Informationen zur Internet-Sicherheit

Teil 1: Sicherheit im Allgemeinen

Das Thema Sicherheit hat nicht zuletzt durch ein mittlerweile allseits bekanntes „I Love You“ an Bedeutung gewonnen und ist dadurch intensiver in das Bewusstsein nahezu jedes Internet-Surfers vorgedrungen. Neben anderen kleinen Tierchen und Konsorten, wie Viren, Würmern, Trojaner wollen wir im Rahmen unserer „Sicherheits-Serie“ Möglichkeiten aufzeigen wie Sie sich, Ihre Daten und Ihren PC schützen können bzw. Sie im Hinblick auf das Thema Sicherheit sensibilisieren.

Dabei muss erhöhte Sicherheit nicht immer gleichzusetzen sein, mit eingeschränktem Komfort. Aber bilden Sie sich einfach selbst Ihre Meinung und treffen Sie eine Einschätzung welche Vorkehrungen Sie an Ihrem PC treffen sollten oder welche nicht.

Im Rahmen unserer Reihe werden wir in den kommenden Wochen folgende Themen behandeln:

1. **SPAM** bzw. unerwünschte Nachrichten
2. **Sicheres OnlineBanking** - Grundlagen
3. **Dialer** – wie kann ich meine Telefonkosten im Griff behalten
4. **Viren** – nicht nur Organismen die sich auf Personen übertragen
5. **Tojaner** – bereits dem alten Troja zum Verhängnis geworden
6. **Würmer** – nicht nur für Fische verhängnisvoll
7. **Zusammenfassung und Sammlung einiger Links zum Thema „Sicherheit im Internet“** sowie **Feedback & Stimmungsabfrage**

Die von uns zusammengestellten Themen erheben natürlich nicht den Anspruch auf 100%tige Vollständigkeit. Vielmehr soll Ihr Interesse und Ihre Aufmerksamkeit im Hinblick auf diesen nicht zu vernachlässigenden Bereich gelenkt werden.

Im Rahmen unserer Serie wollen wir aktuelles Thema aufgreifen, welches uns bereits in unserer täglichen Praxis von einigen Kunden geschildert wurde. Dieses „Problem“ lässt sich jedoch relativ einfach und unkompliziert lösen. Lesen einfach selbst …

1. SPAM bzw. unerwünschte Nachrichten

Als SPAM bzw. SPAMMING wird die unerwünschte Direktwerbung per E-Mail bzw. das unaufgeforderte massenhafte Verbreiten von Informationen auf elektronischem Weg verstanden. Auch eine Verbreitung über den in Windows integrierten Nachrichtendienst ist möglich.

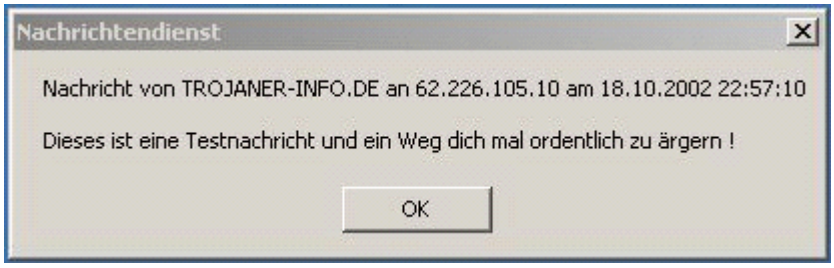
Man könnte **SPAM** auch direkt mit dem Begriff „Werbemüll“ bezeichnen. Beim Versand des „Werbe-Mülls“ oder auch „Werbe-Mails“ wird die E-Mail-Adresse des Internet-Nutzers benötigt. Diese kann der „Übeltäter“ auf unterschiedliche Art und Weise erlangen, das Ergebnis ist jedoch immer das gleiche.

Der Datenmüll erzeugt bei den Providern enorme Datenvolumen und das Postfach des Nutzers wird evtl. je nach Größe der Werbe-Mails lahm gelegt bzw. der Nutzer wird unter Vortäuschung falscher Tatsachen (Absendername bzw. Betreffzeile) dazu verleitet auf einen in der Mail hinterlegten Link zu klicken, der ihn auf „ungewollte“ Seiten (Sex- oder Casinoseiten) bringt.

Im schlimmsten Fall lädt sich der Nutzer einen sogenannten „**Dialer**“ (kleines Einwahlprogramm) auf seinen Rechner, der unbemerkt als Standardverbindung ins Internet eine teure 0190-Nummer installiert und dadurch die Telefonrechnung des Surfers unbemerkt ins Uferlose treiben kann (diese Problematik wird Thema des dritten Teils unserer Serie sein).

Aber nicht nur durch E-Mails, sondern auch durch direkten Nachrichten-Versand kann der Nutzer irritiert bzw. geschädigt werden. Gerade durch die starke Verbreitung der Windows-Betriebssysteme ist es möglich gleichzeitig einer Vielzahl von Internet-Usern zu schaden. Dies geschieht auch im Falle des „**Windows-Nachrichtendienstes**“. Mit diesem von Microsoft in Windows integrierten Dienst ist es „Spammern“ (Personen, die durch den Versand von Massen-E-Mails Schaden anrichten) möglich, Usern ungewünschte Nachrichten zukommen zu lassen, die mit Ihrem PC direkt mit dem Internet verbunden sind, also ohne zwischengeschaltete „Firewall“.

