

# Aufklärungsblatt: Viren und Würmer

In den vergangenen Jahren wurden durch Computerviren und -würmer immer wieder große Schäden verursacht. Diese Schäden können auf Deinem eigenen Computer entstehen, aber auch auf anderen PCs verursacht werden, die von dem Virus / Wurm von Deinem PC aus angegriffen werden. Deshalb ist es wichtig, dass Du Deinen PC vor Viren und Würmern schützt!

Auf den folgenden Seiten findest Du Erklärungen, was Viren und Würmer sind, wie man sie bekommt und wie man sich dagegen schützen kann.

Bitte lies Dir die Erklärungen aufmerksam durch. Falls Du weitere Fragen hast, werden wir Dir gerne helfen.

## Inhalt:

1. Was sind Viren / Was sind Würmer?
2. Wie bekomme ich einen Virus?
3. Was machen Viren?
4. Warum muss ich mich vor Viren schützen?
5. Ich habe ein Antivirus-Programm installiert. Kann mir jetzt nichts mehr passieren?
6. Wie kann ich mich vor Viren schützen? Was muss ich beachten?
7. Fazit
8. Weitere Informationen

## 1. Was sind Viren / Was sind Würmer?

Viren sind kleine Programme, die sich meist selbständig und ohne Wissen des Nutzers auf einem Computer installieren. Als Wurm bezeichnet man diese Programme dann, wenn sie sich z.B. durch das Versenden von Kopien per Mail selbstständig verbreiten.

Für den betroffenen Rechner unterscheiden sich Viren und Würmer kaum. Deshalb wird im Folgenden nur noch von Viren gesprochen.

## 2. Wie bekomme ich einen Virus?

Viren verbreiten sich für gewöhnlich über das Internet, z.B. als Attachments (Anhang) von Mails. Gefährlich sind dabei alle Attachments, die sogenannte ausführbare Dateien enthalten. Solche Dateien sind z.B. \*.EXE, \*.BAT, \*.SCR. Aber auch Office-Dateien, also \*.DOC, \*.XLS und \*.PPT können Viren enthalten.

Außerdem können Viren in Programmen (Spielen, ...) versteckt sein und auf Disketten oder CDs weitergegeben werden. In manchen Fällen reicht sogar das Öffnen einer Webseite aus, um sich einen Virus einzufangen.

Gerade in letzter Zeit nutzen Viren aber auch immer häufiger Schwachstellen in Programmen und Betriebssystemen aus, um sich zu verbreiten. Durch diese Schwachstellen ist es anderen z.B möglich, Zugriff auf Deinen Computers zu erhalten.

Schwachstellen können durch das Installieren sogenannter „Patches“, die vom Hersteller der Software oder des Betriebssystems bereitgestellt werden, geschlossen werden. (Siehe hierzu auch: „Wie kann ich mich vor Viren schützen? Was muss ich beachten?“)

### 3. Was machen Viren?

Viren können sehr unterschiedliche Dinge tun. Welche Schäden genau angerichtet werden, hängt also vom Virus ab.

Manche Viren ändern nur den Bildschirmhintergrund, blenden Bildchen ein oder sorgen dafür, dass der Mauszeiger nicht mehr normal gesteuert werden kann.

Andere Viren können PCs zum Absturz bringen, Dateien und Programme beschädigen oder sogar die Festplatte formatieren, also alle gespeicherten Daten löschen.

Wieder andere Viren versuchen, Server durch millionenfache Anfragen zum Absturz zu bringen oder sie so stark zu „beschäftigen“, dass normale Anfragen an diesen Server, von diesem nicht mehr beantwortet werden können, und der Server somit praktisch nicht mehr erreichbar ist. Diese Form eines Angriffs wird DOS-Attacke genannt (DOS = Denial of Service).

Zusätzlich machen Computerviren aber das, was reale Viren auch tun - sie vermehren und verbreiten sich! In den meisten Fällen geschieht das dadurch, dass der Virus das im Mailprogramm gespeicherte Adressbuch öffnet, eMail-Adressen in gespeicherten Dokumenten sucht oder diese beim Surfen von Webseiten herunterkopiert. Anschließend schickt der Virus dann Mails an alle eMail-Adressen, die er gefunden hat, und hängt an diese Mails als Attachment eine Kopie von sich selbst an. Auf diese Weise können sich Viren innerhalb von wenigen Tagen über die ganze Welt verbreiten, Millionen Computer infizieren und beträchtliche Schäden verursachen. Viren, die sich selbstständig verbreiten, nennt man auch „Würmer“.

