Vorsicht Falle – Betrug im Internet

Autor: Philipp Otto

Wenn Menschen sich im Internet bewegen, dort einkaufen oder in Sozialen Netzwerken aktiv sind, hinterlassen sie dort personenbezogene private Daten. Eine komplette Sicherheit für all diese Daten gibt es nicht. Diese persönlichen Daten sind heiß begehrt: Neben kommerziellen Anbietern, die damit Marktforschung und Werbung betreiben, versuchen auch Betrüger an sie zu gelangen. Besonders begehrt sind dabei Kreditkarten- und Bankdaten sowie die Zugangscodes zu elektronischen Zahlungssystemen wie PayPal. Es gibt vielfältige Möglichkeiten, um illegal oder unter Ausnutzung der Gutgläubigkeit der Nutzer an sensible Daten zu gelangen. Dieser Text beleuchtet die wichtigsten Systeme zum gezielten digitalen Betrug, Möglichkeiten zur Prävention und die rechtliche Lage.

Es gibt viele verschiedene Formen, wie ein fremdgesteuerter Datenverlust bei Privatnutzern und Verbrauchern stattfinden kann. Unterschiedliche Angriffsmethoden tragen Namen wie Phishing, Spoofing oder Pharming. Beim Phishing versuchen die Angreifer private und sensible Daten von ihren Opfern zu erlangen. Das geschieht auf unterschiedlichste Weise, aber gemeinsam haben alle, dass die Angreifer vorgeben, ein seriöser Anbieter zu sein. Dazu wird dann Spoofing oder Pharming eingesetzt: Methoden, die verschleiern, welche „echte“ Identität sich hinter den Anfragen verbirgt. Es gibt dazu zahlreiche technische Möglichkeiten. Dazu kommen Spionageprogramme, Trojaner und Lockangebote, die nur dazu dienen, sensible Daten auszulesen. Das kann dazu führen, dass nicht nur die Bankdaten missbraucht werden, sondern dadurch, dass der eigene Computer mit sogenannter Malware, also Schadsoftware, infiziert wird, die gesamten Daten von der Festplatte verschwinden können.

Wichtig ist es, an dieser Stelle darauf hinzuweisen, dass das Glas immer halbvoll oder halbleer sein kann. Es geht nicht darum, Panik vor den „unkalkulierbaren Gefahren des Internets“ und möglicher kostenintensiver Fallen zu machen. Es geht vielmehr darum, das Bewusstsein zu schärfen und seine Kenntnisse über mögliche und aktuelle Gefahren zu erweitern.

Mit Phishern auf hoher See

Nahezu täglich finden sich in unseren E-Mail-Postfächern offiziell aussehende Nachrichten und Mitteilungen. Das reicht von der Bank, die uns auffordert, die Kundendaten samt Passwörtern neu einzugeben, da das System durch ein Software-Update überar-

beitet wurde, über das Online-Kaufhaus, das eine wichtige Änderung der Zugangsdaten durchführen will und deswegen das Login des Accounts benötigt, bis zu Aufforderungen, PINs (Kennwort) und TANs (Transaktionsnummer) für Online-Überweisungen zu schicken. Die E-Mail-Masche ist einer der großen Klassiker beim Online-Betrug. Von Banken, Webshops, Paketlieferdiensten oder Datingseiten – alle echten Angebote, die Leistungen oder Waren verkaufen und bei denen persönliche Daten hinterlegt sind, können Opfer eines solchen Betrugs werden, der dann scheinbar in ihrem Namen stattfindet.

Die E-Mails sehen teilweise sehr glaubwürdig aus. Es werden Referenz-Websites angegeben, deren Webadresse (URL) dem offiziellen Link der Bank täuschend ähnlich sieht. Oftmals werden auf den ersten Blick komplette Webseiten – beispielsweise einer Bank – nachgebaut, um dort die geheimen Daten der Nutzer abzugreifen. Banken und andere Einrichtungen unternehmen große Anstrengungen, um solche Seiten so schnell wie möglich wieder aus dem Netz zu bekommen. Doch auch wenn die gefälschten Seiten nur wenige Tage im Netz sind, können sie großen Schaden anrichten.

Besonders perfide wird es, wenn nach Eingabe der Daten eine Fehlermeldung auf dem Bildschirm erscheint, die suggeriert, die Datenübertragung habe gar nicht stattgefunden und den Nutzer dadurch in Sicherheit wiegt. Tatsächlich sind aber die Passwörter und persönlichen Daten schon längst übertragen.

