orell füssli

Norbert Pohlmann / Markus Linnemann

Sicher im Internet

Tipps und Tricks für das digitale Leben

Leseprobe

Inhalt

Einleitung: Erfolgsgeschichte Internet – Chancen und Risiken

Das Internet ist aus unserem Leben nicht mehr wegzudenken! Surfen, E-Mails schreiben und Onlinebanking haben mittlerweile ebenso in unseren Alltag Einzug gehalten wie die rasant wachsenden sozialen Netzwerke Xing, Facebook oder Twitter. Riesig und komplex überwindet das Internet alle geografischen, politischen und administrativen Grenzen sowie kulturellen Unterschiede. Es schafft somit neue Wege, Demokratie und Bürgerbeteiligung zu gestalten – eine neue und ungewohnte Herausforderung für die internationale Gesellschaft und jeden einzelnen Nutzer.

Als Teil einer vernetzten Informations- und Wissensgesellschaft verlagern immer mehr Menschen ihr Berufs-, aber auch ihr Privatleben ins Internet. Die Risiken, denen sie sich dabei aussetzen, sind vielen jedoch unbekannt. Das Internet ist ein gewaltiger Datenspeicher, der begierig alles aufsaugt und nichts vergisst. Dazu gehören auch Informationen und Bilder, von denen wir nicht wollen, dass sie jedem Nutzer des World Wide Web zur Verfügung stehen. Sicherheitskritische Daten wie unsere Kontodaten geben wir im realen Leben nur ungern einem Fremden preis. Sollten wir dann nicht auch in der virtuellen Welt Vorkehrungen treffen, um unsere Daten zu schützen? Die Bedeutung des Themas Sicherheit hat im Internet in den letzten Jahren erheblich zugenommen, denn das Vertrauen der Nutzer in das Medium sinkt aufgrund

negativer Erfahrungen und sich häufender Nachrichten über Datenmissbrauch sowie immer neue Betrugsmaschen zwangsläufig. Sicherheitslücken schließen und die eigene Internetkompetenz stärken – diese Herausforderungen gilt es zu meistern, um die vielfältigen Möglichkeiten des Internets sicher nutzen zu können.

Ihr bester Schutz: IT-Sicherheit und Internetkompetenz

Ob Diebstahl von Identitätsdaten, Passwort-Fishing oder Viren, Würmer und Trojanische Pferde – die Angriffsmöglichkeiten auf unsere Daten werden immer raffinierter und professioneller. IT-Sicherheitsmaßnahmen wie Viren- beziehungsweise Malware-Scanner und Personal Firewalls helfen, diese Risiken zu minimieren, doch 100-prozentige Sicherheit kann es im Internet nicht geben – so wie es sie auch im realen Leben nicht gibt. Wir sind daher ergänzend auf die eigene Internetkompetenz angewiesen, die es uns ermöglicht, uns gefahrlos darin zu bewegen. Denn erst wenn uns die Gefahren bei der Nutzung des Internets bewusst sind, können wir unser Verhalten anpassen und unsere Daten schützen.

Über dieses Buch – ein kurzer Leitfaden

Dieses Buch verschafft Ihnen einen Überblick über die derzeitige Situation des digitalen Lebens und beantwortet all Ihre Fragen rund um das Thema «Sicher im Internet». Zahlreiche Tipps und Tricks helfen Ihnen, die Herausforderungen im

Umgang mit den modernen Medien souverän zu meistern – auch ohne vorher ein Informatikstudium absolviert zu haben.

Auf der Webseite *www.sicher-im-internet.de* erhalten Sie zudem aktuelle Informationen zu bestimmten Themen und Linksammlungen. Außerdem finden Sie dort ergänzende beziehungsweise vertiefende Hintergrundinformationen, Zusatztexte, Hilfen sowie Workshops zu speziellen Fragestellungen – darunter auch einige Screenvideos, welche die wichtigsten Einstellungen und Technologien Schritt für Schritt erklären.

Mithilfe der Softlinks in diesem Buch können Sie bequem den im Text befindlichen Verweisen auf die Webseite folgen, ohne jeweils die komplette Webadresse abtippen zu müssen. Unter *www.sicher-im-internet.de/softlinks/* können Sie den Softlink (dreistellige Nummer) in das Formular eintragen und gelangen dann direkt zum gewünschten Ziel.

