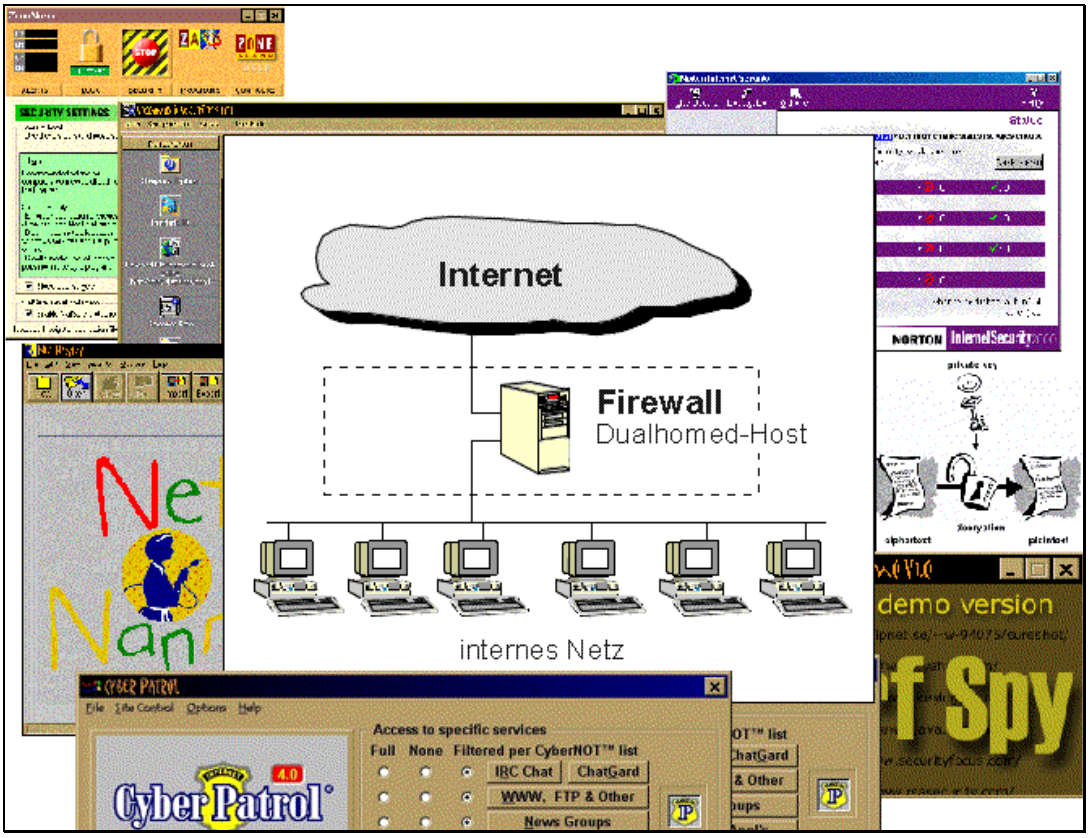
Wolfgang Schmid, Melanie Stachel

Sicherheit im Schulnetz

Hinweise zur Internet-Anbindung für die Schule



Zentralstelle für Computer im Unterricht
Augsburg 2000

Erarbeitet im Auftrag
des Bayerischen Staatsministeriums
für Unterricht und Kultus

Autoren:

Wolfgang Schmid

Melanie Stachel Zentralstelle für Computer im Unterricht, Augsburg

© Nachdruck - auch auszugsweise - nur mit Genehmigung der Zentralstelle für Computer im Unterricht, Augsburg

Zentralstelle für Computer im Unterricht, Schertlinstr. 9, 86159 Augsburg
Telefon (08 21) 2 59 19-0, Telefax (08 21) 2 59 19-19
E-Mail: zentralstelle@zs-augsburg.de
Internet-Angebot: http://www.zs-augsburg.de

Vorwort

Der Einsatz des Internet im Rahmen der Schule ist durch vielfältige äußere Maßnahmen praktikabel und finanzierbar geworden. Die allgemein fortschreitende gesellschaftliche Akzeptanz, hohes Engagement der Kolleginnen und Kollegen und vielfältige Fortbildung haben dazu geführt, dass die Inhalte immer häufiger für den Unterricht verwendet werden. Dennoch bleibt ein Rest von Unsicherheit, der auch darin begründet ist, dass vermehrt Nachrichten über die Schattenseiten dieses Mediums verbreitet werden. Stichworte wie ‘Angriffe aus dem Netz’ und die ‘Verbreitung jugendgefährdender Inhalte’ verunsichern viele Anwender und lassen den Bedarf nach Informationen darüber wachsen, was wesentliche Gefahren im Umgang mit diesem Medium sind.

Es existieren dazu vielfältige Quellen, die die grundsätzliche Problematik einer informationstechnischen Absicherung von Netzwerken betreffen. Auch für den Bereich öffentlicher Verwaltung sind detaillierte technische Unterlagen und organisatorische Ratschläge zu deren Umsetzung vorhanden. Für die Schule jedoch stellt sich ein zusätzliches Problem. Neben der technischen Absicherung der immer längeren Anwesenheit unterrichtlich genutzter Rechner im weltweiten Netz, die sicherlich Grundlage für einen verantworteten Unterricht darstellt, steht zunehmend die didaktisch und ethische Frage zum Umgang mit den Inhalten des Internets im Mittelpunkt.

Für beide Aspekte sollen in dieser Broschüre realisierbare Lösungsvorschläge vorgestellt werden. Im Rahmen der für eine Schule finanzierbaren und organisatorisch zu bewältigenden Mittel werden Maßnahmen und Programme vorgestellt, die Hilfestellung bei der Umsetzung der Aufgabe sein können, sicheren Zugriff auf die Dienste des Internet zu realisieren.

In einer sich permanent und mit rasendem Tempo entwickelnden Umgebung ist dieser Versuch selbstverständlich eine Momentaufnahme. Immer häufiger treffen bei den dafür zuständigen Stellen Informationen, Programmbeschreibungen, Testversionen oder einfach nur Nachrichten über neue, geänderte und in ihrer Funktion verbesserte Programme ein. Sie müssen in ihrer Funktionalität, Handhabbarkeit und Finanzierbarkeit überprüft werden und sollten in einer komplexen Schulwirklichkeit getestet werden. Die ergänzenden Erkenntnisse zu dieser Broschüre werden deshalb in Zukunft aktuell im Internet-Angebot des Bayerischen Schulservers zur Verfügung gestellt.

Augsburg, September 2000

Wolfgang Schmid

Inhaltsverzeichnis

1 Schutzwürdige Bereiche 7
1.1 Schulverwaltung 7
1.2 Unterricht 7
2 Gefahrenquellen 8
2.1 Nutzerverhalten 8
2.1.1 Fahrlässige Systemänderungen 8
2.1.2 Fehlende Dokumentation 8
2.1.3 Fehlende Datensicherung 8
2.2 Viren 8
2.2.1 Was für Viren gibt es? 8
2.2.2 Was tun Viren? 9
2.2.3 Wie kann ich mich schützen? 9
2.2.4 Welche Programme helfen mir? 10
2.3 Angriffe aus dem Intranet 11
2.3.1 Zeitvergleich Intranet - Internet 11
2.3.2 Beaufsichtigte und unbeaufsichtigte Arbeitsplätze 11
2.3.3 Trennung der Netzsegmente 12
2.3.4 Fernzugriff 12
2.4 Angriffe aus dem Internet 12
2.4.1 Schadenstypen 12
2.4.2 Trojanische Pferde 12
2.4.3 Ausführbare Dateien auf dem lokalen Rechner 12
2.4.4 Formen von Hacker-Angriffen 13
2.4.5 Portscanning 13
2.4.6 Hacking (z. B. eines HTTP-Servers) 13
3 Schutzmöglichkeiten 14
3.1 Räumliche Sicherung 14
3.2 Physikalische Zugriffssicherung 14
3.3 Passwörter 14
3.4 Softwarelösungen 15
3.4.1 Steganografie 15
3.4.2 PGP für E-Mail 16
3.5 Firewall 18
3.5.1 Funktionsweisen 18
3.5.2 Hardwarelösung Defendo 20
3.5.3 Softwarelösungen 22
3.5.3.1 ZoneAlarm 22
3.5.3.2 Norton Internet Security 2000 25
4 Internetinhalte 27
4.1 Verwendung lokaler Kopien im Intranet 27
4.2 Protokoll-Programme für den Internet-Zugriff 29
4.3 Proxy-Server mit Negativ/Positivlisten 30
4.4 Kommerzielle Wächtersysteme 32
4.4.1 Cyber Patrol 32
4.4.2 NetNanny 33
4.4.3 Norton Internet Security 2000 35
4.5 E-Mail mit Attachements 36
4.6 Sandbox-System 37
5 Literatur und weitere Hinweise 38
5.1 Quellen: 38
5.2 Literatur 38
5.3 Internet-Links 38

1 Schutzwürdige Bereiche

1.1 Schulverwaltung

Für den Bereich der Schulverwaltung legt das Votum 2000 des Beraterkreis für Schulrechner folgendes fest:

„Beim Einsatz der EDV in der Schulverwaltung muss die Vertraulichkeit, Integrität und Verfügbarkeit aller sensiblen Daten dauerhaft gewährleistet sein. Daher muss sicher gestellt sein, dass unautorisierten Personen ein Zugriff auf personenbezogene Daten und die zugehörigen Programme nicht möglich ist. Die Verantwortung hierfür liegt bei der Schule.
Gemäß der Dienstvereinbarung mit dem Hauptpersonalrat ist bei EDV-mäßiger Verwaltung von Lehrerdaten die Einbindung von Rechnern für Verwaltungs- und Unterrichtszwecke in ein einziges Netz nicht zulässig. Da ein optimaler Schutz nach wie vor nur in einer physikalischen Trennung der jeweiligen Netze gesehen wird, sind grundsätzlich Verwaltungsnetze von Rechnern zu Unterrichtszwecken physikalisch getrennt zu halten.

Wenn zur Nutzung der Datenfernübertragung ein Internetzugang aus dem Verwaltungsnetz nötig ist, so sind besondere Schutzmaßnahmen vor nicht autorisierten Zugriffen auf personenbezogene Daten zu treffen. Als mögliche Sicherheitsmaßnahmen werden empfohlen: Zugangskontrolle über die Einrichtung einer „Firewall“, die den gesamten Datenverkehr zwischen Internet und Schulverwaltungsbereich überprüft und filtert; zeitlich begrenzter Wahl-Zugang zum Internet, keine nach außen bekannte, feste IP-Adresse; Beschränkung des Zugriffs auf als sicher bekannte Adressen mit Identifizierung; eigener Mail-Server mit Beschränkung der angewandten Dienste (z. B. nur gesicherte E-Mails); sichere Nachrichtenübermittlung und zuverlässige Prüfung der eingehenden E-Mails, z. B. durch Virenscanner, Authentifizierung.
Eine detailliertere Zusammenstellung von Schutzmaßnahmen ist in der Neufassung der Erläuternden Hinweise zum Datenschutz bzw. in der Dienstvereinbarung mit dem Hauptpersonalrat enthalten.“

Der Einsatz einer Firewall zwischen Internet und Schulverwaltungsrechner ist am einfachsten über den Einsatz einer persönlichen Firewall auf dem betroffenen Rechner zu realisieren (z. B. ‘ZoneAlarm’, s. u.). Besteht jedoch die Notwendigkeit, den Zugang zum Internet über ein gemeinsames Gateway von Schulverwaltung und Schulnetz zu realisieren, so sind bei der Konfiguration des Netzwerk-Routers besondere Sicherheitsmaßnahmen zu treffen. In jedem Fall sollten physikalisch getrennte Netzwerkkarten mit getrennten Adressräumen eingerichtet werden, damit ein gegenseitiges Routing aus dem Schulnetz ins Schulverwaltungsnetz ausgeschlossen werden kann. Zusätzlich sollten die unten genannten physikalischen Zugriffssperren unbedingt genutzt werden. Nach Vorliegen der Neufassung der Erläuternden Hinweise zum Datenschutz bzw. der Dienstvereinbarung mit dem Hauptpersonalrat ist diesen Hinweisen zu folgen.

1.2 Unterricht

Für den Bereich außerhalb der direkten Schulverwaltung muss grundsätzlich unerschieden werden:

- Technischer Schutz der lokalen Rechner im LAN (Local Area Network)
- Inhaltlicher Schutz vor unerwünschten Inhalten im Internet

Beides ist Voraussetzung einer verantworteten Nutzung des Internets im Rahmen der Schule. Während für ersteren Bereich bereits umfangreiche Ausarbeitungen zur Verfügung stehen (siehe ‘Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet’, erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Mai 2000 bzw. ‘IT-Grundschutzhandbuch’ des Bundesamtes für Sicherheit in der Informationstechnik), ist der zweite Bereich noch wenig bearbeitet und unterliegt doch wachsender Nachfrage.

Diese Broschüre versucht, konkrete Umsetzungsmöglichkeiten für beide Bereiche anzubieten. Dabei werden speziell Produkte vorgestellt, die im Rahmen der an der Schule zur Verfügung stehenden Ressourcen beschafft und verwaltet werden können. Speziell der Bereich von technischen und inhaltlichen Schutzmöglichkeiten eines kompletten LANs ist derzeit noch nicht umfassend darstellbar, da die Produkte einerseits noch sehr hohe Kosten nach sich ziehen würden, sie andererseits noch nicht in einer komplexen Schulsituation getestet werden konnten. Daher kann der Anspruch, eine für alle Schulen gleichermaßen finanzierbare, einfach handhabbare und gleichzeitig flexible Lösung für ein komplettes Schulnetz zur Verfügung zu haben, noch nicht erfüllt werden.

2 Gefahrenquellen

Zunächst gilt es, die möglichen Ursachen für den Ausfall von Rechnersystemen bzw. die dadurch entstehende Behinderung von Unterricht aufzuzeigen und bezüglich Häufigkeit und Gefahrenpotential einzuordnen. Dabei wird unterschieden zwischen ‘unbeabsichtigten’ Gefährdungen durch Nutzer und Betreuer während der normalen Nutzung des Systems, absichtlichen Angriffen aus dem Intranet und solchen aus dem Internet.

2.1 Nutzerverhalten

„Mitarbeiter größte Gefahr für EDV“ titelte am 12.8.2000 die Augsburger Allgemeine. Weiter heißt es: „Die größte Bedrohung für die Sicherheit der EDV-Systeme von Unternehmen sind nicht die Angriff von fremden Computerviren, sondern die eigenen Mitarbeiter.“ Glaubt man der Analyse der Hamburger Unternehmensberatung Mummert und Partner, so sind ‚zwei Drittel aller aktiven oder unbeabsichtigten Systemangriffe in Deutschland auf Angriffe der eigenen Mitarbeiter zurückzuführen’. Selbst wenn absichtliche Sabotageversuche im Bereich der Schul-EDV eher selten anzutreffen sein werden, so zeigt doch die eigene Beobachtung, dass vielfach eigenes, unbeabsichtigtes Fehlverhalten zu einer großen Gefahr für den Datenbestand der Schule werden kann. Im Folgenden sollen einige grundsätzliche Fehlerquellen angesprochen werden:

2.1.1 Fahrlässige Systemänderungen

Die Rechnerräume und damit verbunden die Programme und Daten auf Servern und Einzelarbeitsplätzen werden vermehrt zur Grundlage für Unterricht. Es sollte daher eine Selbstverständlichkeit für jeden verantwortungsbewussten Systembetreuer sein, dass Änderungen am System nur zu vorher bekannt gegebenen Zeitpunkten und in planbaren Abständen durchgeführt werden, sofern die Eingriffe nicht zur Wiederherstellung der Funktionsfähigkeit des Systems unabdingbar sind.

Die Installation neuer Software oder von Software-Updates sollte vorher unbedingt auf einem anderen als dem ‚Produktions’-Rechner erfolgen und erst nach Sicherstellung der Lauffähigkeit des gesamten Systems übernommen werden.

2.1.2 Fehlende Dokumentation

Jede Änderung am System sollte dokumentiert werden. Damit kann sichergestellt werden, dass einerseits eine funktionierende Systemkonfiguration beschrieben und danach wiederhergestellt werden kann, andererseits ist sie notwendige Voraussetzung für den problemlosen Weiterbetrieb des Systems, wenn ein Wechsel bei der Betreuung des Systems, sei es durch die zuständige Firma oder den Systembetreuer vorgenommen wird.

2.1.3 Fehlende Datensicherung

In Verbindung mit einer ausreichenden Dokumentation sollte vor jeder Änderung am Server eine Datensicherung selbstverständlich sein, um auf den Stand vor der Änderung zurückkehren zu können. Für die Arbeitsplatzrechner gilt: Pro Client-Typ sollte eine Kopie des lauffähig installierten Betriebssystems und den lokal gespeicherten Programmen als Backup im Netz oder auf CD zur Verfügung stehen, um den Arbeitsplatz schnell wieder herstellen zu können.

2.2 Viren

2.2.1 Was für Viren gibt es?

Echte Viren

Ein Computervirus ist ein Programm, das sich selbst reproduzieren und Manipulationen an Dateien vornehmen kann. Die Benennung „Virus“ stammt von der Vergleichbarkeit hinsichtlich Ansteckung und eigener Reproduktion mit einem biologischen Virus.
Es gibt unterschiedliche Arten von Viren:

- **Programm-Viren** kopieren sich in Programm-Dateien und verändern die Befehlsfolge, so dass sie zuerst ausgeführt werden.
- **Boot-Viren** lagern den Inhalt der nicht sichtbaren Boot-Sektoren eines Datenträgers aus und schreiben sich selbst in diesen Bereich ein. Wird der Rechner neu gebootet, gelangt der Virus in den Arbeitsspeicher und kann so andere, nicht schreibgeschützte Datenträger infizieren.
- **Stealth-Viren** sind intelligente Programm-Viren, die bei Lesezugriffen auf Dateien den Originalinhalt mit den original Dateiinformationen zurückgeben. Dadurch wird der vom Virus erzeugte Unterschied nicht erkennbar.
- **Polymorphe Viren** verändern ihre Befehlsabfolge oder verschlüsseln diese, um das Entdecken ihrer charakteristischen Befehlsfolgen zu verhindern.

- **Makro-Viren** sind Programmroutinen, die in Dokumenten verborgen sind. Neuere Versionen von Microsoft Word und Excel beispielsweise erlauben, Makros in Visual Basic direkt in den Dokumenten zu speichern. Diese Viren sind im Gegensatz zu den anderen Typen plattformunabhängig. Das heißt, ein und derselbe Makro kann z. B. sowohl auf einem Macintosh als auch auf einem PC ablaufen, so das Programm, mit dem das Dokument erstellt wurde, installiert ist.

Unechte Viren

Hier geht es um sogenannte „**Hoaxes**“, einfacher Text, der als E-Mail in Umlauf gebracht wird. Der Inhalt der Mail kann die Warnung vor einem Virus sein oder auch die Aufforderung, einen Kettenbrief weiterzuleiten. Auch wenn von diesen Mails keine direkte Gefahr ausgeht, so sind die verbrauchten Ressourcen aufgrund unkontrollierbarer Massenverbreitung nicht zu unterschätzen.

2.2.2 Was tun Viren?

Nur ein geringer Teil der bekannten Computerviren sind mit absichtlichen Schadensroutinen programmiert. Viele sind vermeintlich harmlose „Scherz“-Viren, die nur durch Ausgabe von Meldungen, Bildern oder Ton den Nutzer des Rechners ärgern sollen. Häufig beinhalten diese Viren allerdings Programmierfehler, die zu Datenverlusten führen. Jeder Virus verursacht zumindest dadurch Probleme, dass er Arbeitsspeicher und Festplattenplatz belegt und den Rechner durch die Kontrolle der Schreib- und Lesezugriffe verlangsamt. Der größte Schaden entsteht eigentlich durch den Aufwand, die Viren zu suchen, ihre Herkunft festzustellen und sie zu eliminieren.

2.2.3 Wie kann ich mich schützen?

Grundsätzliches

Die wichtigste Maßnahme gegen jede Bedrohung durch Viren ist die Datensicherung. Von wichtigen Daten sollten mindestens 2 Sicherheitskopien auf separaten Datenträgern vorhanden sein.
Jegliche Art von Disketten sollten vor Gebrauch grundsätzlich geprüft und mit einem Schreibschutz versehen werden. Auch CDs können Viren enthalten, sogar wenn sich auf ihnen Originalsoftware befindet – selbst Microsoft hat schon verseuchte CDs in Umlauf gebracht. Daher ist es sinnvoll, neue CDs auch zuerst von einem Antivirenprogramm durchsuchen zu lassen.

