Content-Filterung

*Bert Weingarten, Hamburg **

Für Unternehmen in Europa und Deutschland besteht Handlungsbedarf. Das Internet nimmt in immer mehr Unternehmen einen festen Platz in der Kommunikationsstruktur ein. Es wird benutzt, um Informationen auszutauschen, z. B. via E-Mail, oder aber, um komplexe Datenbanken und Content-Angebote abrufen und fernwarten zu können. Jedes Unternehmen, das einen Zugang zum Internet besitzt, hat dadurch die Möglichkeit, schnell auf unzählige Informationen zuzugreifen. Diese Flut an Informationen aus allen Interessenbereichen kann aber auch dazu führen, dass sich die Mitarbeiter eines Unternehmens auf Internetseiten und bei Content-Angeboten aufhalten, die sie persönlich interessieren, die aber nicht unmittelbar die Interessen des Unternehmens, für welches sie tätig sind, abdecken.

1 Produktivitätsverlust durch uneingeschränkte Internet-Nutzung

Dies kann die Produktivität einer Firma enorm senken. Wenn sich ein Mitarbeiter nur 1 Stunde pro Tag auf Internetseiten und Web-Content seines persönlichen Interesses aufhält, summiert sich das auf den Monat und das Jahr gesehen zu einem Zeitverlust für die jeweilige Firma von 240 Arbeitsstunden.

Neben dem Produktivitätsverlust kann es in ungünstigen Fällen auch zu Imageschäden des Unternehmens führen. Wenn sich ein Mitarbeiter z. B. auf pornografischen Angeboten oder anderen extremen Inhalten aufhält und beim Kommunizieren die E-Mail

Abbildung 1

Adresse der Firma benutzt, so kann es passieren, dass eine Firma verklagt wird, wenn vom Mitarbeiter dieser Firma z. B. jemand unter Druck gesetzt oder verbal angegriffen worden ist. Auch vorstellbar ist die Situation: Ein Mitarbeiter benutzt den Internetzugang der Firma, um mit verbotenen Videos oder Bilder, zu handeln. Die Anklagen und die daraus resultierenden Unannehmlichkeiten wie Hausdurchsuchung, Beschlagnahme von Gerätschaften bis hin zur Anzeige der Unternehmensführung sind oftmals das unerwünschte Resultat.

Content-Filterung ist eine Möglichkeit, um ein Unternehmen vor Produktivitätsverlust, vor Imageschäden und vor beträchtlichen wirtschaftlichen Schäden zu bewahren, ganz gleich, ob das Unternehmen schon lange am Internet ist, erst kürzlich angeschlossen worden ist, oder noch angeschlossen wird. Content-Filterung verbessert in jedem Fall die Arbeit und Arbeitsweise der Mitarbeiter des Unternehmens mit dem Internet.

Content-Filterung ermöglicht den Unternehmen, Bandbreite zu sparen. Es ist den Mitarbeiten nicht mehr ohne weiteres möglich, für ihr privates Interesse, z. B. Videos, MP3-Files oder Bilder aus dem Internet zu la-

INHALT:

* Geschäftsführer PAN AMP

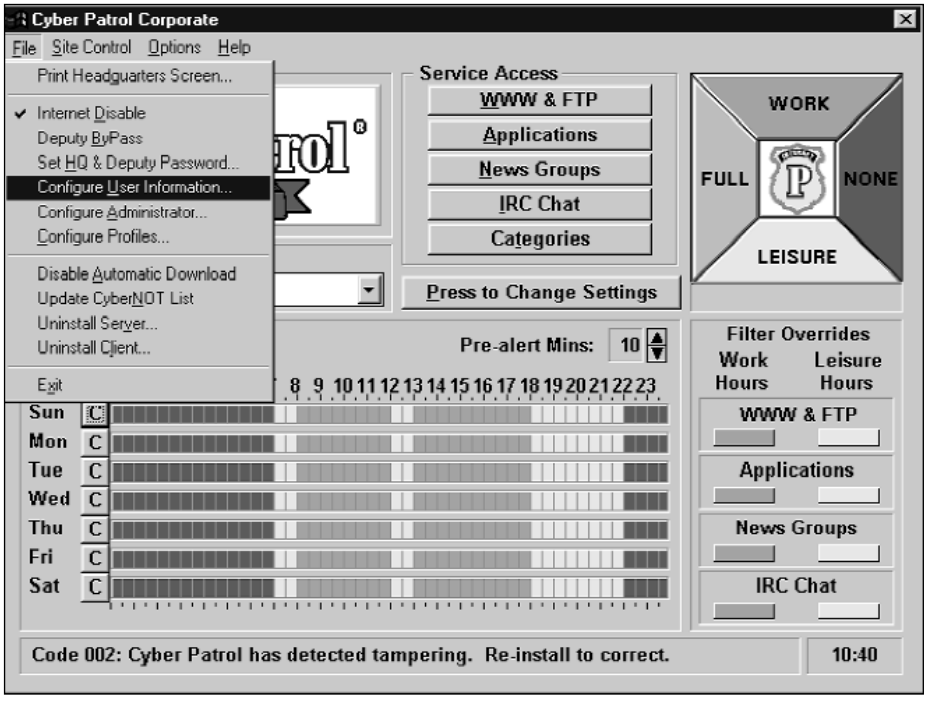

Abbildung 2

den. Die Zugangsleitung zum Internet wird dadurch oft stundenlang benutzt und verlangsamt den Zugriff auf Inhalte, die für die Firma von Interesse sind.

Bevor man ein System zur Content-Filterung installiert, sollte man überprüfen, ob alle Systemanforderungen eingehalten werden. Im folgenden Beispiel beziehe ich mich vorwiegend auf die Installation von Cyber Patrol-Corporate als Content-Filter in ein bestehendes Windows 3.1-, 9x-, NT-Netzwerk.

Die Installation muß in einem Netzwerkordner erfolgen, auf den alle Benutzer Zugriff haben. Jeder Benutzer muß sowohl Zugang zum Internet als auch zu dem Netzwerkordner haben.

