Trojaner im Postfach

Betrüger legen Bankkunden mit täuschenden E-Mails herein oder prellen Gutgläubige, die vom großen Geld träumen. Ein Bochumer Verein berät die „Phishing“-Opfer.

GETTY IMAGES

Franz W. muss schnell noch etwas überweisen. Er ist auf Online-Banking umgestiegen, weil das praktisch ist. Egal ob morgens, abends oder am Wochenende – bloß ein paar Mausklicks, und schon hat der Empfänger sein Geld. Alles läuft wie immer. Der Augsburger gibt die Empfängerdaten ein, Name, Kontonummer, Bankleitzahl. Dann den Betrag. Noch mal die Eingaben überprüfen, jetzt alles bestätigen.

Aber was ist das? „Die eingegebene TAN ist ungültig.“ W. wird misstrauisch, ruft seine Bank an. Die versichert, dass die eingegebene TAN-Nummer weder falsch sei noch bereits benutzt wurde. Vertippt hat er sich auch nicht. Seltsam. Als er wenige Tage später die Überweisung mit derselben Nummer wiederholen will, tritt ihm der Schweiß auf die Stirn. Wieder eine Fehlermeldung: „TAN verbraucht.“

Diesmal leider zu Recht. Franz W. erfährt, dass mit Hilfe der zuvor ausgespähten TAN von seinem Konto 4125 Euro an einen ihm unbekannten Empfänger überwiesen worden sind. Der Bayer ist Opfer betrügerischer „Phisher“ geworden. Doch er hat Glück im Unglück – das Geld ist noch nicht gutgeschrieben. Seine Bank zieht die Überweisung zurück.

Ähnlich ist es auch Johann K. ergangen. Als der Versicherungsangestellte eines Tages seine Kontoauszüge überprüfte, stellte er fest, dass Ende vorigen Jahres 7140 Euro auf das Konto einer Ilona S. überwiesen worden waren. Das war schlechterdings unmöglich: K. kannte diese Frau überhaupt nicht. Der 49-Jährige grübelte und grübelte.

Dann fiel es ihm wie Schuppen von den Augen. Im Dezember hatte K. eine Mail erhalten, in der er aufgefordert worden war, anlässlich einer „Sicherheitsüberprüfung“ PIN- und TAN-Nummer einzugeben – eine Phishing-Mail. Der Begriff ist abgeleitet von den Wörtern „password“ und „fishing“. „Das sind leider keine Einzelfälle“, weiß Georg Borges von der „Arbeitsgruppe Identitätsschutz im Internet“ (a-i3). Borges: „Allein bei uns werden jede Woche bis zu 15 solcher Fälle bekannt.“

Die Gruppe a-i3 ist in ihrer Struktur einmalig. Gegründet von dem Medien- und Wirtschaftsjuristen Borges sowie Experten für Informationstechnik, kümmert sich das Team um Identitätsmissbrauch im Internet. Die Arbeitsgruppe wurde im Mai 2005 an der Ruhr-Universität Bochum ins Leben gerufen und vier Monate später in einen Verein umgewandelt, der sich aus Mitgliedsbeiträgen, Spenden und Sponsorengeldern finanziert.

KAFFEE UND KONTO

Die Bank ING Direct hat in mehreren US-Städten Cafés eingerichtet, in denen die Kunden online ihre Bankgeschäfte erledigen, im Netz surfen und nebenbei Kaffee trinken können.

„Einzigartig an der Organisation ist, dass hier Juristen und IT-Fachleute zusammenarbeiten“, erläutert Borges. Ziel sei, Internet-Nutzern, deren Identifizierungsdaten missbraucht wurden, Hilfe anzubieten. „Gemeinsam suchen wir nach technischen und rechtlichen Lösungen, mit denen sich der Einzelne schützen kann.“

Dazu haben die Bochumer unter der Nummer 0234-322 80 58 eine Hotline geschaltet. Dort können sich Opfer von Phishing-Attacken jeden Dienstag und Donnerstag Rat holen. Zwar darf der Verein keine umfangreiche Rechtsberatung offerieren – das verbietet das deutsche Recht. Aber das Sorgentelefon kann Haftungsregeln erläutern. Im Zweifelsfall wird den Betroffenen geraten, sich an einen Anwalt zu wenden.

