Von Viren, Würmern und Trojanern

Viren

E-Mail

Internet

Handy & PDA

Sicherheit

Mehr Info

Von Viren, Würmern und Trojanern

Inhalt

Viren – ein Problem?

Computerviren, Datenmissbrauch, Hacker, Cracker. Schlagwörter, die uns oft begegnen und jährlich Kosten in Millionenhöhe verursachen – so jedenfalls stellen es die Medien dar. Sind Viren & Co. wirklich so gefährlich, wie immer behauptet wird?

Wenn Sie tatsächlich glauben, die Bedrohung durch Viren sei eher gering, dann stellen Sie sich einmal folgende Situation im Büro oder zu Hause vor:

Angenommen, Ihre Antiviren-Software wurde seit einigen Monaten nicht mehr aktualisiert. Nun möchten Sie doch ein Update durchführen und stellen dabei fest, dass alle Ihre Excel-Tabellen mit einem neuen Virus infiziert sind, der willkürlich Zahlen verändert. Natürlich haben Sie Backups von all Ihren Daten. Aber vielleicht haben Sie schon seit Monaten Sicherungskopien von infizierten Dateien erstellt. Wie können Sie nun herausfinden, welche Zahlen die richtigen sind?

Oder es ist ein neuer E-Mail-Virus aufgetreten, und Sie schließen Ihren E-Mail-Gateway, um Ihre Firma vor der zu erwartenden E-Mail-Flut zu schützen ... und verlieren dadurch einen wichtigen Kundenauftrag.

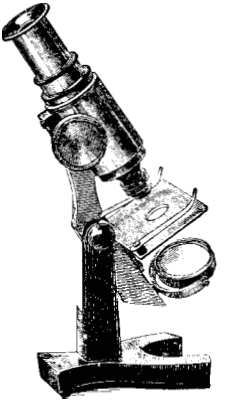
Stellen Sie sich weiterhin vor, Sie sitzen zu Hause und schreiben an Ihrer Diplomarbeit. Sie sind schon fast fertig, als eines Ihrer Kinder ein neues Spiel auf Ihrem PC installiert und ihn mit einem Virus infiziert. Der Virus löscht die gesamte Festplatte ... und damit auch Ihre Diplomarbeit, an der Sie vielleicht schon seit Monaten gearbeitet haben.

Angenommen, ein Bekannter schickt Ihnen per E-Mail einige Dateien, die er im Internet gefunden hat. Ohne jegliche Bedenken öffnen Sie die Dateien (schließlich vertrauen Sie Ihrem Freund) und lösen einen Virus aus, der vertrauliche Dokumente an jeden Eintrag aus Ihrem Adressbuch sendet ... u. a. auch an Ihre Wettbewerber.

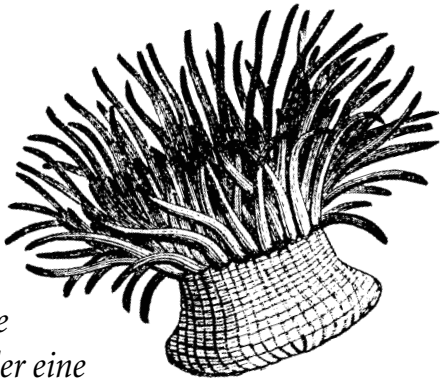
Stellen Sie sich vor, dass Sie versehentlich ein Dokument an eine andere Firma schicken, das mit einem Virus infiziert ist. Glauben Sie, dass diese Firma Sie dann immer noch als guten Geschäftspartner betrachten wird ...?

Diese Schreckensszenarien sind nicht etwa frei erfunden, sondern haben bereits irgendwo in der Welt stattgefunden. In allen Fällen hätten die unangenehmen Folgen durch einige kleine, noch nicht einmal teure Vorsichtsmaßnahmen verhindert werden können.

Mit dem vorliegenden Büchlein möchten wir über mögliche Gefahren aufklären und Ihnen Tipps geben, wie Sie das Schlimmste verhindern können.



Von Viren, Würmern und Trojanern



Mitte der 80er Jahre stellten die Brüder Basit und Amjad Alvi aus Lahore in Pakistan fest, dass von ihrer Software zahlreiche Raubkopien existierten. Nicht gerade erfreut darüber, schrieben sie den ersten Computervirus, der eine Kopie von sich und einen Copyright-Vermerk auf jede kopierte Diskette legte. Aus diesen Anfängen heraus hat sich eine eigenständige Szene entwickelt: Viren verbreiten sich heutzutage innerhalb weniger Stunden über den gesamten Erdball und sorgen immer öfter für Schlagzeilen in den Medien. Viele Menschen sind fasziniert davon, wie ein einziger Virus zahlreiche Unternehmen lahm legen kann, jedoch wissen die wenigsten Genaueres über Viren. Im folgenden Kapitel wird der Virenmythos genauer unter die Lupe genommen.

Was ist eigentlich ein Computervirus?

Bei einem Computervirus handelt es sich um ein Computerprogramm, das sich in Computern und Netzwerken verbreitet, indem es sich selbst kopiert.

Viren können äußerst unangenehme Auswirkungen haben, die von einer unsinnigen Textmeldung bis hin zum Löschen sämtlicher Dateien auf Ihrem Computer reichen.

Wie kann ein Virus einen Computer infizieren?

Ein Virus kann einen Computer nur dann infizieren, wenn der Virencode gestartet wird.

Doch aufgepasst! Auch wenn Sie beim Öffnen von verdächtigen Dateien noch so vorsichtig sind: Viele Viren sind so programmiert, dass sie unbemerkt ausgelöst werden. So hängen sie sich beispielsweise an andere Programme an oder verstecken sich in Codes, die automatisch ausgeführt werden, sobald bestimmte Dateitypen geöffnet werden.

Eine infizierte Datei kann auf einer Diskette, in einem E-Mail-Attachment oder über das Internet auf Ihren PC gelangen. In dem Moment, in dem Sie die Datei öffnen, wird der Virencode ausgeführt. Nun kann sich der Virus in andere Dateien auf Ihrem Computer kopieren.

Genauere Informationen über die Wirkungsweise von unterschiedlichen Virentypen finden Sie in den Abschnitten „Bootsektorviren“, „Programmviren“ und „Makroviren“.

Trojanische Pferde

Ein Trojanisches Pferd ist ein scheinbar ungefährliches Programm, in dem sich allerdings ein gefährliches Virenprogramm verbirgt, das ohne Wissen des Anwenders Schaden anrichtet.

Ein Trojanisches Pferd verlässt sich darauf, dass der Anwender ein angeblich harmloses Programm ausführt und somit die versteckten und meist Schäden verursachenden Funktionen aufruft.

Troj/Zelu beispielsweise tarnt sich als Programm, das die Folgen des so genannten Y2K-Problems rückgängig macht; in Wirklichkeit überschreibt es jedoch die Festplatte.

Trojanische Pferde werden oft genutzt, um Computer mit einem Virus zu infizieren.

Schlimmer noch sind so genannte Backdoor-Trojaner. Mit deren Hilfe können andere Anwender über das Internet die Kontrolle über Ihren PC übernehmen.

Würmer

Würmer sind in ihrer Wirkung den Viren sehr ähnlich, allerdings benötigen Sie keinen „Wirt“ (z. B. ein Makro oder einen Bootsektor) für ihre Verbreitung, da sie Kopien von sich selbst erzeugen und die Kommunikationskanäle zwischen Computern nutzen, um sich zu verteilen.
Viele Viren, wie z. B. *Kakworm (VBS/Kakworm)* oder der *Loveletter-Virus (VBS/LoveLet-A)* verhalten sich wie Würmer, da sie sich selbst per E-Mail an andere Anwender weiterleiten.

Was können Viren anrichten?

Die wichtigste Frage für die meisten Anwender ist, welche Schäden ein Virus auf ihren PCs anrichtet. Die häufigsten Auswirkungen von Viren auf PCs sind:

Textmeldungen — *WM97/Jerk* zeigt eine Textbox mit der Meldung „I think (Name des Anwenders) is a big stupid jerk!“ an.

Musik — *Yankee* spielt täglich um 17.00 Uhr den Song „Yankee Doodle Dandy“.

Zugriffsverweigerung — *WM97/NightShade* schützt das aktuelle Dokument mit einem Kennwort am Freitag, dem Dreizehnten.

Datenklau — *Troj/LoveLet-A* sendet per E-Mail Daten über den Anwender und den Rechner an eine Adresse auf den Philippinen.

Datenänderung — *XM/Compatable* ändert Daten in Excel-Tabellen.

Löschen von Daten — *Michelangelo* überschreibt am 6. März Teile der Festplatte.

Lahmlegen von Hardware — *CIH* oder *Chernobyl* (*W95/CIH-10xx*) versucht am 26. April, das BIOS zu überschreiben und den Rechner somit funktionsunfähig zu machen.

Wo liegen die Risiken?

Dies sind die Hauptangriffspunkte für Viren in Ihrem Unternehmen:

Internet

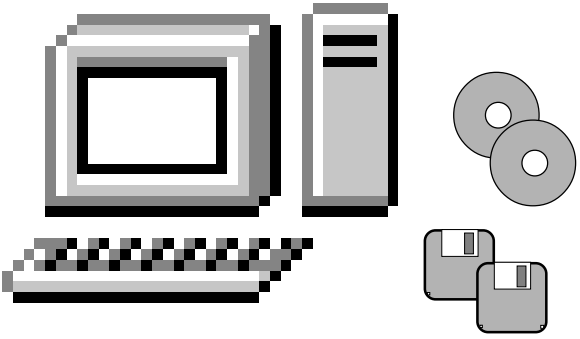
Programme oder Dokumente aus dem Internet sind häufige Quellen von Viren.

Dokumente und Tabellen

Dokumente und Tabellen können Makroviren enthalten, die andere Dokumente oder Tabellen infizieren oder verändern.

Programme

Programme mit einem Virus infizieren Ihren PC in dem Moment, in dem Sie die Programme ausführen.



E-Mail

E-Mails können infizierte Attachments enthalten. Allein durch einen Doppelklick auf diese Attachments kann Ihr PC infiziert werden. Einige E-Mails können Virencode enthalten, der ausgeführt wird, sobald Sie die E-Mail lesen.

Disketten und CDs

Disketten können sowohl Viren im Bootsektor als auch infizierte Programme und Dokumente enthalten. Auch auf CDs können sich infizierte Objekte befinden.

So schützen Sie sich vor Viren

Mit einigen einfachen Vorsichtsmaßnahmen können Sie sich vor Viren schützen und im Falle einer Virusinfektion richtig reagieren.

Informieren Sie die Anwender

Informieren Sie alle Mitarbeiter und Kollegen in Ihrem Unternehmen über das Risiko beim Diskettenaustausch, bei Internet-Downloads und beim Öffnen von E-Mail-Attachments.

Installieren Sie Antiviren-Software

Antiviren-Programme dienen nicht nur der Virenerkennung, sondern können oftmals auch Viren entfernen. Bietet die Software Überprüfungen bei Zugriff, sollten Sie diese Option auf jeden Fall aktivieren. Eine solche Überprüfung schützt vor Viren, indem der Zugriff auf infizierte Dateien verweigert wird. Weitere Informationen dazu finden Sie im Abschnitt „Antiviren-Software“.

Sichern Sie Ihre Daten

Erstellen Sie von allen Daten und der Software, die Sie im Einsatz haben (auch von den Betriebssystemen), Sicherungskopien. Wird Ihr System mit einem Virus infiziert, können Sie Ihre Dateien und Programme einfach durch saubere Kopien ersetzen.

Genauere Informationen finden Sie im Kapitel „Viren? – Kein Problem!“.

