Gefahren für Ihren PC und deren Abwehr

Autoren: Michael Eckel
Daniel Fischer
Ralf Decher

Ort: FH Gießen-Friedberg

Datum: 29.06.2006

Dozent: Anke Roos

Inhaltsverzeichnis

Michael Eckel
Daniel Fischer
Ralf Decher

1 Gefahren für Ihren PC

Seit Beginn der Computer-Epoche und der Erfindung der „Personal Computer“ (PCs) gibt es bereits Schwachstellen in diesen Systemen, was sich vor allem auf die Software und weniger auf die Hardware bezieht. Diese Schwachstellen der Software können ausgenutzt werden, um dem System Schaden zuzufügen, was durch einen „Computervirus“ geschehen kann. Computerviren selbst sind auch „nur“ Software, obwohl sie, je nach System, auch der Hardware erheblichen Schaden zufügen können. Anfangs dienten sie nur zum Aufzeigen diverser Schwachstellen in den Systemen und waren recht harmlos. Doch bald erkannte man das (negative) Potential, das in Computerviren steckte. Es folgten rasante Weiterentwicklungen der Schädlinge und der Ausbau ihrer Fähigkeiten. Von simplen Viren, die nur Dateien löschten, über solche die Daten ausspionierten bis hin zu solchen, die eine Hintertür (Backdoor) im infizierten System öffneten und Benutzern von außerhalb Zugriff auf das System gewährten.

Bis heute wurden die Schädlinge noch sehr viel weiter entwickelt und kommen fast nur noch in Mischformen vor, d.h. sie bestehen aus Kombinationen von verschiedenen Schädlingstypen. Die Schädlinge werden heutzutage mit dem Wort „Malware“ bezeichnet, was soviel bedeutet wie „boshafte Software“.

Trotz all dieser Mischformen kann man die Schädlinge in verschiedene Kategorien einordnen und ihnen typische Funktions- und Verhaltensweisen zuordnen. Im Folgenden werden diese näher beschrieben.

1.1 Computerviren

Computerviren verbreiten sich passiv, d.h. sie haben keine eigenen Funktionen, um sich zu verbreiten. Auf andere Systeme kann das Virus gelangen, wenn z.B. infizierte Programme per Diskette oder Netzwerk auf das neue System kopiert werden. Genau wie das biologische Virus, braucht das Computervirus auch einen Wirt, um seine Schadensfunktion auszuführen, was typischerweise Computerprogramme sind. Die Reproduktion erfolgt, indem es sich in andere Computerprogramme einschleust und diese somit infiziert. Wird ein infiziertes Computerprogramm aufgerufen, wird das Virus mit ausgeführt und kann somit seine Schadensfunktion verrichten und andere noch nicht infizierte Programme infizieren. Die Schadensfunktion kann von harmlosen Störungen bis hin zu Datenverlust oder sogar beschädigter Hardware führen.

Um von Virus-Such-Programmen (Virenscannern) möglichst unentdeckt zu bleiben, versuchen Viren möglichst nicht aufzufallen. Dazu verwenden sie verschiedene Techniken, wie z.B. Verschlüsselung oder Tarnung, und verschiedene Infektionsarten.

Die Funktionsweisen und Eigenschaften unterschiedlicher Virenarten werden im Folgenden verdeutlicht.

1.1.a Bootviren

Wie der Name schon sagt, werden Bootviren beim Starten des PCs (Bootvorgang) geladen. Sie zählen zu den ältesten Arten von Viren und waren bis 1995 eine sehr verbreitete Art von Viren. Bootviren infizieren Bootsektoren von Festplatten oder Disketten oder den Master Boot Record (MBR) einer Festplatte. Bootsektoren und der MBR sind spezielle Bereiche auf Datenträgern, welche physikalisch direkt am Anfang des Datenträgers bzw. der Partition liegen. Sie werden direkt nach dem Start des PCs ausgeführt und enthalten meist einen sogenannten Boot-Loader, der die Aufgabe hat, ein installiertes Betriebssystem zu starten. D.h. Boot-Loader werden gestartet bevor, das Betriebssystem startet. Für Bootviren sind diese Bereiche also sehr interessant. Legt man z.B. eine mit einem Bootvirus infizierte Diskette in den PC ein und bootet von dieser, kann der Bootvirus die Bootsektoren und den MBR der Festplatte befallen. Hat er das geschafft, wird er beim nächsten Start des PCs aktiviert und kann den Start des Betriebssystems verhindern oder manipulieren. Wenn der Bootvirus das Betriebssystem startet, aber selbst noch im Hintergrund aktiv ist, kann er z.B. beim Einlegen einer Diskette in den PC, diese infizieren und sich somit vermehren. Der Benutzer merkt in der Regel nichts

davon. Gibt er diese Diskette nun an andere Personen weiter, welche diese in ihren PC einlegen, kann der Bootvirus dort weiter Schaden anrichten.

Aus technischen Gründen, müssen Bootviren mit sehr wenig Speicherplatz auskommen, da ein Bootsektor nur sehr wenig davon besitzt (444 Bytes). Dies hat zur Folge, dass die Programmierer solcher Viren sehr professionell vorgehen müssen, um möglichst viele Funktionen in den Virus zu „packen“.

Im Jahre 2005 kam eine spezielle Art von Bootviren hinzu, und zwar solche, die CD-ROM-Abbilddateien (ISO-Images) infizieren können. Brennt man diese infizierten Abbilder auf CD, und bootet von diesen, verrichtet der Bootvirus seine üblichen Funktionen.

Heute bieten Betriebssysteme und das BIOS des Computers einen guten Schutz, um Bootvirus-Infektionen zu verhindern. Es gibt zwar Bootviren, die dies umgehen können, doch die Verbreitung ist trotzdem sehr schwer, sodass Bootviren heutzutage fast „ausgestorben“ sind.

1.1.b Dateiviren und Linkviren

Diese Arten von Viren sind die am häufigsten anzutreffenden. Sie infizieren Programme und Programm-Bibliotheken.

Die Infektion erfolgt meist durch das Anhängen des Virus an ein Programm und die Manipulation der Startroutine des Programms, sodass direkt nach dem Ausführen des Programms zum schädlichen Code des Virus gesprungen wird. Nach Aufruf des infizierten Programms und dem Ablauf der Schadensfunktion des Virus, lassen diese Viren meist das Programm normal weiterlaufen, um möglichst lange unentdeckt zu bleiben. Spezielle Formen von Linkviren infizieren sogar bestimmte Programmfunktionen, welche erst ausgeführt werden, wenn das Wirtsprogramm darauf zugreift.

Eine andere Form der Verbreitung ist das komplette ersetzen einer Programmdatei durch die Programmdatei des Virus. Diese Viren zu erkennen ist für Virenscanner kein Problem, da das Virus in seiner reinen Form vorliegt und nicht an eine Programmdatei angehängt wurde.

1.1.c Makroviren

Makros werden in vielen Anwendungen unterstützt, vor allem in Büro-Anwendungen wie Microsoft Office oder OpenOffice, aber auch in vielen anderen Anwendungen. Sie können vom Benutzer erstellt

werden. um bestimmte Abläufe und wiederkehrende Aufgaben in Dokumenten zu automatisieren. Diese Makros werden mit im Dokument abgespeichert. In manchen Anwendungen gibt es Makros, die automatisch beim Öffnen des Dokuments ausgeführt werden können, was für Makroviren natürlich sehr zuvorkommend ist. Somit können sie sich allein beim Öffnen eines Dokuments aktivieren, ihre schädliche Funktion ausführen und sich weiter vermehren. Neben Programmdateien können sie zusätzlich noch nicht infizierte Dokumente befallen, indem sie ihren eigenen Makrovirus-Code dort hinein schreiben.