Stand-Alone-Rechner

Auf jedem Computer sollte ein speicherresidentes Viren-Schutzprogramm laufen, das einmal monatlich auf den aktuellen Stand gebracht wird. Zum Schutz vor neuen Boot-Viren ist es zweckmäßig, die Boot-Reihenfolge im BIOS so einzustellen, dass grundsätzlich zuerst von dem Festplattenlaufwerk (z. B. C:) gebootet wird. Zusätzlich sollte man den Viren-Schutz im BIOS aktivieren.
Bei den Programmen WINWORD, EXCEL, ACCESS und POWERPOINT kann der Makro-Viren-Schutz aktiviert werden, sofern nicht ständig mit makrobehafteten Dateien gearbeitet werden muss.
Es ist günstig, den Windows Scripting Host zu deinstallieren. Dieser wird bei Windows 98 und 2000 automatisch installiert, bei den anderen Versionen kann er durch andere Programme (z. B. Internet-Explorer) nachträglich unbemerkt installiert werden.
Die Anzeige der Dateinamen sollte im Menü Ansicht/Optionen des Explorers auf „Alle Dateien anzeigen“ und „MS-DOS-Erweiterungen eingeschaltet“ stehen. Dadurch kann kein Virus unbemerkt die Festplatte mit Dateien füllen.
Einen starken Schutz für Festplatteninhalte, die nicht veränderbar sein sollen, bietet eine Protektorkarte. Nur die Bereiche, in denen Daten gespeichert werden können, müssen dann mit einem Virenschutz versehen werden.

Über ein LAN vernetzte Rechner

Für diese Rechner gelten die selben Regeln wie für Stand-Alone-Geräte. Zusätzlich sollte man darauf achten, dass beispielsweise in einem Windows-Netz die Freigaben nur lesend eingerichtet werden. Schreib-Freigaben können mit Passwörtern versehen werden.

Server

Da der Server der Dreh- und Angelpunkt in einem Netz ist, sollte sein fehlerfreier Betrieb gewährleistet sein. Auch und gerade hier gilt, dass regelmäßige Sicherungen überaus wichtig sind, um eventuell von Viren angerichtete Schäden auszubügeln. Um einem Virenbefall des Servers so weit wie möglich zu erschweren, sollten Schreibrechte sehr restriktiv vergeben werden. Auf Programmdateien braucht bei den heutigen Programmen kein Anwender mehr Schreibrechte. Ein Bereich auf dem Server, der mehreren Benutzern offen steht und von ver-

schiedenen Stationen einsehbar ist, birgt das Risiko einer Verbreitung etwaiger vorhandener Viren. Um auch in diesen Fällen geschützt zu sein, empfiehlt es sich, auf dem Server eine spezielle, für den entsprechenden Server entwickelte Antivirensoftware einzusetzen. Viele Firmen bieten ein aufeinander abgestimmtes Konzept von Antivirensoftware vom Server bis hin zu den Clients an.

Rechner am Internet

Der Rechner selbst sollte genauso abgesichert sein wie ein Stand-Alone-Gerät. Zusätzlich sind aber noch eine Reihe von anderen Punkten zu beachten. In Internet-Seiten gibt es sogenannte „aktive Inhalte“, die mit Hilfe von Java, JavaScript oder ActiveX dargestellt werden können. Java ist eine Programmiersprache, mit der grundsätzlich alles programmiert werden kann. Da direkte Zugriffe auf die Hardware durch das Sicherheitssystem der virtuellen Java-Maschine nicht erlaubt sind, ergeben sich dadurch Einschränkungen in Bezug auf die direkte Rechnermanipulation. JavaScript dagegen ist ein sehr eingeschränktes Werkzeug, mit dem nur Dinge innerhalb des Browsers programmiert werden können, etwa die Reaktion auf einen Mausklick (Menüs und Kontrollkästchen), die Anzeige von Datum und Uhrzeit oder die Berechnung von Werten innerhalb einer HTML-Seite. ActiveX bietet einen enormen Funktionsumfang, der gleichzeitig ein großes Sicherheitsloch darstellt. Den Kern von ActiveX bilden die ActiveX-Controls, das sind direkt ausführbare Software-Bausteine, die eine völlige Kontrolle über den Zielrechner ermöglichen. Ein Control besitzt bei Ausführung auf dem Rechner genau die Rechte des Benutzers, der gerade angemeldet ist. Mit diesen Controls ist es möglich, über OLE Programme auf dem Rechner zu starten und übertragene Dateien darin zu öffnen – mit allen Gefahren, die hier durch Makro-Viren entstehen. ActiveX läuft grundsätzlich nur auf 32bit-Windows-Umgebungen und hier nur im Microsoft-Browser Internet-Explorer.
Bei Internet-Browsern sollte daher die Ausführung von Java und ActiveX generell ausgeschaltet sein, da nicht auszuschließen ist, dass hier Schadfunktionen enthalten sind.
Um das ungewollte Verbreiten neuer Makro-Viren zu verhindern, kann beim Versand von WORD-Dokumenten das Rich-Text-File-Format (*.RTF) verwendet werden.
Der Versand von Dateien als Attachement sollte im Text der E-Mail erwähnt werden, um abzusichern, dass die Datei vom angegebenen Absender geschickt und nicht von einem Virus verbreitet wird.

2.2.4 Welche Programme helfen mir?

Firma	Programm	Plattformen	Bemerkung	Internet
H&B EDV	Antivir	DOS, Windows, OS/2, NetWare, Linux	Kostenlose Version für Privatanwender unter www.free-av.de	www.antivir.de
GDATA	AVK	DOS, Windows	Updates für 10 Jahre	www.gdata.de
PerComp, DataFellows	F-Secure	DOS, Windows		www.f-secure.de
Computer Associates	InoculateIT	DOS, Windows		www.cai.com
NAI	McAfee VirusScan, Dr. Solomons	DOS, Windows, OS/2, NetWare, Linux, Mac		www.nai.com
Norman Data Defense	Virus Control	DOS, Windows, OS/2, NetWare	Norman unterstüzt die Initiative „Schulen ans Netz“	www.norman.no/de
Symantec	Norton AV	DOS, Windows		www.symantec.com /region/de/

Die Erkennungsraten der Programme sind teilweise in Tests sehr unterschiedlich angegeben, was sich allerdings im Allgemeinen nach dem nächsten Update der Virendatenbank wieder ganz anders darstellt. Wichtig ist vor allem eine regelmäßige Aktualisierung der Software, die sonst keinen ausreichenden Schutz bieten kann.
Auf die Angabe von Preisen wurde verzichtet, da die Firmen sehr unterschiedliche Lizenzierungsmodelle und Preisstaffelungen haben.

Weitere interessante Internet-Adressen:

www.av-test.org
Projekt der Arbeitsgruppe Wirtschafts-Informatik am Institut für Technische und Betriebliche Informationssysteme der Otto-von-Guericke-Universität Magdeburg in Zusammenarbeit mit GEGA Software- und Medienservice

www.vhm.haitec.de
Die VHM ist ein privater Zusammenschluß von Antivirus-Forschern aus dem deutschsprachigen Raum, die Betroffenen von Computerviren Informationen und Hilfestellungen geben wollen.

www.tu-berlin.de/www/software/antivirus.shtml
Vielfältige Informationen zu Viren und Antivirus-Programmen

2.3 Angriffe aus dem Intranet

2.3.1 Zeitvergleich Intranet - Internet

Eine der, immer unter den am häufigsten genannten, Befürchtungen beim Anschluss der Schule ans Internet ist der Angriff von Hackern auf das Netz der Schule. Diese Gefahr besteht prinzipiell, muss jedoch deutlich relativiert werden. Um einen erfolgreichen Angriff aus dem Internet auf das System der Schule zu starten, sind mehrere Voraussetzungen unabdingbar:

- Der Angreifer muss Kenntnis darüber haben, dass die Schule zu einem bestimmten Zeitpunk online am Internet angeschlossen ist. Wird, wie bei den meisten Schulen, eine Wählleitung benutzt, die in Abhängigkeit von den Anforderungen im Netz der Schule die Verbindung jedes Mal ab- und wieder aufbaut, so ist diese Kenntnis nur schwer zu erhalten.
- Der Angreifer benötigt die IP-Adresse des Rechners, den er angreifen möchte. Auch hier sind wesentliche Hindernisse zu überwinden. Zum einen wechselt die IP-Adresse eines nicht verseuchten Verbindungsrouters üblicherweise bei jeder Verbindung zum Provider, wenn er diese dynamisch aus dem Vorrat von IP-Adressen des Providers bezieht. Zum zweiten erhält der Angreifer beim Einsatz eines Proxy-Servers oder NAT-fähigen Routers nur dessen gültige IP-Adresse, nicht die der im LAN dahinterliegenden Clients.
- Der Angreifer muss wissen, welches System er angreift (Betriebssystem, Serversoftware, Netzsoftware, Serverprogramme auf dem Zielrechner usw.). Dies erfordert zunächst Zeit und üblicherweise bereits die Überwindung einer Firewall in Form eines Proxy-Servers.
- Der Angreifer benötigt Kenntnis darüber, über welche Dienste bzw. Ports er auf den Zielrechner zugreifen kann. Um dies zu erreichen, wird üblicherweise ein sog. Port-Scanner eingesetzt, der als Ergebnis die benutzten Dienste ermittelt. Auch dies benötigt Zeit. Werden die unterschiedlichen Dienste zusätzlich im LAN auf unterschiedlichen Servern ausgeführt, auf denen zusätzlich unterschiedliche Software eingesetzt wird, so wird die Schwelle für einen erfolgreichen Angriff schon sehr hoch angesetzt.

Hier soll nicht verschwiegen werden, dass trotz dieser Hürden für erfahrene Hacker immer noch Möglichkeiten bestehen, in ein System einzudringen und Schaden anzurichten; Angriffe auf die Rechner großer Firmen und Organisationen bestätigen dies immer wieder. Wie jedoch aus den vorgenannten Bedingungen leicht ersichtlich, ist die Wahrscheinlichkeit für einen Angriff aus dem Internet auf Daten und Programme in einem hausinternen Netzwerk sehr gering, wesentlich geringer jedenfalls, als der Angriff aus dem hausinternen Netz selbst!

Beinahe alle der oben genannten Schwierigkeiten entfallen für diese zweite Angriffsmöglichkeit, wenn der Angreifer sich bereits im LAN befindet (beispielsweise an einem unbeaufsichtigten Rechner in Klassen- oder Fachräumen). Weder die üblicherweise nahezu unbegrenzt vorhandene Zeit noch die netztechnischen Hürden stellen vergleichbar hohe Ansprüche an den Angreifer. Daher ist auf den Schutz der wirklich kritischen Datenbestände (Schulverwaltung etc.) vor Angriffen innerhalb des Netzes ein besonderes Augenmerk zu richten. Die eigentliche Gefahr droht in den meisten Fällen von innen!

2.3.2 Beaufsichtigte und unbeaufsichtigte Arbeitsplätze

Für den Einsatz von Computern in den Klassen- bzw. Fachräumen gilt wie für jede Unterrichtssituation der Grundsatz, dass der Unterrichtende die Verantwortung für das Geschehen im Klassenzimmer trägt. Daher bilden die beaufsichtigten Arbeitsplätze ein wesentlich kleineres Problem.
Wie oben bereits erwähnt, sind vor allem unbeaufsichtigte Rechner mit entsprechender Ausstattung (TCP/IP-Anschluss) ein potenzieller Gefahrenherd. Ist aufgrund der Unterrichtssituation bzw. des Einsatzzwecks die Anbindung an das hausinterne Netzwerk unabdingbar, so sollte zum einen die Zeit unbeaufsichtigter Nutzung möglichst gering gehalten werden. Zum anderen empfiehlt es sich, die Zugriffe des Rechners transparent zu protokollieren, d. h. dass der Nutzer weiß, dass seine Tätigkeit im Netz an diesem Arbeitsplatz aufgezeichnet und nachverfolgt werden kann und wird. Empfehlenswerte Programme für diesen Zweck sind Programme wie SurfSpy oder Norton Internet Security.

2.3.3 Trennung der Netzsegmente

Einen wesentlichen Beitrag zur Absicherung schützenswerter Daten im schulinternen LAN bieten die Möglichkeiten des Netzwerks selbst. Bestehen in einem Netzwerk unterschiedliche Stufen von Datensicherheit, so sollten sie auch unbedingt technisch wie organisatorisch getrennt werden. Dies geschieht üblicherweise durch die Segmentierung in verschiedene Teilnetze, die über entsprechende Routing-Vorschriften voneinander getrennt werden. Sowohl bei der Planung als auch bei der Realisierung dieser Maßnahmen ist der Rat erfahrener Netzwerktechniker unabdingbar und kostengünstig im Vergleich zur Behebung eines einmal eingetretenen Schadens.

2.3.4 Fernzugriff

Im Zeitalter immer schneller werdender Telekommunikationseinrichtungen wurde und wird verstärkt der Wunsch laut, sich in das Netzwerk der Schule von außen einzuwählen, um Dateien zu übertragen, Unterrichtsvorbereitungen für den nächsten Tag abzuspeichern oder ausdrucken zu lassen oder das Netzwerk zu administrieren. Bei allem Komfort, den diese Möglichkeiten bieten, muss grundsätzlich festgestellt werden, dass sie ein erhöhtes Sicherheitsrisiko nach sich ziehen. Wenn auch die Möglichkeit, den Einwahlrechner außerhalb der Firewall zu platzieren besteht, die Anmeldeberechtigungen der Netzwerkbetriebssysteme immer ausgefeilter werden und die Zugangsberechtigungen über Passwörter u. dgl. begrenzt werden, so ist ein Netzwerk ohne Fernzugriffsmöglichkeit auf jeden Fall sicherer, als eines mit dieser Option. Ein verantwortlicher Systembetreuer sollte daher diese Möglichkeit nur dann einplanen, wenn sie unabdingbar ist und die Einwahlmöglichkeit auf jeden Fall auf der ‘unsicheren’ Seite der Firewall installieren. So kann beispielsweise über den Vergleich mit einer Liste von akzeptierten Rufnummern der Zugriff geöffnet werden.

2.4 Angriffe aus dem Internet

2.4.1 Schadenstypen

In der Literatur finden sich grundsätzlich mehrere Beschreibungen von Schäden, die durch Angriffe auf das System unterschieden werden können. Die wesentlichen sind (aus Erkennung und Behandlung von Angriffen aus dem Internet, Wolf, Häger, Schorn, Gastbeitrag in Handbuch zur Datenschutz CD, Klaus Utech, Juni 2000):

- Manipulation von Dateien (z. B.Veränderung/Löschung von Dokumenten)
- Außer-Betrieb-Nehmen der Dienste (Denial-of-Service) (z. B. Ausschalten eines WEB-Servers)
- Vorspiegeln falscher Identität (z. B. Versand einer E-Mail unter falschem Namen)
- Unberechtigte Vertraulichkeit erwerben (z. B. fremde Daten mitlesen)

2.4.2 Trojanische Pferde

Diese Form von Programmen führt neben der Funktion, die dem Anwender bekannt ist und die dieser durchaus wünscht (z. B. Fernwartung eines entfernten Systems über das Internet) noch weitere, verborgene Funktionen aus, die unberechtigten Personen die Manipulation von Daten auf dem befallenen System ermöglicht. Die bekanntesten Vertreter sind Programme namens ‘Back Orifice ‘ für Windows-95/98 oder ‘rootkit’ für Unix-Systeme.

2.4.3 Ausführbare Dateien auf dem lokalen Rechner

Hier muss unterschieden werden zwischen Cookies, JavaScript, JavaApplet, ActiveX und Activ Scripting: Cookies sind kleine Datenmengen, die in einem speziellen Verzeichnis (meist gleichen Namens im Systemverzeichnis) abgespeichert werden, um üblicherweise Benutzereinstellungen beim Besuch einer Web-Site auszulesen und damit zu personalisieren. Beispielsweise wird beim Besuch der Website einer Bank das Datum des letzten Besuchs abgespeichert, um beim nächsten Aufruf die Kontenauszüge ab diesem Termin anzuzeigen. Eine Manipulation von Daten im System durch Cookies selbst ist nicht möglich. Dennoch kann die Analyse der vorhandenen Cookies auf einem Rechner Aufschluss über das Nutzerverhalten auf diesem System ermöglichen.

Java-Script ist eine Scriptsprache der Firma Netscape, die plattformunabhängig die Mängel der Seitenbeschreibungssprache HTML ausgleicht. Wesentliche Funktionen der in den HTML-Code der jeweiligen Seite eingebundenen Script-Anweisungen sind Überprüfung von Eingaben, Behandlung von Bildschirmfenstern und Formularfunktionen. Eine Manipulation der auf dem Nutzersystem vorhandenen Daten durch Java-Scripts ist nicht möglich, dennoch wurden sowohl die Ausforschung von Nutzerdaten als auch die Überlastung von Rechnern als Sicherheitsprobleme erkannt.

Im Unterschied zu Java-Script sind Java Applets eigenständige Anwendungen, die in der Programmiersprache Java (Vorteil: plattformunabhängig) programmiert wurden und auf dem Anwendersystem ausgeführt werden können. Einzige Voraussetzung ist das Vorhandensein der JVM (virtuelle Java Maschine) auf dem Zielrechner. Applets aus dem Netz unterliegen sehr strengen Sicherheitskontrollen und können beispielsweise selbst keine

anderen Programme starten oder Systemfunktionen aufrufen. Nur durch Implementierungsfehler sind Angriffe auf das System möglich. Als Vorsichtsmaßnahme kann die Ausführung von Java-Applets im Browser gesperrt und nur im Bedarfsfall für zertifizierte Applets geöffnet werden.

Die größte Gefahr für Windows 95/98-Systeme geht von den sog. Active-Dokumenten aus: ActiveX Controls können als eigenständige Programme aufgerufen werden, Active Documents erlauben die Anzeige von Nicht-HTML-Dokumenten (z. B. Word- oder Exel-Dateien) und Active Scripting ermöglicht das Verwalten und die Kommunikation von ActiveX Controls. Alle 3 Funktionen stellen ein erhebliches Risiko dar und sollten, wenn nicht unabdingbar, tunlichst abgeschalten werden.

2.4.4 Formen von Hacker-Angriffen

Analog zur obigen Einteilung von Schadenstypen können verschiedene Formen von Angriffen benannt werden. Die wichtigsten Formen sind im Folgenden kurz beschrieben:

2.4.5 Portscanning

Jeder Dienst im Internet ist einem Port (virtuelle Schnittstelle) zugeordnet, da beispielsweise auf einem Server mehrere Dienste (WWW, FTP, SMTP...) angeboten werden können. Um herauszubekommen, ob und welche Ports auf einem Rechner geöffnet sind, kommen Portscanner zum Einsatz, die in der einfachsten Form die gesamte Liste der angebotenen Ports in einer Textdatei abspeichern und damit angreifbar machen. Um Portscanning auf dem angegriffenen Rechner zu entdecken, müssen die Log-Dateien von installierten Firewalls regelmäßig kontrolliert werden. Dies geschieht sinnvollerweise nicht manuell, sondern mit sog. IDS/IRS - Programmen (Intrusion Detection/Response). Diese erkennen Angriffsversuche automatisch und können, möglichst in Echtzeit, darauf reagieren. Danach kann versucht werden, über die IP-Adresse des Absenders zu klären, ob es sich um ein Versehen, einen legitimen Vorgang (z. B. Sicherheitsüberprüfung des Providers) oder um einen Angriff handelt. Ein Index der offiziell vergebenen Port-Nummern findet sich z. B. unter ftp://ftp.isi.edu/in-notes/rfc1700.txt

2.4.6 Hacking (z. B. eines HTTP-Servers)

Die Manipulation von Web-Inhalten kann auf mehrere Weisen erreicht werden. Einige wesentliche können unterschieden werden und arbeiten nach folgenden Prinzipien:

- Der Angreifer verschafft sich Zugang zum Originalrechner des Zielsystems z. B. über Portscanning (s. o.), den Einsatz von Sniffern (Programme, die den TCP/IP-Datenstrom mitlesen) oder massenhafte Versuche mit verbreiteten Passwörtern (Brute-Force-Attacke).
- Der Angreifer gibt seine eigene, manipulierte Webseite als die des Angegriffenen aus. Dabei kann der DNS-Server manipuliert werden (DNS-Spoofing) oder können Suchmaschinen so manipuliert werden, dass Anfragen an den Rechner des Angreifers gelenkt werden (Web-Spoofing).
- Der Angreifer manipuliert die IP-Pakete zwischen dem Anwender und dem korrekten Server.
- Der Angreifer sorgt für einen Ausfall des gesamten HTTP-Dienstes auf dem Server (Denial-of-Service-Attacke), indem er ihn mit einer massenhaften Verbindungsanfrage überhäuft. Dabei wird als Absender-IP die eines abgeschalteten Systems verwendet, um den angegriffenen Rechner in einen Wartezustand für jede einzelne dieser Verbindungen zu versetzen (SYN-ACK.Bit wird erwartet). Der für die Wartefunktion bereit gestellte Speicher lässt sich damit soweit reduzieren, dass der gesamte Dienst ausfällt.

