Phishing: Angriffe in immer neuen **Varianten**

Von Matthias Gärtner und Frank W. Felzmann

Längst haben es Kriminelle nicht mehr nur auf das Ausspionieren von Bankdaten sondern auch des Nutzerverhaltens abgesehen, meinen Matthias Gärtner und Frank W. Felzmann. Sie konstruieren vermehrt Trojaner, die die Kontrolle über den befallenen PC übernehmen. Um so gefährlicher ist der allzu laxe Umgang vieler Nutzer mit ihren persönlichen Daten im Internet. Eine weitere Tendenz: Es wird nicht mehr unbedingt der zentrale Rechner eines Unternehmens angegriffen, sondern eher ein einzelner Arbeitsplatz. Das Erstellen oder Anpassen krimineller Programme wird immer einfacher. Zudem wird Schadsoftware oft auch sehr gezielt eingesetzt, warnen die Autoren. Red.

Die Methoden von Kriminellen, an Nutzerdaten und Passwörter zu kommen, werden immer trickreicher – und dadurch für den Nutzer schwerer zu erkennen. Vorsicht und Skepsis sind mehr denn je gefragt. Zwar sind Phishing-E-Mails unverändert im Umlauf, um Bankkunden zur Übersendung von Zugangsdaten und Transaktionsnummern zu verleiten, doch Phishing (Password fishing) findet inzwischen nicht mehr nur per E-Mail statt.

Außerdem haben es die Kriminellen nicht mehr ausschließlich auf Banking-Seiten abgesehen: Anfang des Jahres wurde in den Medien darüber berichtet, dass Phisher versuchten, Twitter- und Facebook-Anwendern die Login-Daten zu stehlen. Dazu versandten sie über die sozialen Netzwerke Nachrichten mit Inhalten wie: „Hey, I found a website with your pic on it … check it out here." Die Nachrichten enthielten Links zu Websites, die Twitter und Facebook ähnlich sahen und die Login-Daten des Nutzers abfingen.

Trojanische Pferde weiterhin im Trend

Das wichtigste Werkzeug um Passwörter zu stehlen oder Internetnutzer gezielt auszuspionieren, sind aktuell allerdings nicht gefälschte Nachrichten, die den Nutzer zur direkten Preisgabe seiner Daten motivieren sollen, sondern Trojanische Pferde. Sie installieren sich heimlich und bringen einen einzelnen Rechner unter die Kontrolle des Angreifers. Die meisten dieser Schadprogramme sind modular aufgebaut und verfügen über mehrere Funktionen. So kann beispielsweise ein Trojanisches Pferd gleichzeitig über Backdoor- und Spywarefunktionen verfügen, einen Keylogger verwenden und den befallenen Rechner zusätzlich an ein Bot-Netz anschließen. Zudem verfügen die meisten Schadprogramme über Updatefunktionen, sodass neue Programme oder Tarnmechanismen jederzeit nachgeladen werden können. Bot-Rechner, die mehrfach am Tag mit Updates versorgt werden, sind daher Standard.

Die Anzahl gezielter Angriffe mit multifunktionalen Trojanischen Pferden zu Spionagezwecken nimmt unverändert zu. In den Jahresberichten der Verfassungsschutzbehörden des Bundes und der Länder finden sich Informationen über Art und Urheber elektronischer Angriffe auf Wirtschaftsunternehmen und Behörden durch ausländische Nachrichtendienste. Wurden dabei früher hauptsächlich zentrale Server einer Behörde oder eines Unternehmens angegriffen, um das dahinter liegende Netz auszuspionieren, haben sich die Angriffe jüngst auf einzelne Arbeitsplatzrechner verlagert.

Seriöse Websites werden manipuliert

Durch geschicktes Social Engineering werden IT-Anwender dazu gebracht, eine präparierte E-Mail oder Webseite zu öffnen oder einen manipulierten Datenträger, etwa einen USB-Stick, anzuschließen. Selbst

Zu den Autoren

Matthias Gärtner ist Sprecher und **Frank W. Felzmann** ist Referatsleiter Sicherheit in Betriebssystemen des Bundesamtes für Sicherheit in der Informationstechnik, Bonn.

erfahrene Computernutzer sind manchmal unachtsam – oder der Trojaner wird so geschickt versteckt, dass er nur mit Glück zu entdecken ist. Bei Angriffen über manipulierte E-Mail-Anhänge werden aufgrund der weiten Verbreitung am häufigsten Microsoft-Office-Dateien, wie Word oder Power-Point, oder PDF-Dateien missbraucht. Für das Opfer ist die Manipulation in der Regel nicht auf den ersten Blick zu erkennen.

