infoRUM

INFOrmationsforum des Rechenzentrums der Universität Münster

Jahrgang 23, Nr. 2 – Mai 1999 ISSN 0931-4008

Inhalt

Impressum

infoPUM

ISSN 0931-4008

Westfälische Wilhelms-Universität
Zentrum für Informationsverarbeitung (Universitätsrechenzentrum)
Röntgenstr. 9 – 13
48149 Münster

E-Mail: ziv@uni-muenster.de
WWW: http://www.uni-muenster.de/ZIV/

Redaktion: W. Bosse (✆ 83-31561, ✉ bosse@uni-muenster.de)
R. Perske (✆ 83-31582, ✉ perske@uni-muenster.de)
H. Pudlatz (✆ 83-31672, ✉ pudlatz@uni-muenster.de)
E. Sturm (✆ 83-31679, ✉ sturm@uni-muenster.de)

Satzsystem: Corel WordPerfect 8.0 für Windows 95/NT

Druck: Zentrum für Informationsverarbeitung
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

Editorial

R. Perske

Liebe Leser,

nutzen Sie das Internet? Natürlich.

Verwenden Sie dabei gängige Programme der marktbeherrschenden Firmen?

Ihnen ist ja sicherlich bewusst, dass Sie dann keine Privatsphäre mehr besitzen. Oder glaubten Sie ernsthaft, die Daten auf Ihrem Rechner wären noch wirklich vor fremden Zugriff geschützt? Daran haben diese Firmen doch überhaupt kein Interesse, denen sind gläserne Kunden doch viel lieber. Ohne Ihnen Bescheid zu geben und ohne Ihr Einverständnis einzuholen, übertragen Programme dieser Firmen Ihre persönlichen Daten und Vorlieben und ermöglichen auch Dritten, Ihre persönlichen Daten abzurufen und noch üblere Sachen anzustellen. Welche Mechanismen dabei verwendet werden und wie Sie sich doch ein wenig schützen können, mögen Artikel aus diesem infoPUM erläutern. Wie viele Spuren im Netz Sie selbst dann noch hinterlassen, wird sicherlich manchen von Ihnen auch noch nicht bekannt sein.

Aus Platzgründen mussten Artikel entfallen, die zum Beispiel erläutern, weshalb man niemals Softwareprodukte online registrieren lassen sollte oder wieso man niemals anonyme Briefe mit Microsoft Word schreiben sollte – immerhin soll der Autor des seit einigen Wochen kursierenden, trotz aller Aufregung relativ harmlosen Trojanischen Word-Makros „Melissa“ genau dadurch identifiziert worden sein, dass er „Melissa“ mit demselben Rechner wie andere von ihm stammende Dokumente erstellt hat – Word, Excel usw. markieren ungefragt jedes Dokument mit einer Rechneridentifizierungsnummer. Dass diese bei der Online-Registrierung von Windows 98 und anderen Produkten ohne jeglichen Hinweis zusammen mit den persönlichen Angaben an den jeweiligen Hersteller übermittelt wird, passt ins Bild.

Nun, fast alle diese unerwünschten Funktionen können Sie ausschalten, lassen Sie sich diesbezüglich bitte von Ihrer IVV (Informationsverarbeitungs-Versorgungseinheit) beraten.

RUM-Aktuell

Detailregelungen zur Verwendung von Namen im Datennetz der WWU Münster

K.-B. Mertz

Auf Grund eines Entwurfes des Zentrums für Informationsverarbeitung (ZIV) vom 13.10.1998 hat die IV-Kommission in ihrer Sitzung vom 13.1.1999 eine Regelung für die Verwendung von Namen, soweit diese im Rechnernetz der WWU von Belang sind, beschlossen.