3 Schutzmöglichkeiten

Welche Möglichkeiten gibt es, die Rechnersysteme einer Schule (Schulverwaltung und Unterricht) vor Missbrauch zu schützen?

3.1 Räumliche Sicherung

So selbstverständlich der Hinweis klingen mag, so oft wird er immer wieder missachtet. Räume, in denen Computer mit sensiblen Daten untergebracht sind, müssen physikalisch abgeschlossen und bei Bedarf mit zusätzlichen Sicherungen versehen sein. Alle logischen, softwaremäßigen Sicherheitseinstellungen helfen nicht, wenn der gesamte Rechner gestohlen oder die Festplatte ausgebaut und entwendet wird.

3.2 Physikalische Zugriffssicherung

Auf eine Festplatte, die nicht läuft, kann nicht zugegriffen werden. Diese einfache Wahrheit sollte genutzt werden, um physikalisch zu verhindern, dass Missbrauch mit schützenswerten Daten betrieben wird. So kann beispielsweise mit relativ geringem finanziellen Aufwand zusätzlich zu einer ersten Festplatte, die das Betriebssystem und wesentliche Programme enthält, eine zweite Festplatte zur Aufnahme der sensiblen Daten in einem Wechselrahmensystem installiert werden, dessen Stromzufuhr bei Nichtbenutzung der Daten mit dem eingebauten Schlüsselschalter unterbrochen wird. Bei Abwesenheit des Betreuers kann sie mit einem Handgriff entfernt und an einem sicheren Ort, beispielsweise dem Schulsafe, untergebracht werden.

Durch eine derartige Lösung ist sichergestellt, dass mit einem Gerät sowohl gefahrenfrei im Intra- und/oder Internet gearbeitet werden kann (bei abgeschalteter 2. Platte), als auch die zu schützenden Daten verarbeitet werden können, wenn die Platte eingeschaltet ist.

3.3 Passwörter

Zitat aus dem IT-Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik 2000:
„Folgende Regeln zum Passwortgebrauch sollten beachtet werden:

- Das Passwort darf nicht leicht zu erraten sein wie Namen, Kfz-Kennzeichen, Geburtsdatum.
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Das Passwort sollte mindestens 6 Zeichen lang sein. Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Passwort muss geheimgehalten werden und sollte nur dem Benutzer persönlich bekannt sein.
- Das Passwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt wird. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren (vgl. M 2.22 Hinterlegen des Passwortes).
- Das Passwort muss regelmäßig gewechselt werden, z. B. alle 90 Tage.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist.
- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.

Falls IT-technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern („BBBBBB“, „123456“) sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen.
- In Netzen, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpasswörtern.
- Nach dreifacher fehlerhafter Passworteingabe sollte eine Sperrung erfolgen, die nur vom Systemadministrator aufgehoben werden kann.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter nicht unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.

- Die Passwörter sollten im System zugriffssicher gespeichert werden, z. B. mittels Einwegverschlüsselung.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).

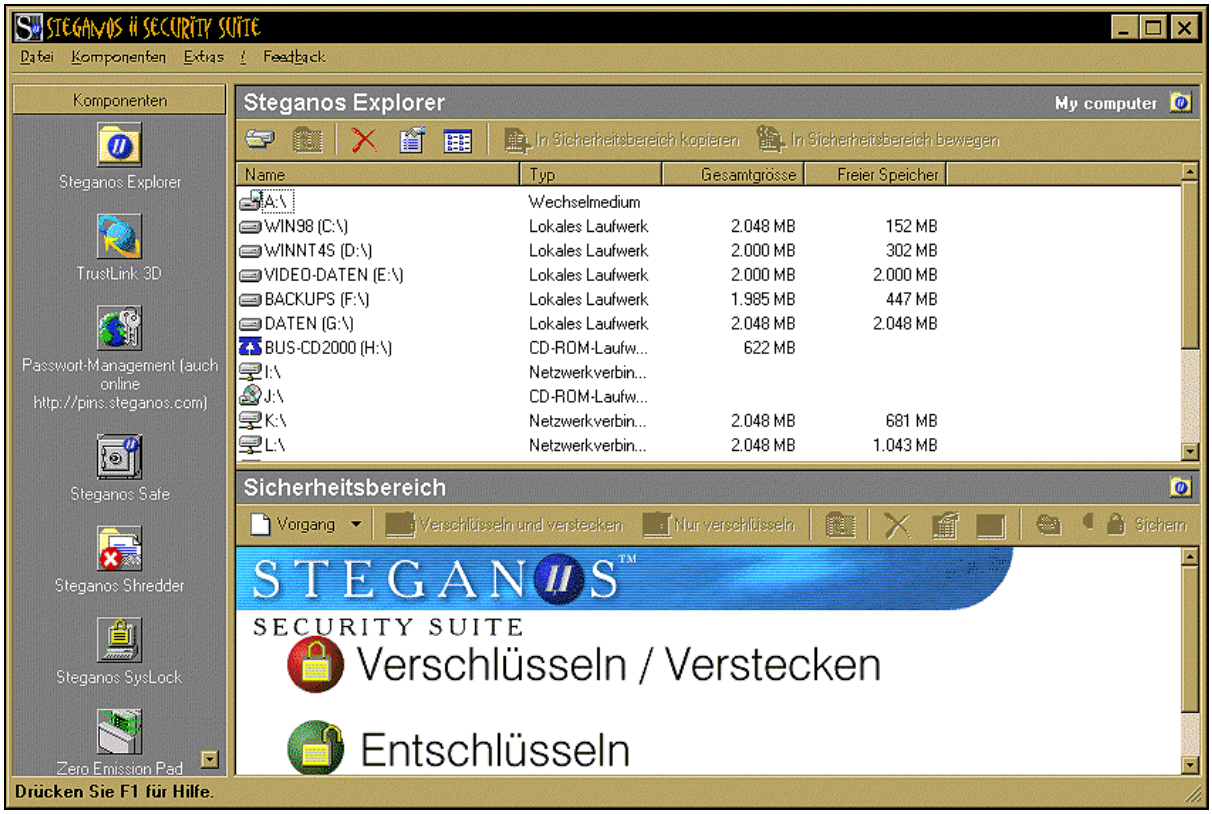
Ergänzende Kontrollfragen:

- Sind die Benutzer über den korrekten Umgang mit Passwörtern unterrichtet worden?
- Wird die Passwort-Güte kontrolliert?
- Wird der Passwort-Wechsel erzwungen?
- Ist jeder Benutzer im Netz mit einem Passwort ausgestattet? „

3.4 Softwarelösungen

3.4.1 Steganografie

Unter Steganografie versteht man das Verstecken von Daten in Dateien. Dazu werden die zu übertragenden Daten komprimiert und mit Hilfe eines Passworts verschlüsselt. Danach werden sie in eine bestehende, unverfängliche Text- oder Bilddatei so integriert, dass keine Veränderung sichtbar wird. Als Beispiel für ein komfortables und gleichzeitig sehr leistungsfähiges Produkt kann Steganos II Security Suite der Firma Demcom dienen.



Die Funktionsweise wird wie folgt beschrieben: ‚Steganos benutzt das am wenigsten signifikante Bit eines Datenelementes, um Daten darin zu verstecken. Ein Element sind 8 Bit (1 Byte) in einer 8-Bit-Datei und 16 Bit (2 Byte) in einer 16-Bit-Datei. Beispielsweise benutzt Steganos nur die niederwertigsten Bits der Bytes in einer 8-Bit-Wave-Klangdatei, um Daten in ihr zu verstecken. Da diese Veränderungen vom menschlichen Ohr nicht hörbar sind (z. B. wegen des Grundrauschens), sind diese Daten tatsächlich versteckt. Bei Bildern werden die Farben so geringfügig verändert, dass man die Veränderung nicht sehen kann. Steganos versteckt keine Daten im Header einer Trägerdatei. Der von DEMCOM entwickelte DyCeS-Algorithmus (Dynamic Cell Spreading) sorgt dafür, dass die zum Verstecken genutzten Bits gleichmäßig über die Trägerdatei verteilt werden. Dies erhöht die Sicherheit vor einer Erkennung erheblich. Der Algorithmus wurde speziell für das Verstecken in Bild- und Tondateien entwickelt. Um Daten in Textdateien zu verstecken, hängt Steganos Frei- und Tabulatorzeichen an die Zeilenenden an. Steganos versteckt so ein Byte pro Textzeile (die 8 Bit werden durch die Kombination von acht Freizeichen und Tabulatoren dargestellt). Im Unterschied zum Verstecken von Daten in Bildern oder Klängen, kann diese Methode leicht entdeckt werden.

Anwendungsbereiche:
Das interessanteste Modul der Suite ist SAFE. Das Programm stellt ein virtuelles Laufwerk zur Verfügung, in das die zu verschlüsselnden Daten mit herkömmlichen Dateioperationen kopiert oder abgespeichert werden können. Mit einem Mausklick in der Symbolleiste wird der Safe geschlossen, d. h. alle darin befindlichen Dateien werden verschlüsselt in der Datei namens SteganosSafe.sef abgespeichert. Diese wiederum kann nur von der Suite mit dem korrekten Passwort geöffnet werden. Ein so geartetes Laufwerk bietet sich für die Abspeicherung sicherheitsrelevanter oder personenbezogener Daten an, z. B. für Daten der Schulverwaltung. Damit wäre auch eine Forderung des Datenschutzbeauftragten des Landes Niedersachsen erfüllt, in der es zum Umgang mit Laptops heißt: ‘Zumindest personenbezogene Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen oder einen hohen Grad an Schutzbedürftigkeit aufweisen, sind verschlüsselt zu speichern. Damit soll erreicht werden, dass im Falle eines Diebstahls oder Verlustes des Gerätes die Daten für Dritte nicht verwertbar sind.’

Daneben können Dokumente jeglicher Art in geeignete Bild-, Ton- oder Textdateien versteckt und diese dann ohne Sicherheitsbedenken über das Internet als E-Mail-Attachements verschickt werden.

Die integrierte Passwortgenerierung bzw. -verwaltung könnte einen Beitrag leisten zur Verbesserung der Sicherheit bei Passwörtern, da sie zum einen auf Wunsch sichere Passwörter erzeugt und diese dann komfortabel zugänglich hält, ohne an Sicherheit einzubüßen.

3.4.2 PGP für E-Mail

Die bekannteste Art, sicher per E-Mail zu kommunizieren, ist die Verschlüsselung per PGP (Pretty Good Privacy). Das Programm stellt eine Lösung dar für die beiden wichtigsten Probleme bei schriftlicher Kommunikation im unsicheren Netz:

- Wie kann ich sicher sein, dass die E-Mail, die ich erhalte, auch von demjenigen stammt, der sie angeblich geschrieben hat? (Authentizität)
- Wie kann ich dafür sorgen, dass nur der Kommunikationspartner, den ich tatsächlich ansprechen möchte, die Nachricht auch lesen kann und kein anderer? (Geheimhaltung)

Das Verfahren beruht auf der Generierung von Schlüsselpaaren: Möchten zwei Briefpartner sicher miteinander kommunizieren, so werden pro Anwender 2 Schlüssel generiert, ein privater und ein öffentlicher.

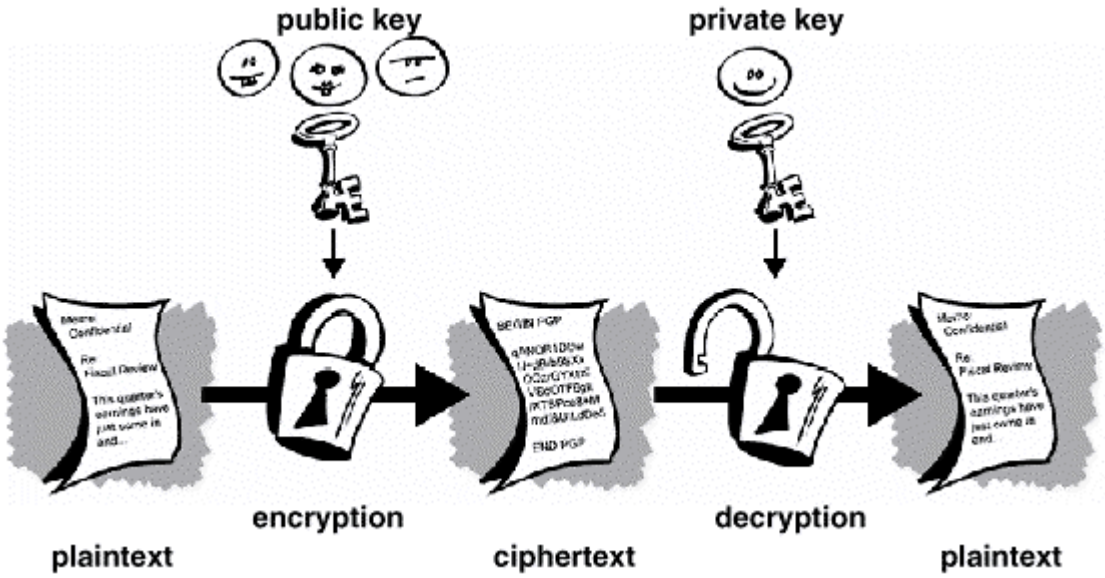


Abbildung: Funktion von PGP (aus PGP Users Guide)

Wie der Name schon sagt, hat auf den **privaten Schlüssel** nur der Eigentümer Zugriff. Er dient zum einen der Signatur der eigenen Texte und Dateianhänge. Dadurch ist sichergestellt, dass kein Fremder in der Lage ist, unter falschem Namen einen Text zu erstellen (Authentizität). Zum anderen dient er der Entschlüsselung von eingehenden, codierten Nachrichten:
Zum **Verschlüsseln** von Nachrichten dient der jeweils öffentliche Schlüssel des Adressaten. Ein mit diesem öffentlichen Teil des Schlüsselpaares codierter Text kann nur mit dem privaten Teil entschlüsselt werden, nicht mit dem öffentlichen. Dadurch ist sichergestellt, dass nur der Besitzer des privaten Schlüssels und kein anderer die Nachricht lesen kann. (Geheimhaltung).

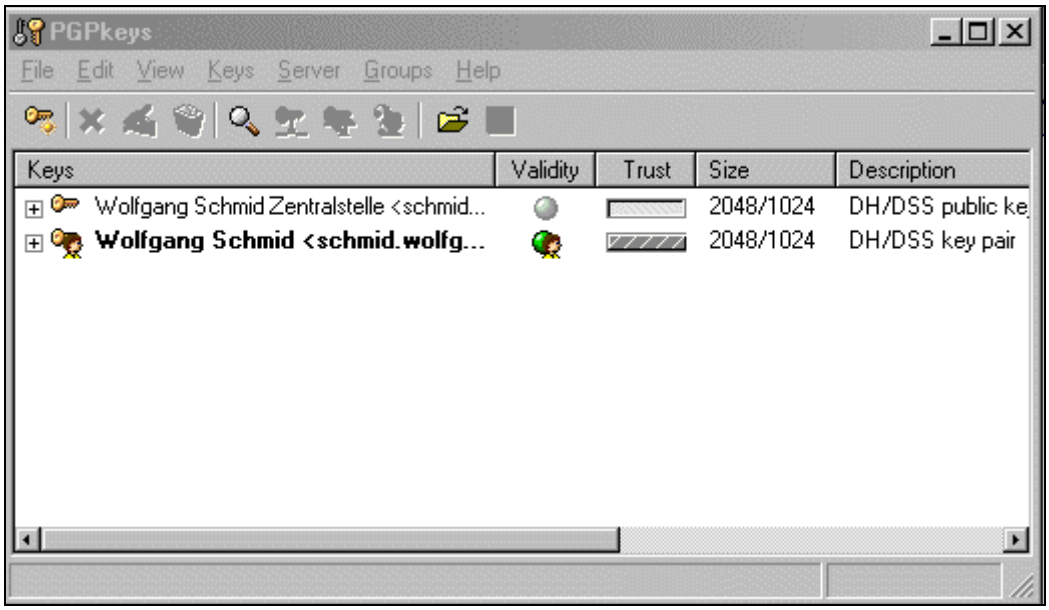


Abbildung: Verwaltung von privaten und öffentlichen Schlüsseln

Zur Aufbewahrung der öffentlichen Teile von Schlüsselpaaren dienen entsprechende Server (z. B. i-map://certserver.pgp.com), auf denen jeweils der Public Key hinterlegt ist und in denen entsprechende Such-funktionen bereit stehen. Er kann jedoch auch an E-Mails angehängt werden, damit der Kommunikationspartner nicht erst lange suchen muss.

Die Software selbst ist als Freeware für jedermann zugänglich (siehe http://www.pgpi.org/). Mittlerweile ist auch die Bedienung sehr vereinfacht worden. Es existieren sowohl für die E-Mail-Clients von Netscape, als auch für Outlook entsprechende Plug-In's, die Ver- und Entschlüsseln auf Knopfdruck ermöglichen:

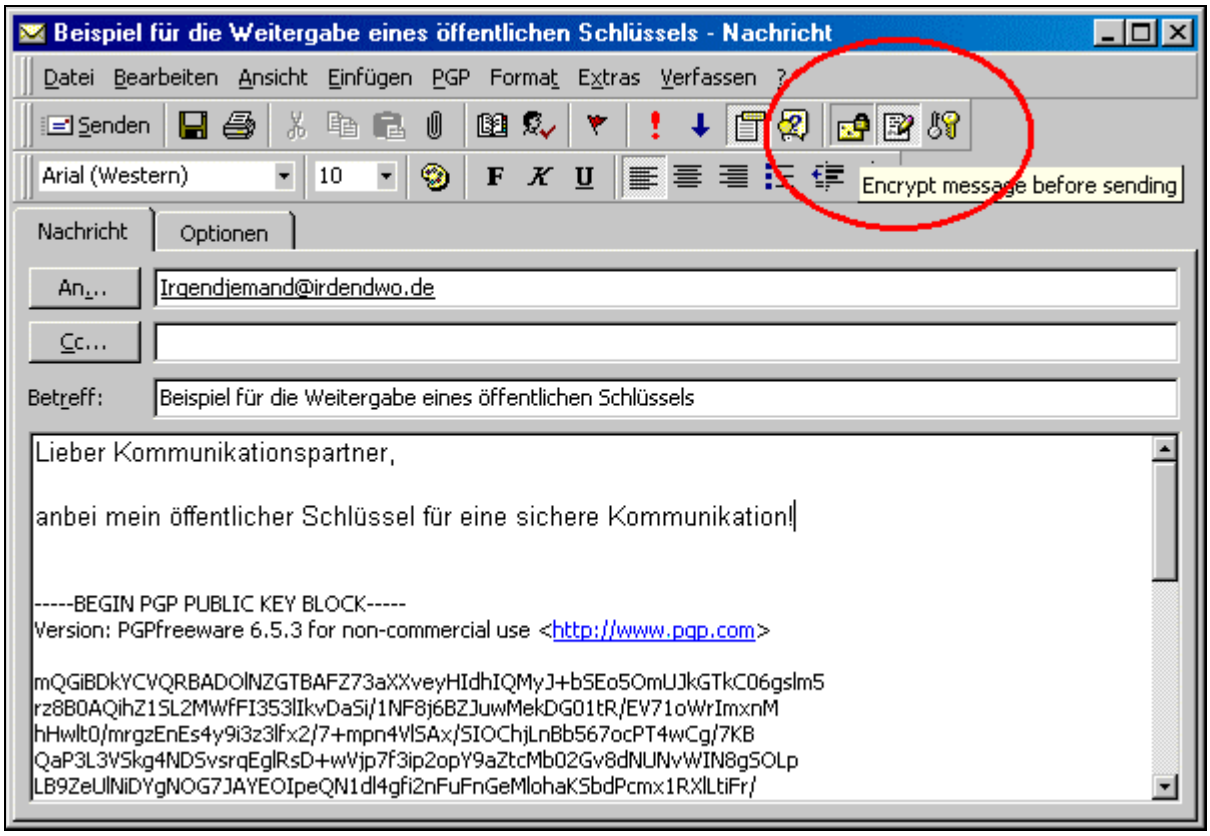


Abbildung: PGP-Funktionalität integriert in MS Outlook

3.5 Firewall

Die am meisten vorgeschlagene Lösung zum Schutz von Arbeitsstationen vor Angriffen aus dem Internet ist die Errichtung einer Firewall (engl. etwa Brandschutzmauer). Generell wird darunter eine „Anordnung von Hard- und Software verstanden, die als Übergang zwischen 2 zu trennenden TCP/IP-Netzen dient, von denen das eine einen höheren Schutzbedarf hat“ [Chapman95]. Neben der rein technischen Einrichtung sollten zusätzlich die Entwicklung einer passenden Sicherheitspolitik, die Protokollierung und das Management dieser Einrichtung berücksichtigt werden. Speziell die beiden letzteren, zeit- und personalintensiven Anforderungen können bei einer Schutzeinrichtung, die nicht nur Schutz suggeriert, sondern tatsächlich ernsthaft realisiert, nicht durch den Einkauf von Hard- und Software alleine erfüllt werden.

