DuD
Datenschutz und Datensicherheit

Phishing

Dirk Fox

Hintergrund

Phishing ist eine der jüngsten Herausforderungen des Internet – und eine der Besorgnis erregendsten. Der Begriff geht auf das „Fischen" der ersten Internet-Kriminellen nach Passwörtern und Kreditkarteninformationen von Internet-Nutzern zurück. Die Schreibweise mit „ph" wurde vermutlich in Anlehnung an das Hacken von Telefonsystemen in den 80er Jahren, genannt „phreaking", gewählt.

Die erste dokumentierte Nutzung des Worts Phishing findet sich in einem Posting der Newsgroup alt.2600 vom 28.01.1996[1]; möglicherweise wurde es jedoch schon früher benutzt. Bezeichnet wurde damit zunächst das Hacken eines (Internet-) Accounts. Solche Accounts mit bekanntem Passwort erlaubten eine Nutzung des Internet auf fremde Kosten; sie wurden in Hackerkreisen „Phishes" genannt und wie eine digitale Währung gehandelt. Mit dem Preisverfall der Zugangskosten verlor Phishing an Bedeutung. Erst dank der explosionsartigen Zunahme von Spam erlebt es seit Oktober 2003 eine Renaissance – mit geändertem Angriffsziel: Jetzt stehen Ebay- und Bank-Accounts im Fokus der „Phisher".

Deutsche Banken gerieten erstmals Anfang des Jahres 2004 in den Fokus der Phisher. Viele deutsche Nutzer waren durch die englischen Phishing-Mails sensibilisiert, und auch für die Banken kam das Phänomen nicht überraschend. Daher hielten sich die Schäden in Deutschland in Grenzen, während in den USA bis zu 5% der Empfänger von Phishing-Mails die darin angegebenen Webseiten anklickten.

Techniken

Im Kern besteht ein Phishing-Angriff üblicherweise aus zwei Teilen:

- Erstens einer E-Mail, die den Empfänger unter einem (mehr oder weniger glaubwürdigen) Vorwand zum Besuch einer bestimmten Webseite auffordert.

In einer solchen, vermeintlich z. B. von Ebay oder einer Bank stammenden E-Mail, die das Corporate Design des vorgeblichen Senders möglichst echt nachbildet, werden die Empfänger aufgefordert, eine in der E-Mail verlinkte Webseite aufzurufen. Dieser Weblink wird entweder verschleiert (z. B. durch Verstecken des Links hinter dem korrekten Verweis auf die Bank-Webseite in HTML) oder es wird eine ähnlich lautende, jedoch dem Phisher zuzuordnende Domäne angegeben (z. B. „www.meine-bank-online.info" bzw. mit abweichender, aber ähnlicher Schreibweise, wie „I" statt „l").

Die Versendung der gefälschten E-Mails erfolgt über Spam-Verteiler. Als Absender- und Reply-to-Adresse dienen existierende oder zumindest korrekt gebildete E-Mail-Adressen der Domain des angeblichen Absenders. Zu erkennen ist die Absenderfälschung nur an der Adresse des letzten Hosts vor der Auslieferung – dieser Eintrag im Kopf der E-Mail lässt sich nicht fälschen und verrät den Spam-Verteiler. Allerdings ist dies nur für einen Experten erkennbar.

- Zweitens einer Webseite im Corporate Design des vorgeblichen E-Mail-Absenders, auf der Auhtentifikationsdaten (ID, PIN, TAN) abgefragt werden.

Oft ist die Webseite eines Phishers zusätzlich mit Schadsoftware versehen, die den Rechner des Nutzers befällt.

Gegenmaßnahmen

Durch Phishing ist aus der Belästigung Spam ein Sicherheitsrisiko geworden. Umgekehrt ist jede wirksame Maßnahme gegen Spam auch ein Schutz vor Phishing: Erreicht die Phishing-Mail den Empfänger nicht, wird er auch nicht zum Besuch der gefälschten Webseite und zur Eingabe von PINs oder Kreditkartendaten verleitet.

Darüber hinaus hilft nur Aufklärung. Fast alle Kreditinstitute informieren inzwischen auf ihren Webseiten über Phishing und hoffen, Ihre Kunden so für gefälschte E-Mails zu sensibilisieren. Bei Verzicht auf kritische Einstellungen wie das HTML-Format für E-Mails sind Phishing-Mails für aufmerksame Nutzer erkennbar.

Hilfreich ist auch die Authentifikation der Anbieterseiten mit einem SSL-Zertifikat. Allerdings haben zahlreiche Institute in der Vergangenheit „gesündigt": So wurde das Online-Banking von vielen Banken an externe Dienstleister vergeben, die nun die Seiten unterschiedlicher Banken in ihrer eigenen Domaine verwalten. Da hilft auch SSL nicht mehr: Der Browser zeigt in den Seiteneigenschaften (sofern diese Funktion dem Kunden überhaupt bekannt ist) nicht ein SSL-Zertifikat der Bank, sondern nur eines für die Domäne des Dienstleisters – und die ist für den Kunden nicht von der eines Phishers zu unterscheiden.

Phisher dürfen daher leider davon ausgehen, dass ihre eigene Webseite auch bei einem sensibilisierten Online-Kunden keinen Verdacht auslösen wird, sofern sie ein offizielles SSL-Zertifikat trägt.

Stand und Ausblick

Tatsächlich sind bislang – zumindest in Deutschland – nur wenige erfolgreiche Phishing-Angriffe publik geworden, zudem ausschließlich solche, bei denen die betroffene Bank unrechtmäßige Überweisungen noch stoppen konnte. Vermutlich ist die Summe der Schäden, die zweifellos von den betroffenen Banken kulant geregelt wurden, inzwischen jedoch erheblich.

Bislang haben oft die fehlerhafte Sprache und die stümperhafte Fallkonstruktion deutsche Phishing-Mails unglaubwürdig erscheinen lassen. Das ändert sich aber derzeit. Und mittlerweile sind auch zunehmend unterschiedliche deutsche Banken von Phishing-Angriffen betroffen, nachdem sich die Phisher lange Zeit auf die Deutsche Bank und die Postbank beschränkten.

Gefährlicher aber als die „Verfeinerung" der Phishing-Nachrichten ist die Weiterentwicklung der Techniken. So sind inzwischen per Phishing „beworbene" Webseiten aufgetaucht, die beim Besucher trojanische Pferde installieren, die gezielt PINs, TANs und Passworte mitprotokollieren und die gesammelten „Schätze" an den Phisher zurück senden. Oder es werden wichtige Konfigurationsdateien wie die Windows-hosts-Datei verfälscht, damit Zugriffe auf bestimmte Online-Banking-Webseiten automatisch im Hintergrund umgelenkt werden. Phishing stellt so die Vertrauenswürdigkeit des Internet vor eine neue Zerreissprobe.

[1] Ollmann, Gunter: *The Phishing Guide – Understanding & Preventing Phishing Attacks*. NGS White Paper, v1.01, 23.09.2004; http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf