e-teaching.org

Spam, Viren und Phishing

Autor/in: Redaktionsteam PELe
Portalbereich: Medientechnik
Stand: 07.06.2005

Inhaltsverzeichnis

Einleitung

Sicherheit im Internet und E-Mail-Verkehr ist ein sehr wichtiges Thema, das alle, die diese Techniken nutzen, etwas angeht. Bei nachlässigem Umgang können unter Umständen die Verletzung von Persönlichkeitsrechten, Datenspionage bis zum Datenverlust und finanzieller Schaden die Folge sein. Wenn Sie den Computer als tägliches Arbeitsgerät gebrauchen sind dort wichtige und schützenswerte Daten versammelt. Nehmen Sie die IT-Sicherheit also nicht auf die leichte Schulter.

Im Folgenden haben wir Informationen rund um die wichtigsten Gefahren oder Ärgernisse im Zusammenhang mit E-Mail- und Internetbenutzung zusammengestellt. Begriffe wie Spam, Viren, Würmer oder Phishing werden erklärt und Möglichkeiten zum Schutz vorgestellt. Für weiterführende Hinweise zum Thema IT-Sicherheit empfehlen wir die Seiten des Bundesamts für Sicherheit in der Informationstechnik (BSI) [http://www.bsi-fuer-buerger.de/] in Bonn, das sehr gute Informationen auf leicht verständliche Weise bereitgestellt hat.

1 Was ist Spam?

Unter Spam versteht man nach einer Definition der EU-Kommission unverlangt zugesandte (Massen-)-E-Mails. Diese können aus kommerziellen Angeboten oder nicht-kommerziellen, z.B. religiösen oder weltanschaulichen, Inhalten bestehen. Die Bezeichnung "Spam" stammt von einem Markennamen für Dosenfleisch SPAM (**Sp**iced H**am**) und erhielt ihre heutige Bedeutung wahrscheinlich in Anspielung auf einen Sketch von Monty Python's Flying Circus, in dem ein Gast in einem Restaurant, dessen Angebot ausschließlich aus Gerichten mit Spam besteht, ein Essen ohne Spam bestellen möchte, während eine im Hintergrund singende Gruppe Wikinger Spam anpreist [http://web1.austria182.server4free.de/downloads2/linux/multimedia/videos/Monty_Python-Spam.mpg].

Eine aktuelle Studie des Bundesamts für Sicherheit in der Informationstechnik über Antispam-Strategien [http://www.bsi.bund.de/literat/studien/antispam/index.htm] geht davon aus, dass heute

bis zu 90 % des gesamten E-Mail-Aufkommens aus Spam besteht. Der dadurch weltweit entstehende volkswirtschaftliche Schaden geht in die Milliarden. Die allermeisten Massen-E-Mails werden heute von professionellen Spammern versandt.

Eine Maßnahme zum Schutz vor Spam-E-Mail kann die Geheimhaltung oder Verschleierung der eigenen E-Mail-Adresse sein. Werden E-Mail-Adressen auf Webseiten nicht als Text, sondern als Grafik dargestellt, oder wird ihre Schreibweise (schmidt[at]mail.de oder das Einfügen offensichtlicher Schutzwörter schmidt.spamschutz@mail.de) verändert, kann dies ein automatisches Erkennen verhindern helfen. Ebenso wie diese Maßnahmen kann das Nichterscheinen in Email-Verzeichnissen einen – wenn auch geringen – Schutz bieten. Dennoch sollten Sie sensibel im Mitteilen oder Veröffentlichen Ihrer E-Mail-Adresse sein (etwa bei Internet Eingabeformularen) und gegebenenfalls beim Rechenzentrum das Streichen aus dem Hochschul-E-Mailverzeichnis veranlassen und sich über weitere Schutzmöglichkeiten informieren. Auch Kolleginnen und Kollegen oder Bekannte können zur Weitergabe Ihrer Adresse beitragen, indem sie bei einer E-Mail, die an eine größere Personengruppe geschickt wird, die „Kopie an"-Funktion (CC - Carbon Copy) gebrauchen. Dann sind für jede/n Empfänger/in alle anderen Empfängeradressen sichtbar. Benutzten Sie selber in solchen Fällen immer die BCC („Blind-Carbon-Copy") -Funktion und fordern Sie andere auf, es auch so zu handhaben. Die praktikabelste Methode zum Schutz vor der Müll-Mail ist jedoch das Filtern eingehender Nachrichten.