Makroviren waren um das Jahr 2000 herum die meist verbreitete Form von Viren, da den meisten Benutzern von den Büro-Anwendungen nicht bewusst war, dass Text-Dokumente auch Viren enthalten können.

1.1.d Skriptviren

Ein Skript ist eine Text-Datei, welche Code einer interpretierten Programmier-Sprache (= Skriptsprache) enthält. Dieser Code wird erst nach dem Starten des Skripts in eine interne Repräsentation (Maschinencode) umgewandelt und dann ausgeführt, was ein passender Interpreter erledigt.

In Java Script und Visual Basic Script geschriebene Skripte lassen sich auch problemlos in Internetseiten (= HTML-Seiten) einbetten, da diese einen speziellen Skript-Bereich haben, welcher vom Internet-Browser geladen und ausgeführt wird. Ein Skriptvirus nutzt Sicherheitslücken mit Hilfe der Skriptsprache aus und infiziert, wie alle anderen Viren auch, Dateien und führt schädlichen Code aus. Skriptviren auf Internetseiten finden rasche Verbreitung, da ein Benutzer die infizierte Internetseite nur besuchen muss, um sich das Skriptvirus „einzufangen“.

1.1.e Mischformen

Man kann Computerviren nicht alle in bestimmte Kategorien einordnen, da es auch Kombinationen von verschiedenen Virentypen gibt, wie z.B. Viren, die Bootsektoren und Dateien infizieren oder Skript- und Makroviren, die ausführbare Programmdateien infizieren. Fast alle möglichen Kombinationen sind denkbar.

1.2 Würmer

Der wesentliche Unterschied zwischen Viren und Würmern besteht darin, dass Würmer sich aktiv um ihre Verbreitung bemühen, wobei Viren passiv darauf warten weitergegeben zu werden. Da die Rechnervernetzung heutzutage drastisch zugenommen hat, verbreiten sich Würmer hauptsächlich darüber, vor allem über das Internet, und infizieren andrere PCs. Die Verbreitung erfolgt z.B. über das Versenden infizierter E-Mails, über Instant-Messaging-Programme, Dateifreigaben oder Tauschbörsen (Peer-to-Peer Netzwerke), aber auch über Sicherheitslücken in verschiedenen Diensten, die auf dem PC laufen.

Die häufigste Verbreitungsmethode ist via E-Mail, wobei der Wurm sich selbst an möglichst viele Empfänger versendet und meist Schaden am System verursacht, was aber nicht unbedingt immer so ist. Bekanntester Wurm dafür ist der „I-love-you-Virus“, welcher fälschlicherweise als Virus bezeichnet wird und sich im Jahr 2000 stark verbreitete. Allein durch ihre Verbreitung können Würmer durch die daraus entstehende Belastung der Netze erheblichen wirtschaftlichen Schaden verursachen.

Würmer können aber, wie Viren auch, in Programmdateien versteckt sein. Ein Wurm bestehend aus einer Kombination von Verbreitungsmethoden und hat größere Chancen sich zu verbreiten.

1.3 Trojanische Pferde

Trojanische Pferde, auch „Trojaner“ genannt, sind Computerprogramme, die eine nützliche Funktion (z.B. Bildschirmschoner, Spiel) vortäuschen, aber im Hintergrund, ohne Wissen des Anwenders, ganz andere Funktionen verrichten. Das muss nicht heißen, dass diese Funktionen dem System Schaden zufügen, jedoch ist dies sehr oft der Fall. Trojaner werden oft dazu benutzt, andere Schadensprogramme in das System einzuschleusen, wie z.B. Viren, Würmer oder Spyware.

Es gibt verschiedene Arten von Trojanern. Die häufigsten sind Dropper (engl.: *to drop* „ ablegen“), welche ein anderes Programm, meist Malware, auf dem System installieren. Nach dem Beenden und ggf. Löschen des Trojaners, bleibt die Malware allerdings im System vorhanden und verrichtet weiter ihre Schadensfunktion.

Seltener findet man Trojaner, die selbst versteckte Funktionen enthalten. Ein Beispiel hierfür sind Plug-Ins. Diese Trojaner bestehen aus einem einzigen Programm. Nach dem Löschen des Trojaners stehen auch keine geheimen Funktionen mehr zur Verfügung.

Öfter findet man auch Trojaner, die aus einer Kombination von 2 unabhängigen Programmen bestehen. Dabei werden 2 Programmdateien zu einer zusammengeführt und beim Start beide geladen. Dabei wird typischerweise Malware an ein „normales“ Programm angehängt.

1.4 Spyware

Als Spyware werden Computerprogramme bezeichnet, die ohne Wissen des Anwenders persönliche Daten ausspionieren und über das Internet an Dritte weitergeben, meistens an den Hersteller der Software. Der Hersteller erhofft sich daraus, anhand der gesammelten Daten, dem Benutzer gezielt Werbebanner einzublenden mit Werbung, die ihn interessieren könnte.

Spyware läuft so gut wie immer im Hintergrund und nistet sich sehr tief ins System ein. Für die Entwicklung von Spyware wird sehr viel Geld investiert, was sich damit bezahlt macht, dass sie technisch auf einem sehr hohen Niveau ist. Es sind sehr viele Maßnahmen enthalten, die das Löschen und Beenden der Spyware verhindern sollen wie z.B. das gleichzeitige Laufen mehrere Prozesse, die sich gegenseitig neu starten, falls einer beendet wird oder das Entziehen der Berechtigung zum Löschen der Spyware von der Festplatte.

1.5 Adware

Als Adware bezeichnet man Software, die auf ihrer Bedienoberfläche Werbung anzeigt. Solche Software ist meist kostenlos und wird durch diese Werbung finanziert. Die Werbung besteht häufig aus Werbebannern, welche dynamisch über das Internet nachgeladen werden und in bestimmten Zeitabständen wechselt.

Strittig ist allerdings, ob es sich bei Adware auch um Spyware handelt, da allein anhand der Verbindungsdaten Rückschlüsse auf das Nutzungsverhalten getroffen werden können.

1.6 Dialer

Dialer (deutsch: Einwahlprogramme) sind Programme, die sich über das analoge Telefonnetz bzw. ISDN-Netz ins Internet einwählen. Betriebssysteme bringen standardmäßig solche Programme mit und einige Anbieter von Internet Services liefern ihre eigenen aus.

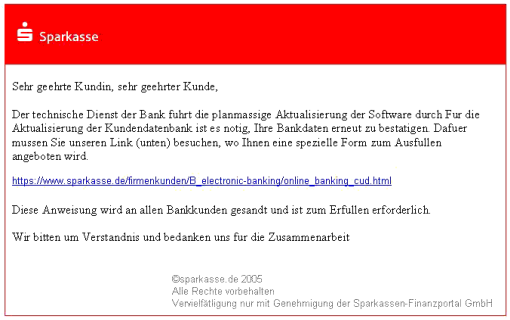
Der Begriff Dialer bezeichnet heute allerdings unerwünschte Programme, die sich im Hintergrund automatisch und ohne Wissen des Anwenders mit teuren Rufnummern verbinden. So entstehen sehr hohe Kosten, da die angewählten Nummern meist sehr hohe Tarife und Einwahlgebühren haben. Der Anbieter, der angewählt wurde verdient an den fälligen Onlinekosten, womit der Sinn von Dialern klar auf der Hand liegt.

Durch den verstärkten Ausbau von Breitbandnetzen wie DSL und das ständige sinken der Kosten für Breitband-Internet-Tarife, gewinnen die Anbieter immer mehr Kunden. Da Breitbandverbindungen keine Einwahlverbindungen sind, haben Dialer hier keine Chance. Und mit der raschen Verbreitung von Breitbanddiensten, sterben Dialer langsam aus.

1.7 Phishing

Phishing (von engl. fishing „fischen“) ist eine Trickbetrugsmethode, um persönliche und vertrauliche Daten vom Anwender zu erlangen.

