Viren und Spam

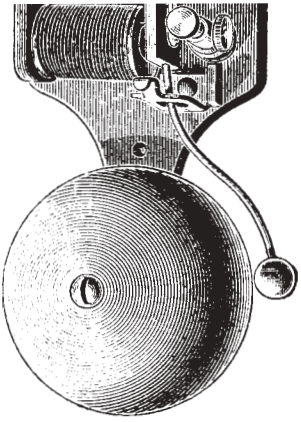
Was Sie schon immer wissen wollten

SOPHOS

Viren und Spam

Was Sie schon immer wissen wollten

Egal, ob Sie Netzwerkadministrator sind, im Büro am Computer arbeiten oder einfach nur E-Mails lesen – dieses Buch ist wie für Sie gemacht! Hier wird in verständlicher Sprache alles erklärt, was Sie über Computerviren und Spam wissen müssen.



Sophos ist einer der weltweit führenden Antiviren- und Antispam-Hersteller. Mehr als 25 Millionen Unternehmensanwender weltweit vertrauen auf den Schutz von Sophos. Nähere Informationen über die gesamte Sophos-Produktpalette für Spam- und Virenschutz und zur Durchsetzung von E-Mail-Richtlinien finden Sie auf unserer Website www.sophos.de.


Viren


Spam


Hoaxes


Sicherheit


Mehr Info

ISBN 0-9538336-4-X

Website: www.sophos.de

Inhalt

Viren, Würmer und Trojaner 5

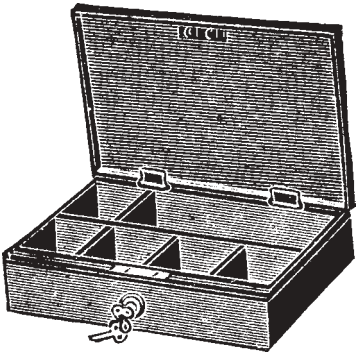
Spam 27

Hoaxes und Warnungen 41

Tipps für sichere Computerarbeit 49

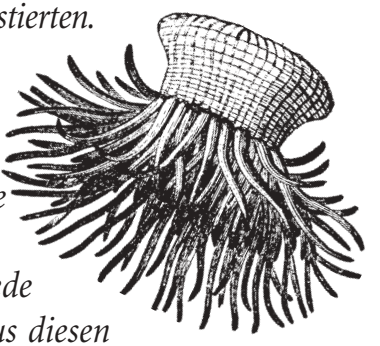
Glossar 53

Index 63



Viren, Würmer und Trojaner

Mitte der 80er Jahre stellten zwei Brüder in Pakistan fest, dass von ihrer Software zahlreiche Raubkopien existierten. Sie reagierten, indem sie den ersten Computervirus schrieben – ein Programm, das eine Kopie von sich selbst und einen Copyright-Vermerk auf jede kopierte Diskette legte. Aus diesen Anfängen heraus hat sich eine eigenständige Szene entwickelt. Neue Viren verbreiten sich heutzutage innerhalb weniger Minuten über den gesamten Erdball. Sie können Daten beschädigen, Netzwerkverkehr verlangsamen oder den Ruf von Unternehmen schädigen.

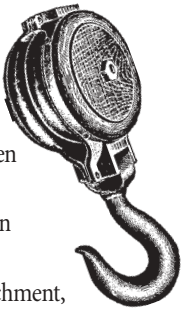


Was ist eigentlich ein Computervirus?

Ein Virus oder Wurm ist ein Computerprogramm, das sich auf Computer und in Netzwerken verbreitet, indem es sich selbst kopiert, ohne dass der Anwender darüber Bescheid weiß.

Viren können äußerst unangenehme Auswirkungen haben. So können sie irritierende Textmeldungen anzeigen, Daten stehlen oder anderen Anwendern die Steuerung Ihres Computers ermöglichen.

Wie infiziert ein Virus einen Computer?



Ein Virus kann Ihren Computer nur infizieren, wenn er gestartet wurde. Viren haben ihre Methoden, um dafür zu sorgen, dass dies geschieht. Sie können sich an andere Programme anhängen oder ihren Code so verstecken, dass er automatisch startet, wenn Sie bestimmte Dateitypen öffnen. Viren können auch Sicherheitslücken im Betriebssystem Ihres Computers ausnutzen, um automatisch zu starten und sich zu verbreiten.

Eine infizierte Datei können Sie als E-Mail-Attachment, per Internet-Download oder auf einer Diskette erhalten. Sobald die Datei aufgerufen wird, startet auch der Virencode. Der Virus kann sich dann in andere Dateien oder auf Datenträger kopieren und Änderungen auf Ihrem Computer vornehmen.

Trojanische Pferde

Trojanische Pferde sind Programme, die vorgeben, legitime Software zu sein. In Wahrheit jedoch verfügen sie über versteckte Schadensfunktionen.

DLoader-L wird beispielsweise als E-Mail-Attachment versendet und täuscht vor, ein dringendes Update von Microsoft für Windows XP zu sein. Wenn man es startet, lädt es ein Programm herunter, das sich über Ihren Computer mit bestimmten Websites verbindet, um sie zu überlasten (dies wird Denial-of-Service-Attacke genannt).

Trojaner können sich nicht so schnell wie Viren verbreiten, da sie keine Kopien von sich erstellen. Sie treten jedoch immer häufiger in Kombination mit Viren auf. Viren können Trojaner herunterladen, die gedrückte Tasten speichern oder Daten stehlen. Trojaner können aber auch dazu benutzt werden, einen Computer mit einem Virus zu infizieren.

Würmer

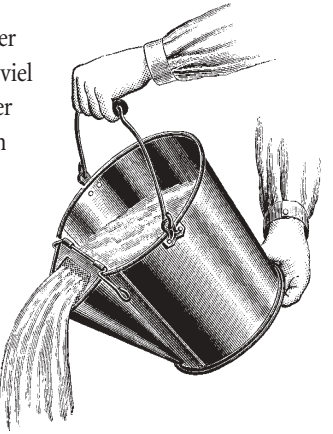
Würmer sind vergleichbar mit Viren, benötigen allerdings kein „Wirt"-Programm oder Dokument für ihre Verbreitung.

Würmer erstellen exakte Kopien von sich und nutzen die Kommunikationsflüsse zwischen Computern, um sich zu verbreiten (siehe auch Abschnitt „Internetwürmer").

Viele Viren, z. B. *MyDoom* oder *Bagle*, verhalten sich wie Würmer und leiten sich in E-Mails weiter.

Was können Viren anrichten?

Früher haben Viren Streiche gespielt oder den Computer lahm gelegt. Heute schaden sie der Sicherheit auf heimtückischere Weise:



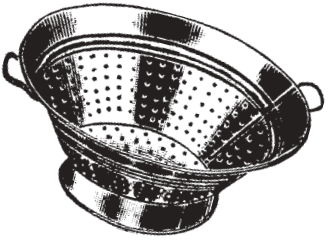
- **Verlangsamen der E-Mail.** Viren, die sich per E-Mail verbreiten, wie z. B. *Sobig*, können so viel E-Mail-Verkehr erzeugen, dass sich die Server verlangsamen oder gar abstürzen. Auch wenn dies nicht passiert, reagieren manche Unternehmen auf Gefahren, indem sie vorsorglich ihre Server herunterfahren.

- **Diebstahl vertraulicher Daten.** Der *Bugbear-D* Wurm speichert die von einem Anwender gedrückten Tasten, gelangt somit an Kennwörter und gibt dem Virenschreiber Zugriff zu den Daten.

- **Website-Attacken mit Hilfe Ihres Computers.** *MyDoom* hat mit Hilfe infizierter Computer die Website des Software-Unternehmens SCO mit Daten überflutet, so dass sie nicht genutzt werden konnte (eine Denial-of-Service-Attacke).

- **Missbrauch Ihres Computers durch Dritte.** Manche Viren legen auch „Backdoor-Trojaner" auf dem Computer ab, so dass sich ein Virenschreiber mit Ihrem Computer verbinden und ihn für seine eigenen Zwecke missbrauchen kann.

- **Datenänderung**. Der *Compatable* Virus ändert Daten in Excel-Tabellen.
- **Löschen von Daten**. Der *Sircam* Wurm kann versuchen, an einem bestimmten Tag die Festplatte zu löschen oder zu überschreiben.
- **Lahmlegen von Hardware**. *CIH* oder *Chernobyl* versucht jedes Jahr am 26. April, das BIOS zu überschreiben und den Computer somit funktionsunfähig zu machen.
- **Späße**. Mit dem *Netsky-D* Wurm infizierte Computer haben einen Morgen lang für mehrere Stunden in unregelmäßigen Abständen Pieptöne erzeugt.
- **Anzeigen von Textmeldungen**. Jeweils im Monat Mai zeigt *Cone-F* ein politisches Statement an.
- **Verlust der Glaubwürdigkeit**. Wenn ein Virus sich von Ihrem Computer an Ihre Kunden und Geschäftspartner weiterleitet, möchten diese möglicherweise die Geschäftsbeziehungen mit Ihnen beenden oder fordern sogar Schadenersatz.



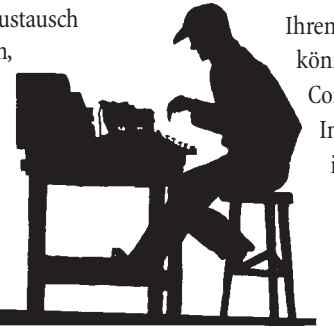
- **Peinlichkeiten**. *PolyPost* legt beispielsweise Ihre Dokumente und Ihren Namen bei Sex-Newsgroups ab.