TIPP: Antworten Sie nie auf Spam-E-Mails, um sich zu beschweren oder die Unterlassung weiterer Nachrichten zu fordern. Die Spam-Absender freuen sich nur über die Information, dass ihre E-Mail-Adresse gültig ist und die Nachrichten gelesen werden. Für gültige, aktuelle E-Mail-Adressen werden im kriminellen Adress-Handel höhere Preise erzielt. Der Hinweis zum Nicht-Antworten auf E-Mails gilt übrigens auch für Nachrichten, in denen Ihnen die Möglichkeit angeboten wird, sich von einem E-Mail-Verteiler streichen zu lassen.

2 Spamfilter

Die Filterung einkommender Mail nach erwünschten und unerwünschten Nachrichten kann nach unterschiedlichen Prinzipien vorgenommen werden. Eine Methode überprüft die IP-Adressen der Absender-Mailserver und gleicht diese mit einer ständig aktuell gehaltenen Blacklist ab. In dieser Blacklist sind Server-Adressen verzeichnet, von denen bekannt ist, dass sie (und zwar fast ausschließlich) Spam-Mail versenden. Mails von diesen Servern werden nicht angenommen und zurückgesandt. Manche Verfahren arbeiten zusätzlich mit Whitelists, die vertrauenswürdige Server enthalten. Der Positivfehler, also der Fall, dass eine harmlose Mail fälschlich als Spam abgewiesen wird, ist beim Blacklist-Verfahren sehr unwahrscheinlich. Die meisten Universitätsrechenzentren und auch einige E-Mail-Dienste wenden diese Verfahren an. Nachteilig ist jedoch die hohe Zahl der Spam-Mails, die diese Hürde passieren können und in Ihrem Postfach landen.

Eine andere Methode filtert die E-Mails nach inhaltlichen Kriterien, in dem nach einzelnen Schlüsselwörtern in der Betreffzeile oder der Absender-Adresse gesucht wird. Auf diese Weise arbeitet beispielsweise die Junk-Email-Funktion des E-Mail-Programms Outlook. Im Produktsteckbrief [http://www.e-teaching.org/technik/produkte/outlookexpresssteckbrief] von e-teaching.org finden Sie nähere Informationen zum Programm. Wesentlich effektiver sind jedoch Filter, die auf dem

Bayes-Wahrscheinlichkeitstheorem aufbauen. Dabei werden alle Wörter einer E-Mail analysiert und jedem Wort wird ein bestimmter Wert zugewiesen. Daraus wird anschließend die Wahrscheinlichkeit ermittelt, mit der die Nachricht als Spam einzuschätzen ist. Dazu muss der Filter allerdings über eine Statistik der Worthäufigkeiten verfügen, die mittels vieler Nachrichten, die vom Anwender als Spam gekennzeichnet wurden, erstellt wird. Der besondere Vorteil der Programme mit Bayes-Filter ist ihre Trefferquote, ihre Lernfähigkeit und ihre Anpassung an das Anwenderprofil. Wird eine Nachricht nämlich als ungewiss eingestuft, entscheidet der Anwender, ob sie als Spam oder Ham (Ausdruck für gewünschte E-Mails) gewertet wird. Dadurch ändern sich die Wortwerte, der Filter passt sich an die Einschätzung des Anwenders an.

2.1 Antispam-Programme

Da das Uni-Rechenzentrum in der Regel lediglich Blacklist-Überpüfungen durchführt, um möglichst keine erwünschte E-Mail auszufiltern, ist es angeraten zusätzlich spezielle Antispam-Programme zu verwenden, die sich zwischen Mail-Server und E-Mail-Programm (Outlook, Outlook Express, Thunderbird, Eudora Mail, Pegasus etc.) schalten. Sie filtern die Nachrichten und markieren verdächtige E-Mails, die sich dann über die Filterregel des E-Mail-Programms in Ordner sortieren oder sofort löschen lassen. Wie Sie beispielsweise in Outlook [Express] Filter definieren, haben wir in einer Outlook-Anleitung [http://www.e-teaching.org/technik/kommunikation/email/outlook.pdf] beschrieben.

Ein Open-Source Antispam-Programm, das auf der Basis von Black- und Whitelists arbeitet und zusätzlich zu den Maßnahmen des Rechenzentrums oder privat genutzt werden kann, ist SpamPal [http://spampal.de/pmwiki/pmwiki.php]. Es liegt in deutscher Sprache vor, funktioniert aber nur auf der Windows-Plattform. Sie sollten sich die separate Anleitung downloaden, die auch Erklärungen für die Benutzung von Spampal in Verbindung mit verschiedenen E-Mail-Programmen (Eudora, Outlook[Express], Pegasus, Thunderbird) enthält. SpamPal schaltet sich zwischen den Pop3-Server bzw. Ihr Pop3-Postfach und Ihr E-Mail-Programm. Jede Nachricht wird vom Antispam-Programm über DNSBL-Server (steht für Domain Name System-based Blackhole List) mit den Listen bekannter Spam-Absenderadressen verglichen und gegebenenfalls markiert.

