CYBERKRIMINALITÄT – SO KÖNNEN SIE SICH SCHÜTZEN

© ISTOCK.COM/ANYABERKUT

BETRUGSVERSUCH **IM INTERNET**

Online-Banking

– ein Quantensprung mit Restrisiko

Tipps für den sicheren Umgang mit den Bankgeschäften im Internet.

SYMBOLFOTO: UNSPLASH

Von Frank Beckenbach

Göttingen. Das Online-Banking boomt gewaltig. Immer mehr Bankkunden nutzen diesen Service, den es schon seit knapp 40 Jahren gibt. Online-Banking ist sicher, wenn der Nutzer sich an die Regeln hält. Spezialisten der hiesigen Banken und des Vereines für Cybersicherheit geben Tipps, was der Nutzer unbedingt beachten sollte.

Von einem Randgeschäft zum Mainstreambusiness, so lässt sich der Verlauf des Online-Bankings in den vergangenen 40 Jahren vielleicht am besten beschreiben. Im Jahr 1983 war es die Bank of Scotland, die ihren Kunden den „Homelink" anbot, das erste Online-Banking-Angebot überhaupt. Es war langsam, teuer, aber ein Beginn. Die Kundenzahlen ließen sich aber noch an den Händen abzählen. Der Software-Anbieter Microsoft kreierte eine „Personal Finance Software", in der er auch Online-Banking integriert hatte, das war allerdings mehr als zehn Jahre später, im Jahr 1994. Die Verbreitung des Online-Bankings nahm sehr langsam Geschwindigkeit auf. Etwa 100.000 Menschen sollen dieses Microsoft-Angebot damals genutzt haben.

In Deutschland begann das Zeitalter des Online-Bankings erst Ende der 1990er Jahre. Acht Prozent der Bankkunden nutzten im Jahr 1998 dieses Angebot. Den Aufschwung des Online-Bankings konnte auch die Finanzkrise 2007/2008 nur kurz abbremsen. Bis zum Jahr 2014 waren es schon fast 50 Prozent der Bankkunden, die Bankgeschäfte via Internet abwickelten.

Experten sprechen von drei Kriterien, die für den massiven Aufschwung des Online-Bankings verantwortlich waren. Zum einen wurde das Telefonieren im Fest- und Mobilnetz deutlich preisgünstiger. In den 1990er Jahren wurden Minutentakte beim Telefongespräch abgerechnet, heutzutage kaum noch vorstellbar. Beim Mobilfunk waren die Kosten noch deutlich höher als bei der Festnetztelefonie und auch die Geräte waren noch ziemlich unkomfortabel.

Der nächste, auch für die Kunden, sehr wichtige Schritt in der Online-Banking-Geschichte war die SSL-Verschlüsselung der Verbindungen. SSL steht für Secure Sockets Layer (heute mit seiner Weiterentwicklung Transport Layer Security) und bezeichnet eine Methode, um den Datenverkehr zwischen einem Browser und einer Webseite so zu verschlüsseln, damit kein Hacker die Daten mitlesen oder verändern kann. Diese Methode stellt also sicher, dass die Daten, die zwischen zwei Systemen übertragen werden, beispielsweise vom Online-Banking-Kunden zur Website seiner Bank, privat bleiben.

Mit dieser Technologie konnte den sogenannten „Man-in-the-Middle-Angriffen" ein Riegel vorgeschoben werden. Denn so lange es das Internet gibt, versuchen Hacker an fremde Daten zu gelangen und daraus Kapital zu schlagen. Die Hacker setzen dafür ein Abhörprogramm auf einen Server ab, der eine Website hostet. Gibt ein Nutzer nun Daten auf dieser Website ein, wird das Abhörprogramm aktiv, erfasst diese Daten und schickt sie gleich an den Hacker weiter. Ist eine Website aber SSL-verschlüsselt, kommt es zwischen Browser und Server zu einer verschlüsselten Verbindung, der Hacker und sein Abhörprogramm haben keine Zugriffsmöglichkeiten – sie sind ausgesperrt.