Allein im vergangenen Dezember waren im Netz 28 000 Phishing-Seiten aufgeflogen. Das Problem ist so massiv, dass die Banken extra IT-Dienstleister beschäftigen, um derlei Seiten außer Gefecht zu setzen.

Inzwischen gibt es bereits zwei Generationen solcher Mails, warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI ist der zentrale IT-Sicherheitsdienstleister des Bundes und berät ebenso Behörden wie Privatleute.

Die erste Generation der Schummel-Mails gleicht täuschend echt dem offiziellen Schreiben eines Geldinstituts. Darin wird der Kontoinhaber aufgefordert, einen Sicherheitscheck vorzunehmen und mit PIN und TAN zu bestätigen – so wie Johann K. hereingelegt wurde. Dabei betonen die Banken immer wieder, dass sie ihre Kunden niemals per E-Mail zur Eingabe von Kontonummer, PIN oder TAN auffordern würden.

In der zweiten Generation der Mail-Tricks wird auf Einschüchterung gesetzt. Mal kommt eine angebliche Mahnung von der GEZ, mal droht vermeintlich das Bundeskriminalamt mit einem Ermittlungsverfahren wegen unerlaubten Downloadens, oder es landen fiktive Telekom-Rechnungen über Hunderte Euro im elektronischen Postfach.

PETER ALBAUM / JOKER

RATGEBER
Das in Bonn ansässige Bundesamt für Sicherheit in der Informationstechnik berät Behörden, Firmen und Privatleute.

Das Prinzip ist immer gleich: Wer den Anhang öffnet, fängt sich umgehend einen „Trojaner“ ein: ein kleines tückisches Programm, das still und heimlich Daten ausspäht und an den Absender schickt. Oder es wird die sogenannte Hosts-Datei des Rechners manipuliert, mit der einer Website eine IP-Adresse zugeordnet werden kann. Wird nun der Name einer Homepage eingegeben, landet der Betrogene postwendend auf einer Fälschung. „Pharming“ heißt diese Variante des Phishings.

Meist finden die Geschädigten auf ihrem Konto gähnende Leere vor – das ganze Guthaben einfach abgephisht. Und nicht nur das: Auch die Kreditlinie wird bis an den Rand ausgeschöpft. Der durchschnittliche Schaden beträgt rund 5000 Euro. „Die Betroffenen sollten sofort mit ihrer Bank sprechen“, rät Paul Dienstbach, juristischer Mitarbeiter bei a-i3. Denn wenn man schnell reagiert, lässt sich manche Überweisung noch zurückziehen. „Darüber hinaus sollte Strafanzeige erstattet werden.“ Im schlimmsten Fall freilich ist das Geld weg.

Und dann wird es kompliziert. „Im Prinzip muss die Bank haften,“ weiß Dienstbach, „denn sie hat die Überweisung ja ohne Auftrag ausgeführt.“ Indes

Online-Banking

iTAN-Verfahren
Ersetzt mehr und mehr das unsichere PIN/TAN-Verfahren. Der Kunde erhält von der Bank eine TAN-Liste. Bei einer Transaktion fragt die Bank eine bestimmte TAN ab, die der Kunde eingeben muss. Phishing funktioniert nicht; Pharming und Trojaner-Angriffe sind möglich.

eTAN-Verfahren
Der Kunde erhält von der Bank ein kleines Gerät (TAN-Generator), das nach einem bestimmten Algorithmus eine elektronische TAN erzeugt, die für die Transaktion verwendet werden soll. Trojaner-Angriffe und Pharming sind möglich. Phishing jedoch ausgeschlossen, weil die TAN erst im Rahmen des Auftrags generiert wird.

