

**Immer mehr Gefahren durch E-Mails, Viren,  
Hacker, Dialer, Trojaner und unvorsichtige  
Benutzer.**

**Das kleine E-Mail 1 x 1**

- Mails sind **n i c h t** absolut zuverlässig bezüglich der Übertragungsdauer, Lesbarkeit und der Übermittlung überhaupt. Der Aspekt der Ausspionierung sei hier noch nicht einmal berücksichtigt. Es lässt sich kaum voraussagen wie und über welche Server eine Mail wann und ob überhaupt weitergeleitet wird. Und deshalb gibt es auch eine maximale Bearbeitungsdauer nicht. Ein durch Virenversand überlasteter Mailserver im Internet kann unter Umständen mehrere Stunden brauchen um zu reagieren. Eine Möglichkeit zur Prüfung auf Erhalt wäre die Lesebestätigung. Sie wird jedoch nicht von allen Benutzern oder Administratoren zugelassen, also zurückgeschickt.
- Aber : Nicht zustellbare Mails kommen in 99% der Fälle immer mit einer DAEMON-Meldung zurück. (550: unknown user . ...., Quota Exceeded = Postfach übertoll )
- Viren versenden sich inzwischen von befallenen Systemen aus unter einem beliebigen Absendernamen ( wer eben gerade aus dem Adressbuch ausgewählt wird). Darum bekommen auch Sie immer öfter von gesicherten Systemen die Meldung . „... sie haben uns eine verseuchte E-Mail geschickt ... „, oder ähnlich.
- Viren kommen in sehr vielen Fällen von Bekannten oder Geschäftspartner, da sich die Viren über Adressbucheinträge in Mail-Programmen verbreiten, wenn diese Programme nicht ausreichend gesichert sind. Aber auch über einen Dritten wie im vorgenannten Beispiel.
- Man sollte sich angewöhnen E-Mails immer zuerst vom Betreff her zu lesen und nicht zuerst jeden Anhang auszuführen bzw. zu öffnen. Allein im Betreff steht oft schon nichts Sinnvolles. Im E-Mail Text stehen dann auch meist nur allgemeine (englisches) Phrasen. Der Anhang sind dann sehr häufig Dateien mit dem Anhang PIF, SCR, VBS, EXE
- Die gefährlichsten Anhänge sind z.B. : VBS, EXE, COM, SCR, PIF, CLSID ( lange Zahlen+Buchstabenreihen), CMD, URL ( sie zeigen auf verseuchte Seiten oder bösartige Programme im Internet), MSI, REG, JS, DLL. Aber auch in einem ZIP-Archiv oder einem WORD oder Excel, Powerpoint-Dokument kann ein Virus schlummern.

- Aber: Viele Viren werden sogar schon aktiv, wenn Sie nur die Vorschau/Voransicht in Ihrem Mailprogramm aktiviert haben. Sie brauchen die Mail also nicht einmal zu öffnen.
- Wenn auch nur ein Benutzer in Ihrer Firma sich nicht an die Vorgaben hält, kann Ihr gesamtes Firmennetz von Viren befallen und geschädigt werden.
- Die meisten Viren nutzen zu Ihrer Verbreitung einen sogenannten „EXPLOIT“. Das sind kleine Programmlücken, die i.d.Regel bewusst durch einen „künstlich“ erzeugten Ausnahmezustand erzeugt werden.
- Es werden grundsätzlich von keinem Hersteller unaufgefordert Programm-Updates oder sogenannte Sicherheits-Update verschickt. Ebenso unsinnig ist es mit einem per E-Mail erhaltenen Passwort irgendeine ZIP-Archive oder Programme zu öffnen, wenngleich dies der Absender auch suggerieren möchte.

## **Immer mehr SPAM**

Die Spammer werden heute immer aufdringlicher und die SPAM-Mails immer schwerer zu blocken. Sie wollen zumeist etwas verkaufen und es entstehen ihnen auf diesem Weg praktisch keine Kosten für das Versenden.

Spammer ändern ständig Ihre Absenderadresse und auch den Mailserver über welchen sie verschicken. Es gibt unzählige „offene Relays“, über die jeder unter jedem Namen versenden kann. Die SPAM-Stichworte werden jedes Mal minimal verändert. So wird aus Million, Million, Mill!ion, Mi!!;on, ..... Alle diese möglichen Schreibweisen lassen sich gar nicht alle in einen entsprechenden SPAM-Blocker eingeben.

Häufig werden nur Bilder als Inhalt verschickt und ein Bild lässt sich praktisch nicht (nur schwer, aufwendig) nach entsprechenden Textteilen durchsuchen-. Viele Spammer versenden nur Links, d.h. beim Öffnen der Mail wird eine Verbindung zu Webseite aufgebaut und damit weiß der Spammer schon, dass diese Mail-Adresse auch existiert.

98% der Internet-Präsenzen haben eine [INFO@xxxxxx](mailto:INFO@xxxxxx) - Mailadresse. D.h. sind die einfachste Angriffsfläche für einen Spammer. Diese Mail kommt garantiert an. Zusätzlich sind auf den Webseiten jeder Präsenz mehrfach viele Mailadressen hinterlegt, sodaß automatische Programme diese Adressen quasi nur noch einzusammeln brauchen. Es gibt jedoch auch Möglichkeiten diese Mailadressen zumindest vor diesen Adress-Scannern zu verbergen. Fragen Sie uns wie Sie sich schützen können.

## Dialer, Trojaner und Konsorten

Dialer hatte man bisher recht schnell auf einem Rechner. Inzwischen hat sich die rechtliche Lage gebessert und es muss deutlich der Installation zugestimmt werden bevor ein Dialer installiert werden kann. Auch die Kosten für die Nutzung der Dialer sind nun nach oben begrenzt.

Es kann sich ein Dialer aber nur dann einwählen, wenn auch die Infrastruktur stimmt. D.h. er benötigt eine angeschlossene ISDN-Karte oder eine analoges Modem. Per DSL kann er sich nicht verbinden. Er wählt i.d.Regel teure Telefonnummern und das geht eben nur mit Modem oder ISDN-Karte.

Trojaner hat man hingegen noch schneller auf seinem System und sie können sich mit jeder Internet-Verbindung auch nach draussen verbinden. Deshalb sollte man grundsätzlich im Internet-Explorer entsprechend höhere Sicherheitseinstellungen nutzen und gelegentlich mit einem speziellen Programm nach bereits „eingenisteten“ Trojanern suchen. Da nur die wenigsten Trojaner auch eine virenähnliche Schadensfunktion haben werden auch nicht alle von ihnen durch Virens Scanner gefunden und beseitigt.

## Darum sollten Sie sich schützen :

durch

1. Aktuelle Software-Versionen mit den aktuellsten Service-Packs und Sicherheits-Patches ( Hotfix)
2. Virenschutz für E-Mail-Anhänge und Datei-Viren ( per Diskette, CD, DVD, USB-Geräten)
3. Firewalls um Hackerangriffe während der Online-Verbindung abzuwehren
4. SPAM-Blocker um nach gewissen Worten und Inhalten zu suchen und diese Mails zu löschen

**Fragen Sie uns! Wir sind die Profis hierfür und helfen Ihnen garantiert weiter .**



**MÜLLER-IT**  
Ingenieurbüro für Inform@tions-Technologie

Hofgartenstrasse 3  
Tel 07139 / 45 20 80

74196 Neuenstadt  
Fax 07139 / 45 20 81

weitere Infos unter [www.mueller-it.com](http://www.mueller-it.com)

**Microsoft®**  
**CERTIFIED**  
Systems Engineer