Wir wünschen Ihnen bei der Lektüre dieses Ratgebers viele hilfreiche Einsichten und fordern Sie auf, uns unter der E-Mail-Adresse *feedback@sicher-im-internet.de* Feedback zu geben. Wir werden dann entsprechende Updates zur Verfügung stellen (Softlink 101).

Und noch ein Hinweis zum Schluss: Grundsätzlich bestehen Gefahren für alle Betriebssysteme, egal ob Mac OS, Linux oder Windows. Allerdings ist das Risiko eines Angriffs auf einen Mac-OS- und Linux-Rechner momentan noch geringer, weil sich die Angreifer wegen der hohen Verbreitung von Windows-Systemen auf diese konzentrieren. Deshalb gehen wir bei den Beschreibungen auch grundsätzlich von einem Windows-System aus, wobei die meisten Tipps für alle Betriebssysteme gleichermaßen gelten, da das Internet plattformunabhängig ist. Ist das einmal nicht der Fall, werden die Unterschiede an der jeweiligen Stelle kurz erläutert.

puter. Das Gleiche wird auch mit Programmen versucht, die vom Nutzer direkt aus dem Internet heruntergeladen werden sollen, um die angeblich gefundene Malware zu neutralisieren. Doch genau das Gegenteil ist der Fall: Die Malware wird von

... inhaltlicher Sprung ...

TIPP: Gesunder Menschenverstand

- Fallen Sie nicht auf unrealistische Sonderangebote und Versprechungen im Internet herein.
- Deinstallieren Sie Programme, die Sie nicht mehr benötigen. Weniger Programme bedeuten weniger Angriffsfläche für Malware.
- Verwenden Sie fremde USB-Sticks (und andere Speichermedien) nur, wenn Sie aus einer vertrauenswürdigen Quelle stammen.
- Lassen Sie sich von Scareware nicht zu voreiligen Handlungen verleiten. Im Zweifelsfall tun Sie besser nichts und holen den Rat eines Experten ein. Generell gilt im Internet: Sind Sie sich nicht sicher, unterlassen Sie die jeweilige Aktivität besser!
- Überprüfen Sie einen angebotenen Link im Web, bevor Sie einfach darauf klicken (siehe Seite 29f.).

Der Internetbrowser – sinnvoll einstellen, sinnvoll nutzen

Der Internetbrowser ist Ihr Tor zur digitalen Welt und das wichtigste Hilfsmittel, um im World Wide Web Informationen zu sammeln, Bankgeschäfte zu erledigen, einzukaufen, mit Freunden zu chatten, Zeitung zu lesen oder zu spielen. Diese Liste ließe sich fast endlos weiterführen. Gerade deshalb ist es

so wichtig, dass Sie einerseits einen sicheren Browser verwenden, andererseits aber auch wissen, wie dieser funktioniert und wie Sie ihn zu bedienen haben.

Erhältlich sind derzeit mehrere Browser von verschiedenen Herstellern. Von Vorteil ist, dass sie im Normalfall kostenlos angeboten werden. Sie haben also die Qual der Wahl, welchen Browser Sie verwenden wollen, oder Sie nutzen mehrere im Wechsel. Die bekanntesten und am häufigsten verwendeten Browser sind (in alphabetischer Reihenfolge):

- Google Chrome
- Mozilla Firefox
- Opera
- Safari
- Windows Internet Explorer

In der Linux-Welt gibt es noch zusätzliche Ableger, beispielsweise den Konqueror.

Der Begriff Browser kommt, wie die meisten Begriffe in der Informatik, aus dem Englischen und heißt so viel wie «umschauen» oder «schmökern». Und genau das lässt sich mit allen genannten Vertretern wunderbar erledigen. Das Anzeigen von Webseiten ist die wichtigste Funktion des Browsers. Früher gab es hier bereits die ersten Probleme, da die unterschiedlichen Browser die Webseiten auf verschiedene Arten darstellten, um sich voneinander abzuheben. Heute halten sich die Browserhersteller im Großen und Ganzen an die Vorgaben des W3C (**W**orld **W**ide **W**eb **C**onsortium). In diesem Konsortium sind alle wichtigen Firmen vertreten, um Standards für das Web zu erarbeiten und umzusetzen.