Die immer größere Verbreitung von Betriebssystemen der Firma Microsoft, die eine auf NETBIOS und WINS basierende Kommunikation ermöglichen, macht es u. a. erforderlich, die Benutzung von Namen (Kennungen) für Benutzer, Benutzergruppen, Rechner, Arbeitsgruppen (Workgroups), LAN-Domains usw. zu regeln, damit keine unerwünschten Effekte auftreten wie fehlgeleitete Meldungen oder Behinderungen bei der Anmeldung in einzelnen Domains. Insbesondere ist es wegen der Einschränkungen im Bereich des WINS notwendig, dafür zu sorgen, dass kein Name in mehr als einer Bedeutung benutzt wird, dass also z. B. kein Rechner einen Namen hat, der auch Benutzerkennung ist. Darüber hinaus werden im Bereich des lokalen Rechnernetzes Netzwerk-Protokolle benutzt wie Appletalk oder Novell Netware, in denen Namen verwendet werden, über die bisher noch keine Detailregelungen bestehen, so dass bei Störungen die Ermittlung der Ursache sehr schwierig sein kann.

Entsprechend seiner Verpflichtung gemäß §3, Nr. 1 und 2 der zur Zeit gültigen „Betriebsregelung für das Datennetz der WWU Münster“ schlägt das ZIV folgende Detailregelung vor, durch die §3, Nr. 2 und §4, Nr. 2 und 3 dieser Betriebsregelung präzisiert werden:

1. Namensbereiche, Netz- und Nutzerdatenbank

1.1. Objektnamen im Datennetz der WWU

Im Bereich des Datennetzes der WWU Münster werden durch die verwendeten Netzprotokolle Namen oder Kennungen für folgende Typen von Objekten benutzt:

- Domain (LAN-Server, Windows NT),
- Subdomain (IP),
- Zone (Appletalk),
- Bereichs-Id/Scope (Windows NT),
- Arbeitsgruppe/Workgroup (Windows),
- Endgerät im Netz (z. B. Rechner oder Drucker),
- Benutzergruppe (Windows, UNIX, VMS),
- Account/Benutzer.

Gewisse Dienste im Datennetz können i. Allg. nur dann störungsfrei funktionieren, wenn diese Namen/Kennungen netzweit eindeutig sind und zwar innerhalb der Gesamtheit dieser Objekte. Das ZIV muss daher alle verwendeten Namen in Übereinstimmung mit den Anforderungen der IV-Versorgungseinheiten und den Betreibern von Endgeräten vergeben und kontrollieren, so dass die Eindeutigkeit der Namen gewahrt bleibt.

1.2. Netzdatenbank

Das ZIV unterhält eine Netzdatenbank, mit deren Hilfe alle Namen mit Ausnahme der Benutzerkennungen soweit notwendig verwaltet werden (Vergabe und Speicherung zum Zweck der Betriebsführung). Diese Namen sowie weitere Daten aus dieser Datenbank können bei berechtigtem Bedarf einem Personenkreis, der von den IV-Versorgungseinheiten zu benennen ist, unter Beachtung des Datenschutzes und der Netzsicherheit sowie der Sicherheit der Endsysteme im Netz zugänglich gemacht werden.

(Anmerkung: Die Daten der Netzdatenbank werden erst nach der erforderlichen Umstellung, die voraussichtlich noch in diesem Jahr erfolgen wird, für andere zugänglich sein.)

1.3. Benutzerdatenbank

Das ZIV betreibt eine zentrale Benutzerdatenbank, in der alle Benutzerkennungen registriert sind, die in den Rechnersystemen des ZIV sowie den IV-Versorgungseinheiten, die der zentralen Nutzerverwaltung angeschlossen sind, benutzt werden. Weiterhin werden in dieser Datenbank Benutzergruppen im Sinne von z. B. Unix, VMS und Windows NT registriert, die dort als Projekte bezeichnet werden.

Diese Namen sowie weitere Daten aus dieser Datenbank können bei berechtigtem Bedarf einem Personenkreis, der von den IV-Versorgungseinheiten zu benennen ist, unter Beachtung des Datenschutzes und der Datensicherheit zugänglich gemacht werden.

