoppen und Surfen im Internet ist jedoch Umsicht geboten, um die Vorzüge des WWW unbeschwert genießen zu können. E-Mails mit falschen Absenderangaben und gefälschte Webseiten, mit denen Betrüger Zugangsdaten für das Online-Banking ausspionieren wollen - so genanntes Phishing (kurz für *Password fishing*) – wirken aber bei aufmerksamen, informierten Kunden nicht. Die Sparda-Banken klären daher über Sicherheitsmaßnahmen beim Online-Banking auf, damit Datendiebe und Betrüger keine Chance bekommen. In einer eigens zu diesem Thema erstellten Kundenbroschüre (**sparda aktuell** zum Thema Sicherheit) sowie online zugänglichen Hilfeseiten gehen die Sparda-Banken das heikle Thema offensiv an:

Regel Nummer 1: Kein leichtfertiger Umgang mit E-Mails
Vorsicht ist bei eingehenden E-Mails geboten, deren Absender angeblich die Hausbank ist, die dazu auffordert, die PIN oder TAN einzugeben. Dabei handelt es sich um klassische Phishing-Versuche von Betrügern. Denn die Sparda-Banken fragen niemals in E-Mails nach persönlichen Informationen oder vertraulichen Daten oder fordern Kunden auf diese Weise zum Online-Banking auf. Am besten ist es, derartige E-Mails sofort zu löschen. Darin enthaltene Adressen oder Knöpfe sollten niemals angeklickt, Anhänge niemals geöffnet werden.

Anti-Viren-Software auf dem PC regelmäßig aktualisieren
Zum umsichtigen Umgang mit dem Internet gehört auch die Kontrolle des eigenen PCs. Die Sparda-Banken empfehlen ihren Kunden, die Sicherheitseinstellungen von Browser und E-Mail-Programm immer so hoch wie möglich zu stellen und eine Anti-Viren-Software auf dem PC einzusetzen, die regelmäßig aktualisiert wird. Im Idealfall sollte die Software täglich auf Updates überprüft werden. Die meisten Programme besitzen hierfür eine automatische Prüffunktion und benachrichtigen den Nutzer, sobald eine neue Version des Programms oder neue Virusdefinitionen verfügbar sind.

Zusätzlich sollte ein Firewall-Programm eingerichtet sein, das den Rechner vor Angriffen schützt und verhindert, dass Spionageprogramme Kontakt über das Internet aufnehmen können.

Für weitere Informationen zu diesen Sicherheitsprogrammen verweisen die Sparda-Banken ihre Kunden auch auf die Seiten des BSI (Bundesamt für Sicherheit in der Informationstechnologie):**www.bsi-fuer-buerger.de.** Dort finden sich im Download-Bereich auch Quellen für kostenlose Sicherheits-Programme.

Modernste Sicherheitstechnik beim Online-Banking

Zum Schutz der persönlichen Daten auf dem Bankrechner und der damit verbundenen Kommunikation zwischen dem Kunden- und dem Bankrechner setzen die Sparda-Banken modernste Sicherheitstechniken ein. Diese lassen sich in drei Bereiche aufteilen:

1) Absicherung der Datenübertragung

è Datenverschlüsselung mit 128 Bit SSL-Zertifikat
Die Sparda-Banken setzen für ihre Internetbanking-Anwendung ein Sicherheitszertifikat mit hoher Verschlüsselungsstärke ein (128 Bit). Expertenmeinungen besagen, dass der Einsatz eines Schlüssels mit einer Länge von 128 Bit ausreichen sollte, dass in den nächsten Jahren derart verschlüsselte Datenströme nicht von Dritten ausgelesen oder verändert werden können.

Für die Übertragung der Daten wird vorab zwischen den beteiligten Rechnern (Kunden-PC und Bankrechner) ein geheimer

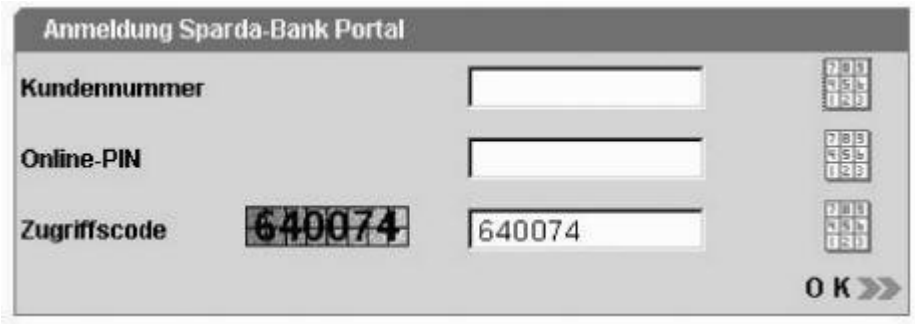
Schlüssel ausgetauscht.