Wo liegen die Risiken?

Auf diesen Wegen gelangen Viren auf Ihren Computer – nähere Informationen finden Sie auf den folgenden Seiten.

Programme und Dokumente

Programme und Dokumente können mit Viren infiziert sein. Die Infektion verbreitet sich beim Austausch mit anderen Anwendern, wenn Programme und Dokumente im Netzwerk oder im Intranet abgelegt oder wenn sie versendet werden.



E-Mail

E-Mails können infizierte Attachments enthalten. Wenn Sie auf ein infiziertes Attachment doppelklicken, riskieren Sie, dass Ihr Computer infiziert wird. Einige E-Mails enthalten sogar schädliche Skripts, die starten, sobald Sie die E-Mail über eine Vorschau ansehen oder nur den Text lesen.

Internet

Heruntergeladene Programme oder Dokumente können infiziert sein. Durch Sicherheitslücken in Ihrem Betriebssystem können Viren Ihren Computer über eine Internetverbindung infizieren, ohne dass Sie überhaupt etwas tun.

CDs und Disketten

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

Welche Dateien werden infiziert?

Viren können sich an jeden Code anhängen, der auf Ihrem Computer läuft: Programme, Dokumente oder Dateien, die das Betriebssystem starten.

Programme

Einige Viren infizieren Programme. Wenn Sie das infizierte Programm starten, wird zunächst der Virus gestartet. Diesen Virentyp gibt es schon seit den frühesten Anfängen der Virengeschichte. Doch auch heute noch stellt er eine Bedrohung dar, da Programme über das Internet schnell und einfach ausgetauscht werden können.

Dokumente

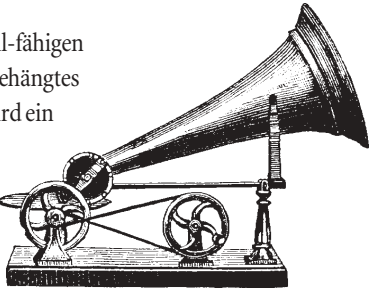
Textverarbeitungs- oder Tabellenkalkulations-Anwendungen benutzen häufig „Makros", um Tasks zu automatisieren. Manche Viren nehmen die Form eines Makros an, um sich von einem Dokument auf das nächste zu verbreiten. Wenn Sie ein Dokument öffnen, das einen Virus enthält, kopiert sich der Virus in die Startdateien der Anwendung und infiziert andere Dokumente, die Sie mit dieser Anwendung öffnen.

Bootsektoren

Wenn Sie Ihren Computer einschalten, greift er auf einen Teil der Festplatte zu, der „Bootsektor" genannt wird, und ruft ein Programm auf, welches das Betriebssystem startet. Schon die frühesten Viren haben diesen Bootsektor mit ihrer eigenen, veränderten Version ersetzt. Wenn der Anwender seinen Computer von einer infizierten Festplatte startet, wird der Virus aktiv.

E-Mail-Viren

Viele der häufigsten Viren sind E-Mail-fähig: Sie verbreiten sich automatisch per E-Mail.



Typischerweise muss bei E-Mail-fähigen Viren der Anwender auf ein angehängtes Dokument klicken. Dadurch wird ein Skript gestartet, das infizierte Dokumente an andere Anwender weiterleitet. Der *Netsky*-Virus durchsucht den Computer beispielsweise nach Dateien, die E-Mail-Adressen enthalten könnten (z. B. EML- oder HTML-Dateien). Mit Hilfe eines E-Mail-Programms auf Ihrem Computer sendet sich der Virus dann an diese Adressen. Einige Viren, wie z. B. *Sobig-F*, benötigen noch nicht einmal Ihren E-Mail-Browser. Sie besitzen ihre eigene „SMTP-Engine" zum Versenden von E-Mails.

E-Mail-Viren können die Sicherheit Ihres Computers beeinträchtigen oder Daten stehlen. Am häufigsten erzeugen sie jedoch eine Unmenge an E-Mail-Verkehr und verursachen Server-Abstürze.

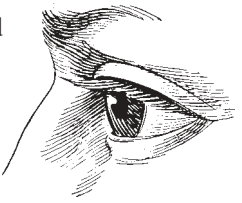
E-Mail-Anhänge

Jeder Anhang, den Sie per E-Mail erhalten, könnte einen Virus in sich tragen. Wird der Anhang aufgerufen, kann Ihr Computer infiziert werden.

Auch ein Attachment mit einem scheinbar sicheren Dateityp, z.B. eine Datei mit einer .txt-Erweiterung, kann gefährlich sein. Bei dieser Datei kann es sich nämlich um ein schädliches VBS-Skript handeln, bei dem der tatsächliche Dateityp (.vbs) versteckt ist.

Infektion schon beim Lesen von E-Mails?

Sie müssen nicht unbedingt ein Attachment öffnen, um sich per E-Mail zu infizieren. Nur das Ansehen einer E-Mail ist bereits ein Risiko.

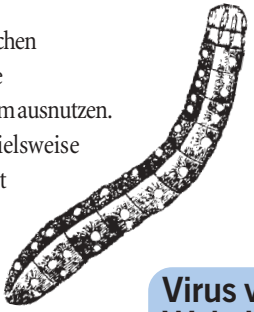


Einige Viren, z. B. *Kakworm* und *Bubbleboy,* infizieren Anwender, sobald diese die E-Mail lesen. Sie sehen aus wie jede andere E-Mail, enthalten aber ein verstecktes Skript, das startet, sobald Sie die E-Mail öffnen oder sie nur über eine Vorschaufunktion ansehen (bei Outlook mit der entsprechenden Version des Internet Explorers). Dieses Skript kann Systemeinstellungen ändern und den Virus per E-Mail an andere Anwender senden.

Microsoft stellt Patches zur Verfügung, mit denen solche Sicherheitslücken geschlossen werden. Um sich darüber zu informieren, welche Patches Sie benötigen, besuchen Sie windowsupdate.microsoft.com. Um sich über zukünftige Patches zu informieren, können Sie sich bei einer Mailingliste unter www.microsoft.com/technet/security/bulletin/notify.asp registrieren.

Internetwürmer

Ein Risiko für eine Virusinfektion besteht, sobald Sie sich mit dem Internet verbinden, auch wenn Sie keine verdächtigen E-Mails öffnen.



Internetwürmer bewegen sich zwischen verbundenen Computern, indem sie Sicherheitslücken im Betriebssystem ausnutzen.

Der *Blaster*-Wurm nutzt beispielsweise eine Schwachstelle in dem Dienst „Remote Procedure Call" auf Windows NT-, 2000- und XP-Computern aus und sendet eine Kopie von sich an einen anderen Computer. Wenn sich der Wurm verbreitet, erzeugt er ein hohes Maß an Internetverkehr, so dass er die Kommunikation verlangsamt oder Computer abstürzen. Dieser Wurm nutzt den Computer später, um eine Microsoft-Website mit Daten zu überfluten, damit auf sie nicht mehr zugegriffen werden kann.

Microsoft (und andere Betriebssystem-Hersteller) stellen Patches zur Verfügung, die Sicherheitslücken in ihrer Software schließen. Um Ihren Computer zu aktualisieren, sollten Sie regelmäßig die Website des Herstellers besuchen.

Virus von einer Website?

Webseiten werden in HTML (Hypertext Markup Language) geschrieben. HTML kann keinen Virus enthalten, allerdings kann es Programme oder Dateien aufrufen, die wiederum einen Virus enthalten. Durch das Surfen auf eine HTML-Seite können Sie nicht infiziert werden, es sei denn, Ihr Computer hat eine Sicherheitslücke, durch die ein Programm gestartet und Ihr Computer infiziert werden kann.

Backdoor-Trojaner

Ein Backdoor-Trojaner ist ein Programm, das einem Dritten über das Internet die Steuerung über den betroffenen Computer ermöglicht.

Ein Backdoor-Trojaner kann sich als legitime Software tarnen, wie andere Trojaner-Programme auch, so dass es der Anwender ahnungslos startet. Allerdings – und das kommt immer häufiger vor – kann auch ein Virus einen Backdoor-Trojaner auf dem Computer ablegen. Sobald der Trojaner gestartet wird, fügt er sich zur Autostart-Routine des Computers hinzu. Er kann dann den Computer überwachen, bis der Anwender mit dem Internet verbunden ist. Sobald der Computer online ist, kann der Sender des Trojaners auf dem infizierten Computer Programme starten, auf persönliche Dateien zugreifen, Dateien verändern und hochladen, die von dem Anwender gedrückten Tasten nachverfolgen oder Spam-Mails versenden. Zu den bekanntesten Backdoor-Trojanern gehören *Subseven*, *BackOrifice* und *Graybird,* der als Problembehebung des berüchtigten *Blaster*-Wurms getarnt war.

Spyware

Mit Spyware werden in der Werbebranche Daten über die Gewohnheiten von Computer-Nutzern gesammelt.

Spyware-Programme sind keine Viren (sie können sich nicht auf andere Computer verbreiten). Sie können aber unerwünschte Auswirkungen haben.

Spyware kann auf Ihren Computer gelangen, wenn Sie bestimmte Websites besuchen. In einem Pop-Up-Fenster wird Ihnen mitgeteilt, dass Sie eine erforderliche Software herunterladen oder sie wird einfach ohne Ihr Wissen heruntergeladen.