Eine solche Nachricht sieht in etwa wie folgt aus:



Die Spammer benötigen nicht einmal, wie bei klassischer „Spam“, E-Mail-Adressen der Opfer; die „IP-Adresse“ (Weltweit eindeutige Adresse für an das Internet angeschlossene Rechner. Eine IP-Adresse besteht aus vier Byte, die durch Punkte getrennt sind: z. B. 194.95.179.205) reicht vollkommen aus.

Nachdem diese neue Spam-Methode in den USA bereits im großen Stil eingesetzt wird, erreichen 'http://www.heise-online.de' die ersten E-Mails Betroffener aus Deutschland. Der Windows-Nachrichtendienst dient eigentlich dazu, im „lokalen Netzwerk“ Sofortnachrichten zu verbreiten.

XP installiert diesen Nachrichten-Dienst per Default, also automatisch und ruft ihn bei jedem Systemstart im Hintergrund auf. Auch Windows 2000 enthält den Dienst und startet ihn beim Hochfahren. In anderen Windows-Versionen lässt sich der Dienst ebenfalls installieren; dort ist er aber nicht automatisch aktiv. In englischen Windows-Versionen nennt sich der Dienst „Messenger“. Dies hat jedoch nichts mit dem hauseigenen „Instant Messenger“ zu tun.

UnsereTipps für Sie:

1. Grundsätzlich sollten Sie eine „Firewall“ installiert haben. Diese Art von Software verhindert den Zugriff aus dem „Netz“ auf Ihren PC bzw. lässt diesen nur mit Ihrer Einwilligung zu. Auf der anderen Seite verhindert diese Software ebenfalls den Zugriff von Progammkomponenten Ihres Rechners in das Internet sofern Sie dies nicht wünschen.

   Ein empfehlenswertes Programm bietet die **Firma Zone Labs** im Internet unter www.zonelabs.com an. Einziges Manko, das Programm ist auf Englisch, wird jedoch regelmäßig aktualisiert und kostet nichts. Eine deutsche Konfigurationsanleitung finden Sie unter www.computec.ch/dokumente/firewalling/zonealarm-handbuch/

Aber auch Programme von **Symantec** http://www.symantec.de oder **McAffee** http://www.mcaffee.de bieten diese Funktionen, jedoch gegen Bezahlung, an. Der Preis für eine Komplettpaket Firewall & Virenschutz liegt hier bei ca. 80 Euro.

2. Im Hinblick auf SPAM per Windows-Nachrichtendienst beachten Sie bitte folgende Punkte:

   Deaktivieren Sie den Windows-Nachrichten-Dienst in Ihrem Windows-Betriebssystem, falls dieser aktiviert sein sollte. Eine Anleitung zur Deaktivierung des Nachrichtendienstes gibt es z.B. unter http://www.trojaner-info.de/nachrichtendienst/index.html

3. Im Hinblick auf SPAM per E-Mail beachten Sie bitte folgende Punkte:

   - **Legen Sie sich ein zweites E-Mail-Postfach an.**
     Kostenfreie E-Mail-Adressen gibt es z. B. bei http://www.web.de.
     Nutzen Sie das eine Postfach für die Kommunikation mit Freunden usw. und das zweite verwenden Sie im Internet überall dort wo die Eingabe einer E-Mail-Adresse erforderlich ist.
   - **Nutzen Sie den „SPAM-Schutz“ Ihres E-Mail-Anbieters.**
     Kostenlose Maildienste sind ein beliebtes Ziel von Werbeversendern. Auch wenn Sie Ihre neue Adresse an niemanden weitergegeben haben, kann es sein, dass Sie schon innerhalb von kürzester Zeit mit unerwünschten Nachrichten belästigt werden. Abhilfe schafft hier der Spam-Schutz. Bei Hotmail heißt dieser Dienst zum Beispiel "Junk-Mail-Filter", bei GMX müssen Sie unter Optionen "AntiSpam" aktivieren.
   - **Fallen Sie nicht auf falsche Absenderangaben oder Betreffzeilen herein!**
     Bevor Sie Mails mit dem Absender „Volksbank“, Kundenservice, Rechtsabteilung usw. oder mit den Betreffzeilen wie "Re: Ihre Anmeldung", "Will Dich wiedersehen" oder "Sie haben gewonnen!" öffnen, sollten Sie diese am sichersten löschen. Haben Sie die Mail bereits geöffnet, dann vermeiden Sie unbekannte darin enthaltene Links anzuklicken. Oft sollen die Absenderangaben bzw. die Betreffzeilen lediglich die Aufmerksamkeit des Nutzers wecken und halten nicht, was sie versprechen bzw. bringen böse Überraschungen mit sich.