27. Juni 2017

Mit Sicherheit sicheres Online-Banking

Die Nutzung moderner IT ist mittlerweile ein so fester Bestandteil unseres Lebens geworden, dass der Umgang mit PC, Tablet und Smartphone eine vertraute Selbstverständlichkeit ist. Die Altersgrenzen der Nutzer haben sich in diesem Kontext auch beträchtlich nach unten und nach oben hin erweitert. Und so ist es nicht erstaunlich, dass nahezu 50% aller Deutschen Computertechnik auch für ihre Bankgeschäfte nutzen. Doch längst nicht jeder kennt die Gefahren und Risiken, die trotz gut funktionierender Technik nach wie vor vorhanden sind. Wir zeigen Ihnen deshalb in dem folgenden Überblick auf, wie Sie Ihre Geldgeschäfte sicher abwickeln können.

Spielregeln

Für das Online-Banking gelten deshalb ganz prinzipiell dieselben Regeln, wie für alle anderen sensiblen Datenbereiche auch:

- So sollten Sie beispielsweise Ihre persönlichen Zugangsdaten wie Passwörter oder Geheimzahlen nie auf dem Computer speichern.
- Betrüger werden immer dreister und raffinierter. Die Versendung täuschend echt nachgeahmter Mails mit dem Erscheinungsbild von Banken und anderer Finanzdienstleister nimmt in einem bislang nicht gekannten Ausmaß zu.
- Das gilt übrigens auch für Links zu Internetadressen, die auf dem ersten Blick absolut vertrauenswürdig ausschauen, es aber nicht sind.
- Eine weitere Masche sind auch Telefonanrufe, mit dem Hinweis auf angebliche Gefährdungslagen oder Sicherheitsprobleme, mit der Aufforderung Daten und Passwörter anzugeben, um die Gefährdungslage zu beseitigen.

Dabei ist es eigentlich ganz simpel, wie Sie sich vor derlei Betrug schützen können:

- Banken und Finanzdienstleister fordern Sie niemals per Mail auf, Ihre Daten, Tan (Transaktionsnummer) oder Passwörter einzugeben oder zu überprüfen.
- Es ruft Sie auch keiner über das Telefon an, um Sie auf eine Gefährdungslage hinzuweisen, mit dem Versprechen, Ihnen zu helfen.
- Klicken Sie keine Links in E-Mails an, deren Absender Sie nicht kennen und öffnen Sie in solchen Mails grundsätzlich keine Anhänge.
- Geben Sie die Internetadresse Ihrer Bank immer händisch ein oder speichern Sie diese in der Favoritenleiste Ihres Browsers (natürlich ohne Passwörter oder Geheimzahlen). Achten Sie darauf, dass solche Adressen immer mit http**s**:// beginnen.
- Sie müssen auch kein „Technik-Freak“ sein, um Gefahren zu erkennen. Oftmals meldet sich unser „Bauch“, also der sogenannte gesunde Menschenverstand. Brechen Sie dann das Online-Banking unvermittelt ab.

Ihr Computer

Sie müssen nicht unbedingt das technisch aktuellste Computersystem haben, um sicheres Online-Banking betreiben zu können. Sie müssen aber Ihre Software stets auf dem aktuellen Stand halten. Dies gilt insbesondere für die sogenannte Betriebssystem-Software und für den von Ihnen verwendeten Internet-Browser. So stellen Anbieter wie beispielsweise Microsoft regelmäßig sogenannte „Patches“ bereit, die erkannte Gefahren zumindest minimieren können. Nutzen Sie die Möglichkeit automatisierter Updates, die Ihnen Ihr Betriebssystem bietet.

Neben den bereits seit vielen Jahren verfügbaren und sicherlich auch obligatorischen Virenschutzprogrammen sollten Sie darüber hinaus auch spezielle „Malware Scanner“ einsetzen. Malware, eine Kombination aus dem englischen „malicious“ (bösartig) und „ware“ (Software), ist die Bezeichnung für ein schädliches Programm (Schadsoftware).

So gehört beispielsweise die aktuell hochproblematische Verbreitung sogenannter „Ransomware“ zu der Familie der Malware. Ransomware, von englisch „ransom“ für „Lösegeld“, auch bekannt als Erpressungstrojaner, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden Daten auf dem Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.