Bootsektorviren

Bootsektorviren waren die ersten Viren überhaupt. Sie verändern den Bootsektor, d. h. den Sektor, auf dem sich das Programm befindet, mit dem Ihr Computer gestartet wird.

Wenn Sie Ihren Rechner einschalten, sucht die Hardware nach dem Bootprogramm auf dem Bootsektor und führt es aus. Der Bootsektor liegt normalerweise auf der Festplatte, kann sich aber auch auf Diskette oder CD befinden. Dieses Programm lädt dann den Rest des Betriebssystems in den Speicher.

Ein Bootsektorvirus ersetzt den originalen Bootsektor mit seiner eigenen, veränderten Version und versteckt den originalen Bootsektor meist irgendwo auf der Festplatte. Wenn Sie Ihren Computer nun das nächste Mal hochfahren, wird der infizierte Bootsektor verwendet, und der Virus aktiviert.

Ihr PC kann also nur dann infiziert werden, wenn Sie ihn von einem infizierten Speichermedium booten, z. B. von einer Diskette mit einem infizierten Bootsektor.

Viele Bootsektorviren sind heutzutage schon ziemlich alt. Bootsektorviren, die für DOS-Rechner geschrieben wurden, verbreiten sich im Allgemeinen nicht auf Computern unter Windows 95, 98, Me, NT und 2000. Jedoch können sie auch auf diesen Rechnern Probleme beim Booten verursachen.

Form

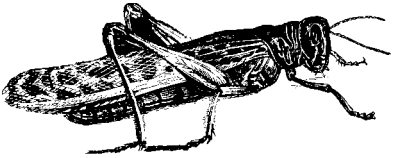
Form ist ein Bootsektorvirus, der auch zehn Jahre nachdem er das erste Mal aufgetreten ist, immer noch weit verbreitet ist. Die originale Version wird am Achtzehnten eines jeden Monats ausgelöst und erzeugt ein Klicken, wenn die Tastatur betätigt wird.

Parity Boot

Ein Virus, der willkürlich die Meldung „PARITY CHECK“ anzeigt und das Betriebssystem einfriert. Diese Meldung kann leicht mit einer echten Fehlermeldung verwechselt werden, die erscheint, wenn Fehler im Speicher aufgetreten sind.

Programmviren

Programmviren, auch Dateiviren genannt, hängen sich an Programme bzw. ausführbare Dateien an.



Wenn Sie ein Programm starten, das mit einem Programmvirus infiziert ist, wird zunächst der Virus ausgeführt. Um sich weiter im Verborgenen zu halten, führt der Virus dann das eigentliche Programm aus.

Das Betriebssystem auf Ihrem Computer sieht den Virus als Teil jenes Programms an, das Sie ausführen wollten, und gibt ihm dieselben Rechte. Mit diesen Rechten kann sich der Virus selbst kopieren und im Speicher installieren oder sich selbst aktivieren.

Programmviren gibt es schon seit den frühesten Anfängen der Virengeschichte, und auch heute noch stellen sie einen Großteil der heutigen Viren dar. Das Internet hat die Verbreitungsmöglichkeiten von Programmen und somit auch von Programmviren vervielfacht.

Jerusalem

Löscht am Freitag, dem Dreizehnten, jedes Programm, das gestartet wird.

CIH (Chernobyl)

Am 26. Tag bestimmter Monate überschreibt dieser Virus Teile des BIOS und macht den Computer damit unbrauchbar. Der Virus überschreibt außerdem die Festplatte.

Remote Explorer

WNT/RemExp (*Remote Explorer*) infiziert Windows NT-Programmdateien. Er war der erste Virus, der als Dienst laufen konnte, d. h., er kann auf NT-Systemen starten, ohne dass jemand am Netzwerk angemeldet sein muss.

Makroviren

Makroviren nutzen Befehle, so genannte Makros, aus, die in Dateien eingebettet sind und automatisch gestartet werden.

Makros werden in vielen Anwendungen, wie z. B. Textverarbeitung und Tabellenkalkulation, genutzt.

Ein Makrovirus ist ein Makroprogramm, das sich selbst kopiert und von Datei zu Datei verbreitet. Wenn Sie eine Datei öffnen, die einen Makrovirus enthält, kopiert sich der Virus in die Startup-Files der Anwendung. Der Computer ist nun infiziert.

Wenn Sie jetzt eine Datei in derselben Anwendung öffnen, wird diese Datei ebenfalls von dem Virus befallen. Ist Ihr Computer an ein Netzwerk angeschlossen, kann sich der Virus noch rascher verbreiten: Beim Weiterleiten der infizierten Datei wird der Virus an den Empfänger übertragen.

Ein Makrovirus kann auch Ihre Dokumente oder Einstellungen verändern. Makroviren infizieren häufig verwendete Dateitypen. Einige Makroviren können mehrere Dateitypen, wie Word- oder Excel-Dateien, infizieren. Sie können sich auch auf jeder Plattform verbreiten, auf der die „Wirt"-Anwendung läuft. Die Verbreitung von Makroviren ist deshalb so einfach, weil heutzutage Dokumente per E-Mail und über das Internet problemlos ausgetauscht werden können.

WM/Wazzu

Infiziert Word-Dokumente. Verschiebt zwischen einem und drei Wörtern und fügt das Wort „wazzu" willkürlich ein.

OF97/Crown-B

Kann Word-, Excel- und PowerPoint-Dateien infizieren. Wird ein Word-Dokument infiziert, wird der Makroschutz in anderen Office 97-Anwendungen deaktiviert, so dass auch diese infiziert werden können.

Antiviren-Software

Antiviren-Software erkennt Viren, verweigert den Zugriff auf infizierte Dateien und kann häufig auch Viren entfernen. Nachfolgend werden verschiedene Software-Typen zum Schutz vor Viren vorgestellt.

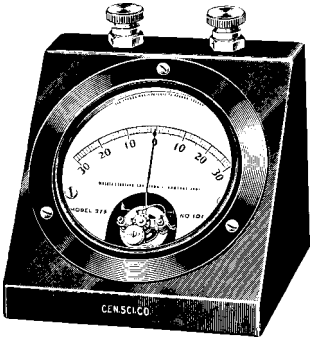
Scanner

Virenscanner erkennen alle Viren, die zum Zeitpunkt der Herstellung bekannt sind. Die meisten Virenscanner können Viren auch entfernen. Virenscanner sind die häufigste Form des Virenschutzes, sie müssen jedoch regelmäßig aktualisiert werden, damit sie auch die neuesten Viren erkennen.

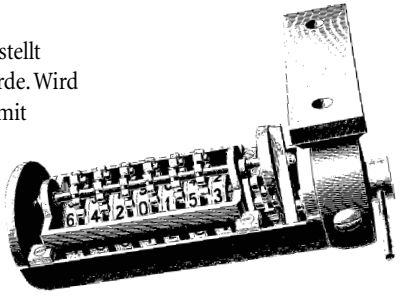
Es gibt Virenscanner, die *bei Zugriff (on access)*, und Virenscanner, die *bei Bedarf (on demand)* überprüfen. Bei den meisten Produkten ist beides möglich.

Mit Überprüfungen *bei Bedarf* können Sie bestimmte Dateien oder Laufwerke auch zu bestimmten Terminen überprüfen.

Wenn Überprüfungen *bei Zugriff* möglich sind, haben Sie einen ständigen Virenschutz auf Ihrem Rechner. Wenn Sie eine Datei öffnen möchten, wird diese Datei zunächst auf Viren durchsucht.



Prüfsummen-Tools



Mit Prüfsummen-Tools kann festgestellt werden, ob eine Datei verändert wurde. Wird ein Programm oder ein Dokument mit einem Virus infiziert, zeigt das Prüfsummen-Tool die Änderung an.

Der Vorteil von Prüfsummen-Tools ist, dass sie praktisch keinerlei Informationen über Viren benötigen und auch keine Viren erkennen brauchen. Daher müssen Prüfsummen-Tools auch nicht regelmäßig aktualisiert werden.

Der Nachteil von Prüfsummen-Tools ist allerdings, dass sie den Unterschied zwischen einem Virus und einer normalen Änderung nicht erkennen können und es dadurch häufig zu Fehlalarmen kommt. Besonders Dokumente bereiten hier oft Probleme, da sie relativ häufig geändert werden.

Hinzu kommt, dass Prüfsummen-Tools erst dann Alarm schlagen, wenn es eigentlich schon zu spät ist, nämlich wenn die Infektion bereits erfolgt ist. Sie können den Virus nicht identifizieren und befallene Dateien auch nicht säubern.

Heuristische Software

Heuristische Software versucht, Viren – sowohl bekannte als auch unbekannte – mit Hilfe von allgemeinen Virenmustern zu erkennen. Im Gegensatz zu Virenscannern gibt es bei heuristischer Software keine regelmäßigen Updates über alle bekannten Viren.
Wenn beispielsweise ein neuer Virentyp auftritt, kann diese Software diesen Virentyp nicht erkennen. Erst wenn sie aktualisiert oder ersetzt wurde, ist sie dazu in der Lage.
Auch bei heuristischer Software sind Fehlalarme keine Seltenheit.

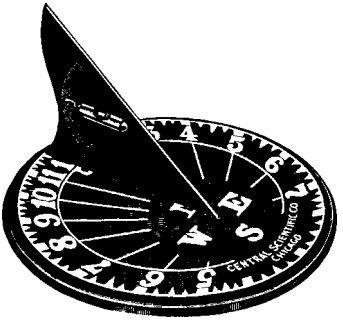
Geschichte der Computerviren

1949 Der Mathematiker John von Neumann stellt theoretische Überlegungen über die selbständige Reproduktion von Computerprogrammen an.

50er Bell Labs entwickeln ein experimentelles Spiel, in dem die Spieler gegenseitig ihre Computer mit Schäden verursachenden Programmen angreifen.

1975 John Brunner, Autor von Science-Fiction-Romanen, entwickelt die Idee von einem „Wurm", der sich in Netzwerken verbreiten kann.

1984 Fred Cohen führt den Begriff „Computervirus" für Programme mit den entsprechenden Eigenschaften ein.



1986 Der erste Computervirus, *Brain*, wird angeblich von zwei Brüdern in Pakistan geschrieben.

1987 Der Wurm *Christmas tree* legt das weltweite IBM-Netzwerk lahm.

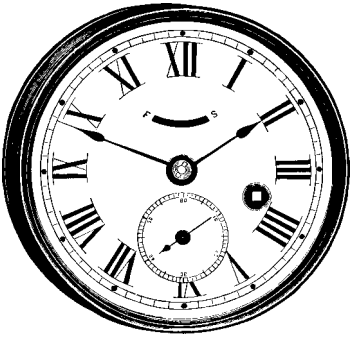
1988 Der *Internet worm* verbreitet sich im US-DARPA-Internet.

1990 Mark Washburn schreibt *1260*, den ersten „polymorphen" Virus, der sich nach jeder Infektion verändert („mutiert").

1992 Der Virus *Michelangelo* sorgt weltweit für Panik, obwohl nur wenige Computer infiziert werden.

1994 *Good Times*, der erste richtige Virenhoax, erscheint.

1995 Der erste Makrovirus, *Concept*, erscheint. Im selben Jahr programmieren australische Virenschreiber den ersten Virus speziell für Windows 95.



1998 *CIH* oder *Chernobyl* ist der erste Virus, der Computer-Hardware beschädigt.