Technisch realisiert wird die Einrichtung einer Firewall durch Installation eines Softwarefilters (Packet-Filter bzw. Applikation-Gateway s. u.) am Übergang zwischen Internet und LAN (Local Area Network).

3.5.1 Funktionsweisen

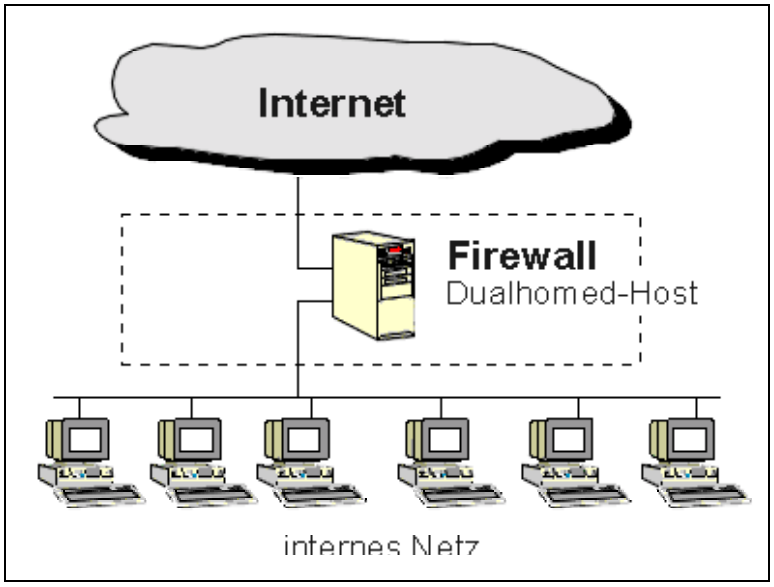


Abbildung aus ABB1: Firewall mit 2 getrennten IP-Bereichen (Dual-Homed)

Da die Firewall selbst auch angegriffen werden kann, ist es grundsätzlich sinnvoll, entweder dezidierte Geräte speziell für diesen Zweck einzusetzen oder auf multifunktional genutzten Geräten die installierten Anwendungen auf das absolute Minimum zu beschränken. Ohne auf die genaueren technische Hintergründe einzugehen (siehe dazu im Literaturverzeichnis Kai Fuhrberg, Internet-Sicherheit, München 2000), kann die prinzipielle Funktionsweise wie folgt beschrieben werden:

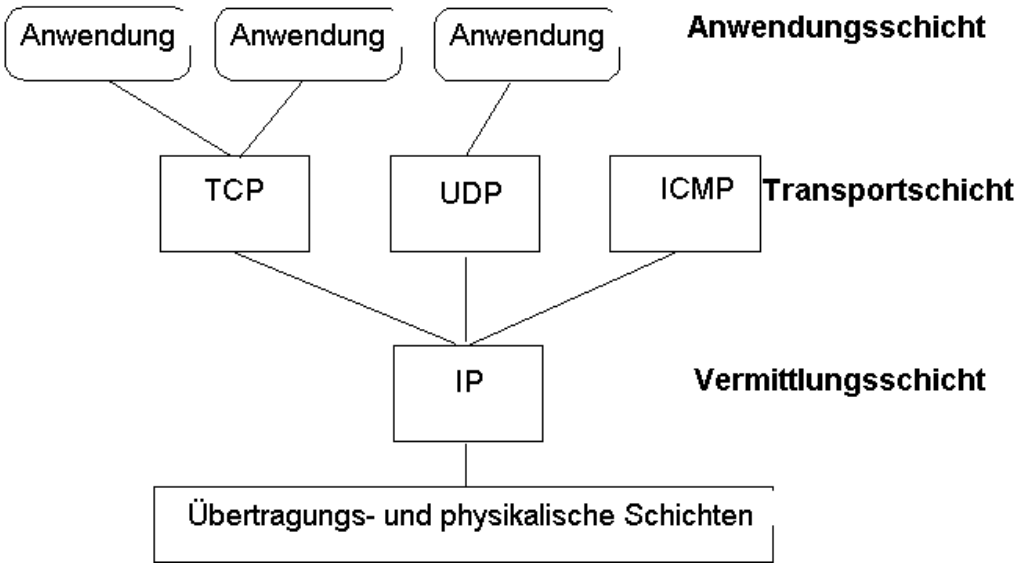


Abbildung aus ABB2: Schichten eines Filters

Daten, die in TCP/IP-Netzen (also z. B. im Internet) übertragen werden sollen, werden in Pakete zerlegt und vom Quell- zum Zielrechner verschickt. Die enthaltenen Absender- und Empfängerinformationen können an der Schnittstelle von LAN und Internet mit einer festgelegten Reihe von Bedingungen verglichen werden. Abhängig davon, ob die Bedingungen erfüllt sind oder nicht, werden die Pakete ins LAN bzw. Internet übernommen oder abgewiesen. Firewalls, die sich auf die Beachtung der Schichten 3 und 4 im ISO/OSI-Modell beschränken (Network-Layer und Transport-Layer), werden als Packet-Filter oder Firewalls der ersten Generation bezeichnet.

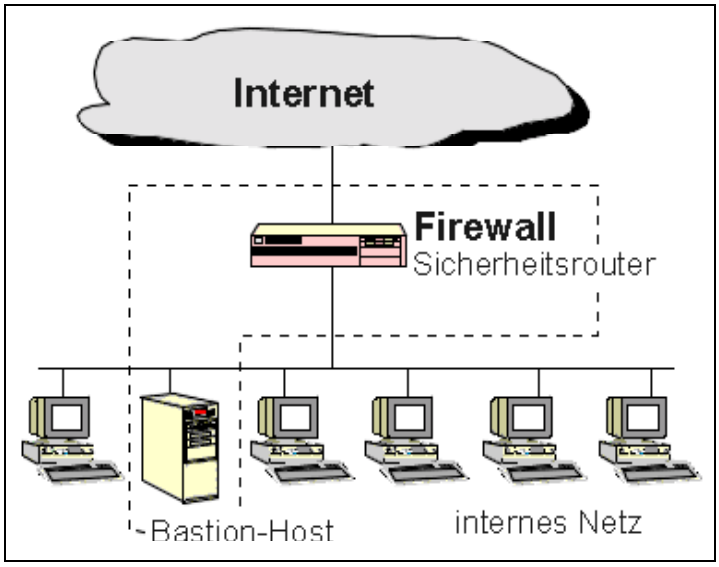


Abbildung aus ABB2:
Firewall als Applikation Filter (Bastion Host) mit zusätzlichem Paket Filter (Sicherheitsrouter)

Im Unterschied dazu verwenden sog. Applikation-Gateways zusätzliche Informationen aus Schicht 7 des ISO/OSI-Modells, der Anwendungsschicht (z. B. Authentisierungsinformationen oder spezifische Befehle der jeweiligen Protokolle). Typischer Vertreter eines solchen Gateways ist der sog. Proxy, auch als Proxy-Server bezeichnet, wenn er mehrere Proxies für die unterschiedlichen Dienste in einem Programm integriert. Ein Proxy stellt die Verbindung ins Internet in 2 getrennten Schritten her: Zunächst stellt der Anwender nur eine Verbindung zum Proxy her und übergibt diesem neben den Anmeldeinformationen auch das eigentlich im Internet anzuwählende Ziel (z. B. den URL einer Web-Seite). In einem getrennten Prozess baut nun der Proxy bei gültiger Authentisierung eine eigenständige Verbindung mit der Proxy-IP-Adresse als Absenderangabe zum Zielrechner im Internet her und erhält die angeforderten Informationen. Diese wiederum werden im ersten Prozess an den eigentlichen Client im LAN weitergegeben. Für das Internet ist nur der Proxy sichtbar, nicht der Client im LAN.

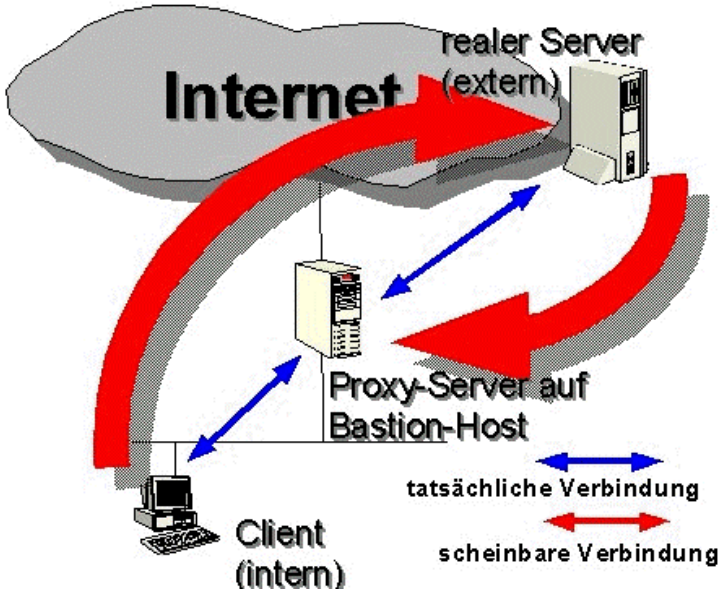


Abbildung aus ABB2: Funktion eines Proxy-Servers

Der Vorteil einer solchen Proxy-Lösung besteht in der Analyse der Nutzdaten, also der Daten, die sich nicht im Header der Datenpakete befinden. Dadurch ist beispielsweise eine sehr umfangreiche Protokollierung möglich, können Dienste benutzerbezogen erlaubt oder verboten werden oder bestimmte URLs gesperrt bzw. zugelassen werden. Wie umfangreich die Konfigurationsmöglichkeiten solcher Applikation-Gateways sein können, wird an den nachfolgenden Softwarebeispielen deutlich.

Die Komplexität einer Firewall-Installation richtet sich generell nach dem Schutzbedürfnis und den vorhandenen zu schützenden Ressourcen. Typische Beispiele für Firewall-Architekturen finden sich in [Fuhrberg], Seite 158 ff.
Speziell dann, wenn sich Datenbank- und/oder WWW-Server innerhalb des zu schützenden Netzwerks befinden, diese jedoch von außen per Standleitung erreichbar sein sollen, ist eine Kombination aus Paket-Filter und Applikation-Gateway empfehlenswert mit mehrfachen Netzwerkkarten, die zu einem jeweils unterschiedlichen Teilnetz gehören (Multi-Homed-Gateway).
Für weniger gefährdete Schulnetze mit Wählleitungsanschluss ans Internet dürfte die Installation eines Proxy-Servers für die notwendigen Dienste (HTTP, FTP, SMTP und POP3, NNTP) ausreichend sein.
Für einzelne Rechner im Bereich der Schulverwaltung kann zusätzlich oder, bei eigener Wählleitung, alternativ eine andere Form eines Applikation-Gateways eine Sicherheitslösung darstellen, wie z. B. ZoneAlarm oder Internet Security 2000 (s. u.).

3.5.2 Hardwarelösung Defendo

Die nachfolgend beschriebene Hardwarelösung DEFENDO der Firma Linogate basiert als eigenständiger Server auf der RedHat-Distribution von LINUX und bietet neben den ausführlicher besprochenen Sicherheitsfunktionen folgende Merkmale:

- Router (für den Anschluß eines oder mehrerer Netzwerksegmente an das Internet) mit NAT (Network Adress Translation)
- Proxy-Cache zur Zwischenspeicherung von WEB-Inhalten
- Web (HTTP)- und FTP-Server
- DHCP-Server (IP-Adressen für die Clients werden dynamisch vergeben)
- DNS-Server mit Cache (URL-Zuordnung zu IP-Adressen wird zwischengespeichert)
- Mail-Server für zeitgesteuerte Mailversorgung und interner Mailverwaltung

Die im Zusammenhang mit dieser Broschüre relevanten Sicherheitseinrichtungen erstrecken sich im Wesentlichen auf folgende Bereiche:

- Virenschutz
- Firewall
- Kontrolle der Inhalte durch Proxy-Cache

Virenschutz
Durch die Installation eines Proxy-Servers ist eine Kontrolle der über Internet eingehenden Inhalte (E-Mail, HTTP- und FTP-Dateien) möglich. Das System erledigt dies durch Integration der Virensoftware von McAfee, die vom Benutzer lizenziert werden muss. Der Server selbst kann so eingestellt werden, dass er in frei definierbaren Zeitabständen auf beliebigen Servern nach den jeweils aktuellen Versionen prüft, sie auf das System überspielt und installiert.

Firewall
Die in DEFENDO integrierten Möglichkeiten, den Zugriff von und in bestimmte Netzwerksegmente bzw. das Internet zu kontrollieren bzw. einzuschränken, erfüllen nach den bisher vorliegenden Erkenntnissen alle für einen technisch sicheren Internetzugang erforderlichen Bedürfnisse. Beim Einsatz mehrerer Netzwerkkarten ist es möglich, vollkommen getrennte Segmente (z. B. für die Schulverwaltung und das LAN der Schule) aufzubauen und voneinander so abzusichern, dass die jeweils gewünschte Zugriffsart ermöglicht wird:

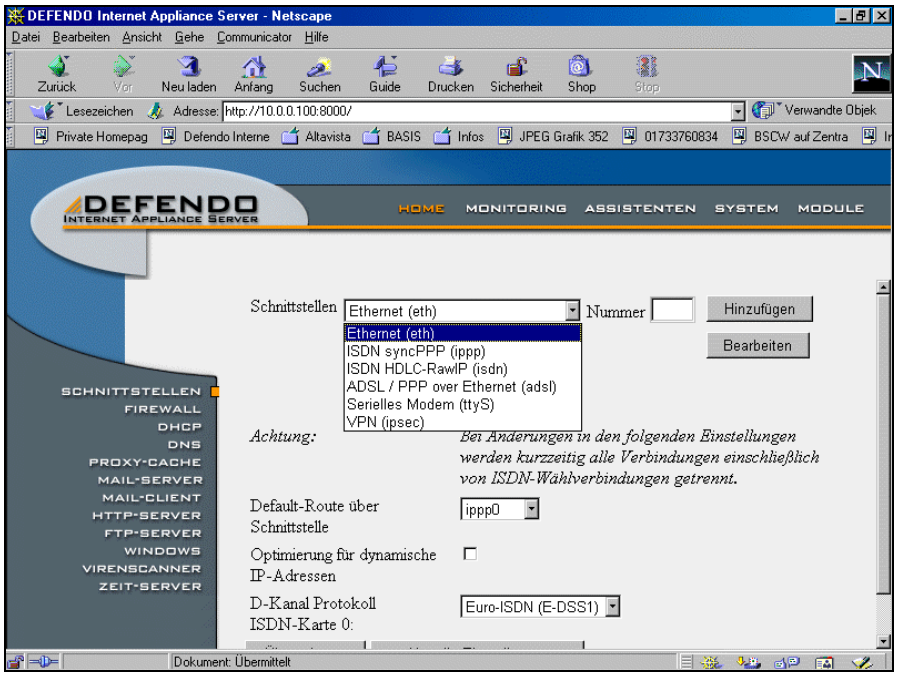


Abbildung: Defendo Schnittstellen

Bedingt durch die Komplexität der Materie an sich (Überlagerung von verschiedenen Protokollen und/oder Ports, Kontrolle ein- oder ausgehender Datenpakete, Routingvorschriften usw.) bietet das System 4 verschiedene sog. Vertrauensstellungen an, in denen die Sicherheitsstufen der Übertragung zusammengefasst sind:

- kein Vertrauen (Internet)
- gering (Demilitarisierte Zone)
- mittel (RAS)
- hoch (LAN)

Ziel dieser Zusammenfassungen von Rechten ist eine leichtere Adiminstrierbarkeit für den Systembetreuer. Die Funktionalität der Firewall ist dadurch jedoch nicht eingeschränkt. Ein erfahrener Anwender hat unabhängig von der pauschalen Einstellung die Möglichkeit, für jede Schnittstelle (Netzwerkkarte und/oder ISDN-Karte) die Einstellungen für IP-Adressen, Port, Netzmasken und andere Vertrauensstellungen in vielfältigster Weise zu konfigurieren:

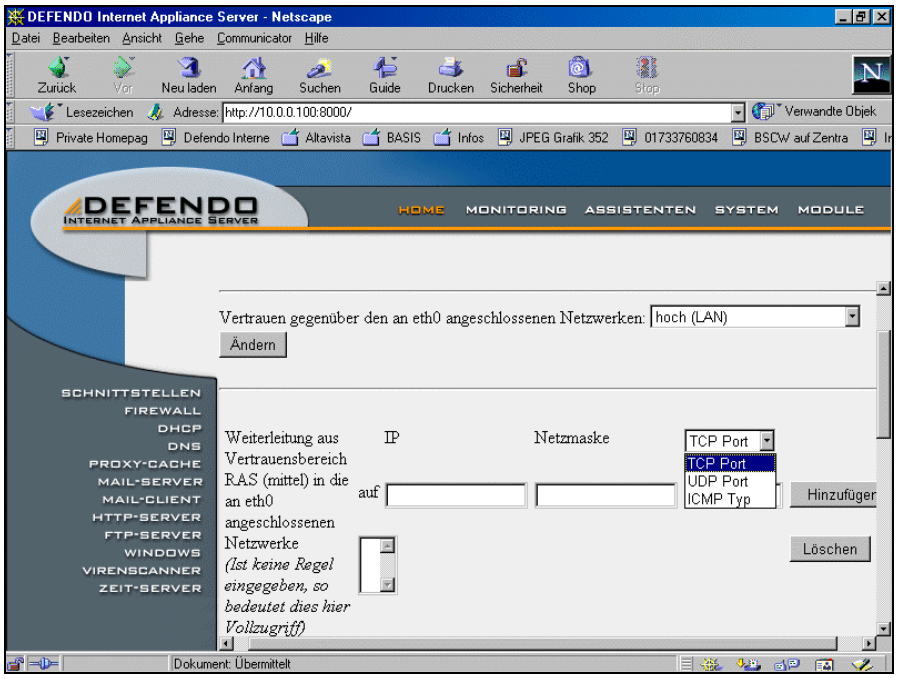


Abbildung: Defendo Firewall

Kontrolle der Inhalte

Neben der technischen Absicherung der Internetanbindung bietet DEFENDO auch eine Kontrollmöglichkeit der Inhalte, die aus den jeweiligen Netzwerken erreicht werden können. Dazu definiert das System drei verschiedene Kontrollmöglichkeiten:

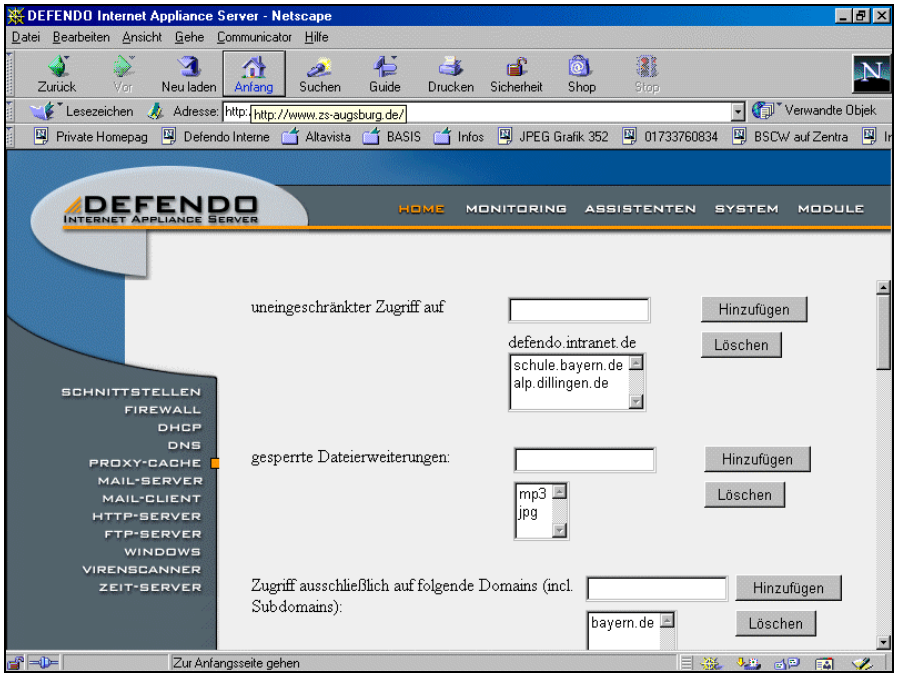


Abbildung: DEFENDO Zugriffsbeschränkung durch Proxy-Einstellungen

Uneingeschränkter Zugriff definiert die Bereiche, auf den jeder Nutzer ohne Einschränkungen Zugriff hat, unabhängig davon, ob anschließende Einschränkungen eingetragen sind. Dabei ist der Intranet-Bereich immer eingeschlossen.