2. Namen für Scopes, Domains, Workgroups usw.

2.1. Netbios-Scopes

Namen für Bereichs-Ids/Scopes innerhalb des Netbios-Protokolls sollten nur dann verwendet werden, wenn dies unbedingt erforderlich ist, da Netbios eine Kommunikation zwischen Rechnern unterschiedlicher Scopes nicht zulässt. Sollen dennoch Scopes verwendet werden, müssen diese Namen vor der Verwendung beim ZIV von den nutzenden Einrichtungen beantragt werden.

2.2. Domains

Namen für LAN-Server- und Windows-Domains müssen von den nutzenden Einrichtungen beim ZIV beantragt werden. Dabei muss angegeben werden, welche Rechner als Primary- oder Backup-Controller benutzt werden sollen.

Es wird empfohlen Namen zu beantragen, die mit einer Kurzbezeichnung des IV-Versorgungsbereiches oder des Instituts beginnen, in dem die Domain betrieben wird. Solche Namens-Präfixe können beim ZIV für die Einrichtungen an der WWU reserviert werden. Verantwortlich für die Anmeldung sind die Leiterinnen/Leiter der Einrichtungen oder die von diesen beauftragten Personen.

Internet-Subdomains werden an der WWU in der Regel nicht verwendet, um den Administrationsaufwand für das Netz gering zu halten. Bei berechtigtem Bedarf können auf Antrag von Einrichtungen der WWU einzelne Subdomains durch das ZIV eingerichtet und administriert werden.

2.3. Workgroups

Windows-Workgroup-Namen können in Entsprechung zu Abschnitt 2.2 vom ZIV reserviert werden. Für registrierte Workgroups besteht ein Anspruch auf ausschließliche Nutzung durch die dafür angemeldeten Rechner (s. u.). Die Durchsetzung dieses Anspruchs kann zur Zeit nicht technisch garantiert werden, jedoch wird das ZIV die Nutzer bei der Bereinigung von Konflikten, soweit möglich, unterstützen.

Bei der Anmeldung von Endgeräten, die in eine Windows-Workgroup eingebunden werden sollen, kann diese angegeben werden, sofern sie beim ZIV registriert ist. Es wird empfohlen, dies grundsätzlich zu tun.

2.4. Appletalk-Zonen

Appletalk-Zonen müssen beim ZIV angemeldet werden. Endgeräte, die Appletalk-Zonen zugeordnet werden sollen, müssen entsprechend angemeldet werden.

3. Namen für Rechner und sonstige Endgeräte

3.1. Vergabe von Namen für Rechner und sonstige Endgeräte

Alle Endgeräte, die an das Datennetz der WWU angeschlossen werden sollen, müssen entsprechend der Betriebsordnung angemeldet werden und erhalten bei der Beantragung durch die nutzende Einrichtung von der zuständigen Abteilung des ZIV

- einen systematischen Namen, bestehend aus Institutskürzel und laufender Nummer,
- bei Bedarf einen oder mehrere weitere Namen nach Wahl des Betreibers mit der Einschränkung, dass die Eindeutigkeit des Namens im gesamten Namensbereich (Rechner-, Benutzer-, Gruppen-, Domain-Namen usw.) des Datennetzes nicht verletzt werden darf; die Kontrolle der Eindeutigkeit wird durch Überprüfung der relevanten Datenbank-Tabellen vom ZIV durchgeführt,
- bei Bedarf einen oder mehrere weitere Internet-DNS-Namen innerhalb von registrierten Subdomains an der WWU nach Wahl der nutzenden Einrichtung, die die Subdomain registrieren ließ (vgl. 2.2); diese Namen werden ausschließlich im Internet-DNS-Dienst an der WWU verwendet. Die Eindeutigkeit innerhalb der Subdomain wird vom ZIV sichergestellt.