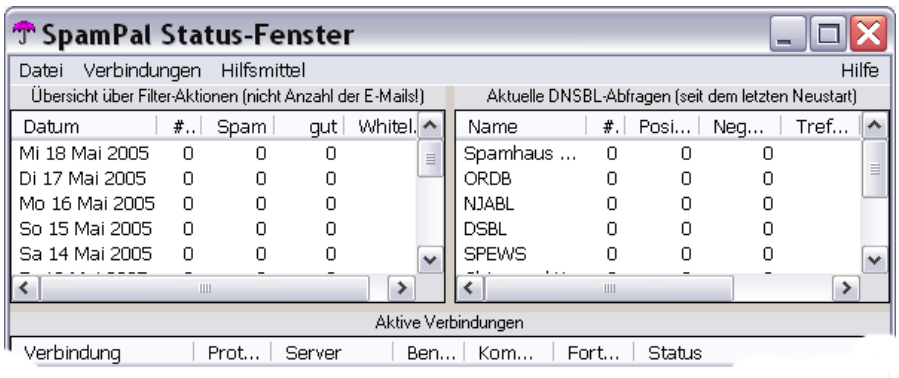

Abbildung 1: Status-Fenster von SpamPal

Für SpamPal gibt es auch ein Plugin [http://spampalbayes.sourceforge.net/], das auf der Bayes-Methode basiert und einen lernenden Filter besitzt.

Ein anderes kostenloses Antispam-Programm für die Windows-Plattform ist der Spamihilator [http://www.spamihilator.com/] von Michael Krämer. Es funktioniert auf Basis eines lernenden Bayes-Filters und schaltet sich genau wie SpamPal zwischen Pop3-Server/Postfach und E-Mail-Programm. Besonders bedienungsfreundlich macht dieses Programm der Spamihilator-Wizard, der die Einstellungen für gängige E-Mail-Programme wie Outlook, Thunderbird, Eudora, Pegasus und einige weitere automatisch vornimmt.

Die ankommende Mail wird beim Serverabruf überprüft und anhand des Spam-Wort-Filters und weiterer Filter kategorisiert. Die innerhalb der letzten Tage angekommene E-Mail wird in einen Trainingsbereich zwischengelagert. Dort können Sie die Nachrichten einsehen und festlegen, welche als Spam gewertet werden und bei welchen es sich um erwünschte E-Mails handelt (Abbildung 2).

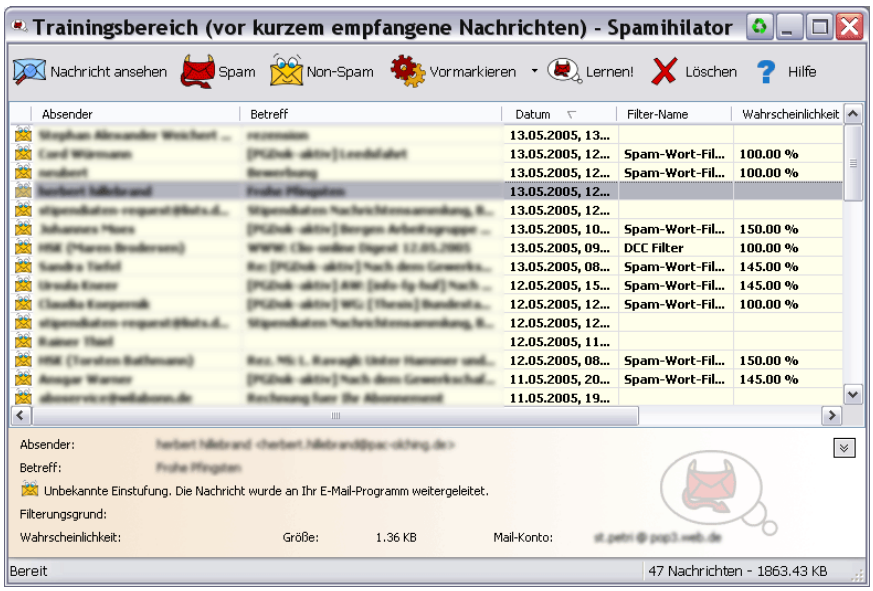

Abbildung 2: Trainingsbereich des Spamihilator

Als Spam markierte E-Mail wird in den Papierkorb geworfen, Non-Spam an Ihr E-Mail-Programm weitergeleitet. Sie können sich mit der Vormarkieren-Funktion vom Spamihilator anzeigen lassen, welche E-Mails das Programm als Spam oder Non-Spam einstuft und sehen auch den zugrunde liegenden Filter und die errechnete Wahrscheinlichkeit.