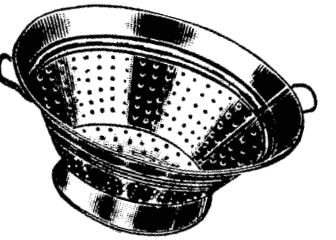
1999 *Melissa*, ein Virus der sich selbst per E-Mail weiterleitet, wird auf der ganzen Welt verbreitet. *Bubbleboy*, der erste Virus, der einen Computer allein durch das Lesen einer E-Mail infiziert, erscheint.

2000 Der *Loveletter-Virus* ist der bisher „erfolgreichste“ Virus. Im selben Jahr tritt der erste Virus für das Palm-Betriebssystem auf, allerdings werden keine Anwender infiziert.

Viren – ganz schön teuer

Viren können zwar Daten verändern oder gar löschen, sie können einem Unternehmen aber auch noch in anderer, nicht sofort sichtbarer Weise schaden.

Jedem ist bekannt, dass Viren sämtliche Daten auf der Festplatte löschen oder Dokumente verändern können. Dies ist natürlich sehr ernst zu nehmen, jedoch lassen sich zerstörte Daten jederzeit durch Backups ersetzen. Viren können aber auch weitaus schlimmere Auswirkungen haben, die nicht immer sofort sichtbar sind.



So hemmen Viren den normalen Arbeitsablauf, wenn in Unternehmen ganze Netzwerke heruntergefahren werden müssen. Als Folge gehen wertvolle Arbeitszeit und damit Umsätze und Profit verloren.

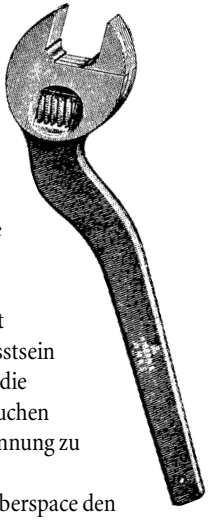
Manche Viren blockieren die Kommunikationskanäle in Unternehmen. So verbreiten sich *Melissa* oder *ExploreZip* über E-Mail und können derart viele E-Mails erzeugen, dass Server sogar abstürzen. Auch wenn ein Server der E-Mail-Flut gewachsen ist, fahren viele Unternehmen ihre E-Mail-Server aus reiner Vorsicht herunter.

Ebenso besteht eine Gefahr für vertrauliche Informationen. *Melissa* kann Dokumente, die vertrauliche Informationen enthalten, an jeden Eintrag in Ihrem Adressbuch weiterleiten.

Den wahrscheinlich größten Schaden durch Viren kann Ihre Glaubwürdigkeit nehmen. Wenn z. B. einem großen Kunden ein infiziertes Dokument geschickt wird, sieht er Sie womöglich nicht mehr als vertrauenswürdigen Geschäftspartner an oder verlangt Schadenersatz von Ihnen. Durch manche Viren können Sie auch in recht peinliche Situationen geraten und so Ihren guten Ruf riskieren. *WM/Polypost* z. B. legt Kopien Ihrer Dokumente in Ihrem Namen bei der Usenet-Newsgroup alt.sex ab.

Wer schreibt eigentlich Viren?

Wenn Ihr Computer von einem Virus befallen wurde, werden Sie sich sicher fragen, wer eigentlich die Schöpfer solcher gemeinen Programme sind.



Auf den ersten Blick scheint es keinen großen Anreiz für das Schreiben von Viren zu geben. Virenprogrammierer haben keine finanziellen Vorteile oder besseren Karrierechancen, noch erlangen sie wirklichen Ruhm. Im Gegensatz zu Hackern haben Virenprogrammierer keine gezielten Opfer, da sich Viren unkontrolliert verbreiten.

Vielleicht hilft es zum besseren Verständnis, wenn man das Virenschreiben mit Vergehen wie dem Anbringen von Graffiti oder Vandalismus vergleicht.

Der durchschnittliche Virenprogrammierer ist jünger als 25 Jahre und Single. Sein Selbstbewusstsein stützt sich sehr stark auf die Bestätigung durch die Clique. Mit dem Programmieren von Viren versuchen solche Leute, sich innerhalb der Gruppe Anerkennung zu verschaffen.

Durch Viren bekommen Virenschreiber im Cyberspace den Erfolg, den sie in der wirklichen Welt vielleicht nie gehabt haben. So ist es auch nicht verwunderlich, dass Virenschreiber sich häufig Namen geben, die durch Heavy-Metal-Musik oder Fantasy-Romane inspiriert wurden, da diese auf ähnlichen Vorstellungen von Tapferkeit und Stärke basieren.

Sind Viren immer schädlich?

Für die meisten von uns sind Viren nur dazu da, um Schaden anzurichten. Trifft dies aber wirklich immer zu?

Es gibt viele „harmlose“ Viren oder auch Viren, die sich einfach einen Spaß mit dem Anwender erlauben und sonst keinen weiteren Schaden anrichten. Wieder andere weisen auf Sicherheitslücken von Software hin. Manche Leute argumentieren sogar, dass Viren nützlich sein können, z. B. um Fehler in Programmen möglichst schnell zu beheben. Allerdings hat sich diese Vorstellung von „harmlosen“ Viren nicht unbedingt bestätigt.

Immerhin nehmen Viren Veränderungen auf den Computern anderer Anwender ohne deren Wissen bzw. Einwilligung vor. Vom ethischen Standpunkt her ist dies unvertretbar – und deshalb in vielen Ländern auch illegal – ganz egal, ob die Absichten gut oder schlecht waren. Niemand sollte sich am Computer eines anderen zu schaffen machen!

Viren verhalten sich auch nicht immer so, wie der Virenprogrammierer es geplant hat. Wenn ein Virus schlecht programmiert ist, kann er unvorhergesehene Probleme verursachen. Auch wenn sich ein Virus auf der Plattform, für die er geschrieben wurde, harmlos verhält, kann er auf anderen Plattformen oder Systemen, die später entwickelt werden, durchaus Schaden verursachen.

Proof of Concept

Manchmal werden Viren nur deshalb geschrieben, um zu beweisen, dass ein neuer Virentyp technisch möglich ist. Diese Viren bezeichnet man als Proof-of-Concept-Viren. Sie haben normalerweise keine Auswirkungen und sollten nicht auf die Computer anderer Anwender übertragen werden.

Forschung?

Virenprogrammierer behaupten gerne, dass sie eigentlich nur Forschung betreiben. Jedoch sind Viren häufig ziemlich schlecht geschrieben und werden willkürlich an Anwender übertragen. Es gibt keine Möglichkeit, die Ergebnisse zu sammeln und auszuwerten. Ob dies als Forschung zu bezeichnen ist, bleibt dahingestellt.

Hoaxes

Wurden Sie schon einmal vor Viren namens „Good Times“, „Budweiser Frogs“ oder „Zlatko“, gewarnt? Dann gehören auch Sie zu den Opfern von Hoaxes. Virenhoaxes werden meist per E-Mail verschickt und sind inzwischen sehr weit verbreitet. Sie können sich für ein Unternehmen als genauso kostspielig und zeitaufwendig erweisen wie ein echter Virus.

Was sind Hoaxes?

Ein Hoax ist eine Meldung über einen angeblichen Virus, der in Wirklichkeit jedoch gar nicht existiert. Hoaxes werden normalerweise per E-Mail verbreitet und haben die folgenden typischen Merkmale:

- Hoaxes warnen vor einem neuen, extrem zerstörerischen Virus, der von Antiviren-Software nicht erkannt wird.
- Sie fordern dazu auf, keine E-Mails mit einer bestimmten Betreffzeile zu lesen, z. B. „Join the Crew“ oder „Budweiser Frogs“.
- Hoaxes geben an, dass diese Warnung von einem der großen Software-Unternehmen, einem Internet-Provider oder einer Regierungsbehörde autorisiert wurde, z. B. IBM, Microsoft, AOL oder FCC.
- In Hoaxes wird behauptet, dass ein neuer Virus Schäden verursacht, die relativ unwahrscheinlich sind. So will z. B. „A Moment of Silence“ weismachen, dass ein neuer Computer auch dann infiziert bleibt, wenn sämtliche Programme ausgetauscht werden.
- Hoaxes verwenden eine extrem hochgestochene technische Sprache. „Good Times“ beispielsweise droht, dass der Virus den PC-Prozessor „in einen endlichen Binärring mit unendlicher Komplexität“ bringt.
- Hoaxes fordern dazu auf, die Warnung an andere Anwender weiterzuleiten.

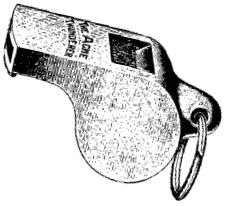
Der Hoax, der keiner war

Am 1. April 2000 kam eine E-Mail namens „Rush-Killer virus alert“ in Umlauf. Diese E-Mail warnte vor Viren, die über das Modem die Nummer 911 (Notruf-Nummer in den USA) wählen und den Empfänger auffordern, die Warnung weiterzuleiten. Die E-Mail wies alle Merkmale eines Hoax auf. Allerdings handelte es sich hierbei um einen echten Virus. Es war einer der *BAT/911*-Viren, die sich über Windows-Freigaben verbreiten und die 911 wählen. Es ist schwierig, einen Hoax von einer wirklichen Warnung zu unterscheiden, deshalb sollten Sie den Abschnitt „Was tun mit Hoaxes?“ am Ende dieses Kapitels lesen.

Warum sind Hoaxes so gefährlich?

Hoaxes können genauso störend und kostenintensiv sein wie echte Viren.

Wenn Anwender eine Hoax-Warnung an sämtliche Freunde und Kollegen weiterleiten, kommt es zu einer regelrechten Flut von E-Mails. E-Mail-Server werden überlastet und stürzen im schlimmsten Fall ab. Dies hat dann denselben Effekt, den auch der Loveletter-Virus hervorgerufen hat, allerdings muss der Verfasser eines Hoax dazu noch nicht einmal einen Viren-Code schreiben.



Es sind aber nicht nur die End-User, die gerne überreagieren. Auch Unternehmen, die einen Hoax erhalten, greifen zu drastischen Maßnahmen und fahren beispielsweise ihre E-Mail-Server oder ihr Netzwerk herunter. Dadurch wird die Kommunikation teilweise stärker gelähmt als durch echte Viren, da so der Zugang zu E-Mails verwehrt wird, die für ein Unternehmen wirklich wichtig sein könnten.

Diese falschen Warnungen lenken die Aufmerksamkeit überdies von wirklichen Virenbedrohungen ab.

Es ist im Übrigen erstaunlich, wie hartnäckig Hoaxes sein können. Da Hoaxes keine Viren sind, werden sie auch von keiner Antiviren-Software erkannt bzw. gestoppt.

Was kam zuerst?

Ein Hoax kann auch erst die Idee für einen neuen Virus liefern, oder ein Virus gibt den Anstoß für einen Hoax. Nachdem der Hoax „Good Times“ für Schlagzeilen gesorgt hatte, warteten einige Virenschreiber ab, bis dieser als Hoax entlarvt war, und schrieben dann einen echten Virus mit demselben Namen (von Antiviren-Software-Herstellern *GT-Spoof* genannt).

Was tun mit Hoaxes?

Wie auch bei Viren oder Kettenbriefen, hängt die Wirksamkeit von Hoaxes von ihrer Verbreitung ab. Wenn Sie die Anwender davon überzeugen können, diese Kette zu durchbrechen, kann der Schaden erheblich vermindert werden.

