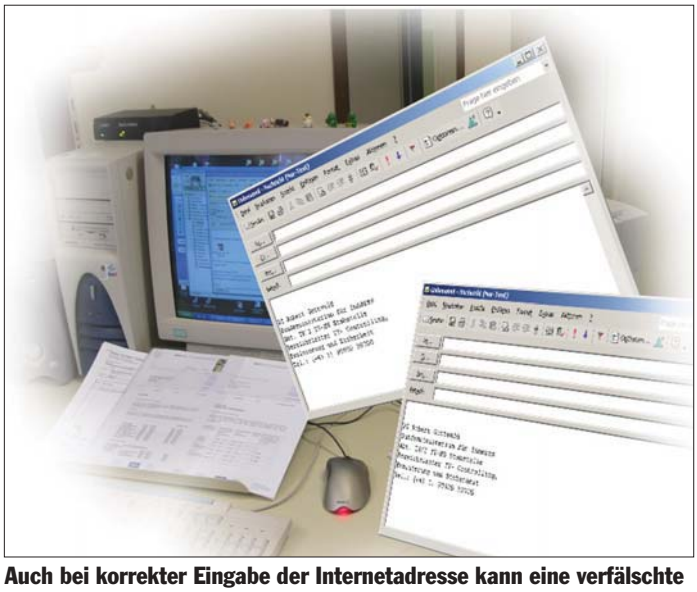
Neue Phishing-Methoden

In Österreich ist eine neue Methode des betrügerischen Ausspionierens der persönlichen und vertraulichen Zugangsdaten von Nutzern des Online-Bankings aufgetaucht.

In der *Öffentlichen Sicherheit 5-6/04* wurde erstmals auf die Gefahren des „Phishings“ hingewiesen. Praktisch alle Unternehmen, die Dienstleistungen über das Internet anbieten, warnen mittlerweile davor, persönliche Zugangsdaten, Kontonummern oder ähnliche persönliche und vertrauliche Daten über Internetseiten zu ändern, deren Internetadresse *(URL)* via E-Mail versandt wird. Dadurch hat sich bei vielen Internetnutzern bereits herumgesprochen, E-Mails, die den Verdacht erwecken, Phishing-Mails zu sein, einfach sofort zu löschen und keinesfalls die mit diesen Mails versandten Links zu benutzen, sondern immer nur die normalerweise zum Aufrufen der Dienstleistung verwendeten Internetadressen direkt über die Adresszeile des Browsers einzugeben.



Auch bei korrekter Eingabe der Internetadresse kann eine verfälschte Web-Seite aufgerufen werden.

Das Bedrohungsszenario hat sich inzwischen drastisch verändert. Auch bei der korrekten Eingabe der Internetadresse über die Adresszeile des Browsers kann bereits eine verfälschte Web-Seite aufgerufen werden.

Eine der Ursachen liegt in der immer stärker um sich greifenden Unart, dass E-Mails nicht als normale Textnachrichten, sondern vermehrt im so genannten HTML-Format versandt und vor allem gelesen werden. Das heißt, statt eines einfachen Textes wird ein zusätzlicher Programmcode versandt, der beim Anzeigen des Textes auf dem Rechner ausgeführt wird und dabei im schlimmsten Fall unbemerkt Schaden anrichtet.

Eine zweite Ursache resultiert daraus, dass immer noch sehr viele Rechner nur ungenügend geschützt ans Internet angeschlossen werden. Entweder ist kein Virenschutzprogramm vorhanden, oder es ist nicht aktiviert bzw. die Virensignaturdateien sind so veraltet, dass das Virenschutzprogramm die ständig neu im Internet auftauchenden Viren, Würmer, Trojaner, usw. nicht mehr als Gefahrenpotenzial erkennt. Zusätzlich erhöhen Betriebsysteme das Sicherheitsrisiko beträchtlich, ebenso veraltete Webbrowser oder Mailclients, die im Erstinstallationszustand belassen werden.

Die für das aktuelle Bedrohungsszenario ausschlaggebende Ursache basiert auf der missbräuchlichen Nutzung einer standardmäßig vorhandenen Netzwerkfunktionalität.

Jedem Rechner, der sich im Internet befindet, ist eine weltweit eindeutige nummerische Kennung zugewiesen, die so genannte IP-Adresse (Internet-Protokoll Adresse).

Da es praktisch unmöglich ist, sich alle Nummern für die Vielzahl der Rechner, die im täglichen Umgang mit dem Internet genutzt werden, zu merken, wurde bereits in den Urzeiten des Internets ein Verfahren gefunden, bei dem den einzelnen IP-Adressen mehr oder weniger aussagekräftige Server- bzw. Domänen-Namen zugeordnet werden können.

