

Virenschutz

Selbstverständlich können Sie sich einen Mac anschaffen oder nur noch mit dem Betriebssystem Linux arbeiten oder MS-Outlook nicht mehr verwenden. Dadurch würden Sie einen ziemlich großen Schutz vor Viren erhalten.

Jedoch sieht der Büro-Alltag anders aus: In sehr vielen Büros werden PCs mit dem Betriebssystem Windows und der Anwendung MS-Outlook verwendet. Die Gefahren, die durch diese Konstellation entstehen, sind nicht unerheblich. Durch Viren können ganze Mail-Systeme von Firmen lahmgelegt werden. Viren können mitunter erhebliche Kosten verursachen, verunsichern die Kollegen und Mitarbeiter und führen zu einem oftmals dramatischen Produktionsverlust! Daher tut Aufklärung Not und ein wirksamer Schutz ist unerlässlich.

Bei einem Computervirus handelt es sich um ein kleines Programm, das meist - in einem „Wirtsprogramm“ versteckt - in das System eingeschleust wird und dort großen Schaden anrichten kann. Das Virenproblem sollte zwar nicht überbewertet werden, doch auch für Verharmlosung gibt es keinen Grund. Denn derzeit existieren mehr als 50.000 verschiedene Viren, von denen inzwischen mehr als die Hälfte als gefährlich einzustufen sind. Und: Jede Sicherheit ist trügerisch, denn Monat für Monat kommen viele neue (mehr oder weniger) gefährliche Virenexemplare hinzu. Inzwischen existieren im Internet sogar schon Seiten mit Anleitungen für die Programmierung von Viren.

Die wichtigste Grundregel lautet daher: Installieren Sie unbedingt ein Virenschutzprogramm z. B. von www.norton.de, www.mcafee.de oder www.antivir.de (**kostenlos für Privatanwender**)

- ✓ das die Festplatte auf Viren untersuchen kann,
- ✓ das mit einem Schutzmechanismus auch Daten untersucht, die Sie gerade im Dateisystem ablegen,
- ✓ das Ihre ein- und ausgehenden E-Mails auf Viren untersucht,
- ✓ das mind. wöchentlich ein update zulässt und
- ✓ das mind. wöchentlich ein kompletten Scan der Festplatte ermöglicht.

Doch bedenken Sie: Auch das beste Schutzprogramm ist immer nur gegen bekannte Viren wirksam, gegen neue Viren ist es bis zur Aktualisierung machtlos. Folglich bleibt auch bei einem hochwirksamen Virenschutz immer ein gewisses Restrisiko. Deshalb sollten Sie die folgenden Regeln zur Abwehr von Viren beachten, um auch dieses Risiko zu minimieren. Am besten machen Sie auf diese Regeln durch einen Aushang in Sichtweite der PCs aufmerksam. So werden Sie und Ihre Kollegen ständig an die Gefahren durch Viren erinnert.

Weitere Infos finden Sie auf www.bsi-fuer-buerge.de (Homepage des Bundesamtes für Sicherheit in der Informationstechnik)

Die wichtigsten Regeln für den Virenschutz

1. Eine **Diskette (auch eine fabrikneue!)** sollten Sie **nie ohne einen Virencheck** in das Laufwerk legen. Auch fremde Datenträger sollten Sie immer prüfen. Disketten oder **selbst gebrannte CDs** mit Programmen „vom Nachbar“ oder von „einem Freund“ dürfen auf keinen Fall ohne einen Virencheck eingesetzt werden. Übrigens exakt auf diese Weise verbreitet sich die eine Hälfte der Viren, die andere über das Internet!
2. **E-Mails**, die bereits im Betreff Dinge enthalten, die ganz sicher **nicht firmeninterner Natur** sind (insbesondere in anderen Sprachen, wie "Visit Russian Ladies" oder „Farn 1 Million \$ per month“), sollten **sofort gelöscht** werden.
Generell gilt: Eine E-Mail von einem unbekanntem Absender oder in einer fremden Sprache, die einen Anhang enthält, sollte man mit größter Vorsicht behandeln. Besonders gefährlich sind aber Computer-Würmer, die die **Ab-senderadresse fälschen**. Daher scheinen die Mails von bekannten und vertrauenswürdigen Absendern zu kommen. Wenn Sie also nicht sicher sind, ob die Mail einen Virus enthält, löschen Sie diese und informieren Sie den Versender.
Das Öffnen der E-Mail selbst ist noch nicht so gefährlich (es gibt allerdings schon einige wenige Viren, die sich beim Öffnen der E-Mail verbreiten), sondern nur das Öffnen eines Anhangs. Daher ist das Löschen einer verdächtigen E-Mail immer noch das wirksamste Mittel!
3. **Anhänge** einer fragwürdigen E-Mail dürfen auf keinen Fall geöffnet werden und müssen sofort incl. E-Mail **gelöscht** werden, wenn sie folgenden Dateityp aufweisen:

