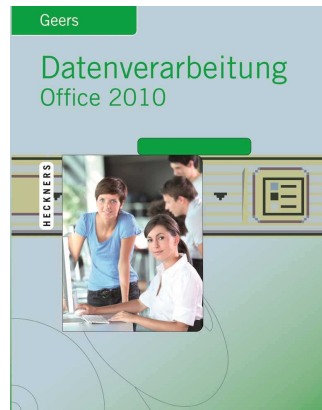


Werner Geers

Datenverarbeitung Office 2010

ISBN:978-3-427-61034-4

Bestellnr.:61034



 Bildungsverlag EINS

Zusatzinformationen

1	COMPUTERVIREN UND SONSTIGE SCHÄDLICHE PROGRAMME	2
1.1	Vorbemerkungen.....	2
1.2	Viren, Trojaner und andere Schädlinge.....	2
1.3	Virenarten.....	3
1.4	Backdoor-Steuerprogramme und Dialer	3
1.5	Virenschutz.....	4
1.6	Virenschutzprogramme	5
1.7	Virenschutz mit AntiVir Personal Edition.....	6
1.8	Spam-Schutz, Firewall, AntiSpy	6
1.9	Datensicherung auf Datenträgern usw.....	7
1.10	Sonstige Sicherungsmaßnahmen	7

Dieses Skript darf im Unterricht in Verbindung mit dem oben angegebenen Lehrbuch oder einem anderen Lehrbuch desselben Schulbuchautors eingesetzt werden.

1 Computerviren und sonstige schädliche Programme

1.1 Vorbemerkungen

Computerviren und ähnliche Programme, die über das Internet verbreitet werden, verursachen ungeheure wirtschaftliche Schäden. Daher ist es unbedingt notwendig, sich gegen Viren zu schützen. Dies ist vor allem durch einen vernünftigen, überlegten Umgang mit Daten aus dem Internet möglich, aber auch die Installation von Virenschutzprogrammen, die die Infizierung von Rechnern verhindern.

1.2 Viren, Trojaner und andere Schädlinge

Unterschiedliche Computerschädlinge verbreiten sich immer wieder über das Internet und per E-Mail. In der folgenden Übersicht werden die wichtigsten Begriffe erklärt:

Art	Erklärung
Viren	Ein Computervirus ist eine Sabotagesoftware, ein meistens in böswilliger Absicht geschriebenes Programm, das in Programme und/oder Dateien eingefügt wird und Fehlfunktionen und Störungen verursacht. In der Regel verbreiten sich Computerviren selbstständig, sodass innerhalb kürzester Zeit sehr viele Computer infiziert werden können. Neben Viren, die einen wirtschaftlichen Schaden verursachen, indem sie beispielsweise die Ausführung von Programmen verhindern, Datenträger und/oder Dateien löschen oder zerstören, gibt es auch Viren, die keinerlei Schaden verursachen.
Trojaner	Trojaner (Trojanische Pferde) geben vor, eine bestimmte, nützliche Aufgabe zu erfüllen. Das Programm vollzieht jedoch im Hintergrund eine vom Benutzer nicht gewollte Aktion. So werden beispielsweise Zugangsdaten und Passwörter ausgespäht. Damit können z. B. fremde Nutzer über das Internet Zugriff auf einen Computer erlangen oder über ausspionierte Passwörter Bestellungen, Zahlungen usw. über das Internet vornehmen. Mithilfe dieser Daten kann dann ein großer wirtschaftlicher Schaden entstehen.
Würmer	Ein Wurm verfügt meistens über keinerlei Schadensroutinen für den Computer, den er infiziert. Er nistet sich in der ersten Phase in Millionen von Computern ein und schlummert vor sich hin, ohne einen Schaden zu verursachen. Nach einer gewissen Zeit wird der Wurm automatisch aktiviert, alle infizierten Rechner nehmen z. B. Kontakt zu Internetservern auf, die dann unter der Last der vielen Kontakte für eine gewisse Zeit nicht mehr zu erreichen sind. Würmer verbreiten sich außerordentlich effektiv. Sie versenden sich beispielsweise automatisch über die Adressen eines Adressbuches eines E-Mail-Programms und/oder über die E-Mail-Adressen, die aufgrund von eingegangenen Mails vom E-Mail-Programm gespeichert wurden. Daher werden innerhalb kürzester Zeit weltweit außerordentlich viele Computer infiziert. In zunehmendem Maße werden Würmer mit Viren ausgestattet. Daher ist nicht auszuschließen, dass Wurmattacken in Zukunft vermehrt schwere wirtschaftliche Schäden verursachen.
Hoaxes	Als Hoaxes bezeichnet man Falschmeldungen, die oftmals als Virenwarnungen per E-Mail verbreitet werden. Sie richten keinerlei Schaden an. Oftmals wird in der Mail der Hinweis gegeben, guten Bekannten vor dem vermeintlichen Virus zu warnen. Auf diese Weise wird die Meldung schnell verbreitet.

1.3 Virenarten

Im Laufe der Zeit sind verschiedene Virenarten aufgetreten. Die wichtigsten sind in der nachfolgenden Tabelle aufgeführt:

Art	Erklärung
Bootviren	Die ältesten bekannten Computer-Viren sind die Boot-Viren, die sich im Bootsektor einer Festplatte oder einer Diskette einnisten. Bootviren sind besonders unangenehm, da vom BIOS aus alle im Rechner vorhandenen Festplatten, Disketten usw. infiziert werden. Es ist möglich, dass nach erfolgreicher Virenbeseitigung durch das Einlegen einer Diskette, die nicht „gereinigt“ wurde, der Virus sich erneut einnistet. Eine Entfernung des Virus mit einem Antiviren-Programm ist nur möglich, wenn von einem schreibgeschützten noch nicht infiziertem Datenträger gebootet wird.
Dateiviren	Dateiviren hängen sich an ausführbare Dateien (*.exe, *.com). Die Programme werden um den Code des Virus erweitert oder Teile des ursprünglichen Programms werden überschrieben. Eine Entfernung von Dateiviren ist nicht immer möglich, u. U. muss die Datei gelöscht werden. Der Virus kann so programmiert werden, dass beispielsweise Festplatten formatiert, Dateien gelöscht usw. werden.
Makro-Viren	Verschiedene Programme, so beispielsweise die Microsoft Office Programme, verfügen über die Möglichkeit, verschiedene Befehle in einem Makro zusammenzufassen. Damit ist die Möglichkeit gegeben, in Makros auch für den Anwender unerwünschte, schädliche Befehle einzufügen. Nicht bekannte Makros sollten daher in Dokumenten deaktiviert werden.
Script-Viren	Script-Viren werden beispielsweise mit Java-Script und Visual Basic Script programmiert und werden z. B. über HTML-Dokumente verbreitet. Sie können unterschiedliche Schäden verursachen.

1.4 Backdoor-Steuerprogramme und Dialer

Neben den Versuchen, mit Viren einen Schaden zu bewirken, gibt es Versuche, Daten von Computern zu stehlen oder durch Umleitung bei der Einwahl eines Computers in das Internet für den Benutzer hohe Kosten zu verursachen.

Backdoor-Steuerprogramme	Über Backdoor-Steuerprogramme wird versucht, in den Rechner von außen über das Internet einzudringen und danach den Rechner zu steuern und beispielsweise Daten zu stehlen. Unternehmensdaten wie Konstruktionspläne, Kundenlisten usw. sind hochsensible Daten, die, wenn sie von Fremden missbraucht werden, große wirtschaftliche Schäden verursachen können. Die Ausspähung von Passwörtern kann beispielsweise dazu genutzt werden, über das Internet Produkte zu beziehen. Die Zahlung erfolgt dann z. B. mithilfe einer gestohlenen Kreditkartennummer.
Dialer	Dialer versuchen, die Verbindung zum Internet über eine teure Einwahlmöglichkeit (z. B. 0900-Nummern) umzuleiten. Sie verursachen damit hohe Kosten, obwohl z. B. ganz normal im Internet gesurft wurde. Dialer werden oftmals über unseriöse Angebotsseiten im Internet verteilt.

