Computerviren – Gefahren aus dem Cyberspace

Gefahren lauern überall - auch im Internet

Erschreckende Meldungen zum Thema Computerviren gibt es reichlich zu lesen: Glaubt man den Aussagen einiger Anbieter von Antivirenprogrammen, tummeln sich mittlerweile über 12000 verschiedene Viren auf den Rechnern von Unternehmen, Behörden und privaten Anwendern.

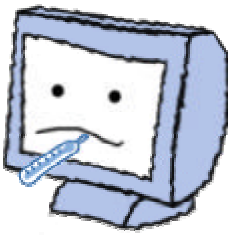
Man hört immer öfter von neuen Viren oder Würmern - Programmen also, die sich selbstständig verbreiten oder über E-Mails versandt werden und Schäden auf Ihrem PC anrichten können. Aber auch von Trojanischen Pferden ist oft die Rede. Das sind dann Programme, die vom Nutzer unbemerkt sicherheitskritische Funktionen durchführen, indem sie beispielsweise Passwörter abfangen.

Damit ein Virenangriff aber überhaupt stattfinden kann, benötigt das angreifende Programm in irgendeiner Art Zugang zu Ihrem PC - entweder über eine Netzwerk- oder Telefonverbindung oder über Datenträger, wie Disketten oder CD-ROMs.

Was sind Computerviren?

Computerviren sind kleine von Menschen geschriebene Programme. Sie entstehen nicht einfach so, sie werden programmiert und verfolgen oft einen bestimmten Zweck. Sie verfügen mindestens über einen Programmteil, durch welchen sich der Virus verbreitet. Dadurch kopiert sich der Virus in andere Programmdateien hinein und verbreitet sich systematisch von einer Datei zur anderen, von einem Rechner zum nächsten. Eine weitere Komponente ist die Nutzlast oder Schadensroutine. Es ist die Programmkomponente, die bestimmte Symptome oder Schäden am infizierten Rechner hervorruft.

Welche Schäden können Computer-Viren anrichten?



Das Ausmaß der Schäden durch Viren reicht von der Zerstörung von Programmen und Dateien auf Disketten und Fest-platten bis zur Beeinflussung der eingesetzten Hardware. Häufig bemerken Sie eine Infektion nicht sofort, sondern erst später, wenn Sie den Auslöser aktiviert haben.

Ein Wurm ist autonom

Eine Variante von Viren, von denen man in letzter Zeit immer öfter hört, sind so genannte Würmer. Die Infektion erfolgt oftmals über E-Mail. Startet man eine angehängte Datei, wird der Virus aktiviert und verbreitet sich anschließend selbst weiter. Durch Sicherheitslücken in einigen E-Mail-Programmen können sich die Würmer besonders schnell verbreiten. Im Gegensatz zu Viren und Trojanischen Pferden infizieren Würmer jedoch keinen fremden Code, um sich fortzupflanzen. Sie sind auf die selbstständige Verbreitung in Netzwerken ausgerichtet und stehlen lediglich Rechenzeit. Die „Absicht" eines Wurms ist es, so viele Computer wie möglich zu befallen. Neben seiner Fähigkeit, sich schnell und selbsttätig zu verbreiten, hat ein Wurm eine Ladung „an Bord", das eigentliche Schadprogramm. Dieses Schadprogramm tobt sich dann wie ein herkömmlicher Virus innerhalb des befallenen PCs aus.

Was ist ein Trojaner?

Ein scheinbar nützliches Programm hat ein anderes sozusagen im Bauch, das dann unbemerkt eindringt und sich auf dem PC installiert. Nach dem Start des Tarn-Programms wird auch die schädliche Ladung auf dem PC aktiviert. Das Gefährliche an Trojanern ist, dass sie unbemerkt so viele Benutzer-