Zunehmende Gefahr geht auf der rein technischen Seite auch von den sogenannten Drive-by-Downloads aus. Angreifer manipulieren dabei vermehrt seriöse Webseiten, um unbemerkt Schadcode auf den PC zu schleusen. Sicherheitslücken im Webbrowser oder in installierten Zusatzkomponenten (Plug-Ins) lassen sich zu solchen Zwecken ausnutzen. Die mit Abstand meisten Schwachstellen im Zusammenhang mit Webbrowsern wurden im Jahr 2007 in Active-X-Steuerelementen entdeckt, die zur Darstellung von aktiven Inhalten verwendet werden.

Spyware erstellt Benutzerprofile

Untersuchungen von Sicherheitsunternehmen zufolge wurden im Zeitraum von Januar bis März 2008 durchschnittlich 15 000 infizierte Webseiten pro Tag entdeckt. Davon gehörten 79 Prozent zu an sich harmlosen Internetangeboten. Die meisten Angriffe erfolgen dabei über das Einschleusen von sogenannten Inlineframes, das mit geringem Aufwand automatisiert möglich ist, wenn die Webseite eine Schwachstelle enthält. Ein einzelner Angreifer kann auf diese Weise mehrere Tausend Webseiten innerhalb weniger Stunden infizieren. In den meisten Fällen müssen dazu aktive Inhalte wie zum Beispiel Java Script auf dem Rechner frei geschaltet sein, damit die Schadprogramme eingeschleust und ausgeführt werden können.

Manche Trojanische Pferde und Spyware-Programme können nach dem Installieren das Surf-Verhalten einer Person im Internet ausspionieren, um Benutzerprofile zu erstellen. Diese werden dann entweder vom Spyware-Ersteller selbst genutzt oder an kommerzielle Firmen verkauft, damit diese zielgerichtet Werbeeinblendungen platzieren können.

Schäden im Bereich des Onlinebankings zurückgegangen

Wenn Spyware auch Anmeldedaten wie Benutzername oder Passwort heimlich mitprotokolliert, wird dadurch für die Angreifer Identitätsdiebstahl möglich. Dazu sammeln sie neben Kreditkarten-, Zugangs- und Transaktions-Daten außerdem Informationen zur Identität des Opfers, wie etwa Geburtsdatum, Anschrift und Führerscheinnummer. Mit den gewonnenen Daten werden nunmehr kriminelle Aktivitäten im Bereich von E-Commerce-Angeboten durchgeführt. Bereits jetzt resultieren daraus weltweit Schäden in Milliardenhöhe – mit steigender Tendenz.

Der finanzielle Vorteil, den sich die Kriminellen durch Missbrauch personenbezogener Daten verschaffen, muss also nicht zwingend über das Eindringen in einen fremden Banking-Account realisiert werden. Trotz trickreicheren Vorgehens der kriminellen Programmierer sind die Schäden im Bereich des Online-Bankings sogar zurückgegangen, was hauptsächlich durch verbesserte Sicherheitsmaßnahmen wie e-TAN- oder m-TAN-Verfahren erreicht wurde. Diese Schadensreduzierung wird jedoch durch neue betrügerische Betätigungsfelder der Kriminellen wieder ausgeglichen.

Individuelle Vorsicht und Skepsis sind angebracht

Identitätsdiebstahl wird aber nicht nur durch die kriminelle Energie von Betrügern, sondern zunehmend auch durch aktives Zutun der Nutzer begünstigt. Die Popularität von Social Networks, in denen Mitglieder freiwillig eine Vielzahl privater Daten preisgeben, vereinfacht Phishing und Datenmissbrauch erheblich. Technische Lösungen stoßen hier an ihre Grenzen, der unbedachte Umgang mit persönlichen Daten lässt sich nur durch die weitere Aufklärung und Sensibilisierung der Nutzer eindämmen.

