Fachhochschule Bonn-Rhein-Sieg

Jugendschutz in öffentlichen Bibliotheken und Entwicklung eines HTTP-Plugins für Agnitums Personal Firewall Outpost

Stand: 02. Dezember 2004

Daniel Stojceski

Praxisprojektbericht zur Erlangung eines Leistungsnachweises

Einleitung (Begründung, Ziele und Aufbau dieser Arbeit)

Diese Arbeit beschäftigt sich mit der Umsetzung des Jugendschutzes in öffentlichen Bibliotheken und skizziert die rechtlichen Hintergründe, die von öffentlichen Bibliotheken mit frei zugänglichen, internetfähigen Rechnern beachtet werden sollten (Kapitel zwei). Minderjährige könnten an öffentlichen Internet-Arbeitsplätzen an jugendgefährdende Web-Inhalte gelangen, wenn von Seiten der Bibliotheken keine Gegenmaßnahmen ergriffen werden. Wie eine solche Gegenmaßnahme realisiert werden kann, zeigt das im Rahmen dieser Arbeit entwickelte Plugin für Agnitums Outpost Personal Firewall. Das Plugin erlaubt vor allem das Aufzeichnen von aufgerufenen Ressourcen (URL) mittels HTTP-Protokoll im World Wide Web. Durch Analyse der Aufzeichnungen kann festgestellt werden, ob Web-Adressen mit jugendgefährdenden Ressourcen (z.B. Bilder) aufgerufen wurden, so dass mittels eines speziellen Filters gezielt der Zugang zu diesen Web-Adressen gesperrt werden kann. Die Sperrung solcher Web-Ressourcen könnte der Bibliothek zu einem jugendgerechteren Internetzugang verhelfen. In Kapitel vier wird nach einer kurzen Einführung in die Architektur der Outpost Firewall, das Funktionsprinzip des Plugins erörtert. Außerdem werden in dieser Arbeit in Kapitel drei verschiedene Personal Firewalls vorgestellt, die in direkter Konkurrenz zu Agnitums Outpost Personal Firewall stehen. Es wird näher auf die Eigenschaften dieser Personal Firewalls eingegangen. Mittels so genannter Leaktests werden zudem die Firewalls darauf getestet, ob sie unerlaubten ausgehenden Datenverkehr zu einem HTTP-Server (Port 80) im Internet feststellen, blockieren und dem Anwender melden. Eine kurze Zusammenfassung der Arbeit liefert Kapitel fünf.

Inhaltsverzeichnis

1 Definitionen und Abgrenzungen

Im Rahmen des zehnwöchigen Praxisprojekts auf der Fachhochschule Bonn-Rhein-Sieg sollte in Kooperation mit der Hochschul- und Kreisbibliothek für die in der Bibliothek eingesetzte pluginfähige Personal Firewall Outpost von Agnitum, ein Plugin entwickelt werden. Das Plugin soll die Aufzeichnung des ein- und ausgehenden HTTP-Verkehrs der in der Hochschulbibliothek eingesetzten Internetrechner erlauben, so dass dieser analysiert werden kann. Besonderes Augenmerk wird dabei auf Kinder- und Jugendgefährdende Internetadressen gelegt, da die Hochschulbibliothek gleichzeitig auch die Funktion einer öffentlichen Kreisbibliothek einnimmt. Das bedeutet, dass Bürgerinnen und Bürger der Region, die mindestens 14 Jahre alt sind, die selben Leistungen und Dienste nutzen können wie Hochschulangehörige, also auch die Multimedia-PCs mit Anschluss an das Internet. Durch Analyse des HTTP-Verkehrs mit Hilfe des HTTP-Plugins, sollen in Zukunft solche Web-Inhalte mit Hilfe eines speziell dafür eingesetzten Filters gefiltert oder geblockt werden um einen jugendgerechten Zugang zum Internet zu gewährleisten. Neben der Entwicklung des HTTP-Plugins sollte eine Produktsichtung anderer Personal Firewalls erfolgen.

Nachfolgend werden Definitionen festgelegt, die für das Verständnis dieser Arbeit benötigt werden.

- Firewall. Filter zwischen einem schützenswerten und einem nicht vertrauenswürdigen Netz, der Funktionen zur Überwachung, Filterung und Analyse von Netzverkehr bietet. Mit Hilfe eines wohldefinierten Filterregelwerks wird entschieden welcher (eingehender und ausgehender) Datenverkehr den Filter passieren darf. Das Filterregelwerk besteht im Allgemeinen aus einer Liste/Tabelle, die Angaben über erlaubte und nicht erlaubte Verbindungen beinhaltet und trägt zu einer in der jeweiligen Institution geltenden Sicherheitspolitik (Security Policy) bei. Der Filter kann je nach Implementierung auf verschiedenen Schichten des Netz-Protokoll-Stacks gem. des ISO/OSI Referenzmodells eingesetzt werden. Dadurch lässt sich unter folgenden Firewall-Typen unterscheiden [Cheswick et. al, 2004]:
  - Paketfilter. Filter für Paket-Header-Informationen in Abhängigkeit ihrer Quell- oder Zieladressen oder –Ports auf der IP-Schicht. Paketfilter sind in der Lage abgehende und eingehende Pakettypen (wie TCP, UDP, ICMP oder IP) zu erkennen und mit Hilfe eines definierten Filterregelwerks zu blocken oder zu erlauben.
  - Anwendungsschicht-Gateway - Proxy. Filter, der jede gewünschte Anwendung auf der Anwendungsschicht kontrolliert und protokolliert. Üblicherweise mit Hilfe der Store-and-Forward-Strategie, d.h. der Filter empfängt zunächst und überprüft anhand des Filterregelwerks die gesamte Anwendungstransaktion, bevor er weiterleitet.
  - Weitere Firewall-Typen, auf die hier nicht mehr weiter eingegangen wird, sind Transportschicht-Gateway (Curcuit-layer-Gateway) oder dynamische Paketfilter.
- Personal Firewall. Dezentrale Firewall, die auf jedem Client eines lokalen Netzwerks installiert sein muss und für die ein individuelles Filterregelwerk erstellt werden kann. Sie bietet üblicherweise Funktionen zur Paketfilterung und Anwendungsfilterung.
- Web-Filter (Content Filter/Proxy). Filter, der unter der Rubrik Anwendungsschicht-Gateway fällt und spezielle Eigenschaften zum filtern von WWW-Inhalten und -Adressen nach festgelegten Kriterien (wie Keywords oder Web-

Adressen) aufweist.

- World Wide Web (WWW). Bezeichnung für die Menge aller Server im Internet, die Informationen meist in Form von HTML-Seiten vorhalten und diese über das HTTP-Protokoll verfügbar machen [Strobel, 1997].
- Vertraute Anwendung. Eine der Firewall bekannte Applikation, die Verbindungen ins Internet aufbauen darf und für die bestimmte Filterregeln gelten.
- Hypertext Transfer Protocol (HTTP). Anwendungsschicht-Protokoll, das es erlaubt verteilte, hypermediale Informationssysteme im WWW zu nutzen. Aktuelle Version ist HTTP/1.1 [Fielding et al., 1999]. Um Inhalte auf den Informationssystemen anzusprechen, kommen die Standards Universal Resource Identifiers (URI, RFC 1630) sowie Uniform Resource Locators (URL, RFC 1738) zum Einsatz. Zur Kommunikation zwischen einem Client und einem Server mittels HTTP steht eine Menge an Methoden und Headern zur Verfügung (z.B. GET, POST, HEAD u.a.). Dabei wird eine request/response (Anfrage/Antwort) Strategie eingesetzt, d.h. dass jeder Kommunikationsverlauf mit einem request des HTTP-Clients beginnt bevor der HTTP-Server einen response an den Client zurücksendet, der Informationen (Status-Codes) über Erfolg der Anfrage (2xx), Umleitungsaktionen (3xx), Client (4xx)- oder Serverfehler (5xx) oder nur den Status beinhaltet (1xx) und evtl. die angeforderten Daten sendet (bei Statuscode 2xx). Zum Datentransport wird das Transmission Control Protocol (TCP, RFC 793) verwendet, wobei einem HTTP-Server standardmäßig der Port 80 zugewiesen wird. Während bei HTTP/1.0 [Berners-Lee et al., 1996] für jeden request/response-Austausch eine neue Verbindung zwischen Client und Server initiiert werden musste und dadurch auch jedes Mal eine neue TCP-Verbindung, ist es seit HTTP/1.1 unter anderem möglich, Verbindungen zwischen Client und Server persistent zu halten, d.h. eine Verbindung kann auch nach Beendigung eines request/response fortbestehen, damit der Client weitere requests an den Server richten kann, ohne, dass jedes Mal eine neue TCP-Verbindung aufgebaut werden muss. Dadurch soll vor allem die Netzlast verringert werden, da weniger TCP-Verbindungen auf- und abgebaut werden müssen.
- Malware. Sammelbegriff für Programme, die in „böswilliger Absicht geschrieben und verbreitet werden, meist ohne Einwilligung der Benutzer in Rechner oder Computersysteme eindringen und Irritationen, Störungen oder Schäden verursachen können“ [Der Brockhaus, 2003]. Es wird unter folgenden Malware-Typen unterschieden:
  - Computerviren.
  - Trojanische Pferde.
  - Computerwürmer.