Die Spyware läuft dann auf dem Computer, protokolliert Ihre Aktivitäten (z. B. Besuche auf Websites) und meldet die Ergebnisse an Dritte, z. B. an Werbe-Unternehmen. Sie kann auch die Startseite ändern, die angezeigt wird, wenn Sie Ihren Internetbrowser starten. Über ein Einwahlmodem kann Spyware außerdem 0900-Nummern (Premiumrate) wählen.

Spyware benutzt auch Speicher- und Prozessor-Kapazität, kann den Computer verlangsamen und zum Absturz bringen.

Es gibt Software, die bekannte Spyware-Programme erkennt und entfernt.

Cookies

Wenn Sie eine Website besuchen, kann sie ein kleines Datenpaket, das „Cookie" genannt wird, auf Ihrem Computer ablegen. Die Website kann dadurch Ihre Daten speichern und registrieren, wie oft Sie die Website besuchen.

Cookies stellen keine Gefahr für Ihre Daten dar. Allerdings gefährden sie Ihre Privatsphäre. Wenn Sie lieber anonym bleiben möchten, können Sie Cookies über die Sicherheitseinstellungen Ihres Browsers deaktivieren.

Viren auf Mobiltelefonen?

Mobiltelefone können von Würmern infiziert werden, die sich über das Mobiltelefon-Netzwerk verbreiten. Zum jetzigen Zeitpunkt ist dieses Risiko jedoch sehr beschränkt.

2004 wurde der erste Mobiltelefon-Wurm geschrieben. Der *Cabir-A* Wurm, der das Symbian-Betriebssystem ausnutzt, wird als Telefonspieldatei (eine SIS-Datei) übertragen. Wenn Sie die Datei starten, erscheint eine Meldung auf dem Bildschirm und der Wurm startet dann jedes Mal, wenn Sie Ihr Telefon einschalten. *Cabir-A* sucht nach anderen Mobiltelefonen in der Nähe, die Bluetooth im Einsatz haben, und sendet sich an das erste entsprechende Telefon. Dieser Wurm zeigt, dass eine Infektion möglich ist, er wurde jedoch nicht in einem öffentlichen Netzwerk in Umlauf gebracht.

Es gibt auch konventionelle Viren, die Nachrichten an Mobiltelefone senden. *Timo-A* beispielsweise benutzt Computermodems, um Textnachrichten (SMS) an ausgewählte Mobiltelefon-Nummern zu senden. In solchen Fällen kann der Virus jedoch das Mobiltelefon nicht infizieren oder beschädigen.

Bis heute sind die Gefahren für Mobiltelefone sehr gering. Der Grund dafür liegt wahrscheinlich darin, dass sie viele verschiedene Betriebssysteme verwenden oder auch dass sich die Eigenschaften der Software und Geräte so schnell ändern.

Ist Bluetooth ein Risiko?

Die Bluetooth-Technologie für Mobiltelefone, Computer und andere Geräte kann Wege für Viren, Sicherheitsverstöße und Scherze öffnen.

Mit Bluetooth können Computer, Mobiltelefone und sogar Videorecorder oder Kühlschränke Geräte in der Nähe orten und eine transparente Verbindung mit ihnen aufnehmen.

Bluetooth wurde bereits von einem Mobiltelefon-Wurm ausgenutzt, der so Telefone in der Nähe ausfindig gemacht und sich dann über sie verbreitet hat.

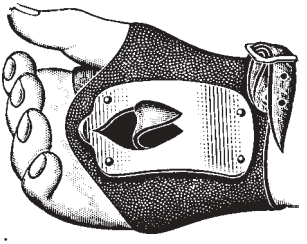
Andere Technologien, die auf Bluetooth basieren, z. B. Jini, ermöglichen auch die Fernsteuerung von Geräten. Bluetooth und Jini wurden so entwickelt, dass nur vertrauenswürdiger Code sensible Aktionen starten kann – solche Technologien eröffnen aber auch die Möglichkeit, dass schädlicher Code Dienste stört.

Mit Telefonen, auf denen Bluetooth aktiviert ist, können andere Telefone in der Nähe geortet werden und ihnen unerwartete – manchmal anstößige – Nachrichten gesendet werden.

Sie können sich vor allen Bluetooth-Bedrohungen schützen – egal, ob vor schädlichen Programmen oder vor unerwünschten Nachrichten –, indem Sie die Bluetooth-Einstellung „Sichtbar für andere“ an Ihrem Telefon ausschalten.

Viren auf Palmtops?

Palmtops oder PDAs bieten neue Möglichkeiten für Viren, allerdings haben Virenschreiber bisher wenig Interesse diesbezüglich gezeigt.



Palmtops oder PDAs laufen mit speziellen Betriebssystemen – wie Palm und Microsoft PocketPC. Diese sind zwar für schädlichen Code anfällig, aber bisher scheinen die Risiken gering zu sein.

Es wurden lediglich ein Virus und ein Trojanisches Pferd für Palm geschrieben, aber keines von beiden wurde in Umlauf gebracht.

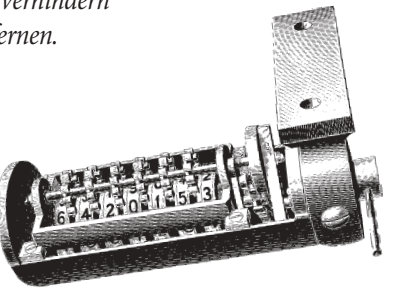
Virenschreiber zielen lieber auf Desktop-Systeme, da sie weiter verbreitet sind und sich Viren auf ihnen schneller per E-Mail und über das Internet verbreiten können.

Die wirkliche Gefahr zurzeit ist eher, dass Ihr Palmtop als Überträger fungiert. Wenn Sie sich mit Ihrem PC zu Hause oder im Büro für die Datensynchronisation verbinden, kann sich ein auf dem Palmtop harmloser Virus auf den PC übertragen und dort durchaus Schäden anrichten. Um diese Gefahr zu vermeiden, folgen Sie den „Tipps für sichere Computerarbeit“ und setzen Sie auf Ihrem Desktop-Computer Antiviren-Software ein.

Antiviren-Software

Antiviren-Software kann Viren erkennen, Zugriff auf infizierte Dateien verhindern und häufig eine Infektion entfernen.

Virenscanner



Virenscanner erkennen und desinfizieren Viren, die dem Scanner bekannt sind. Scanner sind die gängigste Form von Antiviren-Software, aber sie müssen regelmäßig aktualisiert werden, um neue Viren zu erkennen.

Es gibt On-Access- und On-Demand-Scanner. Viele Produkte bieten beides an.

On-Access-Scanner sind auf Ihrem Computer aktiv, solange Sie ihn benutzen. Sie überprüfen Dateien automatisch, wenn Sie versuchen, sie zu öffnen oder zu starten, und verhindern, dass infizierte Dateien benutzt werden.

Mit *On-Demand-Scannern* können Sie eine Überprüfung bestimmter Dateien oder Laufwerke starten oder einen Zeitplan für Überprüfungen festlegen.

Heuristik

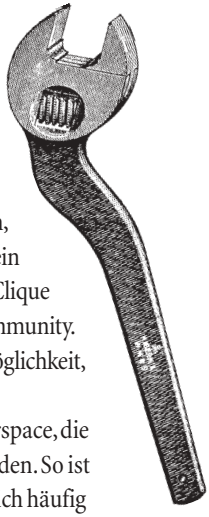
Heuristische Software versucht, Viren – sowohl bekannte als auch unbekannte – mit Hilfe allgemeiner Virenmuster zu erkennen.

Diese Software funktioniert ohne häufige Updates. Fehlarme sind jedoch bei heuristischer Software keine Seltenheit.

Wer schreibt Viren?

Wenn Ihr Computer oder Ihr Netzwerk von einem Virus befallen wurde, werden Sie sich sicher fragen, wer eigentlich die Schöpfer dieser Viren sind.

Virenschreiber möchten manchmal ein politisches Statement verbreiten. Oder sie möchten Unternehmen schaden, die sie missbilligen (viele Viren und Würmer haben beispielsweise Microsoft kritisiert oder zum Ziel gehabt). Sie können auch in die Computer anderer Anwender eindringen oder E-Mail-Adressen aufspüren und diese dann an Spammer verkaufen.



Virenschreiber sind häufig auch von der traurigen Berühmtheit motiviert, die sie durch ihre Schöpfungen erlangen können.

Der durchschnittliche Virenschreiber ist männlich, jünger als 25 Jahre und Single. Sein Selbstbewusstsein stützt sich sehr stark auf die Bestätigung durch die Clique oder zumindest durch eine kleine elektronische Community. Virenschreiben ist, wie Graffiti auch, eine Aktionsmöglichkeit, mit der der Schreiber an Status gewinnt.

Mit Viren erhalten ihre Schöpfer Macht im Cyberspace, die sie in der wirklichen Welt wohl niemals haben werden. So ist es auch nicht verwunderlich, dass Virenschreiber sich häufig Namen geben, die von Heavy-Metal-Musik oder Fantasy-Romanen inspiriert wurden, da diese auf ähnlichen Vorstellungen von Tapferkeit und Stärke basieren.

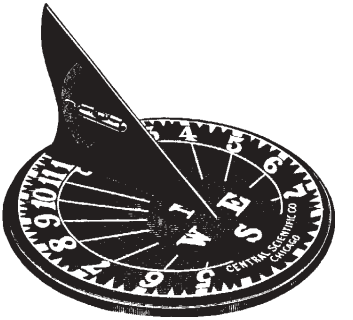
Geschichte der Computerviren

1950er 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 in einer Dissertation 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.

