

Zusammenfassung

Dieses Dokument behandelt Viren und Würmer, deren Zweck darin besteht, ein Gerät wie beispielsweise einen PC oder einen Server ohne das Wissen der Anwender zu infizieren, um dort eine unerlaubte Software auszuführen und um sich von einem Gerät zum nächsten auszubreiten. Von Viren und Würmern kann jede Person betroffen sein, die Informationen per e-Mail sowie per Datenträger austauscht oder Software,

Dokumente sowie jegliche andere Art von Dateien aus dem Internet herunter lädt. Nachfolgend werden die Funktionsweisen und Ausbreitungsmethoden von Viren und Würmern, die möglichen Auswirkungen sowie die vorbeugenden Massnahmen erläutert.

Inhalt

- 1 Was ist ein Virus oder ein Wurm? →
- 2 Wer ist betroffen? →
- 3 Wie funktionieren Viren und Würmer? →
- 4 Warum sollte man sich schützen? →
- 5 Vorbeugende Massnahmen →



1 Was ist ein Virus oder ein Wurm?

Ein Virus ist eine Software oder ein Teil einer Software, die sich, um sich ausbreiten zu können, an jegliche Arten von Dateien oder andere Softwareprogramme anhängt und den Zweck hat, ein Gerät ohne Wissen der Anwender zu infizieren und sich von einem Gerät zum anderen auszubreiten.

Ein Wurm ist eine Software, die in hohem Mass einem Virus ähnelt. Im Gegensatz zu einem Virus benötigt ein Wurm jedoch nicht die Mitwirkung des Menschen, um ein Gerät zu infizieren. Er verfügt über einen "Motor" (Automatismus), der es ihm ermöglicht, seinen Code automatisch auszugeben und auszuführen und in der Folge neu zu infizierende Zielgeräte zu suchen.

2 Wer ist betroffen?

Von Viren und Würmern 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.

Die einfache Tatsache, mit seinem Gerät eine Verbindung zum Internet oder zu einem anderen Kommunikationsnetzwerk aufzubauen, kann in bestimmten Fällen schon ausreichen, um sein Gerät zu infizieren.

3 Wie funktionieren Viren und Würmer?

Die Mehrheit der Viren und Würmer sind in Dateien oder Softwareprogrammen versteckt, die Dateiendungen des Typs .exe, .bin, .com, .vbs, .js und ähnliche haben.

Noch vor einigen Jahren erfolgte die Verbreitung von Viren und Würmern hauptsächlich über Disketten. Das Internet hat neue und viel schnellere Verbreitungsmechanismen mit sich gebracht. Dies ist insbesondere auf die massive Nutzung der e-Mail, der Bereitstellung neuer Datenträger und Softwareprogramme und

auf die wachsende Zahl der mit dem Internet verbundenen Geräte zurückzuführen. Die Zahl der Viren und Würmer nimmt täglich zu. Die Infektions- und Verbreitungsgeschwindigkeit nimmt ebenfalls permanent zu.

Eine weitere beunruhigende Tatsache ist, dass die Entwickler von Viren und Würmern deren Aussehen im Verlauf der Jahre verändert haben. Heute gibt es verschiedene Typen wie etwa Makroviren, Flash Worms und aus mehreren Teilen bestehende Viren.

Ein Virus wird normalerweise aktiviert, wenn der Anwender die Datei oder die Software ausführt, in die der Virus integriert ist. beispielsweise durch Anklicken einer Datei die als Anhang einer e-Mail verschickt wurde.

Ein Wurm infiziert ein Gerät ohne Eingriff des Menschen. Er versucht, Sicherheitslücken des Betriebssystems (OS) oder der installierten Softwareprogramme auszunutzen, um das Gerät zu infizieren. Sobald sich der Wurm auf einem Gerät befindet, wird sein Code automatisch ausgeführt. Ein Wurm verfügt im Allgemeinen über einen Mechanismus, der es ihm ermöglicht, neu zu infizierende Zielgeräte zu suchen und sich so automatisch auszubreiten. Dies erfolgt beispielsweise durch das Surfen im Internet.

BEISPIELE:

Morris Wurm - Wurm, der seinen Namen von seinem "Schöpfer" Robert Morris erhalten hat. Er gehört mit zu den ersten Würmern (1988) die sich schnell im Internet ausbreiteten und mehrere Millionen Geräte infizierten.

Iloveyou - Virus, der sich im Jahr 2000 in hohem Mass über die e-Mail verbreitete und den Anwender aufforderte, einen sogenannten Liebesbrief zu öffnen, der sich in einer angehängten Datei befand.

Blaster - Wurm, der sich während des Sommers 2003 stark ausbreitete und der in wenigen Tagen mehrere Millionen mit dem Internet verbundene Geräte infizierte. Mehrere Monate später waren noch immer viele Geräte von Blaster infiziert, ohne dass sich ihre Besitzer dessen bewusst waren.

4

Warum sollte man sich schützen?

Die Viren und Würmer stellen eine beträchtliche Bedrohung für alle Anwender von EDV-Systemen dar und können zu beträchtlichen Verlusten führen. Um diese zu vermeiden, ist ein effizienter Schutz erforderlich. Zu den Verlusten gehören:

direkte finanzielle Verluste

- Zerstörung kritischer Daten,
- Ausserbetriebsetzung Ihres gesamten EDV-Systems...

Ansehensverlust

- Verbreitung streng vertraulicher Informationen,
- Begünstigung der Ausbreitung des Virus oder Wurms und Infizierung anderer...

Zeitverlust

- Beseitigung von Viren oder Würmern vom EDV-System,
- Aufwand für die Wiederherstellung der zerstörten Daten,
- Verhinderung einer fortgesetzten Ausbreitung...

5

Vorbeugende Massnahmen

Um sich gegen eine Virus- oder Wurm-Infektion zu schützen, gibt es drei wesentliche Schutzmassnahmen:

Einzelpersonen: diese Softwareprogramme sind im Einzel- und Fachhandel erhältlich. Diese Produkte umfassen meistens kostenlose Aktualisierungen innerhalb eines Zeitraums von mehreren Monaten oder sogar Jahren.

- ➔ Verwenden Sie ein oder mehrere Virenschutzprogramme und eine Firewall auf Ihrem Gerät. Es ist wichtig, ihre Virenschutz-Software regelmässig zu aktualisieren, um sich gegen die Verbreitung neuer Viren und Würmer zu schützen.
- ➔ Öffnen Sie keine e-Mails, Softwareprogramme oder jegliche andere Dateien, deren Betreff oder Inhalt Ihnen ungewöhnlich oder verdächtig vorkommt.
- ➔ Installieren Sie regelmässig sogenannte Patches für Ihr Betriebssystem (OS) und andere installierte Softwareprogramme. Diese bieten ebenfalls einen Schutz gegen die meisten Infektionen und Ausbreitungen von Viren und Würmern.

Mithilfe dieser drei Schutzmassnahmen können Sie eine Vielzahl der Probleme auf Ihrem Gerät verhindern.

Beachten Sie ausserdem die folgenden allgemeinen Sicherheitsmassnahmen:

- ➔ Gewährleisten Sie eine individuelle Zugangskontrolle zu den Anwendungen.
- ➔ Unternehmen Sie alle Massnahmen, um ein effektives Sicherungssystem zu garantieren.
- ➔ Schützen Sie Ihre Geräte physikalisch.
- ➔ Halten Sie sich über neue Bedrohungen auf dem Laufenden.