Wenn derselbe Betreiber mehrere Endgeräte anschließen lässt, kann er beantragen, dass diese Endgeräte Namen bekommen, die aus einem festen Namensteil (Präfix) und einer Nummer bestehen. Derartige Präfixe müssen von der nutzenden Einrichtung eigens beantragt und beim ZIV registriert werden.

Verantwortlich für die Anmeldung sind die Leiterinnen/Leiter der Einrichtungen oder die von diesen beauftragten Personen. Das ZIV wird darauf achten, dass Namen mit einem registrierten Präfix nur für Endgeräte der nutzenden Einrichtung vergeben werden, die das Präfix beantragt hat.

Es wird empfohlen, ein beantragtes Präfix für Rechnernamen auch in den Namen der Domain und/oder der Workgroup zu verwenden, in die die Rechner eingebunden werden sollen (vgl. 2.2).

(Anmerkung: Im Bereich der IVV4 „Naturwissenschaften außer Geowissenschaften“ ist diese Form der Namen für die am DECNET angeschlossenen Rechner seit langem üblich; diese Präfixe sind bereits vom ZIV registriert und müssen nicht mehr neu beantragt werden.)

3.2. Verwendung von Namen für Rechner und sonstige Endgeräte

In allen Netzwerk-Protokollen dürfen für die fest an das Datennetz der WWU angeschlossenen Endgeräte nur die vom ZIV vergebenen Rechnernamen benutzt werden, also z. B. auch bei der Anmeldung beim WINS oder im Appletalk-Bereich. In den WINS-Servern des ZIV werden diese Namen fest eingetragen.

Sofern im verwendeten Netzwerk-Protokoll zugelassen und erforderlich, sind Zusätze zum Rechnernamen erlaubt, die auf die Funktion des Endgerätes oder einen auf ihm angebotenen Dienst hinweisen (z. B. im Appletalk „ATK-DECNET-Gateway on VNWZ00“).

Rechner, die nach Einwahl über Modem oder ISDN etc. mittels PPP oder vergleichbarer Protokolle vorübergehend an das Datennetz der WWU angebunden werden, müssen sich im WINS mit der Nummer des eigenen Telefon-Anschlusses einschließlich Vorwahl und Ländercode anmelden (z.B. 49251987654321), um die Eindeutigkeit zu gewährleisten.

4. Namen für Benutzergruppen und Accounts (Benutzerkennungen)

4.1. Vergabe von Namen für Benutzer und Benutzergruppen

Jedem Benutzer wird auf Antrag vom ZIV eine Kennung zugewiesen (in der Regel nur eine Kennung), die dann in allen beteiligten Systemen gleich ist, zu denen er Zugang haben soll (zentral registrierte Kennung).

Die Benutzerkennungen werden Projekten zugeordnet, die von den Einrichtungen beim ZIV beantragt werden können. Jedem Projekt sind ein oder mehrere Rechner-Systeme zugeordnet, auf denen seine Mitglieder Zugang mit entsprechenden Gruppenrechten haben. Die Zugehörigkeit von Benutzern zu Benutzergruppen im Sinne der Betriebssysteme (z. B. Unix, VMS, Windows NT) entsteht auf Grund der Zuordnung zu den Projekten. Als Namen für Benutzergruppen werden nach Möglichkeit die Namen der entsprechenden Projekte benutzt.

Bei der Vergabe von Namen im übrigen Netzbereich wird zur Einhaltung der Eindeutigkeit die zentrale Benutzerdatenbank berücksichtigt und umgekehrt.

4.2. Verwendung von Benutzernamen

In Systemen, deren Benutzer sich bei zentral administrierten Diensten wie z. B. dem WINS-Service des ZIV anmelden können, dürfen nur Benutzerkennungen verwendet werden, die entweder in der zentralen Benutzerdatenbank für den jeweiligen Benutzer registriert sind (zentral registrierte Kennungen) oder mit dem Namen des Rechners, der Workgroup bzw. der Domain oder dem entsprechenden Namens-Präfix beginnen (vgl. Abschnitt 3.1), auf das ein Unterstreichungszeichen (Underscore) folgen muss (lokale Kennungen), oder entsprechend der Standard-Installation des Systems besondere Berechtigung für Notfälle haben und nur in Notfällen benutzt werden (z. B. „Administrator“).