Hier unterscheiden sich die verschiedenen Versionen von CyberPatrol grundlegend in ihren Anforderungen, da bei CyberPatrol Proxy und auch bei CyberPatrol LAN nur der Server-Rechner Zugang zum Internet haben muss und dieser den Client-Rechnern den Zugang zum Internet ermöglicht.

Der Administrator bestimmt einen Rechner, mit dem er den Content-Filter administrieren will. Von diesem Rechner aus installiert er das Programm in den Netzwerkordner auf dem Server. Die Datenfiles werden installiert.

Vor dem Start des Programms erscheint die Nachfrage, ob der Internetzugang durch eine Firewall geschützt ist. Ist dies der Fall, trägt man den Socks-Server-Namen und die weiteren Angaben in die Dialogbox ein.

Unter CyberPatrol Corporate werden die folgenden Daten in das Verzeichnis c:\windows installiert:

- !cp.exe
- dbadm.dll
- ic.exe
- icp.log
- ts.dll
- ts16.dll
- ts32.dll
- unwise.dll
- usage.log

Zur Deinstallation des Content-Filters ist die Benutzung des Uninstall-Clienten empfohlen, um das oben genannte Sperr-Verhalten nicht auszuführen.

Auf Windows NT Systemen kann der Administrator die Lese- und Schreibrechte selbst festlegen und braucht deshalb die obigen Hinweise auf mögliche Datenveränderungen nicht zu beachten.

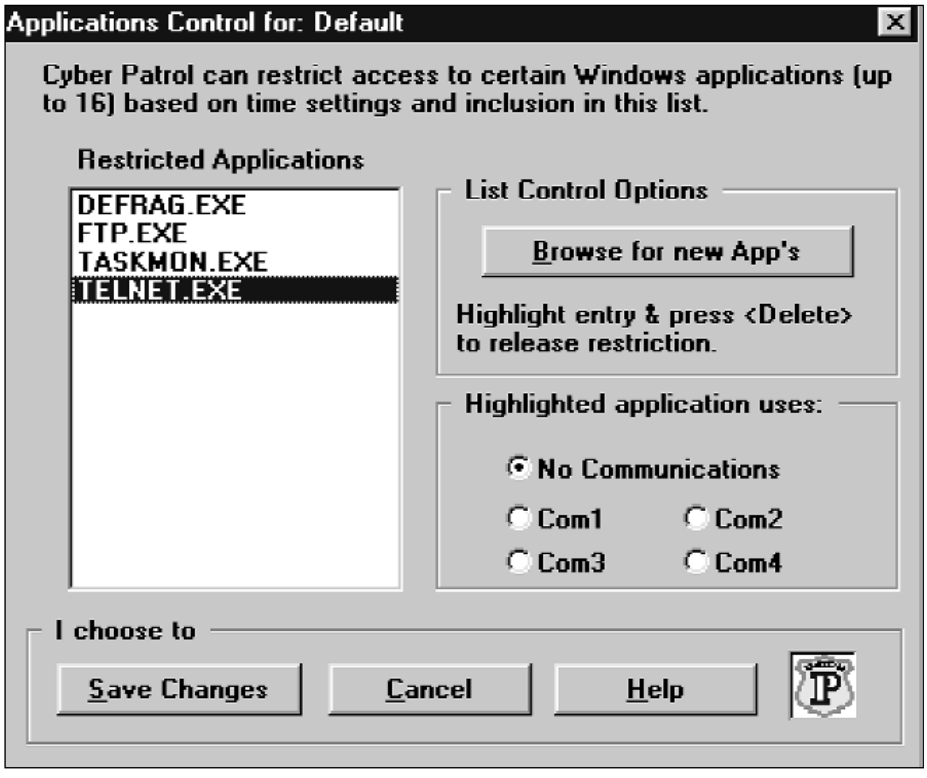

Abbildung 2

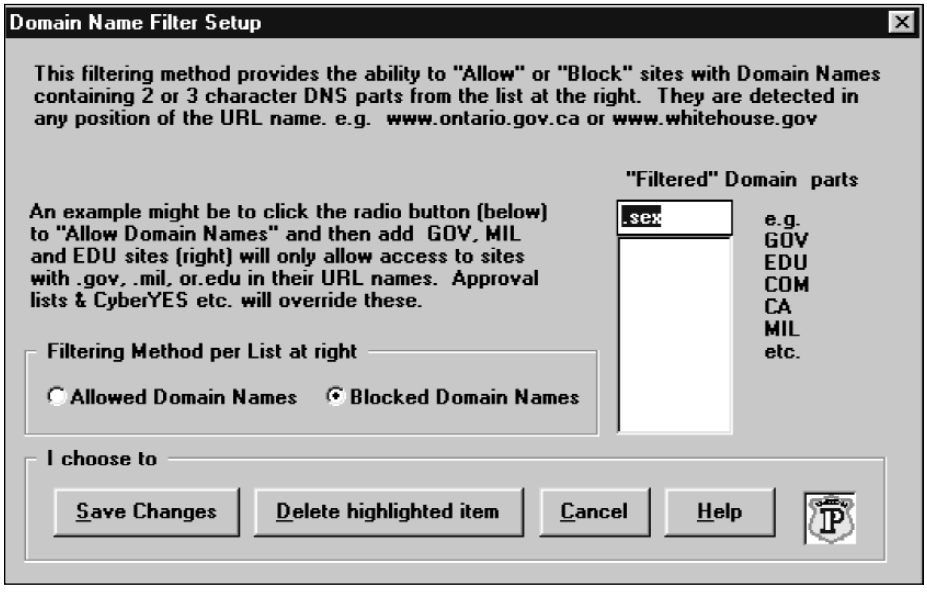

Abbildung 4

2 Content-Filter – Konfiguration

Anhand der CyberPatrol Corporate-Version führe ich Ihnen in Abbildung 1 und 2 die wesentlichen Leistungsmerkmale eines Content-Filters auf :

Nach der erfolgreichen Installation erfolgt der Erstaufruf des Content-Filters. Es erscheint ein Eingabefester zur Festlegung und Bestätigung des „Head Quarter Password“ kurz „HQP“ (Abb. 1). Das vergebene Passwort sollte nicht in Vergessenheit geraten.