Unternehmensrichtlinie für Virenwarnungen

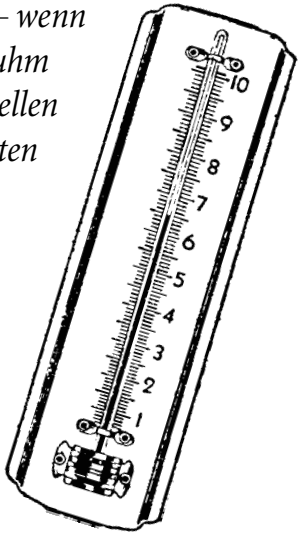
Mit Hilfe einer Unternehmensrichtlinie über Virenwarnungen können Sie diesem Problem begegnen. Hier ein Beispiel: „Leiten Sie jegliche Virenwarnungen an keinen weiter außer an den Antiviren-Verantwortlichen. Es ist völlig egal, ob die Virenwarnungen von einem Hersteller für Antiviren-Produkte oder Ihrem besten Freund kommen oder ob sie von einem großen Computerunternehmen autorisiert wurden. Alle Virenwarnungen sollten nur an <Name des Verantwortlichen> geschickt werden. Es ist dessen Aufgabe, Virenwarnungen zu versenden. Virenwarnungen aus jeder anderen Quelle werden ignoriert.“ Solange die Anwender diese Richtlinie befolgen, wird es keine Flut von E-Mails geben, da einzig der Antiviren-Verantwortliche entscheidet, ob wirklich Gefahr besteht.

Info über Hoaxes

Auf dieser Website finden Sie ausführliche Informationen über Hoaxes: www.sophos.com/virusinfo/hoaxes

„Berühmte“ Viren

Einige Viren sind auf Grund ihrer weiten und ausdauernden Verbreitung zu großem – wenn auch zweifelhaftem – Ruhm gelangt. Im Folgenden stellen wir die bisher bekanntesten Viren vor.



Loveletter

(VBS/LoveLet-A)

Der Loveletter-Virus ist der bisher bekannteste Virus. Er tarnt sich als Liebesbrief und verlässt sich auf die Neugierde der meisten Anwender. So konnte er sich problemlos innerhalb weniger Stunden weltweit verbreiten.

Aufgetreten: Mai 2000
Ursprung: Philippinen
Alias: Lovebug
Typ: Visual-Basic-Script-Wurm
Auslöser: Erstinfektion
Auswirkungen: Die originale Version schickt eine E-Mail mit der Betreffzeile „I LOVE YOU“ und dem Text „kindly check the attached love letter coming from me“. Beim Öffnen des Attachments wird der Virus ausgeführt. Wenn Microsoft Outlook auf dem Rechner installiert ist, versucht der Virus, sich an sämtliche Adressen im Outlook-Adressbuch weiterzuleiten. Der Virus kann sich auch an Newsgroups-User weiterleiten, Benutzerdaten stehlen und bestimmte Dateien überschreiben.

Form

Seit acht Jahren ist der Virus „Form“ in den Top Ten der Viren vertreten, und auch heute noch ist er weit verbreitet. Unter DOS und den frühen Windows-Versionen verhält sich der Virus eher unauffällig, so dass er sich problemlos verbreiten konnte.

Aufgetreten: 1991
Ursprung: Schweiz
Typ: Bootsektorvirus
Auslöser: Am Achtzehnten eines jeden Monats
Auswirkungen: Erzeugt einen Klickton, beim Drücken jeder Taste. Computer unter Windows NT können nicht mehr einwandfrei booten.

Kakworm

(VBS/Kakworm)

Durch Kakworm können Benutzer ihre PCs bereits beim Lesen einer E-Mail mit einem Virus infizieren.

Aufgetreten: 1999
Typ: Visual-Basic-Script-Wurm
Auslöser: Während der Erstinfektion (für die meisten Effekte) oder am Ersten eines jeden Monats (beim Herunterfahren von Windows)
Auswirkungen: Der Wurm verbreitet sich mit Hilfe einer E-Mail-Nachricht. Wenn Sie Outlook oder Outlook Express mit dem Internet Explorer 5 verwenden, kann der Rechner bereits infiziert werden, wenn die E-Mail gelesen oder über „Ansicht“ geöffnet wird. Der Virus verändert die Einstellungen von Outlook Express so, dass sämtliche ausgehenden E-Mails den Virencode automatisch übernehmen. Am Ersten eines jeden Monats um 17.00 Uhr erscheint die Meldung „Kagou-Anti _Kro$oft says not today“, und Windows wird geschlossen.

Anticmos

Anticmos ist ein typischer Bootsektorvirus. Mitte der 90er Jahre war er sehr weit verbreitet und regelmäßig unter den Top-Ten-Viren vertreten.

Aufgetreten: Januar 1994
Ursprung: Erstmals in Hongkong aufgetreten, der Ursprung wird jedoch in China vermutet.
Typ: Bootsektorvirus
Auslöser: Willkürlich
Auswirkungen: Versucht, Informationen über die Typenbezeichnung der installierten Disketten- und Festplattenlaufwerke zu löschen.

Melissa

(WM97/Melissa)

Melissa verbreitet sich mit Hilfe psychologischer Tricks. Der Virus versendet sich in einer E-Mail, die angeblich von einem Bekannten stammt und ein Dokument enthält, das für den Empfänger von Interesse zu sein scheint. Auf diese Weise konnte sich Melissa innerhalb eines einzigen Tages auf der ganzen Welt verbreiten.

Aufgetreten:	März 1999
Ursprung:	Ein 31-jähriger Programmierer aus den USA legte ein infiziertes Dokument bei einer alt.sex-Usenet-Newsgroup ab.
Typ:	Word 97-Makrovirus, auch Word-2000-fähig.
Auslöser:	Erstinfektion
Auswirkungen:	Schickt eine Nachricht an die ersten fünfzig Einträge in allen Adressbüchern, auf die Microsoft Outlook zugreifen kann, und verwendet den Namen des jeweiligen Anwenders in der Betreffzeile. Die E-Mail enthält ein Attachment mit einer Kopie des infizierten Dokuments. Sind Tag und Minute beim Öffnen des Dokuments gleich (z. B. 10:05 Uhr am 5. Mai), fügt der Virus Text über das Spiel Scrabble in das Dokument ein.

New Zealand

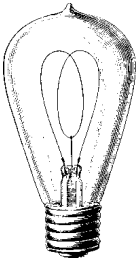
New Zealand war einer der häufigsten Viren in den frühen 90er Jahren.

Aufgetreten:	Ende der 80er Jahre
Ursprung:	Neuseeleand
Alias:	Stoned
Typ:	Bootsektorvirus
Auslöser:	Bei einem von acht Bootversuchen von Diskette
Auswirkungen:	Gibt die Meldung „Your PC is now Stoned!“. Legt eine Kopie des originalen Bootsektors in den letzten Sektor des Rootverzeichnisses einer 360 KB großen Festplatte. Größere Platten können dadurch beschädigt werden.

Concept

(WM/Concept)

Der Erfolg von Concept war vorgezeichnet, denn er wurde versehentlich mit offizieller Microsoft-Software geliefert. Er war der erste Makrovirus „in the wild“ und einer der häufigsten Viren zwischen 1996 und 1998. Der Virus übernimmt die Kontrolle mit Hilfe des Makros AutoOpen, das Word automatisch ausführt, und infiziert den Computer mit dem Makro FileSave, das ausgeführt wird, wenn Word ein Dokument speichert. Es gibt zahlreiche Varianten.



Aufgetreten: August 1995

Typ: Makrovirus

Auslöser: Keiner

Auswirkungen: Wenn Sie ein infiziertes Dokument öffnen, erscheint eine Textmeldung mit dem Titel „Microsoft Word“ und dem Text „1“. Der Virus enthält auch den Text „That's enough to prove my point“, allerdings wird dieser nicht angezeigt.

CIH (Chernobyl)

(W95/CIH-10xx)

CIH war der erste Virus, der die Hardware eines Computers beschädigen konnte. Er überschreibt das BIOS, so dass der Computer nicht benutzt werden kann, bis der BIOS-Chip ausgetauscht ist.

Aufgetreten: Juni 1998

Ursprung: Geschrieben von Chen Ing-Hau aus Taiwan

Typ: Programmvirus, der auf Computern unter Windows 95 läuft

Auslöser: 26. April, jedoch gibt es Varianten, die am 26. Juni oder am 26. eines jeden Monats ausgelöst werden.

Auswirkungen: Überschreibt das BIOS und dann die Festplatte.

Parity Boot

Parity Boot nistet sich auf den Bootsektoren von Disketten ein. Der „Erfolg" von Parity Boot zeigt, dass Bootsektorviren, die in den 80er und frühen 90er Jahren am weitesten verbreitet waren, heutzutage immer noch aktuell sind. Noch im Jahre 1998 war Parity Boot unter den häufigsten Viren vertreten, besonders in Deutschland, wo er sich 1994 über eine Beilage-CD in einem Magazin verbreitet hat.

Aufgetreten:	März 1993
Ursprung:	Vermutlich Deutschland
Typ:	Bootsektorvirus
Auslöser:	Willkürlich
Auswirkungen:	Zeigt die Meldung „PARITY CHECK" an und friert den Computer ein. Dies täuscht einen echten Fehler im Speicher vor. Die Anwender glauben so, dass ein Problem im Arbeitsspeicher vorliegt.

Happy99

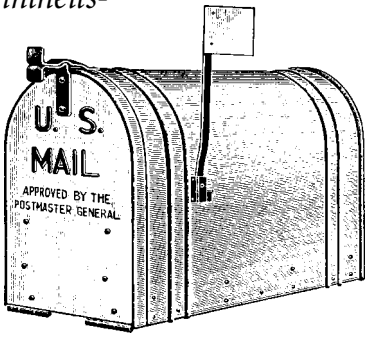
W32/Ska-Happy99

Happy99 war der erste bekannte Virus, der sich selbst relativ schnell per E-Mail verbreitet hat.

Aufgetreten:	Januar 1999
Ursprung:	Ein französischer Virenschreiber namens „Spanska" legte den Virus bei einer Newsgroup ab.
Typ:	Programmvirus, der auf Rechnern unter Windows 95/98/Me/NT/2000 läuft
Auslöser:	Keiner
Auswirkungen:	Erzeugt ein Feuerwerk auf dem Bildschirm mit der Meldung „Happy New Year 1999". Der Virus verändert die Datei wsock32.dll im Windows-Systemverzeichnis, so dass immer dann, wenn eine E-Mail verschickt wird, eine zweite E-Mail mit dem Virus an denselben Empfänger versandt wird.

E-Mail

Die im Moment wohl bekanntesten Viren sind der Loveletter-Virus und Melissa. Beide Viren konnten deshalb zu einem so hohen Bekanntheitsgrad gelangen, weil sie sich per E-Mail auf der ganzen Welt verbreitet haben. E-Mails haben sich inzwischen zum größten Übertragungsmedium von Viren entwickelt. Solange Viren lediglich auf Disketten übertragen wurden, haben sie sich nur sehr langsam verbreitet. Unternehmen hatten die Möglichkeit, Disketten zu verbieten oder jede Diskette auf Viren zu überprüfen. Mit dem zunehmenden E-Mail-Verkehr ist das anders geworden. Dateien werden heutzutage so schnell ausgetauscht, dass Ihr PC mit einem einzigen Mausklick infiziert werden kann. So können sich auch herkömmliche Viren schneller verbreiten, und neue Viren können die Arbeitsweise von E-Mail-Programmen geschickt ausnutzen.



Gefahr beim E-Mail-Lesen?

Viele Anwender glauben, dass sie auf der sicheren Seite sind, solange sie ihre E-Mails öffnen, ohne die Attachments darin zu starten. Seit einiger Zeit ist diese Annahme jedoch falsch.

