Internet

Identitätsraub

Im Visier der Passwort-Fischer

Viren sind out – Identitätsraub ist in. Die gegenwärtig am schnellsten wachsende Form der Computerkriminalität ist «Phishing» – Fachjargon für professionelle E-Mail-Betrugsmaschen, die heute auch für erfahrene Anwender eine der grössten Internetgefahren darstellen. Die Methode hat Erfolg. Sicherheitsfirmen melden einen geradezu explosionsartigen Anstieg von Phishing-Aktivitäten im Web. Anlass genug für einen kurzen Überblick zum Thema und den wichtigsten Punkten, die es zu beachten gilt.

Thomas Vauthier
th.vauthier@bluewin.ch

Der Begriff «Phishing» ist eine Zusammensetzung der englischen Wörter *password* und *fishing* und bedeutet sinngemäss so viel wie «Fischen nach Passwörtern oder anderen sensiblen Daten». Mit verblüffend professionell gefälschten E-Mails und Webseiten von bekannten, überwiegend aus dem Finanzbereich stammenden Unternehmen versuchen Kriminelle, ihren Opfern vertrauliche Informationen wie etwa Bankzugangsdaten oder Kreditkartennummern zu entlocken. Die gestohlenen Zugänge werden dann von den Betrügern genutzt, um Geld auf eigene Konten abzuzweigen oder im Internet bestellte Waren auf Kosten des Opfers zu bezahlen.

Ablauf eines Phishing-Betrugs

Professionelle Betrüger richten auf einem eigenen oder gehackten Webserver eine täuschend echte Kopie einer bekannten Website ein. Die Betrüger wählen dabei meist Unternehmen, die finanzielle Dienstleistungen anbieten – etwa Banken, Kreditkartenfirmen, Online-Auktionshäuser und so weiter. Die Betrüger versenden im Namen des «gephishten» Unternehmens – zumeist dringliche – Aufforderungen zur Aktualisierung der Kontodaten oder andere Vorgänge, die die Eingabe der Zugangsinformationen erfordern. Damit die Phishing-Mails möglichst viele Empfänger erreichen, arbeiten die Betrüger zunehmend mit Spammern zusammen.

Klickt der Empfänger auf die in der Phishing-Mail enthaltenen Links, landet er auf der Site der Betrüger, die fast durch nichts von der Original-Site des Unternehmens zu unterscheiden ist. Die kopierte Site enthält eine gefälschte Kunden-Login-Seite, welche die dort eingegebenen Benutzernamen und Passwörter an eine von den Betrügern eingerichtete, nicht rückverfolgbare E-Mail-Adresse weiterleitet. Die gestohlenen Zugangsdaten nutzen die Betrüger, um die ihnen nun zugänglichen Konten zu plündern oder Online-Bestellungen vorzunehmen.

Wie erkennt man Phishing-Mails?

Waren die Phishing-Mails der ersten Generation noch durch Anfängerfehler wie ungeschickte oder fremdartige Formulierungen zu erkennen, so sind viele der heute versendeten Betrugsmails nahezu makellos und nur schwer von der offiziellen Korrespondenz des vorgegaukelten Unternehmens zu unterschieden. Dennoch: Auch die kleinsten Rechtschreib- und Grammatikfehler im Mailtext sollten den Empfänger Verdacht auf einen Betrugsversuch schöpfen lassen.
Da Phisher meist einen Vorwand benutzen, um ihre Opfer auf die von ihnen gefälschte Website zu locken, muss der Empfänger E-Mails mit dringlichen Aufforderungen in der Betreffzeile besondere Aufmerksamkeit schenken.
Einige Beispiele typischer Phishing-Mail-Betreffzeilen:
«Security Update», «Online Banking Alert», «Account Verification», «Important Security Issue!!!» und so ähnlich.
Bei verdächtigen HTML-Mails kann der Quelltext angezeigt werden, um die URL der enthaltenen Links zu überprüfen.

Beispiel:

```
<p>
Follow the link to make sure you
are on a secure eBay webpage.<br>
<A
HREF="http://phish.co.kr/signin/">
https://signin.ebay.com/ws/eBayISA
PI.dll?SignIn</A>
<p>
Thank you for using eBay!<br>
```

Hinter dem in der Mail angezeigten Link https://signin.ebay.com/... versteckt sich in Wirklichkeit die URL des Betrügers http://phish.co.kr/...

Wie schützt man sich vor Phishing-Betrügern?

Einen wirksamen Softwareschutz vor Phishing-Betrug gibt es derzeit nicht, auch wenn Softwarehersteller fieberhaft an praktikablen Lösungen arbeiten. Mit anderen Worten: Der derzeit beste Schutz besteht aus einer Kombination von hoher Aufmerksamkeit, einem gesunden Mass an Misstrauen sowie einigen wichtigen Regeln, die es zu beachten gilt:
Wenn Sie eine E-Mail erhalten, die vorgeblich von einer Bank, einem Kreditkartenunternehmen oder einem anderen Internetdienstleister stammt, bei dem Sie ein Konto führen, und diese Sie – meist dringlich – dazu auffordert, persönliche Daten einzugeben, sollten Sie

- auf gar keinen Fall Ihre vertraulichen Zugangsdaten in ein eventuell im Mail vorhandenes Formular eingeben.
- in der Mail keine Links anklicken, wenn Sie auch nur den leisesten Verdacht hegen, sie könnte gefälscht sein. Geben Sie stattdessen die Ihnen bekannte Firmen-URL direkt in die Adresszeile Ihres Browsers ein oder verwenden Sie Ihre Bookmarks. Sollte Ihr Dienstleister tatsächlich Daten von Ihnen bedürfen, dann wird er Ihnen das in der Regel nach dem Login auf der Website mitteilen.

Darüber hinaus sollten Sie grundsätzlich

- Betriebssystem, Browser und E-Mail-Programm stets auf dem aktuellsten Stand halten, inklusive aller verfügbaren Updates und Patches.
- eine Antiviren-Software verwenden, die über eine ständige, im Hintergrund laufende Virenprüfung verfügt und täglich mit neuen Viren-Signaturen versorgt wird.
- eine persönliche Firewall einsetzen.
- Online-Banking und E-Commerce-Transaktionen via PC in Internetcafés vermeiden.

Link zur Anti-Phishing Working Group mit nützlichen Infos:
www.antiphishing.org/

Fortsetzung folgt …