Dabei wird mit Hilfe von E-Mails versucht, den Anwender auf gefälschte Internetseiten zu locken, sodass er dort seine vertraulichen Zugangsdaten und Passwörter preisgibt. In den meisten Fällen bezieht sich dies auf Online-Banking.


Sparkasse

Sehr geehrte Kundin, sehr geehrter Kunde,

Der technische Dienst der Bank führt die planmassige Aktualisierung der Software durch Fur die Aktualisierung der Kundendatenbank ist es notig, Ihre Bankdaten erneut zu bestatigen. Dafuer mussen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfullen angeboten wird.

https://www.sparkasse.de/firmenkunden/B_electronic-banking/online_banking_cud.html

Diese Anweisung wird an allen Bankkunden gesandt und ist zum Erfullen erforderlich.

Wir bitten um Verstandnis und bedanken uns fur die Zusammenarbeit

©sparkasse.de 2005
Alle Rechte vorbehalten
Vervielfältigung nur mit Genehmigung der Sparkassen-Finanzportal GmbH

Abbildung 1: Phishing-Mail Sparkasse

Die E-Mails, die ein Anwender in seinem Postfach hat, erwecken den Eindruck von offiziellen Schreiben versehen mit einer Bitte, die den Anwender auffordert seine Zugangsdaten zu bestätigen (siehe *Abbildung 1*). Klickt der Anwender nun auf den in der E-Mail hinterlegten Link, gelangt er auf eine Internetseite, die exakt so aussieht wie das Original. Der Anwender merkt in den meisten Fällen aber nicht, dass er auf einer ganz anderen Seite gelandet ist und tippt seine Zugangsdaten und Passwörter ein. Diese gelangen nun ohne das Wissen des Anwenders an die Trickbetrüger, welche sich

nun mit geklauter Identität bei der „richtigen“ Seite anmelden können. Wenn es sich um Betrug mit Online-Banking handelt, können die Trickbetrüger nun z.B. Geld aufs eigene Konto überweisen.

1.8 Sniffing

Unter Sniffing (engl.: schnüffeln) versteht man das Abhören des Datenverkehrs in einem Netzwerk. Dabei werden Daten, die zu und von anderen Rechnern im Netzwerk gesendet werden, von Dritten (z.B. einem Hacker) mitgelesen. Somit ist es möglich, dass sensible Daten, wie z.B. der Benutzername und das Passwort für einen Online-Shop oder die Kontonummer und das dazugehörige Zugangspasswort fürs Online-Banking, von fremden Personen eingesehen werden können.

Betrachtet man Sniffing etwas technischer, spricht man auch von Packet-Sniffing, da einzelne Datenpakete mitgelesen werden. In Netzwerken, die die Ethernet-Technologie einsetzen, wird die sogenannte Broadcast-Technik eingesetzt. Bei dieser Technik wird ein Paket, das für einen Rechner bestimmt ist, an alle Rechner im Netzwerk ausgesandt. Läuft auf einem Rechner nun ein Sniffing-Programm (z.B. „SNOOP“), ist dieser in der Lage den Datenverkehr mitzuhören.

1.9 Rootkits

Der Name „Rootkit“ stammt von Unix-basierten Betriebssystemen. Dort kennzeichnet der Benutzer „root“ den Systemadministrator, der uneingeschränkten Zugriff auf einem PC besitzt. „Rootkit“ bedeutet soviel wie „Administratorausrüstung“.

Ein Rootkit kommt nach erfolgreichem Eindringen in einen fremden PC zum Einsatz. Dabei wird es im fremden Rechner ohne Wissen des Anwenders installiert. Wie der Name schon sagt, können Dritte somit auf dem kompromittierten System Administratorrechte erlangen und haben somit vollen Zugriff auf den PC. Das heißt, ein Rootkit kann z.B. einem Eindringling vereinfacht Zugriff von außerhalb gewähren (Hintertür), Prozesse verstecken, Software installieren oder Dateien verstecken. Von den ganzen Aktivitäten bekommt der Anwender nichts mit. Häufig ist der Sinn und Zweck eines Rootkits das Verstecken von Malware, das Mitlesen von Tastatureingaben, das Kopieren des Bildschirminhalts (Screenshot) oder das „Mithören“ des Netzwerkverkehr mittels eines Sniffers (siehe Kapitel 1.8).

Es gibt verschiedene Arten von Rootkits. Die ersten waren Application-Rootkits und waren modifizierte Versionen von Systemprogrammen. Die Modifikationen verstecken dabei die Aktivitäten des Eindringlings, sodass der eigentliche Systemadministrator keinen Verdacht auf fremde Aktivitäten schöpfen konnte. Diese Art von Rootkits gibt es heute kaum noch, da sie von Virenscannern mit sehr einfachen Techniken als solche erkannt werden können. Heutzutage treten eher Kernel-Rootkits und Userland-Rootkits auf.

Kernel-Rootkits ersetzen dabei grundlegende Teile vom Betriebssystem-Kern (Kernel) mit ihren eigenen, um so getarnt zu agieren und dem Angreifer zusätzliche Funktionen zur Verfügung zu stellen. Meist werden dazu Kernel-Module bei Bedarf nachgeladen, ohne dass der Benutzer etwas davon merkt. Andere Arten von Kernel-Rootkits kommen ohne das Nachladen von Modulen aus, indem sie direkt den Bereich im Arbeitsspeicher manipulieren, in dem der Kernel liegt.

Userland-Rootkits funktionieren gänzlich ohne das Manipulieren des Kernels aus. Sie sind unter dem Betriebssystem Windows sehr verbreitet und können sich direkt in Prozesse einklinken und diese manipulieren. Die Manipulation erfolgt dadurch, dass Funktionsaufrufe des Betriebssystems auf das Rootkit umgeleitet werden und es somit diese Funktionen verändern und die Daten mitlesen kann.

Neuerdings, seit Beginn des 2. Quartals 2006, gibt es noch eine andere Art von Rootkits, die so genannten „Virtual Machine Based Rootkits“ (VMBR).

Diese Rootkits lassen das eigentliche Betriebssystem in einer Virtuellen Machine laufen. Das bedeutet das eigentliche Betriebssystem läuft in einer vom Rootkit vorgegaukelten Umgebung, welche einen normalen PC simuliert. Da das Rootkit sozusagen über dem Betriebssystem läuft, hat das Rootkit Zugriff auf alles, was darunter läuft, d.h. auf alles, was mit dem Betriebssystem, darunter installierten Programmen, Daten und Hardware zu tun hat.

Es gibt gängige Methoden, mit denen ein Programm feststellen kann, ob es in einer virtuellen Umgebung läuft, doch dies wurde auch schon umgangen.

1.10 Hacker

„Ein Hacker ist […] ein überaus talentierter Computer-Spezialist, der insbesondere Sicherheitsbarrieren überwinden und in fremde Systeme eindringen kann.“ [COBA06]

Hacker haben das nötige Know-How und das nötige Werkzeug, um in fremde Systeme eindringen zu können, was natürlich nicht immer leicht fällt bzw. nicht selten auch misslingt. Typische Software-Werkzeuge (Tools) von Hackern sind Portscanner, Sniffer, Rootkits und viele andere. Hat ein Hacker es geschafft in ein System einzudringen, setzt er meist ein Rootkit ein, um sich auch in Zukunft leichter Zugriff zu dem System verschaffen zu können. Hacker verschaffen sich jedoch selten ohne Grund Zugriff zu einem System, gewöhnlich nur dann, wenn es für sie von hoher Priorität ist oder sie einen Auftrag bekommen haben. Deshalb ist es auch unwahrscheinlich, dass Privat-Anwender von einem Hacker-Angriff betroffen sind, was aber nicht auszuschließen ist.