Diese werden dann anstatt der IP-Adresse beim Anwählen eines Rechners bzw. einer Webseite angegeben. Im Netzwerkverkehr selbst wird jedoch nur mit den IP-Adressen gearbeitet, das heißt, irgendwo müssen die eingegebenen Namen auf IP-Adressen umgewandelt werden. Früher, als das Internet nur aus wenigen Rechnern bestand, reichte es aus, dass die für den Internetverkehr notwendigen Rechnernamen mit ihren zugehörigen IP-Adressen in einer Datei mit dem Namen „Hosts“ auf dem eigenen Rechner abgelegt wurden.

Für die Wartung dieser Datei war jeder Internetbenutzer selbst verantwortlich (ähnlich den elektronischen Telefonbüchern der Mobiltelefone, bei denen die einzelnen Telefonnummern zu Namen hinterlegt werden können).

Mit wachsender Anzahl von Servern und Domänen im Internet wurde es jedoch praktisch unmöglich, auf diese Art und Weise immer alle notwendigen Adressen verfügbar zu halten. Die Verwaltung der Namen und zugehörigen IP-Adressen wurde daher durch eigene DNS-Anbieter („Domain Name Service“) übernommen (siehe Abbildung 1).

Die Funktionalität der lokalen Hosts-Datei blieb dabei aber weiterhin aufrecht. Wenn in dieser Datei zu einem Rechner- bzw. Domänen-Namen eine gültige IP-Adresse eingetragen ist, wird bei der Eingabe des Rechner- bzw. Domänen-Namens sofort zu der in der Hosts-Datei angegebenen IP-Adresse umgelenkt und kein DNS-Server (der die richtige IP-Adresse beinhalten würde) kontaktiert.

Umleitung auf gefälschte Seite. Wenn also in der Hosts-Datei durch ein per E-Mail versandtes oder über eine Webseite geladenes Programm unbemerkt ein falscher Eintrag vorgenommen wurde, erfolgt ab dem nächsten Aufruf der betroffenen Webadresse eine Umleitung auf die gefälschte Seite (siehe Abbildung 2). Diese Umleitung erfolgt – unabhängig von der verwendeten Browsertype für alle Browser gleich.

Neben den bereits bekannten und der zuvor beschriebenen Methoden gibt es für Angreifer grundsätzlich noch weite-

Foto: IT-MS

re Möglichkeiten, zu ihren Zugangsdaten zu gelangen. Bei einer – in Österreich noch nicht aufgetauchten – Variante wird mittels Trojanersoftware ein Keylogger-Programm (so genannte „Spyware“) auf dem Rechner installiert, das alle Tastatureingaben aufzeichnet. Dadurch wird es dem Angreifer möglich, trotz der Verwendung verschlüsselter Datenübertragung (https://) dennoch die PIN, TAN bzw. TAC auszuspionieren, da diese sofort bei der Eingabe im Klartext aufgezeichnet werden.

Unmittelbar nach der Eingabe der vertraulichen Daten wird die Verbindung zur Bankseite abgebrochen (z.B. Error 404 – Seite kann nicht angezeigt werden) und die Daten werden an den Angreifer übermittelt. Das Fatale an dieser Methode ist, dass sich der User bis zum Zeitpunkt des Verbindungsabbruchs immer auf der Originalseite seiner Online-Bank befindet.

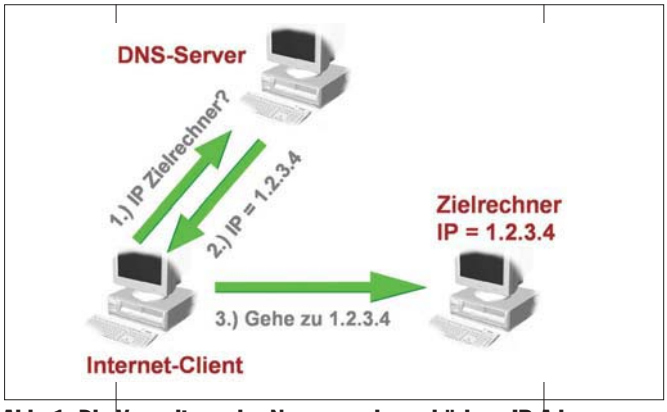


Abb. 1: Die Verwaltung der Namen und zugehörigen IP-Adressen wurde durch eigene DNS-Anbieter übernommen.

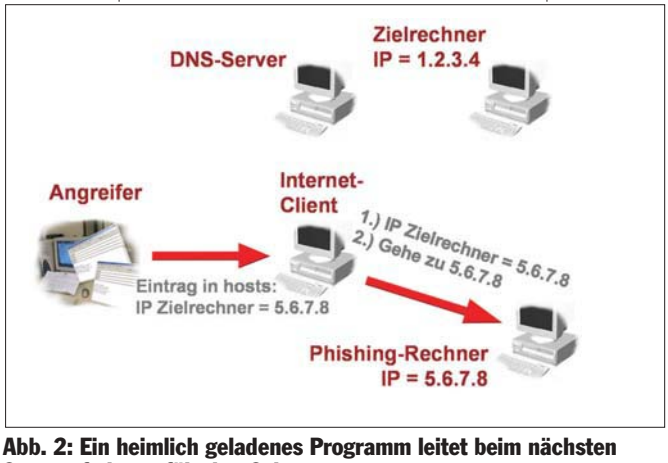


Abb. 2: Ein heimlich geladenes Programm leitet beim nächsten Start auf eine gefälschte Seite um.

