



Phishing: Das größte Sicherheitsrisiko beim Online Daten-Klau bleibt der Mensch

Die Bundeskammer der Architekten und Ingenieurkonsulenten empfiehlt 10 goldene Regeln zum optimalen Schutz vor Phishing & Co

Wien, 02. Februar 2007 – Ein Bericht aus dem renommierten deutschen Fachmagazin für Informationssicherheit und Compliance „IT-Sicherheit“ bringt es auf den Punkt: „Das größte Sicherheitsrisiko bleibt der Mensch“. Derselben Ansicht ist auch Mag. Rudolf Unterköfler vom österreichischen Bundeskriminalamt zur Bekämpfung von Online-Kriminalität: „Das Sicherheitsbewusstsein beim Phishing ist europaweit stark gestiegen, nicht zuletzt durch die verstärkte Zusammenarbeit der Behörden auf internationaler Ebene. Dennoch bleibt als Schwachpunkt der Internet-Benutzer. Verstärkte Bewusstseinsbildung und Sensibilisierung sind von zentraler Wichtigkeit.“

Staatlich befugte IT-Ziviltechniker helfen

Sollte berechtigter Zweifel an der Vertrauenswürdigkeit des Computersystems oder ein konkreter Hinweis auf Viren, Würmer, Trojaner oder Spyware den Computer bestehen, kann es hilfreich sein, IT-Ziviltechniker beizuziehen, um weiterreichende Probleme zu verhindern. „Der beeidete IT-Ziviltechniker prüft und beurteilt Computersysteme in sicherheitstechnischen Fragen und gibt Empfehlungen ab, wie Systeme vor Angriffen effektiv geschützt werden können“, so Dr. Wolfgang Prentner, Vorsitzender der Bundesfachgruppe Informationstechnologie der Bundeskammer der Architekten und Ingenieurkonsulenten.

Die österreichische Wirtschaft investiert massiv in Sicherheitslösungen. So auch die heimischen Banken, die viel Geld zur Abwehr von potenziellen Angriffen auf ihre Internet-Banking-Systeme aufwenden. Allen kritischen Studien zum Trotz richten sich die Angriffe nicht mehr auf die technische Infrastruktur der Geldinstitute, für Angreifer sind unwissende und sicherheitstechnisch nicht interessierte Internet-Nutzer das deutlich lohnendere Ziel.

Laufende Untersuchungen und Überprüfungen zeigen, dass österreichische Bankinstitute modernste Sicherheits- und Verschlüsselungstechnologien einsetzen, um vertrauliche Kundeninformationen bestmöglich abzusichern. Dazu zählen kryptographisch sichere Fingerprints, Zufallsgeneratoren zur Erzeugung von sicheren PINs für die Anmeldung und TANs zur Autorisierung von Geldüberweisungen, die Erweiterungen der herkömmlichen Geldtransaktionsautorisierung zum iTAN (indizierte TANs) oder TAN+ Verfahren, die Einführung mobiler TAN-Nummern, die über das Handy an die Banking Benutzer gesendet werden, und nicht zuletzt die digitale Signatur erhöhen das Sicherheitsniveau. Kommuniziert wird heute über verschlüsselte SSL-Verbindungen mit sicherer 128-Bit Verschlüsselung, die dem aktuellen Stand der Technik entspricht.

Gefahren für Internet-Nutzer

Die aktuellen Gefahren sind vielen Internet-Nutzern bereits bekannt und bewusst, dennoch gibt es immer wieder erfolgreich durchgeführte Angriffe. Woran liegt das?

Die Gründe für erfolgreiches Phishing liegen vielfach im fehlenden Bewusstsein, der Leichtgläubigkeit der Kunden und dem Informationsdefizit, wenn sie z. B. per E-Mail oder über gefälschte Internetseiten aufgefordert werden, Benutzerkennung und Transaktionsnummern Preis zu geben.

Nahezu jeder Internet-Nutzer kann zum potenziellen Opfer des Online Daten-Diebstahls werden. Phishing stellt für alle Anwendungsbereiche im Internet eine Bedrohung dar, für deren Nutzung der Anwender persönliche Autorisierungsdaten benötigt. Beispiele dafür sind etwa Online-Bezahlsysteme, Internetshops und Versandhäuser aber auch Versteigerungsportale und Internet-Casinos. Die Berichterstattung fokussiert in letzter Zeit allerdings vor allem im Zusammenhang mit Internet-Banking, wo Betrüger und Hacker immer wieder versuchen, an heikle Daten wie persönliche Identifikationsnummern (PIN) und Transaktionsnummern (TAN) heranzukommen.

Virenschutz und Personal Firewalls

Virenschutz und Personal Firewall sollten zur Software-Grundausstattung jedes PCs gehören. Egal ob dieser „nur“ privat oder aber betrieblich genutzt wird. Personal Firewalls, die z.B. in den Betriebssystemen Windows XP und Vista bereits integriert sind, bieten in Verbindung mit einem Internet Security-Paket einen hohen Schutz vor Viren, Würmern, Spyware, Phishing und sonstigen Schädlingen.

