

Online-Banking: Wenn Phisher Daten angeln

Ulrike Peter

Es ist einfach, komfortabel und schnell: PC, Laptop oder Smartphone einschalten, Verbindung zur Hausbank herstellen und online die Geldgeschäfte erledigen. Was soll schon passieren? Ein Trugschluss. Denn in Deutschland nehmen die Betrugsfälle im Zusammenhang mit Online-Banking drastisch zu. Eine Ursache: Sicherheit wird als selbstverständlich vorausgesetzt und den Finanzinstituten zugeschrieben, eigene Schutzmaßnahmen ergreifen die wenigsten – eine verhängnisvolle Sorglosigkeit, die Hacker und Datendiebe antreibt.

IN DIESEM ARTIKEL ERFAHREN SIE...

- welchen Phishing-Gefahren User beim Online-Banking ausgesetzt sind.
- wie Anwender sich schützen können.

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN...

- Kein spezielles Vorwissen

Phishing ist das Stichwort. Dabei ist das ‚Abfischen‘ von individuellen Zugangsdaten und persönlichen Informationen nichts anderes als der alte Haustür-Trick, der die Arglosigkeit des Gegenübers ausnutzt. Er findet im IT-Zeitalter eben im Internet statt. Denn das World Wide Web nutzen immer mehr Menschen, gerade auch für ihre Finanzen.

Fast 26 Millionen Deutsche erledigen ihre Bankgeschäfte mittlerweile online. Das sind, so hat es im Mai 2010 der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) ermittelt, rund zwei Millionen mehr als im vergangenen Jahr. Damit nutzen derzeit 41 Prozent aller Bundesbürger quer durch alle Altersklassen (von 16 bis 74 Jahren) Online-Banking. 2003 waren es erst 21 Prozent.

Angst vor Hackern, aber kaum Eigeninitiative

Aber die Medaille hat zwei Seiten: 49 Prozent der Deutschen haben Angst vor kriminellen Übergriffen, wenn sie ihre Bankgeschäfte im Internet erledigen. Für jeden fünften Kontoinhaber ist dies Grund genug, komplett auf Online-Banking zu verzichten.

Und obwohl Datenschutz und -sicherheit ganz oben auf der Anforderungsliste der Nutzer stehen, sind sie kaum bereit bzw. sehen keine Veranlassung, selbst

aktiv zu werden. Eigene Schutzmaßnahmen ergreifen die wenigsten – geschweige denn, dass sie sich über die Risiken oder Sicherheitslösungen informieren. So ist beispielsweise der sichere Standard – die mobile TAN-Technik (mTAN) – den meisten gar nicht bekannt. Nicht einmal jeder zehnte Bankkunde schätzt das Sicherheitsniveau des modernen Verschlüsselungssystems richtig ein. Dies förderte die Anfang September 2010 veröffentlichte Studie „Online-Banking“ des Hamburger Software- und Beratungshauses PPI zu Tage.

So klafft die Lücke zwischen denen, die aus Angst die Finger ganz von Finanztransaktionen im Internet lassen und denen, die die Einstellung vertreten „Die Bank wird’s schon richten“. Diese Haltung könnte jedoch zum Verhängnis werden.

Phishing nimmt bundesweit zu

Eigeninitiative scheint mehr denn je anbracht, betrachtet man die Anfang August 2010 in der „Financial Times Deutschland“ (FTD) veröffentlichten Zahlen. So verzeichnete das Bayerische Landeskriminalamt (LKA) für das erste Halbjahr 2010 laut FTD eine Verdopplung der Phishing-Attacken. Die bislang gemeldeten 770 Fälle liegen bereits heute über Vorjahresniveau mit 736 Anzeigen. Und es werden weitere Bundesländer zi-

tiert: „Wir haben schon jetzt die Zahlen des Vorjahrs erreicht“, soll ein Sprecher des Berliner LKA bestätigt haben (2009: rund 500 Fälle). Auf FTD-Anfrage hätten ebenfalls die Sprecher des Hessischen und des Baden-Württembergischen LKA angegeben, dass die Tendenz stark steigend sei.