1.5 Virenschutz

Das Bundesamt für Sicherheit in der Informationstechnologie (www.bsi.bund.de) hat *Empfehlungen für den Umgang mit Computer-Viren aus dem Internet* veröffentlicht. Die wichtigsten Empfehlungen für den Endanwender, also den Nutzern von Computern, wurden wörtlich in der folgenden Übersicht übernommen:

Maßnahmen für Endanwender

1. Einstellungen am Rechner

Bereits durch das Aktivieren verfügbarer Sicherheitsfunktionen wird das Eindringen von Computer-Viren erheblich erschwert.

- Alle vorhandenen Sicherheitsfunktionen des Rechners aktivieren (Passwort-Schutz, Bildschirmschoner mit Passwort, etc.), damit während der Abwesenheit des berechtigten Benutzers Unbefugte keine Möglichkeit haben, durch unbedachte oder gewollte Handlungen den Rechner zu gefährden.
- Aktuelles Viren-Schutzprogramm mit aktuellen Signatur-Dateien einsetzen, das im Hintergrund läuft (resident) und bei bekannten Computer-Viren Alarm schlägt.
- Im Microsoft Explorer sollte die Anzeige aller Dateitypen aktiviert sein.
- Makro-Virenschutz von Anwendungsprogrammen (WinWord, Excel, Powerpoint, etc.) aktivieren und Warnmeldungen beachten.
- Sicherheitseinstellungen von Internet-Browsern auf höchste Stufe einstellen (Deaktivieren von aktiven Inhalten [ActiveX, Java, JavaScript] und Skript-Sprachen [z. B. Visual Basic Script, VBS]), etc.
- Keine Applikationsverknüpfung für Anwendungen mit potentiell aktivem Code (MS-Office) im Browser nutzen oder Anwendungen über Internet aktivieren.

2. Verhalten bei E-Mail

2a) Eingehende E-Mail

Eingehende E-Mail ist das größte Einfalltor für Computer-Viren. Bei sicherheitsbewusstem Verhalten lassen sich hierbei schon die meisten Computer-Viren herausfiltern.

- Offensichtlich nicht sinnvolle E-Mails von unbekanntem Absendern sofort ungeöffnet löschen.
- Bei E-Mail auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern prüfen, ob der Text der Nachricht auch zum Absender passt (englischer Text von deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.
- Vorsicht bei mehreren E-Mails mit gleichlautendem Betreff.
- Kein "Doppelklick" bei ausführbaren Programmen (*.COM, *.EXE) oder Script-Sprachen (*.VBS, *.BAT), Vorsicht auch bei Office-Dateien (*.DOC, *.XLS, *.PPT) sowie Bildschirmschonern (*.SCR).
- Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten.
- Nur vertrauenswürdige E-Mail-Attachments öffnen (z. B. nach tel. Absprache). Es ist zu beachten, dass die Art des Datei-Anhangs (Attachment) bei Sabotageangriffen oft getarnt ist und über ein Icon nicht sicher erkannt werden kann.

Maßnahmen für Endanwender (Fortsetzung)**2b) Ausgehende E-Mail**

Durch Beachtung der folgenden Maßnahmen kann die Gefahr reduziert werden, dass ein Endanwender unabsichtlich Computer-Viren verteilt.

- E-Mails nicht im HTML-Format versenden, auch wenn es vom eingesetzten Mail-Programm her möglich wäre; ebenso sind aktive Inhalte in E-Mails zu vermeiden.
- WinWord-Dokumente im RTF-Format versenden (Damit wird auch die Weiterleitung von ggf. vertraulichen Informationen im nicht direkt sichtbaren Verwaltungsteil der DOC-Datei verhindert.)
- Keine unnötigen E-Mails mit Scherz-Programmen und ähnlichem versenden, da diese evtl. einen Computer-Virus enthalten können.
- Keinen Aufforderungen zur Weiterleitung von Warnungen, Mails oder Anhängen an Freunde, Bekannten oder Kollegen folgen, sondern direkt nur an den IT-Sicherheitsbeauftragten senden. Es handelt sich nämlich meist um irritierende und belästigende Mails mit Falschmeldungen (Hoax oder "elektronische Ente", Kettenbrief).
- Gelegentlich prüfen, ob E-Mails im Ausgangs-Postkorb stehen, die nicht vom Benutzer selbst verfasst wurden.