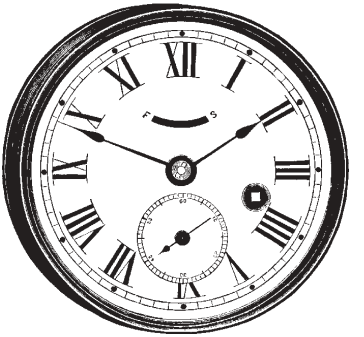
1988 Der *Internet worm* verbreitet sich im US-DARPA-Internet.

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

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

1995 Der erste Dokumentenvirus, *Concept*, erscheint.

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



1999 *Melissa*, ein Virus der sich selbst per E-Mail weiterleitet, verbreitet sich weltweit. *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.

2001 Ein Virus, der angeblich Bilder der Tennisspielerin Anna Kournikova enthält, infiziert Tausende Computer weltweit.

2002 David L Smith, Autor von *Melissa*, wird von US-Gerichten zu 20 Monaten Haft verurteilt.

2003 Der *Blaster*-Wurm verbreitet sich mit Hilfe einer Sicherheitslücke in der Software von Microsoft im Internet. Gemeinsam mit dem E-Mail-Virus *Sobig* macht er den August 2003 zum bisher schlimmsten Monat der Virenvorfälle.

2004 Die Schöpfer der *Netsky*- und *Bagle*-Würmer wetteifern, welcher Wurm wohl die größeren Auswirkungen hat.

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 den Anwender „veralbern" und sonst keinen weiteren Schaden anrichten. Wieder andere weisen auf Sicherheitslücken in Software hin. Manche Leute argumentieren sogar, dass Viren nützlich sein können, z. B. um Fehler in Programmen möglichst schnell zu beheben. Leider stimmt diese Vorstellung von „harmlosen" Viren nicht unbedingt mit der Realität überein.

Immerhin nehmen Viren Änderungen auf den Computern anderer Anwender ohne deren Zustimmung vor. Vom ethischen Standpunkt aus 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 es ihr Programmierer geplant hat. Ein schlecht programmierter Virus kann unvorhergesehene Probleme verursachen. Auch wenn ein Virus auf einem System harmlos ist, kann er auf anderen durchaus Schaden anrichten.

Und Viren verbreiten sich willkürlich: Ihr Schöpfer kann nicht kontrollieren, wer sie erhält.

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 programmiert und werden willkürlich auf Anwender übertragen. Es gibt keine Möglichkeit, die Ergebnisse zu sammeln und auszuwerten. Ob dies als Forschung zu bezeichnen ist, ist fragwürdig.

So haben Viren keine Chance

Mit einfachen Maßnahmen können Sie eine Infektion vermeiden oder Viren behandeln. Ausführliche Informationen finden Sie im Kapitel „Tipps für sichere Computerarbeit“.

Aufklärung über die Gefahren

Erklären Sie, dass es immer gefährlich ist, E-Mail-Attachments zu öffnen, Dateien aus dem Internet herunterzuladen oder Disketten auszutauschen.

Antiviren-Software und regelmäßige Updates

Antiviren-Programme können Viren erkennen und häufig entfernen. Sofern diese in der Software enthalten sind, nutzen Sie On-Access-Überprüfungen.

Software-Patches für Sicherheitslücken

Informieren Sie sich über „Patches“ für Ihr Betriebssystem. Patches schließen häufig Sicherheitslücken, die von Viren benutzt werden.

Firewalls

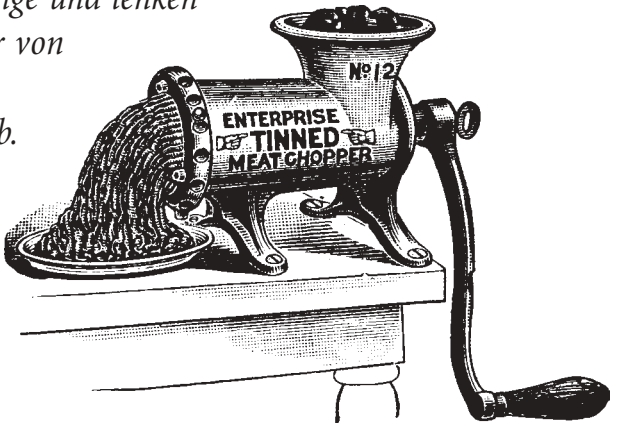
Eine Firewall kann unbefugte Zugriffe auf Ihr Netzwerk abblocken und verhindern, das Viren Daten versenden.

Sicherungskopien aller Daten

Erstellen Sie Sicherungskopien aller Daten und Software, auch der Betriebssysteme. Sollte ein Virus Ihren Computer infizieren, können Sie Ihre Dateien und Programme durch virenfreie Kopien ersetzen.

Spam

Höchstwahrscheinlich haben Sie schon E-Mails erhalten, in denen Ihnen Medikamente ohne Rezept, Darlehen oder Möglichkeiten, schnell zu Geld zu kommen, angeboten wurden – häufig geschickt als persönliche E-Mail getarnt. Mehr als die Hälfte aller weltweit versendeten E-Mails sind solche „Spam“-Mails. Sie verstopfen Posteingänge und lenken Anwender von wichtigen E-Mails ab.



Was ist eigentlich Spam?

Spam sind nicht angeforderte kommerzielle E-Mails, das elektronische Äquivalent zur Werbepost in Ihrem Briefkasten.

Die meisten Spam-Mails bieten Folgendes an:

- verschreibungspflichtige Medikamente, Medikamente zum Vergrößern oder Verschönern von Körperteilen, Kräutermittel oder Medikamente zur Gewichtsabnahme
- Möglichkeiten, schnell zu viel Geld zu gelangen
- Finanzdienstleistungen, z. B. Hypotheken oder Schuldenabbau
- Qualifikationen, z. B. Universitätsabschlüsse oder Berufsbezeichnungen gegen Bezahlung
- Online-Spiele
- reduzierte Software oder Raubkopien.

Spam kann sich tarnen, beispielsweise mit einer Betreffzeile, die wie eine persönliche E-Mail klingt, z. B. „Sorry about yesterday“, wie eine Geschäfts-E-Mail, z. B. „Your account renewal now due“ oder eine Nicht-Zustellbar-Nachricht.

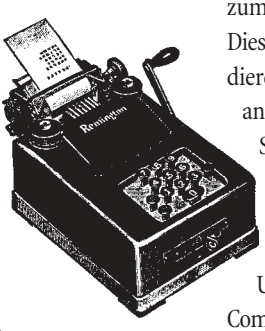
Warum Spam?

Spam wird versendet, weil es sich lohnt. Spammer senden Millionen E-Mails im Rahmen einer einzigen Kampagne zu geringen Kosten (und wenn sie die Computer Dritter zum Versenden von E-Mails missbrauchen, sinken die Kosten noch mehr). Wenn auch nur ein Empfänger von Tausend eine Bestellung aufgibt, verzeichnet der Spammer einen Gewinn.

Ist Spam wirklich ein Problem?

Spam-Mails sind zwar keine Bedrohung für Ihre Daten wie Viren, allerdings schädigen sie auch Unternehmen.

- Spam vergeudet die Zeit der Mitarbeiter. Nutzer ohne Spamschutz müssen prüfen, welche E-Mails Spam sind und diese dann löschen.
- Nutzer können schnell wichtige E-Mails übersehen oder sogar löschen, weil sie sie mit Spam verwechseln.
- Spam, wie Hoaxes und E-Mail-Viren auch, verschwendet Bandbreite und verstopft Datenbanken.
- Manche Spam-Mails sind anstößig. Arbeitgeber können zur Verantwortung gezogen werden, da sie für eine sichere Arbeitsumgebung Sorge tragen.
- Spammer nutzen häufig die Computer Dritter, um Spam zu versenden („Hijacking“).



Hijacking

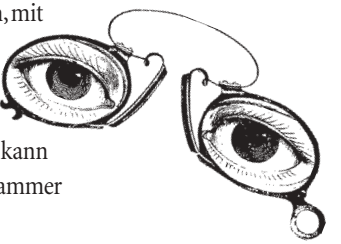
Spammer missbrauchen oft die Computer anderer Anwender zum Weiterleiten von Spam. Diese Hijacking-Opfer bombardieren dann unwissentlich andere Anwender mit Spam. Spammer achten darauf, dass ihre Spuren nicht zurückverfolgt werden können. Das heißt, das Unternehmen, dessen Computer missbraucht wurden, erhält die Beschwerden und erleidet unter Umständen eine Rufschädigung.

Spammer merken, wenn Sie lesen

Für zukünftige Kampagnen möchten Spammer wissen, wer ihre E-Mails liest und wer nicht.

Auch wenn Sie auf Spam nicht antworten, kann ein Spammer herausfinden, dass Sie die Spam-Mail empfangen haben.

- Wenn Ihr E-Mail-Programm so eingestellt ist, dass E-Mails in einer Vorschau angezeigt werden (z. B. in einem Fenster unterhalb der Liste mit allen E-Mails), kann der Spammer feststellen, ob eine E-Mail empfangen wurde.
- Wenn Sie auf einen Link klicken, mit dem Sie sich von einer Mailing-Liste abmelden, bestätigen Sie damit, dass Ihre E-Mail-Adresse aktiv ist. Der Spammer kann Ihre Adresse dann an andere Spammer verkaufen.



- Spammer können in ihren E-Mails einen „web bug" einfügen. Dies ist ein Link, der sich mit der Spammer-Website verbindet, sobald die E-Mail gelesen oder in einer Vorschau angesehen wird.

Wenn Spammer nicht erfahren sollen, dass Sie ihre E-Mail empfangen haben, folgen Sie den Hinweisen im Abschnitt „Vermeidung von Spam".

