Bundesamt
für Sicherheit in der
Informationstechnik

Computer-Viren-Schutzkonzept

- Beispiel -

Stand: Dezember 2008

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

INHALTSVERZEICHNIS

A. Sensibilisierung

1 Einleitung

Ziel des Computer-Viren-Schutzkonzepts ist die Unterstützung der Schaffung eines effektiven Computer-Viren-Schutzes für die IT-Systeme sowie die Dokumentation aller diesbezüglichen Entscheidungen. M 2.154

Die Gesamtheit der enthaltenen organisatorischen Regelungen hat verbindlichen Charakter, so dass Verstöße gegen die Inhalte zu arbeitsrechtlichen Konsequenzen führen können.

Hinweis:

Bemerkungen und Hinweise, an welchen Stellen sich eine individuelle Anpassung oder Ergänzung des Musterkonzeptes besonders empfiehlt, sind gelb hinterlegt.

2 Schadensszenarien

Durch einen Computer-Virenbefall ist die Verfügbarkeit ganzer IT-Systeme gefährdet. Viren können Festplatten unbrauchbar machen, so dass es zu Fristversäumnissen durch eine verzögerte Bearbeitung von Aufträgen aufgrund nicht funktionsfähiger IT-Systeme kommen kann. Des Weiteren können finanzielle Schäden durch den Verlust von Daten entstehen, da diese unter Umständen nur mit erheblichem Aufwand rekonstruiert werden können. z. B. G 4.56

Ein Viren-Befall kann darüber hinaus zum Verlust der Integrität der Daten oder des IT-Systems führen. Dadurch können beispielsweise aufgrund einer falschen Datenbasis oder durch einen fehlerhaften Programmablauf fehlerhafte Ergebnisse generiert werden. Dies kann in gleicher Weise auch für komprimierte Dateien gelten, wenn das Viren-Schutzprogramm nicht geeignet ist. z. B. G 5.2

Durch ein Trojanisches Pferd kann die Vertraulichkeit von Daten gefährdet werden, indem persönliche oder weitere vertrauliche Informationen „gestohlen“ werden.. Der Verlust personenbezogener Daten oder Zugangsdaten kann zudem einen Verstoß gegen Datenschutzgesetze darstellen. Im Falle des Verlusts interner vertraulicher Informationen können Wettbewerbsvorteile verloren gehen. z. B. G 5.21

Wenn Computer-Viren an Kunden/Bürger oder Geschäftspartner weitergegeben werden, kann einen Imageschaden entstehen. Darüber hinaus können Imageschädigungen dadurch eintreten, dass Geschäftsprozesse oder einzelne Dienstleistungen nicht aufrechterhalten werden können und somit Verzögerungen entstehen.

3 Infektionswege

IT-Systeme können durch Viren auf verschiedene Weisen infiziert werden. Nachfolgend sind die häufigsten Infektionswege aufgezeigt. Die Reihenfolge der dargestellten Wege orientiert an der Wahrscheinlichkeit bzw. der Häufigkeit des Auftretens. Die größte Gefahr besteht in der Öffnung der internen Netze nach außen, so dass die Gefahren insbesondere aus externer E-Mail-Kommunikation, dem Internetzugang und dem Austausch von Datenträgern resultieren. Das interne Netz kann die Ausbreitung in der Institution „begünstigen“.

a) E-Mail

E-Mail dient immer öfter als Ersatz oder als Ergänzung zu anderen Bürokommunikationswegen. Mit Hilfe von Attachments (Anhängen) können Dateien effizient transportiert und E-Mail als Groupware-Lösung genutzt wer- M 5.88

A. Sensibilisierung

den. Die angehängten Dateien können mit einem Virus infiziert sein und mittels E-Mail von außen in die Institution eingebracht und dort weiterverbreitet werden.