3. Verhalten bei Downloads aus dem Internet

Daten und Programme, die aus dem Internet abgerufen werden, stellen einen Hauptverbreitungsweg für Computer-Viren und Trojanische Pferde dar, um Benutzerdaten auszuspähen, weiterzuleiten, zu verändern oder zu löschen. Es muss darauf hingewiesen werden, dass auch Office-Dokumente (Text-, Tabellen- und Präsentations-Dateien) Makro-Viren enthalten können.

- Programme sollten nur von vertrauenswürdigen Seiten geladen werden, also insbesondere von den Originalseiten des Erstellers. Private Homepages, die bei anonymen Webpace-Providern eingerichtet werden, stellen hierbei eine besondere Gefahr dar.
- Die Angabe der Größe von Dateien, sowie einer evtl. auch angegebenen Prüfsumme, sollte nach einem Download immer überprüft werden. Bei Abweichungen von der vorgegebenen Größe oder Prüfsumme ist zu vermuten, dass unzulässige Veränderungen, meist durch Viren, vorgenommen worden sind. Daher sollten solche Dateien sofort gelöscht werden.
- Mit einem aktuellen Viren-Schutzprogramm sollten vor der Installation die Dateien immer überprüft werden.
- Gepackte (komprimierte) Dateien sollten erst entpackt und auf Viren überprüft werden. Installierte Entpackungsprogramme sollten so konfiguriert sein, dass zu entpackende Dateien nicht automatisch gestartet werden.

1.6 Virenschutzprogramme

Viren werden in der Regel mit sogenannten Virenschutzprogrammen bekämpft. Diese Programme sind meistens gegen Entgelt zu erhalten; einige Programme sind jedoch auch als FreeWare zu erhalten bzw. stehen Privatanwendern kostenlos zur Verfügung. Oftmals werden die Programme auf den Datenträgern aktueller Computerzeitschriften und auf den Internetseiten der Anbieter angeboten.

Ein gutes Virenschutzprogramm sollte u. a.

- Datenträger auf Virenbefall prüfen und alle bekannten Viren erkennen und löschen,
- regelmäßig durch Updates auf den neuesten Stand gebracht werden können,
- automatisch beim Einschalten eines Computers aktiviert werden,
- alle eingehenden E-Mails und aus dem Internet geladene Dateien auf Virenbefall prüfen und eventuelle Viren unschädlich machen,
- u. U. befallende Dateien, aus denen Viren nicht gelöscht werden können, löschen.


1.7 Virenschutz mit AntiVir Personal Edition


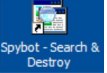
Virenschutzprogramme müssen in der Regel käuflich erworben werden. Das Programm **AntiVir Personal Edition** (www.free-av.de) wird für Privatpersonen kostenlos zur Verfügung gestellt und stellt einen guten Schutz vor Viren dar, da es jederzeit über das Internet auf den neuesten Stand gebracht werden kann. Auf dem beiliegenden Datenträger finden Sie im Ordner *Anleitungen* eine mehrseitige Anleitung als PDF-Datei zur Arbeit mit dem Programm. Durch die Anwendung des Programms schützen Sie Ihren Computer und die Daten auf dem Computer. Außerdem lernen Sie den Umgang mit einem Virenschutzprogramm kennen.



1.8 Spam-Schutz, Firewall, AntiSpy


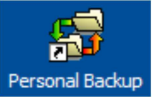
Neben Viren wird die Sicherheit durch andere schädliche oder lästige Programme und Daten aus dem Internet beeinträchtigt. Nachfolgend werden die wichtigsten Probleme beschrieben. Auf dem beiliegenden Datenträger finden Sie Programme und Erklärungen (PDF-Dateien), die eventuelle Probleme beheben können.