Für die Aufgaben der System-Administration sind im normalen Betrieb zentral registrierte oder lokale Kennungen zu verwenden. Für lokale Kennungen ist keine Konfliktfreiheit gewährleistet.

5. Einsatz und Nutzung zentraler und dezentraler namenssensitiver Dienste

Systeme, die namenssensitive Administrierungsdienste wie z. B. WINS benutzen, aber nicht zentral registrierte Benutzerkennungen und nicht lokale Kennungen entsprechend 4.2 verwenden, müssen eigene, für das entsprechende Protokoll gegebene Unterscheidungsmerkmale (bei Netbios Bereichs-Ids) verwenden, wenn es sonst zu Identifikationskonflikten kommt. Die entsprechenden Server wie z. B. WINS-Server dürfen dann ebenfalls nur so betrieben werden, dass keine Konflikte mit zentralen Diensten entstehen (z. B. nutzereigene WINS-Server nur mit eigenen Bereichs-Ids). Zur Sicherstellung des universitätsweiten Regeldienstes sind diese nicht zentral bereitgestellten Server beim ZIV anzumelden; ihr Einsatz ist auf solche Fälle zu beschränken, in welchen der fachgerechte Betrieb gewährleistet ist (in der Regel nur durch die IV-Versorgungseinheiten oder in Abstimmung mit diesen) und triftige Gründe den Mehraufwand rechtfertigen.

Domain-Name-Server (Internet-DNS-Server) sind ausschließlich vom ZIV in ausreichender Zahl zur Gewährleistung der Betriebssicherheit zu betreiben. Dies betrifft auch den DNS-Dienst für Subdomains innerhalb der WWU. Das ZIV kann von dieser Regelung aus triftigen Gründen (z. B. bei hochkritischen Rechneranwendungen) abweichen, wenn die korrekte Verteilung der Namensinformationen sichergestellt ist; das ZIV stellt dann aktuelle Informationen automatisiert bereit.

6. Übergangs-, Fortschreibungs- und Kontroll-Regelungen

6.1. Anmeldung von alten und neuen Namen

Bereits benutzte Namen für Domains, Workgroups und Scopes usw. sind so bald wie möglich dem ZIV zu melden. Vor der Anwendung neuer Namen in diesen Bereichen ist eine Anmeldung beim ZIV erforderlich. Das ZIV wird baldmöglichst entsprechende Anmeldeverfahren, die möglichst DV-unterstützt abgewickelt werden sollen, anbieten.

6.2. Aufhebung von bestehenden Namenskonflikten

Weil bisher die Vergabe von Rechnernamen und Benutzerkennungen durch das ZIV unabhängig voneinander erfolgte, gibt es zur Zeit noch Überschneidungen der Namensbereiche, die im Einvernehmen mit den Betroffenen durch Ändern der Rechner- oder der Benutzerkennung nach und nach behoben werden.

6.3. Erweiterungen der geregelten Namensräume

Sofern weitere Objekte mit vergleichbarer Bedeutung wie in 1.1. bekannt werden, wird das ZIV weitere Regelungen in sinngemäßer Entsprechung zu den aufgeführten Regeln und in Abstimmung mit den IV-Versorgungseinheiten, im Zweifel auch mit der IV-Kommission, festlegen.

6.4. Überprüfung der Regelungen

Die vorstehenden Regelungen sind in regelmäßigen Abständen auf ihre Durchführbarkeit und Wirksamkeit hin zu überprüfen.