Antispam-Software

Antispam-Programme können unerwünschte E-Mails erkennen und verhindern, dass sie in den Posteingang der Nutzer gelangen.

Diese Programme verwenden eine Kombination mehrerer Methoden, um festzustellen, ob es sich bei einer E-Mail um Spam handelt. Diese Programme können:

- E-Mails abblocken, die von Adressen aus einer Blacklist stammen. Dies kann eine kommerziell verfügbare Liste oder eine „lokale" Liste mit Adressen sein, von denen Ihr Unternehmen zuvor schon Spam erhalten hat.
- Prüfen, ob E-Mails von einer tatsächlichen Domäne oder Internet-Adresse stammen. Spammer verwenden oft gefälschte Adressen, um Antispam-Programme zu umgehen.
- Nach Stichwörtern oder typischen Wendungen in Spam suchen (z. B. „Kreditkarte", „Gewichtsabnahme").
- Nach Mustern suchen, mit denen ein Sender den Text zu verbergen versucht (z. B. bei „hardc*re p0rn").
- Nach unnötigem HTML-Code (Code zum Schreiben von Webseiten) in E-Mails suchen, da Spammer damit ihre E-Mails tarnen und Antispam-Programme verwirren möchten.

Das Programm kombiniert alle gefundenen Informationen und berechnet eine Wahrscheinlichkeit dafür, dass die E-Mail Spam ist. Ist die Wahrscheinlichkeit hoch genug, kann die E-Mail abgeblockt oder gelöscht werden, je nach den von Ihnen gewählten Einstellungen.

Software, die lernt, welche E-Mails Sie wirklich möchten

Einige Antispam-Software ist „adaptiv“: Sie lernt, welche E-Mails Sie akzeptabel finden und welche nicht.

Angenommen, ein Pharma-Unternehmen installiert eine Antispam-Software. Zunächst versucht die Software, Spam ausfindig zu machen, indem sie nach Wörtern sucht, etwa nach: Kredit, kostenlos, Schulden, Hypothek, Medikamente, Rezept, Arzneimittel, Arzt. Die Software blockt E-Mails mit zu vielen dieser Stichwörter ab, gibt allerdings einzelnen Nutzern die Möglichkeit, die E-Mails zu erhalten, die sie lesen möchten.

Einige Mitarbeiter in der Forschungsabteilung stellen fest, dass echte E-Mails über neue Medikamente abgeblockt wurden, und bitten um Freigabe dieser E-Mails. Die Software lernt, dass der Nutzer häufig E-Mails über Medikamente erhält – und gibt Stichwörtern in Bezug auf Medikamente weniger Gewichtung, wenn nach Spam gesucht wird.

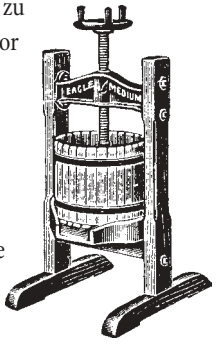
In der Finanzabteilung fordern Nutzer E-Mails mit Finanzbegriffen an. Die Software lernt so, dass diese Wörter eine geringere Gewichtung haben sollten – blockt aber für diesen Nutzer trotzdem E-Mails über Medikamente ab.

Blocken Antispam-Programme keine echten E-Mails?

Viele Nutzer befürchten, dass Antispam-Software wichtige E-Mails löscht. Ihre E-Mails sind sicher und Sie können sich auch ausgewählte Spam-Mails ansehen.

Antispam-Programme sind sehr genau. Typischerweise wird in zehntausend oder hunderttausend E-Mails eine echte E-Mail abgeblockt.

Auch wenn das Programm fälschlicherweise eine E-Mail als Spam identifiziert, kann es so konfiguriert werden, dass diese E-Mail in einem „Quarantäne"-Bereich abgelegt wird, anstatt sie zu löschen. Ein Administrator kann entscheiden, ob die E-Mail zugestellt oder gelöscht wird. Einige Programme geben jedem Nutzer die Möglichkeit, E-Mails aus der Quarantäne anzufordern.



Ich will aber Spam!

Was für den einen Spam ist, ist für den anderen interessant.

Jemand, der für ein Finanzunternehmen arbeitet, möchte sich vielleicht über die Zinsraten anderer Unternehmen informieren. Oder eine Software-Firma möchte wissen, ob Spammer Raubkopien verkaufen. Einige Antispam-Software lässt sich so anpassen, dass Spam-Mails, die für den Nutzer interessant sind, akzeptiert werden.

Die Tricks der Spammer

Spammer sind ständig auf der Suche nach Methoden, ihre E-Mails zu tarnen und Antispam-Software zu umgehen. Hier finden Sie einige der häufigsten Tricks:

Lost in Space

Der Spammer fügt Leerzeichen zwischen die Buchstaben von Wörtern ein, die er verbergen möchte, z. B. „M e d i k a m e n t e“. Der Spammer hofft, dass die Buchstaben nicht als ein Wort gelesen werden. Dieser Trick ist leicht zu erkennen.

Schwarzes Loch

Mit Hilfe von HTML-Code (Code zum Schreiben von Webseiten) fügt der Spammer ein Leerzeichen zwischen Buchstaben ein und stellt die Größe des Leerzeichens auf Null.

Das sehen Antispam-Programme:

```
V<font  size=0> </
font>i<font  size=0>
 </font>a<font  size=0> :</
font>g
<font  size=0> </font>r<font  size=0>
 </font>a
```

Das sehen Sie:

```
Viagra
```

Die Tricks der Spammer

Geheimtinte

Manchmal möchten Spammer, dass das Antispam-Programm eine harmlosere Nachricht liest als der Leser. Sie verwenden HTML-Code, um eine harmlos scheinende Nachricht einzufügen, und zwar in derselben Farbe wie der Hintergrund.

Das sehen Antispam-Programme:

```
<body bgcolor=white> Viagra
<font color=white>Hi, Johnny! It was
really nice to have dinner with you.
See you soon, love Mom</font></body>
```

Das sehen Sie:

```
Viagra
```

Mikrozeichen

Der Spammer fügt einen zusätzlichen Buchstaben in die Mitte des Wortes ein, das er tarnen möchte, und verwendet dabei eine sehr kleine Schriftgröße. Das Antispam-Programm sieht den Buchstaben und liest das Wort falsch, aber der Empfänger der E-Mail liest das Wort korrekt.

Zurück zum Sender

Der Spammer sendet seine E-Mail absichtlich an eine ungültige Adresse, allerdings schreibt er Ihre Adresse in das Sender-Feld. Die E-Mail kann nicht zugestellt werden, deshalb sendet sie der Server des Service Providers zurück ... und zwar an Sie.

Die Tricks der Spammer

Zahlenspiel

Ein Spammer kann ein Wort schreiben, indem er für jeden Buchstaben den speziellen HTML-Code verwendet anstelle von normalen Buchstaben. Der Buchstabe „a“ kann geschrieben werden, indem &#97 eingegeben wird.

Das sehen Antispam-Programme:

```
&#86;<font  size=0> </
font>&#105;<font
size=0> </
font>&#97;<font  size=0> 
</font>&#103;<font  size=0> </font>
&#114;<font  size=0> </font>&#97
```

Das sehen Sie:

```
Viagra
```

Scheibchenweise Zerlegung

Spammer zerlegen Text mit Hilfe von HTML-Dateien in Spalten.

Das sehen Antispam-Programme:

V	i	a	g	r	a			
P	r	o	b	e	n	l	o	s
K	o	s	t	e	n			

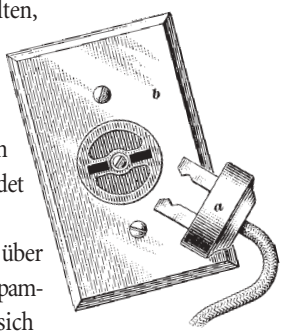
Das sehen Sie:

```
Viagra
Proben
kostenlos
```

Spam und Viren kombiniert

Spammer und Virenschreiber können sich auch zusammentun, um E-Mail-Nutzern noch viel mehr Probleme zu bereiten.

Viren können Spam neue Möglichkeiten eröffnen. Ein Virenautor kann einen Virus schreiben, der anderen Nutzern die Möglichkeit gibt, die Steuerung über den Computer zu erhalten, ohne dass der legitime Benutzer darüber Bescheid weiß. Wenn der Virus den Computer infiziert hat, sendet er eine Nachricht an den Virenschreiber, der die Liste aller infizierten Computer an einen Spammer verkaufen kann. Der Spammer versendet dann über diese Computer Spam-Mails.



Mehr als 30% aller Spam-Mails werden derzeit über missbrauchte Computer versendet. Indem sie ihre Spam-Mails auf diese Weise versenden, distanzieren sich Spammer von ihren Aktivitäten und erschweren die Rückverfolgung.

Spammer können sich revanchieren, indem sie bei der Verbreitung von E-Mail-Viren helfen. Ein Virenschreiber kann einen Virus starten, indem er ihn per E-Mail an eine große Anzahl Nutzer versendet. Dabei verwendet er die Adressliste eines Spammers. Bei so vielen Empfängern aktivieren sicher viele Anwender den Virus, so dass dieser sich weiterleiten und schnell verbreiten kann.

Es gibt einige Hinweise darauf, dass es Geheimabsprachen zwischen Spammern und Virenschreibern gibt. Der *Mimail-L*-Virus beispielsweise hat versucht, eine Denial-of-Service-Attacke gegen verschiedene Antispam-Websites zu starten.

Vermeidung von Spam

Antispam-Software

Antispam-Software kann die Zahl unerwünschter E-Mails senken, besonders, wenn sie über Ihr „Feedback" lernt, was Spam sind.