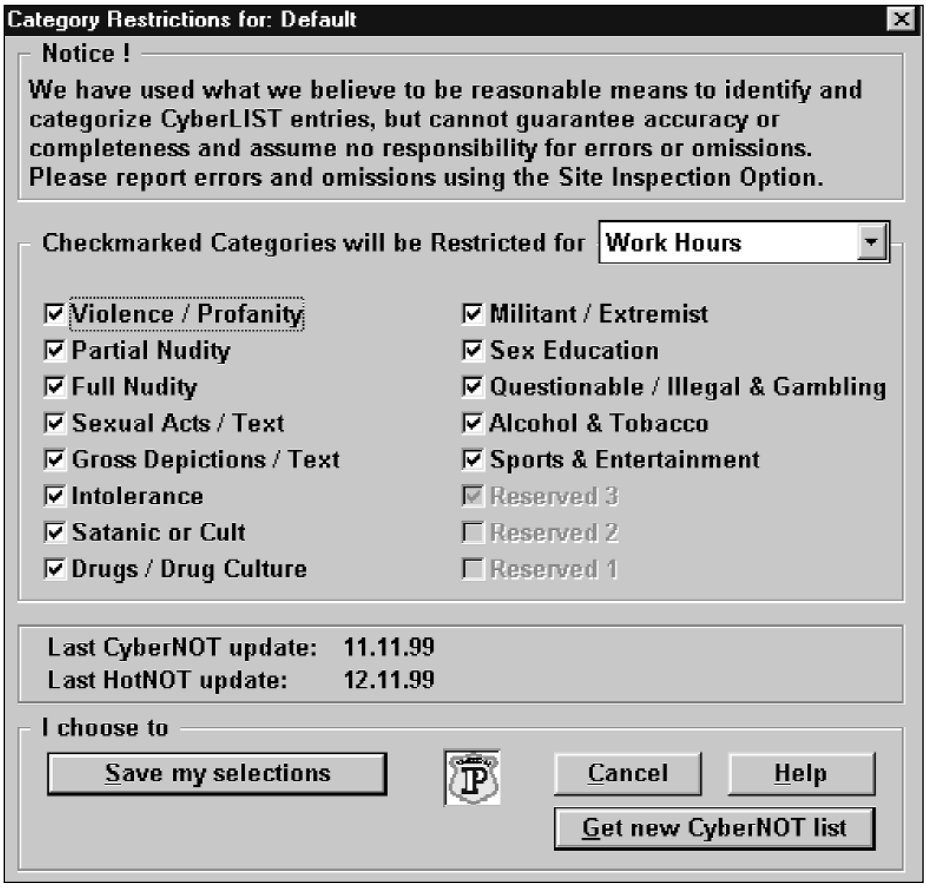

Abbildung 5

Über das Main-Menue erfolgt die Erstellung von Profilen und die Zuweisung der User in das Main-Menue (Abb. 2). Es ist möglich, neun verschiedene Profile zu erstellen, denen jeweils uneingeschränkt viele User zugewiesen werden können.

Jedem Profil kann ein Passwort zugeteilt werden, welches bei jedem Aufruf einer Anwendung abgefragt wird. Diese ständige Passwortabfrage kann man aber auch deaktivieren. Wie sich daraus ablesen lässt, spielt dabei die Winsock.dll eine große Rolle. Wenn also der Zugang zum Internet vollkommen untersagt ist, ist der Zugang zur Winsock.dll durch den Content-Filter gesperrt.

3 Content-Filterung – weitere Optionen

Als weitere Option stehen die folgenden Applikationen für Administratoren zur Verfügung: siehe Abbildung 3 und 4.

Applications Control:

Content-Filter bieten die Möglichkeit, den Aufruf von Anwendungen zu kontrollieren (Abb. 3). Dazu trägt man die *.exe Datei einfach in die Liste der Anwendungen ein, die man kontrollieren will, und diese wird je nach Einstellungen, die zu diesem Zeitpunkt auf dem Client-Rechner gelten, behandelt.

Wenn also z.-B. der Zugang zur notepad.exe kontrolliert werden soll und es gerade keinen Zugang für dieses Profil gibt, so kann die Anwendung Notepad nicht gestartet werden. Erst wenn das Profil wieder Zugang erhält, sei es auch nur teilweise, kann die Anwendung wieder gestartet werden. Programme können mit einer Auswahlfunktion in Sperrliste aufgenommen werden. Diese Funktion ist für öffentliche Terminals eine oft nachgefragte Erweiterung, um Systemmanipulationen vorzubeugen.

Keyboard-Monitoring-Tools:

Der Chat Gard ist ein integriertes Keyboard-Monitoring-Tool. Es über-

wacht alle Einträge, die der Benutzer während seiner Online Zeit macht. Im Menü vom Chat Gard lassen sich wichtige Informationen wie die Telefon- und Kreditkarten Nummer eintragen. Wenn der Benutzer nun die Kreditkartennummer der Firma an Dritte weitergeben möchte, die diese Informationen aber gar nicht erhalten sollen, so überschreibt der Chat Gard diese Zeilen mit „x“. Es können aber auch alle anderen erdenklichen Worte mit in die Liste aufgenommen werden, wie zum Beispiel Passwörter.

Pics Rating:

Verschiedene Content-Filter unterstützen den „Recreational Software Advisory Council (RSAC) Internet Bewertungsstandard“. Die RSACi liefert für Internetseiten eine Bewertung nach Gewalt, Sex, Nacktheit und Sprache. Administratoren können diesen Zusatzfilter nutzen oder ausschalten.