2 Rechtlicher Hintergrund

Ein zentrales Problem von Bibliotheken mit Internetzugang besteht darin, dass Minderjährige an jugendgefährdende Web-Inhalte gelangen können, sei es durch Zufall (z.B. Tippfehler), Neugierde oder bewusst, die die Entwicklung und Erziehung der Minderjährigen negativ beeinflussen könnten. Im Folgenden werden, die aus rechtlicher Sicht für Bibliotheken mit Internetzugang relevanten Gesetze und Institutionen mit Bezug auf Jugendschutz aufgeführt und kurz erläutert:

- das Grundgesetz (GG) Art. 5, Abs.2 und Art. 6, Abs. 2. Verpflichtet unter ande-

rem den Staat Jugendliche vor jugendgefährdenden Medien zu schützen [Müller, 1999].

- das Jugendschutzgesetz (JuSchG), vom 23. Juli 2002, soll vor allem den Gefährdungen für die Erziehung und Entwicklung von Kindern und Jugendlichen begegnen, die von Computerspielen und Internetangeboten ausgehen.
- der Jugendmedienschutz-Staatsvertrag der Länder (JMStV), vom 10.-27. September 2002, soll für einen einheitlichen Schutz der Kinder und Jugendlichen vor Angeboten in elektronischen Informations- und Kommunikationsmedien sorgen, die vor allem die Menschenwürde oder sonstige durch das Strafgesetzbuch geschützte Rechtsgüter verletzen.
- Bundesprüfstelle für jugendgefährdende Medien. Führt eine Liste jugendgefährdender Medien, darunter auch Web-Adressen und -Domains. Die Liste enthält vor allem unsittliche, verrohend wirkende, zu Gewalttätigkeit, Verbrechen oder Rassenhass anreizende Medien und besteht aus vier Teilen:
  - Teil A. Öffentliche Liste der Trägermedien, die den Verbreitungsverboten des § 15 JuSchG unterliegen.
  - Teil B. Öffentliche Liste der Trägermedien, die weitergehenden Verbreitungsverboten des StGb unterliegen. Vor allem § 86, §130a, § 131 und § 184 Abs. 2 oder 4.
  - Teil C. Nichtöffentliche Liste der Telemedien, die den Verbreitungsverboten des § 4 JMStV unterliegen, sowie von Trägermedien, die den Verbreitungsverboten des § 15 JuSchG unterliegen und deren Listenaufnahme aus Gründen des Jugendschutzes nicht öffentlich gemacht wird (sog. Werbeeffekt).
  - Teil D. Nichtöffentliche Liste der Telemedien, die weitergehenden Verbreitungsverboten StGb unterliegen, sowie von Trägermedien, die auch den Verbreitungsverboten unterliegen und deren Listenaufnahme aus Gründen des Jugendschutzes nicht öffentlich gemacht wird (sog. Werbeeffekt).
- das Strafgesetzbuch (StGb). Hier sind vor allem wichtig:
  - § 86, Verbreiten von Propagandamitteln verfassungswidriger Organisationen.
  - § 130, Volksverhetzung.
  - § 131, Gewaltdarstellung.
  - § 184, Pornographische Schriften.
- Gesetz über die Nutzung von Telediensten (TDG), vom 22. Juli 1997. Sorgt für einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste.

Resultierend aus den oben aufgeführten Gesetzen gelten vor allem Inhalte, die

- die Menschenwürde verletzen,
- Propagandamittel im Sinne des § 86 des StGb verbreiten,
- Menschen in einer die Menschenwürde verletzenden Weise darstellen,
- Jugendliche in unnatürlicher, geschlechtsbetonter Körperhaltung zeigen,

- die pornographisch sind,
- Gewalttätigkeiten sexuellen Missbrauchs von Kindern oder Jugendlichen oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben,
- Volksverhetzung zum Gegenstand haben,
- Aufstachelung von Rassenhass zum Gegenstand haben,
- Gewalt verherrlichen oder verharmlosen

als (schwer) jugendgefährdend.

Entscheidend für öffentliche Bibliotheken mit Internetzugang ist die Frage, ob ihrerseits aktive Schutzmaßnahmen gegen solche zum Teil schwer jugendgefährdende Inhalte zu ergreifen sind und, ob sie sich sonst nicht im Sinne des StGb strafbar machen. Einerseits sind aus dem StGb und dem JMStV zwei Folgerungen ersichtlich, die bei Zuwiderhandlung zu Strafmaßnahmen führen können [Müller, 1999]:

1) Schwer jugendgefährdende Medien dürfen unter 18-jährigen in keiner Weise überlassen werden (d.h. anbieten, überlassen, zugänglich machen,…), darunter fällt auch die Darstellung von Web-Inhalten auf einem Bildschirm.
2) Sonstige jugendgefährdende Medien dürfen nach einer Indizierung (öffentliche und nicht öffentliche Liste) durch die Bundesprüfstelle unter 18-jährigen nicht mehr zugänglich gemacht werden.

Andererseits gilt, dass Bibliotheken – haben sie öffentlich zugängliche Internetzugänge – Anbieter von Telediensten gemäß § 2, Absatz 2 und § 3, TDG sind, aber gemäß § 9 TDG „für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln nicht verantwortlich“ sind. Auch sind Diensteanbieter gem. § 8 TDG nicht dazu verpflichtet „ die von ihnen übermittelte oder gespeicherte Informationen zu überwachen oder nach Umständen zu forschen, die auf einer rechtswidrigen Tätigkeit hinweisen“, aber sie sind gem. den §§ 10 und 11 dazu verpflichtet unverzüglich Maßnahmen zu ergreifen, um die Informationen zu entfernen oder den Zugang zu ihr zu sperren, sobald sie Kenntnis von rechtswidriger Information haben. Insgesamt lässt sich somit schlussfolgern, dass sich öffentliche Bibliotheken mit offen zugänglichem Internetzugang für jugendgefährdende Inhalte auf fremden Servern nicht strafbar machen, jedoch Sorge dafür tragen müssen, dass solche Inhalte für unter 18-jährige nicht zugänglich sind. Hier greift § 5 JMStV (Entwicklungsbeeinträchtigende Angebote) Abs.1 und Abs. 3, Nr. 1: „Sofern Anbieter Angebote, die geeignet sind, die Entwicklung von Kindern oder Jugendlichen zu einer eigenverantwortlichen und gemeinschaftsfähigen zu beeinträchtigen, verbreiten oder zugänglich machen, haben sie dafür Sorge zu tragen, dass Kinder oder Jugendliche der betroffenen Altersstufen sie üblicherweise nicht wahrnehmen“ und „Der Anbieter kann seiner Pflicht aus Absatz 1 dadurch entsprechen, dass er 1. durch technische oder sonstige Mittel die Wahrnehmung des Angebots durch Kinder oder Jugendliche der betroffenen Altersstufe unmöglich macht oder wesentlich erschwert“. Mit technischen Vorkehrungen sind dabei vor allem Verschlüsselung und Jugendschutzprogramme gemeint [Bundesministerium für Familie, Senioren und Jugend, 2003]. Zudem kommt hinzu, dass öffentlichen Bibliotheken im Allgemeinen eine aktive Rolle bezüglich des Jugendmedienschutzes zugeschrieben wird [Müller, 1999]. Das verpflichtet die Bibliotheken, jugendgefährdende oder –beeinträchtigende Inhalte - vor allem durch die Bundesprüfstelle indizierte Web-Seiten, Bücher, Spiele und sonstige Medien - soweit es möglich ist, nicht für unter 18-jährige zugänglich zu machen.