2 Abwehr

2.1 Firewall

Der Begriff Firewall, welcher im Deutschen soviel bedeutet wie Brandschutzmauer, schützt vor unbefugten Zugriffen aus dem Internet durch fremde Benutzer oder schädliche Programme wie z.B. Trojaner oder Dialer. Ob man nun mit dem Browser auf den Lieblings-Webseiten unterwegs ist, E-Mails versendet/empfängt oder über ein Messaging-Programm mit Freunden Neuigkeiten austauscht: in all diesen Fällen können Gefahren entstehen, da der Computer mit anderen Systemen im Internet kommuniziert und einen Informationsaustausch über so genannte Ports abwickelt.

Da das Internet eine ganze Reihe unterschiedlicher Dienste anbietet, gibt es tausende solcher Kommunikationsports. Das Problem ist im Grunde recht einfach. Über diese Ports können andere Computer direkten Kontakt mit Ihrem PC aufnehmen, ohne dass eine Prüfung stattfindet, ob es sich hierbei um einen erwünschten Informationsaustausch handelt, beispielsweise der Inhalt einer Webseite, die gerade aufgerufen wurde, oder aber einen ungebetenen Gast, der gerade versucht einen Wurm oder ein Backdoor-Programm („Hintertür“) ins System einzuschleusen.

Um diese Prüfung vorzunehmen, kommt nun eine Firewall ins Spiel. Sie überprüft sowohl die ausgehenden Zugriffe auf verschiedene Server im Internet als auch die eingehenden Verbindungen von einem im Netz befindlichen System und fungiert somit wie ein Türsteher für den PC, der ungebetene Gäste einfach draußen stehen lässt.

Handelt es sich um Daten, die ausdrücklich vom Anwender angefordert wurden, öffnet die Firewall die zugehörigen Ports, sodass ihr PC mit der betreffenden Gegenstelle im Internet Informationen austauschen kann. Alle anderen Ports aber werden von der Firewall verschlossen. Angreifer haben es somit wesentlich schwieriger, die Existenz des Computers im Internet ausfindig zu machen.

Firewalls gibt es in verschiedenen Arten und von unterschiedlichen Anbietern. So ist es gar möglich, dass bei der Verbindung ins Internet über einen Router, dieser schon einen Großteil der Sicherheitsrisiken abfängt (Hardware-Firewall). Im Bereich der Softwarelösungen gibt es eine Menge an Firewalls, die für privaten Einsatz kostenlos im Internet zum Herunterladen angeboten werden und welche zusätzlich zu einer Hardware-Firewall schützen kann. Oft werden solche Programme als „Personal Firewall“ betitelt, da sie für die Eigenanwendung am Heimcomputer bestimmt sind.

Anbieter von Personal Firewalls sind unter anderem Agnitum, Sygate und Zone Labs. Im Zuge der Popularität und aufgrund der zusätzlichen Sicherheit ist auch Microsoft auf die Idee gekommen und bietet seit dem Service Pack 2 unter Windows XP ebenfalls eine Firewall an, die so genannte Windows-Firewall.

Auf den Einsatz einer Firewall sollte also in keinem Fall verzichtet werden, wenn man im Internet unterwegs ist, denn mitunter vergehen nur wenige Minuten, bis der Computer von einem Wurm, Virus oder anderen Schädling angegriffen und infiziert wird. Selbst, wenn der Router mit einer Firewall versehen ist, sollte man auf jeden Fall den eigenen PC mit einer Personal-Firewall absichern. Nimmt man beispielsweise das Notebook ab und an mit in ein Internet-Café, ist es nun auch außerhalb des heimischen Netzwerks mit dem Firewallschutz versehen.

2.1.a ZoneAlarm

Eine der beliebtesten Personal-Firewalls ist ZoneAlarm von der Firma Zone Labs. Sie ist in einer deutschsprachigen Version unter www.zonelabs.com für den privaten Anwender und gemeinnützige Einrichtungen kostenlos zu beziehen. ZoneAlarm ist erhältlich für die gängigsten Betriebssysteme der Windows-Familie und bietet einen optimalen Schutz des PCs, da sie alle aktuellen Protokolle und Einstellungen von E-Mail-Server, Web-Browser und Messaging Programmen unterstützt. Des Weiteren ist die Installation und Konfiguration wegen eines Assistenten („Wizard“), der aufeinander folgende Dialoge anzeigt, für jeden Leihen durchführbar.

Abbildung 2: ZoneAlarm Personal Firewall

Bei jeder Anfrage ins Internet, wird man durch ein Fenster in der Startleiste („Popup“) aufgefordert, die Informationsanfrage zu bestätigen, um der Firewall mitzuteilen, dass es sich hierbei um einen gewollten Zugriff handelt. Diese Bestätigung kann dann auch für das jeweilige Programm, das mit dem Internet kommuniziert durch einen Klick gespeichert werden, sodass es ihm immer gestattet ist, Informationen auszutauschen und sie es nicht bei jeder Anwendung erneut absichern müssen. Nach dem gleichen Prinzip funktioniert ein Zugriff aus dem Internet auf ihren PC. Wiederum wird man

durch ein Popup in Kenntnis gesetzt, von wo jemand auf den Computer zugreifen will und es bedarf allein der Entscheidung des Anwenders dem zuzustimmen oder abzulehnen. Somit hat man immer einen Überblick, wann der Computer mit anderen Systemen kommunizieren möchte und man überlässt diese nicht einfach dem Rechner oder anderen Personen, welche es auf diesen abgesehen haben.

2.2 Anti-Virus

Um Dateien und Dokumente zu schützen, sollte auf den Einsatz einer Anti-Virus-Software unter keinen Umständen verzichtet werden. Denn Computerviren, Trojaner, Würmer etc. sind heimtückische Programme, die den PC und darauf gespeicherte Daten manipulieren, ausspähen oder sogar löschen können. Wie bei den Personal Firewalls gibt es auch im Bereich der Virenerkennung und -beseitigung zahlreiche Programme, die für private Anwender kostenlos zur Verfügung gestellt werden.

Moderne Anti-Viren Programme bieten einen so genannten Anti-Virus-Guard (*Abbildung 3*), meist auch Wächter oder Autoprotect genannt, an. Dieser wird automatisch bei jedem Start des Betriebssystems geladen und sucht im Hintergrund in größeren Abständen die Festplatte auf Virenbefall ab („scannen“).

Abbildung 3: AntiVir Guard

Natürlich ist es auch möglich Suchroutinen eigenhändig einzustellen und dem Programm somit mitzuteilen, dass es beispielsweise ihre kompletten Festplatten und Speicher im System durchsucht, um einen Virenbefall von bereits vor dem Einsatz der Anti-Virus-Software vorhandenen Dateien auszuschließen.

Aber eine Anti-Virus-Software arbeitet nur dann richtig, wenn sie in regelmäßigen Abständen auf den neusten Stand gebracht wird. Dieses kann man manuell tun oder so einstellen, dass sich das Programm selbständig die neusten Informationen von Viren über das Internet holt. Da es fast täglich neue Virendefinitionsdateien gibt, welche Auskunft über die Typen der verschiedenen Viren geben und es dem Programm überhaupt erst ermöglichen neuere Viren zu identifizieren, sollte man darauf achten, dass diese Dateien immer aktuell gehalten werden.

Eine absolute Sicherheit ist jedoch nie gegeben, da Viren oder ähnliche Schädlinge sich durchaus auf einem neueren Stand befinden können als die Anti-Virus-Software.

Abbildung 4: AntiVir - Status des letzten Updates

Ein bekanntes und häufig genutztes Programm ist AntiVir PersonalEdition Classic der Firma Avira, welches für den privaten und nicht-kommerziellen Einsatz kostenlos von der Seite www.free-av.de herunter geladen werden kann. Auch hier ist die Installation ohne Probleme auch von Anfängern durchführbar und der mitgelieferte AntiVir Guard integriert sich selbstständig ins System und nimmt sofort seine Arbeit auf. AntiVir besitzt neben der wichtigsten Funktion, dem Scannen nach Viren, auch eine ausführlich Berichterstattung von infizierten Dateien und durchgeführten Updates.