Internet Relay Chat Control:

Der Internet Relay Chat Filter benutzt das gleiche Prinzip wie der Domain Name Filter.

In eine Liste kann man Schlüsselwörter eintragen, wie z. B. „sex“ oder „porn“. Wenn nun eines dieser Wörter in den Namen der Chaträume vorkommt, kann man diesen Raum nicht betreten. Es ist jedoch möglich, explizit Chaträume zuzulassen, indem man die Raumnamen in eine separate Liste einträgt. Domain Name Filters:

Mit dem Domain Name Filter ist es möglich, ganze Domain Namen zu sperren oder freizugeben (Abb. 4). Es ist auch möglich, nur ein Teilwort einzugeben, was herausgefiltert wird. Dieses Tool untersucht genauestens den Domainnamen, den der Benutzer eingibt. Wenn man zum Beispiel „ney“ in die Liste der gesperrten Domain Namen einfügt, so ist der Aufruf von www.disney.com untersagt. Steht in dieser Liste zusätzlich noch „de“, so kann kein Domain Name mit der Endung „.de“ aufgerufen werden.

Abbildung 6

Möglichkeit	Farbe	Beschreibung
None	Rot	Der Internet-Zugang ist gesperrt.
Full	Blau	Kompletter, uneingeschränkter Internetzugang.
Work	Grün	Gefilterter Zugang mit Augenmerk auf die Arbeitsstunden.
Leisure	Gelb	Gefilterter Zugang mit Augenmerk auf die Freizeitstunden.

Somit können gesamte Content-Ausrichtungen von Top-Level Domain Names ausgegliedert werden.

Diese Option wird mit Freigabe der neuen Top-Level-Domain`s (TLD`s) wie z.B. „.sex“ eine wichtige Funktion ausüben.

4 Kernstück der Content-Filterung – die Sperr- und Freigabe-Listen

Das „Kernstück“ von Content-Filtern besteht aus den Sperr- und Freigabe-Listen.

Die Speer-Liste liegt in verschlüsselter Form im Hauptverzeichnis. Sie beinhaltet Seiten, auf denen der Internetzugang für den jeweiligen Benutzer verweigert werden soll. Die Sperr-Listen sind in die folgenden Kategorien (Abb. 5) unterteilt:

- Violence/Profanity: Bilder oder Texte, die extreme Gewalt oder Grausamkeiten darstellen
- Partial Nudity/ Full Nudity: Z. B. Akt-Fotos
- Sexual Acts: Explizite Darstellung von Geschlechtsverkehr
- Gross Depictions: Explizite Darstellung von grob vulgären oder perversen Handlungen
- Intolerance: Alle Arten von Diskriminierungen, z. B. gegen Rassen, Hautfarben, Religion
- Satanic or Cult:: Bilder oder Texte mit satanischen Inhalten

und andere ...

5 Umfassende Verwaltung von Nutzerprofilen und Filter-Listen

In größeren Unternehmen gibt es verschiedene Abteilungen, die unter-

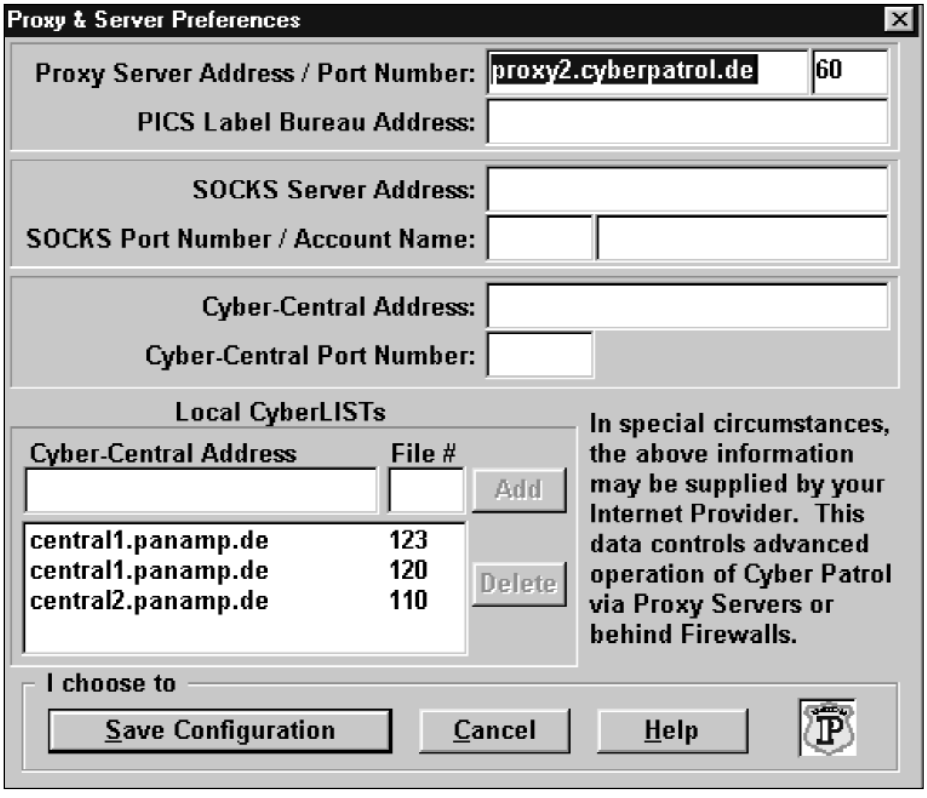

Abbildung 7

schiedliche Aufgaben wahrnehmen. Mit Content-Filterung ist es möglich, für jeden dieser Bereiche ein eigenes Profil anzulegen, welches sich von den verwendeten Listen, Kategorien und den Zeitintervallen unterscheiden kann. So kann man dem Logistik Bereich ein anderes Profil zuteilen als der Fertigungsabteilung und den Mitarbeitern der Nachtschicht nach Ablauf ihrer Arbeitszeit Zugang zu Seiten gewähren, die zum gleichen Zeitpunkt für die Frühschicht gesperrt sind. Ein individueller Internetzugang, entsprechend der Aufgabenstellung der Mitarbeiter, ist möglich und kann in Einzel- oder Gruppen-Profilen hinterlegt werden.

