PHISHING

Kriminelle Datenfischer

Immer mehr Internet-Nutzer werden Opfer von "Phishing-E-Mails". Kriminelle verwenden die von leichtgläubigen Internetanwendern ergaunerten vertrauliche Daten für Betrügereien.

Unter "Phishing" wird das "Abfischen" vertraulicher Daten über das Internet verstanden. Ausgangspunkt sind als Geschäftskorrespondenz aufbereitete E-Mails mit Vertrauen erweckendem Firmenlogo eines Kreditkarteninstituts, einer Bank, eines Online-Aktionshauses oder eines anderen Unternehmens. In den E-Mails wird per beigefügtem Link um den Aufruf der Firmen-Web-Seite und die Korrektur der Zugangsdaten, des Passworts oder anderer Daten ersucht. Tatsächlich landen die Internet-Nutzer beim Anklicken des Links auf einer gefälschten Seite. Die dort vom Benutzer eingetragenen vertraulichen Daten werden für betrügerische Zwecke ausspioniert.

Sicherheitslücken

Möglich wird diese Art des Betruges durch Sicherheitslücken in einigen Browsern und E-Mail-Clients. Dabei werden bei E-Mails, die im HTML-Format verfasst wurden, sowohl im sichtbaren Text als auch in der Statusanzeige des Browsers die vermeintlich authentischen WWW-Adressen (URL) der Webseiten angezeigt. Im HTML-Code versteckt, befindet sich jedoch eine andere WWW-Adresse, die beim Anklicken des Links tatsächlich geladen wird.

Ausgenützt wird die Leichtgläubigkeit vieler Anwender. Aufforderungen für notwendige, wichtige Änderungen an den Zugangsverfahren oder an den persönlichen Zugangsdaten werden üblicherweise nicht per E-Mail zugesandt, sondern per Brief oder auch telefonisch angekündigt. Außerdem sind solche Maßnahmen zur Manipulation der Zugangsverfahren eher unwahrscheinlich.

Spam-Prinzip

Bei den "Phishing"-Mails handelt es sich im Prinzip um Spam-Mails (unerwünschte Massenzusendungen), durch die möglichst viele Internetbenutzer dazu gebracht werden sollen, ihre persönlichen Zugangsdaten oder sonstigen vertraulichen Daten bekannt zu geben. Die Internetadresse wird verschleiert und eine vertrauenswürdige Web-Adresse vorgetäuscht. Es findet also die Kombination mehrerer, seit längerer Zeit bekannter Methoden statt. Wie die in betrügerischer Absicht agierenden "Phisher" zu gültigen E-Mailadressen gelangen, entspricht den üblichen Methoden von "Spammern".

Versteckte Webadresse

Das Problem, dass in einer einem Link hinterlegte Internetadresse einer Web-Seite (Unified Resource Locator – URL) eine zweite WWW-Adresse versteckt mitgeschickt werden kann, ist bereits seit Jahren bekannt. Ursprünglich war die Technik als Erleichterung für den Aufruf von zugangsbeschränkten Web-Seiten (z.B. Seiten mit User-ID- und Passwort-Eingabe) gedacht. Dazu wird in der URL ein Trennzeichen eingefügt, hinter dem Zugangsdaten und eine weitere Web-Adresse angegeben werden können. Mit der Zeit wurde diese Technik

auch für kriminelle Machenschaften genutzt. Allerdings konnte man in der Statuszeile des Browsers oder durch Überprüfen der Eigenschaften des jeweiligen Links die tatsächlich für den Aufruf vorgesehene URLs auf einfache Art und Weise noch vor dem Klicken ermitteln. Solche trügerischen URL setzen sich aus einer vertrauenswürdigen Web-Adresse mit nachfolgenden Leerzeichen, einem der drei Steuercodes @, %00, %01 und einer zweiten Web-Adresse zusammen.

Beispiel eines derartigen Quelltextes: Hier geht’s zur Polizei

Durch einen Fehler in einigen Browserversionen erfolgt beim Aufruf keine vollständige Anzeige der manipulierten WWW-Adresse (weder in der Statuszeile, noch in den Eigenschaften der WWW-Adresse). Mit einem zusätzlichen Steuerzeichen wird in der Adressleiste der tatsächlich aufgerufenen Web-Seite die Adresse der vermeintlichen Web-Seite angezeigt.