Nie über unerwünschte E-Mails bestellen

Mit Ihrer Bestellung sorgen Sie für noch mehr Spam. Ihre E-Mail-Adresse kann zu Listen hinzugefügt werden, die an andere Spammer verkauft werden, so dass Sie noch mehr unnütze E-Mails erhalten. Im schlimmeren Fall können Sie Betrügern zum Opfer fallen.

Bei unbekanntem Sender E-Mail löschen

Die meisten Spam-Mails sind einfach nur lästig, aber sie können manchmal auch Viren enthalten, die den Computer schädigen, sobald die E-Mail geöffnet wird.

Nie antworten und auf keine Spam-Links klicken

Wenn Sie auf Spam antworten – auch wenn Sie sich nur von einer Mailing-Liste abmelden – bestätigen Sie, dass Ihre E-Mail-Adresse gültig ist, und sorgen damit nur für noch mehr Spam.

Keine weiteren Informationen oder Angebote

Wählen Sie beim Ausfüllen von Formularen im Internet nie die Option, weitere Informationen oder Angebote zu erhalten.

Vermeidung von Spam

Kein „Vorschau“-Modus

Viele Spammer können nachverfolgen, wenn eine E-Mail angesehen wird, ohne dass Sie auf die E-Mail geklickt haben. Die Vorschau öffnet die E-Mail und Spammer wissen dann, dass Sie ihre E-Mails erhalten haben. Versuchen Sie allein über die Betreffzeile zu entscheiden, ob es sich bei E-Mails um Spam handelt oder nicht.

Bei E-Mails an mehrere Personen „bcc“-Feld verwenden

Im „bcc“- oder „Blind Copy“-Feld ist die Empfängerliste für andere Anwender unsichtbar. Wenn Sie alle Adressen in das „An“-Feld einfügen, können Spammer diese Adressen aufspüren und sie zu einer Mailingliste hinzufügen.

E-Mail-Adresse niemals im Internet angeben

Erwähnen Sie Ihre E-Mail-Adresse nie im Internet, in Newsgroups oder anderen öffentlichen Foren im Internet. Spammer können mit Programmen an solchen Stellen im Internet nach Adressen suchen.

E-Mail-Adresse nur an vertrauenswürdige Personen

Geben Sie Ihre E-Mail-Adresse nur Freunden und Bekannten.

„Sekundäre“ E-Mail-Adressen nutzen

Wenn Sie Formulare im Internet ausfüllen, von denen Sie keine weiteren Informationen wünschen, nutzen Sie eine sekundäre E-Mail-Adresse. Sie schützen somit Ihre Hauptadresse vor Spam.

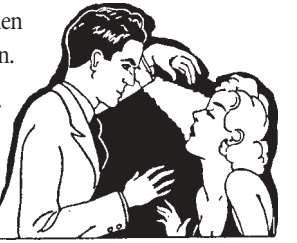
Hoaxes und Warnungen

Wenn Sie schon einmal eine E-Mail erhalten haben, in der Sie vor einem unwahrscheinlichen neuen Virus gewarnt wurden, in der Ihnen ein kostenloses Mobiltelefon angeboten wurde oder in der Sie aufgefordert wurden, Ihre Bankkontodaten mitzuteilen, dann sind Sie einem Hoax zum Opfer gefallen. Hoax-E-Mails können die Arbeit unterbrechen, Mailsysteme überlasten oder Sie auch dazu bringen, persönliche Zugangsdaten und Kennwörter an Kriminelle weiterzugeben.

Viren-Hoaxes

Viren-Hoaxes sind Meldungen über nicht existierende Viren. Diese E-Mails haben gewöhnlich folgende Merkmale:

- Sie warnen vor einem extrem zerstörerischen neuen Virus, der nicht erkannt werden kann.
- Sie fordern dazu auf, keine E-Mails mit einer bestimmten Betreffzeile zu lesen, z. B. „Join the Crew" oder „Budweiser Frogs".
- Sie behaupten, dass die Warnung von einer großen Software-Firma, einem Internet Provider oder einer Behörde, wie z. B. IBM, Microsoft, AOL oder FCC, herausgegeben wurde.
- Sie behaupten, dass ein neuer Virus Schäden verursacht, die relativ unwahrscheinlich sind, z. B. behauptet der Hoax *A moment of silence*, dass „neue Computer infiziert werden, auch wenn keine Programme ausgetauscht werden".
- Sie verwenden eine hochtechnische Sprache. So behauptet *Good Times*, dass der Virus den PC-Prozessor „in einen unendlichen Binärring mit endlicher Komplexität" bringt.
- Sie fordern dazu auf, die Warnung an andere Anwender weiterzuleiten.



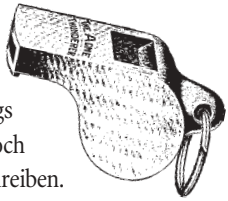
Der Hoax, der keiner war

Am 1. April 2000 kam eine E-Mail namens *Rush-Killer virus alert* in Umlauf. Diese E-Mail warnte vor Viren, die die Nummer 911 (Notruf 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 ist schwierig, einen Hoax von einer wirklichen Warnung zu unterscheiden. Folgen Sie den Hinweisen im Abschnitt „Vermeidung von Hoaxes".

Sind Hoaxes 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 an E-Mails. E-Mail-Server werden überlastet und stürzen im schlimmsten Fall ab. Dies hat dann denselben Effekt, den auch der echte *Sobig*-Virus hervorgerufen hat, allerdings muss der Verfasser eines Hoax dazu noch nicht einmal einen Computer-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 sind.

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 einigen Antiviren-Herstellern *GT-Spoof* genannt).

Page-Jacking

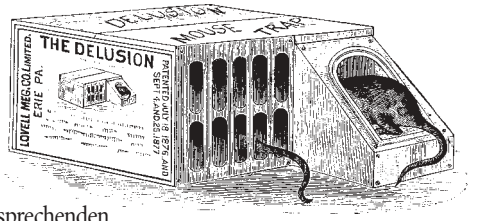
Page-Jacking bezeichnet Repliken namhafter Websites, mit denen Anwender auf andere Websites umgeleitet werden sollen.

Page-Jacker kopieren Seiten einer renommierten Website und stellen sie auf eine neue Website, die legitim erscheint. Sie registrieren dann diese neue Website bei gängigen Suchmaschinen, so dass Nutzer, die eine Suche starten, diese Website finden und auf den entsprechenden Link klicken. Wenn die Nutzer dann auf die Website gelangen, werden sie automatisch auf eine andere Website umgeleitet, die Werbung anzeigt oder andere Dienstleistungen anbietet.

Page-Jacking ist lästig und kann Nutzer mit anstößigem Material konfrontieren. Außerdem wird so der Erfolg legitimer Websites reduziert, und Suchmaschinen sind weniger nützlich.

In einigen Fällen kann Page-Jacking auch für „Phishing"-Attacken benutzt werden (siehe nächste Seite).

Sie können auf Page-Jacking nicht hereinfallen, wenn Sie ein Lesezeichen oder einen Favoriten verwenden bzw. die Internetadresse (URL) direkt eintippen.



Mouse-Trapping

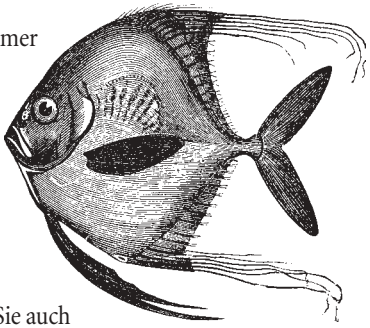
Wenn Sie auf eine gefälschte Website umgeleitet werden, lässt sie sich möglicherweise nicht über die Zurück- oder Schließen-Schaltfläche schließen. Das nennt man „Mouse-Trapping" (Mausefalle). Zum Verlassen der Seite geben Sie eine URL im Adressfeld ein, verwenden Sie ein Lesezeichen oder Sie wählen in der Liste der zuletzt besuchten URLs die Vorletzte. Um die Zurück- oder Schließen-Schaltfläche wieder zu benutzen, schließen Sie den Browser oder starten den Computer neu.

Phishing

Beim „Phishing“ werden Anwender mit gefälschten E-Mails und Websites dazu gebracht, vertrauliche und persönliche Daten zu senden.

Typischerweise erhalten Sie eine E-Mail, die scheinbar von einem renommierten Unternehmen stammt, wie z. B. einer Bank. In der E-Mail ist ein Link enthalten, der scheinbar auf die Website des Unternehmens führt. Wenn Sie dem Link jedoch folgen, werden Sie mit der Replik der Website verbunden. Alle Daten, die Sie dann eingeben, wie z. B. Kontonummern, PINs oder Kennwörter, können von den Hackern, die die gefälschte Website erstellt haben, gestohlen und benutzt werden.

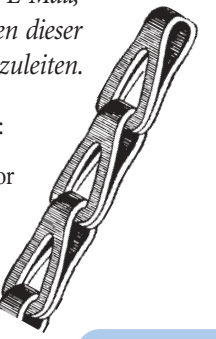
Sie sollten bei Links in E-Mails immer misstrauisch sein. Geben Sie stattdessen die Adresse der Website im Adressfeld ein oder verwenden Sie ein Lesezeichen oder einen Favoriten, um sicherzugehen, dass Sie auf die echte Website gelangen.



Mit Antispam-Software können Sie auch Phishing-E-Mails abblocken.

Kettenbriefe

Ein elektronischer Kettenbrief ist eine E-Mail, in der Sie aufgefordert werden, Kopien dieser E-Mail an andere Anwender weiterzuleiten.