Über ein derartiges Profil können somit in festgelegten Zeitabständen jeweils unterschiedliche Freigaben und Einschränkungen die Möglichkeit der Internetnutzung am Arbeitsplatz definieren. Weitere Einstellungen können in Form einer auszuwählenden Zeitklassifizierung aktiviert bzw. deaktiviert werden. Hierzu gehören die folgenden Möglichkeiten, welche durch einen Farbcode in einer nach Wochentag und Uhrzeit angeordneten Liste frei definierbar sind, siehe Abb. 6.

Als Administrator hat man die Möglichkeit, über das Hauptmenüe Kategorien und Applikationen aufzurufen, einzustellen und bestimmte Kategorien zuzulassen oder zu sperren.

Die Lösung für ein ideal zusammengestelltes Benutzer- oder Gruppenprofil liegt in der Einteilung von Sperr- und Freigabe-Listen in Abhängigkeit von unterschiedlichen Zeitintervallen und Pauseneinstellungen. So kann z. B. für ein Gruppenprofil am Montag von 8:00 Uhr bis 11:00 Uhr eine unternehmenseigene Freigabe-Liste aktiv sein, die nur enthaltene Seiten freigibt. Von 11:00 Uhr bis 13:00 Uhr kommt die Sperr-Liste zum Einsatz und stellt Internet-Content ohne kritische Inhalte zur Verfügung. Ab 13:00 Uhr wird eine weitere Freigabe-Liste aktiv, welche einen neuen Content-Bereich im Internet freigibt.

Es besteht weiterhin die Möglichkeit, Zeitintervalle festzulegen, in denen der Internetzugang gefiltert wird. Man kann z. B. festlegen, dass ein Angestellter von 8-12 und von 13-17 Uhr nicht auf Sport- und Unterhaltungsseiten zugreifen darf, diese aber während der Mittagspause und nach Arbeitsschluss besuchen kann: Die Freigabe-Liste liegt ebenfalls verschlüsselt im Hauptverzeichnis. Wählt man diese an, hat der jeweilige Benutzer nur den Zugriff auf die Internetseiten, die in dieser Liste enthalten sind, und der Zugang zu allen anderen Seiten wird verweigert. Dies konzentriert den Bereich der erreichbaren Seiten natürlich erheblich.

Um als Administrator nicht erfasste Seiten zu sperren oder erreichbar zu machen, kann man zusätzliche Seiten definieren. Man kann eine eigene Freigabe- oder Sperr-Liste definieren und sie zusätzlich oder alleinstehend wie ausgeführt als Filter einsetzen. CyberPatrol bietet die Möglichkeit, jedem Profil verschiedene Filtermöglichkeiten an verschiedenen Tageszeiten zuzuweisen.

CyberPatrol bietet einen automatischen Update Service für die Freigabe- und die Speer-Liste (Abb. 6). Sofern man den Menüpunkt „automatisches Update“ nicht deaktiviert, erhält man vom CyberCentral-Server alle 6 Tage das neuste Update dieser Listen. Da sich der Inhalt und der Umfang der Internets laufend ändern, ist dieser Update Service notwendig, um optimale Sicherheit im Umgang mit Internet-Content im Unternehmen zu gewährleisten. Zusätzlich zu diesem wöchentlichen Update existiert die HotNOT-Liste. Dies ist eine Sperr-Liste, die alle aktuellen Veränderungen der letzten 24 Stunden beinhaltet. Man kann also seine Sperr-Liste öfter updaten als alle 6 Tage, wenn dies gewünscht ist.

6 Besseres Kostenmanagement und höhere Netzsicherheit

Weiterhin spart weniger Internetaufenthalt bei kapazitätsabhängigen Internetzugängen Provider-Kosten, die dem Unternehmen anfallen.

Content-Filterung erhöht die Sicherheit der Rechner- und Betriebsyste-

Nr.	Spaltenname	Typ	Wert	Beschreibung	Grösse	Index
1	DATAVERS	Character		Version of the data	5	N
2	USERNAME	Character		User's network login ID	32	N
3	LOGDATE	Date		Log date	8	N
4	STARTTIME	Character		Start time	8	N
5	ENDTIME	Character		End time	8	N
6	ACTIVETIME	Character		Active time	8	N
7	ACTIVESEC	Numeric		Active seconds	5	N
8	IPADDRESS	Character		IP Address	15	N
9	SERVERNAME	Character		Server name	128	N
10	DIRECTORY	Character		Directory name	128	N
11	CONNECTIME	Character		User connect time	5	N
12	RECVTIME	Character		Received time	5	N
13	FTP	Character	[1]/None	FTP blocked	1	N
14	BLOCKED	Character	[1]/None	Site blocked	1	N
15	MIDNIGHT	Character	[1]/None	Open at midnight	1	N
16	PROFILENUM	Numeric		Profile name	2	N

Tabelle 1

me und schützt vor Spionageangriffen, denn mit der Verminderung der Aufenthaltszonen im Internet bzw. dem Aufenthalt auf nur von dem Unternehmen autorisierten Internetseiten fällt die Wahrscheinlichkeit, dass ein Mitarbeiter unwissentlich ein Virus in das Firmennetz einschleust, das entweder zu Datenverlust oder, wenn es ein Trojaner-Virus ist, zu Datenspionage führen kann.

Die verschiedenen Produkt-Versionen von Content-Filter-Programmen bieten die Möglichkeit, das Produkt in sehr viele bestehende oder neu aufgebaute Firmennetzwerke mit Internetzugang zu integrieren.

7 Auswertung von Nutzerverhalten und Reports

Als weitere Option besteht für Administratoren die Möglichkeit, alle Aktivitäten eines Profils mitzuloggen. Der nachfolgende Report (Tab. 1) zeigt die zur Verfügung stehenden Auswahlkriterien auf.

