Parasol Island

Virenschutzkonzept

Dateiname:	02_08_PSL_ISMS_Virenschutzkonzept_v00.10_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Philip Hansen
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	07.11.2017 | Justus Heinser
Exportiert am:	07.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	07.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	-

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	15.09.2017	Justus Heinser	Ergänzung
00.10	07.11.2017	Justus Heinser	Finalisierung

Parasol Island

Inhaltsverzeichnis

Parasol Island

1. Einleitung

Ziel des Computerviren Schutzkonzepts ist die Unterstützung der Schaffung eines effektiven Computer Virenschutzes für die IT-Systeme sowie die Dokumentation aller diesbezüglichen Entscheidungen.
Die Gesamtheit der enthaltenen organisatorischen Regelungen hat verbindlichen Charakter, sodass Verstöße gegen die Inhalte zu arbeitsrechtlichen Konsequenzen führen können.

3. Schadensszenarien

Durch einen Computervirenbefall ist die Verfügbarkeit ganzer IT-Systeme gefährdet. Viren können Festplatten unbrauchbar machen, sodass 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.
Ein Virenbefall 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 Virenschutzprogramm nicht geeignet ist.
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.
Wenn Computerviren an Kunden/Bürger oder Geschäftspartner weitergegeben werden, kann ein Imageschaden entstehen. Darüber hinaus können Imageschädigungen dadurch eintreten, dass Geschäftsprozesse oder einzelne Dienstleistungen nicht aufrechterhalten werden können und somit Verzögerungen entstehen.

4. Infektionswege

IT-Systeme können durch Viren auf verschiedene Weisen infiziert werden. Nachfolgend sind die häufigsten Infektionswege aufgezeigt. Die Reihenfolge der dargestellten Wege orientiert sich an der Wahrscheinlichkeit bzw. der Häufigkeit des Auftretens. Die größte Gefahr besteht in der Öffnung der internen Netze nach außen, sodass 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“.

E-Mail

E-Mails sind mittlerweile der Haupt Kommunikationsweg eines jeden Unternehmen. Mit Hilfe von Attachments (Anhängen) können Dateien effizient transportiert und E-Mails als Groupware-Lösung genutzt werden. Die angehängten Dateien können mit einem Virus infiziert sein und mittels E-Mail von außen in die Institution eingebracht und dort weiterverbreitet werden.

Internet

Doch auch durch die immer größere Verbreitung von aktiven Inhalten auf WWW-Seiten entsteht die Gefährdung der Virusinfektion. 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.
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.

Internes Netz

Der interne Austausch von E-Mails und die Vernetzung der Rechner können die Ausbreitung eines Computervirus 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.

Wechseldatenträger

Über Wechseldatenträger (CDs, DVDs, USB-Sticks etc.) können Dateien oder Programme mit Computerviren IT-Systeme infizieren.

5. Erfassung der bedrohten IT-Systeme

Für ein effektives und effizientes Computer Virenschutzkonzept sind die potentiell von Computerviren 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.
Prinzipiell sind alle IT-Systeme durch Computerviren gefährdet. Man kann die IT-Systeme zum besseren Verständnis in vier Gruppen einteilen:

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

6. Festlegung der Sicherheitsmaßnahmen

Alle Mitarbeiter werden entsprechend ihrer Rolle und Vorbildung regelmäßig geschult.
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 Computerviren erhöht. Durch die Abkopplung vom Netz wird die Übertragung von Computerviren 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 Virenschutzprogramms sicherzustellen. Zusätzlich sollen auch lokale Computer Virenschutzprogramme 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).
- Es dürfen grundsätzlich keine Rechner ohne residenten Virenschutz betrieben werden (dies schließt Laptops mit ein).
- Ein- und ausgehende E-Mails sind zentral am Gateway auf Computerviren hin zu prüfen.
- Die Internetnutzung ist sicher zu gestalten, indem aktive Inhalte möglichst vermieden werden.
- Dateien und Programme sind nur durch Berechtigte von vertrauenswürdigen Quellen herunterzuladen. Dies ist technisch zu unterstützen.
- Es ist auf den Servern eine Firewall zu installieren, die aktive Inhalte filtert. Gleiches gilt für Laptops, wenn sie auch mobil genutzt und ans Internet angeschlossen werden. Seiten mit aktiven Inhalten können vom Informationssicherheitsbeauftragten einzeln zugelassen werden, wenn der Betreiber vertrauenswürdig ist und der Zugang aus dienstlichen Gründen erforderlich ist.
- 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 Normal Umgebung zu verhindern.
- 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).

- Innerhalb der Default-Einstellungen ist sicherzustellen, dass Dateiendungen nicht unterdrückt werden. Andernfalls wird es dem Nutzer erschwert, Dateitypen (z. B. Textverarbeitungs- oder Anwendungsdateien) zu unterscheiden und Gefährdungspotentiale einzuschätzen.

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

7. BIOS-Sicherheitseinstellungen

Für das BIOS sind Sicherheitsmaßnahmen erforderlich, weil nahezu alle technischen Virenschutzmaßnahmen 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.