Für Macintosh-Rechner gibt es leider keine kostenlose Antispam-Software. Als kommerzieller Anbieter hat die Softwarefirma Intego den Intego Personal Antispam X3 und weitere Sicherheitspakete im Angebot [http://www.intego.com/de/personalAntispam/].

2.2 Spamfilter in E-Maildiensten

E-Mail-Dienste wie Hotmail, Web.de, GMX oder Yahoo-Mail haben eigene Spam-Filter eingerichtet, die meist mit einer Kombination aus IP-Adressen-Blacklist-Überprüfung, Schlüsselwörtern und Bayes-Filtern arbeiten. Diese Filter sortieren einkommende Mail automatisch in den Posteingang oder einen Ordner, der beispielsweise Spamverdacht oder Junk-Mail heißt. Die hier abgelegten E-Mails wurden vom Filter als problematisch eingestuft und werden nach einigen Tagen (variiert zwischen ca. 5 und 30 Tagen) gelöscht. Schauen Sie regelmäßig in diesem Ordner nach, ob sich nicht doch eine gewünschte E-Mail unter den Spam-Mails befindet.

Selbstverständlich können Sie die Filter der E-Mail-Dienste auch mit den oben beschriebenen Antispam-Programmen kombinieren, zwei Filter finden mehr unerwünschte Werbe-E-Mail als einer!

3 Virenschutz

Bei der Benutzung von E-Mail und Internet stellen Computerviren ein großes Sicherheitsrisiko dar. Der Schutz vor Viren ist folglich äußerst wichtig. Was aber sind eigentlich Computerviren? Wikipedia definiert ein Computervirus als „eine nichtselbständige Programmroutine, die sich selbst reproduziert, indem sie sich an andere Computerprogramme oder Bereiche des Betriebssystems anhängt. Einmal gestartet, nimmt sie vom Anwender nicht kontrollierbare Veränderungen an selbigen vor“. Nach dieser Definition nicht zu den Computerviren gehörend, aber im allgemeinen Verständnis dazu gezählt, werden Würmer und Trojanische Pferde. Würmer sind sich selbst reproduzierende Programme, die sich wurmartig über ein Computernetzwerk - z.B. per E-Mail - ausbreiten und an Computerprogrammen oder Betriebssystemen Manipulationen vornehmen. Trojanische Pferde sind Programme, die sich als nützliche Programme tarnen, aber in Wirklichkeit schädliche Software einschleusen und im Verborgenen unerwünschte Aktionen ausführen.[1]

Hinweis: Keine Virenabwehr, aber dennoch eine Maßnahmen zum Schutz Ihrer Daten, ist das regelmäßige Anlegen von Sicherungskopien (Backups). Die je nach Bedarf tägliche, wöchentliche oder monatliche Sicherung Ihrer Daten sollte zur Routine im Umgang mit dem Arbeitsgerät Computer gehören

3.1 Maßnahmen zum Schutz vor Viren, Würmern und Trojanischen Pferden

Vor dem Angriff von Viren, Würmern und Trojanischen Pferden können Sie sich auf verschiedene Weisen schützen. Einige einfache Regeln im Umgang mit Software und E-Mail begrenzen das

[1] Trojanische Pferde werden häufig auch als Trojaner (*trojans*) bezeichnet, obwohl nach Homers Ilias die Trojaner die Geschädigten der griechischen Kriegslist waren.

Risiko einer Infizierung. In erster Linie sind Rechner mit Windows-Plattform von Virenangriffen betroffen, für die Betriebssysteme Mac OS und Linux sind kaum verbreitete Viren bekannt. Daher beziehen sich die folgenden Informationen und Empfehlungen auf Windows-Rechner.