Anmerkung:

Der Wert für Ftp, Blocked und Midnight kann 1 oder None sein. Wenn der Wert 1 ist, dann bedeutet dies, dass der Benutzer versucht hat, eine gesperrte Seite aufzurufen.

Man kann sich diese Werte auch direkt in einstellbaren Zeitintervallen auf dem Drucker ausgeben oder in eine Datei schreiben lassen. Für diese Automatismen braucht man das Zusatztool CyberPatrol Gateway: Dies wandelt das Collect.log auf dem Server in ein Log.dbf File um, damit es besser les- und druckbar ist.

Eine Auflistung von geblockten Seiten sieht somit wie in Tab. 2 aus.

8 Crystal-Reports, Highend der Nutzerauswertung

Ein Content-Filter beinhaltet eine weitere noch detailreichere Möglichkeit, die Nutzung des Internets auszuwerten: „Internet Use Detail Report“, welcher mit dem beiliegenden Tool Crystal Reports erstellt wird. Diese Art der Auswertung ist in der Darstellungsform als professionellste Auswertung zu benennen.

Ein Beispiel eines Crystal Reports, der die Seiten, die von jedem Benutzer aufgerufen worden sind, sowie das Datum, die Uhrzeit und Zugriffszeit sortiert nach Profilen aufzeigt, siehe Tab. 3.

User: Administrator
panamp1

Blocked-Report
14.11.1999

Domain	Blocked	Start	End	Active
www.doktorspiele.com	B	04:42:14	04:42:20	00:00:06
www.ejakulation.de	B	01:05:25	01:05:43	00:00:18
www.hustler.com	B	03:10:02	03:10:20	00:00:18
www.nba.com	B	04:43:23	04:43:53	00:00:30
www.nfl.com	B	04:43:20	04:43:23	00:00:03
www.planetquake.com	B	04:42:55	04:43:05	00:00:09
www.playboy.com	B	00:21:36	00:26:03	00:04:27
www.playboy.com	B	04:42:02	04:42:08	00:00:06
www.sex.de	B	00:38:31	00:38:37	00:00:06

Tabelle 2

Cyber Patrol Corporate Internet Use Detail Report

11/14/99	04:39:23	04:39:26	0.1		WWW.TOMSHARDWARE.DE/mainboard/99q4/991111/athlon_boards-01.html
11/14/99	04:39:26	04:39:26	0.0		CLASSIC.ADLINK.DE/accipiter/adserver.exe/clcategory=it_multimedia.hw_sw/site=cl_tomshardw
11/14/99	04:39:26	04:39:56	0.5		CLASSIC.ADLINK.DE/accipiter/adserver.exe/clcategory=it_multimedia.hw_sw/site=cl_tomshardw
11/14/99	04:39:56	04:39:56	0.0		WWW.TOMSHARDWARE.DE/mainboard/99q4/991111/athlon_boards-02.html
11/14/99	04:39:56	04:39:56	0.0		CLASSIC.ADLINK.DE/accipiter/adserver.exe/site=bu_tomshardware_de/adtype=gif/39405600725
11/14/99	04:39:56	04:39:56	0.0		WWW.TOMSHARDWARE.DE/mainboard/99q4/991111/athlon_boards-02.html
11/14/99	04:39:56	04:39:56	0.0		CLASSIC.ADLINK.DE/accipiter/adserver.exe/clcategory=it_multimedia.hw_sw/site=cl_tomshardw
11/14/99	04:39:56	04:40:06	0.2		CLASSIC.ADLINK.DE/accipiter/adserver.exe/clcategory=it_multimedia.hw_sw/site=cl_tomshardw
11/14/99	04:40:06	04:40:06	0.1		WWW.TOMSHARDWARE.DE/mainboard/99q4/991111/athlon_boards-03.html
11/14/99	04:40:06	04:40:06	0.1		CLASSIC.ADLINK.DE/accipiter/adserver.exe/site=bu_tomshardware_de/adtype=gif/39405600825
11/14/99	04:40:06	04:40:06	0.1		WWW.TOMSHARDWARE.DE/mainboard/99q4/991111/athlon_boards-03.html
11/14/99	04:40:06	04:40:06	0.0		CLASSIC.ADLINK.DE/accipiter/adserver.exe/clcategory=it_multimedia.hw_sw/site=cl_tomshardw
11/14/99	04:40:06	04:40:17	0.2		CLASSIC.ADLINK.DE/accipiter/adserver.exe/clcategory=it_multimedia.hw_sw/site=cl_tomshardw
11/14/99	04:40:17	04:40:17	0.0		WWW.TOMSHARDWARE.DE/mainboard/99q4/991111/athlon_boards-04.html
11/14/99	04:40:17	04:40:17	0.0		CLASSIC.ADLINK.DE/accipiter/adserver.exe/site=bu_tomshardware_de/adtype=gif/39405601057
11/14/99	04:40:17	04:40:20	0.1		CLASSIC.ADLINK.DE/accipiter/adserver.exe/clcategory=it_multimedia.hw_sw/site=cl_tomshardw
11/14/99	04:40:17	04:41:56	1.7		WWW.TOMSHARDWARE.DE/mainboard/99q4/991111/athlon_boards-04.html
11/14/99	04:40:20	04:40:20	0.0		CLASSIC.ADLINK.DE/accipiter/adserver.exe/clcategory=it_multimedia.hw_sw/site=cl_tomshardw
11/14/99	04:41:56	04:42:02	0.1	B	www.sex.de
11/14/99	04:42:02	04:42:08	0.1	B	www.playboy.com
11/14/99	04:42:09	04:42:14	0.1	B	www.hustler.com
11/14/99	04:42:14	04:42:20	0.1	B	www.doktorspiele.com
11/14/99	04:42:17	04:42:26	0.2		WWW.SHARKYEXTREME.COM
11/14/99	04:42:20	04:42:20	0.0		WWW2.SHARKYEXTREME.COM/cgi-bin/bd.m?dir=2000000a&count=1908&image=abit/banner10
11/14/99	04:42:20	04:42:20	0.0		WWW2.SHARKYEXTREME.COM/cgi-bin/bd.m?dir=2000001e&count=1315&image=upgradesource
11/14/99	04:42:20	04:42:23	0.1		WWW2.SHARKYEXTREME.COM/cgi-bin/bd.m?dir=20000020&count=1368&image=audiosales/
11/14/99	04:42:20	04:42:23	0.1		AD.DOUBLECLICK.NET/ad/n819.sharkyextreme/b16282;sz=468x60;ord=[timestamp]?
11/14/99	04:42:20	04:42:20	0.0		ADFORCE.IMGIS.COM/?adlink|2|20139|1|1|adforce
11/14/99	04:42:23	04:42:23	0.0		AD.DE.DOUBLECLICK.NET/ad/n339.247europe.com/b15642.2;sz=468x60;ord=1999.11.14.03:42
11/14/99	04:42:23	04:42:35	0.2		SNCOPMAIL.COM/cgi-bin/sharky/tx.pl?member=1|home:page=01
11/14/99	04:42:32	04:42:35	0.1		WWW.ANANDTECH.COM
11/14/99	04:42:35	04:42:35	0.0		AD.DOUBLECLICK.NET/ad/n818.anandtech/b16282;sz=468x60;ord=822704
11/14/99	04:42:35	04:42:35	0.0		WWW.ANANDTECH.COM/cgi-bin/adjuggler.exe?mg_only=/fptopbutton&nocache=index.cfm|opb
11/14/99	04:42:35	04:42:35	0.0		WWW.ANANDTECH.COM/cgi-bin/adjuggler.exe?mg_only=/fomain&nocache=index.cfm|mpos2
11/14/99	04:42:35	04:42:35	0.0		WWW.ANANDTECH.COM/cgi-bin/adjuggler.exe?mg_only=/mushkin/fpbutton2&nocache=/fbutto
11/14/99	04:42:35	04:42:35	0.0		ADFORCE.IMGIS.COM/?adlink|2.0|2|24777|1|1|misc=647813;loc=300
11/14/99	04:42:35	04:42:35	0.0		ADFORCE.IMGIS.COM/?adlink|2.0|2|30514|1|1|misc=875433;loc=300
11/14/99	04:42:35	04:42:50	0.4		AD.DE.DOUBLECLICK.NET/ad/n339.247europe.com/b15642.2;sz=468x60;ord=1999.11.14.03:42
11/14/99	04:42:56	04:43:05	0.2	B	www.planetquake.com
11/14/99	04:43:05	04:43:08	0.1		WWW.GWESTWOOD.COM
11/14/99	04:43:08	04:43:08	0.0		WWW.GWESTWOOD.COM/newwin.ex.html
11/14/99	04:43:08	04:43:08	0.0		WWW.GWESTWOOD.COM/topnav1.html