Im beschriebenen Beispiel erfolgt in der Statuszeile und unter den Link-Eigenschaften nur die Anzeige http://www.polizei.gv.at/. Tatsächlich wird die Startseite von http://www.bmi.gv.at/ aufgerufen. Dabei ist zu bedenken, dass eine URL für sich allein nichts über die dahinter liegenden Web-Seiten und eventuell versteckt ablaufende Programme aussagt. Internet-Surfern steht im Zweifel die Möglichkeit offen, sich im Quelltext der HTML-Seite die hinter einem Link tatsächlich liegende URL anzusehen. Dadurch werden alle Schwachstellen der Browser ausgeschaltet.

Allerdings ist zu bedenken, dass man nicht immer wissen kann, was sich hinter dieser Adresse verbirgt, auch wenn die Originalität der aufzurufenden URL bekannt ist. Seriös klingende URL-Texte müssen nicht unbedingt auf seriöse Web-Seiten verzweigen.

Die von den "Phishern" ergaunerten vertraulichen Zugangsdaten werden für Betrügereien verwendet, etwa für unberechtigte Überweisungen.

Wie kann ich mich schützen? Zwei alte, aber immer aktuelle Tipps zum Surfen im Internet:

- Verwenden Sie unbedingt ein auf dem aktuellsten Stand befindliches Virenschutzprogramm. Sorgen Sie dafür, dass die dazu gehörenden Signatur-Dateien laufend auf den neuesten Stand gebracht werden. Und schalten Sie das Virenschutzprogramm auch ein.

- Verwenden Sie bei Ihrem Browser beim Surfen auf Web-Seiten, solange diese Ihnen nicht absolut vertrauenswürdig sind, nach Möglichkeit eine hohe Sicherheitsstufe (Verbieten des Ausführens von Scripts und ActiveX, bzw. Ausführen nur mit Eingabebestätigung)

Ausführlichere Informationen über allgemeine Schutzmaßnahmen beim Surfen im Internet finden Sie auf den Internetseiten des Bundesministeriums für Inneres: http://www.bmi.gv.at/kriminalpolizei/warnungen_14.asp

Robert Gottwald/Ernst Österreicher

TIPPS GEGEN PHISHING

Vorsicht Datenklau

Um sicherzugehen, dass Sie keine versteckte WWW-Adresse aufrufen, klicken Sie auf keinen Fall auf den in einer Mail angezeigten Link. Tippen Sie stattdessen die in der Mail sichtbare URL in die Adressenleiste Ihres Browsers. Nur so können Sie sicher sein, genau diese Web-Seite aufzurufen.

Achten Sie darauf, dass Sie die angegebene Web-Adresse kennen. Am besten rufen Sie die Web-Seite der Bank oder des Kreditkartenunternehmens genau so auf, wie Sie sonst immer die Web-Seiten starten (z.B. über die Favoriten).

Wenn tatsächlich Änderungen an Ihren Zugangsdaten notwendig geworden sind, dann erfolgt die Aufforderung dazu üblicherweise erst nachdem Sie wie gewohnt die Web-Seiten mit Ihren bis dahin gültigen Zugangsdaten aufgerufen haben.

Haben Sie tatsächlich Probleme mit Ihren Zugangsdaten (z.B. haben Sie Ihr Passwort vergessen), dann benutzen Sie die dafür vom Anbieter der Web-Seiten vorgesehenen Kommunikationskanäle. Diese werden entweder auf der Homepage (Startseite) Ihrer Bank, Ihres Kreditkartenunternehmens, usw. beschrieben, oder sie wurden Ihnen bei der Erstausstellung ihrer Zugangsdaten mitgeteilt.

Sollten Sie daher Opfer einer derartigen Phishing-Attacke geworden sein, wenden Sie sich bitte umgehend an die nächste Polizei- oder Gendarmeriedienststelle. Dabei ist es von Vorteil, wenn die Original-E-Mail mit dem irreführenden Link noch vorhanden ist.