Um sich gegen Phishing und andere Angriffe zu schützen, sind von jedem ein paar technische Vorkehrungen zu treffen, aber vor allem sind individuelle Vorsicht und Skepsis gefragt. Theoretisch kann jede E-Mail, jedes Dokument, jeder Anhang und jeder USB-Stick mit einem Trojaner oder einer anderen Schadsoftware befallen sein, die sich dann auf den eigenen Rechner überträgt. Deshalb sollte man vor dem Speichern und Ausführen von Dateien deren Herkunft prüfen und sie bei eventueller Unsicherheit mit entsprechender Software auf Viren, Trojaner und Spyware testen.

Wie leicht man in eine Falle tappen kann zeigt sich bei manchen IT-Sicherheitstests von Unternehmen: Eine bekannte Test-Methode ist, auf dem Firmenparkplatz ein paar USB-Sticks auszulegen. In der Regel gibt es Mitarbeiter, die den gefundenen USB-Stick an ihren Arbeitsrechner anschließen – ohne zu wissen, wo der Datenträger herkommt und welche Daten er enthält. Das Testergebnis lautet dann: durchgefallen.

Aktuelles Anti-Viren-Programm benötigt

Damit es so weit nicht kommt, bietet das Bundesamt für Sicherheit in der Informationstechnik für Unternehmen und Verwaltungen auf seiner Homepage (www.bsi.bund.de) umfangreiche Informationen zum Schutz sensitiver Daten, etwa die Broschüre „Leitfaden IT-Sicherheit", spezielle Fachstudien sowie umfassende Unterlagen zum IT-Grundschutz. Privatanwender finden auf dem Webangebot des www.bsi-fuer-buerger.de umfangreiche Informa-

tionen zum Schutz ihres PCs; über aktuelle Gefahren im Internet informiert der Warn- und Informationsdienst www.buerger-cert.de.

Die neben der Sensibilisierung der Nutzer zu ergreifenden technischen Vorkehrungen lassen sich nahezu beliebig ausweiten. Grundsätzlich ist der Einsatz von Anti-Viren- und Anti-Spyware-Programmen nach wie vor mehr als geboten. Wichtig ist, dass diese Programme aktuell sind und ständig auf dem neuesten Stand gehalten werden. Auch sollte darauf geachtet werden, dass alle anderen zum Einsatz kommenden Programme, vor allem das Betriebssystem und der Browser, mit Updates versorgt werden, weil diese in der Regel bekannte Sicherheitslücken schließen.

Elektronisches Wettrüsten

Allerdings halten die Angreifer bei diesem elektronischen Wettrüsten mit: Insbesondere die Autoren von Trojanischen Pferden und die Botmaster, die sich mit hoher krimineller Energie einen finanziellen Vorteil verschaffen wollen, verbessern ständig ihre Schutzmechanismen, um die Erkennung und Analyse des Schadcodes zu erschweren. Die meisten Schadprogramme schützen sich inzwischen mit kryptografischen Verfahren und passen ihr Verhalten an – je nachdem, ob sie in einer typischen Analyseumgebung oder auf einem echten Anwender-PC ausgeführt werden.

Hinzu kommt, dass es mittlerweile sehr einfach ist, bösartige Programme zu erstellen oder vorhandene Exemplare an die jeweiligen kriminellen Bedürfnisse anzupassen. Aussagen über die genaue Anzahl von Schadprogrammen sind dadurch inzwischen schwierig geworden. Je nach Klassifikation und Zählweise unterscheiden sich die Werte der IT-Sicherheitsunternehmen erheblich.

Eines ist jedoch sicher: Es gibt Millionen von Schadprogrammen, deren Anzahl immer schneller wächst. Jeden Monat kommen Zehntausende hinzu. Die Herstellung und der Einsatz von Schadprogrammen verhelfen organisierten Kriminellen zu Gewinnen in Milliardenhöhe und sind fester Bestandteil in ihrer „Wertschöpfungskette".

Millionenfacher Datenklau

Obwohl immer mehr Schadsoftware im Umlauf ist, werden einzelne Schadprogramme jetzt gezielter eingesetzt als früher und nicht mehr wahllos an möglichst viele Opfer verteilt. Je geringer die Verbreitung eines bestimmten Schadprogramms ist, desto niedriger ist die Wahrscheinlichkeit, dass es den Herstellern von Virenschutzprogrammen rasch bekannt wird und damit von einem Schutzprogramm erkannt wird. Die Einsatzdauer eines Schädlings lässt sich so verlängern.