eTAN-Plus-Verfahren/Smart-TAN-Verfahren
Erweitertes eTAN-Verfahren. Während einer Transaktion erhält der Kunde von der Bank eine Kontrollnummer. Er schiebt seine EC-Karte in einen TAN-Generator und gibt über dessen Tastatur diese Nummer ein. Dadurch wird eine TAN generiert, die für die Transaktion übernommen werden muss. Dieses Verfahren ist nach heutigem Stand absolut sicher.

mTAN-Verfahren
Der Versand von TANs erfolgt per SMS auf ein bei der Bank angemeldetes Mobiltelefon. Während der Transaktion wird von der Bank eine TAN erzeugt und dem Kunden auf sein Handy übermittelt. Die TAN ist ausschließlich für diesen Vorgang gültig. Phishing, Trojaner und Pharming funktionieren nicht. Das Verfahren verursacht kostenpflichtige SMS und ist von der Erreichbarkeit des Handynetzes abhängig.

Glossar 2

Phishing
Diebstahl sensibler Daten, etwa zum Online-Banking, durch gefälschte Internet-Seiten.

Pharming
Manipulation des Rechners durch einen Trojaner, der bei Eingabe einer korrekten Web-Adresse auf eine Fälschung umleitet.

IP-Adresse
Eine Art Postleitzahl im Internet zur Adressierung von Rechnern.

Wurm
Schadprogramm für konzertierte Angriffe durch Botnetze. Diese sollen Websites durch Überlastung zum Absturz bringen.

Wurmdrossel
Bestandteil von Windows-XP-Servicepack 2. Ermöglicht, dass der angegriffene Rechner die gleichzeitig laufenden Verbindungsversuche limitiert. Soll Würmer ausbremsen.

stellt manches Geldinstitut sich quer – und verweist auf den Leichtsinn des Kunden. Erst im vergangenen Oktober hatte der Ombudsmann des Bundesverbandes der Deutschen Volks- und Raiffeisenbanken in einem umstrittenen Schlichtungsvorschlag entschieden, dass ein Phishing-Opfer seinen Schaden selber zu tragen habe.

Vom Konto des Geschädigten waren 4800 Euro an einen Geldkurier überwiesen worden. Obgleich der Rechner des Opfers nachweislich mit einem Trojaner infiziert war, entschied der Ombudsmann gegen den Mann: Der habe die Transaktion anscheinend selber vorgenommen. Und selbst wenn nicht – dann hätte er eben mit PIN- und TAN-Nummern geschlampt. Das Problem: Wie soll ein Kunde nachweisen, was ein Trojaner genau gemacht hat?

Allerdings: „Wenn jemand ohne jede Vorsichtsmaßnahme wie Virenscanner oder Firewall in das Internet geht“, mahnt der Jurist, „dann könnte ihm das als Fahrlässigkeit ausgelegt werden.“ Schließlich haben auch solche Geprellten das Nachsehen, die ihre PIN-Nummern neben der Kreditkarte im gestohlenen Portemonnaie liegengelassen hatten.

Gekaperte Rechner

Cyberkriminelle nutzen Sicherheitslücken aus.

Es war ein schwarzer Tag für das Internet-Portal StudiVZ: Ende Februar knackten Hacker die studentische Netzplattform und stahlen Tausende registrierter Profildaten. Damit konnten die Cyberkriminellen problemlos jede beliebige Identität annehmen. Nicht nur E-Mail-Adressen oder Handy-Nummern, auch private Details fielen den unsichtbaren Häschern anheim.

Wie groß der Schaden genau ist, lässt sich nicht mehr ermitteln. Aber mit zwei Millionen Nutzern ist StudiVZ eine der größten studentischen Communitys im Netz. Nun konnten die Hacker nach Herzenslust fremde Korrespondenzen lesen. Wer auf Nummer sicher gehen wollte, musste seine E-Mail-Adresse wechseln.

Experten befürchten, dass noch ganz anderer Schaden droht. Denn die ehemals idealistischen Hacker, die einfach nur Sicherheitslücken aufdecken wollten, haben längst ihre Unschuld verloren. Sie verkaufen die geknackten Adressen für ein Trinkgeld an Massenversender ungebetener Werbe-Mails weiter. Oder, noch schlimmer: Die gekaperten Rechner dienen als Zwischenlager krimineller Inhalte.