Gesperrte Dateierweiterungen verhindern den Download unerwünschter Dateien (z. B.ausführbare Programme, Scripten oder Sounddateien).

Zugriff ausschließlich auf folgende Domains definiert eine sog. Positivliste bzw. White-List. Ist sie definiert und der uneingeschränkte Zugriff nicht definiert, so können nur URLs aus den eingetragenen Bereichen abgerufen werden.

3.5.3 Softwarelösungen

3.5.3.1 ZoneAlarm

Die beste Nachricht zuerst: das Programm steht als Freeware zur Verfügung und weist dennoch im Vergleich mit kommerziellen Produkten ein hohes Maß an Leistung auf. Es ist komplett in englischer Sprache abgefasst, kann aber im Wesentlichen über das grafische Interface konfiguriert und bedient werden.
Das Programm ist für den Einsatz auf einer lokalen Arbeitsstation gedacht und kontrolliert auf diesem Arbeitsplatz die IP-Verbindungen mit einem vorhandenen LAN (Local Area Network) bzw. mit dem Internet in beide Richtungen. Dazu teilt es die gesamte Arbeitsumgebung des Nutzers in zwei Bereiche ein: Privates Netzwerk (Local) und alles außerhalb (Internet). Für das private Netzwerk können beliebige „vertrauensvolle“ Hosts (auch im Internet), einzelne IP-Nummern, ganze IP-Bereiche oder Sub-Netze definiert werden, die dann als lokale Arbeitsstationen mit deren Sicherheitsumgebung behandelt werden. Alle einstellbaren Berechtigungen werden getrennt nach diesen beiden Bereichen vergeben.
ZoneAlarm besteht im Wesentlichen aus 2 Modulen:

- Security (bestimmt das Verhalten des lokalen PCs im Internet)
- Programs (bestimmt, welches Programm in welcher Weise Zugriff auf das private Netzwerk bzw. das Internet hat)

Daneben verfügt ZoneAlarm über die Möglichkeit, Zugriffe aus dem Internet zu protokollieren (Alert) und den gesamten Internet-Verkehr manuell oder automatisch (z. B. bei Abwesenheit) zu blockieren (Lock).

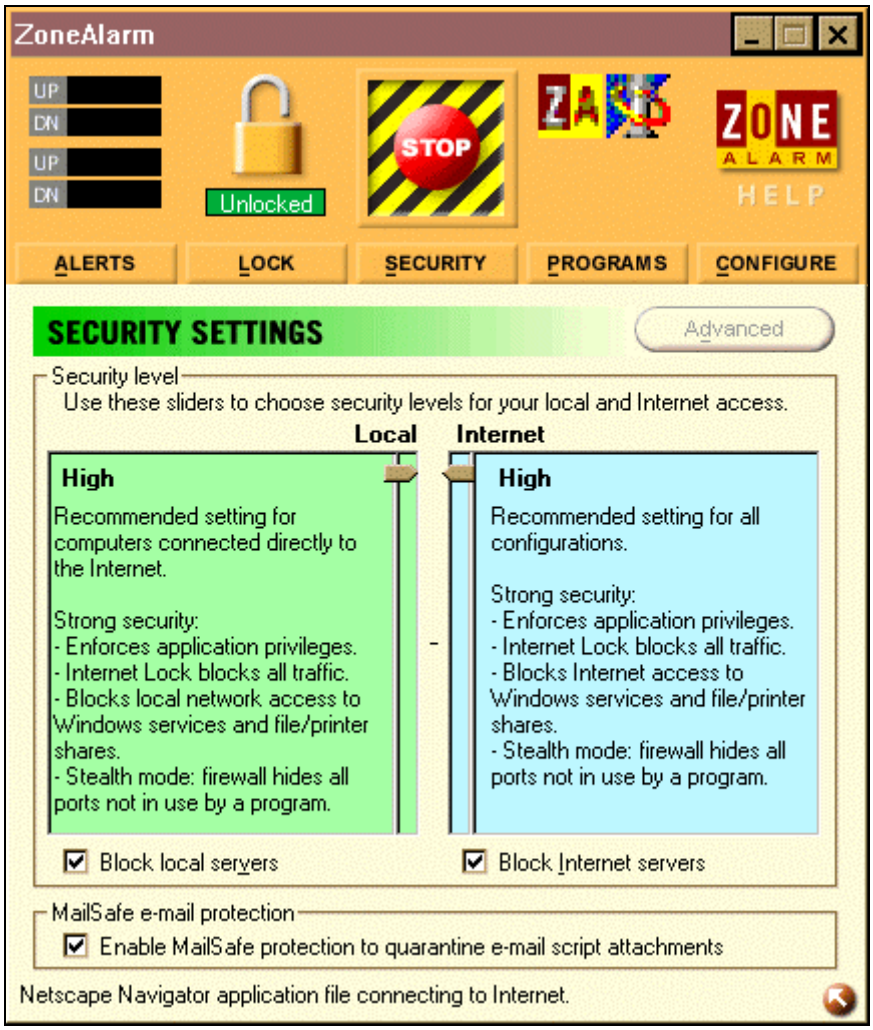


Abbildung: Modul Security

Ähnlich wie Norton Internet Security 2000 versucht das Programm, die komplexen technischen und organisatorischen Vorgänge bei der IP-gesteuerten Verbindung mit anderen Rechnersystemen in einfach zu steuernden Sicherheitsstufen zusammenzufassen. Es bietet, getrennt für lokales Netz und Internet, die Einstellungen High, Medium und Low. Dabei wird in der höchsten Stufe

- die lokale Arbeitsstation komplett (alle nicht benutzten Ports) hinter der Firewall verborgen (stealth mode),
- jeglicher Zugriff auf Windows-NETBIOS-Funktionen sowie lokale Windows-Ressourcen (Freigaben) blockiert,
- bei Einschalten der Funktion ‚Lock' jede IP-Verbindung ins und aus dem Internet unterbrochen und
- alle Applikationen auf Erlaubnis in der Definition ‚Programs' überprüft.

Entsprechendes gilt für die Verbindung ins private Netz. Die Sicherheitsfunktionen werden mit geringer werdender Stufeneinstellung reduziert. Die Programm-Einstellungen für den Zugriff aufs jeweilige Netz und die Lock-Funktion bleiben jedoch auch auf unterster Ebene erhalten. Ab der Version 2.15 ist eine Überprüfung von Dateianhängen an E-Mails integriert.

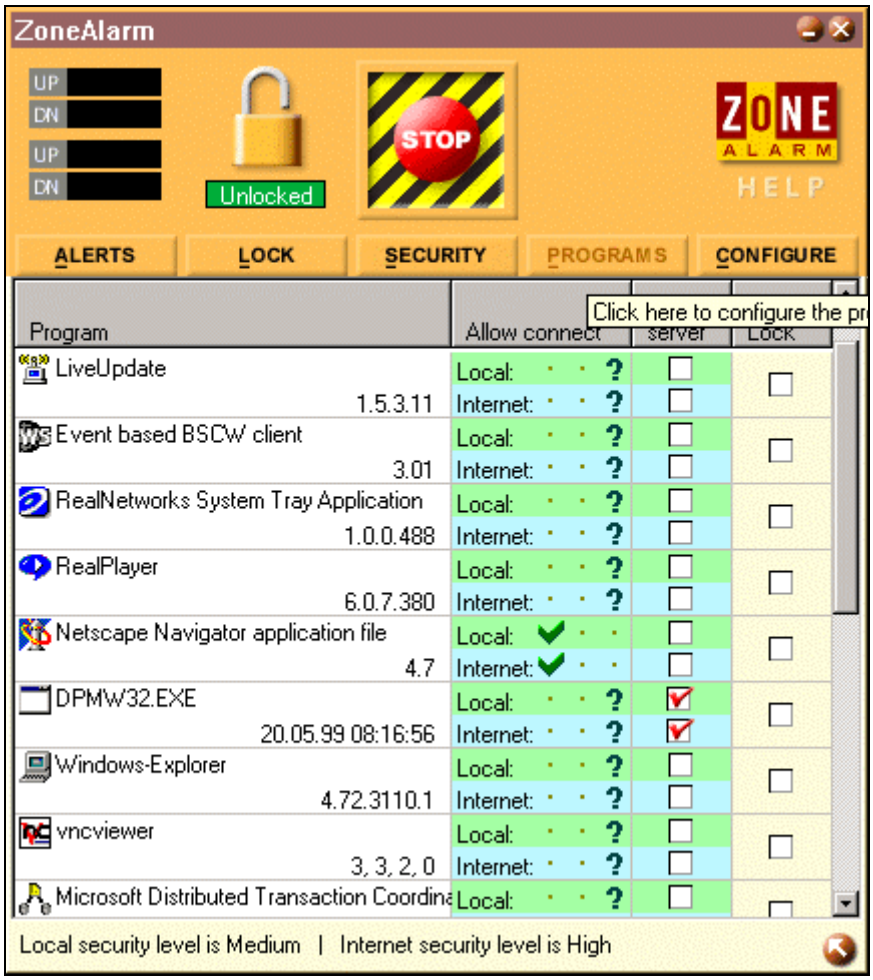


Abbildung: Modul Programs

Für jedes Programm, das über TCP/IP Zugriff entweder auf das lokale Netz oder das Internet benötigt, kann festgelegt werden, ob der Zugriff generell gewährt, generell verweigert oder nach Abfrage erlaubt werden soll. Dies geschieht im Regelfall beim ersten Aufruf des Programms. Zusätzlich kann für geeignete Programme (z. B. lokale Mail- oder Web-Server) definiert werden, ob sie als Server aus dem jeweiligen Netz angesprochen werden können und ob das Programm bei aktivierter Lock-Funktion dennoch mit dem jeweiligen Netz kommunizieren kann.

Anwendungsbereich

Das Programm dient der technischen Absicherung lokaler Arbeitsstationen auf Protokollebene. Es bietet keinerlei Funktionen, die die Inhalte der übertragenen Seiten überprüft oder bewertet. Es eignet sich daher vor allem zur Absicherung von Einzelrechnern, die selbstverantwortet im LAN und/oder Internet arbeiten und technisch gegen unerlaubte Zugriffe von außen gesichert werden sollen bzw. auf denen z. B. durch Fehlfunktionen verursachte Zugriffe ins Internet verhindert werden sollen. Die Erfahrungen beim Einsatz des Programms waren durchwegs positiv. Wie bei allen im Hintergrund arbeitenden Programmen ist von Zeit zu Zeit der Warnhinweis über angeforderte Zugriffe lästig, kann aber durch konsequentes Nutzen der Einstellungen für das jeweilige Programm erheblich gemildert werden. Gelegentlich trat der unerklärliche Effekt auf, dass ein Programm (z. B. Netscape Browser) kurzzeitig erst dann weiterlief, wenn ZoneAlarm abgeschalten wurde. Nach einem Neustart des Programms lief alles wieder reibungslos.

3.5.3.2 Norton Internet Security 2000

Die in deutscher Sprache vorhandene ‚Komplettlösung für Internet-Sicherheit' aus dem Hause Symantec bietet mit dem Programmmodul ‚Sicherheit' einen leistungsfähigen Baustein für eine sichere Verbindung zum Internet.

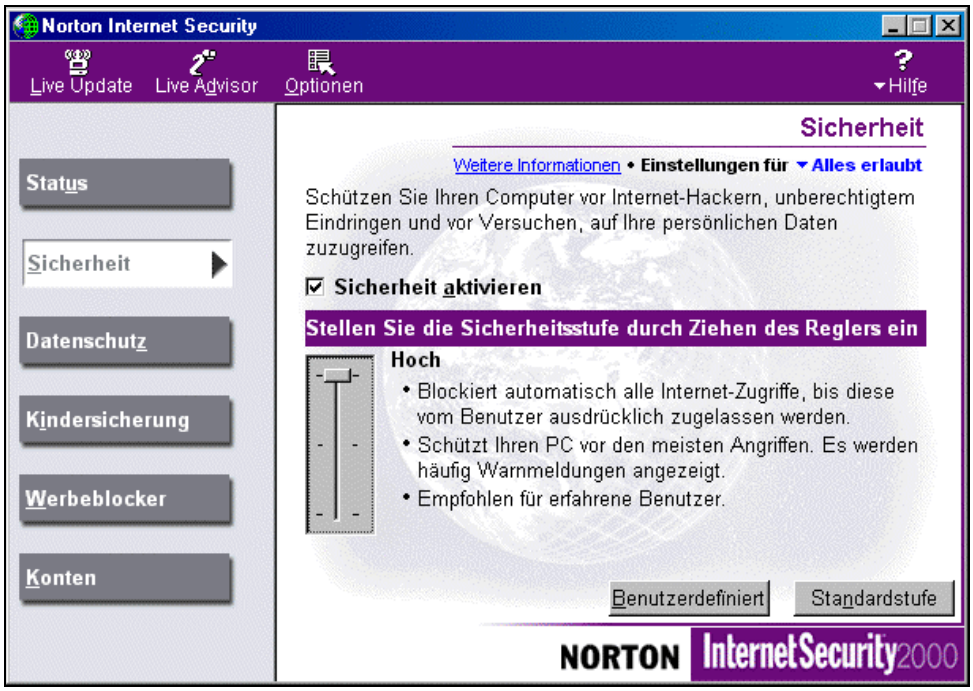


Abbildung: Gesamtbildschirm Sicherheit

Dabei versucht das Programm, die naturgemäß komplizierte und komplexe Materie dem am unkomplizierten Schutz interessierten Benutzer auf einfach handhabbare Weise zu präsentieren, indem die intern voreingestellten Schutzmechanismen in drei Gruppen von Sicherheitsstufen (hoch, mittel und niedrig) zusammengefasst werden. Der Benutzer muss sich, wenn er sich dieser Standardeinstellungen bedient, darauf verlassen, dass die Einstellungen sinnvoll vorgenommen wurden: die Beschreibung der einzelnen Stufen ist eher trivial und wenig aussagekräftig (Beispiel Hohe Sicherheit: ‚Schützt Ihren PC vor den meisten Angriffen. Es werden häufig Warnmeldungen angezeigt.').

Möchte der Nutzer detailliertere Einstellungen vornehmen, so kann er die Sicherheitseinstellungen in einer zweiten Stufe über den Menüpunkt ‚Benutzerdefiniert' erreichen:

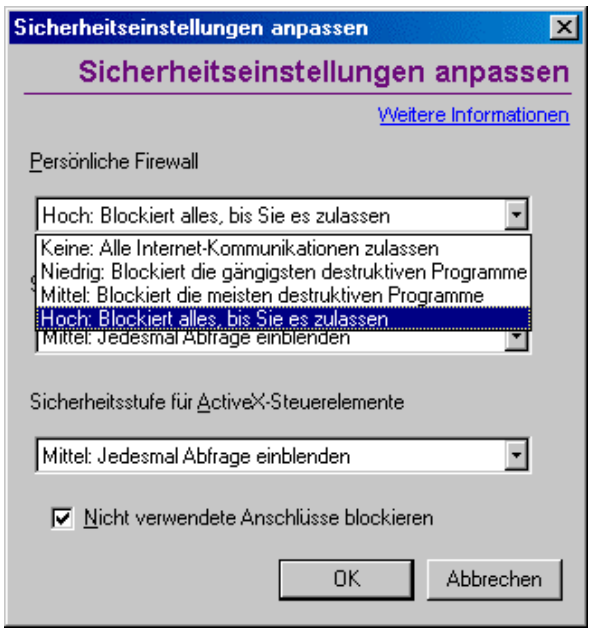


Abbildung: Benutzerdefiniert

Doch auch hier gehen die Einstellungsmöglichkeiten nicht weit über die der Standardstufen hinaus: Für Java-Applets und ActiveX-Elemente kann jeweils definiert werden, dass sie gar nicht, nach Abfrage oder jedes Mal akzeptiert werden. Zusätzlich können alle nicht verwendeten Anschlüsse (Ports) blockiert werden.
Die Definition für die persönliche Firewall ist begrifflich noch undifferenzierter: Der Unterschied in den Formulierungen ‚blockiert die gängigsten destruktiven Programme' und ‚blockiert die meisten destruktiven Programme' erschließt sich sicher erst nach längerem Nachdenken.

Die tatsächlich in hohem Maße eingebauten Sicherheitsoptionen des Programms können jedoch von erfahrenen Nutzern in vollem Umfang genutzt und ausgebaut werden, wenn sie über den Menüpunkt Optionen/Erweiterte Optionen/Firewall aufgerufen werden.

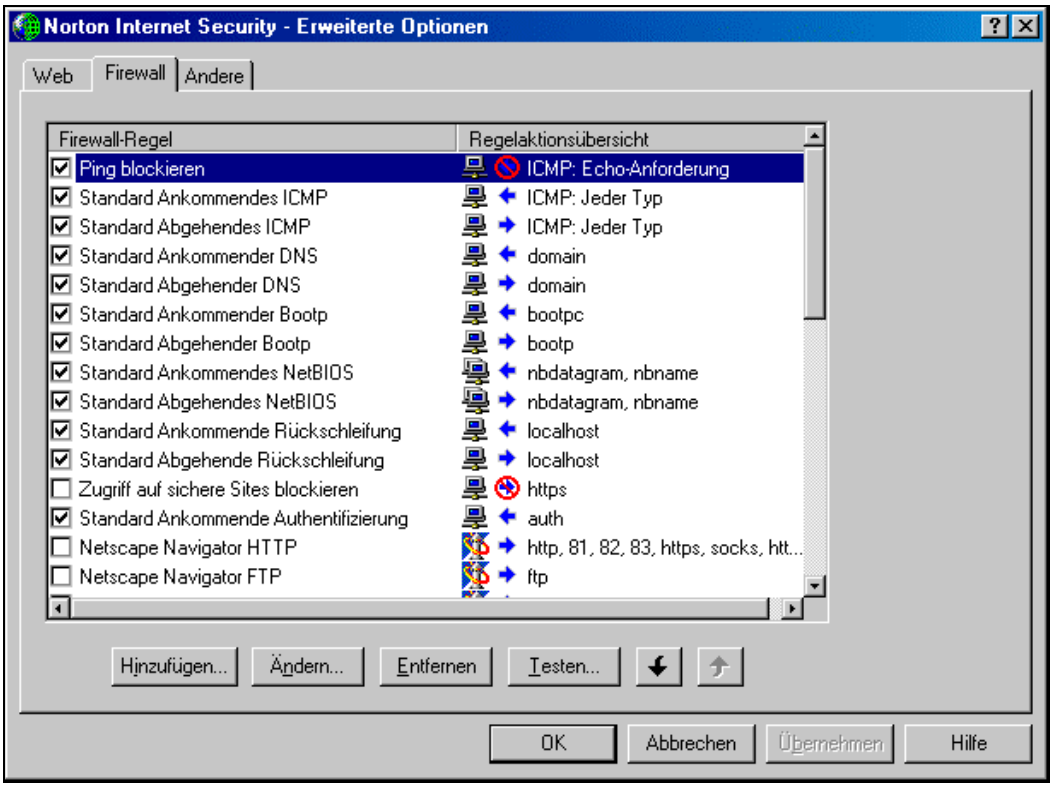


Abbildung: Firewalloptionen

Für jede sogenannte Firewall-Regel lassen sich Kommunikationsrichtung, Protokoll, Portadresse, IP-Adressbereiche von Absender und/oder Empfänger und Log-Option einstellen, so dass eine Vielzahl von Kontroll- und Einschränkungsmöglichkeiten bestehen. Zusätzlich kann jede dieser Regeln einer bestimmten Kategorie von Anwendungen zugewiesen werden, die dann wiederum im Rahmen der ‚Kindersicherung' für einzelne Benutzer(profile) gesperrt oder freigegeben werden können.