Die „Anbieter“ solcher Betrugsversuche verfeinern ihre Technik immer weiter und passen sie auch auf die neuen Formen der Kommunikation an. So sind inzwischen auch Social-Media-Dienste wie Twitter oder Soziale Netzwerke wie Facebook davon betroffen. Auch hier gilt: Höchste Vorsicht beim Klicken auf Links und der folgenden Preisgabe von privaten Daten. Vor allem bei Lockangeboten und besonderen Schnäppchen sollte man widerstehen; diese können einen Phishing-Versuch verschleiern.

Checkliste: Wie erkenne ich eine Phishing-E-Mail?
Die folgenden Punkte können auf eine Phishing-E-Mail hinweisen:

- Es wird nach vertraulichen Daten wie Passwörtern, PINs, TANs und anderen relevanten Zugangsdaten im Zusammenhang mit der Angabe der eigenen Kontoverbindung gefragt.
- Die E-Mails sind oft im HTML-Code geschrieben. Das erkennt man daran, dass der Text der E-Mail mit verschiedenen Schriftarten und Schriftgrößen formatiert wird, Bilder (z.B. Logos) verwendet werden und/oder der Hintergrund eine andere Farbe hat.

- Der angegebene Link wirkt auf den ersten Blick echt, auf den zweiten erkennt man jedoch durch ungewöhnliche oder falsch geschriebene Bestandteile der URL, dass es sich um eine falsche Internet-Adresse handelt.
- Auf der Webseite, auf die man geführt wird, funktionieren die anderen angezeigten Menüpunkte nicht, beziehungsweise erzeugen Fehlermeldungen.
- In der E-Mail wie auch auf der Webseite finden sich Grammatik- und Rechtschreibfehler.
- Hinweise auf Änderung der Abrechnungssysteme oder Software-Updates bei Online-Kaufhäusern wie Amazon oder Ebay oder bei Banken sind ein deutliches Phishing-Warnsignal.
- Oftmals kommt die E-Mail auch von einer „komischen“ Absenderadresse oder wird in Kopie (E-Mail in Kopie (CC)) an zahlreiche weitere Empfänger geschickt.
- Die E-Mail ist nicht in der üblichen landestypischen Sprache der Bank geschrieben.
- Die E-Mail verwendet eine nicht-personalisierte Anrede wie “Sehr geehrte Damen und Herren”.
- Ein deutliches Warnsignal ist, wenn sich in der E-Mail ein Hinweis findet, dass die Daten binnen einer knappen Frist eingegeben werden müssen.
-

Tipp:
Finden sich im Anhang der verdächtigen E-Mail Dokumente oder andere Dateianhänge, so ist höchste Vorsicht angebracht. Diese sollte man nicht öffnen, da sich darin möglicherweise zusätzlich noch Schadprogramme befinden, die auf dem Rechner gespeicherte Passwörter auslesen.

Beispiel-Screenshot für eine Phishing-E-Mail, die vorgibt von der Deutschen Bank zu stammen. Quelle: E-Mailbox des Autors vom 25. Juli 2011

Von: Deutsche Bank <business@deutsche-bank.de>
Betreff: **Wichtige Mitteilung - Ihr Konto ist inaktiv**
Datum: 25. Juli 2011 01:36:15 MESZ
Antwort an: noreply@deutsche-bank.de

Leistung aus Leidenschaft.
Deutsche Bank

Sehr geehrter **Deutsche Bank** Kunde,

Als Teil unserer Sicherheitsmaßnahmen untersuchen wir die Aktivität in dem Deutsche Bank System regelmäßig.

Für die Sicherheit unserer Kunden hat Deutsche Bank eine neue Sicherheitsmaßnahme eingeführt:

- Periodisch muß jeder unserer Kunden beweisen daß sein TAN-Block sich noch in seinem Besitz befindet.

WICHTIG:

- Folgen Sie den von uns nächstens angegebenenen Schritten nur falls Sie den im Moment aktiven TAN-Block bei Ihnen haben.
- Diese Sicherheitsmaßnahme kann nur durch der von uns angegegebenen Webaddresse durchgeführt werden, versuchen Sie es bitte nicht direkt aus Ihrem Konto.

Folgen Sie den von uns vorgeschriebenen Schritten bitte genauestens.