Besonders geeignet sind Universitätsnetzwerke, wo die meisten Rechner einen superschnellen Internet-Zugang besitzen. Eindringlingen kommt zugute, dass viele Netzwerkbetreiber Computer-Laien sind. Während erfahrene Netzadministratoren auf solche Einbrüche meist schnell reagieren und sich umgehend an die Staatsanwaltschaft wenden, merken viele Heimanwender noch nicht einmal, dass sie Opfer von Cyberkriminellen geworden sind.

Das Problem ist, dass viele Menschen mit ihrem Rechner völlig ungeschützt ins Netz gehen – und das zu Zeiten von Highspeed-DSL. Dabei würden oft schon ein einfaches Antivirus-Programm und eine Software-Firewall helfen, die gröbsten Gefahren zu bannen.

CHRISTIAN SCHROTH

VIRTUELLER CAMPUS
Im Oktober 2005 riefen drei Berliner Jungunternehmer die Studentenbörse StudiVZ ins Leben. Ende 2006 übernahm der Holtzbrinck-Konzern die Netzgemeinde für rund 85 Millionen Euro.

Vinton Cerf, ein Pionier des Internet, schätzt, dass bis zu 150 Millionen der etwa 600 Millionen Rechner im Internet mittlerweile Zombies sind. Zombies sind ferngesteuerte Rechner in sogenannten Botnetzen. Völlig unbemerkt von ihren Besitzern agieren solche Rechner und überfluten dann das Netz mit ungebetener Werbung. Oder sie werden für einen massenhaften Web-Angriff auf Websites genutzt.

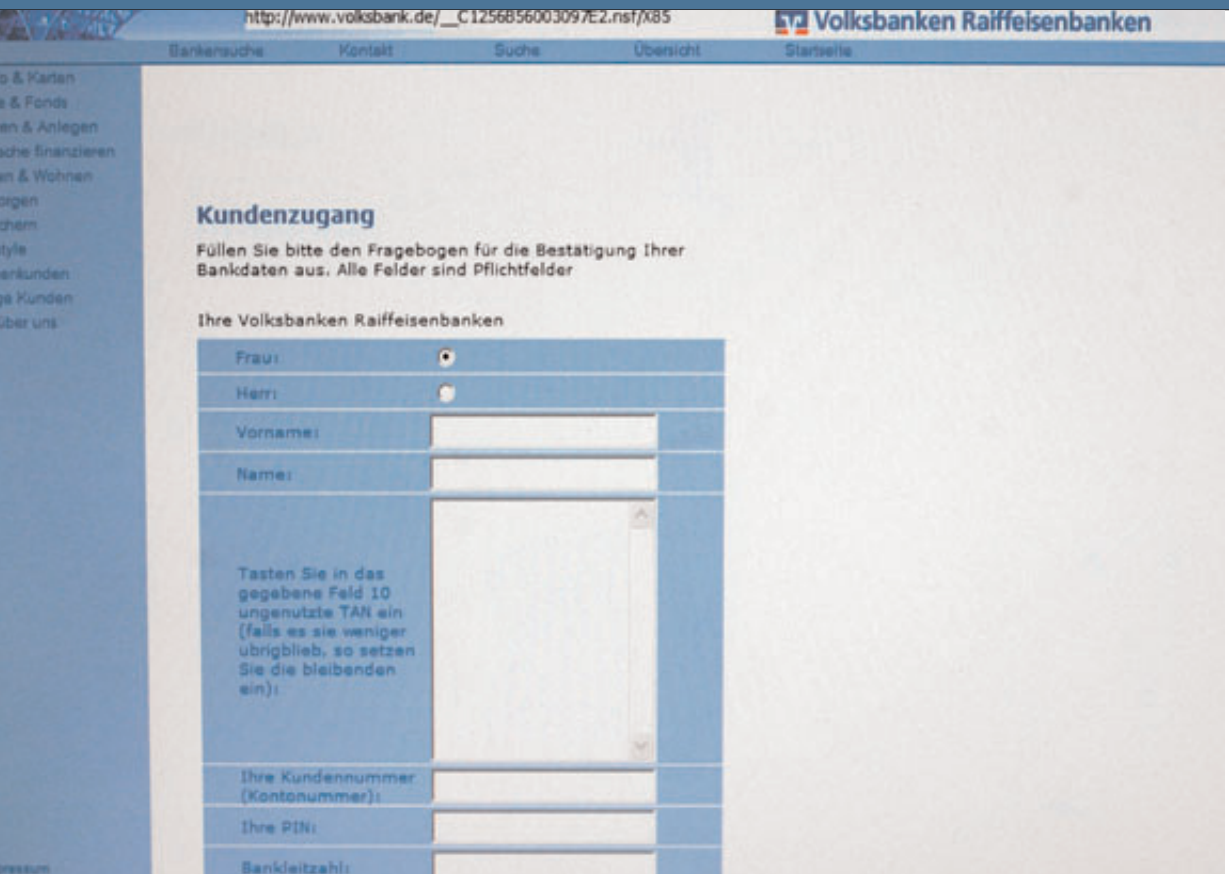
Als zeitweise sogar die Homepage von Microsoft lahmgelegt war, reagierten die Redmonder Software-Entwickler mit einer „Wurmdrossel“: Sobald ein Rechner zu viele Verbindungsversuche gleichzeitig unternimmt, wird die Reißleine gezogen – die Verbindung wird abgebrochen und neu aufgebaut.