Erfahrungen beim Einsatz des Programms über längere Zeit liegen leider noch nicht vor. Demnach lässt sich auch nicht einschätzen, in welchem Umfang die Voreinstellungen für den an einfacher Bedienung und schneller Installation interessierten Benutzer auf Dauer Angriffe aus dem Internet abwehren. Nachdem jedoch zumindest die Option auf Anpassung und Erweiterung für jeden Anwender offen steht und über eine (nach einem Jahr kostenpflichtige) Updatefunktion evtl. auftretende neue Probleme abgefangen werden können, stellt sich das Programm als sehr leistungsfähig für den Einsatz am Einzelarbeitsplatz dar. Die Absicherung ganzer Schulungsräume bzw. Netzwerke kann angesichts einer fehlenden Multiplikationsmöglichkeit nicht mit vertretbarem Aufwand erreicht werden.

4 Internetinhalte

Neben der technischen Absicherung des internen Schulnetzwerks steht vor allem die Sorge um ‘sichere’ Inhalte bzw. der Schutz vor unerwünschten Angeboten beim Arbeiten im Internet im Vordergrund vieler Schulen. Dabei gilt es zu bedenken, dass dieses Netz von seinem Ursprung her als universitäres Netzwerk für Forschung und Gedankenaustausch angelegt war und sowohl seiner Struktur nach als auch vom Leitgedanken her auf möglichst wenig Beschränkung ausgelegt war und immer noch ist. Die jetzige Belastung des Netzwerks mit trivialen, kommerziellen und mehr und mehr gefährdenden Inhalten wurde bei der Konzeption der verwendeten Protokolle, technischen Realisierungen und konzeptionellen Grundlagen nicht implementiert und führt jetzt zu einem erhöhten Nachrüstbedarf in Hinsicht auf mehr Sicherheit.

Die Schule befindet sich dabei in einer grundsätzlichen Güterabwägung: Wird das eigentliche Ziel des Einsatzes von Internet im Unterricht ernst genommen, nämlich innovativ in einer projektorientierten Gruppe gemeinsam Inhalte zu finden, sie zusammenzutragen, zu diskutieren, zu bewerten und das Ergebnis in geeigneter Form für sich und Andere verfügbar zu machen, so erfordert diese freie, von vornherein kaum vorherseh- oder gar kontrollierbare Arbeit eine möglichst uneingeschränkte Freizügigkeit im Umgang mit allen Diensten, die das Netz anbietet. Die dabei auftretenden Probleme müssen auf anderem Wege als technisch restriktiv erkannt, aufgenommen und behoben werden. Das inhaltliche Gespräch und eine dauernde Betreuung der Lernenden in Verbindung mit vertrauensvoller Zusammenarbeit mit kompetenten Lehrern kennzeichnen eine derartige Unterrichtssituation.

Andererseits bestehen berechtigte Bedenken, an z. T. unkontrollierten Arbeitsplätzen (z. B. in Bibliotheken oder an Arbeitsplätzen für Facharbeiten oder Unterrichtsprojekte) allen zu jeder Zeit die gesamten Möglichkeiten des weltumspannenden Netzwerks ohne Beschränkung zur Verfügung zu stellen. Können unerwünschte Inhalte natürlich zu jeder Zeit auch außerhalb des Internet beschafft oder auf privaten oder öffentlich zugänglichen Rechnern außerhalb der Schule erreicht werden, so stellt sich für die in den Räumen der Schule und in deren Verantwortung beschafften Inhalte eine erhöhtes Maß an Verantwortung. Selbst wenn Juristen über rechtliche Verantwortung evtl. unterschiedlicher Auffassung sein sollten, so wird jeder an sinnvoller Erziehung Interessierte einen in diesem Sinne verantwortlichen Umgang mit den beschafften Inhalten nicht ablehnen wollen.

Welche Möglichkeiten gibt es also, unerwünschte Inhalte möglichst auszuklammern?

4.1 Verwendung lokaler Kopien im Intranet

Die sicherste und zudem kostengünstigste Lösung besteht darin, lokale Kopien der Inhalte aus dem Internet auf dem internen Netz abzuspeichern und im Unterricht nur mit diesen Kopien zu arbeiten. Dabei kommen verschiedene Verfahren zum Einsatz:

WWW2LOC

Funktionsweise:
Das Programm liest den lokalen Zwischenspeicher eines Arbeitsplatzes aus und bietet die Möglichkeit, die dort gefundenen Inhalte als lokale Kopie inhaltlich geordnet abzuspeichern und allen zentral zur Verfügung zu stellen. Bei den nachfolgenden Zugriffen wird die Kopie auf der Serverplatte statt des Originaldokuments abgerufen.

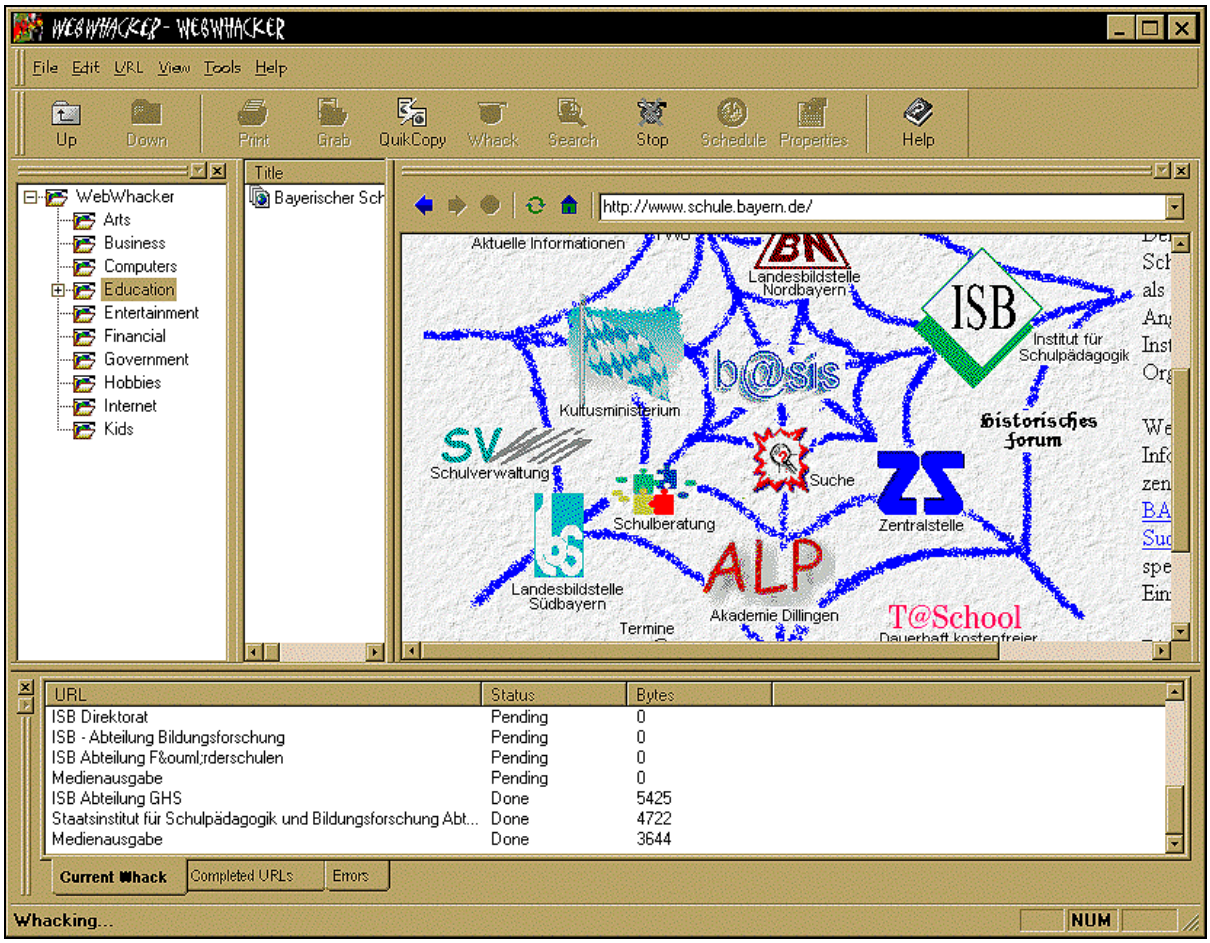


Abb.: Webwhacker (Quelle z. B. http://www.tucows.de/offline95_rating.html):

Funktionsweise:

Die sogenannten OFFLINE-BROWSER-Programme kopieren, ausgehend von einer Ursprungsseite im Internet, alle zugehörigen Inhalte bis zu einer einstellbaren Verschachtelungstiefe auf die lokale (Server-) Festplatte, ohne dass ein ‘Vor-Surfer’ alle entsprechenden Seiten manuell aufrufen oder gesehen haben muss. Externe Links auf diesen Seiten können bei Bedarf ebenfalls verfolgt werden (meist beschränkt auf eine Zielseite). Im Unterschied zum oben genannten Verfahren kopiert ein solches Programm sozusagen ein komplettes ‘Wandergebiet’ auf die lokale Platte, während bei WWW2LOC nur der ‘Wanderpfad’ des ‘Vor-Surfers’ zur Verfügung steht.

Die Vorteile solcher Lösungen sind neben der bereits erwähnten Sicherheit und Kostenreduktion (es fallen nur einmalig beim ‘Vor-Surfer’ Kosten an) vor allem eine gesteigerte Sicherheit und Geschwindigkeit. Der Schüler kann mit der Geschwindigkeit der lokalen Ausstattung (LAN bzw. Festplatte) nur die Inhalte aufrufen, die ihm von der Schule zur Verfügung gestellt werden und muss sich daher auf diese konzentrieren. Eine wie auch immer geartete Belästigung mit Unerwünschtem ist nahezu ausgeschlossen.

Die Nachteile einer jeden derartigen OFFLINE-Lösung liegen bei einer wie oben beschriebenen Ausrichtung des Einsatzes von Internet ebenso deutlich auf der Hand: Es handelt sich nicht wirklich um Anwendung des Internet im eigentlichen Sinne, sondern um die Verfügbarmachung von Seiten, die ursprünglich zwar aus dem Internet stammen, in gleicher Weise jedoch auch von CD-ROM oder anderen Datenträgern geladen werden könnten. Zudem ist der Zugriff auf den Dienst WWW (HTTP-Protokoll) beschränkt: interaktive Anwendungen wie das Lesen von Newsgroups, Chat oder E-Mail können nicht zur Verfügung gestellt werden. Auch die kopierten HTML-Seiten selbst weisen Nachteile auf: sie sind weder authentisch (der eigentliche URL ist nicht mehr erkennbar) noch aktuell, was besonders bei sich schnell ändernden Inhalten einen derartigen Einsatz beeinträchtigt. Auch ist die Erschließung von Inhalten nicht wirklich innovativ, sondern es werden nur die Inhalte verwendet, die aus den zwangsläufig beschränkten Kenntnissen des ‘Vor’-Surfers resultieren. Dadurch wird eine selbständige Erweiterung der Wissensbasis nicht gefördert.
Als Anwendungsbereich bieten sich für den Einsatz dieser Programme in erster Linie bereits bekannte, relativ stabile Inhalte (z. B. Angebote von Museen, statistisches Material aus der Vergangenheit oder geografische Daten) in ausreichend großem Umfang an, wenn sie z. B. für Einführungsveranstaltungen oder Erarbeitungsphasen mit fester Ergebnismenge eingesetzt werden.

4.2 Protokoll-Programme für den Internet-Zugriff

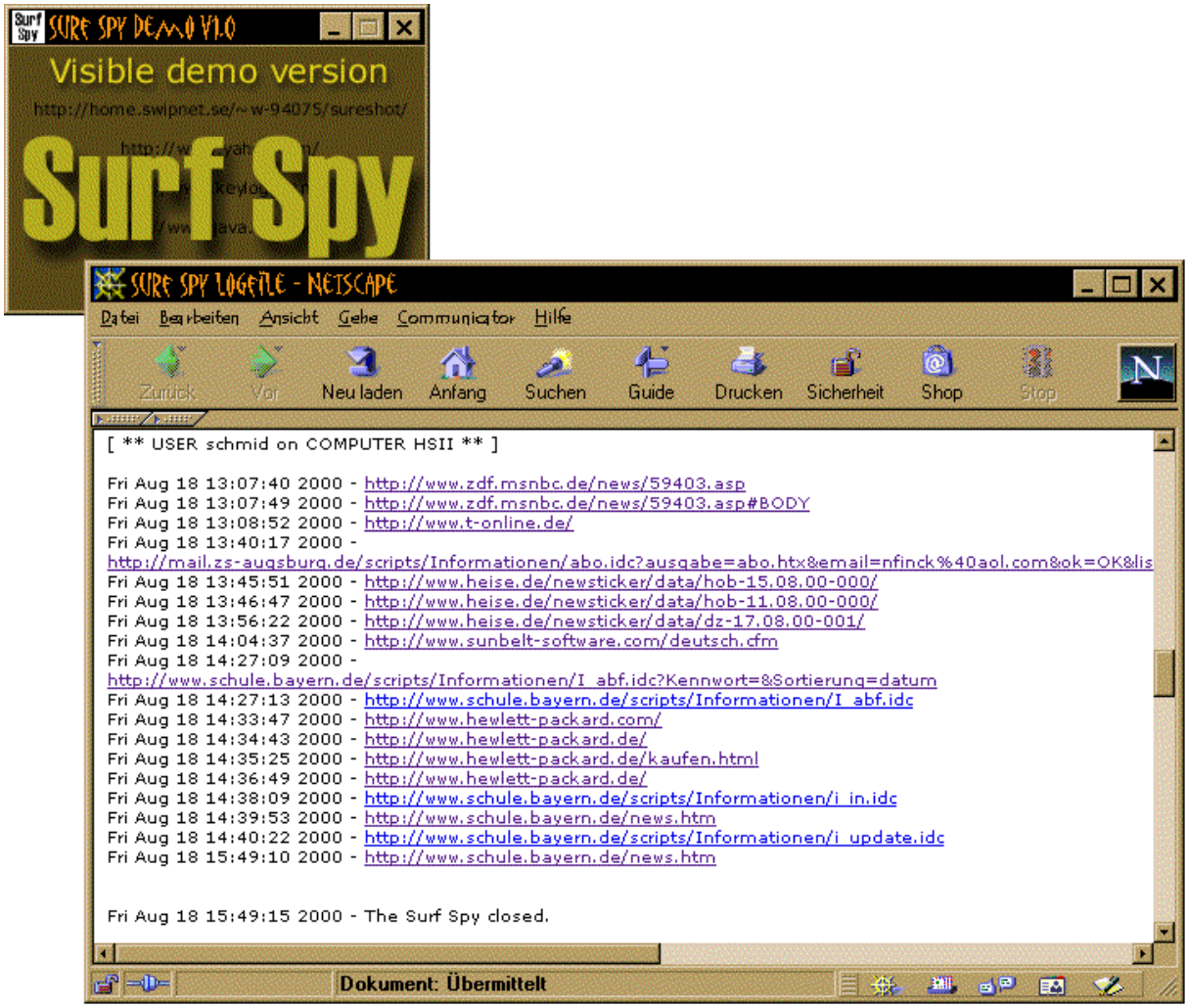


Abbildung: Protokoll Surf Spy

Eine erste Stufe der Regulierung von Internetzugriffen kann durch Bewusstmachung von Dokumentationsmöglichkeiten erfolgen. Dabei wird weder ein Zugriff reglementiert noch blockiert, es wird lediglich die Möglichkeit vorgestellt, dass je nach Installation bestimmte oder alle Zugriffe ins Internet protokolliert werden und eine Anonymität nicht oder nur eingeschränkt gewährleistet ist. Dadurch bereits entsteht bei vielen Nutzern eine freiwillige Beschränkung auf problemfreie Inhalte, Irrtümer immer ausgeschlossen. Als selbstverständliche Voraussetzung für den Einsatz von derlei Programmen sollte sich von selbst verstehen, dass die Nutzer VORHER über den Einsatz und den Umfang dieser Dokumentationen unterrichtet werden.

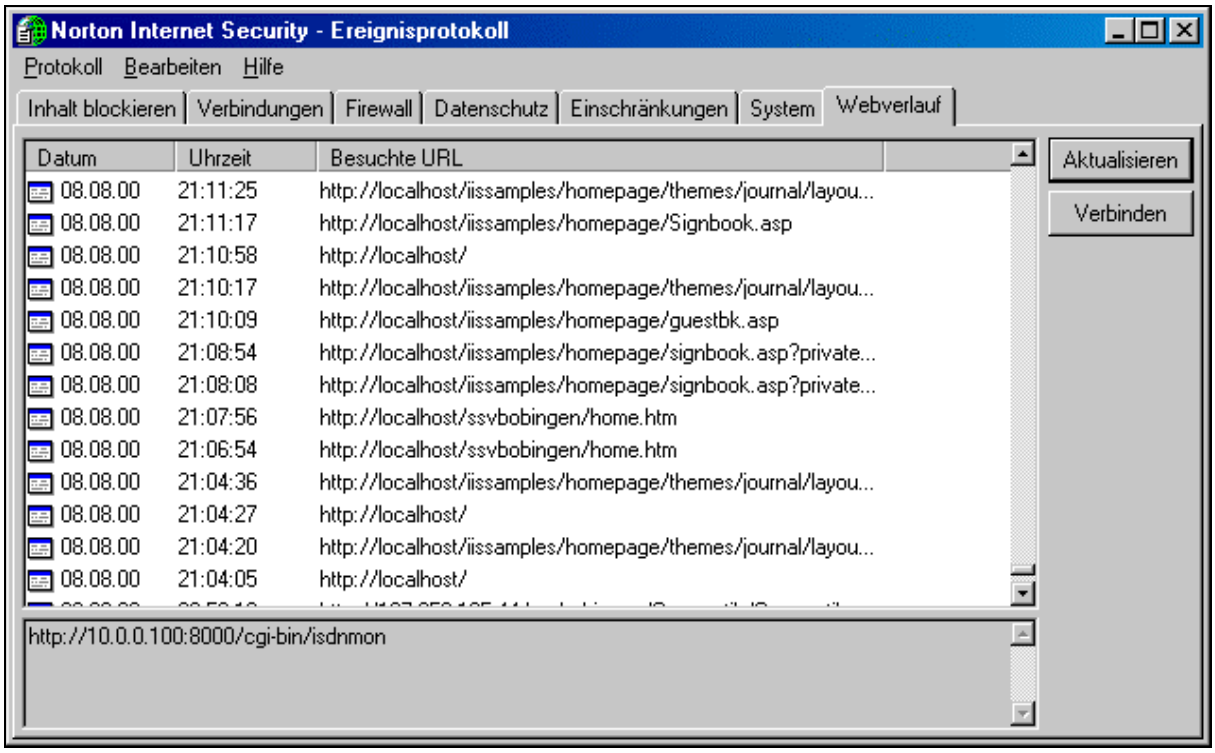


Abbildung: Norton Internet Security 2000

Neben dem evtl. problematischen Geruch der Schnüffelei bieten diese Programme keinerlei Sicherheit dagegen, dass unerwünschte Dienste nicht in Anspruch genommen werden bzw. unerwünschte Inhalte trotzdem aufgerufen werden. Sie sollten demnach nur dafür eingesetzt werden, wofür sie gedacht sind: der Überwachung eines Systems, nicht dessen Nutzern.