Neben klassischer Schadsoftware auf dem einzelnen Anwender-PC gibt es eine weitere Methode, an sensible Daten zu kommen: das Einhacken in Datenbanksysteme. Erst im Januar 2009 berichteten Medien darüber, dass sich Computerhacker Zugang zu den Datenbanken eines Kreditkarten-Unternehmens in Princeton im US-Bundesstaat New Jersey verschafft haben. Schätzungen gehen davon aus, dass Millionen Kreditkartendaten gestohlen wurden, mit denen sich funktionsfähige Kopien der Kreditkarten anfertigen lassen.

Zum gleichen Zeitpunkt wurde bekannt, dass Kriminelle Nutzerinformationen der deutschen Online-Stellenbörse „Monster" entwendet haben. Zwar seien wohl keine sensiblen Daten wie Sozialversicherungsnummer betroffen, dennoch wurde darauf hingewiesen, dass die E-Mail-Adressen für Phishing-Mails missbraucht werden könnten. Hier stehen die betroffenen Unternehmen in der Verantwortung, Maßnahmen gegen Cyber-Angriffe zu treffen. Das BSI bietet dazu umfangreiche Informationen an.

bank und markt
Zeitschrift für Retailbanking

Verlag und Redaktion:
Verlag Fritz Knapp GmbH
Aschaffenburger Straße 19, 60599 Frankfurt am Main,
Postfach 111151, 60046 Frankfurt am Main,
Telefon 069/970833-0, Telefax 069/70784 00,
www.kreditwesen.de,
E-Mail: red.bum@kreditwesen.de

Herausgeber: Klaus-Friedrich Otto

Chefredaktion: Dr. Berthold Morschhäuser, Swantje Benkelberg, Philipp Otto

Redaktion: Lars Haugwitz, Alexander Hofmann, Barbara Hummel, Frankfurt am Main.

Redaktionssekretariat: Elke Hildmann

Die mit Namen versehenen Beiträge geben nicht immer die Meinung der Redaktion wieder. Bei unverlangt eingesandten Manuskripten ist anzugeben, ob dieser oder ein ähnlicher Beitrag bereits einer anderen Zeitschrift angeboten worden ist. Beiträge werden nur zur Alleinveröffentlichung angenommen.

Verlagsleitung: Uwe Cappel

Anzeigenleitung: Ralf Werner, Tel. 069/970833-43.

Anzeigendisposition: Anne Guckes, Tel. 069/970833-26,

sämtl. Frankfurt am Main, Aschaffenburger Straße 19.

Zurzeit gilt Anzeigenpreisliste Nr. 38 vom 1.1.2009.

Erscheinungsweise: Am 1. jeden Monats.

Bezugsbedingungen: Abonnementspreise inkl. MwSt. und Versandkosten: jährlich € 333,76, bei Abonnements-Teilzahlung: ½jährlich € 170,96. Ausland: jährlich € 341,12. Preis des Einzelheftes € 17,90 (zuzügl. Versandkosten).

Verbundabonnement mit der „Zeitschrift für das gesamte Kreditwesen": jährlich € 648,24, bei Abonnements-Teilzahlung: ½jährlich € 337,80. Ausland: jährlich € 664,56.

Studentenabonnement: 50% Ermäßigung (auf Grundpreis).

Der Bezugszeitraum gilt jeweils für ein Jahr. Er verlängert sich automatisch um ein weiteres Jahr, wenn nicht einen Monat vor Ablauf dieses Zeitraumes eine schriftliche Abbestellung vorliegt.

Bestellungen aus dem In- und Ausland direkt an den Verlag oder an den Buchhandel.

Probeheftanforderungen bitte unter
Tel.-Nr. 069/970833-32 oder -25

Als Supplement liegt „cards Karten cartes" jeweils am 1. Februar, 1. Mai, 1. August und 1. November dieser Zeitschrift bei.

Bei Nichterscheinen ohne Verschulden des Verlages oder infolge höherer Gewalt entfallen alle Ansprüche.

Bankverbindungen: Postbank Frankfurt 60482-609 (BLZ 50010060), Landesbank Hessen-Thüringen-Girozentrale 10555001 (BLZ 50050000), sämtliche in Frankfurt am Main.

Druck: Druckerei Hassmüller Graphische Betriebe GmbH & Co. KG, Königsberger Straße 4, 60487 Frankfurt.

ISSN 1433-5204