Dies kann z.B. dadurch erreicht werden, dass ein Softwarefilter dem Internetzugang vorgeschaltet wird. Relevant sind in diesem Fall die Personal Firewall und der Web-

Filter. Dadurch, dass die Personal Firewall dezentral ist, erlaubt sie individuelle Einstellungen für das Filterregelwerk. Somit läst sich z.B. realisieren, dass nur bestimmte Rechner mit einer Personal Firewall ausgerüstet werden und nur diese an Jugendlichen unter 18 Jahren zugewiesen werden. Die Personal Firewall sollte die Möglichkeit bieten, nicht nur ausgewählte Anwendungen der Anwendungsschicht und Paket-Header-Informationen zu kontrollieren und zu überwachen, sondern idealerweise zusätzlich einen integrierten Web-Filter. Der Web-Filter sollte vor allem Funktionen zur Filterung nach in Inhalten auftauchenden Keywords und unerwünschter Webadressen aufweisen.

Nachfolgend werden verschiedene Personal Firewalls vorgestellt und evaluiert.

3 Evaluierung von Personal Firewalls

Im Folgenden wird näher auf Eigenschaften der Personal Firewalls Kerio Personal Firewall (Vers. 4.0.16), Securepoint Personal Firewall (Vers. 3.6), Sygate Personal Firewall (Vers. 5.5), ZoneAlarm (Vers. 4.5 Pro) sowie look 'n' stop (Vers. 2.05) jeweils in den Pro-Versionen eingegangen. Aufgrund der kurzen Praxisprojektdauer, konnte nicht detaillierter auf die Personal Firewalls eingegangen werden. Das bedeutet, dass im Folgenden nur grundlegende Eigenschaften der Personal Firewalls aufgeführt werden. Anhang A.2 enthält genauere Angaben zu den Eigenschaften. Mittels Personal Firewall Leaktester wird außerdem versucht, Schwachstellen der vorgestellten Firewalls für ausgehende Verbindungen aufzudecken. Dabei kommt es primär nicht darauf an, ob es einem Testtool gelingt eine Verbindung ins Internet aufzubauen um Daten zu senden oder empfangen. Vielmehr wird getestet, ob es einer der Firewall vertrauten Anwendung, die zuvor mit Hilfe eines Testtools modifiziert oder infiltriert wurde, gelingt, unbemerkt eine Verbindung zu einem HTTP-Server im Internet aufzubauen und dann Daten zu senden und zu empfangen. Solche Strategien verfolgt üblicherweise Malware Software, z.B. Trojaner, die durch interne Täter oder unerfahrene Anwender (z.B. öffnen von nicht vertrauten E-Mail Anhängen) auf einem Rechner installiert wurde. Auf Tests für eingehende Verbindungen wurde verzichtet, da die hier vorgestellten Personal Firewalls alle Ports nach der Installation geschlossen halten (getestet mit Nmap 3.55). Anhang A.1 – Firewall Testergebnisse - zeigt tabellarisch die Testergebnisse für die hier vorgestellten Personal Firewalls und den verwendeten Testtools.

Leaktester sind Tools, die mit Hilfe verschiedener Methoden versuchen bekannte Schwachstellen von Firewalls auszunutzen um z.B. eine Verbindung ins Internet aufzubauen und Daten zu übertragen oder zu empfangen. Der Anwender wird dann über den Erfolg oder Misserfolg informiert. Gelingt es einem Tool eine Schwachstelle aufzudecken, dann hat das zur Folge, dass Malware dieselbe Methode anwenden könnte um unbemerkt von der Firewall eine Verbindung ins Internet aufzubauen. Neben Leaktester-Programmen werden Programme verwendet, die mittels Direct Link Lybrary-Injection (DLL-Injection) die Firewall umgehen wollen. Bei DLL-Injection lädt sich ein Programm in einem der Firewall vertrauten Prozess (z.B. ein Browserprozess wie opera.exe) und wird Teil dieses Prozesses. Dadurch können mit Hilfe des Prozesses unbemerkt von der Firewall Daten gesendet und empfangen werden. Alle Tests erfolgen in der Out-of-the-Box-Einstellung (Grundeinstellung) der Firewalls.

Im Einzelnen kommen folgende Tools zu Einsatz:

- LeakTest (Vers. 1.2). Etabliert eine TCP-Verbindung auf Port 80 zu einem im Internet bekannten Server (grc.com) und baut die Verbindung wieder ab. Dadurch können Trojaner, Viren, etc. simuliert werden, die Daten mit einem im Internet befindlichen Server austauschen wollen. Folgende Tests können durchgeführt werden:

1. Masquerading (vertraute Anwendung). Die ausführbare LeakTest-Datei wird umbenannt in einen Dateinamen, der der Firewall vertraut ist und Verbindungen ins Internet aufbauen darf, z.B. iexplorer.exe. Die Originaldatei iexplorer.exe wird durch die umbenannte LeakTest-Datei ersetzt und schließlich ausgeführt. Dieser Test stellt fest, ob eine Firewall ihr vertraute Anwendungen nur anhand der Anwendungsnamen behandelt oder auch Modifizierungen an der Anwendung feststellen kann (z.B. Feststellen von Änderungen an Dateien mittels einer Prüfsumme).

2. Masquerading (Standard-Anwendung). Wie oben, jedoch wird der Dateiname so gewählt, dass er der Firewall nicht vertraut ist.

3. Stealth Modus. LeakTest kann mit der Option „stealth“ gestartet werden. Es versucht dann eine bekannte Schwachstelle im Windows-Betriebssystem auszunutzen um sich an der Firewall vorbeizuschleusen. Es handelt sich um eine Schwachstelle beim Windows Socket-Netzwerk-Interface.

- Tooleaky. Leaktester, der den Internet Explorer im „hidden-Modus“ aufruft um Daten zu senden (zu Port 80) und empfangen.
- Firehole 1.01. DLL-Injection-Tool, das den Standard-Browser des Betriebsystems aufruft um Daten über Port 80 zu einem Server im Internet zu senden und empfangen.
- pcAudit 3.0.0.9. DLL-Injection-Tool, das mit Hilfe des Windows Explorers Daten ins Internet sendet.
- Phatbot. Internetwurm, der unter anderem Methoden zum Beenden von Prozessen beinhaltet. Z.B. versucht der Wurm den aktiven Prozess einer Firewall auf einem Windows-Betriebssystem zu beenden, um ungestört Daten senden und empfangen zu können. Mit Hilfe des Wurms kann getestet werden, ob eine Personal Firewall Schutzmechanismen gegen nicht autorisierte Beendigung des Firewall-Prozesses bietet. Aus Sicherheitsgründen wurden die Testergebnisse aus [Brauch, 2004] entnommen.

3.1 Kerio Personal Firewall

Die Kerio Firewall bietet folgende Eigenschaften:

- Programm und Hilfstexte in Deutsch.
- Lernmodus vorhanden.
- im Lieferzustand keine Verbindungen ins Internet erlaubt.
- Regeln können einmalig oder permanent zugelassen oder blockiert und leicht verändert werden.
- Erkennung von Subnetzen und Einstufung des Subnetzes als vertrauenswürdig, d.h. andere Rechner aus dem LAN können auf Datei- und Druckerfreigaben zugreifen, aber auch vorhandene Malware hat dadurch diesen Zugriff.
- Anwender erhält keine Beschreibung über bekannte Anwendungen, die ins Internet wollen (wie svchost.exe - Namensauflösung unter Windows) und somit keine Hilfestellung bzgl. der Zulassung oder Blockierung dieser Anwendungen. Das heißt, Anwender muss anhand der Programmnamen entscheiden, ob ein Programm eine Verbindung ins Internet aufbauen darf.
- IP- und Portbereiche können explizit erlaubt oder blockiert werden.