Wer also Bankgeschäfte im Netz nutzt, sollte unbedingt darauf achten, dass die Adresszeile im Browser immer mit „https" beginnt, das ist wie das Schloss ein Zeichen für eine verschlüsselte Verbindung. Und bei jedem Besuch sollte die Internet-Adresse die gleiche sein, auch darauf muss der Nutzer immer achten. Sollte das nicht der Fall sein, die Seite zum Beispiel zwar aussieht wie das Original, aber eine nicht vertraute Adresse hat, ist diese besser umgehend zu schließen.

Die beiden Faktoren, die günstigeren Verbindungskosten und die sichere Verbindung durch die SSL-Verschlüsselung, brachten die Akzeptanz der Kunden, so dass das Online-Banking komplett durchstartete.

Heute ist das Online-Banking quasi die Hauptgeschäftsstelle eines jeden Bankhauses. Bei der Sparkasse Göttingen sind beispielsweise 64 Prozent der Girokonten für das Online-Banking freigeschaltet. Bei Firmengirokonten sind dies sogar 72 Prozent, bei Privatgirokonten 62 Prozent. Auch bei den VR-Banken Mitte und Südniedersachsen, der Volksbank Kassel Göttingen sowie der Sparkasse Duderstadt werden mehr als die Hälfte der Konten via Online-Banking betrieben, Tendenz weiter stark steigend.

Die Spezialisten der Sparkassen Göttingen und Duderstadt, der VR-Banken Mitte und Südniedersachsen, der Volksbank Kassel Göttingen sowie der Vorsitzende des Vereins für Cybersicherheit e.V. geben nun wertvolle Tipps rund um das Online-Banking:

JAN DANIEL BREMER

VR-BANK IN SÜDNIEDERSACHSEN

„Aufgrund der Anforderungen der Aufsichtsbehörden, wie auch aus eigener Verantwortung heraus, erfüllen die Banken in Deutschland generell sehr hohe Schutzanforderungen an die IT", sagt Jan Daniel Bremer, Business Administrator der VR-Bank Südniedersachsen. „Die von der Bank angebotenen Verfahren können bei richtiger Anwendung als sicher angesehen werden. Angriffspunkte für die Betrüger ist generell ein potenzielles Fehlverhalten des Nutzers. Geben Sie niemals Zugangsdaten oder TAN-Nummern weiter, auch dann nicht, wenn Sie es mit einer vermeintlich seriösen Person (Bankmitarbeiter, Sicherheitsbeauftragter, Microsoft-Mitarbeiter, Polizei,...) zu tun haben. Die Bank-Mitarbeiter werden Sie niemals nach Ihren TAN, persönlichen Passwörtern oder PIN fragen. Nicht per Mail, nicht per Telefonanruf und auch nicht an der Haustür. Gleiches gilt auch für die Polizei oder Microsoftmitarbeiter." Und: „Nach einer Online-Banking-Sitzung sollte man sich immer ausloggen."

MARCEL WAGENER

SPARKASSE GÖTTINGEN

„Seien Sie grundsätzlich aufmerksam, wenn es um das eigene Online-Banking geht", empfiehlt Marcel Wagener, verantwortlich für den Bereich Online-Banking bei der Sparkasse Göttingen. „Wenn Ihre Zugangsdaten per Telefon oder per E-Mail abgefragt werden oder Sie auf elektronischem Wege eine Nachricht über die Sperrung Ihres Online-Bankings mit einem Link zur Wiederherstellung erhalten, sollten Sie diesen Vorgang sofort abbrechen." Er empfiehlt in einem solchen Fall selbst Kontakt mit der Bank aufzunehmen und nachzufragen. „Im Zweifelsfall gilt: Lieber einmal zu viel, als einmal zu wenig bei Ihrem Kundenberater oder Ihrer Kundenberaterin anrufen."

ANNETTE BÖHLE

VOLKSBANK KASSEL GÖTTINGEN

„Von grundlegender Bedeutung ist der Basisschutz auf den Geräten, das heißt, Betriebssystem und Programme sollten aktuell und sicher sein, Virenschutzprogramme und Firewalls verwendet werden", sagt Annette Böhle, Abteilungsleiterin Zahlungsverkehr der Volksbank Kassel Göttingen. Essentiell seien sichere Passwörter, die sich aus Kombinationen von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen zusammensetzen und die regelmäßig geändert werden. Downloads sollten nur von bekannten und vertrauenswürdigen Quellen erfolgen. „Niemals dürfen die Zugangsdaten zum Online-Banking im Browser gespeichert werden und auch nicht an Dritte weitergegeben werden", sagt Böhle.