Verhaltensregeln zum Schutz vor Computerviren

- Öffnen oder führen Sie niemals unbekannte Programme oder Programme aus unsicherer Quelle aus und sind Sie generell beim Öffnen von Dateien achtsam. Insbesondere bei verdächtigen Dateien, die per E-Mail zuschickt werden, ist Vorsicht angeraten. Solche Dateien sollten, wenn überhaupt, erst nach Überprüfung mit einem aktuellen Antivirenprogramm geöffnet werden.
- Halten Sie Betriebssystem und Anwendungen aktuell (Installation der Service Packs, Verbesserungen und Erweiterungen).
- Nutzen Sie die eingebauten Schutzfunktionen des Betriebssystems. Deaktivieren Sie beispielsweise das automatische Öffnen von Dateien aus dem Internet und die Autostartfunktion für CD-ROMs und DVD-ROMs. Dadurch wird verhindert, dass Programme bereits beim Einlegen eines Datenträgers ausgeführt werden und ein System infizieren. Eine Schützmöglichkeit besteht darin, im Alltagsgebrauch nicht als Administrator mit allen Rechten, sondern als Nutzer mit eingeschränkten Rechten zu arbeiten. So kann verhindert werden, dass sich Software automatisch installiert.
- Deaktivieren Sie in Ihrem E-Mail-Programm das automatische Öffnen von Dateianhängen.
- Deaktivieren Sie in Ihrem Browser ActiveX oder VBScript. Dabei handelt es sich um Funktionen, die das Downloaden aktiver und damit potentiell gefährlicher Inhalte ermöglichen.
- Konfigurieren Sie die auf den meisten Windowsrechnern vorinstallierte Software von Microsoft (z.B. Internet Explorer oder Outlook Express) nach Sicherheitsaspekten oder vermeiden Sie sie ganz, da diese weit verbreiteten Programme häufige Angriffziele sind.
- Seien Sie vorsichtig bei Virenwarnmeldungen per E-Mail von Unbekannten, aber auch von (gutgläubigen) Kollegen oder Bekannten. Es können u. U. mit den Warnungen selbst Viren eingeschleust werden oder es handelt sich um so genannte Hoaxes (engl. für Scherz, Falschmeldung), die nur der Panikmache dienen oder dazu auffordern unsinnige oder schädliche Manipulationen am System vorzunehmen.

Informationen über Hoaxes [http://www.tu-berlin.de/www/software/hoax.shtml] und eine Liste aktueller Falschmeldungen [http://www.tu-berlin.de/www/software/hoaxlist.shtml] stellt die TU Berlin bereit. Zu den Hoaxes werden im Übrigen auch Kettenbriefe gerechnet, die bei Weiterleitung an möglichst viele Adressaten dem Absender Glück versprechen oder einem kranken Kind in Afrika die Heilung ermöglichen sollen. Diese Nachrichten sind im besten Falle harmlos, binden aber

bei Beantwortung in jedem Fall Arbeitszeit und lösen garantiert nicht das in ihnen behauptete Versprechen ein. Sie sollten unbeachtet in den Papierkorb verschoben werden.

Das Bundesamt für Sicherheit in der Informationstechnik hat im Jahr 2000 Empfehlungen zum Schutz vor Computer-Viren [http://www.bsi.de/av/texte/empfehlung.htm] aus dem Internet zusammengestellt, die immer noch beachtenswert sind.

Das Vermeiden von Virenangriffen ist eine wichtige Vorsichtsmaßnahme zum Schutz gegen Virenbefall, reicht aber nicht aus. Ein Antivirenprogramm sollte in jedem Fall zur Standardausstattung eines Computers mit Windows-Plattform gehören.

3.2 Virenschutzprogramm

Ebenso wie die Zahl der Viren und Würmer wächst auch die Zahl der verfügbaren Antivirenprogramme immer weiter an. Das Geschäft mit der Internetsicherheit ist sehr lukrativ und es fällt schwer, im großen Angebot den Überblick zu behalten. Als Beschäftigte/r einer Universität, Fachhochschule oder Forschungseinrichtung ist der erste Schritt auf der Suche nach geeigneter Software zum Schutz vor Viren der Kontakt mit dem Rechenzentrum oder der EDV-/Ist-Abteilung. Diese haben Virensoftware zum Schutz der Server im Einsatz und bieten außerdem Lizenzen für Standard-Antivirenprogramme an. Dieser Service ist für Hochschulangehörige fast immer kostenlos, Sie sollten davon Gebrauch machen. Das Rechenzentrum oder die entsprechenden Abteilungen beraten Sie auch darüber, was im Falle eines Virenbefalls zu tun ist. Nicht immer ist das selbständige Löschen des Virus die beste Lösung!

Können Sie nicht auf die Angebote eines Rechenzentrums zurückgreifen oder möchten Sie Ihren (Privat-)Rechner selbst vor Infektionen schützen, gibt es eine Vielzahl guter kommerzieller und kostenloser Antivirenprodukte. Eine Liste aktueller Antivirenprogramme mit Links zu den Anbietern [http://www.heise.de/security/dienste/antivirus/links.shtml] hat der renommierte Heise-Verlag zusammengestellt.

Es ist zu unterscheiden zwischen Antivirenprogrammen, die Sie auf Ihrem Rechner installieren und Angeboten, die einen Online-Virenscan ermöglichen. Bei letzteren laden Sie eine oder mehrere Dateien auf den Server des Virenschutzanbieters hoch und lassen dort eine Prüfroutine laufen. Dieses Verfahren bietet sich an, wenn Sie einzelne Dateien überprüfen möchten. Anbieter von Online-Scans sind:

Ikarus [http://www.ikarus-software.at/portal/modules.php?name=Content&pa=showpage&pid=4],

Kapersky [http://www.kaspersky.com/remoteviruschk.html] und

MCAffee [http://us.mcafee.com/root/mfs/default.asp].