Der Bankrechner kann bei dieser Art der Verbindung anhand eines Zertifikates eindeutig identifiziert werden. Für die Sparda-Banken wird das Zertifikat von der Firma **„VeriSign“** ausgestellt.

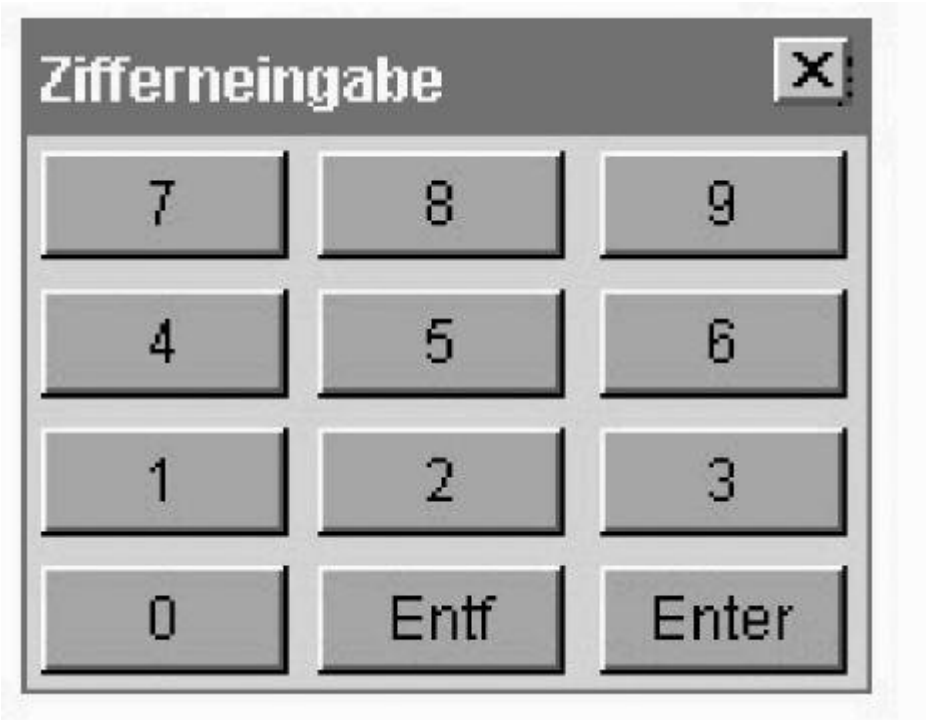
2) Absicherung der Anmeldung

• Eingabe eines Zugriffscodes auf der Login-Seite
Die Login-Seite enthält einen 6-stelligen Zugriffscode. Die darin enthaltenen Ziffern, die pro Login-Vorgang wechseln, sind so aufgebaut, dass sie auf Grund der unscharfen Darstellung, des Farbverlaufs im Hintergrund sowie der horizontalen und vertikalen Linien innerhalb des Bildes nur schwer computergestützt erkannt werden können.

Diese Ziffernfolge kann von schädlichen Programmen, welche z.B. eine automatisierte Anmeldung ausführen sollen, nicht ausgelesen werden. Erst wenn der Kunde diese Ziffernfolge zusätzlich zu seinen Zugangsdaten eingegeben hat, ist der Anmeldevorgang erfolgreich abgeschlossen worden.



• Zugangsdaten können mit einem Tastaturblock eingegeben werden Oftmals kommen im Bereich des Internetbetrugs sog. Trojanische Pferde zum Einsatz, die mit einem „Keylogger“ ausgestattet sind. Diese Programme schneiden die (unverschlüsselten) Tastatureingaben des Nutzers mit und verwerten diese unrechtmäßig weiter. Um Schadenssoftware dieser einfachen Art keine Angriffsfläche zu bieten, ist bei den Sparda-Banken die Eingabe der Kundennummer, der PIN sowie des Zugriffscodes auch mittels eines Tastaturblocks möglich. So können die Zifferneingaben mittels Mausklick eingegeben werden.



Neben jedem Eingabefeld in der Anmeldemaske (Kundennummer, Online-PIN sowie Zugriffscode) befindet sich eine Schaltfläche, mit welcher man den Tastaturblock aufrufen kann. Als weitere Sicherheitsmaßnahme wird dieser an einer zufällig ausgewählten Stelle des Bildschirms angezeigt. Die Eingaben, welche mit der Maus am Tastaturblock vorgenommen werden, gelangen direkt in das Eingabefeld.

