Beck kompakt

Sicherheit beim Surfen und Kommunizieren im Internet

Was Sie beachten sollten

von
Prof. Dr. Rolf Schwartmann, Dr. Tobias Oliver Keber, Prof. Dr. Patrick Godefroid

1. Auflage

Verlag C.H. Beck München 2014

Das mTAN-Verfahren

Das heute bei vielen Banken gängige mTAN-Verfahren ist keine bloße Weiterentwicklung der vorgenannten Verfahren. Es unterscheidet sich dadurch, dass keine Papierlisten mehr verschickt und geheim gehalten werden müssen. Hierfür kommt ein neuer Übertragungsweg ins Spiel: Der Mobilfunk. Beim mTAN-Verfahren werden die Transaktionsnummern erst in dem Moment erzeugt, in dem der Kunde eine Transaktion im Online-Banking eingibt. Die mTAN wird dann **per SMS auf das Handy** des Bankkunden übermittelt. Dazu ist es notwendig, dass der Bankkunde im Vorfeld seine Mobiltelefonnummer bei der Bank hinterlegt und diese verifiziert hat. Der Bankkunde liest die mTAN von seinem Handydisplay ab und gibt sie in das entsprechende Feld im Online-Banking-System ein, um die Transaktion freizugeben.

Das mTAN-Verfahren weist gegenüber den anderen Verfahren ein **erhöhtes Sicherheitsniveau** auf. Da der Kunde nicht mehr mit TAN-Listen hantieren muss, können diese auch nicht mehr verloren gehen oder gestohlen werden. Zudem ist jede **mTAN nur für die Transaktion gültig, für die sie angefordert wurde**.

Was vorher für die TAN-Listen galt, gilt nun allerdings für das Handy des Kunden: Er muss sicherstellen, dass sein Mobiltelefon (genauer: seine SIM-Karte) nicht in die Hände von Angreifern fällt; ansonsten könnten diese Transaktionen im Namen des Kunden ausführen.

Als Bankkunde sollte man aus der Sicherheitsperspektive **mindestens das mTAN-Verfahren einsetzen**. iTAN und klassisches PIN/TAN sollten nicht mehr verwendet werden.

TAN-Generatoren

TAN-Generatoren bieten ebenfalls ein gutes Maß an Sicherheit für die Freigabe von Transaktionen im Online-Banking und werden bereits von vielen Banken und Sparkassen angeboten. Es handelt sich dabei um spezielle Geräte, die ähnlich aussehen wie Taschenrechner. Sie dienen dazu, **Transaktionsnummern zu erzeugen**, wobei je nach Bank unterschiedliche Verfahren eingesetzt werden. Wie beim mTAN-Verfahren, bieten auch TAN-Generatoren den Vorteil getrennter Übertragungswege für Transaktion und Berechtigungsnummer und somit eine **erhöhte Sicherheit.**

HBCI

Das **Home-Banking-Computer-Interface-Verfahren** ist ein einheitlicher Online-Banking-Standard, der von der deutschen Kreditwirtschaft entwickelt wurde. Innerhalb des Standards können unterschiedliche Legitimationsverfahren verwendet werden. Als besonders sicher gilt hierbei das Legitimationsverfahren **per Chipkarte und Chipkartenleser**. Um HBCI als Privatanwender nutzen zu können, benötigt man, sofern man das genannte Legitimationsverfahren einsetzen möchte, also einen speziellen Chipkartenleser. Zu

beachten ist dabei jedoch, dass nicht alle Banken HBCI für Privatanwender anbieten.

Phishing

Beispiel:

„Ihr Konto wird in Kürze gesperrt": So lautet die Betreffzeile der E-Mail, die Herr Meier heute von seiner Bank bekommen hat. Die Mail sieht täuschend echt aus. Sie ist in den Farben der Bank gehalten und trägt sogar ihr Logo. Im Text heißt es, dass sein Konto aufgrund ungewöhnlicher Kontobewegungen in Kürze gesperrt werde. Wenn er das nicht möchte, solle er sich über einen angegebenen Link bei seiner Bank melden. Herr Meier klickt natürlich sogleich auf den Link und landet auf der Website seiner Bank. Dort wird er gebeten, zur Anmeldung seine Online-Banking-Nummer, seine PIN und – aufgrund der hohen Sicherheitsanforderungen – zehn TAN-Nummern aus seiner TAN-Liste einzugeben. Das erledigt Herr Meier sofort und ist glücklich, die drohende Kontosperrung abgewendet zu haben. Einige Tage später muss er allerdings feststellen, dass von seinem Konto insgesamt 9.000 EUR auf ein Konto im Ausland transferiert wurden. Was ist passiert?