b) Internet

Doch auch durch die immer größere Verbreitung von aktiven Inhalten auf WWW-Seiten entsteht die Gefährdung der Viren-Infektion. Momentan ist hiermit Java, ActiveX und Javascript gemeint, künftig könnten auch noch weitere Techniken hinzukommen. Auch können über Plug-Ins aus dem Browser heraus andere Programme gestartet werden. Auch Dateien und Programme, die aus dem Internet heruntergeladen werden, können infiziert sein. M 5.69

Gefährlich sind Schadprogramme, die sich über das Internet verbreiten und technisch so konstruiert sind, dass sie über eine nicht geschlossene Sicherheitslücke eines Programms (z. B. Browser oder Betriebssystem) direkt den Rechner infizieren.

c) Internes Netz

Der interne Austausch von E-Mails und die Vernetzung der Rechner können die Ausbreitung eines Computer-Virus oder anderer Schadprogramme innerhalb der Institution herbeiführen. Sofern eine standortübergreifende Vernetzung vorhanden ist (z. B. Virtual Private Network) wird hierdurch die Verbreitung auch auf andere Standorte ermöglicht.

Auch Rechner, die nur temporär in das Netz eingebunden sind, sind durch Viren bedroht. So können durch fehlende oder mangelhafte Anpassungen an Veränderungen des IT-Systems Sicherheitslücken entstehen.

d) Wechseldatenträger

Über Wechseldatenträger (Disketten, CDs, DVDs, USB-Sticks etc.) können Dateien oder Programme mit Computer-Viren IT-Systeme infizieren. M 2.45

B. Sicherheitsmaßnahmen

4 Erfassung der bedrohten IT-Systeme

Für ein effektives und effizientes Computer-Viren-Schutzkonzept sind die potentiell von Computer-Viren bedrohten IT-Systeme zu identifizieren, um angemessene Maßnahmen zu veranlassen. Es ist eine Übersicht aller IT-Systeme zu erstellen, die im Einsatz sind oder deren Einsatz geplant ist. Daraus können die IT-Systeme herausgefiltert werden, für die Viren eine Bedrohung darstellen oder über die Viren verteilt werden können. M 2.155

Prinzipiell sind alle IT-Systeme sind durch Computer-Viren gefährdet. Man kann die IT-Systeme zum besseren Verständnis in vier Gruppen einteilen:

- E-Mail-Server/Gateway — M 5.110, M 5.94
- Laptops; weil sie teils im Intranet, teils mobil ohne Netzanschluss verwendet werden und dadurch besonderen Gefahren unterliegen. — M 4.27
- vernetzte Systeme (Client/Server) — M 2.322
- Stand-Alone-Systeme, die nicht ans Intranet angeschlossen sind und daher z. B. eine Sonderrolle bei der Softwareverteilung einnehmen, die wesentlich aufwendiger ist. — M 5.46

5 Festlegung der Sicherheitsmaßnahmen

Alle Mitarbeiter werden entsprechend ihrer Rolle und Vorbildung regelmäßig geschult. M 3.5

Generell ist zu prüfen, inwiefern alle Rechner zwingend an das interne Netz angeschlossen bzw. mit anderen Rechnern verbunden werden müssen. Durch die Vernetzung von IT-Systemen wird das Risiko der Verbreitung von Computer-Viren erhöht. Durch die Abkopplung vom Netz wird die Übertragung von Computer-Viren von einem auf einen anderen Rechner erschwert und eine mögliche Infektion bleibt lokal isoliert.

Rechner, auf denen Daten mit sehr hohem Schutzbedarf verarbeitet werden, dürfen nicht direkt ans Internet angeschlossen werden.

Folgende Sicherheitsmaßnahmen sind zu installieren.