Bitte loggen Sie sich so bald wie möglich in Ihr Konto ein, um die Sperrung Ihres TAN-Blocks zu vermeiden.
Einloggen

© 2011 Deutsche Bank AG

Was tun, wenn ich eine Phishing-E-Mail bekommen habe?

Wenn eine E-Mail als Phishing-Versuch erkannt wurde, kann man die E-Mail einfach löschen und sollte den Absender auf die Spamliste setzen, also blockieren. Ist diese besonders perfide, so empfiehlt es sich, das betroffene Unternehmen über die Existenz eines solchen Phishing-Versuchs zu informieren. Nahezu jede Bank hat ein Warnsystem eingerichtet, das es ermöglicht einen schnellen Kontakt zum Unternehmen zu bekommen. Hier bietet es sich an, die Kontaktdaten beim eigenen Kreditinstitut zu erfragen, bevor man als Opfer von Phishing zeitnah reagieren muss. Die Bank benötigt diese Informationen, um möglichst schnell an die verwendeten Server heranzukommen und diese ausschalten zu lassen. Da Phishing-E-Mails oft zu tausenden verschickt werden, ist eine schnelle Reaktion für die Unternehmen überaus wichtig.

Ist man schon in die Falle getappt und hat auf einer Phishing-Website seine Kontodaten oder vertrauliche Transaktionsdaten eingegeben, so sollte man schnell handeln. Denn ist der Verursacher der Phishing-Attacke erstmal im Besitz der Daten, so kann er

binnen Minuten hohe Summen transferieren oder Kaufvorgänge in Gang setzen. Um für diese Vorgänge Zeit zu gewinnen, werden normalerweise sehr zügig die ursprünglichen Zugangsdaten durch neue ersetzt, so dass der Nutzer nicht mehr an seinen eigenen Account kommt. Selbst versierte Internetnutzer können in diese Falle tappen.

Grundsätzlich gilt:

- Die Software – vor allem der Webbrowser (z.B. Firefox, Internet Explorer, Opera, Safari) und das Betriebssystem des Computers – sollten immer auf dem aktuellen Stand gehalten werden. Insbesondere sollte man angebotene Sicherheits-Updates regelmäßig einspielen, um Sicherheitslücken zu schließen.
- Hat man online Zugriff auf sein Konto, so sollte man regelmäßig beobachten, ob Abbuchungen stattgefunden haben, die man nicht zuordnen kann.
- Hat man solche Abbuchungen identifiziert, so sollte man im ersten Schritt bei seiner Bank anrufen und sein Konto vorläufig sperren lassen. Zudem empfiehlt sich ein Hinweis an den entsprechenden Anbieter (Ebay, Amazon, PayPal etc.), in dessen Gewand die Phishing-E-Mail sich gekleidet hat. Damit macht man den Anbieter auf die aktuelle Phishing-Attacke aufmerksam, so dass dieser Vorkehrungen treffen kann, um solche Attacken in Zukunft zu verhindern; im gleichen Zuge kann man einen gegebenenfalls auch dort eingerichteten Account als Vorsichtsmaßnahme vorläufig sperren lassen.
- Ist man schon zu spät dran und die Überweisung wurde ausgeführt, so sollte man mit Hilfe der Bank versuchen, die Überweisung sofort rückgängig zu machen. Das funktioniert allerdings nicht immer, da die Überweisungsziele fast immer im Ausland liegen und die Summen, vergleichbar mit einer Reihenschaltung, zur Verschleierung oftmals zügig an andere Konten weitergeleitet und dann abgehoben werden.

Wer haftet, wenn durch eine Phishing-Attacke Geld von meinem Konto abgebucht wurde?

Liegt eine Abbuchung vom eigenen Konto vor und eine Rückbuchung des Geldes ist gescheitert, dann stellt sich die Frage der Haftung. Die Banken verweisen in diesen Fällen sodann immer auf ihre Allgemeinen Geschäftsbedingungen (AGB). Beispielhaft lauten diese bei der Berliner Sparkasse in Nr. 20, Absatz 2 (www.berliner-sparkasse.de/pdf/vertragsbedingungen/AGB.pdf?IFLBSERVERID=IF@@051@@IF, PDF-Format, Stand: Juli 2012) „Mitwirkungs- und Sorgfaltspflichten des Kunden“ wie folgt: „Schäden und Nachteile aus einer schuldhaften Verletzung von Mitwirkungs- und sonstigen Sorgfaltspflichten gehen zu Lasten des Kunden. Bei schuldhafter Mitverursachung des Schadens durch die Landesbank richtet sich die Haftung nach den Grundsätzen des Mitverschuldens, Paragraf 254 Bürgerliches Gesetzbuch.“