Viren wie *Kakworm* und *Bubbleboy* infizieren den PC bereits beim bloßen Lesen dieser E-Mails. Diese E-Mail-Viren sehen aus wie jede andere Nachricht, allerdings enthalten sie ein verborgenes Skript, das ausgeführt wird, sobald die E-Mail geöffnet oder auch nur im Ansichtfenster angesehen wird (wenn Sie Outlook mit der entsprechenden Version des Internet Explorers verwenden). Durch dieses Skript werden Ihre Systemeinstellungen geändert, und der Virus wird per E-Mail an andere Anwender versendet.

Microsoft hat inzwischen ein Patch zur Verfügung gestellt, das diese Sicherheitslücke schließt. Es kann unter www.microsoft.com/technet/security/bulletin/ms99-032.asp heruntergeladen werden.

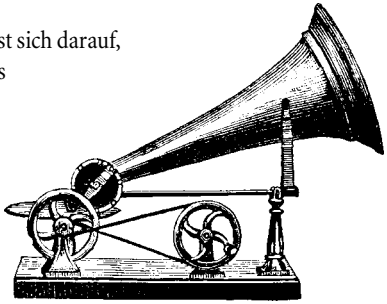
E-Mail-Hoaxes

E-Mails sind auch ein sehr beliebtes Medium für Hoaxes. Hoaxes sind Falschmeldungen über neue Viren, in denen der Empfänger aufgefordert wird, die Nachricht an so viele Leute wie möglich weiterzuleiten.

Ein Hoax kann sich innerhalb eines Netzwerks genauso ausbreiten wie ein richtiger Virus und somit eine regelrechte E-Mail-Flut auslösen. Im Unterschied zu einem Virus muss für einen Hoax noch nicht einmal ein Virencode programmiert werden; der Erfolg liegt einzig und allein in der Leichtgläubigkeit der Anwender. Weitere Informationen dazu finden Sie im Kapitel „Hoaxes“.

Viren, die sich selbst per E-Mail versenden

Die heutzutage „erfolgreichsten" Viren verbreiten sich automatisch per E-Mail.



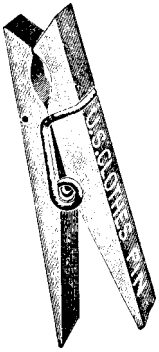
Diese Art von Viren verlässt sich darauf, dass der Anwender auf das angehängte Dokument in der E-Mail klickt. Dadurch wird ein Skript ausgeführt, das mit Hilfe des E-Mail-Programms infizierte Dokumente an andere Anwender weiterleitet. *Melissa* beispielsweise schickt eine Nachricht an die ersten fünfzig Einträge im Adressbuch, auf das Microsoft Outlook zugreift. Andere Viren wiederum senden sich selbst an alle Einträge im Adressbuch.

Was ist Spam?

Als Spam-Mail werden E-Mails bezeichnet, die einem Empfänger unaufgefordert zugeschickt werden. Meist handeln sie von schnellen Verdienstmöglichkeiten, Kreditangeboten oder pornographischen Webseiten. Diese E-Mails haben häufig einen gefälschten Absender, so dass es schwierig ist, den Urheber ausfindig zu machen. Solche E-Mails sollten einfach gelöscht werden.

Gefährliche Attachments

Das im Moment wohl größte Risiko für Ihren PC, von einem Virus infiziert zu werden, stellen nicht E-Mails an sich, sondern E-Mail-Attachments dar.



Alle Programme, Dokumente oder Tabellen, die Sie per E-Mail erhalten, sind potentielle Überträger von Viren. Mit einem einzigen Mausklick auf ein infiziertes Attachment wird Ihr Computer infiziert.

E-Mails sind in den letzten Jahren immer beliebter geworden, und viele Anwender tauschen auf diesem Weg Bildschirmschoner, Grußkarten, Animationen oder witzige Programme aus. Dass diese Attachments Virenüberträger sein können, wird dabei meistens vergessen.

Auch Attachments mit anscheinend sicheren Dateitypen, wie Dateien mit der Erweiterung .txt, können gefährlich sein. Solche „Text-Dateien" können genausogut ein Schäden verursachendes VBS-Skript sein, das seine wirkliche Dateierweiterung (.vbs) einfach nur verbirgt.

Der Wurm *VBS/Monopoly* ist ein Beispiel für ein Schäden verursachendes Programm, das sich als Spaß-Programm tarnt. Es verkleidet sich als „Bill-Gates-Joke" und zeigt ein Monopoly-Spiel mit Microsoft-Bildern an. Allerdings versendet sich das Programm per E-Mail an weitere Anwender und leitet Informationen über Ihr System an bestimmte E-Mail-Adressen weiter. Die Vertraulichkeit von Daten ist somit stark gefährdet.

E-Mails mitlesen und verändern

Eine E-Mail kann nur während der Übertragung heimlich gelesen werden. Mit Hilfe von E-Mail-Verschlüsselungen können Sie sich davor schützen.

E-Mails können auch unbemerkt verändert werden, indem z. B. ein gefälschter Absender angegeben oder der Inhalt der E-Mail geändert wird. Digitale Signaturen bieten Schutz vor solchen Änderungen.

So schützen Sie sich vor E-Mail-Viren

Richtlinien zum Umgang mit E-Mail-Attachments

Mit ein paar einfachen Verhaltensmaßnahmen können Sie sich vor E-Mail-Viren schützen. Öffnen Sie keine Attachments, selbst wenn sie von Ihrem besten Freund kommen. Lassen Sie sich auch nicht dadurch verleiten, dass Ihnen ein „harmloser Scherz“ versprochen wird. Wenn Sie nicht absolut sicher sind, dass ein Attachment virenfrei ist, sollten Sie zunächst immer davon ausgehen, dass es infiziert ist. Eine Unternehmensrichtlinie kann regeln, dass alle Attachments freigegeben und mit Antiviren-Software überprüft werden müssen, bevor sie ausgeführt werden.

Deaktivieren Sie Windows Scripting Host

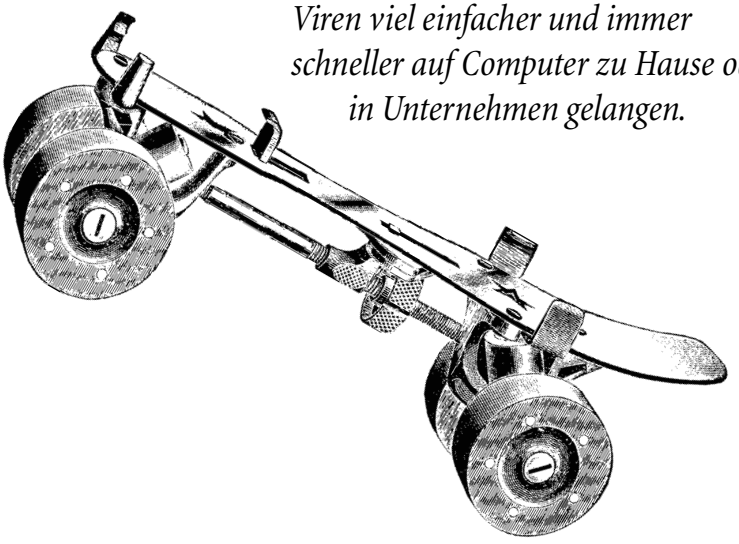
Windows Scripting Host (WSH) automatisiert bestimmte Vorgänge, z. B. das Ausführen von VBS- oder Java-Skripts. Allerdings gibt WSH auch Viren, wie dem Loveletter-Virus, die Möglichkeit, sich zu verbreiten. Möglicherweise kommen Sie ohne WSH aus (fragen Sie dazu bitte Ihren Netzwerkadministrator). Unter www.sophos.com/support/faqs/wsh.html finden Sie Hinweise zum Deaktivieren von WSH. Beachten Sie, dass jedes Mal, wenn Sie Windows oder den Internet Explorer mit einer neueren Version aktualisieren, WSH erneut aktiviert wird.

Setzen Sie Antiviren-Software ein

Setzen Sie auf allen Desktops und an allen E-Mail-Gateways Antiviren-Software ein, die über eine Option zur Überprüfung bei Zugriff (On-Access-Scan) verfügt. Damit sind Sie vor E-Mail-Viren bestens geschützt.

Internet

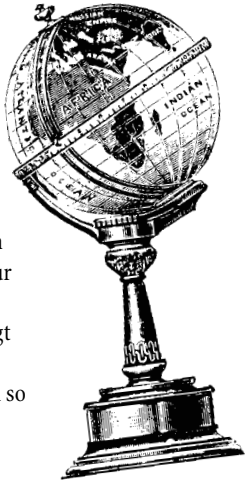
Durch das Internet wird eine stetig wachsende Menge an Informationen für mehr und mehr Anwender zugänglich. Trotz der vielen Vorteile, die das Internet bietet, sollte man auch die Nachteile nicht unterschätzen. Denn mit Hilfe des Internets können auch Viren viel einfacher und immer schneller auf Computer zu Hause oder in Unternehmen gelangen.



Virus per Mausklick?

Durch das Internet ist die Gefahr, dass Ihr Computer mit einem Virus infiziert wird, extrem gewachsen.

Vor ungefähr zehn Jahren wurden die meisten Viren über Disketten verbreitet. Die Verteilung ging daher ziemlich langsam vonstatten und hing hauptsächlich von den Anwendern ab, die die neuen Programme überhaupt erst einmal ausführen mussten. Waren die Auswirkungen des Virus zu offensichtlich, dann sank auch die Wahrscheinlichkeit einer Infektion. Durch das Internet, das von immer mehr Menschen verwendet wird, hat sich in dieser Hinsicht jedoch vieles geändert.



Über das Internet kann Software relativ einfach ausgetauscht werden. Mit einem Mausklick hängt man ein Programm an eine E-Mail an, und ebenfalls mit nur einem Mausklick kann der Empfänger das Programm starten. Programme können auch auf Websites abgelegt werden, von wo aus sie jeder herunterladen kann. Programmviren, die Programme befallen, können sich so im Internet optimal verbreiten.

Makroviren, die Dokumente befallen, profitieren ebenfalls vom regen Informationsaustausch über das Internet. Egal, ob ein Dokument per E-Mail verschickt oder aus dem Internet heruntergeladen wurde: Ein einziger Mausklick auf die Datei reicht aus, um Ihren Computer zu infizieren.

Wenn Sie das Internet häufig nutzen, sollten Sie Dokumente mit einem Viewer anschauen, der Makros ignoriert, und auf keinen Fall Programme starten, die nicht von einer vertrauenswürdigen Quelle stammen.

Risiko Website?

Eine Website nur anzusehen ist weit weniger gefährlich, als unbekannte Programme oder Dokumente zu starten. Die Gefahr, die von Websites ausgeht, hängt davon ab, welcher Code auf der Website verwendet wird und welche Sicherheitsstandards der Service-Provider und auch Sie selbst einsetzen. Im folgenden werden die häufigsten Codes auf Websites kurz erläutert.

HTML

Websites werden in HTML (Hypertext Markup Language) geschrieben. Mit dieser Sprache können Web-Designer Text formatieren und Links zu Grafiken und anderen Websites erstellen. In HTML-Code selbst können sich keine Viren verbergen, allerdings können Websites Codes enthalten, die automatisch Anwendungen ausführen oder Dokumente öffnen. Dann besteht die Gefahr, dass ein infiziertes Objekt unbemerkt ausgeführt wird.

ActiveX

ActiveX ist eine Microsoft-Technologie für Web-Designer, die mit Computern unter Windows arbeiten.

ActiveX-Applets werden für visuelle Effekte auf Websites verwendet und haben vollen Zugriff auf die Ressourcen Ihres Computers. Somit stellen sie eine reelle Gefahr dar. Digitale Signaturen, die beweisen, dass ein Applet authentisch ist und nicht manipuliert wurde, bieten hier einen gewissen Grad an Sicherheit.