Wir reden bei all diesen Maßnahmen über Ihren privaten Rechner. Im Umkehrschluss bedeutet das:

- **Nutzen Sie niemals öffentliche Rechner für Ihr Onlinebanking!**

Zu öffentlichen Rechnern dürfen Sie durchaus auch den Rechner an Ihrem Arbeitsplatz zählen. Auch wenn Sie Ihren Kollegen und Kolleginnen vertrauen… die Sicherheit Ihres Online-Banking muss absolute Priorität haben.

Verfahren des Online-Banking

Die Vielzahl angebotener Verfahren macht es oftmals für den Einsteiger in das Online-Banking schwierig, sich zu orientieren.

Das **iTan**-Verfahren ist der „Klassiker“, weil es zu den „Urvätern“ der Onlinebanking-Verfahren

zählt. Bei diesem Verfahren händigt Ihnen die Bank eine Papierliste mit nummerierten Transaktionsnummern (Tan) aus. Nachdem Sie die Überweisungsdaten am Computer eingegeben haben, gibt Ihnen die Bank nach dem Zufallsprinzip eine Tan von der Liste vor, mit der Sie die Überweisung bestätigen. Die Tan ist nur wenige Minuten und auch nur einmal gültig, dann verfällt sie. Der Sicherheitslevel ist hierbei nicht allzu hoch, weil die iTan nicht an die Überweisungsdaten gebunden ist.

Die Betrugs-Taktik

Sie erhalten eine scheinbar seriöse Mail und sollen auf einen Link klicken. Wenn Sie dem folgen landen Sie auf einer Ihrer Bank-Homepage täuschend echt nachempfundenen Website. Dort geben Sie dann Ihre Zugangsdaten ein und auch die Tan. Die Betrüger haben nun Zugriff auf Ihr Konto!

Nach heutigem Stand der Technik können die folgenden Verfahren als sicherer eingestuft werden:

- **mobileTan**

Bei der mobileTan, auch SMS-Tan genannt, sendet die Bank per SMS die Tan an die von Ihnen angegebene Mobilfunknummer. In der SMS werden auch der Betrag und mindestens die letzten vier Stellen des Empfänger-Kontos genannt.

Die Betrugs-Taktik

Die Rechner von Bankkunden werden mit Schadsoftware infiziert, um Zugangsdaten und Mobilfunknummer zu erhalten. Anschließend wird im Namen des Bankkunden eine neue Sim-Karte für das Handy bestellt. Dann gibt es Betrüger, die sich als Mitarbeiter von Mobilfunkshops ausgeben und wegen angeblichem Verlust eine Ersatz-Sim-Karte für „ihren Kunden“ bestellen.

Versteckte Kosten

Was viele beim mobileTan Verfahren nicht bedenken: Jede SMS kostet Geld. Wie oft die Banken Gebühren für SMS-Tan nehmen, ist jedoch weitestgehend nicht bekannt. Nachforschungen ergaben, dass zwar die ersten SMS kostenfrei sind, dann aber kassieren die Banken pro SMS im Schnitt 9 Cent. Die Kosten pro SMS können aber auch durchaus bis 25 Cent betragen. Vieles spricht dafür, dass diese Gebühr rechtswidrig ist. Genau aus dem Grund läuft derzeit eine Verhandlung beim Bundesgerichtshof (BGH). Das Urteil wird Ende Juli erwartet.

- **ChipTan**

Hierbei wird Ihre Girocard für das Verfahren registriert und bei Ihrer Bank erwerben Sie einen Tan-Generator.

Nach dem Ausfüllen beispielsweise einer Überweisung werden diese in ein Schwarz-Weiß-Bild mit fünf Balken, ähnlich einem Strichcode, gewandelt (Flicker-Code-Verfahren). Sie halten den Tan-Generator nun vor die wechselnd aufleuchtenden Balken. Die Signale werden übertragen und im Tan-Generator wird die Tan angezeigt, die Sie abschließend am Computer eingeben.

Dieses Verfahren ist weitestgehend sicher, weil die Tan auftragsbezogen erzeugt wird und nur mit

Ihrer Girocard arbeitet.

Die Betrugs-Taktik

Aber auch dieses Verfahren hat ein Leck, wenn Sie als Bankkunde das Zulassen: Betrüger infizieren Ihren Computer mit einer Schadsoftware, dann bekommen Sie beispielsweise die Meldung, ein ChipTan-Test sei erforderlich. Oder Sie werden aufgefordert, falsch überwiesenes Geld zurückzuschicken. Oder Ihnen werden hohe Gewinnchancen suggeriert, wenn Sie per Überweisung an einem Gewinnspiel teilnehmen. Nur dass Sie dann nicht die Überweisungsfunktion Ihrer Bank nutzen.