Dahinter verbirgt sich im Grundsatz, dass derjenige, der auf eine Phishing-E-Mail reingefallen ist, auch für den Schaden verantwortlich ist, da er seine Sorgfaltspflicht bei der Eingabe seiner Zugangsdaten in das gefälschte Formular verletzt hat. Die Banken werden in fast allen Fällen darauf verweisen und eine eigene Haftung, also eine Rückerstattung des abgebuchten Geldes, verweigern.

In Ausnahmefällen wird aber eine prozentuale Mithaftung der Bank angenommen. Dies wird grundsätzlich durch den oben im Auszug der AGB zitierten Paragraf 254 BGB zum „Mitverschulden" geregelt. So hat das Berliner Kammergericht in einem Fall entschieden, dass die Bank 70 Prozent und die betroffene Kundin 30 Prozent des Schadens tragen muss. Die Verletzung der Sorgfaltspflicht auf Seiten der Kundin lag in der Eingabe der Transaktionsnummern in das gefälschte Formular; das Mitverschulden der Bank lag darin, dass diese ein veraltetes TAN-Verfahren anstatt des neueren iTan-Verfahrens eingesetzt hat. Der Schadenszeitpunkt in diesem Fall lag vor dem 01.11.2009. Danach ist der neue Paragraf 675v BGB in Kraft getreten.

Dieser regelt unter dem Titel: „Haftung des Zahlers bei missbräuchlicher Nutzung eines Zahlungsauthentifizierungsinstruments", dass der Bankkunde in Phishing-Fällen grundsätzlich nur für „grobe Fahrlässigkeit", nicht aber für einfaches fahrlässiges Verhalten haftet. Ob und in welcher Form die Haftungsverteilung berechnet werden kann, hängt aber naturgemäß stark vom Einzelfall ab.

Vorsicht vor lukrativen Job-Angeboten

Um eine reibungslose Transaktion des Geldes auf ausländische Konten vorzunehmen, bedienen sich die Verursacher von Phishing-Attacken oftmals sogenannter „Finanzkuriere". Diese werden von den Phishern durch Job-Angebote mit sehr guten Verdienstmöglichkeiten angeworben, für die man nichts weiter als ein inländisches Konto und einen Computer benötigt. Ihre einzige Aufgabe ist es, das auf dem inländischen Konto eingegangene Geld auf ein ausländisches Konto weiter zu schleusen. Dafür erhalten sie hohe Provisionszahlungen.

Für die angeworbenen Personen besteht ein hohes rechtliches Risiko wegen Geldwäsche (Paragraf 261 StGB) strafrechtlich belangt zu werden. Aktuell laufen in Deutschland etliche hundert Verfahren gegen Finanzkuriere. Es ist auch bereits zu einer Vielzahl von Verurteilungen mit Bewährungs- und Geldstrafen gekommen. Die Strafverfolgung konzentriert sich aktuell auf diese kleineren Fische, da an die Hintermänner und -frauen des Phishing-Betrugs kaum heranzukommen ist.

Datenklau und Identitätsdiebstahl

"Meine Daten gehören mir" – diesen Satz liest man immer wieder. So richtig diese Aussage als politische Forderung ist, so wenig hat sie mit der praktischen Realität der Nutzer zu tun. Eine Grundregel beim Umgang mit privaten Daten im Netz sollte sein, dass man sparsam, achtsam und vorsichtig mit seinen Daten, mit den online eingestellten Informationen und den eingesetzten Passwörtern umgeht. Man sollte sich aber auch bewusst sein, dass sich Datenklau prinzipiell nie verhindern lässt. Es gibt regelmäßig Berichte, dass großen Unternehmen millionenfach persönliche Daten seiner Kunden wie Zugangsdaten und Passwörter, aber auch komplette Verwaltungs- und Buchungsvorgänge, „abhanden" gekommen sind. Dies zeigt, dass selbst diese Unternehmen, obwohl sie sich grundsätzlich der besonderen Problematik bewusst sind, nicht davor gefeit sind, Opfer von Datenklau zu werden – und damit auch die Daten ihrer Kundinnen und Kunden. Somit kann es auch private Nutzer in einem kleineren Umfang, aber nicht weniger schmerzlich, zu jeder Zeit ebenfalls treffen.