Herr Meier ist Opfer einer **Phishing-Attacke** geworden. Die E-Mail kam nur scheinbar von seiner Bank. In Wahrheit handelt es sich bei den Absendern um Betrüger, deren Absicht es war, an seine **Kontozugangsdaten und TAN-Nummern** zu gelangen, sie also „abzufischen" (engl. = fishing). Dazu versenden Angreifer massenhaft E-Mails an

Internetnutzer und gestalten diese Mails so, dass sie den Anschein erwecken, **als ob sie von einer Bank oder einer Sparkasse versendet worden wären**. Sie nutzen die bekannten Farben der Bank, gestalten die E-Mail im gleichen Layout und verwenden ähnliche Bildelemente sowie das Logo der Bank. Die Qualität dieser Fälschungen differiert, wird aber stetig perfektioniert. Neueste Phishing-Mails sind von echten E-Mails optisch kaum noch zu unterscheiden.

Gefälschte Mail, gefälschte Website

Der Text und auch die Betreffzeile der Phishing-Mails sind dabei stets so formuliert, dass sie den Empfänger unter möglichst starken Zeitdruck setzen und ihm mit ernsten Konsequenzen drohen. Mal ist, wie im obigen Beispiel, von der Sperrung des Kontos die Rede, in anderen Fällen von der Sperrung der Kreditkarte. Manchmal wird der Empfänger in Phishing-Mails auch über eine vermeintlich hohe Abbuchung von seinem Konto informiert, die es schnell zu widerrufen gelte.

Der Handlungsdruck für Herrn Meier war also groß, und so klickte er auf den Link, der in der Phishing-Mail enthalten ist, um das vermeintlich drohende Unheil abzuwenden. Der zentrale Trick beim Phishing ist nun, dass die Links in den Mails ebenfalls gefälscht sind. Opfer wie Herr Meier gelangen über den Link keinesfalls auf die Webseite der Bank, sondern auf eine **nachgebildete Website**, die von den Betrügern betrieben wird. Herr Meier merkt das nicht, denn die Website entspricht genau wie die Phishing-Mail hinsichtlich ihres Erscheinungsbildes der Website seiner Bank. Er kommt gar nicht auf die Idee, dass er gerade Opfer eines

Betrugs wird, sondern gibt tatsächlich sowohl seine Online-Banking-Nummer als auch seine PIN sowie zehn Transaktionsnummern von seiner TAN-Liste in das auf der Website angezeigte Formular ein.

Das Ziel: Zugangsdaten „abfischen“

Er denkt, dass nun alles erledigt sei, dass sein Konto nicht gesperrt wird und dass er sich beruhigt zurücklehnen könne. In Wirklichkeit bestand natürlich nie die Gefahr einer Kontosperrung, denn das hatten sich die Betrüger nur als Köder ausgedacht. Dadurch, dass Herr Meier auf den Link in der Phishing-Mail geklickt hat und dass er seine **Kontodaten inklusive der Transaktionsnummern in die gefälschte Website eingegeben** hat, hat er es den Betrügern überhaupt erst ermöglicht, ihm einen finanziellen Schaden zuzufügen. Sie haben die über die Website erbeuteten Kontozugangsdaten umgehend dazu genutzt, sich **in seinem Namen auf der echten Website der Bank einzuloggen**, und sie haben seine Transaktionsnummern dazu verwendet, den vierstelligen Geldbetrag auf ihr eigenes Konto zu überweisen.

Phishing ist kein Computervirus

Der Fall zeigt, dass es sich beim Phishing nicht um ein Schadprogramm (wie beispielsweise einen Computervirus) handelt. Es ist keine technische Schwachstelle, die hier ausgenutzt wird. Stattdessen wird der Computernutzer gezielt getäuscht und dazu verleitet, Handlungen zu vollziehen, die ihm letztlich selbst schaden. Aus diesem Grund sind

Antivirenprogramme oder Firewalls auch nicht in der Lage, Phishing-Angriffe auf einer technischen Ebene wirksam zu erkennen und zu unterbinden. Möchte man verhindern, dass man Opfer einer Phishing-Attacke wird, muss man als Computernutzer Vorsicht walten lassen.

Wie kann man sich schützen?

Wie sollte man also reagieren, wenn man eine E-Mail bekommt, bei der es sich um eine Phishing-Mail handeln könnte?