Mittlerweile gehen die Fähigkeiten eines Browsers aber weit über das reine Darstellen von Webseiten hinaus. Mit unterschiedlichen Technologien können die Browser auch PDF-Dateien anzeigen, Musik abspielen und animierte Inhalte darstellen.

Dieser Abschnitt stellt einen typischen Browservertreter mit seinen wichtigsten Funktionen vor und erläutert die sicherheitsrelevanten Aspekte bei der Nutzung im Internet. Anhand des flexiblen Open-Source-Browsers Firefox der Mozilla Foundation wird gezeigt, wie Sie Ihren Browser schon mit kleinen Eingriffen sehr gut absichern können, beziehungsweise wie der Browser Sie in Sicherheitsthemen unterstützen kann. Firefox wird gleichermaßen für Windows, Mac OS und Linux angeboten. Open Source bedeutet, dass die Programme, genauer gesagt deren Programmcodes, offen einsehbar sind und dass die Software kostenfrei genutzt werden kann.

Der Aufbau eines Browsers

Jeder Internetnutzer kennt einen Browser. Doch um die richtigen (Sicherheits-)Einstellungen genauer erläutern zu können, ist es sinnvoll, vorab kurz einige Begrifflichkeiten zu klären. Abbildung 5 zeigt auf einen Blick, in welche verschiedenen Anzeigebereiche das Fenster des Browsers aufgeteilt ist.

- Im Inhaltsbereich werden die Webseiten dargestellt.
- Die Bedienelemente und die Adresszeile dienen in erster Linie dazu, Webseiten aufzurufen, zu aktualisieren und zwischen einzelnen Seiten hin und her zu springen.
- Die Komfortfunktion Lesezeichen bietet Ihnen die Möglichkeit, einen direkten Link zu einer Webseite anzulegen, um so mit nur einem Klick – ohne die Internetadresse per

Hand eingeben zu müssen – zu der gespeicherten Internetadresse zu kommen.

- Die Statusleiste befindet sich im Allgemeinen unter dem Anzeigebereich. Sie kann über das Menü «Ansicht» aufgerufen werden und zeigt zusätzliche wichtige Informationen an.

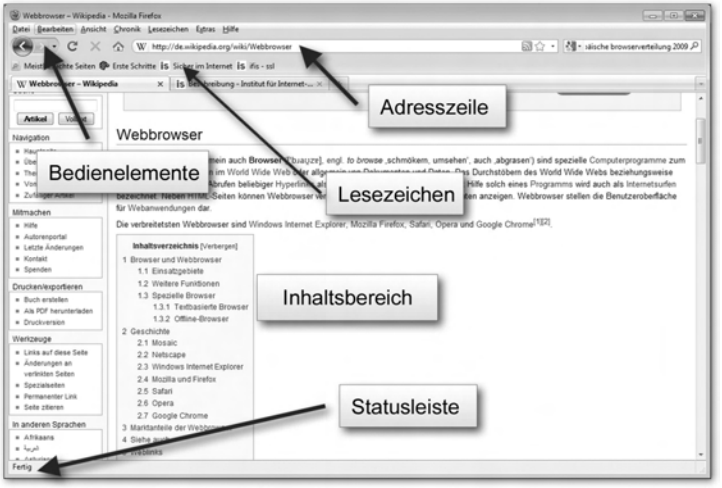

Abbildung 5: Die Anzeigebereiche eines Browsers

Die Funktion «Statusleiste» sollten Sie unbedingt nutzen, denn damit können Sie sich unter anderem die Zieladresse eines Links ansehen (Aufbau von Links beziehungsweise einer URL, siehe Softlink 220). Diese wird automatisch angezeigt, wenn Sie den Mauszeiger auf den fraglichen Link bewegen, ohne ihn anzuklicken (siehe Abbildung 6). Steht hier statt der zu erwartenden eine völlig andere Webadresse, ist Vorsicht geboten, da der Link eventuell manipuliert wurde, um einen Angriff vorzubereiten. Im Zweifelsfall ist es daher immer ratsam, den fraglichen Link nicht zu benutzen.