- Es ist ein zentraler Virenschutz durch die Installation eines zentralen, residenten Computer-Viren-Schutzprogramms sicherzustellen. Zusätzlich sollen auch lokale Computer-Viren-Schutzprogramme eingesetzt werden. In der Regel genügt es, nur ausführbare Dateien, Skripte, Makrodateien etc. zu überprüfen. Ein vollständiges Durchsuchen aller Dateien empfiehlt sich trotzdem in regelmäßigen Abständen (z. B. vor einer Tages- oder Monatssicherung). — M 4.3
- Es dürfen grundsätzlich keine Rechner ohne residenten Virenschutz betrieben werden (dies schließt Laptops mit ein). — M 4.3, M 2.157
- Ein- und ausgehende E-Mails sind zentral am Gateway auf Computer-Viren hin zu prüfen. — M 4.199
- Die Internetnutzung ist sicher zu gestalten, indem aktive Inhalte möglichst vermieden werden. Aktive Inhalte sind nur auf separaten, nicht an das interne Netz angeschlossenen sogenannten Internet PCs zu ermöglichen. — M 2.234
- Dateien und Programme sind nur durch Berechtigte von vertrauenswürdigen Quellen herunterzuladen. Dies ist technisch zu unterstützen. — M 2.154, M 2.224
- Es ist auf den Servern eine Firewall zu installieren, die aktive Inhalte filtert. Gleiches gilt für Laptops, wenn sie auch mobil genutzt und ans — M 2.78, M 4.100f

B. Sicherheitsmaßnahmen

Internet angeschlossen werden. Seiten mit aktiven Inhalten können vom IT-Sicherheitsbeauftragten einzeln zugelassen werden, wenn der Betreiber vertrauenswürdig ist und der Zugang aus dienstlichen Gründen erforderlich ist.

- Es ist für einen Dialerschutz zu sorgen, wenn Modems oder eine ISDN-Anlage/Karte genutzt werden. Kritische Nummernbereiche können z. B. zentral an der ISDN-Anlage gesperrt werden. Auf Laptops können Dialer-Schutzprogramme installiert werden. M 5.98
- Es ist eine Testumgebung festzulegen, um übersandte Dateien mit dem jeweiligen Anwendungsprogramm auf Makro-Viren zu untersuchen. Das automatische Ausführen von Makros ist in der Normalumgebung zu verhindern. M 4.33
- Die Funktion des Browsers, heruntergeladene Daten automatisch zu öffnen, ist zu deaktivieren. Aktive Inhalte dürfen bei der Anzeige in E-Mail-Clients nicht automatisch ausgeführt werden (Vorschaufunktion deaktivieren). M 5.94 M 5.94
- Innerhalb der Default-Einstellungen ist sicher zu stellen, dass Datei-Endungen nicht unterdrückt werden. Andernfalls wird es dem Nutzer erschwert, Dateiarten (z. B. Textverarbeitungs- oder Anwendungsdateien) zu unterscheiden und Gefährdungspotentiale einzuschätzen.

Zu beachten gilt, dass selbst bei einem Computer-Viren-Schutzprogramm, das immer auf dem neuesten Stand ist, kein absoluter Schutz gegeben ist. Das System ist zumindest solange neuen Viren ausgesetzt, bis geeignete Computer-Virensignaturen von den Herstellern von Schutzprogrammen zur Verfügung gestellt werden.

6 BIOS-Sicherheitseinstellungen

Für das BIOS sind Sicherheitsmaßnahmen erforderlich, weil nahezu alle technischen Viren-Schutzmaßnahmen erst nach Starten des Betriebssystems aktiv werden.

BIOS-Einstellungen sind dabei nur durch den autorisierten Administrator durchzuführen.

Passwortschutz

Es ist zu verhindern, dass Unbefugte die BIOS-Einstellungen ändern. Hierfür ist das Setup- oder Administrator-Passwort oder mindestens der Passwortschutz für die Zugriffe auf die BIOS-Einstellungen zu aktivieren. M 4.84

Boot-Reihenfolge

Die Boot-Reihenfolge beim Betriebssystemstart ist so umzustellen, dass generell zuerst von der Festplatte und dann erst von einem externen Medium (Diskette, CD, USB-Sticks) gestartet wird. Dies schützt vor der Infektion mit Boot-Viren, falls versehentlich oder absichtlich ein bootfähiger Datenträger im Laufwerk vergessen wird. M 4.84

C. Regelungen

7 Computer-Viren-Verantwortlicher

Von der Geschäftsführung wurde dem IT-Sicherheitsbeauftragten in Personalunion die Funktion des zentralen Computer-Viren-Verantwortlichen übertragen.