### 4. Warum muss ich mich vor Viren schützen?

Stell Dir vor, Du schreibst gerade einen Praktikumsbericht, eine Hausarbeit oder sogar Deine Diplomarbeit und ein Virus löscht Dir plötzlich alle Dateien. Auch wenn Du Sicherungskopien dieser Daten angefertigt hast, wird es Dich dennoch Zeit und Nerven kosten, bis Du alle Dateien wieder hergestellt hast. Hinzu kommt aber, dass jeder für das verantwortlich ist, was mit und auf seinem Computer passiert, und ggf. für Schäden, die anderen dadurch entstehen, haftbar gemacht werden kann. Gleich, ob diese Schäden vom Besitzer nun bewusst oder unbewusst verursacht wurden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beziffert den von Viren allein in Deutschland verursachten Schaden auf einen dreistellige Millionenbetrag jährlich. Es sollte deshalb jeder für die Sicherheit seines Computers sorgen.

### 5. Ich habe ein Antivirus-Programm installiert. Kann mir jetzt nichts mehr passieren?

Doch! Du bist dadurch nicht automatisch völlig sicher. Ein Antivirus-Programm kann Deinen Computer nur von den Viren schützen, die es kennt. Ein Programm, das Dich auch vor noch unbekanntem Viren schützt, gibt es nicht.

### 6. Wie kann ich mich vor Viren schützen? Was muss ich beachten?

Um Dich zu schützen, solltest Du vor allem 2 Dinge tun.

1. Du solltest ein Antivirus-Programm auf Deinem Rechner installieren.
2. Du solltest einige Verhaltensregeln beachten.

Es ist wichtig zu wissen, dass ein Antivirus-Programm Dich nur dann schützen

kann, wenn Du es regelmäßig aktualisierst (= updatest). Denn diese Programme können Dich nur vor Viren schützen, die sie kennen. Am besten schaust Du mindestens einmal pro Tag nach Updates. Viele Programme bieten auch die Möglichkeit bei jedem Start des Computers automatisch nach Updates zu suchen. Ein Antivirus-Programm, das Du seit einem Monat oder sogar noch länger nicht aktualisiert hast, bietet so gut wie keinen Schutz mehr!!!

Warum ist das so? Genau wie bei Impfstoffen gegen reale Viren, können Antivirus-Programme nur vor den Viren schützen, die sie kennen, bzw. für die sie programmiert wurden. Wenn also neue Viren auftaucht, müssen die Hersteller dieser Programme die Viren erst analysieren und für jeden Virus ein Programm schreiben, das den Virus erkennt und unschädlich macht. Da sich Computerviren genau wie reale Viren deutlich voneinander unterscheiden, muss das für jeden einzelnen Virus immer wieder neu geschehen. Sobald ein Hersteller ein Programm entwickelt hat, mit dem der neue Virus erkannt und ggf. beseitigt werden kann, stellt er dieses als Update zum Download ins Internet. Erst, wenn Du dieses Update auf Deinem Computer installiert hast, kann Dich Dein Antivirus-Programm vor dem neuen Virus schützen - vorher nicht!!!

Allerdings gibt es kein Antivirusprogramm, das jeden Virus erkennt. Deshalb ist es wichtig, dass Du zusätzlich einige Regeln beachtest, um Dich vor Viren zu schützen.

Die meisten Viren verbreiten sich als Attachments von Mails. Deshalb solltest Du sehr vorsichtig sein, wenn Du Attachments zugeschickt bekommst. Ein Attachment, das Dir von jemandem geschickt wird, den Du nicht kennst, solltest Du auf keinen Fall öffnen. V.a. nicht, wenn der Text der Mail keinen persönlichen Bezug zu Dir hat. Meist lauten die Texte wie folgt (oder ähnlich):

*Betreff: Your Application*

*Text der Mail: For details see the attached File*

oder auch:

*Betreff: Re: Movie*

*Text der Mail: For details see the attached File*

Einige Viren täuschen auch vor, dass die Mail nur aus Versehen an Dich geschickt wurde und eigentlich für jemand anderen bestimmt war, z.B.:

*Betreff: DAS MUSST DU SEHEN!!!*

*Text der Mail: Hi Thomas, schau Dir unbedingt das angehängte Bild an. So eine Tolle Frau hast Du noch nie gesehen. Ich komm dann morgen bei Dir vorbei, Werner*

Die Möglichkeiten sind hierbei unendlich. Von einigen Viren werden diese Texte sogar von Mail zu Mail geändert.

Eines ist allerdings immer gleich. In den Attachments (Anhängen) verstecken sich ausführbare Dateien. Also Dateien, die sich installieren, wenn man sie anklickt. Die gefährlichsten Datei-Typen sind hierbei: \*.EXE, \*.SCR und \*.PIF. Allerdings werden - je nach Einstellungen des Computers - oft nur die Dateinamen, aber nicht die Dateiendungen angezeigt. Oder die Dateitypen

werden in doppelten Dateiendungen versteckt, also z.B. mein-bild.jpg.exe, und somit als ungefährliche jpg-Datei (jpg ist ein Bildformat) getarnt. Tatsächlich handelt es sich hierbei aber um eine ausführbare EXE-Datei - egal, was davorsteht.