- Import- und Exportfunktion: Einstellungen der Firewall können gespeichert und nach neuer Installation eingespielt werden.
- Anwender wird gewarnt sobald eine Anwendung auf eine andere zugreifen will. Dies bietet sinnvollen Schutz vor typischen Trojanern, die über diese Methode versuchen, Kontakt mit dem Internet aufzunehmen. Ausnahmen macht Kerio bei Windows-Komponenten, die andere Anwendungen aufrufen.
- Anwender wird nicht gewarnt, wenn ein unbekanntes Programm einen Port in den Zustand LISTEN versetzt. Eine Warnung erfolgt aber, sobald von außen auf den Port zugegriffen wird.
- Werbe- und Popupfilter für Browser.
- Möglichkeit JavaScript, VBScript und ActiveX aus Web-Inhalten herauszufiltern.
- Regel-Import und Export-Funktion.

Bemerkungen zu den durchgeführten Tests

LeakTest bestanden: Es erfolgt ein Hinweis, dass eine Anwendung ersetzt wird.

Tooleaky-Test bestanden: Meldung, dass nicht vertrautes Programm den Internet Explorer startet.

Durchgefallen beim DLL-Injection-Test: Kerio meldet, dass ein unbekanntes Programm (firehole.exe) den Opera-Browser starten möchte. Obwohl dann Blockieren gewählt wird, gelingt es Firehole eine TCP-Verbindung ins Internet aufzubauen und Daten zu senden und zu empfangen - unter der Voraussetzung, dass der Standard-Browser bereits als Prozess läuft.

pcAudit-Test bestanden: Hinweis, dass der Internet Explorer von pcAudit gestartet wird. Wird dies geblockt, kann auch pcAudit nicht gestartet werden.

Kerio versagt beim Phatbot-Test: Programme können die Firewall beenden, ohne dass ein Hinweis oder eine Warnung erfolgt [Brauch, 2004].

3.2 Securepoint Personal Firewall

Eigenschaften:

- Deutsch.
- Übersichtliche Bedienungsoberfläche.
- Per Default benutzt Securepoint nur Anwendungsregeln.
- Im Expertenmodus kann der Anwender über eine Dialogbox IP-, Port- und Protokollregeln erstellen.
- Keine Warnungen bei eingehendem Verkehr wie Portscans oder Verbindungsversuchen. Solche Aktivitäten sind nur in der Protokolldatei vermerkt.
- Bei manchen bekannten ausgehenden Verbindungen erhält der Anwender hilfreiche Erklärungen.
- Nur permanentes Zulassen und Blockieren von Datenverbindungen möglich, d.h. der Anwender hat keine Möglichkeit Datenverbindungen einmalig zu blocken oder zu erlauben.

- Bietet keinen Schutz, wenn vertraute Anwendungen von anderen Anwendungen gestartet werden.
- Anwender wird informiert, sobald ein Prozess versucht die Firewall zu beenden. Der Anwender kann dies dann zulassen oder abbrechen.
- Integrierter Virtual Private Network Client. Protokoll: IPSec.
- Hilfreiche Informationen bekannter Anwendungen in einem Eigenschaften-Fenster.

Es fielen Fehler in der Programmierung (Kinderkrankheiten) auf. Z.B. beim Einfügen des Opera Browsers in die Liste der zugelassenen oder gesperrten Anwendungen. Soll der Status geändert werden, erscheint folgende Fehlermeldung und die Änderung kann nicht durchgeführt werden: „Der Index der Liste überschreitet das Maximum (1)“. Anzahl der Anwendungen in der Liste war fünf. Sonstige Fehler: unvollständige Darstellung der IP-Adressen zu denen eine Verbindung erfolgen soll in den Dialogboxen. Meldet sich ein Benutzer ab und wieder an, kann es sehr lange Dauern bis der Desktop des Rechners zu sehen ist (Windows XP).

Bemerkungen zu den durchgeführten Tests

Erfolgreich beim Leaktest mit dem LeakTest-Tool: Erkennt Modifizierungen an einer Datei, meldet einen Hinweis und kann den ursprünglichen Zustand der modifizierten Datei wiederherstellen.

Durchgefallen beim Test mit Tooleaky. Tooleaky konnte, ohne einen Hinweis der Firewall, Daten senden und empfangen. Internet Explorer war als vertraut eingestuft. Wird der Internet Explorer blockiert, besteht Securepoint den Test.

Securepoint besteht alle DLL-Injection-Tests.

3.3 Sygate Personal Firewall

Eigenschaften:

- Nur Englisch.
- Übersichtliche Oberfläche und schnell erlernbare Bedienung.
- Keine vorgefertigten Regelsätze.
- Lernmodus vorhanden.
- Keine konkrete Hilfestellung beim Erlauben oder Blockieren von Prozessen, die dem Anwender seine Entscheidung erleichtern könnte.
- Im Hauptfenster stellt Sygate den erlaubten und blockierten Netzverkehr als durchlaufenden Graphen dar.
- Portscans und Verbindungsversuche von außen werden in einem gesonderten Diagramm dargestellt. Zusätzlich werden alle Anwendungen angezeigt, die über das Netz kommunizieren.
- Einfache, schnelle und flexible Regeländerungen: Anwendungen können so reglementiert werden, dass sie nur auf bestimmte Ports und an bestimmte IP-Adressen Daten versenden können. Advanced Rules enthalten zudem unabhängig von Anwendungen allgemeingültige Regeln.
- Phatbot-Test kann erfolgreich abgewehrt werden, allerdings ohne Hinweis

der Firewall, dass versucht wurde die Firewall zu beenden [Brauch, 2004].

- Popup-Management.
- Sehr detaillierte Informationen, wenn die Firewall Modifizierungen an vertraute Anwendungen feststellt und versucht wird eine Verbindung ins Internet aufzubauen: z.B. Inhalt des IP-Datagramms, Inhalt der TCP-Nachricht.
- Backtrace-Funktion mit der Möglichkeit Whois-Abfragen zu starten: Rückverfolgung von Datenpaketen über mehrere „Hops“.

Bemerkungen zu den durchgeführten Tests

LeakTest: Hinweis, dass eine vertraute Anwendung modifiziert wurde und Nachfrage, ob Verbindung erlaubt oder blockiert werden soll. Falls Verbindung erlaubt wird, gelingt es LeakTest Daten zu senden und empfangen.

Tooleaky-Test bestanden: Hinweis, dass der Internet Explorer durch tooleaky.exe gestartet wurde und versucht eine Verbindung ins Internet herzustellen. Nach Blockier-Regel für den Internet Explorer gelingt es Tooleaky nicht mit Hilfe des Internet Explorer Daten zu senden und empfangen. Es folgt ein Hinweis: „Application Hijacking has been detected“.

Beim Firehole-Test durchgefallen. Allerdings gibt es die Option DLL-Injection-Erkennung zu aktivieren. Die Firewall erkennt dann die DLL-Injection, blockt zunächst den Netzverkehr für die infiltrierte Anwendung und gibt dem Anwender umfangreiche Informationen aus.

Beim pcAudit-Test durchgefallen: Es erfolgt kein Hinweis der Firewall, dass explorer.exe unerlaubt Daten gesendet hat. (explorer.exe vertraut). Jedoch ein Eintrag in der Log-Datei. Bei eingeschalteter DLL-Injection-Erkennung erfolgt Hinweis, dass neue DLLs geladen wurden; der Netzverkehr für explorer.exe wird aber nicht geblockt und es können Daten gesendet werden.

3.4 Zone Alarm

Eigenschaften:

- Einfache Bedienung.
- Deutsch.
- Kann wahlweise im Hintergrund arbeiten ohne Warnhinweise auszugeben oder bei blockiertem Verkehr Warnhinweise anzeigen.
- Lernmodus vorhanden.
- Erstkonfiguration kann automatisch erfolgen (Zugriffsrechte vorkonfigurieren, z.B. Regeln für svchost.exe und den Windows-Update-Server).
- Tutorial über die Firewall.
- Schutz vor Übertragung von eBay-Passwörtern an nicht erwünschte Seiten (Übertragung nur an eBay-Seiten).
- Vertrauenswürdige Bereiche wie das lokale Netz können festgelegt werden.
- E-Mail-Schutz: bei potenziell gefährlichen Dateianhängen wird die Dateiendung (exe, vbs, pif, bat etc.) umbenannt, sodass diese nicht mehr aus-

führbar sind.

- Warndialog wenn Programme einen Port auf LISTEN setzen.
- Schutz vor Beendigung der Firewall durch nicht autorisierte Programme.
- Popup-Werbeblocker.
- Sicherheitseinstellungen können mit einem Kennwort geschützt werden.