Sehen sie sich zu Online-Virenscanner auch die Informationen des BSI [http://www.bsi-fuer-buerger.de/infiziert/06_0502.htm] an. Die Größe der zu überprüfenden Dateien ist in der Regel auf 1 MB beschränkt. Vor einer Online-Überprüfung des gesamten Rechners, die durchaus möglich ist, wird abgeraten. Hier können sich Sicherheitslücken ergeben. Benutzen Sie für eine Komplett-Scan Ihrer Festplatte besser Programme, die auf Ihrem Rechner installiert werden (Offline-Virenscanner).

Bei Offline-Virenscanner gibt es zwei Varianten der Prüfvorgänge. Zum einen kann der Scannvorgang immer dann ablaufen, wenn Sie ihn explizit wünschen bzw. nach einem von Ihnen festgelegten Zeitschema. Das nennt man On-Demand-Virenscan. Beim On-Access-Virenscan wird jede Datei automatisch bei Zugriff überprüft.

Zu den verbreiteten, kommerziellen Antiviren-Programmen zählen:

McAffee VirusScan [http://de.mcafee.com/],

Norton AntiVirus [http://www.symantec.com/region/de/product/antivirus/index_win.html] und

Norman Virus Control [http://www.norman.com/Product/Home_Home_office/NVC/758/de].

Diese empfehlenswerten Produkte kosten zwischen 40,- und 50,- Euro, können aber als Demo-Versionen kostenfrei für 30 Tage getestet werden. Die Voll-Lizenzen gelten für ein Jahr innerhalb dessen kostenlose Aktualisierungen der Virendatenbank möglich sind. Alle Hersteller bieten auch Mehrjahres-Lizenzen und Pakete mit mehren Sicherheitsprogrammen an.

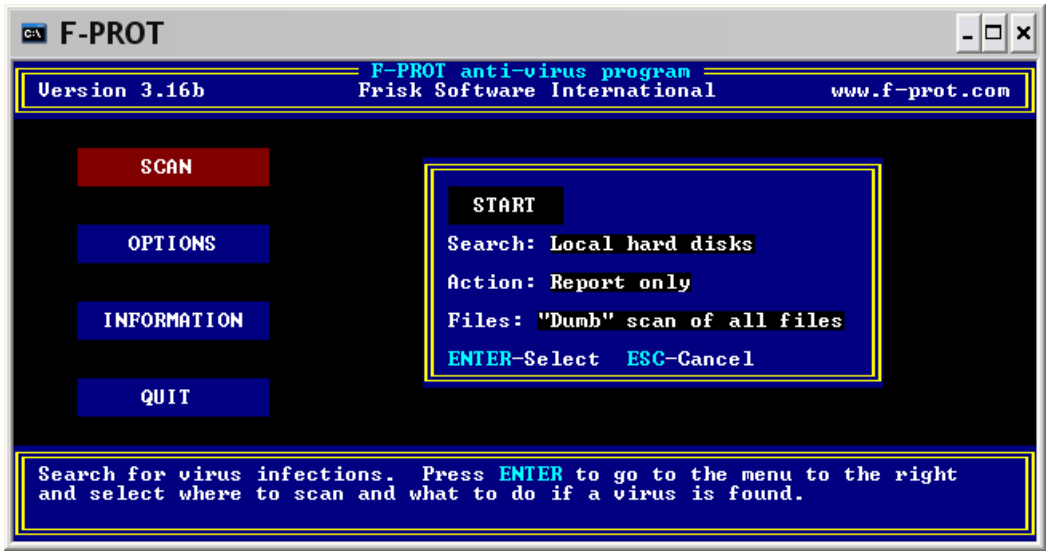

Abbildung 3: Virenscanner F-Prot

Als Alternative zu diesen Angeboten gibt es für Privatanwender kostenfreie Antiviren-Programme. Das bekannte F-Prot Antivirus [http://www.f-prot.com/index.html] des isländischen Unternehmens FRISK Software ist in der Version, die auf der DOS-Ebene des PCs arbeitet, kostenlos (Abbildung 3). Dies schmälert nicht die Leistung im Erkennen von Viren, jedoch den Bedienungskomfort des englischsprachigen Virenscanners. Z.B. ist ein On-Access-Virenscan nicht möglich und das Programm kann nur über die Tastatur bedient werden.

Ein vom BSI empfohlenes, deutschsprachiges und für Privatanwender kostenloses Antiviren-Programm ist die AntiVir PersonalEdition Classic der H+BEDV Datentechnik GmbH. Es ist leicht in der Handhabung und auch für unerfahrene Anwender geeignet. Der Funktionspalette umfasst einen On-Demand-Virenscanner mit Zeitplaner (siehe Abbildung 4) und einen On-Access-Scanner, der

AntiVir Guard genannt wird. Beide Programmteile lassen sich leicht bedienen, die Internetupdate-Funktion ist übersichtlich aufgebaut.