Viren lassen sich aber auch in anderen Datei-Typen verstecken. Z.B. in \*.COM, \*.BAT, \*.VBS und sogar in Office-Dateien, also in \*.DOC, \*.XLS und \*.PPT.

Öffne also keine Attachments, wenn Du nicht vorher mit dem Versender abgesprochen hast, dass er Dir eines schickt. Und selbst dann solltest Du immer noch vorsichtig sein und überprüfen, ob der Text der Mail und der Name des Attachments zu dem passen, was ihr abgesprochen habt.

Es gibt aber auch andere Möglichkeiten, sich einen Virus einzufangen - einfach beim Surfen! Deshalb solltest Du bei Deinem Browser immer die höchste Sicherheitsstufe auswählen und aktive Inhalte (ActiveX, Java, JavaScript) sowie Script-Sprachen (z.B. Visual Basic, Script, VBS) deaktivieren.

Diese „Aktiven Inhalte“ können auch in HTML-Mails versteckt werden. Es können also auch durchaus Mails ohne Attachment gefährlich sein. Aus diesem Grund solltest Du keine HTML-Mails öffnen und natürlich auch nicht verschicken. Wähle also immer „plain text“ (= „nur text“) aus, wenn Du Mails verschickst.

Um sich gegen in HTML-Mails versteckte Inhalte zu schützen, solltest Du Dein Mailprogramm so einstellen, dass es HTML in Mails nicht interpretiert. D.h., dass es dann alle Formatierungsanweisungen als normalen Text anzeigt. Dadurch sind diese Mails zwar schwerer lesbar, aber auch nicht mehr gefährlich.

Auch die Mail-Programme bei Selfnet e.V. interpretieren HTML in Mails nicht, um uns vor dieser Gefahr zu schützen. Da HTML-Mails dadurch aber, wie beschrieben, oft nur noch schwer lesbar sind, und die Bearbeitung dadurch erschwert wird, können wir HTML-Mails leider nicht immer beantworten. Du solltest uns also keine HTML-Mails schicken, wenn Du eine Antwort bekommen möchtest.

Wie oben bereits erwähnt, gibt es für Angreifer aber noch eine weitere Möglichkeit, Viren zu verbreiten. Und zwar durch das Ausnutzen von Schwachstellen in Programmen oder Betriebssystemen. Schwachstellen sind nichts anderes als Fehler in Programmen, die von einem Angreifer z.B. dazu genutzt werden können, Zugriff auf den Rechner und alle darauf installierten Programme und gespeicherten Daten zu erhalten.

Wenn solche Schwachstellen bekannt werden, bieten die Hersteller der betroffenen Software oder des Betriebssystems - nicht die Hersteller von Antiviren-Programmen - meist bereits nach kurzer Zeit sogenannte „Patches“ zum Download an. Durch das Installieren dieser Patches werden die Schwachstellen geschlossen und der Computer gegen derartige Angriffe geschützt.

Service-Packs beinhalten viele solcher Patches und werden in grösseren Abständen von Herstellern von Betriebssystemen herausgebracht. Durch die Installation von Service-Packs werden also viele Schwachstellen auf einmal geschlossen.

Wichtig ist: Wenn Du Dein Betriebssystem neu installierst, musst Du danach auch wieder alle Service-Packs und Patches installieren, da Dein Betriebssystem sonst natürlich wieder alle Schwachstellen beinhaltet.

## 7. Fazit:

100%-igen Schutz vor Viren gibt es nicht. Man kann das Risiko einen Virus zu bekommen aber durch das Installieren von Antivirus-Software, regelmäßige Updates und einige einfache Verhaltensregeln fast auf Null reduzieren.

## 8. Weitere Informationen

Weitere Informationen zum Thema Viren und Würmer, aber auch zu anderen schädlichen Programmtypen, wie den sogenannten „Trojanischen Pferden“ oder „Hoaxes“, zusätzliche Maßnahmen zu Deinem Schutz sowie Informationen über aktuelle Viren, findest Du zum Teil ebenfalls in unserer FAQ, sowie im Internet, z.B auf folgenden Seiten:

- <http://www.bsi.de/>
  - <http://www.bsi.de/av/index.htm>
- <http://www.cert.org/> (englisch)
- <http://cert.uni-stuttgart.de/>
  - <http://cert.uni-stuttgart.de/themen.php>

Aber auch auf den Seiten der Hersteller von Antivirus-Programmen: (diese Auswahl listet einige der uns bekannten Hersteller auf. Die Reihenfolge ist alphabetisch - nicht wertend. Die Liste erhebt keinen Anspruch auf Vollständigkeit und enthält sowohl Links zu Herstellern von kostenlosen Schutzprogrammen (Freeware) als auch zu kostenpflichtigen Shareware-Angeboten.

- <http://www.freeav.de/>
- <http://www.norman.com/de/>
- <http://www.symantec.com/region/de/> bzw. <http://www.norton.de>