14.11.1999 printed for panamp1 04:43:12, Page 6/6

Tabelle 3

9 Content-Filterung – Praxisreport in Deutschland

Der bisher umfassenste Praxistest in Sachen Content-Filterung wurde in Deutschland am 16. November 1997 ausgewertet. Über einen Zeitraum von fünf Wochen wurde ein Cyber Patrol Proxy-Server, mit einem Proxy-Interface-Graph überwacht. Einem Abteilungsbereich mit 20 Mitarbeitern wurde der ausschließliche Zugang zum Internet über unseren Test-Proxy, „Proxy2“, eingerichtet.

Der Test begann an einem Mittwoch der 41. KW. Ziel der ersten Phase war es, eine Gesamt-Nutzer-Statistik der 20 Testnutzer in Form von ausgehenden und einkehrenden Traffic in Bits pro Sekunde ohne Filterfunktion aufzuzeigen.

In der zweite Phase zwischen Montag der 43. KW bis Mittwoch der 44. KW wurde ausschließlich eine zuvor mit dem Administrator erstellte CyberYES-Liste mit 100 ausgewählten Internet-Angeboten freigegeben.

In der dritten und letzten Phase zwischen Mittwoch der 44. KW und Freitag der 45. KW wurde die zuvor verwendete CyberYES-Liste auf die Verwendung von 09:00 bis 11:00 Uhr und 14:00 bis 16:00 Uhr beschränkt. Zwischen 12:00 bis 14:00 Uhr und 16:00 bis 22:00 Uhr war die Standard CyberNot-Liste ausschließlich aktiviert.

Die dritte Phase, eine Mischung aus unternehmenseigener YES- und Verwendung der Standard Cyber-NOT-Liste, wurde zur weiteren Verwendung in der Unternehmung beibehalten, siehe Abb. 8.

10 Von der Technologie-Euphorie bis zum „Benefit“

Bei Betrachtung der Ergebnisse der Internetfilterung in vorangegangenen Auswertungen, stelle ich fest, dass die Verwendung von Internet in Un-