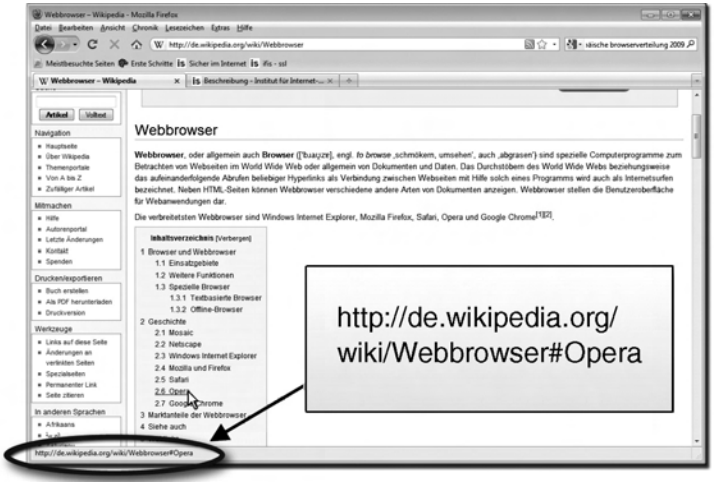

Abbildung 6: Die Statusleiste zeigt die Webadresse an, zu welcher der Link führt. Sie scheint in diesem Fall korrekt zu sein.

TIPP: Statusleiste

Gewöhnen Sie sich an, eine Webadresse immer erst in der Statuszeile genau zu betrachten, ehe Sie sie anklicken. Zeigt die Statuszeile nicht das gewünschte Ziel, meiden Sie den Link. So lässt sich beim täglichen Surfen so mancher Angriff von vornherein vermeiden.

Angriffsfläche Browser – von aktiven Inhalten und anderen Gefahren

Als Tor zur digitalen Welt ist der Browser auch ganz dicht an den Gefahren des Internets dran. Für Angreifer ist er Angriffsziel Nummer eins. Und je vielseitiger die Funktionen und Möglichkeiten des Browsers werden, umso mehr Angriffsmöglichkeiten werden auch eröffnet. Aber Sie können sich gegen viele dieser Angriffe schützen, indem Sie sich richtig verhalten. Wie das geht, zeigen die folgenden Abschnitte.

Risikofaktor aktive Inhalte

Webseiten werden mit der Auszeichnungssprache HTML (HyperText Markup Language) erstellt. Diese lässt jedoch zunächst keine Interaktion beziehungsweise Animation zu. Das ist nur mit zusätzlichen sogenannten aktiven Inhalten möglich. Dabei handelt es sich um kleine «Softwareprogramme», die mithilfe von Werkzeugen wie JavaScript beziehungsweise JScript, Flash, ActiveX-Controls, VBScript, Java-Applets sowie AJAX erstellt und in den HTML-Code eingebettet werden. Aktive Inhalte machen eine Webseite dynamisch (zum Beispiel durch Spiele, Filme und animierte Sequenzen) und ermöglichen eine direkte Interaktion zwischen den Anwendungen auf Ihrem Computer und dem Webserver, um beispielsweise auf eine Datenbank zugreifen zu können. Sie werden automatisch aktiv, sobald die entsprechende Webseite angesurft wird.

Aktive Inhalte bieten also viele Vorteile, stellen aber auch ein großes Sicherheitsrisiko dar. Denn heutzutage wird Malware zum größten Teil über Webseiten mit aktiven Inhalten verbreitet. Dieser Angriff wird Drive-by-Download genannt. Dabei wird eine Schwachstelle des Browsers oder eines Browser-Plugins ausgenutzt, um beim Besuch einer infizierten Webseite im Hintergrund eine Malware auf den Computer herunterzuladen. Allein der Besuch einer solchen Webseite kann ausreichen, um Ihren Computer – ohne dass Sie es merken – zu infizieren.