4.3 Proxy-Server mit Negativ/Positivlisten

Die technische Funktion eines Proxy-Servers besteht darin, dass er die Anfragen eines Nutzers im LAN der Schule nicht ungefiltert ins Internet weiterreicht, sondern unter seiner eigenen IP-Adresse und damit als Bevollmächtigter oder Stellvertreter (daher der Name) weitergibt. Die Tatsache, dass damit jede Information ins und aus dem Internet durch diese Schleuse muss, wird in mehrfacher Hinsicht genutzt. Zum einen können beim Transport von HTML-Seiten diese in einen Zwischenspeicher (Cache) des lokalen Servers kopiert und dort für einen nochmaligen Zugriff gespeichert werden, was die Geschwindigkeit des zweiten Zugriffs wesentlich erhöht. Zum anderen kann bei der Weitergabe kontrolliert werden, ob die gewünschte Adresse im Netz (URL) mit einer vorher festgelegten Menge an erlaubten Adressen (Positivliste) oder verbotenen Adressen (Negativliste) übereinstimmt. Je nach Definition wird beim Vorliegen von Kongruenz die Information geblockt oder ins Netz weitergegeben.
Die meisten der gängigen Proxy-Server verfügen über die Möglichkeit, solche Listen zu definieren. Dabei ist es je nach Programm auch möglich, sog. Wildcards oder Platzhalter zu verwenden. Eine Positivliste mit der Definition ‘*.bayern.de’ würde beispielsweise nur Zugriff auf alle Seiten innerhalb der Domain bayern.de erlauben (also schule.bayern.de ebenso wie sport.bayern.de), eine Negativliste mit der Definition ‘*.com’ würde alle Domains mit der Endung .com ausschließen.

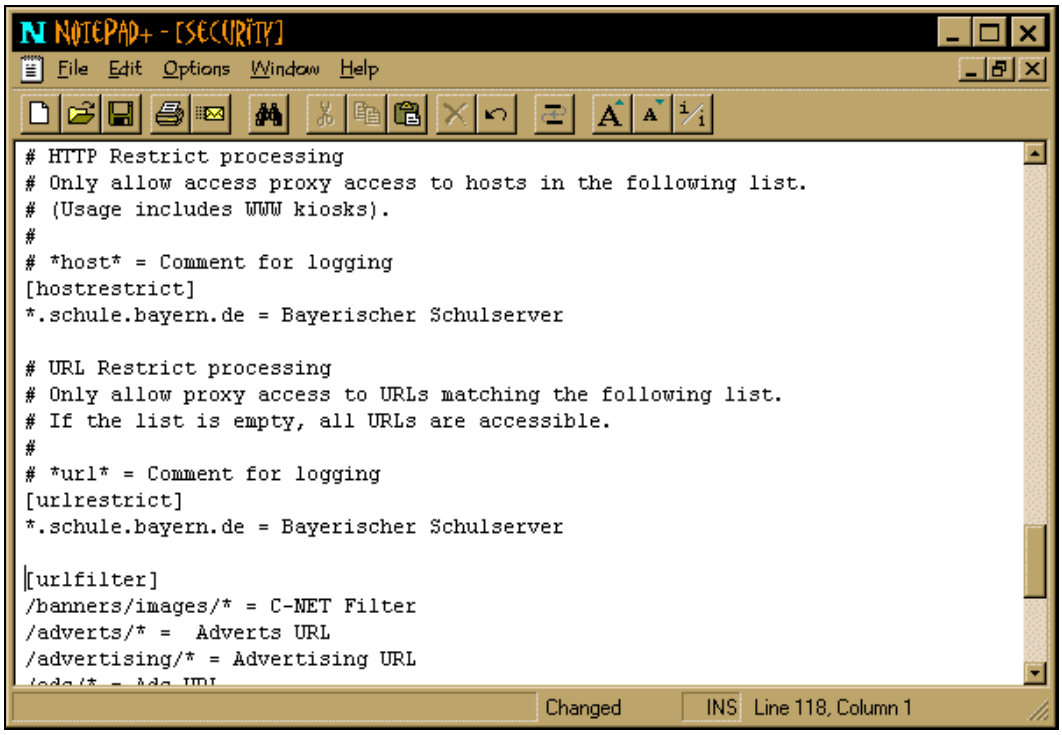


Abbildung: Beispiel: secuity.ini des Freeware-Proxy-Servers Sambar

Die Zuordnung zu einem leicht merkbaren URL zu der eigentlich entscheidenden IP-Adresse erfolgt durch das sog. DNS (Domain Name System). Dabei wird auf einem entsprechenden Server jeweils einer IP-Nummer ein URL zugeordnet (Beispiel 137.250.135.247 → http://www.zs-augsburg.de). Damit entsteht bezüglich der Sicherheit das Problem, dass zwar der Aufruf eines URL beim Vorhandensein in der Negativliste geblockt würde, die unerwünschten Inhalte jedoch über die direkte Eingabe der IP-Nummer nach wie vor erreichbar wären. Bei der Verwendung einer Proxy-Lösung zur Absicherung gegen unerwünschte Inhalte ist daher darauf zu achten, dass sowohl der URL, als auch die zugehörige IP-Nummer (z. B. über einen Vergleich beim DNS-Server) geblockt wird.
Die Einrichtung eigener Negativlisten stößt sehr schnell an Grenzen. Bei der explosionsartigen Vermehrung der im Internet angebotenen Inhalte ist es unmöglich, auch nur einen Großteil der unerwünschten Adressen zu erfassen und zu blockieren. Darüber hinaus besteht die Gefahr, dass die unerwünschten Angebote auf zunächst unverfängliche Web-Adressen kopiert werden (z. B. auf private Homepages der schulischen Nutzer) und dort nur schwer gefunden würden. Dem Einfallsreichtum solcher Umgehungsstrategien sind erfahrungsgemäß kaum Grenzen gesetzt.
Auch der Einsatz anderer Dienste als HTTP (speziell die Weitergabe über Newsgroups von sog. ‘freien’ Newsservern oder FTP-Server und spezieller Software wie ‘Napster’ für Musik) erzwingt weitergehende Maßnahmen. Diese Programme sind z. T. so weitgehend automatisiert, dass die Nutzung am Bildschirm kaum mehr sichtbar ist bzw. so versteckt erfolgen kann, dass auch ein aufmerksamer Beobachter sie kaum mehr wahrnimmt.
Es erscheint daher anzuraten, beim Einsatz von Proxylösungen Positivlisten zu formulieren (Streng nach dem Grundsatz: Was nicht ausdrücklich erlaubt ist, ist verboten.) und diese im Laufe der Zeit und nach Überprüfung von Unbedenklichkeit zu erweitern. Welche URLs aufgenommen werden, sollte sich nach den jeweils schulischen Erfordernissen richten. Eine Liste aller in der Datenbank BASIS des Bayerischen Schulservers aufgenommenen URLs kann bei Bedarf erstellt und als Grundlage für eine solche Positivliste abgerufen werden.

4.4 Kommerzielle Wächtersysteme

Für die Überwachung einzelner lokaler Computer werden zunehmend Softwarepakete angeboten, die sich unter der Bezeichnung ‚Kinderschutz' zusammenfassen lassen. Drei der bekanntesten Vertreter werden im Folgenden dargestellt.

4.4.1 Cyber Patrol

Eine der am besten bewerteten Überwachungsprogramme ist regelmäßig das Produkt der Firma Surfwatch Software, CYBER PATROL.

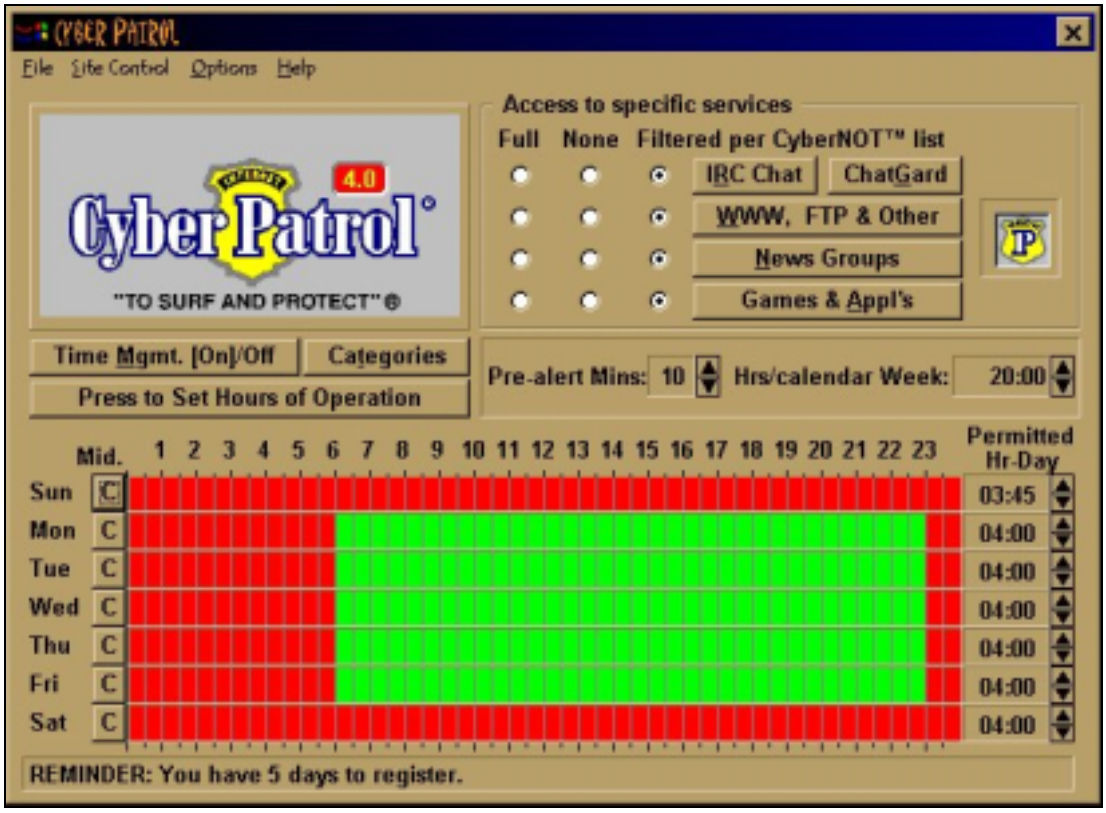
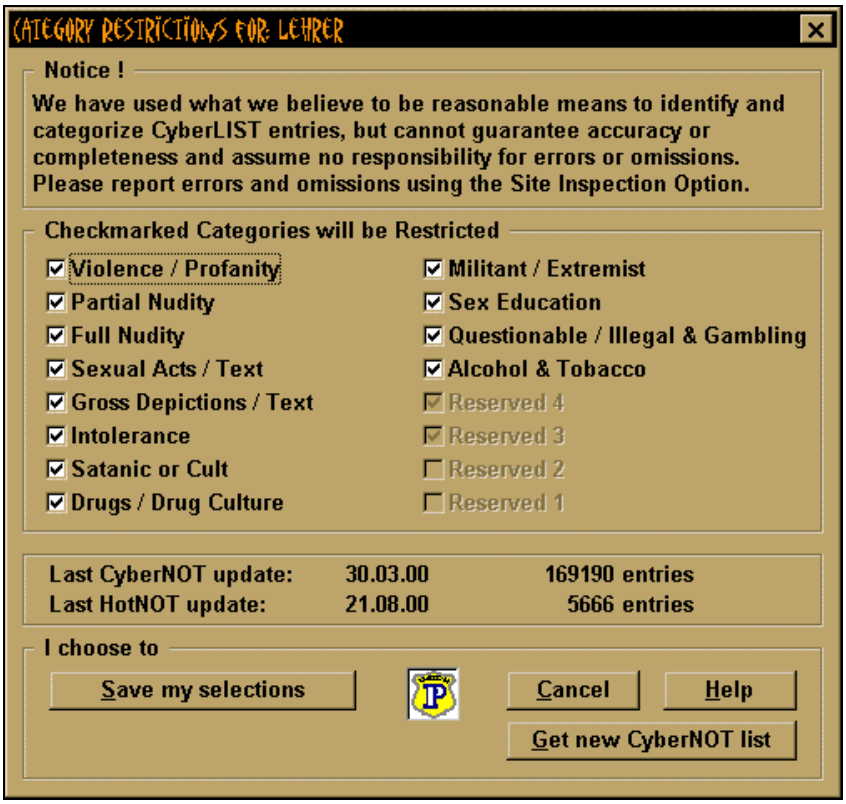


Abbildung: Cyber Patrol Konfigurationsbildschirm

Wie der Name, so sind auch die gesamten Funktionsbezeichnungen dem amerikanischen Polizeijargon entnommen. Die Hauptfunktionen werden demnach im Headquater (kurz HQ) eingestellt: Der Zugriff kann beschränkt werden nach Internet-Diensten wie Chat, WWW, FTP, News und Anwendungen, sowie nach Zeit.
Zur Einschränkung der Zugriffe innerhalb der Dienste verwendet Cyber Patrol sog. YES- bzw. NOT-Listen, die von der Homepage der Firma **in verschlüsselter Form** geladen werden können.
Der Inhalt beider Listen kann nicht eingesehen, aber manuell durch einzelne Einträge ergänzt bzw. eingeschränkt werden. Die vielversprechende Option LOCAL LISTS stellt sich bei näherer Betrachtung als die Möglichkeit heraus, von einem Web-Server eine dort vorrätige Liste über deren Nummer anzugeben. Eine Dokumentation, wie wer und auf welche Weise solche Listen zur Verfügung stellen kann, liegt leider nicht vor, so dass auch die Einbindung z. B. einer auf den Adressen des Bayerischen Schulservers und/oder des Deutschen Bildungsservers gründende LOCAL LIST nicht getestet werden konnte.

Für den Zugang zum Internet über Cyber Patrol können verschiedene Benutzer(-typen) definiert werden, die sich in den Zugangsrechten unterscheiden. Wird dem Default-User jeglicher Zugang verwehrt und den einzelnen Benutzern jeweils ein Passwort zugewiesen, so lassen sich sehr detaillierte, an die Schulsituation angepasste Nutzerspezifikationen erstellen. Zudem besteht die Möglichkeit des sog. DEPUTY BYPASS, einer passwortgeschützten, schnellen Umgehungsmöglichkeit für einen uneingeschränkten Zugriff.

Der gleiche Komfort besteht bei der Anpassung der zeitlich eingeschränkten Zugriffsbeschränkungen und der Sperre von einzelnen Kategorien:



Über den Menüpunkt ‘Domain Name Filter’ lassen sich auf einfache Weise komplette Top Level Domains aus- bzw. einschließen: Die Eingabe von ‘de’ in Verbindung mit einer ‘Allow’-Regel begrenzt den Zugriff auf alle URLs mit der Domain-Endung .de. Das ist zwar sehr elegant, führt jedoch im Detail zu unerwünschten Nebeneffekten. So ist der Aufruf von www.microsoft.de im ersten Schritt zwar ganz kurz erfolgreich, wird jedoch sofort wieder geblockt, weil der URL www.microoft.de nur ein Alias für www.microsoft.com/germany ist!

Der Zugriff auf beliebige Applikationen kann zusätzlich ausgeschlossen werden (z. B. napster.exe), leider jedoch nur, wenn es sich um 16-bit-Applikationen handelt.

Neben der Version für Einzelplätze bietet die Firma jetzt auch Versionen, die zentral am Übergang von Intranet zu Internet (Proxy-Server) eingesetzt werden können. Folgende Produkte stehen zur Verfügung:

CyberPatrol Proxy Microsoft
CyberPatrol Proxy Netscape
CyberPatrol Proxy Novell BorderManager
CyberPatrol Proxy Netscape für Linux
CyberPatrol Proxy Netscape für Solaris

Derzeit liegen zum Einsatz dieser Netzwerk-Produkte keine eigenen Erfahrungen vor, die Schulcomputer der Hansestadt Bremen werden jedoch nach einer Pressemitteilung des deutschen Distributors, der Firma PANAMP, bereits mit dieser Schutzsoftware ausgerüstet. Die Version für Einzelplätze bot bei allen Versuchen einen ausreichenden Schutz vor unerwünschten Testseiten. Auch der Zugang über die jeweils zugehörige IP-Adresse war nicht möglich. Die Aktualität der jeweiligen NOT-Listen war gut, so dass auch aktuelle Web-Sites rechtsradikaler Gruppierungen blockiert wurden.

4.4.2 NetNanny

Während in CyberPatrol alle unerwünschten Seiten im Web in kodierten Listen jeweils aktuell abgerufen und ins Programm integriert werden, herrscht im Programm NetNanny absolute Transparenz. Auch NetNanny bietet als Hauptfunktionen die Sperre unerwünschter bzw. die Erlaubnis für zugelassene Seiten im Internet. Gewährleistet wird dies über maximal 12 frei definierbare Listen zu den Bereichen ‘Words and Phrases’, ‘Internet News Groups’, ‘Personal Information’, ‘IRC Chat Lines’ und ‘Internet Web Sites’.