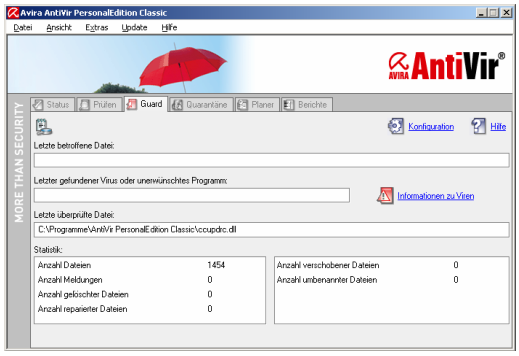


Abbildung 5: AntiVir - Oberfläche

Mit Hilfe des Planers kann man eigene Suchroutinen erstellen mit verschiedenen Eigenschaften wie beispielsweise auf welchen Datenträgern nach Schädlingen gesucht werden soll, an welchem Tag, um welche Uhrzeit oder gar regelmäßig in verschiedenen Intervallen. In einer Quarantäneliste werden infizierte Dateien aufgeführt oder können auch selbst hinzugefügt werden. Diese Dateien sind somit „aus dem Verkehr“ gezogen und können ggf. wiederhergestellt werden oder für immer von der Platte entfernt werden.

Die Firma Avira ist im Rahmen ihrer Anti-Virus-Software sehr bemüht, diese auf dem neusten Stand zu halten und stellt täglich neue Updates der Virendefinitionsdateien zur Verfügung, die in der Regel automatisch von AntiVir erfasst und aktualisiert werden.

Andere Anbieter von vergleichbaren Programmen sind u.a. F-secure, Kaspersky, McAfee Security, Symantec oder Trend Micro.

2.3 Anti-Spyware

Unter dem Begriff Spyware werden Programme definiert, die ohne Einverständnis und Wissen des Benutzers Aktionen wie Anzeigen von Werbefenstern, eine Dialerinstallation oder die Erfassung von Nutzungsgewohnheiten durchführen. Auch Browsereinstellungen („Cookies“) für bestimmte Webseiten, welche unter Umständen wichtige Passwörter und persönliche Daten enthalten, können von Spywareprogrammen ohne jeglichen Einfluss an Internetadressen im Netz versendet werden. Dadurch ist die Sicherheit und Privatsphäre in der heutigen Onlinewelt nicht mehr gewährleistet und sollte durch den Einsatz einer Anti-Spyware-Software sichergestellt werden. Auch hier gibt es

Anbieter, die ihre Software für den privaten Gebrauch ohne Entgelt für den Anwender bereitstellen. Die bekanntesten Programme dürften wohl Ad-Aware SE Personal von Lavasoft, Spybot Search & Destroy oder xp-AntiSpy sein.

Der Funktionsumfang einer solchen Software, bezogen auf Ad-Aware und Spybot, unterscheidet sich kaum von einer aktuellen Anti-Virus-Software. Auch diese Anti-Spyware-Programme durchsuchen die Festplatte und Speicher nach Spionageprogrammen und sind in der Lage diese zu entfernen. Zusätzlich wird die Registrierungsdatei von Windows durchsucht, welche sämtliche Einstellungen und Ladevorgänge des Systems beinhaltet, wodurch es schädlichen Programmen ohne Probleme ermöglicht wird, sich bei jedem Start des Betriebssystems selbstständig in den Speicher zu laden. Überprüft werden auch die aktuell ausgeführten Prozesse und es wird verifiziert, ob es sich hierbei um eine vom System notwendige Komponente handelt oder sich ein Spionageprogramm schon den Weg in den Computer erarbeitet hat.

Auch hier kommt man um einen ständig aktuellen Stand der Software nicht herum, da Entwickler von Spionageprogrammen sich immer neue Sicherheitslücken zu Eigen machen, wodurch sie ins System gelangen können. Damit ist eine Anti-Spyware-Software in der Lage, auch die neuesten Spionagetools zu erkennen und zu entfernen bzw. zu blockieren.

2.3.a Ad-Aware

Das weit verbreitete Anti-Spyware-Programm Ad-Aware SE Personal von Lavasoft kann von der Webseite www.lavasoft.de bezogen werden und beinhaltet umfangreiche Funktionen für die wirkungsvolle Beseitigung von Spionagesoftware auf ihrem Rechner. Wie bei AntiVir kann auch hier eine geeignete Suchroutine spezifiziert werden. Die gefundenen Schädlinge können dann in Quarantäne geschickt oder gelöscht werden, so dass sie keinen Schaden mehr anrichten können.

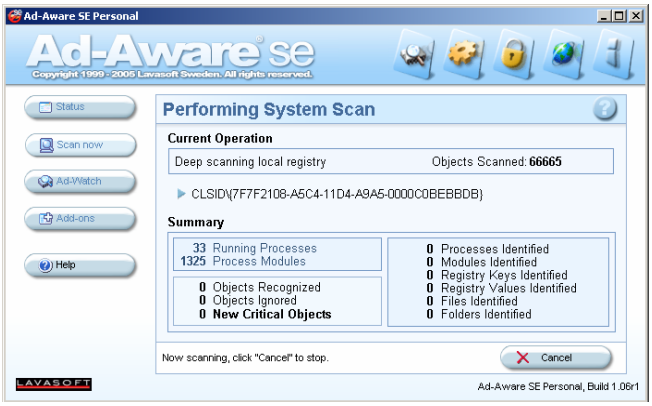


Abbildung 6: Ad-Aware - Oberfläche

Bei Bedarf können (scheinbare) Schädlinge auch wieder aus der Quarantäne zurückgeholt werden. Dies kann beispielsweise dann nötig werden, wenn plötzlich eine Funktion nicht mehr wie vorher funktioniert, weil ein dafür notwendiges und unschädliches Cookie in Quarantäne geschickt wurde.

2.3.b Spybot – Search & Destroy

Genau wie Ad-Aware ist Spybot auch ein Anti-Spyware-Programm und dient der Suche und Vernichtung von Spyware und Dialern. Das Programm ist einfach zu handhaben, da es zum größten Teil selbsterklärend ist. Sollten weitere Fragen bei der Nutzung entstehen kann man auf eine ausführliche Hilfefunktion zurückgreifen.

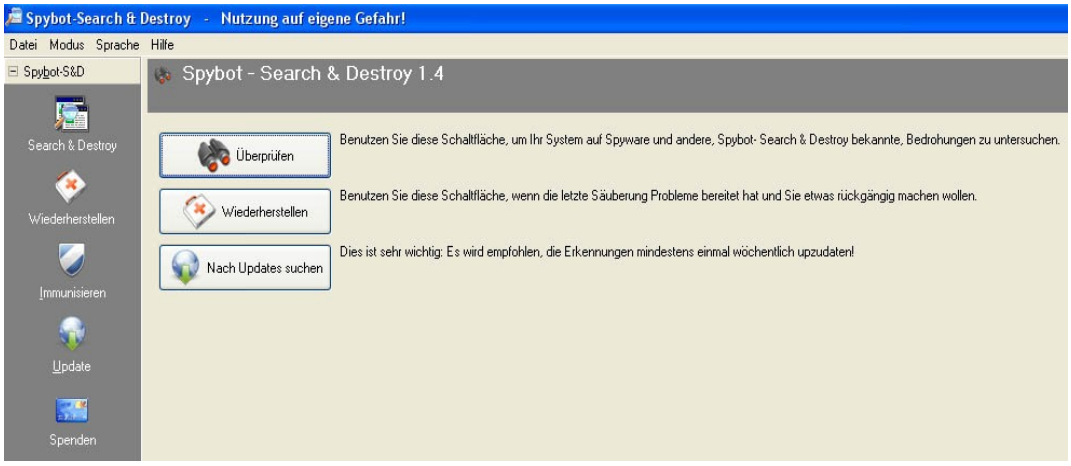


Abbildung 7: Spybot – Programmoberfläche

In *Abbildung 7* sieht man das Hauptmenü des Programms. Von dort aus hat man Zugriff auf alle wichtigen Funktionen, unter anderem hat man hier die Möglichkeit, das System zu immunisieren (siehe *Abbildung 8*), d.h. sich vor allen schon bekannten Bedrohungen automatisch zu schützen. Ebenfalls verfügt Spybot über eine Aktualisierungsfunktion, die dabei hilft, das Programm immer auf dem neuesten Stand zu halten. Ähnlich wie das Anti-Virus-Programm von Symantec läuft auch Spybot im Hintergrund und überwacht das System.