Bemerkungen zu den durchgeführten Tests

LeakTest bestanden: wird als „Firewall Testing Utility“ identifiziert und kann geblockt werden.

Tooleaky konnte mittels Internet Explorer Daten senden und empfangen, auch nachdem Internet Explorer blockiert wurde.

Firehole konnte ohne Hinweis der Firewall den Standardbrowser öffnen und Daten senden und empfangen, d.h. kein Schutz vor DLL-Injection.

Beim pcAudit-Test durchgefallen: explorer.exe war als vertraut eingestuft =>Daten können gesendet werden. Nur wenn explorer.exe gänzlich geblockt wird, ist keine Datensendung möglich.

3.5 Look ’n’ Stop

Eigenschaften:

- Englisch.
- Sehr schlanke und ressourcen-sparende Firewall.
- Umfangreiche Möglichkeiten der Regel-Erstellung.
- Lernmodus (nur permanentes Zulassen oder Blockieren).
- Vordefinierte Regeln, die vor allem bekannte Angriffsmethoden verhindern sollen (neue Filterregeln können aus dem Internet bezogen und leicht in die Firewall integriert werden).
- Internetfilterregeln und Anwendungsregeln können getrennt eingestellt werden. Dadurch können Anwender, die hinter einer zentralen Firewall sitzen, die Internetfilterregeln deaktivieren und müssen nur die Anwendungsregeln anzuwenden.
- Plugin-Fähigkeit (jedoch konnte beim Versuch Plugins zu installieren kein Erfolg verbucht werden: die Plugins wurden nicht erkannt). Eigene Plugins können nicht entwickelt werden.

Bemerkungen zu den durchgeführten Tests

LeakTest bestanden. Merkt Modifizierungen an vertrauten Anwendungen.

Tooleaky: Merkt den Aufruf des Internet Explorer und es können keine Daten gesendet und empfangen werden, indem der Verkehr für tooleaky.exe geblockt wird. Auch wenn der Internet Explorer als vertraut eingestuft wird, gelingt es Tooleaky nicht Daten zu senden.

Firehole: besteht den Test, für den Fall, dass kein Prozess des Standard-Browsers bereits läuft.

pcAudit: ist der Windows Explorer als vertraut eingestuft, gelingt es pcAudit Daten zu senden. Bei Aktivierung der DLL-Injection-Erkennung blockt die Firewall erfolgreich.

3.6 Outpost Personal Firewall

Die Outpost Personal Firewall wird von dem Unternehmen Agnitum in der derzeitigen Pro-Version 2.1 und Free-Version 1.0 angeboten. Gegenüber den meisten anderen Personal Firewalls sticht besonders die Plugin-Fähigkeit hervor. Entwicklern wird die Möglichkeit eingeräumt, mit der frei verfügbaren Entwicklungsumgebung eigene Plugins zu entwickeln, was z.B. bei Look 'n' Stop nicht der Fall ist. Die Plugins können anderen Anwendern zugänglich gemacht werden, wodurch die Leistungsfähigkeit der Firewall erweitert werden kann.

Die Installation verlief problemlos. Der Anwender kann die Autokonfiguration der Firewall nutzen oder überspringen. Die Autokonfiguration übernimmt das Anwenden von vorgegebenen Filterregeln auf gefundene Programme und auf das gefundene Netz. Nach Anwenden der Autokonfiguration sind gefundene Programme eingeschränkt, d.h. versuchen diese Programme eine Verbindung ins Internet aufzubauen wird zunächst beim Anwender nachgefragt. Nach der Installation scheint die Oberfläche aufgeräumt und übersichtlich. Dennoch erweist sich das Auffinden der Filterregeloptionen als schwierig. Diese sind unter verschiedenen Schaltern mehrfach auffindbar. Es gibt folgende Typen von Filterregeln: Filter für Anwendungen, Filter für ICMP, Globale Anwendungs- und Systemregeln und Filter der jeweiligen Plugins.

Eigenschaften:

- Deutsch (Hilfedateien in Englisch).
- Anwendungen können blockiert, erlaubt und eingeschränkt (nur bestimmte Ports/Protokolle erlaubt) werden.
- Lernmodus.
- Keine logische Struktur: Optionen mehrfach vorhanden, Filterregeleigenschaften schwer auffindbar: verbergen sich unter System, Globale Anwendungs- und Systemregeln.
- Filtern auch nach IP-Bereichen/-Ports möglich.
- Standard Plugins:
  - Aktive Elemente (ActiveX, JavaScript, Popup, versteckte Frames,…)
  - DNS-Cache
  - Erkennung von Angriffen (Intrusion Detection)
  - Web-Filter (blockt Inhalte, Adressen/Domains, falls vorgegebenes Keyword detektiert wird)
  - Filter für Dateianhänge für E-Mails.
  - Werbefilter (filtert Werbungen auf WWW-Seiten).
- Kennwortschutz für Sicherheitseinstellungen.
- Import-, Exportfunktion der Firewall-Einstellungen.

<u>Bemerkungen zu den durchgeführten Tests</u>

LeakTest: bemerkt Modifizierung von opera.exe und meldet dies. Nach Blockieren, gelingt es LeakTest nicht eine Verbindung aufzubauen.

Tooleaky: dem Tool gelingt es nicht Daten zu senden. Outpost protokolliert korrekt: „Disable all activity for iexplore.exe because it run hidden“, meldet aber keinen Hinweis an den Anwender.

Firehole: es wird eine Modifizierung an opera.exe festgestellt. Wird opera.exe geblockt, ist es Firehole nicht mehr möglich Daten zu senden. Zudem kann die DLL-Datei angezeigt werden, die opera.exe aufgerufen hat.

pcAudit: es konnten ohne Hinweis der Firewall, Daten zu einem Server im Internet gesendet werden. Dazu gehören: Auf dem Rechner befindliche Daten, Abbild des Monitors und Rechnerinformationen. Andere Daten wären somit auch möglich. In der Log-Datei erscheint der Eintrag: „Windows Explorer HTTP Connection“.

4 Entwicklung eines HTTP-Plugins für die Outpost Personal Firewall

In diesem Kapitel wird näher auf die Architektur der Outpost Personal Firewall sowie auf die konzeptionelle Umsetzung des zu entwickelnden Plugins, welches im Folgenden mit HTTP-Record bezeichnet werden soll, eingegangen. Außerdem erfolgt in Kapitel 4.3 ein kurzer Vergleich zwischen einem bereits verfügbaren Plugin mit ähnlicher Funktion und HTTP-Record.

Definitionen, die zum Verständnis der nachfolgenden Unterkapitel benötigt werden:

- Network Driver Interface Specification (NDIS). Von Microsoft und 3Com entwickelter Treiber auf Kernelebene (setzt direkt auf die Hardware auf), der zwei Funktionalitäten bietet:
  1) Verwalten von Netzadaptern unter einem Microsoft Betriebssystem, worunter auch das Verwalten von gesendeten und empfangenen Daten durch diese Netzadapter fällt.
  2) Dient als Schnittstelle für über der Kernelebene liegende Treiber wie Transport-Protokoll Treiber.
- Transport Driver Interface (TDI). Von Microsoft entwickelte Schnittstelle, die über der NDIS-Ebene liegt. Sie ermöglicht Anwendungsschichtprotokollen auf verschiedene Transportschichtprotokolle zuzugreifen.
- Dynamic Link Library (DLL). Ausführbare Datei, die eine gemeinsam genutzte Bibliothek von Funktionen darstellt. Mittels dynamischer Verknüpfung kann ein Prozess eine Funktion aufrufen, die nicht in seinem ausführbaren Code enthalten ist. Der ausführbare Code der Funktion befindet sich in einer DLL, die eine oder mehrere Funktionen enthält, die kompiliert, verknüpft und unabhängig von den Prozessen, von denen sie aufgerufen werden, gespeichert werden. DLLs erleichtern außerdem die gemeinsame Nutzung von Daten und Ressourcen. Mehrere Anwendungen können gleichzeitig auf den Inhalt einer einzigen Kopie einer im Arbeitsspeicher enthaltenen DLL zugreifen [Microsoft].
- Open Database Connectivity (ODBC). ODBC ist ein Interface, mit dem Anwendungen auf Daten in jeder beliebigen Datenbank zugreifen können, für die ein ODBC-Treiber vorhanden ist.