Aktuelle Browser weisen deshalb mithilfe verschiedener Anzeigen den Nutzer darauf hin, dass aktive Inhalte in einer Webseite enthalten sind und fragen, ob diese zugelassen werden sollen. Erste Reaktion: «Na klar, sonst kann ich ja nicht alle Funktionen der Webseite nutzen!» Doch Vorsicht: Über die vielen flexiblen Möglichkeiten der aktiven Inhalte ist es ver-

gleichsweise einfach, Schwachstellen im Computer für einen Angriff zu nutzen. Sie sollten also deren Einsatz wann immer möglich vermeiden. Allerdings sind aktuelle Webseiten im Web 2.0 fast immer mit aktiven Inhalten ausgestattet – eine Videoplattform ohne Videos ergibt schließlich nicht viel Sinn. Hier ist wiederum Ihr gesunder Menschenverstand gefragt und die Fähigkeit, die Vertrauenswürdigkeit einer Webseite einzuschätzen. Die folgenden Punkte helfen Ihnen dabei:

- Sind der Aufbau und die Inhalte der Webseite für Sie klar nachvollziehbar und machen sie einen vertrauenswürdigen Eindruck?
- Haben Sie mit der Webseite bereits in der Vergangenheit gute Erfahrungen gemacht?
- Ist Ihnen die Webseite von einer vertrauenswürdigen Person empfohlen worden?
- Werden Sie aufgefordert Daten einzugeben, die aus Ihrer Sicht nichts mit Ihrem eigentlichen Anliegen zu tun haben?
- Werden Eingaben verschlüsselt übertragen (siehe Seite 36 ff.)?
- Ist Werbung – sofern vorhanden – klar als solche zu erkennen?
- Steht im Impressum genau, wer für die Webseiten verantwortlich ist? Sind eine Adresse und eine Telefonnummer angegeben?

Um den Anwender in eine Falle zu locken, lassen sich die Angreifer durchaus etwas einfallen. Die Webseite in Abbildung 7 ist von einem Angreifer verändert worden. Der Link in dem kleinen Kasten führt in diesem Fall nicht zu ebay, sondern zu einer gefälschten ebay-Seite, um an die Zugangsdaten des Benutzers zu kommen.

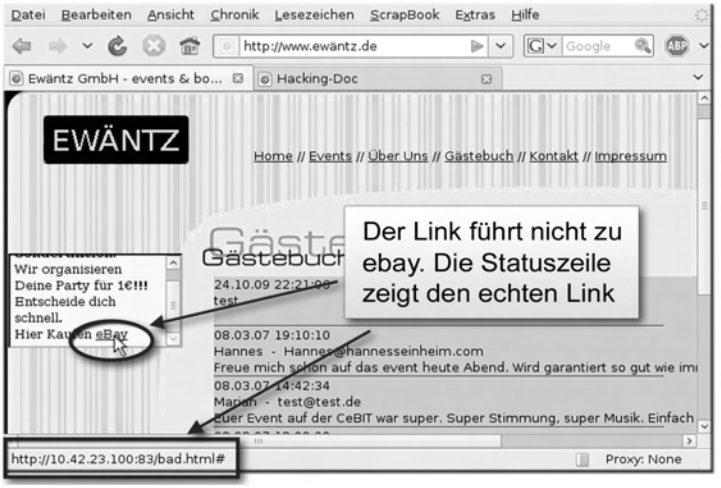

Abbildung 7: Webseite, die einem Cross-Site-Scripting-Angriff zum Opfer gefallen ist

Der in diesem Beispiel vollzogene Angriff nennt sich Cross Site Scripting (XSS). Er nutzt sicherheitstechnisch schwach programmierte Webseiten mit aktiven Inhalten aus – hier eine Webseite mit einem Eingabefeld (Gästebuch), die sicherheitstechnisch nicht sauber programmiert wurde. Gegen den Fehler selbst können Sie als Internetnutzer nichts tun. Aber Sie können durch Achtsamkeit die Manipulation erkennen (wäre der Link echt, würde in der Statuszeile die Webadresse www.ebay.de stehen) und sich dementsprechend schützen (siehe Seite 29f.).

Das in dem Beispiel versuchte «Phishen» (Phishing = Password + Fishing) der Zugangsdaten ist eine gängige Art des Angriffs im Internet. Ein Klick auf den Link im markierten Kasten würde den Nutzer auf eine Webseite führen, die nur so aussieht wie die von ebay. Wenn sich der Nutzer dann auf der falschen ebay-Seite einloggt, gibt er dem Angreifer seine Iden-

tität und das Passwort preis. Dieser Angriff wird «Phishing» genannt, weil nach dem Passwort des Nutzers gefischt wird (siehe Abschnitt «Onlinebanking»).