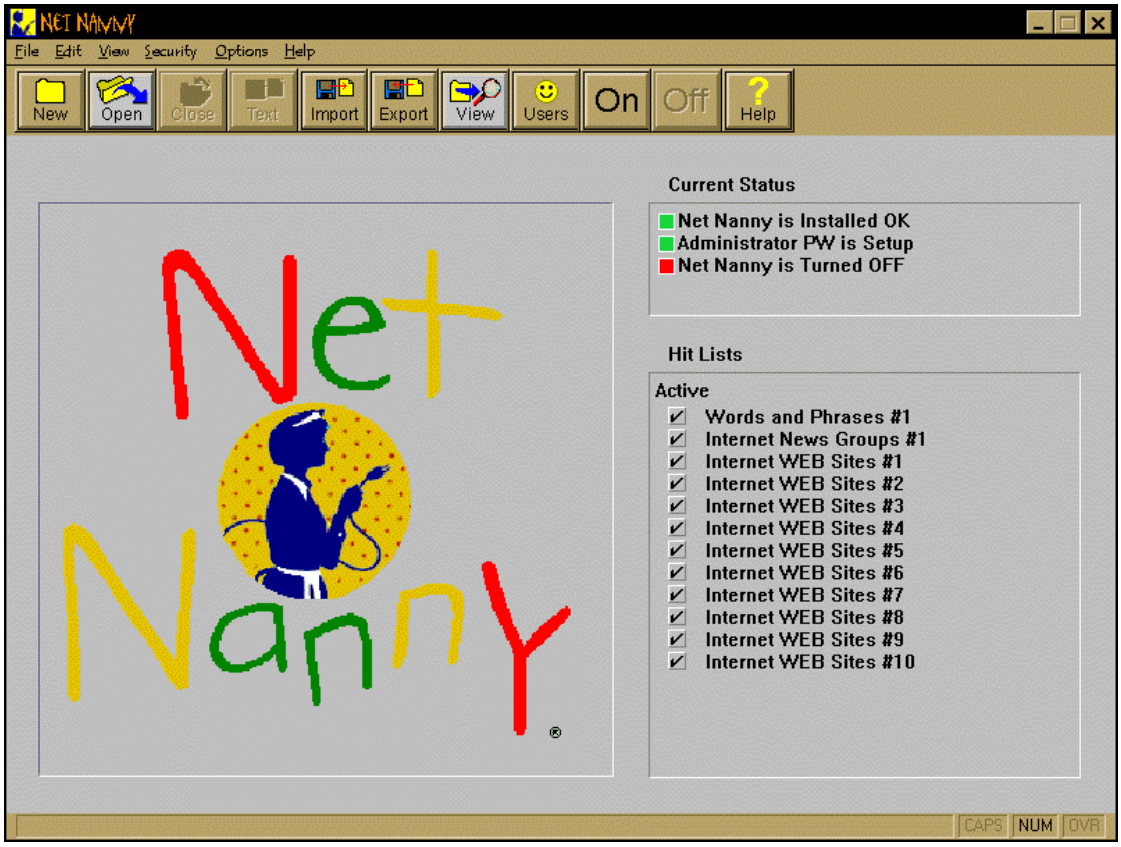
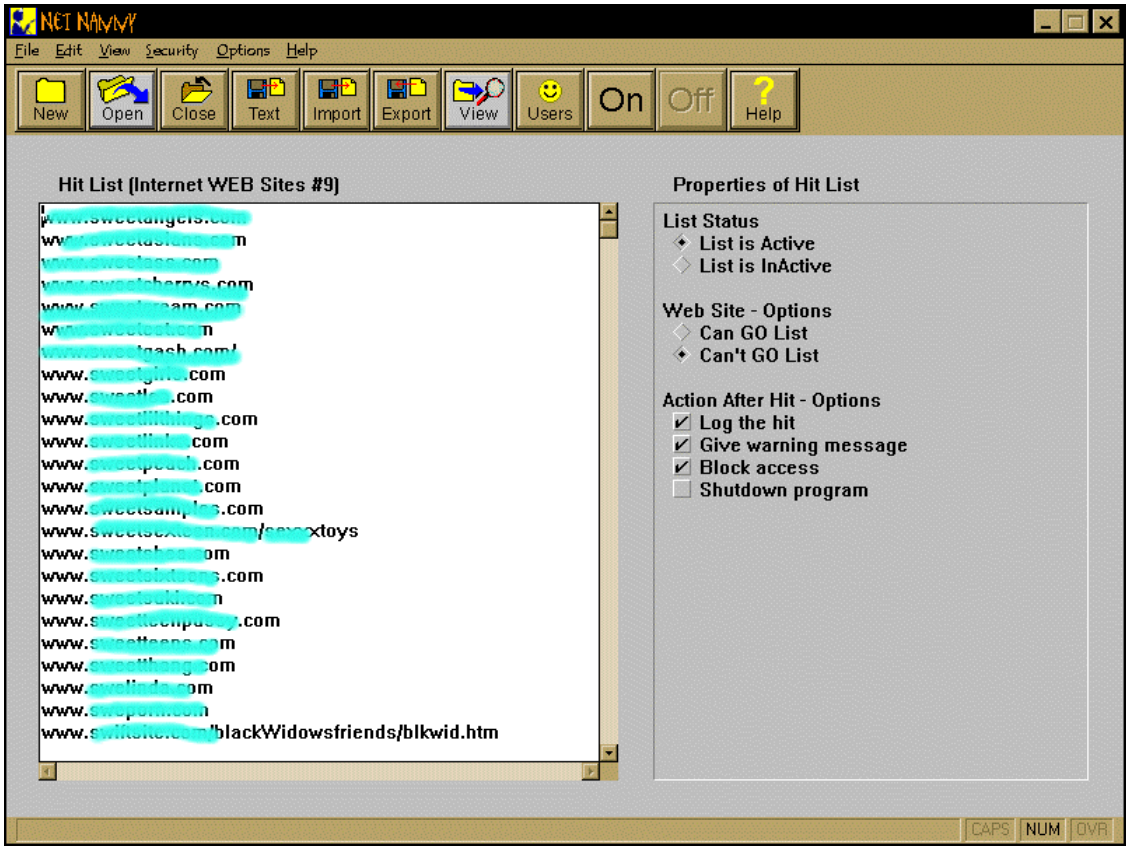


Abbildung: NetNanny Hauptbildschirm

In diese Listen wird im Klartext eingetragen, welche Zeichenketten überprüft und zugelassen oder ausgesperrt werden sollen:



Entspricht eine Web-Seite nicht den Erfordernissen der Listen, wird sie blockiert:



Neben der Sperre von Web-Seite überprüft NetNanny auch die Bildschirminhalte auf gesperrte Wörter und Satzteile. Dies führte bei Tests zu merkwürdigen und nicht nachvollziehbaren Effekten. Eine harmlose Beschreibung eines BASIS-Datensatzes wurde aus unerfindlichen Gründen von NetNanny überschrieben:

Kurzbeschreibung:
in-script - Die Unit für Bildung und Information der Kohtes Klewes Bonn GmbH erstellt im Auftrag von Partnern aus Wirtschaft und öffentlichen Institutionen praxisorientierte und fächerübergreifende Unterrichtsmaterialien. Dei Materialien bestehen aus Lehrermappe mit Folien und Kopiervorlagen und Schülerheften. Z.B. "Achtung vor dem Tier" zum Thema Tierschutz. Mit Auszügen aus dem Tierschutzgesetz. Kostenlos zum Download und zum Bestellen.

Bei eingeschalteter Überwachung von ‘Words and Phrases’ wird daraus:

Kurzbeschreibung: (wichtige Stichworte!)

```
in-script - Die Unit für Bildung und Information der Kohtes Klewes Bonn GmbH
erstellt im Auftrag von Partnern aus Wirtschaft und öffentlichen Institutionen
praxisorientierte und fächerübergreifende Unterrichtsmaterialien. Dei
Materialien bestehen aus Lehrermappe mit Folien und Kopiervorlagen und
Schülerheften. ##################################################################
##########################################################tellen.
```

Nachdem diese Korrekturen auch beim Verfassen von E-Mail plötzlich und unerwartet auftraten und so zum Teil längere Textpassagen unwiederbringlich zerstörten, konnte sehr bald nur noch mit abgeschalteter Funktion gearbeitet werden, was dem Einsatzzweck sicher widerspricht.

4.4.3 Norton Internet Security 2000

Die Firma Symantec bietet unter der Bezeichnung Internet Security 2000 eine ‚Komplettlösung für Internet Sicherheit’ an.

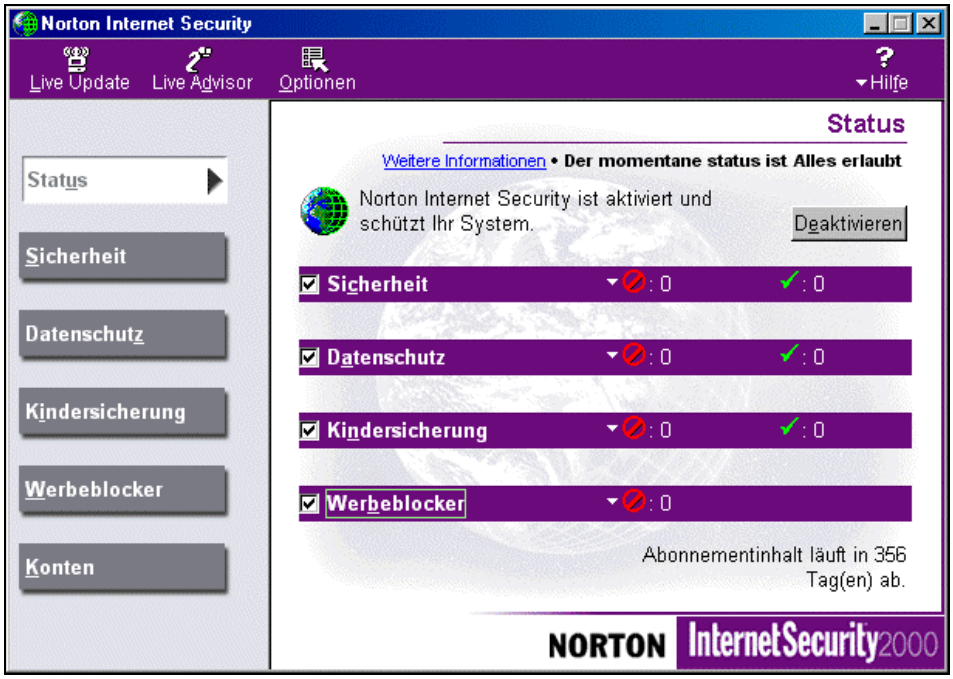


Abb. Gesamtbildschirm Norton Internet Security 2000

Neben den weiter oben angesprochenen technischen Schutzmechanismen (Firewall, Antiviren) bietet das Programmpaket unter dem Stichwort ‚Kindersicherung' auch die Möglichkeit zur Ausfilterung unerwünschter Inhalte aus dem Netz. Zu diesem Zweck lassen sich verschiedene Benutzerkonten mit unterschiedlichen Zugangsberechtigungen definieren.
Der Schutzmechanismus ‚Kindersicherung' besteht im Wesentlichen aus zwei Elementen: Die Kontrolle von zugänglichen Web-Seiten und die Berechtigung, bestimmte Programme auszuführen.

Die Einschränkung von abrufbaren Web-Angeboten kann über Positiv- oder Negativlisten erfolgen. Ist die Option ‚Zugelassene Sites angeben' aktiv, so sind zunächst alle Web-Seiten ausgeschlossen und nur die vom Benutzer anzugebenden URLs können erreicht werden (Positiv-Liste). Dazu muss jeder URL einzeln eingetragen werden. Die Übernahme einer kompletten Liste ist nicht vorgesehen.
Wird die Auswahl erreichbarer Web-Inhalte über Negativ-Listen eingeschränkt, so bietet das Programm bereits eine Liste von Kategorien an, die für das jeweilige Benutzerprofil gesperrt werden können. Die Auswahl der genannten Seiten beruht ‚auf einer umfangreichen nach Kategorien geordneten Websiteliste, die von Symantec erstellt und verwaltet wird' (Zitat Online-Hilfe). Der Bezug der aktuellen Websiteliste ist innerhalb des ersten Jahres nach Installation des Programms kostenfrei, danach wird er kostenpflichtig. Für die gesamte Liste können Ausnahmen definiert werden, die trotz Vorhandensein in der Symantc-Liste dennoch erreicht werden können und es können zusätzlich zu blockierende Seiten aufgenommen werden, die (noch) nicht in der Liste enthalten sind. Der Inhalt der Symantec-Liste kann weder im Klartext noch innerhalb des Programms ermittelt werden.

Die Berechtigung, bestimmte Programme auszuführen, nutzt die weiter oben beschriebene Funktionalität der Firewall im Programm: Jede Anwendung ist einer bestimmten Kategorie zugeordnet (siehe Erweiterte Optionen, Firewall) und diese Kategorien können für das Benutzerprofil zugelassen werden. Eine eigene Zuordnung von bestehenden oder neuen Programmen zu Kategorien ist über die Definition der Firewall-Einstellungen möglich.

Erste Erfahrungen beim Einsatz des Programms zeigen, dass der Aufruf unerwünschter Seiten nur über die Angabe von URLs verhindert werden kann; **bei Eingabe der zugehörigen IP-Adresse konnten die problematischen Seiten zum großen Teil trotz der Sperre geladen werden.** Die Auswahl der in der Block-Liste aufgenommenen URLs ist naturgemäß US-lastig und läßt vermuten, dass die Betreuer der Liste offenbar bisher wenig Einblick in deutsche Verhältnisse haben. So konnten rechtsextreme URLs in USA nur über die Angabe der zugehörigen IP-Adresse, ähnliche URLs in Deutschland jedoch auch über die URL erreicht werden. Speziell politisch fragwürdige Seiten der radikal rechten Szene außerhalb der USA sind in den Listen nicht erfasst und müssen manuell eingetragen werden.
Die Verwendung gesperrter Programme konnte dagegen immer erfolgreich verhindert werden.
Die grundsätzliche Problematik eines Hase-Igel-Rennens bleibt bei der Blockade über eine Negativliste bestehen, zumal eine dauerhafte Aktualität nur über zusätzliche Ausgaben erreicht werden kann. So empfiehlt sich auch hier der Einsatz einer mit der Zeit wachsenden Positivliste.
Der Einsatz des Programms ist auf einen Einzelplatz konzipiert. Daraus folgt für einen schulischen Einsatz, dass sämtliche Einstellungen (z. B. jede Erweiterung der Positivliste oder manuelle Definition von Ausnahmen) für alle Geräte manuell an jedem Gerät vorgenommen werden müssen. Eine Multiplikation über Netzwerk ist nicht vorgesehen, eine Dokumentation der zu kopierenden Dateien nicht vorhanden.
Eine Verwendung auf nicht beaufsichtigten Einzelarbeitsplätzen kann bei Akzeptanz der oben beschriebenen Einschränkungen empfohlen werden, da die grundsätzliche Funktionalität einer weitreichenden Ausblendung unerwünschter Inhalte gegeben ist.

4.5 E-Mail mit Attachements

Nicht zuletzt der I-LOVE-YOU-Virus hat deutlich vor Augen geführt, dass Bequemlichkeit im Umgang mit E-Mail in deutlicher Konkurrenz zu Sicherheitsanforderungen steht. Ursache war die automatische Zuordnung eines verhängnisvollen Visual-Basic-Scripts zum Script-Prozessor, so dass beim Aufruf des Dateianhangs dieses Script automatisch ausgeführt wurde und seine verhängnisvolle Funktion ausüben konnte. Doch nicht nur VBS-Scripte bilden eine potenzielle Gefahr für den Nutzer: Seit Bekanntwerden von Makroviren für WORD und EXCEL stellen auch Dateianhänge mit ehemals unverdächtigen Endungen eine weitere Gefährdung dar.
Als Gegenmaßnahmen bieten sich an:

- In allererster Linie Disziplin beim Umgang mit E-Mails, an die Attachements angehängt sind. Alle Nutzer eines Systems müssen sich bewusst sein, dass Attachements nur von zuverlässigen Absendern und nach Überprüfung mit Virenscannern geöffnet werden sollten.
- Einsatz von Filterregeln. Kann nicht gewährleistet werden, dass ausreichende Erfahrung und korrektes Verhalten im Umgang mit Dateianhängen vorhanden ist, so sollten alle E-Mails mit Dateianhängen über Filterregeln des Mailservers an eine erfahrene Person weitergeleitet und dort überprüft werden.

- Einsatz automatisierter E-Mail-Scanner. Professionelle Produkte bieten die Möglichkeit, jede eintreffende E-Mail auf Virenbefall zu überprüfen, ohne sie manuell öffnen und damit den Inhalt zugänglich machen zu müssen. Leider sind diese Systeme noch teuer und müssen auf ihre Tauglichkeit im Schuleinsatz erst überprüft werden.

4.6 Sandbox-System

Eine spezielle Form dieser Überprüfung stellen sog. Sandbox-Systeme dar. Im Prinzip werden dabei im Gegensatz zu herkömmlichen Viren-Scannern die eintreffenden Anhänge und ausführbaren Dateien nicht gelöscht oder abgewiesen, sondern in einem geschützten, speziell dafür eingerichteten Speicherbereich geöffnet. Innerhalb dieses Spiel-Bereiches (‘Sandkasten’) wird erprobt, ob Schaden angerichtet wird oder nicht. Nach erfolgreicher Überprüfung wird der Anhang weitergeleitet. Auch diese Funktionalität wird derzeit erprobt und kann noch nicht abschließend beurteilt werden.

5 Literatur und weitere Hinweise

5.1 Quellen:

ABB1, ABB2, ABB3: Alexander Geschonneck, Rechenzentrum, Humboldt-Universität zu Berlin, http://www.edvz.tuwien.ac.at/security/archiv/geschonneck1/wien02/index.html

5.2 Literatur

Kai Fuhrberg, Internet-Sicherheit, Hanser-Verlag, München Wien, 2000 ISBN 3-446-21333-3

Karheinz Moewes, Internet - Dienste, Funktionen, Kriminalität, München 1999, Eigenverlag, ISBN 3-00-005605-X

Klaus Utech, Handbuch Datenschutz-CD, UTECH Verlag, Juni 2000, ISBN 3-932783-24-0

5.3 Internet-Links

Quelle	*Beschreibung*	*Link*
Allgemeine Informationen:		
Der Landesbeauftragte für den Datenschutz Niedersachsen		http://www.lfd.niedersachsen.de/
Firewalls - Was leisten sie, was können sie nicht		http://www.edvz.tuwien.ac.at/security/archiv/geschonneck1/wien02/index.html
Angriffsmethoden in Datennetzen	Übersicht	http://www.webdefender.de/dienstleistungen/gefaehr_inh.htm
Netcraft - Web Server Survey	Überprüft beliebige Web-Seiten auf die verwendete Software	http://www.netcraft.com/
Rootshell	Englischsprachige Web-Seite mit jeweils neuesten Sicherheits-Informationen	http://rootshell.com
DFN-CERT GmbH, DFN-PCA und DFN-FWL	Sicherheitsberatung im DFN	http://www.cert.dfn.de/
Konzeption und Realisierung eines Firewallsystems zur Internet-Intranet Kopplung	Diplomarbeit an der Fachhochschule München	http://www.klaus.camelot.de/dip/node1.html
Security Finder	Fachinformationen zu Sicherheitslücken, neuen Produkten + Entwicklungen auf Wunsch täglicher Newsletter	http://www.securityfinder.com/
Sicherheit im Internet	Informationen des Bundesamtes für Sicherheit in der Informationstechnik 2000	http://www.bsi.bund.de/
IT-Grundschutzhandbuch	Informationen des Bundesamtes für Sicherheit in der Informationstechnik 2000	http://www.hu-berlin.de/bsi/gshb2000/
Internet-Kompetenz InternetDepartement für Informatik und vom Institut für Verhaltenswissenschaften der ETH Zürich und Infosense	Weiterführende Links zum Thema ‘ Sicherheitsaspekte bei der Internet-Benutzung’	http://www.internet-kompetenz.ch/sib/
SafeKids.Com	Englischsprachiges Angebot zum sicheren Umgang von Kindern im Internet, Tips für Eltern	http://www.safekids.com/
Security Server	Service des Instituts für Nachrichtenübermittlung der Universität Gesamthochschule Siegen	http://www.uni-siegen.de/security/

Quelle	*Beschreibung*	*Link*
'Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet'	Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder	http://www.datenschutz-berlin.de/to/vnetz/index.htm
E-Mail-Bomben	Web-Seite mit Informationen zu SPAM-MAILS	http://www.spam.abuse.net
Polizeidienststelle Jugend- und Medienschutz	Kommissariat 123 Jugend- und Medienschutz des Polizeipräsidiums München Bayerstr. 35 - 37/IV Stock Telefon: 089/551 72 - 123 Telefax: 089/551 72 - 300	http://www.polizei.bayern.de/ppmuc/post/post.htm
Produkte		
Programme für Zugangsschutz zum Internet	Programmsammlung	http://www.tucows.com/parent95.html
DEFENDO	Kommunikationsserver mit Firewall und Inhaltsschutz über Proxy	http://www.linogate.com
Symantec	Norton Internet Security 2000	http://www.symantec.com/region/de/product/nis/index.html
Download: Firewall-Software und Sicherheit-Utilities		http://www.zdnet.de/download/specials/pcfirewall04-wc.html
PGP websites in German		http://www.pgpi.org/links/www/pgp/de/
The International PGP Home Page		http://www.pgpi.org/
PGP - Pretty Good Privacy Der Briefumschlag für Ihre elektronische Post	deutschsprachige Anleitung	http://www.foebud.org/pgp/html
CyberPatrol PAN AMP	Generaldistributor für Cyber Patrol	http://www.panamp.de
Softguide	Aktuelle Marktübersicht - Software für Datensicherung u. Datenschutz:	http://softguide.de/software/datensicherung-datenschutz.htm
ChipLock	Zugangsabsicherung über Chipkarte	http://www.orga.com/german/produkte/security
Watch Guard Firebox WEBDEFENDER	Firewallsysteme und Dienstleister, bietet auch kostenfreien Check des bestehenden Systems spezielle Schulkonditionen	http://www.shop.webdefender.de/docs/pi345715464.htm
Site Blocker CSM Security Management AG	Kontrollsoftware Firewallsystem Proxyserver MailScanner	http://www.csm.co.at
Sambar Server - European site	Proxy-Server Freeware	http://www.skyweb.se/sambar/index.html http://sambar.jalyn.net/
ZoneAlarm	Persönliche Firewall Freeware	http://www.zonelabs.com
Steganos	Steganografie-Paket 69.-- DM	http://www.demcom.com/deutsch/
Surf Spy	Protokoll-Programm kostenlose Demo-Version Lizenz 30 USD	http://sureshot.virtualave.net/surfspy/index.html
NetNanny	Zugangsschutzprogramm 34,95 USD	http://www.netnanny.com