Für die Entwicklung des Plugins wurden folgende Entwicklungs-Werkzeuge eingesetzt:

- Outpost Software Development Kit (SDK) 2.1. Frei verfügbare Entwicklungs-

umgebung von Agnitum, die das Entwickeln von Plugins für die Outpost Personal Firewall ermöglicht.

- Microsoft Core SDK (Windows Server 2003, Build 5.2.3790.0) aus dem Microsoft Platform SDK.
- Microsoft Visual Studio 6.0 (Service Pack 6).

4.1 Architektur der Outpost Personal Firewall

Die Architektur der Outpost Firewall ist hauptsächlich in zwei Teile gegliedert, der Kernelebene (Abb. 1) und der Outpost Firewall Shell (Abb. 2), die auf die Kernelebene aufsetzt. Wegen des modularen Aufbaus der Kernelebene ist es einem Entwickler möglich, protokollspezifische Plugins in Form von DLLs zu implementieren. Die zentrale Instanz auf Kernelebene ist der FILT Driver, der NDIS- und TDI-Verkehr überwacht, behandelt, die Art des verwendeten Protokolls ermittelt und durch einen spezifischen Code, die Outpost Firewall Shell über die Art des Netzverkehrs benachrichtigt. Der FILT Driver bietet folgende Funktionalität:

- Überwachung von übertragenen Paketen
  - Behandlung von Ethernetframes und filtern der Ethernetadresse.
  - Behandlung von IP-Paketen und Analyse der TCP/UDP/ICMP Header (IP-Adresse, TCP/UDP Portnummer, ICMP-Code).
  - Zusenden von Paketen an Plugins zum Zwecke der Analyse und des Filterns von Netzverkehr.
  - Generierung von Paketen auf Anforderung eines Plugins.
- TDI-Behandlung
  - Überwachung des Öffnens und Schließens von Verbindungen (TCP/IP) durch Anwendungen, die vom TDI-Interface Gebrauch machen.
  - Überwachung des TCP-Verkehrs einer Anwendung.
  - Zusenden des behandelten Datenstroms an die Plugins zur Analyse und Filterung des Datenstroms.
  - Unterbrechen (Pausieren) einer Verbindung im Falle, dass eine Interaktion mit dem Anwender notwendig ist.

In Abb. 1 sind die vom FILT Driver behandelte und überwachte Datenströme veranschaulicht:

1) NDIS-Pakete (blau). Überwachung von IP/TCP/UDP/ICMP-Header und Übergabe der Kontrolle an die Kernel-Plugins (NAT, PROTECT), die ggf. eine Verbindung unterbrechen können.
2) TDI-Verkehr (grün). Überwachung von TCP-Verbindungen und Behandlung des TCP-Datenverkehrs mit Hilfe der Kernel-Plugins (POP3FILT, NNTPFILT, HTTPFILT, MAILFILT, HTMLFILT, ADBLOCK).
3) Datenaustausch mit der Outpost Firewall Shell (rot). Datenaustausch zwischen dem FILT Driver und der Outpost Shell, sobald ein neues Ereignis auftritt.

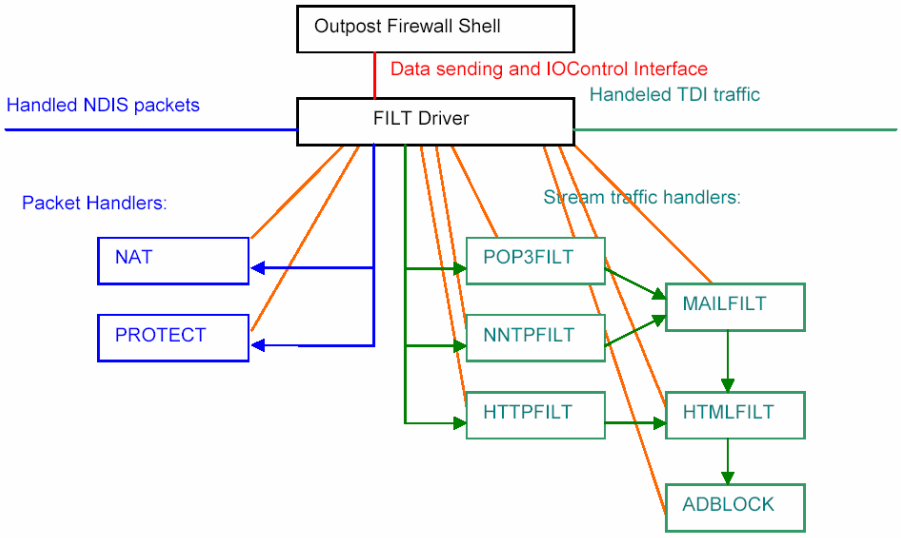

Abb. 1: Aufbau der Outpost Firewall-Architektur auf Kernelebene [Agnitum, 2004]

Die Outpost Firewall Shell (Abb. 2) leitet die von der Kernelebene erhaltenen Pakete an jedes aktive Plugin separat weiter und ist unter anderem für das graphische User Interface zuständig. Die Shell wird durch die ausführbare Datei outpost.exe, die die Firewall und die Plugins lädt und aktiviert sowie die Interaktion mit dem FILT Driver übernimmt, und zwei DLLs realisiert: engine.dll (Engine) und opst_ui.dll (Outpost UI bzw. Outpost User Interface). Die Engine ist immer dann aktiv, wenn outpost.exe gestartet wird. Ihre Aufgabe besteht in der Kommunikation mit den Plugins sowie in der Überwachung von Anwendungen und zu den Anwendungen gehörende Verbindungen und Ports. Das Outpost User Interface wird geladen, wenn sich ein Anwender beim Betriebssystem anmeldet. Es übernimmt die Visualisierung der Outpost Firewall und des Netzverkehrs.

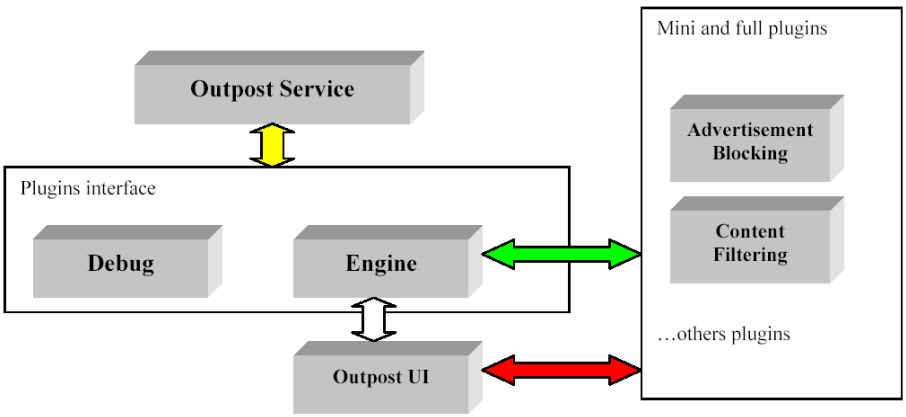

Abb. 2: Aufbau der Outpost Firewall-Shell [Agnitum, 2003]

Das Outpost Journaling System (OJS) weist die in Abb. 3 dargestellte Architektur auf. Die von den Plugins behandelten Daten werden an die Microsoft Datenbank Engine übergeben, wo die Daten aufbewahrt werden. Für Plugin-Entwickler ist das OJS von großem Interesse, da es das Abfragen und Visualisieren der Daten in der Datenbank in Form von Spalten und Zeilen ermöglicht. Den Spalten lassen sich Typen zuordnen (z.B. Zeit/Datum, Zeichenkette, IP-Adresse) anhand derer

sich flexible und gezielte Abfragen tätigen lassen. Dadurch kann eine unübersichtliche lange Liste auf ein Minimum reduziert werden.