Noch gefährlicher ist es, wenn Sie auf eine Webseite gelangen, die versucht, Schadsoftware auf Ihren Computer zu spielen. Damit kann der Computer vollständig übernommen und alle Dateien, inklusive Passwörter und Bankdaten, können ausgespäht werden. Diese Angriffe passieren im Internet täglich. Deshalb ist Wachsamkeit durch nichts zu ersetzen!

TIPP: Sicheres Surfen

- Wenn Sie auf eine Ihnen bekannte Webseite surfen und diese sich plötzlich verändert präsentiert, beispielsweise einen neuen Kasten enthält, wie die Webseite in Abbildung 7, dann sollten bei Ihnen die Alarmglocken läuten.
- Ebenso misstrauisch sollten Sie sein, wenn eine Ihnen unbekannte Webseite aktive Inhalte nutzen will.
- Lassen Sie aktive Inhalte nur auf vertrauenswürdigen Seiten zu, und auch nur dann, wenn sie unbedingt notwendig sind (zum Beispiel um einen Film abzuspielen).
- Seien Sie besonders wachsam, wenn Sie auf Webseiten sicherheitskritische Daten wie Passwörter, Bankdaten, Adressen, Handy-Nummer usw. eingeben.

Risikofaktor sorgloser Umgang mit persönlichen Daten

Ein großes Problem stellt der sorglose Umgang vieler Nutzer mit ihren privaten Daten dar. Dabei ist genau das Gegenteil das Gebot der Stunde: Geben Sie so wenig wie möglich von sich im Internet preis. Und wenn Sie Informationen weitergeben, dann nur solche, die für den entsprechenden Vorgang wirklich notwendig sind – ein Chatroom benötigt keine

On wehrmaß-
nah ... inhaltlicher Sprung ...

Onlinebanking-Verfahren – Welches ist wie sicher?

Zur Durchführung und zum Schutz der Transaktionen gibt es verschiedene Verfahren, die auch ein unterschiedlich hohes Maß an Sicherheit bieten. Die meisten Onlinebanking-Verfahren, mit Ausnahme des FinTS/HBCI-Verfahrens, basieren auf der Kombination aus PIN und TAN. Diese werden im Folgenden kurz erläutert und im Hinblick auf die Sicherheit bewertet. Dabei ist zu beachten, dass alte und unsichere Verfahren mit der Einführung neuer Verfahren abgeschaltet werden müssen, um mögliche Hintertüren zu schließen. Bei einem kürzlich aufgetretenen Betrugsfall war zwar ein neues iTAN-Verfahren eingeführt worden, aber das alte TAN-Verfahren wurde nicht deaktiviert. Somit konnten durch Phishing gewonnene iTANs auch weiterhin uneingeschränkt als TANs genutzt werden. Zuständig dafür ist die Bank. Fragen Sie dort explizit nach und probieren Sie Ihr altes Verfahren nach der «offiziellen» Umstellung noch einmal aus, um sicherzugehen, dass es deaktiviert ist.

TAN

Das einfache TAN-Verfahren basiert auf einer Liste von einmalig zu verwendenden TANs. TANs sind numerische Einmalpasswörter, die meist eine Länge von sechs Stellen haben und dem Nutzer in Form einer Liste von seiner Bank ausgehändigt werden. Dieser wiederum verwendet sie, um seine Transaktionen, zum Beispiel eine Überweisung, zu bestätigen, nachdem er sich per PIN in sein Bankkonto eingeloggt

hat. Erst durch die Eingabe einer korrekten TAN, die der Bank ebenfalls bekannt ist, wird die gewünschte Transaktion tatsächlich ausgeführt. Dabei kann jede TAN auf der Liste nur einmal verwendet werden, die Reihenfolge ist egal. Die TAN-Nummern sind also nicht an bestimmte Transaktionen gebunden. Die TAN wird, bildlich gesprochen, nach ihrer Verwendung aufseiten der Bank und beim Nutzer von der Liste gestrichen.