Die 10 goldenen Regeln zum Schutz vor Phishing

Mit der Berücksichtigung von nur 10 goldenen Phishing-Regeln können Internet-Nutzer selbst aktiv zur Steigerung der Sicherheit beitragen:

Systemsicherheit

1. Nutzung vertrauenswürdiger Computer: Vergewissern Sie sich, dass nur Personen Ihres Vertrauens das Computersystem nutzen oder administrieren. Wickeln Sie niemals Bankgeschäfte über nicht vertrauenswürdige Computer ab.

2. Verwendung sicherheitsoptimierter Betriebssysteme und Browser: Nur gepflegte und gewartete Computersysteme sind gute Computersysteme – das Betriebssystem muss in regelmäßigen Abständen mit den neuesten Erweiterungen der Sicherheitssoftware (Patches) versorgt werden. Aktivieren Sie die automatischen Updates und den Phishing-Filter im Internet-Browser.

3. Einsatz von Virenschutz und Firewall: Verwenden Sie ein State-of-the-art Virenschutzprogramm mit automatischen Updates von Virensignaturen gegen Spyware, Viren und Trojaner. Installieren bzw. aktivieren Sie eine Personal Firewall zum Schutz Ihres Computersystems.

Sicheres Verhalten

4. Vertraulichkeit von PIN und TAN: Geben Sie die Login-Daten (PIN) und Geldtransferautorisierungsdaten (TAN) nur auf der überprüften Internet-Banking-Seite des Geldinstituts ein, zu dem eine Kontoverbindung besteht. Niemals dürfen diese vertraulichen Daten in E-Mails, Formularen oder unbekanntem Internet-Banking Systemen eingegeben werden.

5. Internet-Banking-Adresse der Bank (URL) nur manuell eingeben: Folgen Sie niemals Links aus E-Mails oder von anderen Internet-Seiten zum (vermeintlichen) Internet-Banking-Portal der Hausbank. Auch die Verwendung von Bookmarks birgt Gefahrenpotenzial, da sie von Hackern manipuliert werden können. Deaktivieren Sie die Auto-Vervollständigungsfunktion im Browser, um nicht versehentlich auf eine falsche Web-Seite zu gelangen.

6. Internet-Banking-Seiten prüfen: Die Webseite Ihrer Bank sollten Sie genau lesen und aufschreiben, damit Sie sie beim nächsten Einloggen sofort wiedererkennen. Achten Sie auf eine sichere, verschlüsselte Verbindung. Diese erkennen Sie daran, dass in der Adressleiste des Browsers „https://...“ angezeigt wird. Prüfen Sie auch, ob die Verschlüsselung mittels digitalem Sicherheitszertifikat aktiviert ist. Dazu genügt ein Klick auf das Schloss-Symbol im Browser rechts unten. Wird in der Adressleiste hingegen lediglich „http://...“ angezeigt, erfolgt die Übertragung von Daten unverschlüsselt und ist daher zu unsicher für Online-Bankgeschäfte.

7. Benutzer-PIN und TAN nicht am Computer ablegen: Verwahren Sie Ihre vertraulichen Bankinformationen an einem sicheren Ort. PCs sind dafür nicht unbedingt am besten geeignet. Sollten Sie PIN und TAN dennoch auf Ihrem Computersystem speichern wollen, dann nur verschlüsselt und niemals im Browser selbst!

Mögliche Gefahren beachten

8. Vorsicht bei angeblichen Banken E-Mails: Österreichische Bankinstitute versenden grundsätzlich keine E-Mails, in denen Kunden aufgefordert werden, vertrauliche Zugangs- und Transaktionsinformationen preiszugeben. Dazu zählen Verfügernummer, PIN und TAN. Bei dieser Art von E-Mails handelt es sich immer um Betrugsversuche.

9. Bankeninfos beachten und Vorfälle der Bank-Hotline melden: Beachten Sie die Sicherheitshinweise Ihrer Hausbank auf der entsprechenden Internet-Homepage. Sobald der Verdacht auf Betrug entsteht, geben Sie keinerlei Daten Preis und melden Sie Ihren Verdacht der jeweiligen Bank-Hotline. Bei sicherheitsrelevanten Vorfällen sollte der PIN schnellstmöglich über eine sichere Verbindung geändert werden.

10. Kontoauszüge regelmäßig prüfen: Überprüfen Sie in regelmäßigen Abständen Ihre Kontoauszüge auf Unregelmäßigkeiten. Achten Sie auch besonders auf E-Mails in denen angebliche Finanzagenten Ihnen einen Gewinn z. B. bei der Euro Millionen Lotterie ankündigen und Sie bitten, den zu hoch überwiesenen Betrag zu beheben und rasch an ein anderes Konto zu überweisen. Achtung: Sie werden hier zur Geldwäsche missbraucht und machen sich strafbar!



Dr. Wolfgang Prentner

Für weitere Informationen wenden Sie sich bitte an:

Bundeskammer der Architekten und Ingenieurkonsulenten

Referentin Frau Mag. Barbara Kroisz, Bundessektion Ingenieure

Vorsitzender Dr. Wolfgang Prentner, Vorsitzender der Bundesfachgruppe
Informationstechnologie

Karlsgasse 9/2, 1040 Wien

Tel.: (01) 505 58 07-0, Fax: (01) 505 32 11

Web: www.arching.at