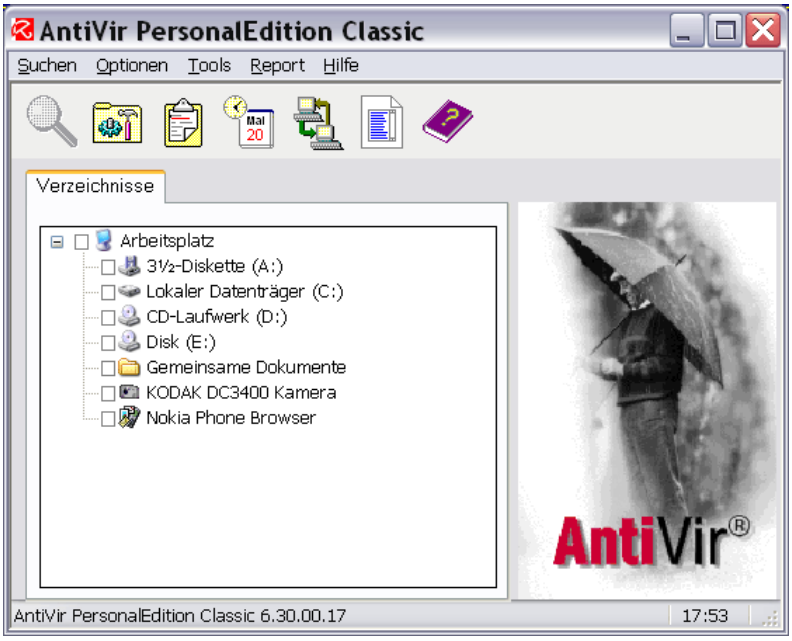

Abbildung 4: AntiVir PersonalEdition Classic

In Tests von Antivirenprogramme schneiden die empfohlenen kommerziellen Produkte oft etwas besser ab als die kostenlosen Alternativprodukte, da sie meist mehr Viren, Würmer und Trojanische Pferde erkennen. Für den nicht-professionellen Nutzer sind F-Prot oder AntiVir jedoch eine gute Wahl.

Wichtig ist in jedem Fall, dass Sie Softwareversionen und die von den Programmen berücksichtigten Virenlisten immer auf dem aktuellen Stand halten. Die genannten kommerziellen Programme und das kostenlose AntiVir bieten die Funktion des automatischen Updates, das in regelmäßigen Abstand die Virendatenbank auf den neusten Stand bringt. Gibt es kein automatisches Update, aktualisieren Sie - wenn möglich - jede Woche die Viren-Datenbank.

3.3 Personal Firewall

Ein Schutzmechanismus, der die Sicherheit im Internet erhöht, sind so genannte Firewalls. Unter einer Firewall versteht man ein Zugangsschutzsystem, das den Datenverkehr zwischen verschiedenen Netzen kontrolliert, um ungewünschten Verkehr zu verhindern und nur den gewünschten Verkehr weiterzuleiten. Sie kann beispielsweise den Datenaustausch zweier verbundenen Firmennetzwerken regeln und Datenzugriff von außen unterbinden. Eine Personal Firewall-Software (auch Desktop Firewall genannt) hingegen dient dem Schutz eines einzelnen Computers und filtert den ein- und ausgehenden Datenverkehr (in der Regel die Kommunikation mit dem Internet) auf dem Rechner selbst. Sie kann nicht vor eigentlichen Viren schützen - dazu benötigt man ein Antivi-

ren-Programm - den Rechner jedoch vor Würmern, Trojanischen Pferden und anderen Zugriffen bewahren. Kein Firewall-Schutz ist wasserdicht, jedes Personal Firewall kann von Spezialisten umgangen werden. Sie sollte daher Teil eines umfassenderen Schutzsystems in Kombination mit einem Antiviren-Programm sein.

Firewalls sind für IT-Laien nicht unbedingt leicht zu konfigurieren und zu bedienen. Sie sollten die Bedeutung von IP-Adressen und Host-/Rechnernamen sowie die gemeldeten Ports kennen, da bei der Erstellung von Firewall-Regeln diese Informationen erfragt werden. Eine Einführung bietet der Eintrag zu Firewalls [http://de.wikipedia.org/wiki/Firewall] in Wikipedia und auf den Seiten des BSI [http://www.bsi-fuer-buerger.de/infiziert/06_0501.htm#Pers_Firewall].