- **PhotoTan**

Das PhotoTan-Verfahren arbeitet ähnlich wie die ChipTan. Auch hier benötigen Sie ein spezielles Lesegerät, das Sie bei Ihrer Bank registrieren lassen.

Nach Eingabe der Überweisungsdaten am Computer, wird auf Ihrem Bildschirm eine farbige Grafik angezeigt, die Sie mit Ihrem Lesegerät scannen. Das Lesegerät entschlüsselt die Bilddaten und die Tan wird generiert.

Dieses Verfahren ist vergleichsweise sicher, wenn die Tan mit dem **zuvor registrierten Lesegerät** erzeugt wird. Die Nutzung einer PhotoTan-**App**, die Sie auf Ihrem Smartphone installieren müssen, verringert diesen Sicherheitsgewinn deutlich.

- **App-Tan (SecureGo der Volks- und Raiffeisenbanken, Bestsign der Postbank)**

Für das AppTan-Verfahren installieren Sie eine kostenlose App auf Ihrem Smartphone, die anschließend aktiviert wird. Dafür erhalten Sie von Ihrer Bank einen Anmeldenamen und eine Ziffernfolge für die Legitimation oder einen QR-Code zum Einscannen mit dem Smartphone.

Dieses Verfahren ist dann relativ sicher, wenn die Banking-App und die AppTan auf **zwei voneinander unabhängigen** Geräten betrieben werden. Aber… wer nutzt schon zwei Smartphones um eine Überweisung zu tätigen?

Die Betrugs-Taktik

Wissenschaftlern gelang es unter Laborbedingungen, das Verfahren durch die Infizierung des Smartphones mit einer Schadsoftware zu überlisten.

Wie die Banken ein sicheres Online-Banking garantieren

Die Banken betreiben für ihre eigene und für die Sicherheit ihrer Kunden einen erheblichen Aufwand, der permanent angepasst wird. Dazu gehören…

- dedizierte Firewalls,
- ein verschlüsselter Datenaustausch,
- regelmäßige Sicherheitschecks durch darauf spezialisierte Firmen,
- die Analyse von Verhaltensmustern und das daraus resultierende Anlegen schwarzer Listen,

um illegale Buchungen bereits vor der Ausführung zu stoppen.

Online-Banking zählt mit Sicherheit zu den sensibelsten Verfahren im Rahmen unseres Umgangs mit Computern. Schließlich hängt unsere materielle Existenz auch davon ab, dass wir unsere Finanzflüsse im Griff haben und andere nicht ohne unsere Zustimmung von unserem Geld profitieren.

Die Banken sorgen weitestgehend und überwiegend für einen sicheren Betrieb des Onlinebanking. Wenn Sie sich für ein sicheres Verfahren entscheiden und auch die unter „Spielregeln“ beschriebenen Sicherheitsaspekte und Vorsorgemaßnahmen strikt befolgen, dann können Sie die Gefahren, die von Internet-Betrügern ausgehen reduzieren und sich an all den Vorteilen, die Online-Banking mit sich bringt, erfreuen.

Und sollten Sie doch mal Probleme haben, dann scheuen Sie nicht den Kontakt. Rufen Sie uns an unter 0214 90 98 400 und vereinbaren Sie einen Termin für eine kostenfreie Erstberatung.

Guido Lenné

Rechtsanwalt aus der Anwaltskanzlei Lenné.
Rechtsanwalt Lenné ist auch Fachanwalt für Bank- und Kapitalmarktrecht.

Wir helfen Ihnen gerne! Kontaktieren Sie uns. Oder vereinbaren Sie hier online einen Termin für eine telefonische kostenfreie Erstberatung.

Lenné Anwaltskanzlei

Zurück

Anwaltskanzlei Lenné · Max-Delbrück-Str. 18 · 51377 Leverkusen · Telefon (0214) 909840-0 · Telefax (0214) 909840-29 · info@anwalt-leverkusen.de · www.anwalt-leverkusen.de
Standort München · Brienner Straße 44 · 80333 München · Telefon (089) 21552745 · Telefax (0214) 21552746 · info@anwalt-muenchen.de · www.anwalt-muenchen.de