

## newsletter

# zum Thema **Phishing** Sicherheitsbedrohung im Internet

**Das Ausspähen geheimer Informationen mittels gefälschter E-Mails und Websites hat sich in letzter Zeit zu einem nicht zu unterschätzenden Sicherheitsrisiko für die E-Mail- und Internetnutzung entwickelt.**

### **Einleitung**

Die Anzahl der Menschen, die über das Internet Einkäufe oder Bankgeschäfte tätigen, nimmt beständig zu. Entsprechend steigt der Verbreitungsgrad von Online-Banking und Online-Shopping via Internet in der Bevölkerung. So erledigen gemäß den aktuellen Zahlen des Bundesverbandes deutscher Banken (BdB) mittlerweile ca. 40 % der deutschen Bankkunden die Standardvorgänge ihrer Bankgeschäfte online.

In gleichem Maße wie sich die Nutzung des Internets immer mehr in alle Lebensbereiche und Geschäftsprozesse ausdehnt, nehmen auch kriminelle und betrügerische Aktivitäten zu. Seit mehreren Jahren sind Internetnutzer Viren, Trojanern, Würmern und anderen Arten der Computerkriminalität ausgesetzt. Noch relativ neu ist das so genannte Phishing, welches sich zur mittlerweile größten E-Mail Sicherheitsbedrohung entwickelt hat.

Auf Grund massiver Phishing-Attacken sah sich eine schwedische Bank dazu veranlasst, kurzfristig ihr Online-Banking zu schließen. In Deutschland wird mittlerweile in mehr als 1000 Fällen durch die Landeskriminalämter wegen Phishings ermittelt.

### **Begriffs- erklärung**

Der Begriff Phishing ist ein Kunstwort und leitet sich aus einer Kombination der englischen Worte „password“ und „fishing“ ab (zu deutsch: Abfischen von Passwörtern). Es handelt sich dabei um eine moderne Form von Trickbetrug über das Internet. Das Ziel einer Phishing-Attacke ist, Internetnutzer mittels gefälschter E-Mails auf einen Angreifer-Server zu leiten, um an sensitive oder geheime Informationen wie z.B. Passwörter, Kreditkartennummern oder Zugangskennungen zu gelangen.

Phishing-Mails ähneln im Erscheinungsbild sehr stark den Mails von Online-Providern oder Online-Banken. Meist enthalten diese E-Mails Links, durch die der Anwender auf eine vom Online-Betrüger erstellte Internetseite gelenkt wird. Diese gleicht nahezu der Seite des Originalanbieters. Häufig variieren die Adressnamen der Phishing-Sites nur geringfügig von den Originaladressen (z.B. www.ebay-ag.de statt www.ebay.de). Diese Tarnung und ein durchaus plausibler Inhalt des Mails wie z. B. die Neueingabe von Benutzerkennung und Passwort aufgrund einer Systemumstellung, sollen Anwender dazu verleiten, vertrauliche Daten preiszugeben. Da die Betrüger sehr geschickt ihre Identität verschleiern, erweisen sich die Ermittlungen als sehr schwierig.

## Ablauf einer Phishing-Attacke

In der Regel werden Phishing-Mails nicht gezielt an Einzelpersonen adressiert, sondern unter Zuhilfenahme von Massenversandtechniken verschickt, die durch die Spam-Versender bereits weit entwickelt sind. Je Phishing-Attacke werden Hunderttausende E-Mails versandt, die vortäuschen, von einer renommierten Organisation (Bank, Provider etc.) zu kommen. Der Versand geschieht dabei nach dem Zufallsprinzip, mit der Aussicht, dass zumindest ein bestimmter Anteil der Adressaten tatsächlich Kunden des entsprechenden Unternehmens sind.

Eine Phishing-Attacke hat typischerweise folgende Phasen:

- Der Angreifer besorgt sich die E-Mail-Adresse seiner potentiellen Opfer,
- Der Angreifer erzeugt eine E-Mail, die in ihrer Gestaltung der einer vertrauenswürdigen Institution (z.B. Online-Bank, eBay) nachempfunden ist und den Anwender zu Aktionen, wie einer Änderung oder Aktualisierung seiner Zugangsdaten auffordert,
- Der Angreifer versendet unter Verwendung einer falschen E-Mail-Absenderadresse die E-Mail an seine potentiellen Opfer (Massenmail) (z.B. userservicev@volksbank.de),
- In Abhängigkeit vom Inhalt der E-Mail füllt das Opfer ein Formular aus, besucht eine (gefälschte) Website oder öffnet angehängte Malware,
- Der Angreifer ist nun im Besitz sicherheitsrelevanter Daten (Passwörter, PINs, TANs, etc.) und kann nun diese mit dem Ziel der Bereicherung nutzen (Abbuchung vom Online-Konto, Einkauf in Online-Shops etc.).

## Aktuelle Zahlen

Im August 2005 wurden gemäß der Anti Phishing Working Group (APWG) weltweit rund 13.700 Aktionen (Phishing-Mail-Kampagnen) registriert. Die Anzahl der Phishing-Websites erreichte im gleichen Monat mit ca. 5.200 einen Höchststand (siehe Grafik). Die durchschnittliche Lebensdauer einer Phishing-Site betrug dabei laut APWG 5,5 Tage, was im Vergleich zu den Vormonaten einen leichten Rückgang bedeutete.