Dieses Verfahren wird heute als unsicher eingestuft, da bei einem Phishing-Angriff mehrere TANs ausgespäht werden können, die der Angreifer dann flexibel für seine Zwecke verwenden kann.

iTAN

Bei der iTAN (der indizierten TAN) muss eine ganz bestimmte TAN benutzt werden, um eine Transaktion zu legitimieren. Die TANs sind zu diesem Zweck auf der TAN-Liste entsprechend nummeriert. Das erschwert dem Angreifer seine Arbeit, da er bei seinem Phishing-Angriff genau die richtige TAN «erbeuten» muss. Er ist somit gezwungen, entweder in Echtzeit zu arbeiten oder eine ganze TAN-Liste zu ergaunern, wodurch sich der Sicherheitslevel beim iTan-Verfahren ein wenig erhöht. Das Verfahren kann aber auch nicht mehr empfohlen werden.

mTAN

mTAN (mobile TAN, auch SMSTAN genannt) verbessert die Sicherheit bereits erheblich, da neben der Bindung an eine bestimmte TAN auch noch ein Medienbruch erfolgt. Das bedeutet, dass die TAN bei der Initiierung einer Transaktion per SMS von der Bank an ein bestimmtes Handy des Onlineban-

king-Nutzers gesendet wird. In der SMS befinden sich neben der TAN auch Informationen zu der gewünschten Transaktion, zum Beispiel der Betrag und die Zielkontonummer, um auszuschließen, dass ein Angreifer die Transaktion manipuliert hat (Filme zu TAN-Verfahren siehe Softlink 342). Aktuell ist mTAN eines der sichersten Onlinebanking-Verfahren, da es für einen Angreifer sehr schwer ist, die Computerkommunikation und parallel die Handykommunikation zu überwachen. Allerdings fallen dabei meist zusätzliche Kosten für die SMS an (teilweise werden diese jedoch auch von den Banken übernommen). Aber es ist eine lohnende Investition, die einen angemessenen Sicherheitsstandard garantiert.

Sm@rtTAN, Sm@rtTAN Plus und ChipTAN

Das Sm@rtTAN-Verfahren stellt eine weitere Alternative zur TAN-Liste dar. Die Basis von Sm@rtTAN ist ein kleines zusätzliches Gerät mit Display, auch Token genannt, in das der Nutzer seine ec-Karte einführen kann. Der Token errechnet dann auf Knopfdruck die TAN, die für die gewünschte Transaktion verwendet werden soll. Dieses Verfahren ähnelt sicherheitstechnisch dem iTAN-Verfahren, da der Vorgang keine Man-in-the-middle-Angriffe verhindern kann, also Angriffe, bei denen sich der Angreifer in die Kommunikation zwischen Absender und Empfänger einklinkt und die Kommunikation zu seinen Gunsten verändert. Das bedeutet, dass der Nutzer nicht nachvollziehen kann, ob beim Transaktionsvorgang direkt mit der Bank kommuniziert wird oder ob sich ein Angreifer dazwischengeschaltet hat.

Daher wurde das Sm@rtTAN-Plus-Verfahren eingeführt, je nach Kreditinstitut auch ChipTAN genannt. Der hierfür benötigte Token besitzt zusätzlich eine eigene Tastatur. Startet

der Nutzer eine Transaktion, erhält er von der Bank zwei Nummern als Antwort angezeigt. Eine beinhaltet Teile der Kontonummer des Empfängers, die zweite ist ein Bankcode. Die Kontonummernteile werden mit der Transaktion verglichen. Dann gibt der Nutzer beide Nummern in den Token ein, der daraus – zusammen mit den Informationen von der eingesteckten ec-Karte – eine TAN errechnet (Filme zum TAN-Verfahren siehe Softlink 334).

Das Sm@rtTAN- beziehungsweise ChipTAN-Verfahren gibt es ganz aktuell auch in einer optischen Lösung. Dazu erhalten die TAN-Generatoren (Token) eine optische Schnittstelle. Nach Eingabe der Transaktionsdaten erscheint eine Animation. Der TAN-Generator wird dann vor den Monitor gehalten und liest den Code aus. Aus dem optischen Code, den Transaktionsdaten und den Daten der Karte werden die TANs generiert und auf der Anzeige des Tokens angezeigt. Dieses Onlinebanking-Verfahren ist vom Sicherheitslevel her ebenfalls gut geeignet. Achten Sie darauf, dass Sie alle Eingaben genau überprüfen. Allerdings fallen auch hier eventuell zusätzliche Kosten für den Token an.