Kein Wunder, dass Bundeskriminalamt (BKA) und Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Vorsicht raten: Aktuell verbreitet sich eine völlig neue Variante von Schadsoftware, die Kreditkarten- und Online-Banking-Daten ausspioniert. Der Trojaner in seiner Ursprungsform treibt bereits seit mehreren Jahren sein Unwesen. Seine neue Variante hat es jetzt gezielt auch auf TANs von Online-Banking-Nutzern abgesehen. Die Ausspähung erfolgt meist durch ein so genanntes Drive-by-Exploit, also den Besuch einer mit Schadcode infizierten Webseite und das hierdurch automatische Herunterladen des Schädlings. Ist der PC infiziert und der Nutzer öffnet die Anmeldemaske seiner Bank, wird er mit manipulierten Inhalten getäuscht und beispielsweise mit folgender Nachricht zur Preisgabe seiner Daten animiert:

„Die XY Portal passt sich den hohen Kundenansprüchen an. Wir bleiben immer auf dem neusten Stand mit Sicherheitsvorschriften um unseren Kunden mehr Sicherheiten zu bieten.

Unser Sicherheitsabteilung erfand ein neues Sicherheitssystem, die Angriffe von Dritten verhindert um Betrugsfälle. Diese Sicherheitssystem muss von allen Online-Banking-Kunden genutzt werden. Wir empfehlen Ihre Daten zu Angleichung anzugeben. Sollte die Anmeldung in 48 Stunden nicht erfolgen, so wird Ihre Karte vorübergehend gesperrt, bis zu Ende der Anmeldevorgang.“ Man beachte: Derartige Zeilen und auch klassische Phishing-Mails weisen gerne sprachliche Mängel auf, also stets auf der Hut sein und sorgfältig lesen.

Im Untergrund: Zero-Day-Exploit

Eine der tückischsten Methoden dieser Art ist sicherlich der Zero-Day-Exploit. Michael Eisenmann, IT-Security-Consultant des Global Sourcing-Spezialisten NIIT Technologies GmbH, erklärt dazu: „Jede Software wie z.B. das Betriebssystem oder der Webbrowser weist Schwachstellen auf, die sich Angreifer zu Nutze machen können. So erlangen sie in einem gewissen Umfang Kontrolle über ein System oder veranlassen es, Aktionen auszuführen. Besonders gefährlich sind Zero-Day-Attacken. Denn sie zielen auf Schwachstellen ab, die noch nicht bekannt sind – der Softwarehersteller wird somit erst zum Zeitpunkt des Angriffs darauf aufmerksam. Daher kann es noch keine signaturbasierte Erkennung und auch keinen Patch geben und der Nutzer hat es schwer, sich zu schützen.“

Die NIIT Technologies hat daher hierzu ein paar Empfehlungen für Anwender zusammengefasst, wie der Schutz vor Zero-Day-Exploit erhöht werden kann:

- Nie mit Administratorrechten arbeiten
- Nicht verwendete Programme deinstallieren
- Diversität: Populäre Software ist Zielscheibe von Angriffen. Dies bei der Auswahl der eingesetzten Software beachten
- Virenschutz namhafter Hersteller, der vor “Zero-Day“-Angriffen schützt, einsetzen
- Betriebssystem, Webbrowser inklusive Pluggins und AddOns sowie weitere installierte Software mittels Updates und Patches auf dem aktuellen Stand halten
- Eine Firewall einsetzen und nur benötigten Datenverkehr erlauben (so restriktiv wie möglich – so frei wie nötig)
- Niemals auf in E-Mails enthaltene Links klicken. Adresse manuell im Browser eingeben und nicht die Browsereigene Erinnerungsfunktion nutzen
- Bei der Eingabe persönlicher Daten darauf achten, dass eine SSL-gesicherte Verbindung (https) aufgebaut wurde
- Das Zertifikat muss von einer anerkannten Stelle ausgestellt worden sein
- E-Mails und darin enthaltene Anhänge nur dann öffnen, wenn sie aus vertrauenswürdiger Quelle stammen. Bei Unklarheiten telefonisch mit dem Absender der E-Mail in Kontakt treten.

Bezahldienste unter Beschuss

Gefahren sind jedoch nicht nur Online-Banking-Kunden, sondern auch die Nutzer des globalen Bezahlendienstes PayPal ausgesetzt. Hier werden immer wieder Phishing-Mails, die vermeintlich von PayPal stammen, in Umlauf gebracht, um individuelle Daten abzugreifen. Der User wird zum Anklicken eines vermeintlich korrekten Links und dann auf einer täuschend echten „Kopie“ der Website zur Eingabe seiner Zugangsdaten aufgefordert – diese landen dann geradewegs in den Händen der Hacker. Gerade in den letzten drei Monaten traten hier immer wieder Phishing-Wellen auf. In einem Fall gaben sich die Betrüger als Vertreter des Bezahlendienstes aus und brachten die Empfänger über einen Link zur Eingabe ihrer Kreditkartendaten. Diese wurden dann direkt ins Notizbuch des Datendiebs diktiert.