Die wichtigsten Kettenbrief-Typen sind:

- **Hoaxes**. Kettenbriefe haben schon vor Terrorangriffen, Betrügereien mit Premiumraten-Telefonnummern und Diebstählen aus Geldautomaten gewarnt. Alle diese Kettenbriefe waren absichtliche Hoaxes oder moderne Sagen.
- **Falsche Gratis-Angebote**. Einige Kettenbriefe behaupten, dass Unternehmen Gratis-Flüge, kostenlose Mobiltelefone oder Bargeld anbieten, wenn diese E-Mail weitergeleitet wird.
- **Politische Proteste**. Dabei handelt es sich meist um Proteste gegen geplante Gesetze. Auch wenn sie echt sind, bleiben sie noch lange im Umlauf, wenn sie schon gar nicht mehr aktuell sind.
- **Scherze und Streiche**. Die E-Mail „Internet cleaning" behauptete, dass das Internet aufgrund von Wartungsarbeiten am 1. April geschlossen wird.

Sind Kettenbriefe ein Problem?

Kettenbriefe beeinträchtigen zwar nicht Ihre Sicherheit, aber sie können:

- Zeit verschwenden und Nutzer von wichtigen E-Mails ablenken.
- unnötigen E-Mail-Verkehr erzeugen und Mailserver verlangsamen.
- falsche Informationen verbreiten.
- Anwender ermutigen, E-Mails an bestimmte Adressen zu senden, so dass diese mit unerwünschten E-Mails überschwemmt werden.

Vermeidung von Hoaxes

Unternehmensrichtlinie für Virenwarnungen

Erstellen Sie eine Unternehmensrichtlinie bezüglich Virenwarnungen, z.B.: „Leiten Sie jegliche Virenwarnungen an niemanden weiter außer an den *Antiviren-Verantwortlichen*. Es ist völlig egal, ob die Virenwarnungen von einem Antiviren-Hersteller oder Ihrem besten Freund kommen oder ob sie von einem großen Computerunternehmen bestätigt wurden. ALLE Virenwarnungen sollten nur an *Name des Verantwortlichen* gesendet werden. Es ist seine Aufgabe, Virenwarnungen zu versenden. Virenwarnungen aus anderen Quellen werden ignoriert."

Informieren Sie sich über Hoaxes

Informieren Sie sich auf unserer Hoaxes-Webseite über die neuesten Hoaxes: www.sophos.de/virusinfo/hoaxes.

Leiten Sie keine Kettenbriefe weiter

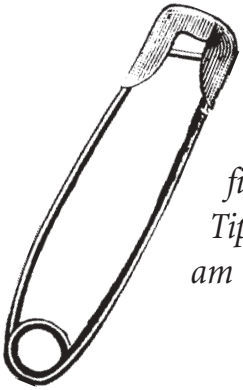
Leiten Sie keine Kettenbriefe weiter, auch wenn Ihnen Belohnungen dafür versprochen werden oder so angeblich nützliche Infos verbreitet werden.

Unangeforderte E-Mails: Vorsicht bei Links

Wenn Sie die Website Ihrer Bank oder eine andere Website besuchen möchten, bei der Sie Kennwörter oder vertrauliche Daten eingeben, klicken Sie nie auf Links in nicht angeforderten E-Mails oder in Newsgroups. Tippen Sie die Adresse selbst ein oder verwenden Sie als Link ein Lesezeichen oder einen Favoriten.

Tipps für sichere Computerarbeit

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



Tipps für sichere Computerarbeit

Vorsicht bei unangeforderten Dateien

Wenn Sie nicht sicher sind, dass etwas virenfrei ist, gehen Sie lieber davon aus, es ist nicht virenfrei. Erklären Sie Ihren Kollegen, warum sie auf keinen Fall nicht freigegebene Programme und Dokumente, auch Bildschirmschoner und Spaßprogramme, aus dem Internet herunterladen sollen. Hilfreich kann eine Richtlinie sein, nach der alle Programme von einem IT-Manager freigegeben und auf Viren überprüft werden müssen, bevor sie benutzt werden.

Keine Dokumente im .doc- und .xls-Format

Speichern Sie Ihre Word-Dokumente als RTF- und Ihre Excel-Tabellen als CSV-Dateien. Diese Formate unterstützen keine Makros, d. h., sie können auch keine Dokumentenviren übertragen. Bitten Sie andere, Ihnen nur RTF- und CSV-Dateien zu senden. Seien Sie aber dennoch vorsichtig! Manche Dokumentenviren tarnen ihr Format. Wenn Sie sicher sein möchten, verwenden Sie reine Textdateien.

Software-Patches für Sicherheitslücken

Informieren Sie sich über Sicherheits-News und laden Sie Patches herunter. Diese schließen oft Sicherheitslücken, die Ihren Computer für Viren oder Internetwürmer anfällig machen. IT-Manager sollten die Mailing-Listen von Software-Herstellern abonnieren, wie z. B. die unter www.microsoft.com/technet/security/bulletin/notify.asp. Heimanwender mit Windows-PCs können windowsupdate.microsoft.com besuchen und dort ihren PC auf Sicherheitslücken prüfen und Patches installieren lassen.

Tipps für sichere Computerarbeit

Dateien mit doppelter Erweiterung am Gateway blocken

Einige Viren verschleiern die Tatsache, dass sie Programme sind, indem sie nach ihrem Dateinamen eine doppelte Erweiterung benutzen, z. B. .TXT.VBS. Auf den ersten Blick sieht eine Datei namens LOVE-LETTER-FOR-YOU.TXT.VBS wie eine harmlose Textdatei oder Grafik aus. Sie sollten alle Dateien mit doppelter Erweiterung am E-Mail-Gateway abblocken.

Unerwünschte Dateitypen am Gateway stoppen

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

E-Mail-Benachrichtigungsservice

Ein Benachrichtigungsservice kann Sie vor den neuesten Viren warnen und Virenkennungen zur Verfügung stellen, mit denen Ihre Antiviren-Software neue Viren erkennt. Sophos bietet einen kostenlosen Benachrichtigungsservice an. Nähere Informationen finden Sie auf www.sophos.de/virusinfo/notifications.

Separates Netzwerk für Internetcomputer

Richten Sie separate Netzwerke für die Computer ein, die mit dem Internet verbunden sind, und für Computer, die keinen Internetzugang haben. Dadurch reduzieren Sie das Risiko, dass Anwender infizierte Dateien herunterladen und sich Viren in Ihrem Hauptnetzwerk verbreiten.

Tipps für sichere Computerarbeit

Einsatz von Firewalls und/oder Routern

Eine Firewall lässt nur freigegebenen Netzwerkverkehr in Ihr Unternehmen. Ein Router steuert die Datenpakete aus dem Internet.

Sicherheit im Internetbrowser

Deaktivieren Sie Java- oder ActiveX-Applets, Cookies usw. oder stellen Sie ein, dass Sie gewarnt werden, bevor solcher Code gestartet wird. Gehen Sie beispielsweise im Microsoft Internet Explorer auf **Extras|Internetoptionen|Sicherheit|Stufe anpassen** und wählen Sie die gewünschten Sicherheitseinstellungen.

Regelmäßige Backups

Wenn Sie mit einem Virus infiziert sind, können Sie verlorene Programme und Daten durch Backups wiederherstellen.

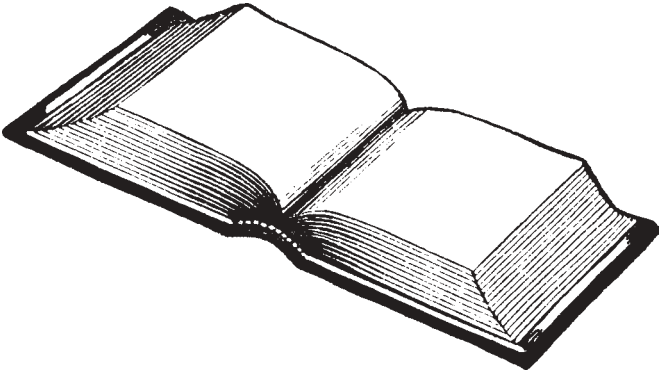
Bootsequenz ändern

Die meisten Computer versuchen zunächst, von Diskette (Laufwerk A:) zu booten. Die IT-Abteilung in Ihrem Unternehmen sollte die Einstellungen so ändern, dass der Computer zuerst von Festplatte gebootet wird. Wenn dann eine infizierte Diskette versehentlich im Computer gelassen wird, kann der Rechner nicht mit einem Bootsektorvirus infiziert werden.

Schreibgeschützte Disketten

Eine schreibgeschützte Diskette kann nicht infiziert werden.

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 angehängt werden.

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

Backdoortrojaner: Trojanisches Pferd (siehe Trojanisches Pferd), das einem remoten Benutzer unbefugten Zugriff auf und die Steuerung über einen Computer ermöglicht.

Backup: Kopie von Computerdaten zur Wiederherstellung von verloren gegangenen, verlegten, beschädigten oder gelöschten Daten.

Bayes-Filter: Statistische Methode zur Bestimmung, ob es sich bei einer E-Mail um Spam handelt oder nicht (basierend auf der Wahrscheinlichkeits-Theorie des Mathematikers Thomas Bayes).

Begleitvirus: Virus, der ausnutzt, dass das Betriebssystem bei zwei Programmen mit gleichem Namen über die Dateierweiterung 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, die direkt mit der Hardware verbunden ist.