✓ .EXE	✓ .BAS
✓ .COM	✓ .CMD
✓ .VB? (das ? steht für ein beliebiges Zeichen)	✓ .HLP
✓ .WS? (das ? steht für ein beliebiges Zeichen)	✓ .CPL
✓ .BAT	✓ .LNK
✓ .PIF	✓ .REG

Bei diesen Dateien handelt es sich um so genannte ausführbare Dateien unterschiedlicher Art, die sofort auf Ihrem System gestartet werden und Viren - wenn welche enthalten sind - auch sofort in das System eindringen lassen. Bei dieser Auflistung handelt es sich um die wichtigsten gefährlichen Typen. Auch die beliebten Bildschirmschoner (.scr) können Viren enthalten! Setzen Sie daher nie einen Bildschirmschoner ohne vorherigen Virentest ein.
Doppelnamen sind ganz gefährlich etwa NAME.DOC.EXE - hier will Sie einer dadurch veralbern, dass er eine gefährliche Datei mit einem harmlosen Namen tarnt. Schlagen Sie ihm ein Schnippchen! Der berühmte ILOVEYOU-Virus beispielsweise war so in einem „unverdächtigen“ Anhang namens versteckt: LOVE-LETTER-FOR-YOU.TXT.vbs (das kleingeschriebene vbs war die Bombe!)
4. **Anhänge** sind dann als **(relativ) ungefährlich** einzustufen, wenn sie folgenden Dateityps sind und von einem internen Absender kommen. Erhalten Sie Dateien mit den folgenden Dateitypen von externen Absendern, können auch diese Viren enthalten (beispielsweise Makro-Viren in Word-Dokumenten oder Script-Viren in PDF-Dateien):

✓ .DOC (Word-Dokument)	✓ .PCX (älteres Grafikformat)
✓ .DOT (Word-Dokumentvorlage)	✓ .BMP (Bitmap-Grafik)
✓ .XLS (Excel-Dokument)	✓ .PDF (Acrobat-Dokument)
✓ .XLT (Excel-Vorlage)	✓ .ZIP (komprimierte Datei)
✓ .PPT (PowerPoint-Dokument)	✓ .TXT (allgemeine Textdatei)
✓ .MDB (Access-Datenbank)	✓ .JPG (Internet-Grafik)
✓ .GIF (Internet-Grafik)	✓ .JPEG (Internet-Grafik)

Speichern Sie diese Anhänge immer in einen separaten Ordner (z. B. mit dem Namen „E-Mail-Anlagen“). **Erst** nach einem **Scan** über den Windows-Explorer dürfen diese Dateien geöffnet werden.
5. **Vorsicht bei HTML-Mails**, denn in einer derartigen E-HTML-Mails (Sie erkennen sie daran, dass sie farbige Elemente oder Abbildungen enthält) können im HTML-Code gefährliche Elemente enthalten sein. Abonnieren Sie Newsletter im Format „Nur Text“, damit Newsletter Sie die potenziell gefährlichen HTML-Mails besser erkennen können.
6. Unterlassen Sie bitte die bekannten **Scherzprogramme oder Hoax-Mails**, die einen Virenbefall vortäuschen. Sie verunsichern nur und lenken von der eigentlichen Gefahr ab. Falls Sie eine Virenwarnung erhalten, prüfen Sie über die Viren-Bibliotheken auf der Site von www.norton.de oder www.mcafee.de die Echtheit der Warnungen. Wirken Sie auch auf allzu sorglose Kollegen ein. Bedenken Sie, dass deren Nachlässigkeit sich auch auf Ihre Arbeit auswirken kann!

Noch ein kleiner Tipp

Um die **MS-DOS-Namen** sichtbar zu machen, sollten Sie auf jeden Fall im Windows-Explorer die Option zum Ausblenden der Dateierweiterung deaktivieren. Da diese Option in den verschiedenen Windows-Versionen an unterschiedlichen Stellen hinterlegt ist und damit Sie nicht lange suchen müssen, lesen Sie in der kleinen Aufstellung, wo sich die Option in Ihrem Windows-Betriebssystem befindet:

Version	Menü
Windows 95	Ansicht -> Optionen -> Ansicht -> Keine MS-DOS-Erweiterung für registrierte Dateien
Windows NT	Ansicht -> Optionen -> Ansicht -> Keine Erweiterung für registrierte Dateien
Windows 98 Windows Me Windows 2000	Extras -> Ordneroptionen -> Ansicht -> Dateinamenerweiterung bei bekannten Dateitypen ausblenden
Windows XP	Extras -> Ordneroptionen -> Ansicht -> Erweiterung bei bekannten Dateitypen ausblenden