Auch hier gilt die Faustregel: Paypal und Kreditkarteninstitute fordern ihre Kunden grundsätzlich nie zur Eingabe solcher Daten auf. Ist man dennoch im Zweifel, empfiehlt sich der Anruf bei Dienstleister, um auf Nummer sicher zu gehen. Des Weiteren sollte man grundsätzlich nie einen Link in einer Mail anklicken, sondern sich die Mühe machen, ihn in den Browser zu kopieren.

Vorsorge statt Nachsorge mit eAusweis

Neben klassischen Schutzprogrammen wie Anti-Viren-Software oder Firewall mit Erkennung von Phishing-Attacken und der eigenen Achtsamkeit kann der elektronische Personalausweis, der zum 1. November 2010 eingeführt wird, Abhilfe schaffen. Mit der Nutzung des Dienstes auf freiwilliger Basis können sich sowohl Nutzer als auch Anbieter von Online-Services ausweisen. Der Bankkunde legt dafür seinen Ausweis auf das spezielle Lesegerät und authentifiziert sich mit seiner persönlichen Identifikationsnummer (PIN). Zum Auslesen seiner digitalen Daten sind dann nur entsprechend zertifizierte Unternehmen bzw. Organisationen berechtigt. Sie müssen zudem jeweils durch den Kartenbesitzer autorisiert werden. Laut BITKOM beabsichtigen fast 40 Prozent der Internet-Nutzer, den neuen Ausweis zukünftig beim Online-Banking zu nutzen.

Fazit: Damit Datendiebe nicht in fremden Gewässern, sondern im Trüben phishen, sollten sich Nutzer von Online-Banking nicht nur auf die Schutzmaßnahmen ihres Finanzinstitutes verlassen, sondern sich ein eigenes Bollwerk gegen Zugriffe von außen aufbauen. Gleichzeitig empfiehlt sich die umfassende Information über Gefahren und Sicherheit sowie eine gesunde Skepsis. Im Zweifel hilft dann „Back to the Roots“: den PC aus- und den guten alten Bankautomaten einschalten.

ULRIKE PETER

Der Autorin ist freie Journalistin und seit zehn Jahren für unterschiedliche Unternehmen und Medien in der IT-Branche tätig. Ihre Spezialisierung liegt hierbei auf den Themenbereichen ICT-Security, Netzwerke, IT-Strategien und Telekommunikation. Ihre Veröffentlichungen erstrecken sich über renommierte Medien aus der Fachpresse bis hin zu Tages-, Online- und Wirtschaftsmedien sowie vertikaler Branchenpresse.



Hacking School - Revolution in der Wissensvermittlung?

Auf den Regalen der Informatikbuchhandlungen findet man immer öfter Produkte zum Thema Hacken. Die Auswahl richtet sich jedoch vor allem an Personen, die schon über ein großes Fachwissen und reichlich Erfahrung verfügen. Für Anfänger, die sich für dieses Thema interessieren, sind diese Bücher zu kompliziert, entmutigend und helfen wenig weiter.

Der CSH Verlag beschloss, diese Marktlücke zu schließen und ein Lernset, welches der Sicherheits- und Hacking-Thematik gewidmet ist, zu veröffentlichen. Das Set ist sowohl für die Anfänger als auch für die Fortgeschrittenen nützlich. Das Produkt dieses Unternehmens ist das von Experten erstellte "Hacking School Set".

Warum ist dieses Buch anders als alle anderen?

Das Schulungsset "Hacking School" stellt sehr gute Einführung ins Hacken dar, sowohl für Anfänger als auch für Fortgeschrittene. Wir empfehlen dieses Set an Personen, welche die ersten Schritte in der Welt des Hackens und der Computersicherheit machen und Personen, die schon praktische Erfahrung besitzen und die von Hackern angewandten Techniken besser und vertiefter kennen lernen möchten.



Promotionscode nur für Leser der Zeitschrift **hakin9**
10% Rabatt: **42448** bei Kauf der Schulung

Bestellung des Schulungsexemplars
auf **www.HackingSchool.de**