Noch mehr Codes

Java

Viele Anwender sind übertrieben vorsichtig bei Java-Viren aus dem Internet. Allerdings verwechseln die meisten dabei Java-Applets, mit denen auf Webseiten spezielle Effekte erzeugt werden können, mit Java-Anwendungen und JavaScripts.

Applets sind in der Regel sicher. Sie werden vom Browser in einer sicheren Umgebung, der so genannten „Sandbox", ausgeführt. Auch wenn ein Applet durch eine Sicherheitslücke gelangen sollte, kann sich ein Schäden verursachendes Applet nicht so einfach verbreiten. Applets werden normalerweise von einem Server auf den Computer des Anwenders kopiert, und nicht von Anwender zu Anwender. Hinzu kommt, dass Applets nicht auf der Festplatte gespeichert werden (abgesehen vom Webcache).

Bei den meisten bösartigen Applets handelt es sich um Trojaner, d. h. Schäden verursachende Programme, die sich als legale Software tarnen.

Java-Anwendungen sind einfache, in Java geschriebene Programme. Wie jedes andere Programm auch, können sie natürlich Viren enthalten. Daher sollten Sie mit derselben Vorsicht behandelt werden wie alle anderen Programme auch.

JavaScript ist ein aktives Skript, das in HTML-Code auf Websites eingebettet ist. Wie andere Skripts auch, kann es bestimmte Vorgänge automatisch ausführen, was ein gewisses Gefahrenpotential darstellt. Sie können aktive Skripts jedoch auch deaktivieren (im Abschnitt „Sicherheit im Internet" am Ende dieses Kapitels finden Sie dazu nähere Informationen).

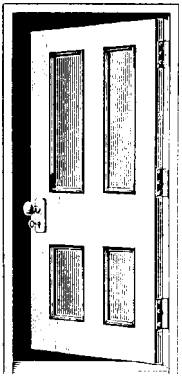
VBS-Skript

Je nach dem verwendeten Webbrowser kann VBS (Visual Basic Script) starten, sobald eine Webseite geöffnet wird. Eine Eingabe des Anwenders ist dabei nicht erforderlich.

VBS-Skript wird z. B. von den E-Mail-Würmern *Kakworm* und *Bubbleboy* ausgenutzt und kann auch von Webseiten aus gestartet werden.

Backdoor-Trojaner

Ein Backdoor-Trojaner ist ein Programm, mit dem man via Internet den PC eines anderen Anwenders kontrollieren kann.



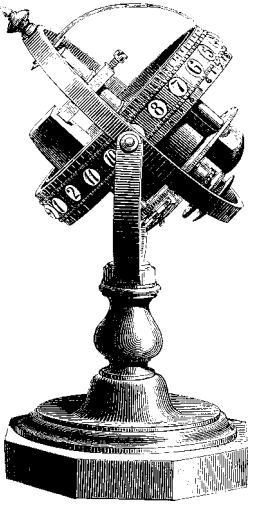
Wie alle normalen Trojaner tarnt sich ein Backdoor-Trojaner als legale oder zumindest interessante Software. Wird das Programm gestartet (normalerweise auf einem Windows-95- oder -98-PC), fügt sich das Programm zur Startroutine des PCs hinzu. Der Trojaner überwacht den Rechner so lange, bis eine Verbindung zum Internet aufgebaut ist. Ist der PC online, kann der Sender des Trojaners mit Hilfe von spezieller Software auf dem infizierten Computer Programme öffnen und schließen, Dateien verändern und auch Druckaufträge an den Drucker senden. Zwei der bekanntesten Backdoor-Trojaner sind *Subseven* und *BackOrifice*.

Sind Cookies ein Risiko?

Cookies stellen keine direkte Bedrohung für Ihren Computer oder Ihre Daten dar. Allerdings gefährden sie Ihre Privatsphäre: Mit Hilfe von Cookies kann eine Webseite Ihre Daten speichern und registrieren, wie oft Sie die Webseite besuchen. Wenn Sie lieber anonym bleiben möchten, können Sie Cookies über die Sicherheitseinstellungen in Ihrem Browser deaktivieren.

Angriffe auf Webserver

Die Gefahr aus dem Internet besteht nicht nur für den End-User. Einige Hacker greifen sogar Webserver an, um deren Webseiten für den Zugriff zu sperren.



Eine häufige Form eines solchen Angriffs ist, derart viele Anfragen an einen Webserver zu senden, dass er extrem langsam arbeitet oder völlig abstürzt. Die Anwender können dann nicht mehr auf die Website, die auf dem Server liegt, zugreifen.

CGI (Common Gateway Interface)-Skripte sind ein weiterer Schwachpunkt. Diese Skripte laufen auf Webservern, um u. a. Suchmaschinen zu unterstützen und Eingaben in Formularen zu verarbeiten. Hacker nutzen die häufig schlecht implementierten CGI-Skripte aus, um die Kontrolle über einen Server zu übernehmen.

Sicherheit im Internet

Um das Internet sicher zu benutzen, sollten Sie die folgenden Ratschläge befolgen:

Getrenntes Netzwerk für Internet-PCs

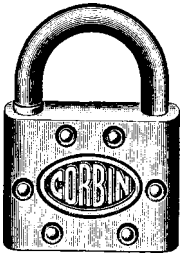
Trennen Sie die PCs, die an das Internet angeschlossen sind, vom übrigen Netzwerk. So reduzieren Sie das Risiko, dass infizierte Dateien heruntergeladen werden und sich Viren in Ihrem Hauptnetzwerk ausbreiten können.

Firewall und/oder Router

Mit Hilfe einer Firewall gelangen nur freigegebene Daten in Ihr Unternehmen. Ein Router steuert den Weg, den Datenpakete aus dem Internet innerhalb Ihres Unternehmens nehmen.

Konfiguration Ihres Internet-Browsers

Deaktivieren Sie Java- oder ActiveX-Applets, Cookies usw. oder lassen Sie sich warnen, wenn solche Codes verwendet werden. Gehen Sie z. B. im Microsoft Internet Explorer auf **Extras|Internetoptionen|Sicherheit|Stufe anpassen** und wählen Sie die gewünschten Sicherheitseinstellungen aus.



Mobiltelefone und Palmtops

Schon heute haben die meisten Menschen von ihrem PC aus Zugang zum Internet. Bald werden wir auch mit Hilfe unserer Handys auf das Internet zugreifen können. Mit den neuesten Mobiltelefonen kann man bereits auf internetähnliche Seiten und Dienste zugreifen, und dies ist erst der Anfang in der Entwicklung solcher Geräte. Je einfacher es allerdings wird, Daten auf mobile Geräte zu übertragen, desto größer wird auch das Sicherheitsrisiko.

Gibt es Viren auch auf Mobiltelefonen?

Zum jetzigen Zeitpunkt gibt es – entgegen allen Behauptungen in den Medien – keine Viren, die Mobiltelefone infizieren können.

Allerdings gab es Viren, die Nachrichten an Telefone gesendet haben. Der Wurm *VBS/Timo-A* verbreitet sich beispielsweise per E-Mail und sendet über das Modem Textnachrichten (SMS) an bestimmte Nummern von Mobiltelefonen. Der berühmt-berüchtigte *Loveletter-Virus* konnte ebenfalls Text an Faxgeräte und Mobiltelefone weiterleiten. Diese Viren sind jedoch nicht in der Lage, ein Mobiltelefon zu infizieren.

Mit zukünftigen, raffinierteren Modellen kann sich dies allerdings sehr schnell ändern.

Daten auf mobilen Geräten

Mobile Geräte bieten auf keinen Fall dieselbe Sicherheit für Daten wie ein PC:

- Sie können verloren gehen oder gestohlen werden.
- Unterbrechungen in der Stromzufuhr können zu Datenverlust führen.
- Daten werden nicht gesichert.

Mobile Geräte werden immer komplexer und somit auch anfälliger für Viren und Hacker.

WAP-Telefone und Viren

WAP (Wireless Application Protocol) taucht immer häufiger als Stichwort im Zusammenhang mit Viren auf Mobiltelefonen auf.

WAP bietet internetähnliche Informationen und Dienste für Mobiltelefone und Organiser. Es basiert auf dem gleichen Modell wie die Web-Kommunikation, d. h., ein zentraler Server liefert den Code, der von einem Browser auf Ihrem Telefon ausgeführt wird. Zum jetzigen Zeitpunkt sind die Verbreitungsmöglichkeiten für Viren auf diesem Weg noch stark eingeschränkt.

So kann ein Virus zwar den Server an sich infizieren, allerdings sind die Chancen, dass er sich verbreitet oder dass Anwender davon betroffen werden, minimal.

Erstens gibt es in einem WAP-System keinen Ort, an dem sich ein Virus kopieren bzw. aufhalten könnte, denn im Gegensatz zum PC sind auf einem WAP-Telefon keine Anwendungen gespeichert. Das Telefon lädt nur den benötigten Code herunter, wobei keine Kopie abgelegt wird, abgesehen von temporären Kopien im Browser-Cache.

Zweitens kann sich ein Virus noch nicht von Anwender zu Anwender übertragen, da zwischen den Client-Telefonen keine netzwerkähnliche Verbindung besteht.

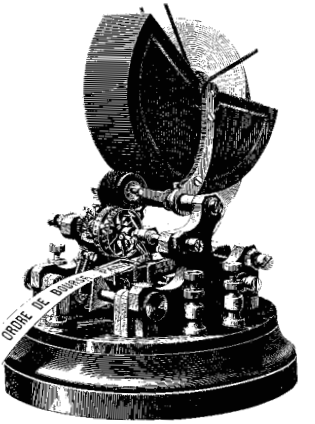
Allerdings könnte ein „Virus“ rein theoretisch *Links* zu WAP-Seiten versenden, auf denen Anwender dazu verleitet werden, gefährliche Anwendungen zu starten. Hierbei wird der Virencode aber immer noch von einem Server aus gestartet.

Schlagwörter

WAP	„Wireless Application Protocol“
WML	„Wireless Markup Language“
WML-Skript	Programmiersprache, ähnlich JavaScript
Cards	Seiten in WML
Deck	Gruppe zusammenhängender Seiten, die ohne weitere Downloads für einen WAP-Browser zur Verfügung stehen

WAP und die möglichen Gefahren

WAP verwendet eine Version von HTTP (dem Protokoll für Seiten im World Wide Web), die durchaus komplexere Inhalte übertragen kann, als WAP-Browser im Moment verarbeiten können. Zukünftige Generationen von Browsern sind wahrscheinlich in der Lage, Dateien sowie Dokumente, die Makroviren enthalten können, herunterzuladen.



Mit der WAP-Technik wird der Server in naher Zukunft in der Lage sein, Inhalte auf Mobiltelefone zu übertragen. Mit der „Push-Technologie“ kann der Anwender benachrichtigt werden, wenn Informationen (z. B. Börsendaten oder Sportergebnisse) aktualisiert werden oder neue E-Mails angekommen sind. Daten können aber auch automatisch in den Cache geladen werden. Viren können damit dieses System ausnutzen, um sich selbst zu verbreiten.

Es gibt aber noch weitere potentielle Probleme. Heimtückische WAP-Seiten können sich als nützliche Dienste tarnen. Später können sie z. B. den Browser zum Absturz bringen oder den ganzen Speicher belegen.

Schlagwörter

XML „eXtensible Markup Language“, empfohlene Sprache zum Gebrauch für das Internet

WTLS „Wireless Transport Layer Security“, Verschlüsselungsmethode in Netzwerken von Mobiltelefonen

Betriebssysteme mobiler Geräte

Palmtops und Persönliche Digitale Assistenten (PDAs) werden in naher Zukunft mit aller Wahrscheinlichkeit ebenfalls neue Angriffsflächen für Viren bieten.