HBCI/FinTS

Mit HBCI (Homebanking Computer Interface) wurde schon vor vielen Jahren ein solider offener Homebanking-Standard in Deutschland eingeführt, der in einer neuen Version inzwischen als FinTS (Financial Transaction Services) bekannt ist. Er sieht die Verwendung einer SmartCard vor, die mit einer elektronischen Signatur ausgestattet ist. Der sogenannte Klasse-3-Kartenleser zeigt in diesem Fall die Überweisungsdaten auf seinem Display an, und der Nutzer bestätigt die Transaktion mit seiner PIN, die direkt in den

Kartenleser eingegeben wird und nicht auf dem Computer. Das bedeutet, dass Computer und PIN völlig unabhängig voneinander sind, wodurch einer Malware auf dem Computer die Angriffsfläche entzogen wird. Der Einsatz von Kartenlesern der Klasse 2 und 1 wird nicht empfohlen, denn die Integrität und die Verbindlichkeit beim Transaktionsvorgang sind nur mit dem Klasse-3-Kartenleser gegeben. Dieser Kartenleser garantiert, dass die Tastatur und das Display des Kartenlesers während einer PIN-Eingabe nur unter der Kontrolle des Kartenlesers stehen und nicht vom Computer beeinflusst werden können.

Das HBCI/FinTS-Verfahren ist in Bezug auf das Sicherheitsniveau mit dem mTAN-Verfahren vergleichbar. Leider ist es jedoch kaum verbreitet, da sowohl die Kartenleser als auch die entsprechende Onlinebanking-Software deutlich teurer sind als andere, unsichere Verfahren.

TIPP: Onlinebanking-Verfahren

- Nutzen Sie für das Onlinebanking möglichst eines der folgenden Verfahren: mTAN, Sm@rtTAN Plus oder FinTS.
- Nutzen Sie neue Verfahren, wenn diese ein höheres Sicherheitsniveau bieten – auch wenn sie möglicherweise mit Zusatzkosten verbunden sind. Die Investition lohnt sich in jedem Fall!
- All diese Verfahren bieten nur dann optimalen Schutz, wenn Sie sie richtig anwenden. Achten Sie also beispielsweise darauf, dass Sie Ihr Handy, in dem Ihre Zugangsdaten gespeichert sind, nicht aus der Hand geben, wenn Sie mTan verwenden.

Onlinebanking mit Banking-Software

Alternativ zum browserbasierten Onlinebanking können Sie auch eine Banking-Software verwenden. Diese Anwendun-

Das Einmaleins für jeden Internetnutzer

Wie kann ich meinen Computer vor Viren, Würmern und Trojanischen Pferden schützen? Wann darf ich meine Kreditkarten-Daten im Internet angeben? Woran erkenne ich vertrauenswürdige Onlineshops und Bankadressen? Was muss ich beim Einrichten eines WLAN beachten? Welche Rechte und Pflichten gibt es im Internet?

Norbert Pohlmann und Markus Linnemann ersetzen den Fachmann in jedem Computerhaushalt. Einfach und verständlich zeigen sie, wie Sie den Basisschutz für Ihren Computer optimieren und den Zugang zum Internet sicher machen. Auch ohne vorher ein Informatikstudium absolviert zu haben.

Mit vielen Tipps und Tricks für schnelle Leser und einem laufend aktualisierten Online-Service mit neusten Informationen (www.sicher-im-internet.de).

Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Direktor des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de).

Markus Linnemann ist Diplom-Informatiker und Geschäftsführer des Instituts für Internet-Sicherheit. Seit der Eröffnung des Instituts 2005 hat sich das Team zu einer der bedeutendsten Kapazitäten für Internet-Sicherheit im deutschsprachigen Raum entwickelt

ISBN 978-3-280-05375-1

orell füssli
www.ofv.ch