Blackhole-Liste: Öffentliche und im Allgemeinen kommerzielle Liste mit IP-Adressen, von denen bekannt ist, dass von ihnen aus Spam verschickt wird. Siehe auch Real-Time-Blackhole-Liste.

Blacklist: Liste mit E-Mail-Adressen und Domänen, von denen keine E-Mails akzeptiert werden.

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 benutzt, um Besuche auf Webseiten zu protokollieren 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.

Denial-of-Service-Attacke: Versuch, ein E-Mail-System oder einen Webserver lahm zu legen, indem außergewöhnlich viele E-Mails oder Attachments gesendet werden.

Dictionary-Attacke: Programm, das einen Mailserver mit alphabetisch erzeugten E-Mail-Adressen bombardiert, in der Hoffnung, dass es manche Adressen korrekt errät. Mit dieser Methode werden auch Kennwörter erraten.

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

Diskette: Austauschbare magnetische Platte zum Speichern von Daten.

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.

False Positive: Meldung, dass ein Virus gefunden wurde (oder dass eine E-Mail Spam ist), wenn dies nicht der Fall ist.

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.

Greylist: E-Mail-Sender, die sich auf keiner Blacklist (ausgeschlossen) oder auf keiner Whitelist (akzeptiert) befinden, können auf eine Greylist gesetzt und aufgefordert werden, zu beweisen, dass sie legitime E-Mails senden.

Hacker: Computeranwender, der absichtlich die Computersicherheit durchbricht, meist um den normalen Betrieb zu stören oder an vertrauliche Daten, wie Finanzdaten, zu gelangen. Ursprünglich bezog sich der Begriff „Hacker“ auf jeden,

	der an Computern interessiert war; heutzutage allerdings bezeichnen die Medien und die Öffentlichkeit damit Computeranwender mit bösen Absichten.
Ham:	E-Mails, die ein Empfänger nicht als Spam betrachtet (siehe Spam).
Harvesting:	Prozess, bei dem das Internet durchsucht wird, um E-Mail-Adressen zu identifizieren, aus denen dann eine Spamming-Liste zusammengestellt wird.
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, meist per E-Mail, die Anwender absichtlich irreführt.
Honeypot:	Computersystem im Internet, das Spammer und Hacker anlocken soll.
HTML:	Hypertext Markup Language. Format für die meisten Dokumente im Internet.
HTTP:	Hypertext Transport Protocol. Protokoll, das Webserver verwenden, um Dokumente für Webbrowser zur Verfügung zu stellen.
HTTP-Überprüfung:	Echtzeit-Überprüfung von HTTP-Verkehr um sicherzustellen, dass Webseiten, die angesehen oder heruntergeladen werden, virenfrei sind.
Hypertext:	Computerlesbarer Text zum umfangreichen Verknüpfen von Dateien.
Internet:	Netzwerk aus verschiedenen, miteinander verbundenen Netzwerken. Das „Internet“ ist das weitaus größte dieser Netze.
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 Webseiten. 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.

Komplexe Wörterbuch-überprüfung: Funktion von Antispam-Software, die Text nach häufig in Spam verwendeten Ausdrücken durchsucht und von den verschiedenen Spam-Tricks, wie das Ersetzen von Buchstaben durch ähnlich aussehende Ziffern oder Zeichen (z. B. „1nterest r@te“), nicht umgangen werden kann.

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.

Mail-Drop: E-Mail-Adresse, die für den Empfang von Antwort-E-Mails auf Spam eingerichtet ist. Der Spammer löst das Konto auf, von dem aus die Spam-Mails versendet wurden, um seiner Erkennung zu entgehen.

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.

Munging: Methode zum Tarnen von E-Mail-Adressen, um sie vor Harvesting-Attacken zu schützen. Empfängern wird mitgeteilt, wie sie die Adresse dekodieren.

Newsgroup: Elektronisches Forum, in dem Leser Artikel und Meinungen zu bestimmten Themen ablegen.

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

Obfuscation: Versuche von Spammern, Daten zu verstecken, um zu verhindern, dass sie erkannt werden. Bezeichnet auch die Tarnung von E-Mail-Adressen, so dass Spammer mittels Harvesting-Attacken nicht an diese gelangen können.

Open Relay: SMTP-E-Mail-Server, der Dritten die Möglichkeit gibt, E-Mails weiterzuleiten. Spammer können diese Server missbrauchen und für die Versendung von Spam benutzen.

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

Parasitischer Virus: Siehe Programmvirus.

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

PDA: Personal Digital Assistant. Kleiner, mobiler Computer zur Datenverwaltung von Adressbüchern und Kalendern.

Phishing: Trick, um Anwender dazu zu bringen, vertrauliche Daten oder Kennwörter zu senden, indem Repliken legitimer Websites erzeugt werden.

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.
Real-Time-Blackhole-Liste (RBL):	Liste, die alle E-Mails (gültige und ungültige) abweist, die von Adressen stammen, die als Spam oder Spammer-Host bekannt sind. Damit können Internet Service Provider dazu gebracht werden, Antispam-Maßnahmen zu ergreifen.
Reverse-DNS-Check:	Überprüfung der E-Mail-Adresse eines Senders in einer Domain Name System Datenbank, um sicherzustellen, dass die E-Mail von einem gültigen Domänennamen oder einer gültigen Internet-Adresse stammt.
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 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:	Alle nicht angeforderten kommerziellen (Unsolicited Commercial Email - UCE) und nicht angeforderten Massen-E-Mails (Unsolicited Bulk Email - UBE), die ein Empfänger nicht erhalten möchte.
Spambot:	Programm, mit dem Spammer E-Mail-Adressen im Internet aufspüren.
Speicherresidenter Virus:	Virus, der im Speicher verbleibt, nachdem er aktiv war und sein Host-Programm beendet ist (im Gegensatz zu anderen Viren, die nur dann aktiviert werden, wenn eine infizierte Anwendung startet).
Spoofing:	Fälschen der Senderadresse in einer E-Mail. Durch Spoofing kann der Ursprung von Spam verschleiert werden. Empfänger können glauben, dass unsichere E-Mails aus einer zuverlässigen Quelle stammen.
Spyware:	Software, die die Benutzeraktivität protokolliert und Daten an Dritte weitergibt, z. B. an Werbefirmen. Das Protokollieren der Benutzeraktivität wird dem Benutzer in der Regel verheimlicht.
Tarpit:	Absichtlich langsamer Server, der als Falle für Spammer gedacht ist, die Harvesting-Programme verwenden.
Tarpitting:	Überwachung des E-Mail-Verkehrs, um remote IP-Adressen ausfindig zu machen, von denen verdächtig viele E-Mails versendet werden.
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 werden.
URL:	Uniform Resource Locator. Eine Internetadresse.
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.
Web-Bug:	Kleine Grafik, die in eine E-Mail oder Webseite eingefügt wird und einen Spammer benachrichtigt, wenn die E-Mail gelesen oder über die Vorschau-Funktion angesehen wird.
Webserver:	An das Internet angeschlossener Computer, der über HTTP Dokumente aus dem Internet zur Verfügung stellt.
Whitelist:	Liste externer E-Mail-Adressen, IP-Adressen und Domänen, die vertrauenswürdig sind, ohne auf Viren und/oder Spam überprüft zu werden.
World Wide Web:	Verbreitetes Hypertextsystem zum Lesen von Dokumenten im gesamten Internet.
Wurm:	Programm, das vielfache Kopien von sich verteilt. Im Gegensatz zu einem Virus benötigt ein Wurm kein „Wirt“-Programm.
WWW:	Siehe World Wide Web.
Zombie:	Unsicherer Computer, der „Hijacked“ ist und für eine DoS-Attacke (siehe Denial-of-Service-Attacke) oder zum Versenden von Spam benutzt wird.

Index

A

Adaptive Software 32
Antispam-Software 31
  adaptiv 32
Antiviren-Software 20
  heuristisch 20

B

Backdoor-Trojaner 15
Bootsektorvirus 11

C

Cookies 16

D

Denial-of-Service 8
Dokumentvirus 11

E

E-Mail-Virus 12, 13

H

"Harmloser" Virus 24
Heuristische Software 20
Hoaxes 41, 42
  Kettenbriefe 46
  Nebeneffekte 43
  Page-Jacking 44
  Phishing 45
  Vermeidung 47
  Viren-Hoaxes 42, 43
HTML
  und Spam 34, 36

I

Internetwurm 14

J

Jini 18

K

Kettenbriefe 46

M

Makrovirus, siehe Dokumentvirus
Mobiltelefone 17
Mouse-Trapping 44


Viren


Spam


Hoaxes


Sicherheit


Mehr Info

P

Page-Jacking 44
Palmtop 19
Phishing 45
PocketPC 19
Programmvirus 11
Proof-of-Concept-Virus 24

S

Sicherheitsregeln 49–52
Spam
  Definition 28
  Nebeneffekte 29
  Tricks zur Tarnung 34–36
  und Viren 37
  Vermeidung 38–39
Spam-Filter 31
  adaptiv 32
Spyware 16

T

Trojanisches Pferd 7
  Backdoor 15

V

Viren-Hoax 42
  Nebeneffekte 43
Virenschreiber 21
Virus
  auf einem Mobiltelefon 17
  auf einem Palmtop 19
  Bootsektor 11
  Definition 6
  Geschichte 22
  "harmlos" 24
  in Programmen 11
  Nebeneffekte 8–9
  Proof-of-Concept 24
  und Spam 37
  verbreitet durch E-Mail 12, 13
  Vermeidung 20, 25, 49–52

W

Web-Bug 30
Websites
  gefälscht 44, 45
  Page-Jacking 44
Wurm 7
  Internet 14