E-Mail an das „Haus der Zahnärzte“:
info@bremer-zahnaerzte haus.de

Internetadresse:
http://www.bremer-zahnaerztehaus.de

Postanschrift:
Haus der Zahnärzte
Universitätsallee 25
28359 Bremen

daten wie möglich verändern, löschen oder ausspionieren. Wenn der Internet-Nutzer persönliche Daten wie zum Beispiel Passwörter oder Kreditkartennummer eingibt, kann der Trojaner quasi mitschreiben und diese Daten per E-Mail an den Hacker übermitteln, also an den Absender des Trojaners. Das kann sogar so weit gehen, dass Hacker mit so genannten Back-door-Trojanern - diese richten sich auf dem Wirtssystem Ports (Backdoors) ein – Zugriff auf fremde Rechner haben und dann die Fernkontrolle über fast alle Funktionen hat. Anders als Computer-Viren können sich Trojanische Pferde jedoch nicht selbstständig verbreiten.
Auch wenn die Gefahren im Internet vielfältig sind - mit einer geeigneten Sicherheitssoftware und etwas Vorsicht im Umgang mit dem Computer/Internet lassen sie sich auf ein Minimum reduzieren.

Tipps zum Virenschutz

Um das Risiko einer Infektion und der Ausbreitung des Computervirus so gering wie möglich zu halten, sollten Sie sich ständig über die Art der Gefahren informieren, einige Vorsichtsmaßregeln beachten, für den Notfall Vorsorge zu treffen und sich weitmöglichst schützen. Die meisten Computer-Viren sind zum Glück nur lästig und vernichten keine Daten und Programme absichtlich. Anstecken kann sich Ihr PC immer dann, wenn Sie Dateien aus dem Internet auf Ihren Rechner laden. Viren können aber auch über Disketten oder CD-ROMs auf Ihren PC gelangen. In jeder ausführbaren Datei, wie zum Beispiel *.exe oder *.com, kann sich ein Virus verstecken. Auch Textdokumente vom Typ *.doc oder Tabellen vom Typ *.xls können virenverseucht sein.

Deshalb:

- Sichern Sie regelmäßig Ihre Daten. Bewahren Sie die Sicherheitskopien sorgfältig auf.
- Die überwiegende Anzahl der Viren kommen per Dokumente als Anhang mit einer E-Mail zu Ihrem PC. Öffnen Sie keine Dateien, die Sie von Unbekannten unaufgefordert zugeschickt bekommen. Selbst wenn der lustige Bildschirmschoner von einem Freund kommt, sollten Sie sich vorher vergewissern, aus welcher Quelle er ursprünglich stammt. Lesen Sie auch keine lustigen kleinen Dateien im Internet auf. Sie wissen schließlich nicht, ob sich darin nicht vielleicht ein Trojanisches Pferd verbirgt, das Ihre persönlichen Daten heimlich ausliest.
- Versehen Sie alle Datenträger, auf denen nicht geschrieben werden muss, mit Schreibschutz.
- Verwenden Sie **aktuelle Anti-Viren-Software** und aktualisieren Sie diese regelmäßig. Zu beachten ist, dass Viren-Suchprogramme mit der Zeit ihre Wirksamkeit verlieren, da sie nur die zu ihrem Erstellungszeitpunkt bekannten Computer-Viren berücksichtigen, neu hinzugekommene jedoch meist nicht erkennen können. Daher ist eine regelmäßige Aktualisierung des Viren-Suchprogramms erforderlich. Lassen Sie das Virenschutzprogramm stets aktiv im Hintergrund laufen. Wenn Sie es deaktivieren, kann es verdächtige Dateien nicht erkennen.

  Im Haus der Zahnärzte im Lande Bremen wird als Viren-Suchprogramm „Symantec Antivirus“ eingesetzt (siehe http://www.Symantec.com/region/de/loesungen/privatanwender.html). Die beste Antiviren-Software nach Anwenderstimmen finden Sie unter: http://www.virus-aktuell.de/ranking/topsites.shtml

- Überprüfen Sie Datenträger und E-Mail-Anhänge, die Sie nutzen, mit dem Anti-Viren-Programm.
- Überprüfen Sie auch vorinstallierte Neugeräte und Geräte, die gewartet wurden.
- Erstellen Sie einen Notfall-Datenträger (Diskette oder CD-ROM).
- Schützen Sie Ihren Computer und alle Datenträger vor fremder Benutzung durch Passwörter.
- Um den besten Schutz vor Boot-Viren zu erhalten, sollten Sie die Boot-Reihenfolge im CMOS-RAM von "A:, C:" auf "C:, A:" ändern (Holen Sie sich den Rat eines Experten).