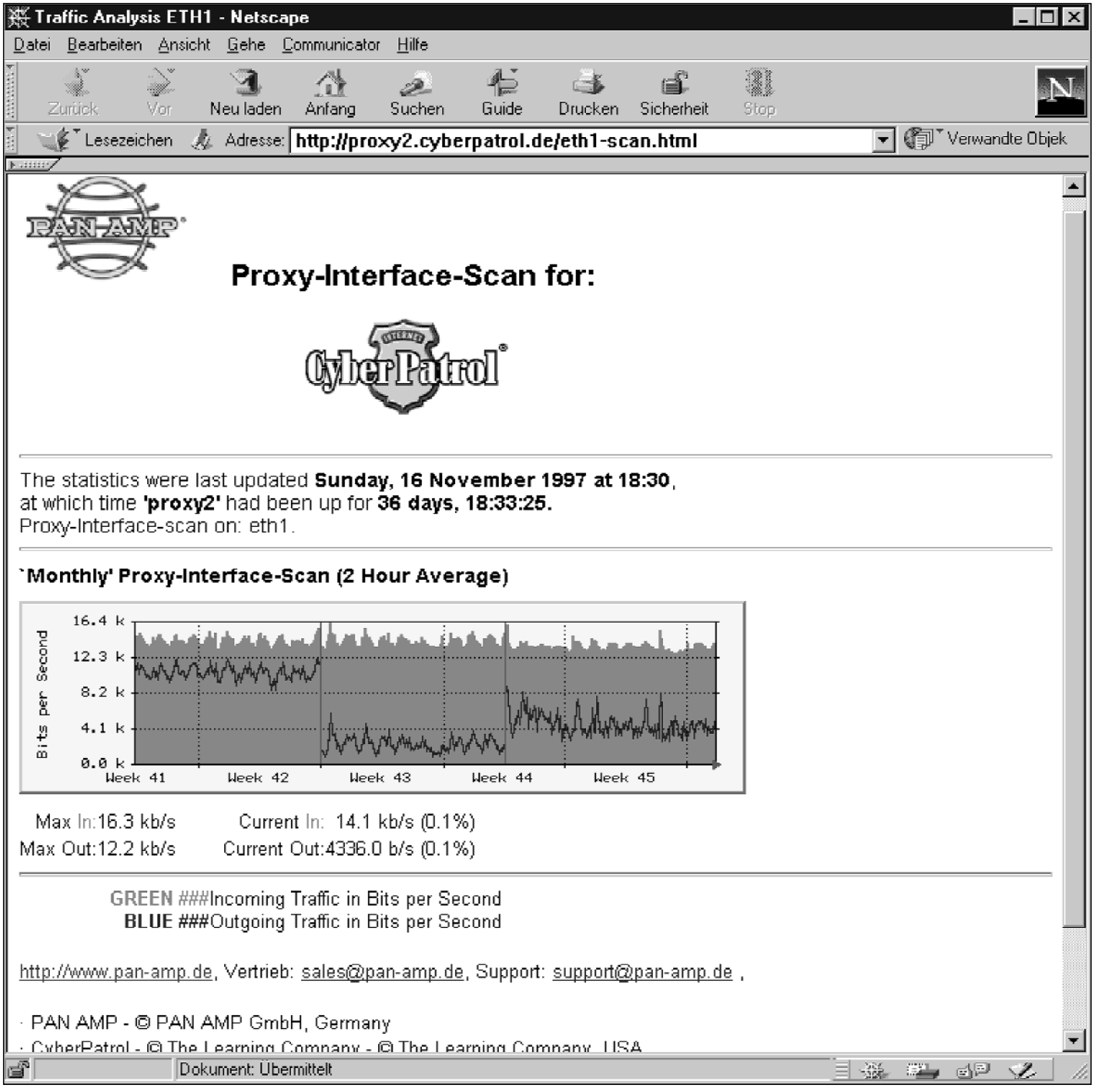

Abbildung 8

ternehmen von drei Entwicklungsphasen im jeweiligen Unternehmens-Management begleitet wird:

Am Beginn steht die „Technologie-Euphorie“ und das ständig wachsende Interesse am Internet in seiner Gesamtheit. In kürzester Zeit wird ein WWW, FTP und E-Mail-Server benötigt und eingerichtet.

Die zweite Phase kann man als das „Protokoll-Syndrom“ bezeichnen. Es entstehen Fragen, in wieweit die Nutzung vom Internet am Arbeitsplatz sich im Sinne des Unternehmens produktiv auswirkt, wie das Unternehmens-Netzwerk gegen unberechtigte Zugriffe von Mitarbeitern und Externen geschützt werden kann und wer die Zuständigkeit erhält, jede Datenabfrage und Fehlermeldung zu protokollieren und alles zu überwachen, was dem Unternehmen Schaden zufügen kann.

Mit der Auswertung der protokollierten Daten, der Bewertung der Datenmengen und der Feststellung, dass eine totale Überwachung Ressourcen bindet, die jenseits ihres Nutzens stehen, wird Phase drei beschritten. Den Entschluss, die Vorteile von Internet-Content und -Kommunikation zu nutzen und auf die Risiken zu verzichten, kann man als „Benefit“ bezeichnen. Wozu sollten Reports über Mitarbeiter erstellt werden,

wenn die Benutzung von negativen Internet-Content nahezu ausgeschlossen ist und Internetadressen, die der Unternehmung Schaden zufügen können, nicht mehr erreicht werden. Die Feststellung, dass man einem mündigen Mitarbeiter eine gewisse Eigenständigkeit in der Gestaltung seiner Arbeitszeit zutraut, führt meist dazu, die Sperr-Liste und gewisse optionale Sperr-Informationen dem jeweiligen Bedarf anzupassen und aktiv einzusetzen. Protokolle werden meist auf sicherheitsrelevante interne Adressen und extreme Zugriffswünsche reduziert und in Verbindung mit einer eigenen Freigabe-Liste und den zuvor aufgeführten None-, Full-, Work- und Leisure- Einstellungen abgerundet.

Content-Filter-Programme sind, beginnend mit der „Technologie-Euphorie“ über das „Protokoll-Syndrom“ bis hin zum „Benefit“ die Wegbegleiter, welche einen optionalen Funktionsbedarf für alle drei Phasen bereitstellen. □

Content-Filterung auf der Cebit2000

Neben der Möglichkeit, sich auf der Cebit2000 Content-Filterung auf dem PAN AMP Stand in der Halle 6 anzuschauen, stehen Ihnen Content-Filter-Versionen als Demoversion mit einer einmonatigen Laufzeit zur Verfügung. Ihre kostenlose Anforderung können Sie an sales@panamp.de richten.

PAN AMP AG

Tel.: +49 (40) 55 30 02-0
Fax :+49 (40) 55 30 02-100
email: weingarten@panamp.de
web: www.panamp.de