Viele Heimfunknetze (W-Lan) sind, ungeachtet aller Warnungen, völlig ungesichert. Die User gehen unverschlüsselt ins Netz, so dass jeder Vorbeifahrende sich mit seinem Notebook ins Heimnetz einloggen und nach Lust und Laune herauf- und herunterladen kann, was er will – bis hin zu den Zugangsdaten für Online-Banking und Börsenportal.

Doch selbst die veraltete WEP-Verschlüsselung bietet keinen ausreichenden Schutz mehr, sie hält einem Angriff gerade mal 60 Sekunden stand.

Dabei haben moderne Geräte eine Reihe von Sicherheitsmöglichkeiten. Zum einen sollte unbedingt eine zeitgemäße Verschlüsselung eingestellt werden, die sich nicht so leicht knacken lässt. Zum anderen lässt sich genau konfigurieren, welche individuellen Rechner sich überhaupt in das Netz einloggen dürfen. Wer schließlich noch das Ausstrahlen der Netzkennung abschaltet, ist schon vor der Mehrzahl der Attacken gefeit.

Mit jeder dritten Phishing-Seite soll Deutschland mittlerweile Europameister sein. Angesichts des dreisten Datenklaus gehen bereits manche Hacker zum Gegenangriff über. Treibende Kraft sind Anbieter von Anti-Phishing-Software wie die britische Firma Netcraft, die gefälschte Websites öffentlich an den Pranger stellen. Die Computerkids erledigen den Rest, löschen die Schad-Software und hinterlassen schnippische Kommentare: „Suchen Sie die Bank, die hier sein sollte? Wir haben sie zerstört, weil sie nicht echt war.“



HEREINGELEGT
Mit einer gefälschten, aber echt aussehenden Internet-Seite einer Bank veranlassen Betrüger Bankkunden, PIN und TAN preiszugeben – mit den Geheimzahlen können sich die Täter dann per Online-Banking vom Konto des Opfers bedienen.

Sperrt sich die Bank hartnäckig, den Schaden zu ersetzen, muss der Geprellte auf eigene Faust versuchen, das Geld vom Empfänger zurückzubekommen. Ein meist hilfloses Unterfangen, denn die vermeintlichen Profiteure sind oft selbst Opfer von Betrügerbanden.

So wie Ilona S., auf deren Konto die 7140 Euro von Johann K. gelandet waren. Die Frankfurterin hatte vorübergehend als nebenberufliche „Finanzagentin“ für ein Dienstleistungsunternehmen gearbeitet. Für eine kleine „Vermittlungsgebühr“ von fünf Prozent sollte S. das Geld ins Ausland weiterleiten.

