COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/sieben-tipps-fuer-dauerhaften-schutz,1908844

Phishing und E-Mail-Attacken

Sieben Tipps für dauerhaften Schutz

Datum: 23.10.2009
Autor(en): Thomas Pelkmann

Die Phishing-Attacken auf Zehntausende von Kunden bei Microsoft Hotmail, Google und schuelerVZ in den vergangenen Wochen zeigen die Sorglosigkeit der Nutzer und die Verwundbarkeiten von weit verbreiteten Diensten im Internet. Insgesamt kursierten wenigstens zeitweise rund 30.000 E-Mail-Zugangsdaten auf dem freien Markt.

Computeranwender nehmen Phishing und E-Mail-Attacken noch immer auf die leichte Schulter, sagt der Software-Hersteller Sophos.
Foto:

Für den erfolgreichen Angriff auf europäische E-Mail-Konten war dem Sicherheitsexperten **Sophos**[1] zufolge keine ausgeklügelte Hacking-Attacke nötig: Einfache Phishing-Mails, die massenweise an Accounts dieser Dienste geschickt wurden, genügten, um den Usern ihre Passwörter zu entlocken.

Laut Sophos wurden die E-Mail-Adressen vermutlich mithilfe eines alphabetischen und für Phisher typischen Verfahrens automatisch generiert. Das erkläre, warum nur solche Accounts von dem Angriff betroffen waren, deren E-Mail-Adressen mit "A" und "B" beginnen.

Einfältig bei der Passwortvergabe

Die Computersicherheitsexperten sehen in dem Vorfall einen Beleg dafür, dass sich Computeranwender noch immer nicht ausreichend der vielfältigen Sicherheitsgefahren im Web und nötigen Vorsichtsmaßnahmen bewusst sind.

Dafür spricht auch die Einfältigkeit, mit der die Inhaber vieler E-Mail-Accounts ihre Postfächer "schützen": Ein Forscher der Web-Sicherheitsfirma **Acunetix**[2] hat sich die Listen mit Passwörtern genauer angeschaut. Von rund 20.000 Accounts hatten 64 das gleiche Passwort, nämlich "123456". Andere nehmen kurze Duden-Wörter und Namen, die im Angriffsfalle in wenigen Sekunden zu knacken sind. Zu den Klassikern gehören auch Zeichenfolgen wie "password", "qwertz" oder "abc123".

Diese Attacke zeige, so das Online-Portal **TecChanncel**[3], dass Phishing-Angriffe noch immer äußerst lukrativ sein können. Verschärft werde die Problematik, weil immer mehr Firmen ihre Dienste an E-Mail-Konten koppelten. So setzt Microsoft beispielsweise für Dienste wie seine Support-Datenbank TechNet, für Xbox Live oder den MyPhone-Synchronisationsdienst auf Live-IDs und Hotmail-Konten. Google steuert via E-Mail Dienste wie Picasa, Google Groups und das Bezahlsystem **Google Checkout**[4]. Und Yahoo bietet nicht nur Zugriff auf Flickr, sondern auch auf **OpenID**[5]. Im schlimmsten Fall haben die Phisher somit Zugriff auf die komplette digitale Identität ihrer Opfer und könne solche Daten beispielsweise auch als Startpunkt für Social Engineering Attacken nutzen.

Zahlenkombinationen in Millisekunden entschlüsselt

Für den dauerhaufen Schutz von E-Mail-Konten gibt Sicherheitsspezialist Sophos die folgenden sieben Tipps.

1. Verwenden Sie schwer zu knackende Passwörter. Bei der Wahl eines Passworts sollten Sie auf Begriffe verzichten, die im Wörterbuch stehen oder sich einfach erraten lassen. Als sichere Variante gilt ein Mix aus mindestens zehn Ziffern, Buchstaben oder Sonderzeichen. Nutzer sollten dabei beachten, für jede geschützte Online-Anwendung Zugang ein anderes Passwort zu verwenden.

Die Internetseite 1Password hat ausgerechnet, wie lange die Entschlüsselung von Passwörtern dauert. Hochleistungsrechner schaffen eine Kombination von zehn Zahlen innerhalb von 0,059 Sekunden. Sechs Großbuchstaben kosten gerade einmal einen Aufwand 1,8 Sekunden. Richtig effizient ist erst die Kombination von Groß- und Kleinbuchstaben und Zahlen. An einer Passwortlänge von acht aus einem Vorrat von insgesamt 62 verschiedenen Zeichen arbeiten leistungsfähige Computer rund 15 Tage. Schon das Hinzufügen eines einzigen weiteren Zeichens hält die Rechner dagegen gleich zweieinhalb Jahre auf Trab - zu lange, um für Hacker-Attacken interessant zu sein.

2. Geben Sie niemals das Passwort für Ihren E-Mail-Account preis. Das gilt insbesondere für den Fall, dass Sie per E-Mail dazu aufgefordert werden. Kein seriöser E-Mail-Provider, keine Online-Shops oder Banken fragen persönliche Daten, wie Passwörter, PIN- und TAN-Nummern per E-Mail ab. Entsprechende Anfragen sollten Sie deshalb einfach nicht beantworten.

3. Vorsicht bei Eingabe sensibler Daten im Internet. Sind Sie auf eine in einer E-Mail verlinkte Webseite gegangen, überprüfen Sie, ob Sie dort die mittlerweile üblichen Sicherheitsmechanismen vorfinden: **HTTPS-Verschlüsselung**[6] und Verifzierung der Seite. Moderne Browser zeigen dies mittlerweile deutlich an. Geben Sie nie persönliche Daten auf unverifizierten, unverschlüsselten Seiten ein.

4. Überlegen Sie genau, wem Sie Ihre E-Mail-Adresse mitteilen. Je mehr Ihre E-Mail-Adresse im Internet Verbreitung findet, desto größer ist die Wahrscheinlichkeit, dass sie in Hände von Phishern und Spammern gelangt.

Passwörter nie speichern

5. Nutzen Sie mehrere E-Mail-Konten. Legen Sie sich zum Beispiel eine Haupt-E-Mail-Adresse zu, die Sie nur vertrauenswürdigen Personen wie Kollegen, Verwandten und Freunden nennen, nicht aber im Internet veröffentlichen. Weitere E-Mail-Accounts können Sie dann zum Anmelden in Foren, Online-Shops oder Social Communities verwenden.

6. Verwenden Sie einen Browser, der keine Passwörter speichert. Stellen Sie Ihren Browser, **zum Beispiel den Firefox**[7], so ein, dass sich bei jedem Schließen automatisch sämtliche Formulardaten und der Cache löschen.

7. Nutzen Sie stets aktuelle Schutz-Software. Gegen Malware, Phishing und Spam gibt es wirksame Anwendungen, die sich selbst regelmäßig aktualisieren, um die neuesten Bedrohungen zu erkennen. Aktivieren Sie unbedingt auch eine Firewall für Ihre Rechner.

Links im Artikel:

[1] **http://www.sophos.de/**
[2] **http://www.acunetix.com/**
[3] **https://www.tecchannel.de/**
[4] **http://checkout.google.com/**
[5] **http://de.answers.yahoo.com/question/index?qid=20080928062806AAXh5GV**

[6] **http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure**
[7] **http://www.firefox-browser.de/wiki/Einstellungen**
