

## Zusammenfassung

Viren und Würmer haben den Zweck, ein Gerät wie beispielsweise einen Computer oder einen Server, ohne das Wissen der Anwender, zu infizieren. Die Infizierung führt zu unerlaubter Ausführung von Software und zur Ausbreitung der Infizierung auf weitere Geräte.

Von Viren und Würmern kann jede Person betroffen sein, die Informationen und Dateien aus dem Internet per E-Mail sowie

über sonstige Datenträger austauscht oder Software, Dokumente etc. herunter lädt.

Dieses Dokument beschreibt, wie Sie sich vor diesen Bedrohungen schützen können.

## Inhalt

- 1 Was ist ein Antivirenprogramm? →
- 2 Wer ist betroffen? →
- 3 Wie funktioniert ein Antivirenprogramm? →
- 4 Warum sollte man sich schützen? →
- 5 Vorbeugende Massnahmen →



### 1 Was ist ein Antivirenprogramm?

Ein Antivirenprogramm ist eine Software, deren Hauptaufgabe der Schutz eines Geräts gegen verschiedene Arten von EDV-Infektionen wie etwa Viren ist.

Es gibt verschiedene Arten von Antivirenprogrammen. Sie unterscheiden sich im Wesentlichen durch die Anzahl der Funktionen, ihre Installation sowie die für die Erkennung von Unregelmäßigkeiten verwendeten Verfahren.

### 2 Wer ist betroffen?

Von Viren kann jede Person betroffen sein, die Informationen per e-Mail sowie per Datenträger austauscht (Disketten, CD-ROMs, Memory Sticks etc.) oder Software, Dokumente sowie jegliche andere Art von Dateien aus dem Internet herunter lädt. Es ist daher wichtig, zum Schutz seiner Informationen und Geräte, ein Antivirenprogramm zu installieren.

### 3 Wie funktioniert ein Antivirenprogramm?

Um ein Gerät zu schützen, verwenden die Antivirenprogramme verschiedene Techniken. Hierbei handelt es sich um:

- ➔ die Echtzeitanalyse der am Gerät ausgeführten Operationen wie etwa das Öffnen/Schliessen von Dateien sowie der Start von Softwareprogrammen und jeglicher Art von Downloads aus dem Internet oder von einem anderen Netzwerk, die vom Gerät ausgeführt werden,
- ➔ das Scannen von Festplatten, Disketten und anderen, zu Speicherzwecken dienenden Peripheriegeräten sowie der Systemkonfiguration des Geräts in zuvor festgelegten regelmäßigen Abständen,

- ➔ die Analyse des Inhalts sowie des Umfangs von eingehenden und abgehenden E-Mails, um sich gegen jene Viren zu schützen, die über eine Routine zur Verbreitung per E-Mail verfügen (so genannte "mass mailers").

Informieren Sie sich kontinuierlich über die neuesten Gefahren.

Bei Erkennung einer Anomalie oder eines Versuchs, das Gerät mit einem Virus zu infizieren, zeigt das Antivirenprogramm in der Regel und abhängig von der vom Benutzer gewählten Konfiguration eine Warnmeldung an, die es dem Benutzer ermöglicht:

- den Versuch einer Vireninfection abzuwehren,
- den infizierten oder bösartigen Inhalt durch das Löschen jeglicher Virensuren zu reparieren,

- den infizierten Inhalt endgültig zu löschen,
- den infizierten oder bösartigen Inhalt unter Quarantäne zu stellen.


Aufgrund der Konvergenz der Techniken zur Infizierung eines Geräts mit einem Virus integrieren bestimmte Softwareentwickler ausserdem Firewall-Funktionen in ihre Antiviren-Lösungen.

## 4

### Warum sollte man sich schützen?

Die Verwendung eines Antivirenprogramms bietet Schutz gegen die folgenden Bedrohungen:

 **Viren**

 **Trojanische Pferde**

 **Würmer**

Ein Schutz trifft zu, sofern das Antivirenprogramm auch über Firewall-Funktionen verfügt.

 **BEISPIEL: Ein Antivirenprogramm erkennt den Versuch ein Gerät mit einem Virus zu infizieren:**

Das Beispiel zeigt, dass das Antivirenprogramm eine versuchte Infizierung per Virus erkennt. Diese Simulation wurde mit einer Testdatei durchgeführt, die von EICAR (European Institute for Computer Antivirus Research) zur Verfügung gestellt wird und unter <http://www.eicar.org> heruntergeladen werden kann.



## 5

### Vorbeugende Massnahmen

Um sich zu schützen, reicht es aus, ein Antivirenprogramm herunterzuladen. Im Internet sind einige Antivirenprogramme kostenlos als Demoversionen verfügbar.

Ein Antivirenprogramm kann seine Aufgabe jedoch nicht erfüllen, wenn die nachfolgend aufgeführten Empfehlungen nicht eingehalten bzw. überprüft werden:

- Stellen Sie eine regelmässige Aktualisierung der Virusdefinition sicher, am Besten über eine automatische, tägliche Aktualisierung.
- Achten Sie darauf keine E-mails, Programme oder sonstige Dateien zu öffnen, deren Titel oder Inhalte ungewohnt oder anormal scheinen.
- Scannen Sie mindestens einmal wöchentlich sämtliche Laufwerke und die Systemdateien des Geräts.
- Überprüfen Sie die korrekte Funktionsweise Ihres Systems mittels der von EICAR unter folgender Adresse zur Verfügung gestellten Testdateien: <http://www.eicar.org>.