DANIEL ZÖPFGEN

SPARKASSE DUDERSTADT

„Es ist tatsächlich so, dass fast ausschließlich der Mensch das Ziel von Kriminellen ist", sagt Daniel Zöpfgen, Fachberater für Giro- und Zahlungsverkehr der Sparkasse Duderstadt. Das bedeute, dass der Online-Banking-Nutzer mit verschiedenen Methoden dazu gebracht werde, entweder eine Überweisung selbst auszuführen oder dem Kriminellen eine Transaktionsnummer (TAN) herauszugeben. „Die wichtigste Waffe gegen Cyberkriminelle ist der gesunde Menschenverstand. Außerdem sollte man sich zeitlich und mental nicht unter Druck setzen lassen (Stichwort Schockanrufe). Und Unbekannten sollte man niemals Zugriff auf den eigenen Rechner gewähren (Stichwort Microsoftanrufe)."

UWE LÜHRIG

VEREIN FÜR CYBERSICHERHEIT NIEDERSACHSEN

„Viele Nutzer benutzen einfache Kennwörter für die Entsperrung der jeweiligen App oder für den Zugang zum Konto", sagt Uwe Lührig, 1. Vorsitzender des Vereins für Cyber-Sicherheit Niedersachsen e.V.. „Oder es wird recht sorglos mit dem Pin-Code für die Konto- oder Scheckkarte umgegangen." Er empfiehlt dringend, Online-Banking nie in einem öffentlichen WLAN durchzuführen. „Selbst wenn ein VPN-Tunnel (VPN ist ein Virtuelles Privates Netzwerk, Anm. der. Red.) genutzt wird, ist dies nicht zu empfehlen, es sei denn der Tunnel wurde von Profis sicher eingerichtet." Und: „Beim Verlust des Handys ist dies unbedingt – genau wie beim Verlust der Scheckkarte – bei dem entsprechenden Bankinstitut zu melden." Hier könne dann, wie beim Verlust der eigenen Scheckkarte, alles weitere in die Wege geleitet werden.

FLORIAN HARTLEIB

VR-BANK MITTE

„Seien Sie skeptisch und kontaktieren Sie im Zweifelsfall immer die Bank. Lieber einmal mehr bei der Bank nachfragen und ein ungutes Bauchgefühl abklären", sagt Florian Hartleib, Prokurist der VR-Bank Mitte, er betont die Wichtigkeit der Präventionsarbeit gerade in diesem Bereich. „Eine wichtige Faustregel ist und bleibt: Niemals würden wir Sie telefonisch oder per Mail um die Weitergabe von PIN und TAN bitten."

NEUN TIPPS **FÜR SICHERES ONLINE-BANKING**

Betrügern keine Chance geben

Mit Online-Banking erledigen Sie Ihre Bankgeschäfte schnell und bequem, rund um die Uhr. Und Online-Banking ist sicher – wenn Sie ein paar wichtige Regeln beachten. Geben Sie Datendieben keine Chance und schützen Sie sich zuverlässig vor Angriffen.

1. Achten Sie auf die richtige Adresse

Wenn Sie Ihre Bankgeschäfte im Netz starten, achten Sie bitte auf die Adresszeile in Ihrem Browser. Die angezeigte Adresse (URL) muss mit „https" starten. Bei jedem Ihrer Besuche sollte die Internet-Adresse die gleiche sein. Gelangen Sie mal auf eine Seite, die zwar richtig aussieht, aber eine nicht vertraute Adresse hat, brechen Sie Ihre Anmeldung sofort ab.

Das „https" in der Internetadresse (statt des üblichen „http") zeigt Ihnen eine verschlüsselte Datenleitung an. Das zusätzliche „s" steht für „secure" – sicher. Die Internetseiten für die Bankgeschäfte sind immer TLS-verschlüsselt. Diese Verschlüsselung stellt sicher, dass niemand während der Übertragung Ihre Daten mitliest oder verändert.