Auf Palmtops und PDAs laufen speziell geschriebene oder speziell zugeschnittene Betriebssysteme – z. B. EPOC, PalmOS und PocketPC (ehemals Windows CE). Mit diesen Systemen können möglicherweise Versionen von üblichen Desktop-Anwendungen verwendet werden, so dass sie ebenso wie Desktop-Computer anfällig für Virencodes werden. Bereits Anfang 2001 gab es Viren, die das Palm-Betriebssystem angegriffen haben.

Palmtops werden regelmäßig an PCs zu Hause oder im Büro angeschlossen, um die Daten zwischen zwei Rechnern zu synchronisieren (z. B. Daten im Adressbuch oder Kalender). Während solcher Datensynchronisationen können sich Viren ganz einfach ausbreiten.

Es ist heute schwer zu sagen, was erfolgreicher sein wird: mobile Computer oder raffinierte Mobiltelefone. Die Sicherheitsrisiken werden auf jeden Fall zunehmen, da die Kommunikationsfähigkeiten von mobilen Computern stetig verbessert werden.

Schlagwörter

EPOC	Betriebssystem für Palmtops
PDA	Persönlicher Digitaler Assistent
PalmOS	Betriebssystem für Palm-Computer
PocketPC	Betriebssystem von Microsoft für Palmtops, ehemals Windows CE
UPNP	Universal Plug and Play, System von Microsoft, um Mobiltelefone mit anderen Geräten zu verbinden

Viren

E-Mail

Internet


Handy & PDA

Sicherheit

Mehr Info

Viren im Kühlschrank?

Geräte werden in Zukunft immer mehr miteinander über Infrarot-Datenübertragung und Niederfrequenzfunk kommunizieren, was eine Vielzahl neuer Sicherheitsrisiken nach sich zieht.

Bluetooth ist ein Standard für die Datenkommunikation per Niederfrequenzfunk über kleinere Distanzen, wie z. B. 10 Meter. Computer, Mobiltelefone, Faxgeräte und sogar Haushaltsgeräte, wie Videorekorder oder Kühlschränke, können mit Hilfe von Bluetooth herausfinden, welche Dienste die Geräte in der Nähe anbieten, und transparent Verbindungen zu ihnen aufbauen.

Es gibt bereits Software, die das Prinzip von Bluetooth ausnutzt. Mit Hilfe der Jini-Technologie von der Firma Sun beispielsweise können Geräte Verbindungen zueinander aufbauen, Java-Code automatisch austauschen und Dienste fernbedienen. Ein Risiko besteht dann, wenn ein unbefugter Anwender oder Schaden verursachender Code mit Hilfe von Bluetooth diese Dienste stört.

Bluetooth und Jini wurden so entwickelt, dass nur ein sicherer Code aus bekannten Quellen sensible Vorgänge ausführen kann. Dadurch ist eine Virenattacke relativ unwahrscheinlich; hat jedoch ein Virus die Sicherheitsbarrieren erst einmal überwunden, ist seine Verbreitung kaum noch aufzuhalten.

Schlagwörter

3G Mobiltelefon-Technologie der „Dritten Generation“

Bluetooth Datenübertragung per Funk über kleine Distanzen

Jini Technologie, mit der verschiedene Geräte Java-Code austauschen können

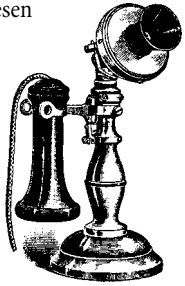
MExE „Mobile station application Execution Environment“, möglicher Nachfolger von WAP, mit dem Service-Provider den Javacode auf ein Telefon herunterladen können

Sicherheit für mobile Geräte

Mit der rasanten Entwicklung auf dem Gebiet der Technologie für Mobiltelefone und PDAs müssen natürlich auch die Sicherheitsstandards mithalten. Eine der Hauptfragen dabei ist, wo Antiviren-Schutzmaßnahmen am effektivsten eingesetzt werden.

Überprüfung am Gateway oder während der Übertragung

In naher Zukunft wird der beste Schutz für mobile Geräte die Virenüberprüfung während der Datenübertragung sein. Bei Mobiltelefonen installiert man einen Virenschutz am besten am WAP-Gateway. Sämtliche Kommunikation geht unverschlüsselt durch diesen Gateway, so dass sich hier eine ideale Möglichkeit für Virenüberprüfungen bietet.



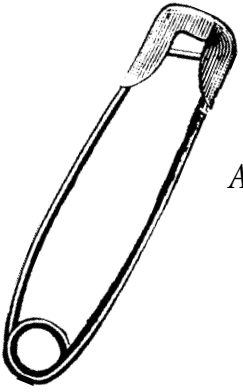
Palmtops werden am besten während der Datensynchronisation mit einem PC auf Viren überprüft. Auf dem PC selbst ist der größte Teil der Software für die Virenüberprüfung installiert, so dass die geringe Leistung und der kleine Speicher eines Palmtops keine Rolle spielen.

Virenüberprüfung auf mobilen Geräten

Da mobile Geräte immer stärker vernetzt werden, wird es sehr schwer, den Datentransfer von einem zentralen Punkt aus zu kontrollieren. Um dieses Problem zu lösen, muss auf jedem Gerät Antiviren-Software installiert werden. Dies ist natürlich erst dann möglich, wenn mobile Geräte über die nötige Leistung und Speicherkapazität verfügen.

Viren? – Kein Problem!

Neben dem Einsatz von Antiviren-Software gibt es noch eine Reihe weiterer Möglichkeiten, wie Sie sich und Ihr Unternehmen vor Viren schützen können. Hier finden Sie die zehn nützlichsten Tipps für sicheres Arbeiten am Computer.



So haben Viren keine Chance

Keine Dokumente in DOC- und XLS-Format

Speichern Sie Ihre Word-Dokumente als RTF (Rich Text Format)- und Ihre Excel-Tabellen als CSV (Comma Separated Values)-Dateien. Diese Formate unterstützen keine Makros, d. h., sie können auch keine Makroviren, einen der häufigsten Virentypen, übertragen. Bitten Sie andere, Ihnen nur RTF- oder CSV-Dateien zu senden. Seien Sie aber dennoch vorsichtig! Manche Makroviren unterwandern den Befehl **Datei|Speichern unter|RTF** und zeigen die Datei zwar mit der Erweiterung RTF an, speichern sie in Wirklichkeit aber in DOC-Format. Wenn Sie hundertprozentig sicher sein möchten, verwenden Sie reine Textdateien.

Vorsicht bei nicht angeforderten Attachments

Führen Sie keine Programme oder Dokumente aus, die Sie nicht persönlich angefordert haben. Wenn Sie nicht absolut sicher sind, dass ein Attachment virenfrei ist, sollten Sie immer davon ausgehen, dass es infiziert ist. Erklären Sie Ihren Kollegen, warum sie auf keinen Fall nicht-freigegebene Programme oder Dokumente – auch Bildschirmschoner oder Spaß-Programme – aus dem Internet herunterladen sollen. Hilfreich können Richtlinien sein, die besagen, dass alle Programme von einem IT-Manager freigegeben und auf Viren überprüft werden müssen, bevor sie benutzt werden.

Virenwarnungen an einen Verantwortlichen weiterleiten

Hoaxes stellen ein ebenso großes Problem dar wie Viren selbst. Erklären Sie Ihren Kollegen, dass es wenig Sinn macht, Virenwarnungen an sämtliche Einträge im Adressbuch weiterzuleiten. Legen Sie in einer Firmenrichtlinie fest, dass alle Warnungen nur an eine bestimmte Person oder Abteilung weitergeleitet werden sollen.

So haben Viren keine Chance

Windows Scripting Host deaktivieren

Wenn Sie Windows Scripting Host (WSH) nicht unbedingt benötigen, sollten Sie es deaktivieren. WSH automatisiert unter Windows bestimmte Vorgänge und gibt so E-Mail-Viren wie *Loveletter* oder *Kakworm* Gelegenheit, sich zu verbreiten. Im Bereich FAQ unter www.sophos.com/support/faqs/wsh.html finden Sie eine Anleitung, wie WSH deaktiviert wird.

Informieren Sie sich

Informieren Sie sich regelmäßig über sicherheitsrelevante Themen, und laden Sie sich Patches zum Schutz vor neuen Viren herunter. Siehe auch Kapitel „Interessante Links“.

Unerwünschte Dateitypen am Gateway stoppen

Viele Viren verwenden VBS (Visual Basic Script)- und SHS (Windows Scrap Objekt)-Dateien für ihre Verbreitung. Da es relativ unwahrscheinlich ist, dass Ihnen solche Dateien extern zugesandt werden, können Sie diese Dateitypen bereits am E-Mail-Gateway zurückhalten.

Bootsequenz ändern

Die meisten Computer versuchen zunächst, von Diskette (Laufwerk :A) zu booten. Die IT-Abteilung in Ihrem Unternehmen sollte die CMOS-Einstellungen auf allen Computern so ändern, dass standardmäßig von der Festplatte gebootet wird. Wenn dann eine infizierte Diskette versehentlich im Computer gelassen wird, kann der Rechner nicht mit einem Bootsektorvirus infiziert werden. Wenn Sie trotzdem einmal von Diskette booten müssen, können Sie diese Einstellungen jederzeit zurücksetzen.

Viren

E-Mail

Internet

Handy & PDA


Sicherheit

Mehr Info

So haben Viren keine Chance

Schreibgeschützte Disketten

Verwenden Sie für Disketten den Schreibschutz, bevor sie diese an andere Anwender weitergeben. Eine schreibgeschützte Diskette kann nicht infiziert werden.

E-Mail-Benachrichtigungsservice

Ein E-Mail-Benachrichtigungsservice informiert Sie über neue Viren und stellt Virenkennungen zur Verfügung, mit denen Ihre Antiviren-Software alle neuen Viren erkennen kann. Sophos bietet einen solchen Service kostenlos unter www.sophos.com/virusinfo/notifications an.

Regelmäßige Backups

Wenn Sie regelmäßig Backups Ihrer Daten erstellen, können Sie nach einer Virusinfektion alle verloren gegangenen Daten und Programme ohne Probleme ersetzen.

Interessante Links

Auf den folgenden Websites finden Sie weitere Informationen:

Vireninformation
www.sophos.com/virusinfo/analyses

Hoaxes und Virenwarnungen
www.sophos.com/virusinfo/hoaxes
www.vmyths.com

Automatische Benachrichtigung über neue Viren
www.sophos.com/virusinfo/notifications

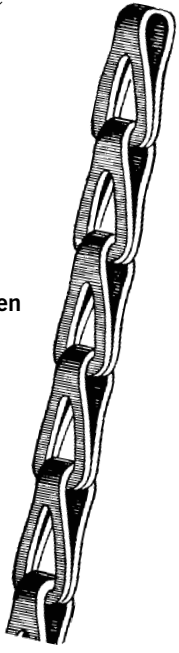
Microsoft Security Bulletins
www.microsoft.com/security

Netscape Security Center
home.netscape.com/security

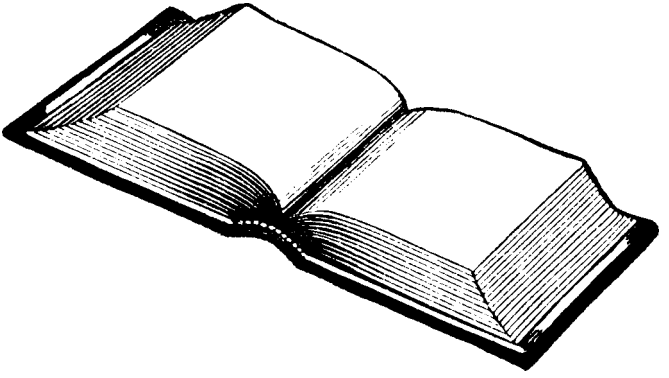
Java Sicherheitsinformationen
java.sun.com/security

The WildList Organization
www.wildlist.org

Virus Bulletin
www.virusbtn.com



Glossar



ActiveX: Microsoft-Technologie zum Erweitern der Kapazitäten eines Webbrowsers.