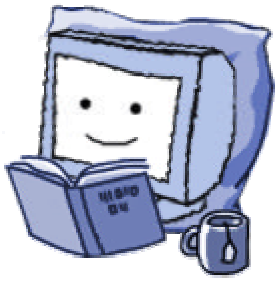
E-Mail an das „Haus der Zahnärzte“:
info@bremer-zahnaerzte haus.de

Internetadresse:
http://www.bremer-zahnaerztehaus.de

Postanschrift:
Haus der Zahnärzte
Universitätsallee 25
28359 Bremen

- Richten Sie mehrere Partitionen (logische Laufwerke) auf dem Rechner ein (lassen Sie sich dieses von einem Experten einrichten oder erklären).
- Sicherheitspatches - nicht nur für Betriebssysteme. Häufig werden Fehler in Software-Produkten bekannt, die dazu führen können, dass die Sicherheit der Computer, auf denen diese Produkte installiert sind, beeinträchtigt wird. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Dies ist ganz besonders wichtig, wenn die betreffenden Systeme mit dem Internet verbunden sind. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen in der Regel Patches oder Updates, die auf dem jeweiligen Computer installiert werden müssen, um den oder die Fehler zu beheben. Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen.

Infiziert – und nun?



10 Dinge, die Sie bei einer Infektion tun sollten:

1. Bei Verdacht auf Virus-Befall sollten Sie die Arbeit schnell, aber wie gewohnt beenden. Vor allem gilt: **Keine Panik!**
2. Schalten Sie den Computer aus.
3. Wenn Sie kein Experte sind, holen Sie sich lieber den Rat eines solchen ein. Manchmal ist zur Virenbeseitigung besondere Fachkenntnis erforderlich, da Viren sich in ihrer Arbeits- und Wirkungsweise stark unterscheiden können.
4. Legen Sie eine virenfreie, schreibgeschützte System- bzw. Boot-Diskette in Laufwerk A: ein und booten Sie den Rechner von dieser Diskette.
5. Überprüfen Sie den PC mit einem aktuellen Viren-Schutzprogramm. Dadurch können Sie feststellen, ob tatsächlich ein Computer-Virus aufgetreten ist und um welchen es sich handelt.
6. Sichern Sie Ihre Daten, falls noch nicht geschehen.
7. Entfernen Sie den Virus abhängig vom jeweiligen Virustyp. In der Regel macht Ihr Anti-Viren-Programm das automatisch. Sollte das nicht klappen, so können vom Hersteller der Anti-Viren-Programme mitgelieferte Virendatenbanken Hilfestellungen geben. Darin sind die Funktionsweise und die Behebung oftmals detailliert beschrieben.
8. Lassen Sie die Festplatte und alle anderen Datenträger noch einmal überprüfen, um sicherzugehen, dass der Virus auch wirklich komplett entfernt wurde.
9. Sollte der Computer-Virus Daten gelöscht oder verändert haben, versuchen Sie, die Daten aus den Datensicherungen und die Programme aus den Sicherungskopien der Programme zu rekonstruieren.
10. Versuchen Sie abschließend die Ursache der Vireninfektion festzustellen. Ist die Quelle auf Original-Datenträger zurückzuführen, dann sollte der Hersteller und das BSI informiert werden (Virusmeldebogen). War die Ursache eine Datei oder E-Mail, dann benachrichtigen Sie den Ersteller oder Absender der Datei. Wenn Sie Daten von einem infizierten Rechner verschickt haben, dann warnen Sie auch die Empfänger Ihrer Daten.

Quellen:
http://www.bsi.bund.de/
Hamburger Zahnärzteblatt Nr. 1 Jan 2004
http://www.datenschutzzentrum.de/

Testen sie ihren Virenscanner

E-Mail an das „Haus der Zahnärzte“:
info@bremer-zahnaerzte haus.de

Internetadresse:
http://www.bremer-zahnaerztehaus.de

Postanschrift:
Haus der Zahnärzte
Universitätsallee 25
28359 Bremen