- Schauen Sie sich die Mail zunächst genau an. Werden Sie nicht mit ihrem **korrekten Namen angeredet**? Finden sich viele **Rechtschreibfehler** oder grammatikalisch merkwürdige Formulierungen im Text der Mail? Beides sind erste Hinweise darauf, dass es sich bei der Mail um eine Phishing Mail handeln könnte.
- Keine Bank versendet E-Mails an ihre Kunden, in denen diese um die Herausgabe ihrer Zugangsdaten oder Transaktionsnummern gebeten werden. Wenn Sie auf einer Webseite Zugangsdaten eingeben, **stellen sie zuvor sicher, dass Sie sich wirklich auf der Website der Bank befinden**. Am sichersten erreichen Sie das, indem sie die Internetadresse der Bank **eigenhändig mit der Tastatur** in das Adressfeld Ihres Browsers eingeben (siehe hierzu auch den Abschnitt „Online-Banking“).
- **Klicken Sie auf keinen Fall auf Links, die in E-Mails enthalten sind**. Da man Phishing-Mails kaum von echten E-Mails unterscheiden kann, muss dieser Hinweis heute generell gelten. Im Zweifel ist es immer sicherer, sich tele-

fonisch an den vermeintlichen Absender zu wenden und zu klären, ob es sich bei der Mail um einen Betrugsversuch handelt.

- Bei Phishing-Angriffen geht es den Betrügern meistens darum, Zugangsdaten für das Online-Banking zu erbeuten. Neben dem Online-Banking sind jedoch auch andere Zugangsdaten für Phishing-Betrüger interessant. Überprüfen Sie also auch bei Mails, die vermeintlich von **Online-Shops** oder **Online-Auktionshäusern** an Sie geschickt werden, deren Echtheit, und handeln Sie genauso vorsichtig.

Die Cloud

> *Beispiel:*
>
> *Als Frau Müller ihr neues Smartphone in Betrieb genommen und erste Fotos damit geschossen hatte, wurde ihr folgende Meldung angezeigt: „Automatische Foto-Uploads aktivieren?". „Warum nicht?", dachte Frau Müller, „ist doch schön wenn die Fotos sicher auf dem Server liegen, falls das Smartphone mal kaputt geht" und klickte auf OK. Seitdem wird jedes Foto, das sie aufnimmt, automatisch auf die Server eines amerikanischen Cloud-Speicherdienstes übertragen. Obwohl das sehr nützlich ist, zweifelt Frau Müller manchmal. Sind ihre Daten dort wirklich sicher? Wer kann sich ihre Privatfotos dort alles ansehen?*

Die **Cloud** – oder genauer das **Cloud-Computing** – ist ein relativ unscharfer Oberbegriff für die Auslagerung von IT-Dienstleistungen in das Internet. Computerprogramme, die

man als Cloud-Computing nutzt, sind **nicht auf dem eigenen Computer** installiert, sondern auf Internet-Servern, die der jeweilige Cloud-Computing-Anbieter betreibt. Das Konzept, Computerprogramme über das Internet zu nutzen, ist keineswegs neu. Bereits seit den Anfängen des World Wide Web zu Beginn der 1990er-Jahre gab es E-Mail-Anbieter, bei denen Nutzer E-Mails im Browser lesen und verfassen konnten. Dieses auch als „Webmailer" bezeichnete Konzept ist bis heute bei vielen kostenlosen E-Mail-Anbietern verbreitet und bei Nutzern beliebt. Auch Internetsuchmaschinen sind Cloud-Anwendungen, denn als Nutzer einer solchen Suchmaschine nutzt man das Suchprogramm ebenfalls per Browser auf dem Server des Anbieters.

Alter Wein in neuen Schläuchen?

Obwohl also bereits bewährt, hat das Cloud-Computing-Konzept erst in den letzten Jahren, vor allem durch technische Entwicklungen in den Bereichen der Rechnervirtualisierung und durch die gestiegene Verbreitung schneller Internetverbindungen, an Relevanz gewonnen. Breit diskutiert werden seine Vorteile besonders in der Unternehmens-IT, weil sich damit **hohe Kosteneinsparungen** realisieren lassen. In vielen Fällen lagern Unternehmen große Teile ihrer Informationstechnologie an Cloud-Computing-Anbieter aus und sparen auf diese Weise Kapazitäten im eigenen Rechenzentrum ein. Im Extremfall betreiben selbst große Unternehmen heutzutage gar **keine eigenen Rechenzentren** mehr, sondern mieten sämtliche benötigte Hard- und Software über Cloud-Dienstleister an.