Boot-Reihenfolge

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

8. Zuständigkeiten bei der Bekämpfung von Computerviren

Der Informationssicherheitsbeauftragte legt in Absprache mit der Geschäftsführung Richtlinien für den Umgang mit Computerviren fest. Die Durchführung der Richtlinien ist Aufgabe der IT-Administration. Diese wird vom ISB kontrolliert.

9. Verhaltensregeln zur Vorbeugung

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 Makroviren innerhalb von Office-Programmen. 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.
Hard- und Software muss vor dem Einsatz freigegeben werden. Softwareänderungen machen eine erneute Freigabe erforderlich.
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.
Es sind die von den Herstellern veröffentlichten Patches und Updates zu beschaffen, insbesondere für Virenschutzprogramme 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 Sicherheitssoft- und Hardware) ergriffen werden.
Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Zusätzlich sind diese mit Hilfe eines aktuellen Virenschutzprogramms zu prüfen, bevor ein Update oder Patch installiert wird.
Da Virenschutzprogramme mit der Zeit ihre Wirksamkeit verlieren, muss eine regelmäßige Aktualisierung erfolgen (Update der Virensignaturen).
Bei der Installation von Updates ist insbesondere darauf zu achten, dass durch voreingestellte Parameter die bestehende Konfiguration des Computer Virenschutzprogramms nicht verändert wird.
Die Computerviren Signaturen sind darüber hinaus zu gegebenen Anlässen, z. B. aufgrund neuer Viren, zu aktualisieren. Es sind mindestens einmal in der 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 Virenschutzprogramm 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 sicherzustellen, 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 Virenschutzprogramms zu überprüfen. Weiterhin sollte geprüft werden, ob nicht-freigegebene oder verbotene Soft- und Hardware genutzt wird oder Benutzer unzulässige Rechte haben.
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.
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 Informationssicherheitsbeauftragte sind regelmäßig über Neuerungen (Bedrohungen und Sicherheitsmaßnahmen) zu informieren. Der ISB berichtet bei Bedarf an den IT-Leiter.

IT-Benutzer

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

- Alle verdächtigen Ereignisse (s. u.) sind unverzüglich dem Computerviren-Verantwortlichen zu melden.
- Verdächtige Dateien dürfen nicht selbständig geöffnet werden. In Zweifelsfällen muss der Computerviren-Verantwortliche um Rat gefragt werden.
- Virenschutzprogramme 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. Smartphones) 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 Computerviren muss sofort gemeldet werden.
- Eingehende und ausgehende Dateien sind im Falle eines Datenträgeraustauschs einer Viren-Prüfung zu unterziehen.
- 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.

10. Verhaltensregeln bei Auftreten eines Computervirus

Anzeichen für einen Virenbefall

Folgende Anzeichen können auf einen Computervirenbefall 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 Computervirus und anschließenden Beseitigung die in den nachfolgenden Kapiteln beschriebenen Schritte durchzuführen.

11. Verhaltensregeln für den IT-Benutzer

Beim Auftreten eines Computerviruses ist zu verhindern, dass weitere IT-Systeme infiziert werden. Daher ist ein entdeckter Computervirus (bzw. der Verdacht) unverzüglich dem Administrator persönlich oder telefonisch zu melden. Ist dies nicht umgehend möglich, muss sofort der Sicherheitsbeauftragte oder die Firmenleitung verständigt werden.
Bis zur Klärung des Sachverhalts durch den Computerviren-Verantwortlichen darf das betroffene IT-System nicht mehr benutzt werden und sollte unverändert belassen werden, um keine Spuren zu verwischen.
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 Virenbefall verursacht hat.

12. Verhaltensregeln für den Administrator

Der Computerviren-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 der Datensicherungen

Anschließend ist der Virenbefall durch den Informationssicherheitsbeauftragten 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 Virenschutz Konzeptes.

13. Schulung

Administratoren

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

IT-Benutzer

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

- Sensibilisierungsmaßnahmen
- („Warum ist das IT-System so wichtig für mich und meinen Arbeitgeber?“)
- Beschreibung der verschiedenen Computerviren
- Gefährdungspotential durch Computerviren
- („Welche Gefahren bestehen für mich und meinen Arbeitgeber durch Virenbefall?“)
- Schulung auf das Erkennen von Computerviren
- („Wie erkenne ich einen Virenbefall?“)
- Korrekte Nutzung des Computer Virenschutzprogramms
- Nutzung des transienten Computer Virenschutzprogramms („Wann und wie muss ich das Programm nutzen?“)
- Nutzung des residenten Computer Virenschutzprogramms (Verbot der Deaktivierung und der Änderung der Konfiguration)
- Sichere Nutzung der sonstigen IT-Dienste
- Verhalten bei Auftreten eines Computervirus (Meldewege etc.)

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

14. Revision

Das Computerviren Konzept ist regelmäßig auf seine Aktualität und Wirksamkeit zu prüfen. Die Ursache jedes Virenbefalls 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 Computerviren Konzepts beachten.

15. Glossar

Laut Definition ist ein Computervirus eine nicht selbständige 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 führt 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 Computerviren 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 Computerwurm 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 Computerviren 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, sodass 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 Computerviren 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.