Behandeln Sie Ihren Rechner wie einen Tresor

Überall da, wo man sich online bewegt, Nutzerprofile und Accounts anlegt und personalisierte Daten hinterlässt, besteht immer die Gefahr des Missbrauchs. Zur Vorbeugung hilft es, wenn man die folgenden grundsätzlichen Regeln beachtet:

- **Passwörter:** Für jedes Angebot sollten unterschiedliche Passwörter verwendet werden. Im Schadensfall wird der Schaden dann begrenzt, da der Eindringling nicht weitere genutzte Dienste missbrauchen kann. Auch sollte man seine Passwörter in regelmäßigen Abständen verändern. Passwörter sollten dabei aus einem Mix aus Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen bestehen, um die Sicherheit zu erhöhen.
- **E-Mail-Adressen:** Man sollte mit mehreren E-Mail-Adressen arbeiten. Die Erstadresse nutzt man für wichtige E-Mails, eine Zweitadresse nutzt man für Anmeldungen bei Online-Diensten wie Verkaufsplattformen, bei Facebook, Twitter, Google+ oder anderen Angeboten.
- **Sparsamkeit:** Im Internet sollte jeder Nutzer ein Schwabe sein. Weniger ist oft mehr, und wer seine Daten gar nicht erst mitteilt, bietet in der Folge potentiellen Angreifern weniger Missbrauchsmöglichkeiten.
- **Zusatzdaten:** „Reale" Daten wie Wohn- und Postanschrift oder die eigene Telefonnummer sollten nur angegeben werden, wenn diese für Online-Dienste zwingend erforderlich sind. In vielen Online-Formularen wird die Eingabe dieser Daten als optionale Möglichkeit geführt.
- **Verschlüsselung:** Es existieren viele verschiedene Möglichkeiten, wie man seine Daten bei der Übertragung im Internet verschlüsseln kann. Professionelle

Nutzer verwenden oft das Verschlüsselungssystem PGP. Den allermeisten Nutzern wird dies aber zu kompliziert sein. Da aber auch den Anbietern von Online-Diensten, wie Facebook oder Webmailern, diese Problematik bewusst ist, bieten sie ihren Nutzern oft die Möglichkeit, zumindest mit relativ einfach verschlüsselten Verbindungen zu arbeiten. Hier sollte man immer die maximale Verschlüsselungsmethode wählen. Dies minimiert die Gefahr, dass Daten zwischendurch abgefangen werden. Genauere Informationen zu Verschlüsselungen und Einstellungen erfährt man bei seinem Anbieter.

Sind Daten missbräuchlich verloren gegangen oder hat sich eine andere Person des eigenen Accounts bemächtigt, so ist auch hier eine schnelle Reaktion wichtig. Man sollte in Kooperation mit seinem Anbieter den entsprechenden Account zügig sperren lassen und die Zugangsdaten verändern.

Niemand ist davor geschützt, dass die eigenen persönlichen Daten und Zugänge missbräuchlich verwendet werden. Da sich die Muster der Betrugsmaschen aber ähneln, ist Vorsorge ein wichtiger Schritt. Es gilt: Ruhig und zügig handeln, um weiteren Missbrauch zu verhindern.

Weiterführende Informationen

- www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html
  Bundesamt für Sicherheit in der Informationstechnik (BSI): Thema Phishing
- www.verbraucher-sicher-online.de/thema/online-banking
  Verbraucher sicher online: Online-Banking und Phishing
- www.klicksafe.de/themen/einkaufen-im-netz/abzocke-im-internet/wie-verhalte-ich-mich-bei-phishing-attacken/
  Wie verhalte ich mich bei Phishing-Attacken?
- www.vz-nrw.de/UNIQ131177108726306/link827891A.html
  Verbraucherzentrale NRW: Phishing-Radar mit aktuellen Warnungen
- www.a-i3.org/content/view/931/202/
  Arbeitsgruppe Identitätsschutz im Internet e. V. (a-i3): Phishing und aktuelle Phishingmails
- www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing.html
  Polizeiliche Kriminalprävention der Länder und des Bundes: Phishing
- http://dejure.org/dienste/vernetzung/rechtsprechung?Text=26%20U%20159/09
  Juristischer Informationsdienst: Urteile zu Haftungsfragen bei Phishing

Aktualisierte Version 2012