Der IT-Sicherheitsbeauftragte legt die Informationssicherheitsanforderungen in Absprache mit der Geschäftsführung fest. Er wird bei seiner Arbeit durch die zuständigen Administratoren unterstützt und überwacht ihre Tätigkeiten.

8 Verhaltensregeln zur Vorbeugung

8.1 Administrator

Soft- und Hardware sind durch den Administrator möglichst so zu konfigurieren, dass ohne weiteres Zutun des Benutzers optimale Sicherheit erreicht wird. Default-Einstellungen sind zu prüfen und Default-Passwörter zu ändern. Die Programme sind sicher einzustellen und vorhandene Sicherheitsfunktionen zu aktivieren, z. B. Schutz vor Makro-Viren innerhalb von Office-Programmen. M 2.87, M 4.30, M 4.79, M 2.11

Das Abschalten der Sicherheitsfunktionen durch den Benutzer ist nach Möglichkeit technisch zu verhindern.

Vor dem Einsatz ist neue Soft- und Hardware zu testen. Dabei sollten nach Möglichkeit Testsystem und Produktivbetrieb getrennt werden. M 4.65

Hard- und Software muss vor dem Einsatz freigegeben werden. Softwareänderungen machen eine erneute Freigabe erforderlich. M 2.9, M 2.62

Das automatische Ausführen von Makros ist zu verhindern.

Um Sicherheitslücken zu schließen, hat sich der Administrator regelmäßig über sicherheitsrelevante Patches, Updates oder sonstige Anleitungen zur Behebung beispielsweise beim Hersteller oder in einschlägigen Informationsquellen, zu informieren. M 2.35

Es sind die von den Herstellern veröffentlichten Patches und Updates zu beschaffen, insbesondere für Viren-Schutzprogramme und andere sicherheitsrelevante Programme wie Browser und Betriebssystem, und auf dem jeweiligen IT-System zu installieren. Sind keine entsprechenden Updates oder Patches verfügbar, müssen zusätzliche Sicherheitsmaßnahmen (Installation von Sicherheits-Soft- und -Hardware) ergriffen werden. M 2.273

Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Zusätzlich sind diese mit Hilfe eines aktuellen Viren-Schutzprogramms zu prüfen, bevor ein Update oder Patch installiert wird.

In jedem Fall muss dokumentiert werden, wann, von wem und aus welchem Anlass Patches und Updates eingespielt wurden, so dass sich der aktuelle Patchlevel des Systems jederzeit schnell ermitteln lässt. M 2.25, M 2.201

Da Viren-Schutzprogramme mit der Zeit ihre Wirksamkeit verlieren, muss eine regelmäßige Aktualisierung erfolgen (Update der Viren-Signaturen). M 2.159

Bei der Installation von Updates ist insbesondere darauf zu achten, dass durch voreingestellte Parameter die bestehende Konfiguration des Computer-Viren-Schutzprogramms nicht verändert wird.

Die Computer-Viren-Signaturen sind darüber hinaus zu gegebenen Anlässen, z. B. aufgrund neuer Viren, zu aktualisieren. Es sind mindestens einmal in der M 2.159

C. Regelungen

Woche, idealerweise täglich, die Informationen des Herstellers abzufragen. Sofern Aktualisierungen notwendig sind, sind diese herunterzuladen.

Innerhalb eines vernetzten IT-Systems sind die Aktualisierungen der Viren-Signaturen auch an den Clients sicherzustellen. Hierbei ist sinnvollerweise durch den Server auf den Clients eine Aktualisierung zu initiieren und somit das Viren-Schutzprogramm der Clients automatisch ohne Zutun des Nutzers zu aktualisieren (Push-Prinzip).

Zu beachten gilt, dass auch Rechner, die keiner bestimmten Person zugeordnet werden können, ebenfalls bei den Aktualisierungen berücksichtigt werden. Dies gilt insbesondere für mobile Rechner (Laptops): Es ist sicher zu stellen, dass auch diejenigen Laptops, die sich während der planmäßigen Aktualisierungen nicht im Haus befinden, zeitnah aktualisiert werden.