Die Windows-Firewall, die bei Windows XP ab Service Pack 2 standardmäßig aktiviert ist, bietet einen gewissen Schutz. Sie lässt sich über das Sicherheitscenter (START → ALLE PROGRAMME → ZUBEHÖR → SYSTEMPROGRAMME → SICHERHEITSCENTER) konfigurieren.

Darüber hinaus gibt es eine Reihe empfehlenswerter Firewall-Software, die für den/die Privatanwender/in kostenlos zur Verfügung steht. Eine leicht zu bedienende und zu konfigurierende Firewall ist ZoneAlarm [http://download.zonelabs.com/bin/free/de/download/znalmDetails.html], die es als kostenlose deutsche Version gibt. Vom BSI wird die Kerio Personal Firewall empfohlen [http://www.kerio.com/kpf_download.html], die 30 Tage als Vollversion und danach mit eingeschränktem Funktionsumfang kostenlos weiter benutzt werden darf.

Der Betrieb von mehreren Firewalls auf einem Rechner ist nicht empfehlenswert, da sie sich gegenseitig behindern können. Wenn Sie eine Firewall installieren, deaktivieren Sie vorher die Windows-Firewall.

4 Phishing: Ungebetener Kennwort-Raub

Bei dem in letzter Zeit immer häufiger in den Medien besprochenem Problem des Phishings (eine Neuschöpfung aus der englischen Wortreihe Password Harvesting Fishing) handelt es sich um das illegale Ausspionieren von Kennwörtern (z.B. für Online-Banking, Kreditkartennummern etc.). Bei dieser Art des Trickbetrugs werden Personen bspw. über gefälschte E-Mails aufgefordert, Internetseiten, die die Seiten von Banken, Händlern etc. täuschend echt nachahmen, zu besuchen und sich dort mit ihren Zugangsdaten oder Kreditkartennummern einzuloggen. Dazu werden in der E-Mail Links auf die angeblichen Bankseiten oder Händler angegeben. Die dort eingegeben Daten gehen dann direkt an die Phisher und können zur Räumung des Bank- oder des Kreditkartenkontos missbraucht werden. Eine modernere Variante besteht in der Zusendung einer E-Mail mit einem HTML-Formular, das direkt zur Eingabe der geheimen Daten auffordert und diese an den Betrüger weiterleitet. Auch Trojanische Pferde werden zum Kennwortdiebstahl eingesetzt. Phishing könnte im Zusammenhang mit kostenpflichtigen Angeboten auch im Bereich des E-Learnings relevant werden.

Die gefälschten E-Mails, Formulare und Internetseiten sehen teilweise sehr echt aus und können von Laien nicht ohne weiteres von den Originalen unterschieden werden. Obwohl einige Programme zum Schutz vor Phishing angeboten werden, ist das Beachten einiger einfacher Regeln ausreichend, um die Gefahr des Phishing zu minimieren.

Verhaltensregeln zum Schutz vor Phishing

- Lassen Sie sich nicht vom offiziellen Charakter der Nachricht und den Adressen täuschen. Internetadressen (URLs) und E-Mail-Absenderadressen sind nicht per se vertrauenswürdig, sie können leicht gefälscht werden.
- Fast alle Banken versenden wichtige Informationen nicht per E-Mail, sondern mit der regulären Post. Bei offiziell aussehenden E-Mails, die zur Herausgabe persönlicher Daten auffordern, sollten Sie nicht reagieren, sondern direkt bei der Bank nachfragen. Phishing E-Mails sollten nach Absprache an die Banken und/oder die Kriminalpolizei weitergeleitet werden.
- Benutzen Sie keine Links aus E-Mails oder von Internetseiten zum Online-Banking, sondern tragen Sie die URL immer von Hand in die Adresszeile des Browsers ein oder benutzen Sie selbst angelegte und geprüfte Lesezeichen. Im Zweifelsfall starten Sie auf der Homepage Ihrer Bank und klicken sich zum Onlinebanking-Bereich durch.
- Werden Sie stutzig, wenn beim Online-Banking unmittelbar nach einer TAN-Eingabe die Verbindung zum Server unterbrochen wird und eine Fehlermeldung erscheint. Ein auf ihren Rechner eingeschleustes Trojanisches Pferd könnte die Ursache sein. Fragen Sie am besten umgehend bei der Bank nach oder blockieren notfalls Sie durch dreimalige Falscheingabe einer TAN den Online-Bankzugang.

Sollten sie nicht sicher sein, ob Ihnen die Schutzmechanismen Ihrer Bank ausreichen, ist ein Wechsel des Bankhauses zu überlegen. Das Fraunhofer Institut Sichere Informationstechnik hat im November 2004 eine Studie zum Phishing-Schutz im Online-Banking veröffentlicht [http://www.sit.fraunhofer.de/cms/media/pdfs/phishing.pdf] und verschiedene Bankangebote verglichen.