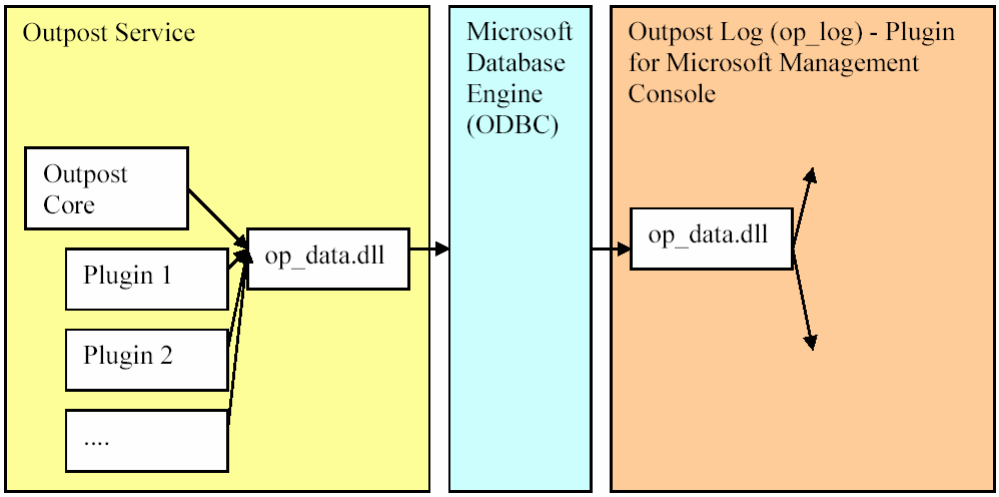

Abb. 3: Architektur des Log Journaling System [Agnitum, 2003]

4.2 Konzept von HTTP Record

Das Einsatzgebiet von HTTP Record sind die für jedermann (vgl. Kapitel 1) verfügbaren Einzelplatzrechner der Hochschul- und Kreisbibliothek und dient der Aufzeichnung von aufgerufenen URLs im Internet in Form einer Liste. Durch Analyse der gespeicherten Liste soll es der Bibliothek ermöglicht werden, festzustellen, ob Benutzer der Rechner jugendschutzgefährdende URLs aufgerufen haben und ggf. diese URL mit Hilfe eines speziellen Proxys unerreichbar zu machen.

Damit ein Benutzer das Plugin nicht deaktivieren kann, wurde von der in der Outpost Firewall integrierten Passwortabfrage Gebrauch gemacht. Versucht der Anwender das Plugin zu deaktivieren erscheint ein Fenster, das zur Passworteingabe auffordert. Das Passwort wurde vorher von einer berechtigten Person festgelegt.

Da jedes Paket mit einem spezifischen Code etikettiert ist, kann ein Plugin die Art des Paketes erkennen (es handelt z.B. um ein HTTP-Paket) und entscheiden, ob es das Paket annimmt und weiterverarbeitet. Abb. 4 zeigt das Funktionsprinzip in Form eines Flussdiagramms auf das HTTP Record beruht. Sobald die Outpost Engine Kenntnis über eine neue Nachricht hat, sendet sie jedem aktiven Plugin die Nachricht zu, in der auch die Identifikationsnummer (ID) über die Art der Nachricht enthalten ist. HTTP Record entscheidet aufgrund dieser ID, ob es sich um eine HTTP-Nachricht handelt. Ist dies der Fall, so werden weitere Informationsstrukturen der Nachricht analysiert. Outpost stellt folgende Informationsstrukturen für eine HTTP-Nachricht zur Verfügung:

- HTTP Anfrage- und Antwort-Headerargumente. Anfrage- und Antwortargumente die sich ein Client und ein Server gegenseitig zusenden wie User Agent (z.B. Browsertyp), Server-Hostname, Server-Typ, akzeptierte Sprachen, usw (weitere Headerargumente siehe [Berners-Lee et al., 1996] bzw. [Fielding et al., 1999). HTTP Record ignoriert diese Informationsstruktur aufgrund großer Informationsmengen und für das spezielle Einsatzgebiet unbrauchbarer Informationen.
- HTTP Anfragedaten. Struktur, die Informationen über die Server-Adresse, die verwendete HTTP-Protokollversion und der aufgerufenen URI (Unified

Resource Identifier: Zeichenkette, die eine verwendete Netzwerkressource, wie z.B. auf den Servern aufgerufene Dateien, identifiziert) liefert.

- HTTP Antwortdaten. Struktur, die Informationen über Server-Adresse, die vom Server auf Client-Anfragen gelieferte Antworten und Statuscodes liefert.
- HTTP URL. Struktur, die Informationen über Server-Adresse und auf Server aufgerufene URL liefert.

Zusätzlich zu den Informationen aus den drei Strukturen wird zu jeder Nachricht die Anwendung ermittelt, die eine HTTP-Anfrage stellt oder eine HTTP-Antwort erhält sowie die Ankunftszeit und das Datum der Nachricht festgehalten.

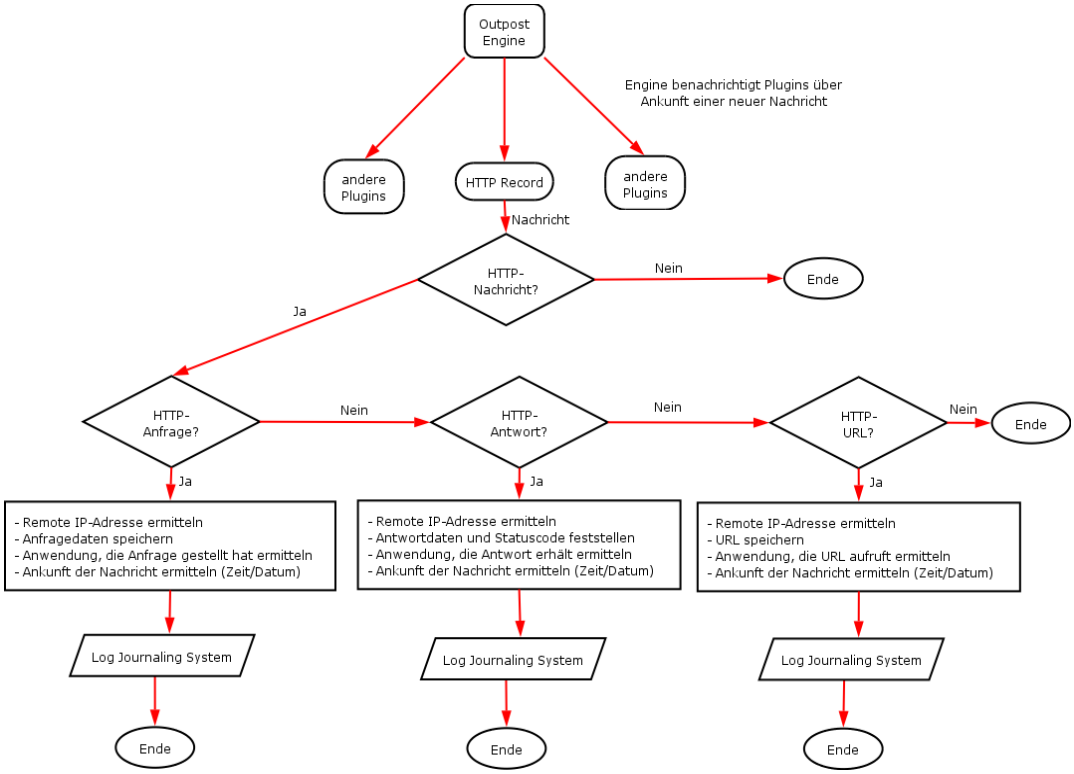

Abb. 4: Funktionsprinzip HTTP Record

Als besonders nützlich erweisen sich die flexiblen Filtermöglichkeiten, die die Outpost Firewall für die in der Datenbank verwalteten Daten bietet. HTTP Record bietet die Spalten Zeit/Datum, Anwendung, Information (URLs, Anfrage- und Antwortdaten), IP-Adresse und Ereignis (Typ der Information in Spalte Information) (Abb. 5).