Art	Erklärung
SPAM-Schutz 	<p>Mit SPAM-Schutz-Programmen wird versucht, der unerwünschten Werbeflut durch E-Mails Einhalt zu bieten. Verschiedene Mechanismen und Einstellungen sollen verhindern, dass SPAM-Mails den Empfänger erreichen.</p> <ul style="list-style-type: none"> • Filter-Mechanismen Bestimmte Bestandteile, Schlüsselwörter usw. werden SPAM-Mails zugeordnet. Der Benutzer kann durch Einstellungen zum Teil selbst bestimmen, welche Mails abgeblockt werden sollen und welche nicht. • Filterempfindlichkeit Eingehende Mails werden z. B. nur abgeblockt, wenn die Erkennungsmethoden offensichtliche, deutliche oder wenige für SPAMS typische Merkmale enthalten. • Individuelle Positiv- und Negativlisten In einer Positivliste werden alle E-Mail-Adressen aufgenommen, von denen gewünschte Mails entgegengenommen werden sollen. Die Negativliste bestimmt alle Mail-Adressen, deren Mails nicht angenommen werden sollen. Da Werbemailer jedoch immer wieder andere Adressen benutzen, ist der Eintrag von Adressen zumeist nicht sehr effektiv. Daher können u. U. alle Adressen in die Negativliste aufgenommen werden, die nicht in der Positivliste sind. Hierbei besteht jedoch eine große Gefahr, dass erwünschte Mails den Empfänger nicht erreichen.

Art	Erklärung
Firewall 	<p>Eine Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Es wird dafür gesorgt, dass jede Kommunikation zwischen den beiden Netzen über die Firewall geführt werden muss. Eine Firewall kann man gleichzeitig als „elektronischen Pförtner“ und „elektronische Brandschutzmauer“ bezeichnen. Sie sichert und kontrolliert den Übergang von einem zu schützenden Netz zu einem unsicheren öffentlichen Netz, also in der Regel dem Internet.</p>
AntiSpy 	<p>Zwielichte Unternehmen und Personen versuchen, Spionageprogramme auf fremden Computern zu installieren, um fremde Daten, z. B. Kreditkartennummern, Konstruktionspläne usw., illegal zu nutzen. Durch eine AntiSpy-Software werden Spionagedateien gesucht und entfernt.</p>

1.9 Datensicherung auf Datenträgern usw.

Die Sicherung von Daten auf Datenträgern, der Schutz von Daten gegen unerlaubte Nutzung usw., wird nachfolgend erklärt. Erklärungen zum Einsatz von Programmen finden Sie im Kapitel *Multimedia* oder als PDF-Datei auf dem beiliegenden Datenträger.

Art	Erklärung
Datensicherung CD/DVD 	<p>Die Sicherung von Daten auf eine CD oder DVD wird von einer sogenannten Brennsoftware vorgenommen. Oftmals wird die entsprechende Software beim Kauf eines Computers mitgeliefert, ansonsten steht mit dem Programm DeepBurner ein günstiges FreeWare-Programm zur Verfügung. Die Möglichkeiten des Programms beschränken sich im Wesentlichen auf die Datensicherung, die Erstellung einer Audio-CD ist ebenfalls möglich.</p>
Daten-Backup 	<p>Die Durchführung eines Daten-Backups ist eine Alternative zur normalen Datensicherung. Große Datenmengen werden beispielsweise auf Bändern, externen Festplatten, USB-Sticks usw. gesichert. Die Speicherkarten können dann beispielsweise dazu eingesetzt werden, die Daten eines Personal Computers auf einen Laptop zu übertragen.</p>

1.10 Sonstige Sicherungsmaßnahmen

Nachfolgend werden weitere Maßnahmen zur Datensicherung angesprochen. Erklärungen finden Sie im Buch oder auf dem beiliegenden Datenträger.

Art	Erklärung
PDF-Dateien	<p>PDF-Dateien (Portable Document Format) können in der Regel nur gelesen und nicht verändert werden. Der Nutzer kann sich das Dokument auf dem Bildschirm ansehen und bei Bedarf ausdrucken. PDF stellt heute ein Standardformat für Dokumente dar.</p>
Schutz von Dokumentinhalten	<p>Tabellen, Texte oder Präsentationen können Daten enthalten, die geheim bleiben oder nicht oder noch nicht für die Öffentlichkeit bestimmt sind. Ein Beispiel für Dokumentenschutz finden Sie im Kapitel <i>Arbeiten mit Word</i>.</p>
Datenkomprimierung	<p>Durch die Datenkomprimierung werden Dateigrößen verringert, eventuell auch mehrere Dateien zu einer Datei zusammengefasst.</p>