Es sind sporadische Kontrollen der Rechner vorzunehmen: So ist die Funktionalität und die Aktualität des Viren-Schutzprorgamms zu überprüfen. Weiterhin sollte geprüft werden, ob nicht-freigegebene oder verbotene Soft- und Hardware genutzt wird oder Benutzer unzulässige Rechte haben. Des Weiteren ist Kapitel 11 („Revision“) zu beachten.

Je nach Betriebssystem sind die notwendigen Schritte bei Virenbefall vorzubereiten, die zur Entfernung der Viren notwendig sind und den Wiederanlauf ermöglichen, wie beispielsweise das Rückspielen von Datensicherungen. Dies ist zu dokumentieren.

Es ist ein Notfallkonzept zu erstellen und Notfallübungen durchzuführen. M 6.3

Die Benutzer sind bei der Arbeit und der Umsetzung von IT-Sicherheitsmaßnahmen zu unterstützen. Hierbei sind die Laptop-Benutzer im Speziellen zu unterstützen. Alle Benutzer und der IT-Sicherheitsbeauftragte sind regelmäßig über Neuerungen (Bedrohungen und Sicherheitsmaßnahmen) zu informieren. Der IT-Sicherheitsbeauftragte berichtet bei Bedarf an den IT-Leiter. M 2.12

8.2 IT-Benutzer

Die Benutzer tragen dafür Verantwortung, IT-Systeme so zu nutzen, dass eine Infektion mit Computer-Viren vermieden wird. Dies heißt im Einzelnen:

- Alle verdächtigen Ereignisse (s. u.) sind unverzüglich dem Computer-Viren-Verantwortlichen zu melden.
- Verdächtige Dateien dürfen nicht selbständig geöffnet werden. In Zweifelsfällen muss der Computer-Viren-Verantwortliche um Rat gefragt werden.
- Viren-Schutz-Programme dürfen nicht deaktiviert werden.
- Vorgegebene Sicherheitseinstellungen dürfen nicht deaktiviert oder umgangen werden.
- Software darf nur von berechtigten Administratoren oder in Absprache mit diesen installiert werden.
- Sofern die Nutzung privater Hardware (z. B. PDAs oder Mobiltelefone) zusammen mit dienstlicher Hardware oder zur sonstigen dienstlichen Nutzung genehmigt wurde, sind die technischen und organisatorischen Maßnahmen im Rahmen des Computer-Virenschutzes zu beachten.
- IT-Systeme sollten sorgfältig hinsichtlich möglicher Gefahren beobachtet werden.
- Jeder Verdacht auf Computer-Viren muss sofort gemeldet werden.
- Eingehende und ausgehende Dateien sind im Falle eines Datenträgeraustauschs einer Viren-Prüfung zu unterziehen.

C. Regelungen

Werden E-Mails nicht über das zentrale E-Mail-Gateway versendet, sind Dateianhänge ebenfalls vorher auf Viren zu prüfen.

- Jeder IT-Benutzer hat vor der ersten Nutzung von IT-Diensten an den angebotenen Schulungen teilzunehmen.

9 Verhaltensregeln bei Auftreten eines Computer-Virus

9.1 Anzeichen für einen Viren-Befall

Folgende Anzeichen können auf einen Computer-Virenbefall hindeuten:

- häufige Programmabstürze
- Programmdateien werden länger
- unerklärliches Systemverhalten
- „unerklärliche“ System-Fehlermeldungen
- Nutzung unbekannter Dienste
- nicht auffindbare Dateien
- veränderte Dateiinhalte
- ständige Verringerung des freien Speicherplatzes, ohne dass etwas abgespeichert wurde

Sofern diese Anzeichen vorliegen, sind zur Feststellung eines Computer-Virus und anschließenden Beseitigung die in den nachfolgenden Kapitel (9.2 „Verhaltensregeln für den IT-Benutzers“ und 9.3 „Verhaltensregeln für den Computer-Viren-Verantwortlichen“) Schritte durchzuführen. M 6.23