Tipp: Am besten steuern Sie Ihr Online-Konto immer von der Internetseite Ihrer Bank aus an. Speichern Sie Ihre Zugangsdaten nicht auf Ihrem Computer. Geben Sie die Daten lieber jedes Mal neu von Hand ein.

2. Nutzen Sie ein sicheres Passwort

Wählen Sie zum Anmelden im Online-Banking ein sicheres Passwort. Verwenden Sie nicht das gleiche Passwort wie zum Beispiel in Shopping-Portalen. Sonst machen Sie es Datendieben leicht.

3. Achten Sie auf das verriegelte Schloss

Am Schlosssymbol in der Adresszeile Ihres Browsers erkennen Sie, ob Ihre Daten sicher übertragen werden. Das Schloss muss dafür immer geschlossen dargestellt sein. Manche Browser färben auch das Adressfeld grün ein.

4. Im Zweifelsfall Online-Banking abbrechen

Zeigt Ihr Browser beim Verbinden mit den Bank-Seiten an, dass ein Schlüssel nicht erfolgreich geprüft werden konnte, wählen Sie sofort „Abbrechen". Denn dann ist nicht garantiert, dass die Verbindung sicher ist. Sagen Sie in einem solchen Fall Ihrer Bank Bescheid.

Bitte beachten Sie: Die Daten-Verschlüsselung schützt Ihre vertraulichen Kontodaten vor Dritten. Ihr Internet-Service-Provider kann trotzdem nachvollziehen, wann und mit wem Sie online Kontakt hatten. Diese Informationen müssen laut Gesetz über einen festgelegten Zeitraum gespeichert werden. Zum Beispiel für die Terrorabwehr.

5. Schützen Sie Ihre PIN und TAN

Mit Ihrer Geheimzahl (PIN) und Ihren Transaktionsnummern (TAN) geben Sie Zahlungen frei. Deshalb sind das sehr sensible Daten. Geben Sie sie nie heraus. Auch nicht, wenn Sie eine scheinbar seriöse Stelle dazu auffordert. Banken werden Sie niemals bitten, Zugangsdaten, PIN oder TAN anzugeben. Weder persönlich, telefonisch noch mit einer E-Mail.

6. Bleiben Sie aufmerksam

Wenn Sie Zweifel haben und Ihnen während der Verbindung zum Online-Banking etwas dubios vorkommt – brechen Sie die Aktion besser ab.

7. Setzen Sie ein Tageslimit

Sie können für Ihre Internet-Bankgeschäfte ein Tageslimit festlegen. Jede Anfrage, die darüber hinausgeht, wird automatisch abgelehnt. Sollten sich Kriminelle tatsächlich Zugang zu Ihrem Konto verschafft haben, können Sie diese so erst einmal ausbremsen. Orientieren Sie sich für Ihr Limit am besten an Ihren durchschnittlichen Überweisungen pro Tag. Natürlich können Sie das Limit aber auch jederzeit wieder ändern.

8. Melden Sie sich immer ab

Machen Sie es beim Internet wie Zuhause: Schließen Sie ab, wenn Sie gehen. Denn das ist sicherer, als einfach nur die Wohnungstür ins Schloss fallen zu lassen. Übertragen auf das Internet heißt das: Schließen Sie nicht einfach das Browserfenster, wenn Sie Ihre Aufgaben erledigt haben. Nutzen Sie immer die Funktion „Abmelden" für Seiten, die nur durch Anmelden erreichbar sind. Wie zum Beispiel Ihr Zugang für Ihre Bankgeschäfte. Nur so wird die Datenverbindung zu einem Internet-Angebot zuverlässig gekappt.

Schließen Sie nach dem Online-Banking auch den Browser. Dies ist besonders wichtig, wenn Sie einen Rechner benutzen, zu dem mehrere Personen Zugang haben.

9. Verwischen Sie Spuren

Löschen Sie zur Sicherheit grundsätzlich am Schluss jeder Sitzung den Zwischenspeicher (Cache) des verwendeten Browsers. Noch besser: Nutzen Sie von vornherein den „privaten Modus" oder „Inkognito-Modus", den moderne Browser anbieten. Dann wird erst gar keine Historie angelegt, die Sie löschen müssten.

(QUELLE: SPARKASSEN-FINANZPORTAL GMBH)