„Vor derartigen Dienstleistungen kann nur eindringlich gewarnt werden“, betont Georg Borges – Finger weg von sogenannten Job offers, die den Spamfilter umgehen und einem ungebeten ins Mail-Fach flattern. Denn der Finanzagent geht ein hohes Risiko ein: „Anders als der Laie denkt, haftet der Vermittler nicht nur in Höhe seiner Provision, sondern für den Gesamtschaden.“

Den Verlockungen erliegt so mancher, wissen die a-i3-Experten. Da bekommt etwa ein Unternehmensberater ein absolut seriös klingendes Angebot, die Geldeinnahmen für ein Internet-Auktionshaus zu transferieren. Umgehend werden seinem Privatkonto 2000 Euro gutgeschrieben. Als der Mann, misstrauisch geworden, nachfragt, wird ihm per E-Mail mit Gewalt gedroht. Wie befohlen, überweist er die Summe und bricht den Kontakt ab.

Nicht immer ist es die Jagd nach dem schnellen Geld, die unüberlegt handeln lässt. Manchmal wird einfach die missliche Lage von Ahnungslosen schamlos ausgenutzt. „Eine Schuhverkäuferin erhielt ein Angebot, als Verkaufsagentin bei Ebay Schuhe zu vertreiben“, erinnert sich Borges. „Die Frau war glücklich, schließlich war sie schon seit längerer Zeit arbeitslos.“ Von der Seriosität der Arbeit überzeugt, räumte sie sofort ein Zimmer leer, um die Ware zwischenzulagern.

Schuhe trafen indes keine ein. Stattdessen wurde die Verdutzte gefragt, ob sie ihrem Auftraggeber einen Gefallen tun könne: Eine Kollegin sei krank, sie solle doch über ihr Privatkonto eine größere Summe Geld weiterleiten. Stutzig geworden, wandte sich die Frau an die a-i3-Berater. „Wir haben ihr erklärt, dass es sich um illegale Geldwäsche handelt“, berichtet Borges. „Die Frau fiel aus allen Wolken.“

Die meist arglosen Finanzagenten fliegen auf, doch an die wahren Täter kommt man nicht heran. Die verwischen geschickt ihre Spur mit Hilfe von Firmen, die sich auf Geldtransferleistungen spezialisiert haben. Die Masche ist immer gleich: „Das Geld wird nicht auf ein Konto überwiesen, sondern als Bargeld per Western Union transferiert“, erklärt Borges. „Meistens nach Osteuropa.“

Was weiter geschieht, liegt im Dunkeln. Insider vermuten, dass sich das Geschäft so abspielen könnte: Die Täter sprechen einen armen Kauz an und geben ihm eine Vollmacht. Der geht damit in ein Auszahlungsbüro und bekommt den Betrag in bar. Doch das unverhoffte Glück währt nur kurz. Verlässt der Mann das Geldinstitut mit vollen Taschen, wird ihm das Geld wieder abgenommen.

Und dann verliert sich die Spur. Wer die Hintermänner sind, weiß niemand. Und noch nicht einmal, ob es sich dabei wirklich um osteuropäische Banden handelt – oder ob die Drahtzieher vielleicht doch in München, Paris oder London sitzen. Borges: „In Zeiten des Internets ist alles möglich.“

ANSGAR MERTIN

Glossar 3

WPA
Funkverschlüsselung für W-Lan-Verbindungen.

WEP
Unsicheres Verschlüsselungssystem, kann mit speziellen Programmen in wenigen Minuten geknackt werden.

MAC-Adresse
Eindeutige Kennung eines bestimmten Netzwerk-Rechners. Mit einer „Positiv-Liste“ lassen sich W-Lan-Netze absichern.

SSID
Funksignal, mit dem sich ein W-Lan-Netz identifiziert.

Hotspot
Öffentliches W-Lan-Funknetz, etwa in Cafés oder Kneipen, in das sich Gäste einloggen und surfen können.