Applet: Kleine Anwendung. Meist im Zusammenhang mit Java-Applets (siehe Java).

Arbeitsplatzrechner: Einzelcomputer, häufig an ein Netzwerk angeschlossen.

ASCII: American Standard Code for Information Interchange. Standardsystem für die Darstellung von Buchstaben und Symbolen.

Attachment: Dokumente, Tabellen, Grafiken, Programme oder andere Dateien, die an eine E-Mail-Nachricht angehängt werden.

Backdoor: Illegale Methode, das normale Zugriffskontrollsystem eines Computers zu umgehen. Siehe auch Backdoor-Trojaner.

Backdoor-Trojaner: Trojanisches Pferd (siehe Trojanisches Pferd), das Anwendern unbefugten Fernzugriff und Fernkontrolle über einen Computer gibt.

Backup: Kopie von Computerdaten zum Wiederherstellen von verloren gegangenen, verlegten, beschädigten oder gelöschten Daten.

Begleitvirus: Virus, der ausnutzt, dass das Betriebssystem bei zwei Programmen mit gleichem Namen über die Dateierweiterungen entscheidet, welches Programm gestartet wird. DOS-Computer beispielsweise starten eine .com-Datei vor einer .exe-Datei. Der Virus erzeugt eine .com-Datei mit Virencode und gibt ihr den Namen einer bereits bestehenden .exe-Datei.

Betriebssystem: Programm, das die Hardware-Ressourcen eines Computers steuert und grundlegende Funktionen ausführt, wie das Erstellen von Dateilisten und das Starten von Programmen.

BIOS: Basic Input Output System. Die niedrigste Stufe von Software; ist direkt mit der Hardware verbunden.

Booten: Erster Prozess nach dem Einschalten eines Computers, bei dem das Betriebssystem von der Festplatte geladen wird.

Bootsektor: Der Teil des Betriebssystems, der nach dem Einschalten eines PCs zuerst in den Speicher gelesen wird. Das Programm auf dem Bootsektor wird dann ausgeführt, wobei der Rest des Betriebssystems geladen wird.

Bootsektorvirus: Virus, der den Bootvorgang unterwandert.

CGI: Common Gateway Interface. Mechanismus, mit dem ein Webserver Programme oder Skripte ausführen kann und die Ausgaben an den Webbrowser des Anwenders schickt.

Cookie: Kleines Datenpaket, das Informationen über den Computer eines Anwenders speichert. Cookies werden üblicherweise benutzt, um Besuche auf Webseiten aufzuzeichnen und Informationen über die Besucher zu speichern.

CSV: Comma Separated Values. Dateiformat, in dem Werte (z. B. in einer Excel-Tabelle) durch Kommas getrennt angezeigt werden. Das Format unterstützt keine Makros, so dass es keine Makroviren übertragen kann.

Dateivirus: Siehe Programmvirus.

Digitale Signatur: Methode, mit der sichergestellt wird, dass eine Nachricht nicht verändert wurde und dass sie tatsächlich vom angegebenen Sender stammt.

Diskette: Austauschbare magnetische Platte zum Speichern von Daten.

Viren

E-Mail

Internet

Handy & PDA

Sicherheit


Mehr Info

DOS-Bootsektor:	Bootsektor, der DOS in den PC-RAM lädt. Häufiger Angriffspunkt für Bootsektorviren.
Download:	Datenübertragung von einem Computer (meist ein Server) auf einen anderen Computer.
Festplatte:	Versiegelte magnetische Platte in einem Computer, auf der Daten gespeichert werden.
Fileserver:	Computer, auf dem zentral Daten und oftmals Dienste für die Arbeitsplatzrechner im Netzwerk gespeichert werden.
Firewall:	Sicherheitssystem zwischen dem Internet und dem Netzwerk eines Unternehmens, das nur freigegebenen Netzwerkverkehr durchlässt.
FTP:	File Transfer Protocol. System, mit dem sich Internetanwender mit Websites verbinden und Dateien dorthin laden oder von dort herunterladen können.
Gateway:	Computer, der entweder zur Datenübertragung dient (d. h. ein E-Mail-Gateway, der sämtliche E-Mails verarbeitet, die in ein Unternehmen gelangen) oder Daten von einem Protokoll zu einem anderen konvertiert.
Hacker:	Computeranwender, der versucht, unbefugt auf die Computersysteme anderer Anwender zuzugreifen.
Heimlicher Virus:	Virus, der sich vor dem Computeranwender und Antiviren-Programmen verborgen hält, indem er Unterbrechungsdienste überlistet.
Heuristischer Scanner:	Programm, das Viren mit Hilfe von allgemeinen Mustern für Viren und deren Verhalten erkennt.
Hoax:	Meldung über einen nichtexistenten Virus.
HTML:	Hypertext Markup Language. Format für die meisten Dokumente im Internet.

HTTP: Hypertext Transfer Protocol. Protokoll, das Webserver verwenden, um Dokumente für Webbrowser zur Verfügung zu stellen.

Hypertext: Computerlesbarer Text zum umfangreichen Verknüpfen von Dateien.

Internet: Netzwerk aus verschiedenen, miteinander verbundenen Netzwerken. Das *Internet* ist das weitaus größte dieser Netzwerke.

Java: Plattformunabhängige Programmiersprache für das Internet, entwickelt von Sun Microsystems. Java-Programme sind entweder Anwendungen oder Applets (kleine Anwendungen).

Java-Anwendung: Java-basiertes Programm mit vollen Funktionen, z. B. Speicherung von Dateien auf Diskette.

Java-Applet: Kleine Anwendung für Effekte auf Websites. Applets werden vom Webbrowser in einer sicheren Umgebung (siehe Sandbox) ausgeführt und können keine Änderungen auf Ihrem System vornehmen.

Kennwort: Zeichenkette, die Zugriff auf ein System gibt.

Laptop: Tragbarer Computer, mit dem überall bequem gearbeitet werden kann.

Linkvirus: Virus, der Verzeichniseinträge unterminiert, so dass sie zum Virencode verweisen und diesen ausführen.

Makro: Anweisungen in einer Datei, die Programmbefehle automatisch ausführen, z. B. Dateien öffnen und schließen.

Makrovirus: Virus, der mit Hilfe von Makros in Dateien aktiv wird und sich selbst an andere Dateien anhängt.

Masterbootsektor: Der erste physische Sektor auf der Festplatte, der beim Bootvorgang geladen und ausgeführt wird. Der kritischste Teil des Startcodes.

Mehrteiliger Virus: Virus, der sowohl Bootsektoren als auch Programmdateien infiziert.

Modem: MOdulator-DEModulator. Konvertiert Computerdaten in eine Form, in der sie per Telefon, Funk oder Satellit übertragen werden können.

Notebook: Computer, der noch kleiner als ein Laptop ist.

Palmtop: Computer, der aufgrund seiner Größe in einer Hand gehalten werden kann.

PC: Personal Computer. Desktop-Computer oder tragbarer Einzelarbeitsplatzrechner.

PDA: Persönlicher Digitaler Assistent. Kleiner, mobiler Computer zur Datenverwaltung von Adressbüchern und Kalendern.

Polymorpher Virus: Virus, der sich selbst verändert. Der Virus verändert seinen Code stetig und ist daher nur schwer zu entdecken.

Programm: Folge von Anweisungen für Aktionen, die ein Computer ausführen soll.

Programmvirus: Computervirus, der sich selbst an ein Computerprogramm hängt und gemeinsam mit dem Programm gestartet wird.

Proxyserver: Server, der Anfragen an das Internet über einen anderen Rechner leitet. Dieser Rechner befindet sich zwischen einem Unternehmen und dem Internet und wird zu Sicherheitszwecken verwendet.

Prüfsumme: Berechneter Wert von Datenobjekten, mit dem festgestellt werden kann, ob Daten verändert wurden.

RAM: Random Access Memory. Temporärer Speicher in einem Computer. Das RAM fungiert als Arbeitsbereich des Computers, jedoch gehen sämtliche dort gespeicherten Daten verloren, sobald der Computer ausgeschaltet wird.

ROM: Read Only Memory. Permanenter Speicher in einem Computer. In einem ROM wird die Software gespeichert, die der Computer beim Booten benötigt.

RTF: Rich Text Format. Format für Dokumente, das keine Makros unterstützt, so dass es keine Makroviren übertragen kann.

Sandbox: Mechanismus zum Ausführen von Programmen in einer kontrollierten Umgebung, speziell von Java-Applets.

SHS: Dateierweiterung für „scrap object" Dateien von Windows. SHS-Dateien können fast jede Art von Code enthalten, der gestartet wird, sobald man darauf klickt. Die Erweiterung kann auch verborgen sein.

SMTP: Simple Mail Transfer Protocol. Übertragungssystem für Internet-E-Mail.

Spam-Mail: E-Mails, die unaufgefordert verschickt werden.

Spoofing: Vortäuschen, eine andere Person zu sein (z. B. indem die Adresse des Senders in der E-Mail gefälscht wird).

TCP/IP: Transmission Control Protocol/Internet Protocol. Sammelbezeichnung für die Standard-Internet-Protokolle.

Trojanisches Pferd: Computerprogramm mit (unerwünschten) Nebeneffekten, die in der Beschreibung nicht erwähnt sind.

URL: Uniform Resource Locator. Eine Internetadresse.

Viren

E-Mail

Internet

Handy & PDA

Sicherheit


Mehr Info

VBS: Visual Basic Script. Code innerhalb einer Anwendung, eines Dokuments oder einer Website, der ausgeführt wird, sobald die entsprechende Seite angesehen wird.

Virenkennung: Beschreibung von Virencharakteristiken, die für die Erkennung von Viren verwendet werden.

Virenscanner: Programm zur Erkennung von Viren. Die meisten Scanner sind virenspezifisch, d. h., sie erkennen die Viren, die bereits bekannt sind. Siehe auch „Heuristischer Scanner“.

Virus: Programm, das sich auf Computern und Netzwerken verbreitet, indem es sich an andere Programme anhängt und Kopien von sich selbst erzeugt.

WAP: Wireless Application Protocol. Internetähnliches Protokoll, das Daten auf Mobiltelefone und Organizer überträgt.

Web: Siehe World Wide Web.

Webbrowser: Programm, mit dem auf Daten im Internet zugegriffen werden kann; die „Client-Seite“ des Internet.

Webserver: An das Internet angeschlossener Computer, der über HTTP Dokumente aus dem Internet zur Verfügung stellt.

World Wide Web: Verbreitetes Hypertextsystem zum Lesen von Dokumenten im gesamten Internet.

WSH: Windows Scripting Host. Dienstprogramm, mit dem auf Windows-Computern bestimmte Vorgänge automatisiert werden, z. B. das Ausführen von VBS oder JavaScript.

Wurm: Programm, das vielfache Kopien von sich verteilt. Im Gegensatz zu einem Virus benötigt ein Wurm kein „Wirt“-Programm.

WWW: Siehe World Wide Web.

Index

Virenindex

Edited and designed by Paul Oldfield.

ISBN 3-00-007954-8

Enquiries: enquiries@sophos.com
Website: www.sophos.com