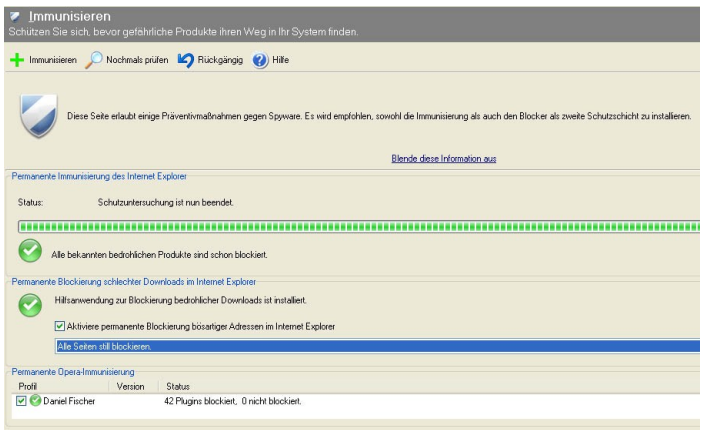


Abbildung 8: Spybot - Immunisieren

2.3.c xp-AntiSpy

xp-AntiSpy unterscheidet sich von anderen Anti-Spyware-Programmen darin, dass es dem Benutzer erlaubt, komplizierte Sicherheitseinstellungen betreffend des Betriebssystems einstellen zu lassen.

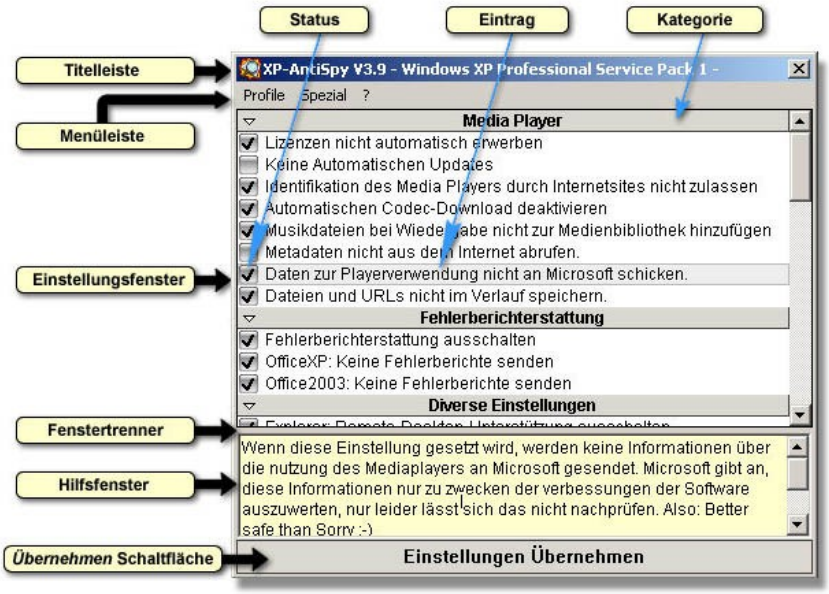


Abbildung 9: xp-AntiSpy - Beschreibung der Oberfläche (Quelle: Hilfedatei von xp-AntiSpy)

Nach erfolgter Einstellung sieht das Programm dann ungefähr so aus wie in *Abbildung 10* dargestellt.

Die grünen Felder weisen darauf hin, dass die Einstellungen den Empfehlungen entsprechen. Das rote Feld zeigt eine Einstellung, die zwar den Empfehlungen entspricht, jedoch nicht aktiviert ist.

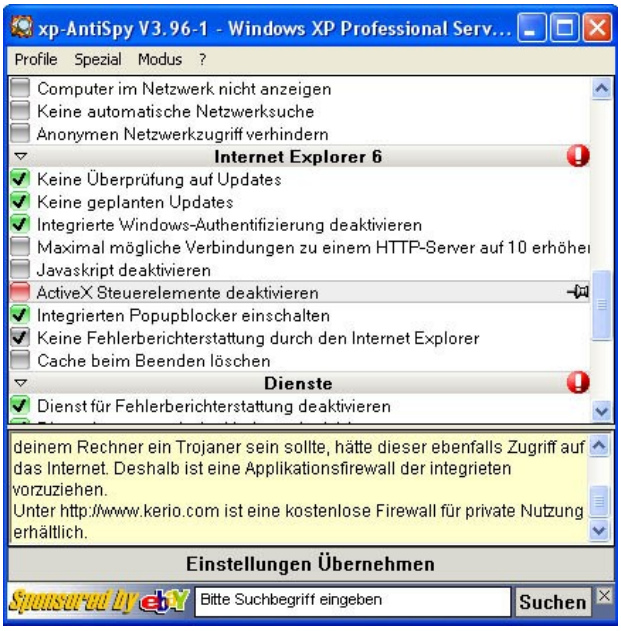


Abbildung 10: xp-AntiSpy (Quelle: Screenshot, eigenes System)

2.4 Security Suites

Aufgrund der fortbestehenden Gefahren und Angriffen aus dem Internet hat sich auch für den kommerziellen Markt eine wahre Lücke ergeben. Viele Firmen bieten so genannte Security Suites an, welche sowohl eine Firewall, ein Anti-Virus Programm als auch einen geeigneten Spywareschutz in einem Paket anbieten. Diese Suites sind aber zum größten Teil kostenpflichtig und erfordern eine offizielle Lizenz der Entwickler. Auch der oben genannte Anbieter Zone Labs bietet in einem Paket seine beliebte Firewall zusammen mit Viren – und Spywareschutz gegen einen geringen Kostenbeitrag an und vereint somit alle wichtigen Funktionen die dem Anwender ausreichende Sicherheit beim Surfen im Netz gewährleistet. Auch der bekannte und erfahrene Softwareentwickler Symantec hat sich auf Sicherheit für Privatanwender und Industrie spezialisiert und bietet mit seiner Norton Internet Security einen umfangreichen Schutz gegen Schädlinge und Angreifer aus dem Internet an.

Diese Security Suites sind in erster Linie für Firmen interessant, die ihre Rechner schützen wollen, da alle kostenlosen Sicherheitsprogramme für den gewerblichen Gebrauch von den Herstellern nicht zulässig sind.

3 Schwachstellen und Empfehlungen

Gibt es den 100-prozentig sicheren PC? Diese Frage kann man ganz klar mit „Nein“ beantworten, denn ein PC ist immer nur so sicher wie ihn der Benutzer oder der Administrator einrichtet und wie sicher die Software, bezogen auf Sicherheitslücken, ist. Man kann zwar versuchen im Internet so unauffällig wie möglich zu agieren, dennoch hinterlässt man überall Spuren.

An dieser Stelle werden einmal drei Beispiele aufgeführt, bei denen es zu teils massiven Schwachstellen und somit zu Problemen in der Sicherheit kommen kann.