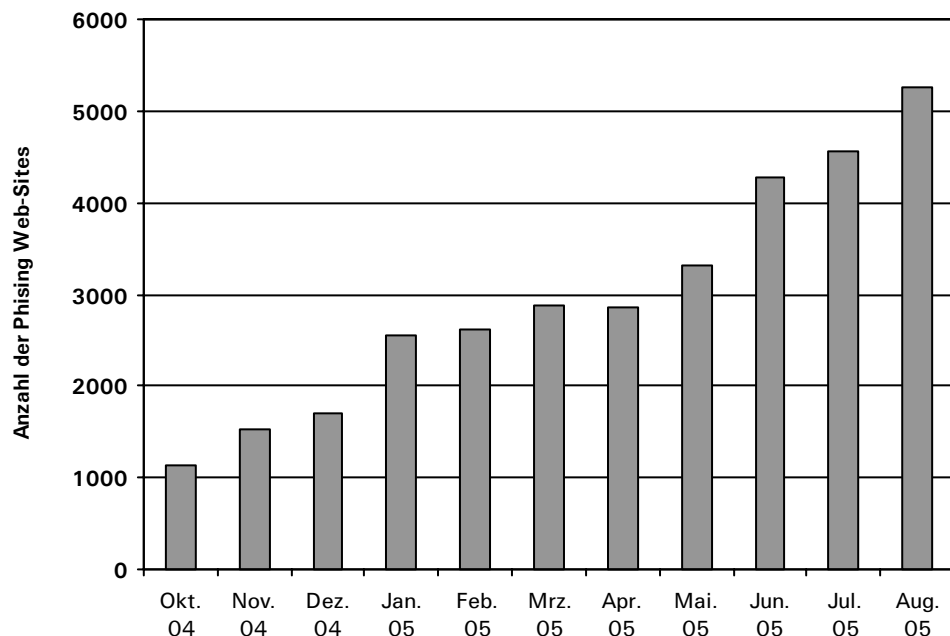


Abb.: Anzahl neuer Phishing-Websites (Okt. 2004 - Aug. 2005) Quelle: APWG

Gemäß den Angaben der APWG werden derzeit täglich 75-100 Mio. Phishing-Mails versandt. Man schätzt, dass knapp 20 % der Empfänger diese Mails öffnen und ca. 3-5 % auch Daten preisgeben.

### **Angriffsziele**

Am stärksten von Phishing-Attacken betroffen sind Finanzdienstleister. Dies gilt sowohl für die Anzahl der erfassten Phishing-Websites als auch für die Anzahl der attackierten Unternehmen. Die Verteilung der Phishing-Attacken nach Wirtschaftsbranchen gestaltet sich wie folgt (Quelle: APWG):

Finanzdienstleister	85,9 %
Internet-Service-Provider	5,6 %
Handel	2,8 %
Andere	5,7 %

Eine der ersten europäischen Banken, deren Kunden gezielt Phishing-Mails erhielten, war die Postbank in Deutschland. Jedoch auch Volksbanken, Sparkassen und andere große Geldinstitute sind in erheblichem Maße dieser Form der Computerkriminalität ausgesetzt.

So sind auch Kunden des Online-Auktionshauses eBay immer wieder Ziele von Phishing-Attacken. Bei zwei spektakulären Fällen konnten Betrüger mittels der durch Phishing erhaltenen Daten bei eBay Waren im Wert von nahezu einer Mio. Euro bestellen.

Für die betroffenen Unternehmen ergibt sich neben den finanziellen Einbußen auch zusätzlich ein Vertrauens- und Imageverlust, der sich insgesamt sehr negativ auf die Akzeptanz des E-commerce und des Online Banking auswirken kann.

### **Hinweise für das Underwriting**

Phishing-Attacken haben für den elektronischen Geschäftsverkehr ein beträchtliches Schadenpotential. Nicht selten entsteht durch Missbrauch der erschlichenen Daten ein erheblicher Schaden für Internetnutzer.

In 2004 sind nach Schätzungen der Gartner Group (USA) durch Phishing den Banken und Kreditkartenunternehmen bereits Schäden in Höhe von insgesamt 1,2 Mrd. \$ entstanden. Andere Schätzungen gehen in diesem Zusammenhang sogar von beträchtlich höheren Schadenssummen aus.

Eine noch stärker zielgerichtete Phishing-Variante, das sog. „spear fishing“, zielt darauf ab, Mitarbeiter in Unternehmen dazu zu bewegen, ihre Passwörter und Zugangs-Codes zum Unternehmensnetzwerk preiszugeben. Durch den Einsatz von ständig variierenden und weiterentwickelten Phishing-Attacken, die auch z. T. mit Spy- und Malware kombiniert werden, erhöht sich die Gefahr, dass betriebliche Daten und Kundendaten erspäht und manipuliert werden.

Entsprechend kann sich die Exposure für Deckungen, die IT-Eigen- und/oder Fremdschäden versichern (wie z. B. Computer Crime Versicherung) erhöhen. Grundsätzlich ist wichtig festzustellen, dass nicht ausreichender Schutz von IT-Systemen gegen unbefugten Zugriff, z.B. wenn das Passwort- und Identifikationskonzept nicht dem Stand der Technik entspricht, durchaus zu Haftungsansprüchen gegen Betreiber solcher IT-Systeme führen kann.

### **Kontakt**

AssTech GmbH  
Postfach 1211  
85766 Unterföhring bei München  
Telefon + 49 89 3844-1585  
Telefax + 49 89 3844-1586  
info@asstech.com  
www.asstech.com