9.2 Verhaltensregeln für den IT-Benutzers

Bei Auftreten eines Computer-Virus ist zu verhindern, dass weitere IT-Systeme infiziert werden. Daher ist ein entdeckter Computer-Virus (bzw. der Verdacht) unverzüglich dem Computer-Viren-Verantwortlichen persönlich oder telefonisch zu melden. Ist dies nicht umgehend möglich, muss sofort die IT-Leitung oder Firmenleitung verständigt werden. M 2.158

Bis zur Klärung des Sachverhalts durch den Computer-Viren-Verantwortlichen darf das betroffene IT-System nicht mehr benutzt werden und sollte unverändert belassen werden, um keine Spuren zu verwischen.

Wenn arbeitsrechtliche Konsequenzen gewünscht sind, sollte es an dieser Stelle vermerkt werden. Der folgende Satz ist lediglich als Beispiel zu verstehen, nicht als Vorgabe des BSI.

Wer einen Viren-Vorfall verschleiert oder ignoriert, muss mit arbeitsrechtlichen Konsequenzen rechnen. Wer dagegen einen Viren-Vorfall meldet und alles tut, um schlimmeren Schaden zu verhüten, wird nicht bestraft, auch wenn er durch fahrlässiges Verhalten den Viren-Befall verursacht hat.

9.3 Verhaltensregeln für den Computer-Viren-Verantwortlichen

Der Computer-Viren-Verantwortliche hat alle erforderlichen Maßnahmen einzuleiten. Dazu gehören:

- Verhinderung einer weiteren Ausbreitung
- Beseitigung des Virus
- Beweissicherung, Recherche, Feststellung der Quelle
- Analyse des Schadens (beispielsweise hinsichtlich Veränderung oder Löschung von Daten)
- gegebenenfalls Warnung der Mitarbeiter
- gegebenenfalls Warnung von Externen
- gegebenenfalls Deaktivierung von IT-Systemen oder bestimmten Diensten
- Komplette Überprüfung aller Rechner und gegebenenfalls Kontrolle

C. Regelungen

der Datensicherungen

Anschließend ist der Virenbefall durch den IT-Sicherheitsbeauftragten zu analysieren, um ein mögliches erneutes Eintreten des Notfalls technisch und/oder organisatorisch zu verhindern. Die Dokumentation und die Analyse bilden eine Grundlage für die Aktualisierung des Viren-Schutzkonzeptes.

10 Schulung

10.1 Administratoren

Ein Administrator hat sich hinsichtlich der Gefahren und der Möglichkeiten, diesen zu begegnen, ausführlich regelmäßig zu informieren. Die Leitung stellt dazu ausreichende Ressourcen zur Verfügung.

10.2 IT-Benutzer

Die Benutzer werden vor der erstmaligen Nutzung der jeweiligen IT-Dienste hinsichtlich der Gefahren sensibilisiert und auf die Sicherheitsmaßnahmen geschult. Schulungsinhalte sind: M 3.4

- Sensibilisierungsmaßnahmen M 2.198
  („Warum ist das IT-System so wichtig für mich und meinen Arbeitgeber?“)
- Beschreibung der verschiedenen Computer-Viren G 5.21, G 5.23
- Gefährdungspotential durch Computer-Viren G 5.21, G 5.23
  („Welche Gefahren bestehen für mich und meinen Arbeitgeber durch Viren-Befall?“)
- Schulung auf das Erkennen von Computer-Viren
  („Wie erkenne ich einen Viren-Befall?“)
- Korrekte Nutzung des Computer-Viren-Schutzprogramms M 3.4f
  - Nutzung des transienten Computer-Viren-Schutzprogramms
    („Wann und wie muss ich das Programm nutzen?“)
  - Nutzung des residenten Computer-Viren-Schutzprogramms
    (Verbot der Deaktivierung und der Änderung der Konfiguration)
- Korrekte Aktualisierung des Computer-Viren-Schutzprogramms M 3.4f
- Sichere Nutzung der sonstigen IT-Dienste M 3.4f
- Verhalten bei Auftreten eines Computer-Virus (Meldewege etc.) M 6.23