Zum einen handelt es sich dabei ganz klar um Computer die öffentlich zugänglich sind und dann natürlich um den PC im eigenen Haushalt.

Ebenfalls werden hier zwei kleine Programme vorgestellt, die helfen können den Computer etwas sicherer zu machen.

3.1 Öffentliche PCs

3.1.a Internet-Café

Internet Cafés gibt es in fast jeder Stadt. Hierher kommen Menschen, die gegen eine Nutzungsgebühr auf der Suche nach Informationen im Internet sind, ihre E-Mails abrufen wollen oder einfach nur einen Breitbandanschluss (z.B. DSL) zum Surfen nutzen wollen. Durch die große Menge von Menschen, die hier täglich ein- und ausgehen, kommt es immer wieder zu Problemen, die die Sicherheit betreffen. Dabei kann es sich um Viren, Trojaner, Spyware oder ähnliche Programme handeln, die das Verhalten des PCs unerwünscht verändern können.

3.1.b Fachhochschulen und Universitäten

Auch hier gibt es eine große Anzahl von öffentlich zugänglichen PCs, die die Studenten nutzen können. Außerhalb der Lehrveranstaltung sind diese jedem Student zugänglich, der über einen so genannten Rechner-Account verfügt. Auch hier gilt: je größer die Anzahl der Benutzer an einem PC, umso größer auch die Wahrscheinlichkeit, dass es zu Problemen kommen kann, die die Sicherheit betreffen.

Doch woher kommt das? Ein Argument ist mit Sicherheit die Einstellung vieler PC-Nutzer zum Thema Sicherheit am PC. Oft werden Warnmeldungen betreffend der Firewall oder des Virenscanners einfach weggeklickt, ohne auch nur einmal einen genauen Blick auf die Warnung geworfen zu haben. Oder die Benutzer vergessen sich abzumelden und bieten somit dem nachfolgenden Nutzer die Möglichkeit wichtige oder relevante Daten zu verändern.

3.2 Private PCs

Heute findet man in fast jedem Haushalt einen PC. Ob er nun zur Textverarbeitung, zum Surfen, zum Musik hören oder zum Spielen genutzt wird, muss jeder für sich selbst entscheiden.

Doch auch hier lauern überall Gefahren. Die größte Gefahr für einen PC ist auch hier ganz klar der Benutzer selbst. Denn er entscheidet letztendlich welche Software wann installiert wird und welchen E-Mail-Anhang er speichert oder öffnet oder welche E-Mail er gleich löscht.

3.3 Empfehlungen

Was kann man also tun um seinen eigenen oder einen öffentlich zugänglichen PC sicherer zu machen? Da es, wie anfangs erwähnt, den 100-prozentigen Schutz nicht gibt, sollen hier einmal grundlegende Dinge aufgeführt werden.

Der wohl wichtigste Schritt ist es, eine Firewall zu verwenden um Zugriffe vom Internet auf den eigenen PC zu unterbinden. Für private Anwender gibt es so genannte „Personal Firewalls“. Diese kann man entweder kostenlos als Freeware herunterladen oder für wenig Geld als Softwarepaket kaufen. Der Vorteil hier ist, dass viele Anbieter wie z.B. Symantec Aktualisierungen ihrer Software (Updates) gratis anbieten.

Ebenfalls zu empfehlen ist die Verwendung eines Anti-Virus-Programms. Auch diese gibt es als Freeware zum herunterladen oder als Software zum Kaufen. Die Möglichkeit zum Aktualisieren besteht auch hier, was man auch regelmäßig tun sollte.

Wichtig ist es darauf zu achten, dass diese beiden Programme auch tatsächlich im Hintergrund laufen und nicht deaktiviert sind. Argumente wie „Deaktivieren spart Ressourcen“ sind hier unangebracht. Moderne PCs haben so viel Reserven, dass zwei Sicherheitsprogramme, die im Hintergrund laufen, überhaupt keine Rolle spielen und kaum Ressourcen verschwenden.

Hier sollten vor allem Administratoren genau darauf achten, dass dem Nutzer keine Möglichkeit geboten wird, diese Programme manuell zu deaktivieren oder zu umgehen.

Ebenfalls wichtig ist es darauf zu achten, dass bei der Verwendung von so genannten E-Mail-Clients die Option „automatisches speichern der Anhänge“ deaktiviert ist. So kann der Benutzer immer noch selbst entscheiden welchem Inhalt er vertraut und welchem nicht und die E-Mail eventuell auch gleich löschen.

Bei allen verwendeten Browsern sollte darauf geachtet werden, dass ActiveX- Steuerelemente deaktiviert sind.

Administratoren sollten nach Möglichkeit Buch führen, wann die letzte Datensicherung vorgenommen wurde oder wann beispielsweise der Virenscanner das letzte mal aktualisiert wurde.

Ein ganz wichtiger Punkt betrifft die Verwendung von mobilen Computern, den so genannten Notebooks. Diese Computer sollten mit speziellen Passwörtern versehen werden, damit bei Verlust des Computers die Daten nicht von anderen Personen eingesehen werden können.

Sollte man einen öffentlichen PC nutzen, sollte man daran denken, sich auf jeden Fall abzumelden, bevor man den Arbeitsplatz verlässt. Noch wichtiger ist dies nach dem Abrufen der E-Mails oder z.B. nach der Benutzung des eigenen eBay-Kontos.

Popups ignorieren! Popup kommt aus dem englischen und heißt soviel wie plötzliches auftauchen. Popups sind kleine Werbefenster die unangekündigt irgendwo auf dem Bildschirm auftauchen können. Diese sollte man in jedem Fall ignorieren, da sie oft auf Seiten mit verbotenem Inhalt führen oder andere negative Folgen mit sich führen. Auch wenn sie nur eine billige Form der Werbung sind, so haben diese Fenster schon bei einigen PC-Anwendern für Ärger gesorgt. Darum Popups einfach schließen und ignorieren.

Als Administrator sollte man auch darauf achten, dass keine fremde Software von außen installiert werden kann. Dies kann zum Beispiel durch eingeschränkte Nutzerrechte realisiert werden

Ebenfalls sollte man darauf achten, dass Wechsel-Medien wie CDs, DVDs oder einfache Speichersticks einer Prüfung des Virenscanners unterzogen werden, bevor diese genutzt werden können.

Man sollte in regelmäßigen Abständen eine Datensicherung vornehmen und alle Daten, die sich während der Nutzungsdauer des PCs angesammelt haben, auf externen Medien speichern. Zur

Datensicherung stehen auch spezielle Bandlaufwerke zur Verfügung. Diese bieten gewöhnlich ein großes Volumen, um eine Sicherung bequem durchführen zu können.

Wichtig hierbei ist, dass man die Daten fern vom eigenen PC bzw. von EDV-Anlagen lagert, für den Fall, dass es z.B. zu einem Brand im Haus oder im Büro kommt. Hierfür eignen sich besonders feuerfeste Tresore oder einfach ein Schließfach bei einer Bank.

Ein weitere Punkt ist das regelmäßige „Zwischenspeichern“. Dieser betrifft zwar nicht direkt die Sicherheit des PCs, kann aber helfen einigem Frust vorzubeugen. Dieser entsteht relativ schnell, nämlich genau dann, wenn der PC sich aus einem beliebigen Grund beispielsweise nicht mehr bedienen lässt. Viele sprechen hier vom „Aufhängen“. Meist kann dann nur noch mit dem Reset Knopf der Computer neu gestartet werden. Die ungespeicherten Daten gehen somit verloren.

Programme wie Microsoft Word oder StarOffice bieten einen Shortcut (eine Tastenkombination die einen Befehl ausführt) zum Speichern des Dokumentes an. Mit den Tasten STRG+S kann man zum Beispiel sofort speichern. Dies sollte man sich möglichst früh angewöhnen, um dem Verlust der Daten entgegen zu wirken.