HTTP Record

Aktualisieren | Filter hinzufügen

Datum/Uhrzeit	Anwendung	Information	IP-Adresse/Domain	Ereignis
14.10.2004 14:47:46	Opera Internet Browser	Not Modified	zylous.bei.t-online.de	ANSWER - 304
14.10.2004 14:47:46	Opera Internet Browser	Not Modified	dict.tu-chemnitz.de	ANSWER - 304
14.10.2004 14:47:46	Opera Internet Browser	http://zylous.bei.t-online.de/images/logo_scorp.gif	zylous.bei.t-online.de	URL
14.10.2004 14:47:46	Opera Internet Browser	GET /images/logo_scorp.gif	zylous.bei.t-online.de	REQUEST
14.10.2004 14:47:46	Opera Internet Browser	http://zylous.bei.t-online.de/standard.css	zylous.bei.t-online.de	URL
14.10.2004 14:47:46	Opera Internet Browser	GET /standard.css	zylous.bei.t-online.de	REQUEST
14.10.2004 14:47:46	Opera Internet Browser	http://dict.tu-chemnitz.de/favicon.ico	dict.tu-chemnitz.de	URL
14.10.2004 14:47:46	Opera Internet Browser	GET /favicon.ico	dict.tu-chemnitz.de	REQUEST
14.10.2004 14:47:46	Opera Internet Browser	Not Found	zylous.bei.t-online.de	ANSWER - 404

Abb. 5: Aufgezeichnete Ereignisse von HTTP Record

Anhand dieser Spalten lassen sich permanente Filter erstellen (Abb. 7), die nur

die im Filter festgelegten Ereignisse aufzeichnen. Abb. 7 verdeutlicht dieses Vorgehen. Die Funktionen der Spalten haben im Einzelnen folgende Bedeutung:

Name der Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit des aufgezeichneten Ereignisses.
Anwendung	Anwendung, die Daten sendet oder Daten empfängt.
Information	Für das entsprechende Ereignis empfange oder gesendete Daten.
IP-Adresse/Domain	Server von dem Daten empfangen oder gesendet werden.
Ereignis	Typ des Ereignisses (URL, Anfrage, Antwort des Servers mit Statuscode)

Abb. 6: Bedeutungen der Spalten in HTTP Record

Dadurch, dass die von HTTP Record aufgezeichneten Daten durch das Outpost Journaling System verwaltet werden, konnte HTTP Record um zusätzliche Funktionalität bereichert werden. Diese sind im Einzelnen:

- Exportieren aller aufgezeichneten Daten – auch für jeden erstellten Filter separat möglich – oder nur in der Liste markierte Einträge in eine Datei.
- Individuelle Einstellung bezüglich der Maximalanzahl der aufzuzeichnenden Einträge sowie der maximalen Zeitdauer in Tagen, in der Ereignisse aufgezeichnet werden sollen.
- Verstecken von einzelnen Spalten.
- Löschen aller Einträge oder Löschen von Einträgen bis zu einem bestimmten Datum.

4.3 Vergleichbare Plugins

Ein vergleichbares Plugin eines Drittanbieters (HTTPLog) bietet ebenfalls das Aufzeichnen von HTTP-Ereignissen. Dieses wurde jedoch für die Outpost Personal Firewall 1.0 entwickelt, die noch kein Journaling System besaß. HTTPLog zeichnete alle Ereignisse in einer Liste auf, die keine weitere Filtermöglichkeit aufwies. Je größer die Liste wurde, desto unübersichtlicher wurde sie auch. Beim Versuch eine aufgezeichnete Liste in eine Datei zu speichern, kam es oft zum Absturz der Firewall. Außerdem wurde die Server-IP-Adresse, von der die angeforderten Daten stammen, nicht aufgezeichnet. Die Vorteile von HTTP Record gegenüber HTTPLog bestehen in seinem Funktionsumfang, seiner Filter-Flexibilität und Stabilität.

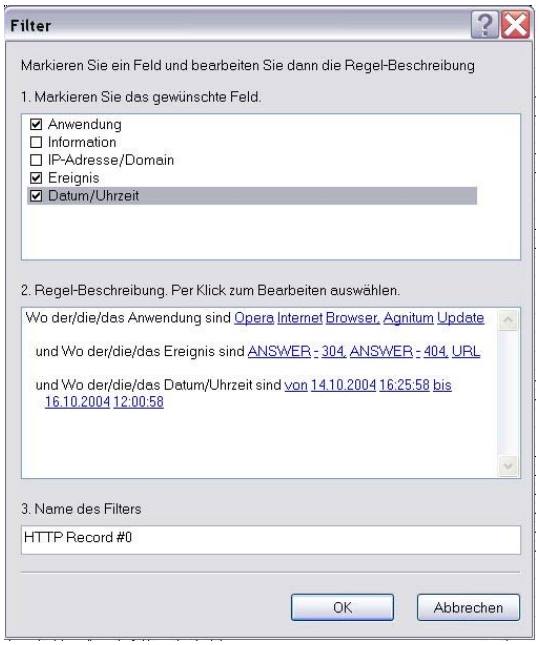

Abb. 7: Beispiel für einen Filter für HTTP Record

5 Zusammenfassung

In dieser Arbeit wurde aufgezeigt, dass in öffentlichen Bibliotheken mit Internet-Arbeitsplätzen (technische) Maßnahmen zu ergreifen sind, die Minderjährige vor jugendgefährdende Web-Inhalte schützen und den Zugang zu diesen erschweren. Aus rechtlicher Sicht sind diese Maßnahmen auf jeden Fall zu ergreifen, wenn die Bibliothek Kenntnis darüber hat, dass rechtswidriger Inhalt aufgerufen wurde. Nicht nur die gesetzlichen Bestimmungen verpflichten zu aktiven Maßnahmen, sondern auch die Tatsache, dass öffentlichen Bibliotheken eine aktive Rolle bzgl. des Jugendmedienschutzes zugeschrieben wird. Eine Möglichkeit zur Erfüllung dieser Pflicht, stellt Filtersoftware dar, die zum einen den Zugang zu jugendgefährdende Inhalte blocken kann und zum anderen zusätzlich vor Malware schützen kann. Außerdem erlaubt sie die Protokollierung des Datenverkehrs. Im Rahmen dieser Arbeit wurde das Protokollier-Werkzeug HTTP Record entwickelt, dass in die Outpost Firewall integriert werden kann und die Protokollierung und flexible Filtermöglichkeiten aufgerufener Ressourcen im WWW durch das HTTP-Protokoll erlaubt. Die von HTTP Record protokollierten Daten können von der Bibliothek verwendet werden, um festzustellen, ob im Sinne der in dieser Arbeit vorgestellten gesetzlichen Bestimmungen rechtswidrige Web-Inhalte von Bibliotheksnutzern aufgerufen wurden.

6 Literatur

Agnitum: Developing of Kernel Plug-ins of Outpost Firewall, o.O. 2004.

Agnitum: Developing of Interface Plug-ins of Outpost Firewall, o.O. 2003.

Berners-Lee, T., Fielding, R., Frystyk, H.: Hypertext Transfer Protocol -- HTTP/1.0, RFC 1945, o.O., Mai 1996.

Brauch, P.: Kostenloser Brandschutz, in: c't, (2004) 13, S. 142 – 147.

Bundesministerium für Familie, Senioren und Jugend (Hrsg.) : Jugendschutz und Jugendmedienschutz-Staatsvertrag der Länder (mit Erläuterungen), Bonn 2003.

Cheswick, R. W.; Bellovin, S. M.; Rubin, A. D.: Firewalls und Sicherheit im Internet, 2. Auflage, deutsche Übersetzung von Thomas Maus, Addison-Wesley, München 2004.

Der Brockhaus. Computer und Informationstechnologie, Bibliographisches Institut & FA Brockhaus AG, Leipzig 2003.

Fielding, R. et al.: Hypertext Transfer Protocol -- HTTP/1.1, RFC 2616, o.O., Juni 1999.

Meinel, C.; Sack, H.: WWW, Springer Verlag, Berlin et al. 2004.

Müller, H.: Jugendschutz und Internet-Zugang (Filtersoftware oder was?), in: Bibliotheksdienst 33. (1999), S. 1905, o.O.

Strobel, S.: Firewalls für das Netz der Netze, dpunkt.verlag, Mörlenbach 1997.

7 Abbildungsverzeichnis

Anhang A.1 - Firewall Testergebnisse

Tests in der Out-of-the-Box-Einstellung

		Leaktester		**DLLInjection**		**Beenden der Firewall**
Firewall	Version	LeakTest	Tooleaky	Firehole	Pcaudit	Phatbot*
Kerio	4.0.16	ok	ok	fail	ok	fail
Securepoint	3_6_8	ok	fail	ok	ok	ok
Sygate	5_5	ok	ok	fail	fail	ok
ZoneAlarm	4.5.594	ok	fail	fail	fail	ok
Look 'n' Stop	2_05	ok	ok	ok	fail**	/
Outpost	2.1.303.4009	ok	ok	ok	fail	fail***

ok: Test bestanden
fail: durchgefallen

* bis auf look 'n' stop, entnommen aus [Brauch, 2004]
** ok bei aktivierter DDL-Injection-Erkennung
*** bei aktivem Passwortschutz ok