Mitarbeiter müssen auf das Problem von Falschmeldungen über Viren hingewiesen und darüber informiert werden, was beim Empfang einer Meldung zu tun ist. M 6.23

11 Revision

Das Computer-Viren-Konzept ist regelmäßig auf seine Aktualität und Wirksamkeit zu prüfen. Die Ursache jedes Viren-Befalls sollte analysiert und die Erfahrungen mit den getroffenen Maßnahmen ausgewertet werden.

Alle Sicherheitsmaßnahmen müssen regelmäßig daraufhin getestet werden, ob sie

- allen betroffenen Mitarbeitern bekannt sind,
- in den Betriebsablauf integrierbar sind.

Darüber hinaus ist regelmäßig zu überprüfen, ob die Mitarbeiter die Vorgaben des Computer-Viren-Konzepts beachten.

D. Glossar

Laut Definition ist ein **Computer-Virus** eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Dies bedeutet, dass der Virus ein Wirtsprogramm benötigt. Diese Eigenschaft und seine Befähigung zur Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung „Virus“.

Trojanische Pferde sind Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen. Im Gegensatz zu Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.

Eine Variante eines Trojanischen Pferdes ist die sogenannte **Backdoor**. Mit einem derartigen Programm wird eine Hintertür geöffnet, die es einem Angreifer ermöglicht, von außen den Rechner fernzusteuern. Diese Programme werden unter anderem auch zu sogenannten Denial of Service (DoS) Angriffen verwendet.

Ein **Computer-Wurm** ist ein Programm, das funktionierende Programme oder Programmsequenzen von sich herstellt. Ein Wurm kann sich über ein Netz selbständig weiter verbreiten. Das Ziel dabei ist, in einem Netz so viele Computer wie möglich zu befallen. Würmer benötigen dabei zum Ausbreiten kein menschliches Zutun. Würmer verbreiten sich rasend schnell. Manche Würmer tragen zusätzlich noch ein Schadprogramm.

Nicht nur Computer-Viren und -Würmer erzeugen einen großen Schaden. Auch unerwünschte Massen-E-Mails verursachen einen wirtschaftlichen Schaden. **Spam** ist eine Bezeichnung für Massen-E-Mail, meist Werbesendungen, die im Internet verbreitet werden. Diese Werbung wird unaufgefordert an Millionen von E-Mail-Adressen versendet. Durch die Übertragung und Bearbeitung von Spam entstehen jährlich Kosten in Milliardenhöhe. Oft ist die Absenderadresse der Spam-Mail gefälscht, so dass der eigentliche Verursacher nur schwer ausfindig gemacht werden kann.

Eine besondere Variante von Massen-E-Mail sind elektronische Enten, sogenannte **Hoaxes**. Diese enthalten häufig „Virus-Meldungen“, die vor einem „ganz neuen, gefährlichen“ Virus warnen. Die Meldungen stimmen jedoch nicht, sie sollen nur ungeschulte Anwender verunsichern und zu schädlichen Aktionen wie dem Löschen von Dateien oder dem Verbreiten der Falschmeldung veranlassen.

Eine weitere Art von Schaden wird durch **Dialer**-Programme verursacht. Zum Teil versuchen betrügerische Anbieter, einen solchen Dialer unbemerkt zu installieren. Die Dialer gelangen durch Computer-Viren oder E-Mail-Anhänge auf den Rechner.

Einige der verschiedenen E-Mail-Würmer benutzen als Absenderadresse eine Adresse aus dem E-Mail-Adressbuch des Benutzers, dessen E-Mail-Programm sie gerade befallen haben. So erhalten die nächsten Opfer die E-Mail, die den Wurm enthält, mit einer bekannten Absenderadresse und sind so eher gefährdet, die E-Mail oder gar den infizierten Anhang zu öffnen.