Schutz vor Phishing. Allgemeine Tipps zum sicheren Surfen im Internet:

- Setzen Sie unbedingt ein Virenschutzprogramm ein. Dabei reicht es nicht aus, dass das Virenschutzprogramm auf dem Rechner installiert ist. Der Virenschutz muss auch aktiviert sein und vor allem müssen die zugehörigen Virensignaturdateien immer auf dem neuesten Stand gehalten werden. Neben einem aktuellen und aktiven Virenschutzprogramm ist es genau so wichtig, die von den Betriebssystem-, Webbrowser- und Mailclient-Herstellern angebotenen Sicherheits-Updates zu installieren.
- Der richtige Einsatz einer Firewallsoftware erhöht die Sicherheit vor unberechtigten Zugriffen auf den Rechner vom Internet aus.
- Beim Surfen im Internet sollten Sie nach Möglichkeit immer eine hohe Sicherheitsstufe (Verbieten des Ausführens von *Scripts* und *ActiveX,* bzw. Ausführung nur mit Eingabebestätigung) verwenden. Versierte Windows-Benutzer können zur Erhöhung der Sicherheit auch den Windows Scripting Host deaktivieren.
- Arbeiten Sie nach Möglichkeit nie mit Administratorrechten, wenn Sie im Internet surfen. Definieren Sie sich dafür auf dem Rechner (sofern das Betriebsystem es zulässt) ein eigenes Benutzerkonto mit eingeschränkten Benutzerrechten.
- Wenn eine sichere Verbindung zu einem Rechner aufgebaut wurde (erkennbar durch die Anzeige von https:// in der Adresszeile), sollten Sie durch einen Doppelklick auf das Schlosssymbol in der Statuszeile überprüfen, ob das verwendete Zertifikat gültig ist und tatsächlich vom Betreiber des Rechners ausgestellt wurde.
- Überlegen Sie sich, ob es wirklich notwendig ist, dass der Inhalt von E-Mail-Nachrichten unbedingt bunt und mit Bildern unterlegt präsentiert werden muss, oder ob es nicht ausreicht, den wichtigen Inhalt der Nachricht als Text dargestellt zu bekommen und für den Informationsgehalt der Mail notwendige Bilder als Dateianhänge zu behandeln.

Textmodus empfohlen. Stellen Sie daher als Standard-Nachrichtenformat für empfangene und zu versendende E-Mails den reinen Text-Modus ein. Damit kann ein mit dem Nachrichtentext verbundener Script-Code beim Aufruf der E-Mail keinen Schaden anrichten. Sollte der E-Mail-Client die Deaktivierung des HTML-Modus nicht ermöglichen, wechseln Sie sicherheitshalber ihre Client-Software (Informationen über sichere E-Mail-Clients finden Sie im Internet, nutzen Sie dabei nur Aussagen und Downloadseiten von vertrauenswürdigen Institutionen).

Um sicher gehen zu können, dass trotz der Einhaltung aller Sicherheitsmaßnahmen nicht Ihre Adresseneingaben auf Phishingseiten umgeleitet werden, kontrollieren Sie regelmäßig den Inhalt der Hosts-Datei. Sie finden die Datei bei Windows-Systemen unter dem Systempfad im Verzeichnis \drivers\etc (zum Beispiel: *c:\windows\system32\drivers\etc\hosts)*.

In dieser Datei befindet sich üblicherweise außer dem Vermerk des eigenen Rechners (127.0.0.0 localhost) kein weiterer Eintrag.

Zeilen, die mit dem Zeichen # beginnen, sind nur Kommentarzeilen und haben keine sicherheitsrelevante Bedeutung. Auf keinen Fall sollten Sie in dieser Datei Einträge von Ihrer Online-Bank oder anderen Dienstleistern vorfinden. Sollte dies der Fall sein, löschen Sie diese Zeilen sofort aus der Hosts-Datei.

Vor allem für Online-Banking-Nutzer ist erhöhte Vorsicht geboten. Es reicht nicht mehr aus, den Link zur Online-Banking-Startseite über die Adresszeile einzugeben:

- Achten Sie vor und bei der Eingabe vertraulicher Daten auf kleinste Unregelmäßigkeiten auf der Webseite Ihrer Online-Bank. Vor allem die Aufforderung zur Eingabe des PIN, TAN, TAC o.ä. an ungewohnter Stelle oder zu einem ungewohnt frühen Zeitpunkt sollte Sie misstrauisch machen.
- Prüfen Sie die angezeigte Adresse. Fehlen Teile der Adresse, die sonst vorhanden sind?
- Überprüfen Sie wie beschrieben regelmäßig die Hosts-Datei.

Robert Gottwald/Ernst Österreicher

Foto: Ti-Ms