Ebenfalls sollte man zu Beginn der Arbeit ein Verzeichnis anlegen und dem Projekt einen eindeutigen Namen geben. Das hilft auch später bei der Datensicherung.

4 Zusammenfassung

Wie man unschwer erkennen kann, ist das Spektrum an Gefahren für den PC heutzutage sehr breit. Die Auswirkungen eines Schädlingbefalls können verheerend sein und Datenverlust oder sogar Schäden an der Hardware des Computers verursachen. Viele Benutzer gehen mit dem Wissen über die Existenz dieser Gefahren viel zu leichtsinnig um oder sind sich nicht im Klaren darüber, wie ernst diese sind. Argumente wie „Warum sollte gerade ich mir einen Virus einfangen?“ oder „Ich will doch nur kurz meine E-Mails abrufen!“ bestätigen diesen Leichtsinn. Benutzer, die auf ihrem PC keine Firewall laufen haben, brauchen sich bloß ins Internet ein zu wählen und in der nächsten Sekunde könnte sich schon unbemerkt ein Schädlingsprogramm auf dem PC befinden.

Man kann Sicherheit am PC nicht allein durch „schützende“ Software erreichen, denn auch beim besten Anti-Virus-Programm beträgt die Viren-Erkennungsrate 99%. Der Benutzer ist also auch gefordert mit zu denken und auf zu passen, um Gefahren aus dem Weg zu gehen. Das ist zwar immer noch kein 100-prozentiger Schutz, denn Sicherheitslücken in Software sind nie auszuschließen, aber das Risiko eines Schädlingsbefalls wird stark verringert.

5 Anhang

5.1 Abbildungsverzeichnis

Michael Eckel
Daniel Fischer
Ralf Decher

5.2 Glossar

Adware
setzt sich aus dem englischen Wort „advertising“ (zu deutsch: „Werbung“) und dem Wort „Software“ zusammen und bezeichnet Computerprogramme, die Werbung (meist in Form von Bannern) in ihrer Bedienoberfläche anzeigen

Backdoor
zu deutsch: „Hintertür“

Bootvorgang, Booten
so wird der Startvorgang oder auch das „Hochfahren“ des PCs genannt

Ethernet
Netzwerk-Technologie, die heute sehr weit verbreitet ist

Hacker
„Ein Hacker ist […] ein überaus talentierter Computer-Spezialist, der insbesondere Sicherheitsbarrieren überwinden und in fremde Systeme eindringen kann.“ [COBA06]

Hardware
So werden Bestandteile des PCs genannt, „alles das, was man anfassen kann“

Internet
weltweites elektronisches Netz

Kernel
so wird der Kern eines Betriebssystems bezeichnet

LAN
„Local Area Network“, lokales Netzwerk

Malware
setzt sich aus dem englischen Wort „malicious“ (deutsch: boshaft) und dem Wort „Software“ zusammen und bezeichnet Computerprogramme, die unerwünschte und/oder schädliche Funktionen ausführen

PC
„Personal Computer“, privater Computer

Plug-In, Plugin

kommt vom Englischen „to plug in“ und bedeutet „anstöpseln“. In der Computerwelt ist ein Plug-In eine Software, die in eine andere Software „eingeklinkt“ werden kann. Die Software muss dies allerdings unterstützen

Port

„Schnittstelle zur Datenübergabe an einem PC. Nur mit der Internet-Adresse und dem dazugehörigen Port kann man einen Internet Dienst erreichen. Dabei gibt es für definierte Dienste feste Port-Nummern, z.B. Port 80 für Web-Server oder Port 21 für FTP-Server.“ [TONL01]

Software

„Software […] bezeichnet alle nichtphysischen Funktionsbestandteile eines Computers bzw. eines jeden technischen Gegenstandes, der mindestens einen Mikroprozessor enthält. Dies umfasst vor allem Computerprogramme sowie die zur Verwendung mit Computerprogrammen bestimmten Daten.“ [COBA13]

5.3 Quellen

Internet

[COBA01] URL http://www.computerbase.de/lexikon/Computervirus,
abgerufen am 08.06.2006

[COBA02] URL http://www.computerbase.de/lexikon/Computerwurm,
abgerufen am 09.06.2006

[COBA03] URL http://www.thgweb.de/lexikon/Linkvirus,
abgerufen am 14.06.2006

[COBA04] URL http://www.computerbase.de/lexikon/Malware,
abgerufen am 12.06.2006

[COBA05] URL http://www.computerbase.de/lexikon/Dropper,
abgerufen am 11.06.2006

[COBA06] URL http://www.computerbase.de/lexikon/Hacker,
aktualisiert am 24.06.2006, abgerufen am 11.06.2006

[COBA07] URL http://www.computerbase.de/lexikon/Trojanisches_Pferd_%28Computerprogramm%29,
abgerufen am 11.06.2006

[COBA08] URL http://www.computerbase.de/lexikon/Rootkit,
abgerufen am 12.06.2006

[COBA09] URL http://www.computerbase.de/lexikon/Spyware,
abgerufen am 15.06.2006

[COBA10] URL http://www.computerbase.de/lexikon/Adware,
abgerufen am 15.06.2006

[COBA11] URL http://www.computerbase.de/lexikon/Sniffer,
abgerufen am 13.06.2006

[COBA12] URL http://www.computerbase.de/lexikon/Datensicherung,
abgerufen am 21.06.2006

[COBA13] URL http://www.computerbase.de/lexikon/Software,
abgerufen am 21.06.2006

[COBA14] URL http://www.computerbase.de/lexikon/Plugin,
abgerufen am 21.06.2006

[COBA15] URL http://www.computerbase.de/lexikon/Hardware,
abgerufen am 21.06.2006

[HEIS01] URL http://www.heise.de/newsticker/meldung/70813,
aktualisiert am 14.03.2006, abgerufen am 12.06.2006

[LYCO01] http://webmaster.lycos.de/glossary/S/,
abgerufen am 15.06.2006

[SIN01] URL https://www.sicher-im-netz.de/default.aspx?sicherheit/hilfreiches/fokus/2,
abgerufen am 25.06.2006

[SIN02] URL https://www.sicher-im-netz.de/default.aspx?sicherheit/ihre/checklisten/checkliste&p=1_3_1,
abgerufen am 25.06.2006

[SIN03] URL https://www.sicher-im-netz.de/default.aspx?sicherheit/ihre/checklisten/checkliste&p=1_4_1,
abgerufen am 25.06.2006

[FRAV01] URL http://www.free-av.de/,
abgerufen am 25.06.2006

[ZONE01] URL http://www.zonelabs.com,
abgerufen am 25.06.2006

[LAVA01] URL http://www.lavasoft.de/,
abgerufen am 25.06.2006

[TONL01] URL http://www2.hilfe.t-online.de/dyn/c/06/54/40/654408.html,
abgerufen am 15.06.2006

Literatur

[CTMAG01] HIMMELEIN, Gerald; SCHMIDT, Jürgen: Sicherheitsrisiko durch DVD-Kopiersperre. In: c't – Magazin für Computer-Technik 05/06 (2006), S. 37

[HACK99] http://WWW.SPEZIALREPORTE.DE
Hacker's Black Book. 1999.

Sonstige

[FI01] ZENKER, Jochen; Fachinformatiker

[SPY01] Software „Spybot“; Hilfeseiten der Software

[XPAS01] Software „xp-AntiSpy“; Hilfeseiten der Software

Michael Eckel
Daniel Fischer
Ralf Decher

5.4 Eidesstattliche Erklärung

Hiermit versichern wir, die vorliegende Arbeit selbstständig unter ausschließlicher Verwendung der angegebenen Literatur und Hilfsmittel erstellt zu haben.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Ort, Datum Namen