• Anzeige zusätzlicher Sicherheitsinformationen nach der Anmeldung Nach seiner Anmeldung erhält der Sparda-Bank-Kunde weitere sicherheitsrelevante Informationen: Durch die Anzeige der bisherigen PIN- und TAN-Fehlversuche kann er mögliche unrechtmäßige Zugriffe auf sein Konto leicht entdecken und ggfs. reagieren, falls er eine illegale Anmeldung vermutet.

3) Absicherung der Transaktionen im Online-Banking

iTAN-Verfahren
Beim herkömmlichen TAN-Verfahren wählt der Kunde zur Freigabe eines Auftrages aus seiner TAN-Liste eine beliebige TAN aus. Beim Verfahren der „indizierten TAN“ (iTAN) fordert der Bankrechner vom Kunden eine ganz bestimmte TAN (diese sind mit laufenden Nummern versehen). Für eine bestimmte Transaktion ist dann auch nur diese eine TAN gültig, sie kann nicht für eine andere Transaktion verwendet werden. Wird also eine TAN „gestohlen“, so ist sie für die spätere missbräuchliche Verwendung nicht nutzbar.

Darauf weisen die Sparda-Banken ihre Kunden immer wieder hin:

Folgende Grundregeln beim Online-Banking sollten Internet-Nutzer beachten:

Vor dem Aufrufen des Online-Banking
• Benutzen Sie keine fremden Rechner, denn sie können Sicherheitslücken aufweisen.
• Schließen Sie alle Browserfenster, bevor Sie das Online-Banking starten.
• Geben Sie die Adresse Ihrer Bank möglichst von Hand in Ihren Browser ein.

Im Online-Banking
• Überprüfen Sie vor und nach der Nutzung Ihre Kontoumsätze: Sie sollten sofort alle neuen Transaktionen sehen können.

Bei der Dateneingabe und -übertragung
• Vergewissern Sie sich, ob die geforderten Eingaben für die von Ihnen gewünschte Aktion sinnvoll sind.
• Melden Sie Abbrüche und andere Unregelmäßigkeiten während des Online-Banking unverzüglich Ihrer Sparda-Bank.

Im Verdachtsfall
• Verlassen Sie das Online-Banking sofort und befolgen Sie keinesfalls die angegebenen Anweisungen. Informieren Sie unverzüglich Ihre Bank und lassen Sie gegebenenfalls Ihren Online-Banking-Zugang sperren.
• So sperren Sie Ihr Online-Banking notfalls selbst: Im Menüpunkt „Service“ haben Sie die Möglichkeit, Ihr Konto sofort online zu sperren. Eine Entsperrung ist nur durch Ihre Sparda-Bank möglich.

Schnelles Handeln im Falle des Falles
Sofern der Kunde konkrete Hinweise darauf hat, dass dennoch ein Angriffsversuch auf seinen Computer stattgefunden hat, ist es wichtig, umgehend zu reagieren. Dann haben die Sparda-Banken umfassende Möglichkeiten, die möglichen Folgen zu unterbinden.

Wichtig sind hierbei detaillierte Angaben durch den Kunden, um entsprechend auf einen Missbrauch reagieren zu können:

• Wann hat der Angriff stattgefunden?
• Welche Daten wurden für den Missbrauch verwendet? (Zugangsdaten, TAN-Nummern)
• Was wurde bereits vom Kunden veranlasst? (z.B. Kontosperrung)
• Sind vor dem Angriff auf dem Kunden-Rechner irgendwelche Unregelmäßigkeiten aufgefallen? (z.B. Zusendung verdächtiger eMails, Abstürze etc.)
• Wurden vom Kunden Daten auf einer gefälschten Web-Seite eingegeben? In diesem Fall benötigen wir die Adresse dieser Seite.

Im Falle einer unrechtmäßig ausgeführten Transaktion kann die Zahlung bei rechtzeitiger Veranlassung durch den Kunden storniert werden. Anhand der vom Kunden gemachten Angaben wird außerdem versucht, den Angreifer selbst ausfindig zu machen.

Phishing-Angriffe gegen die eigenen Kunden werden von den Sparda-Banken gezielt verfolgt und mit entsprechenden Gegenmaßnahmen bekämpft. Hierzu gehört insbesondere, die gefälschten Web-Seiten, welche für den Missbrauch verwendet werden, im Netz ausfindig zu machen und diese abschalten zu lassen.

Darüber hinaus wird den Kunden auch angeboten, den befallenen Rechner von Spezialisten untersuchen zu lassen.

Grundsätzlich wird das Online-Banking natürlich ständig weiter entwickelt, um den Kunden diesen Service mit der bestmöglichen Sicherheit anbieten zu können. Da sich Betrüger immer neue Wege ausdenken, um im Internet ihren kriminellen Handlungen nachzugehen, ist es erforderlich, diesen mit modernsten technischen Mitteln entgegenzutreten.