Automatische WWW-Proxy-Server-Konfiguration

R. Perske

Viele WWW-Programme bieten die Möglichkeit, die WWW-Proxy-Server entweder *manuell* zu konfigurieren oder aber die Konfiguration *automatisch* aus einer zentral vorgehaltenen Datei zu entnehmen. Eine solche Konfigurationsdatei bieten wir seit einiger Zeit an:

```
http://www.uni-muenster.de/proxy.pac
```

Wir möchten Sie bitten, Ihr WWW-Programm entsprechend einzustellen. Verglichen mit der *manuellen* Einstellung genießen Sie bei der *automatischen* Konfiguration eine verbesserte Ausfallsicherheit und teilweise auch besseres Antwortzeitverhalten.

Betrieb von E-Mail-Servern im Netz der WWU

W. Bosse

Zum Betrieb von dezentralen E-Mail-Servern ist eine Betriebsregelung des ZIV vorbereitet worden, die ab Mai 1999 in Kraft tritt.

Am 13. Januar 1999 hat die IV-Kommision der WWU zum Problem der Vermeidung von SPAM-Mail folgenden Beschluss gefasst:

> „Angesichts der Probleme im Zusammenhang mit dem Betrieb von E-Mail-Servern empfiehlt die IV-Kommission, dass die Einrichtung von dezentralen E-Mail-Servern in den IVVen nur nach vorheriger Anmeldung im Rahmen des LAN-Antragsverfahrens mit Zustimmung des Leiters der zuständigen IVV und nach Genehmigung des LAN-Zuganges vorgenommen werden darf. Die die Anträge als Verantwortliche unterzeichnenden Hochschullehrer bzw. Leiter von Forschungsgruppen sollen eigens über die rechtliche Problematik informiert werden. Die technische Umsetzung wird zwischen IVV und ZIV vereinbart."

Für den Betrieb eines E-Mail-Servers sind wichtige Anforderungen hinsichtlich Verfügbarkeit, Datenschutz und Datensicherheit zu erfüllen. Um dem Beschluss der IV-Kommission nachzukommen, müssen auch Anti-SPAM-Filter aktiviert sein und auf dem neuesten Stand gehalten werden.

Die Betriebsregelung beschreibt im Einzelnen die Voraussetzungen zur Administration und zum Betrieb des Servers und erläutert die erforderlichen Maßnahmen zur organisatorischen Umsetzung.

Der Text der Betriebsregelung kann im WWW über das Inhaltsverzeichnis der Seite

`http://www.uni-muenster.de/ZIV/Content--Regelungen.html`

eingesehen werden.

Zentrales Software-Angebot

H. Pudlatz

Gegenüber der Software-Liste im Heft infoRUM Nr. 1/ 1997 hat es zahlreiche Änderungen gegeben.

Das Zentrum für Informationsverarbeitung (Universitätsrechenzentrum) betreut die Softwarenutzung auf folgenden Betriebssystem-Plattformen:

	Windows-Systeme					**Unix-Systeme**				
DOS	Win 3.x	Win 9x	Win NT	OS/2	Mac-OS	Linux	Sola-ris2	AIX	DEC Unix	VMS

Bezüglich Nutzungsart, Erwerbsmöglichkeit und Nutzerkreis werden folgende Software-Kategorien unterschieden:

x = Zur unmittelbaren Benutzung **bereitgestellte** Software (auf PCs des CIP-Pools oder im Unix-Cluster), die nicht kopiert werden kann. Alle mit (x) bezeichneten Produkte können bei Bedarf auf einem ZIV-Server bereitgestellt werden.

a = Software, die auf Grund bestimmter **Forschung&Lehre-Lizenzvereinbarungen** von Universitätseinrichtungen bei autorisierten **Händlern** zu günstigen Bedingungen erworben werden kann. Lizenzen, Datenträger (meist CD-ROM) und Dokumentationen können in flexiblen Mengen bestellt werden, jedoch darf die Anzahl der Dokumentationen die Anzahl der Lizenzen nicht überschreiten. Pro Bestellvorgang wird eine Bearbeitungsgebühr von i. d. R. 10 DM fällig, hinzu kommen Porto- und Verpackungskosten sowie die gesetzliche Mehrwertsteuer. Näheres kann beim jeweiligen Händler erfragt werden:

Steckenborn Computer, Gießen	`http://www.steckenborn.de`
Logibyte GmbH, Berlin	`http://www.logibyte.de`
asknet GmbH, Karlsruhe	`http://www.asknet.de`

Die Bestellung erfolgt auf dem universitätseinheitlichen Bestellformular über die zentrale Beschaffungsstelle. Statt von den genannten Firmen können einige Produkte auch über die IVVen bezogen werden, soweit sie auf Software-Servern des ZIV vorliegen, z. B. das Anti-Virus-Programm von Dr. Solomons. Im ZIV können ebenfalls die Lizenzbedingungen der genannten SW-Verträge eingesehen werden.

b = Software kann zusätzlich auch von **Studierenden oder Mitarbeitern** erworben werden (Nachweis gegenüber dem Händler durch beigefügte Studien- bzw. Dienstbescheinigung). Die Software kann z. T. frei für eigene, aber nicht kommerzielle Zwecke oder nur während der Dauer des Studiums bzw. der Beschäftigung bei der Universität verwendet werden. Um einen güstigen Preis für Studierende angeben zu können, handelt es sich bei den Studentenversionen teilweise um Vorgängerversionen, die sich meist nicht wesentlich von den jeweils aktuellen Versionen unterscheiden (z. B. AutoCAD, Borland FuLPS-Produkte).

c = Software, die **lokal** für **Institute, Mitarbeiter und Studierende** im Geschäftszimmer Einsteinstr. 60 des Zentrums für Informationsverarbeitung vorgehalten wird. (Ausgabe Dienstag Vormittag und Donnerstag Vormittag; Institute gegen Rechnung, andere gegen Barzahlung).

A = a und x
B = b und x
C = c und x

Bei den letztgenannten Kennzeichnungen besteht somit die Möglichkeit, vor Beschaffung der Software diese im ZIV zu testen.

Die obigen Kennzeichnungen geben in der folgenden Tabelle Auskunft über die Art der Verfügbarmachung der gebräuchlichsten Produkte in Verbindung mit den unterschiedlichen Betriebssystemplattformen insbesondere aber alle am Zentrum für Informationsverarbeitung zentral bereitgestellten Produkte. In vielen Fällen handelt es sich bei den Varianten für unterschiedliche Betriebssysteme um weitgehend identische Produkte (z. B. bei WWW-Browsern, PV~WAVE u. a.), in anderen Fällen, etwa bei den Programmiersprachen, können sich hinter der gleichen Bezeichnung sehr unterschiedliche Realisierungen verbergen.

Eine andere, weit größere Palette von Programmen ist auf dem FTP-Server des ZIV (Kommando `ftp ftp2`) als PD-Software bzw. Shareware kopierbar. Eine Darstellung an dieser Stelle würde den Rahmen sprengen. Details entnimmt man den Dateien `files.txt` in den Verzeichnissen `DOS, OS2, WIN31` und `WIN95` auf dem genannten Server.

Bezüglich der Nutzung von Software aufgrund von bestehenden Verträgen mit verschiedenen Firmen (Borland, Digital, IBM, Mansfield, Microsoft, Corel, SAS, SPSS u. a.) sind die unterschiedlichen Lizenzvereinbarungen einzuhalten. Sie sind teils auf den genannten Servern der Händler zu finden, teils können sie auch im Zentrum für Informationsverarbeitung erfragt werden.

Für Rechner (mit den Betriebssystemen VMS und Unix) und Rechnernetze der Fa. Digital sowie für Personalcomputer und Macintosh-Rechner, die im DEC-Cluster eingebunden sind oder dort zugreifen sollen, ist ein hochschulweit gültiger Software-Vertrag (DECcampus) über ein umfassendes Programmspektrum abgeschlossen worden, der im ZIV eingesehen werden kann.

Für Sun-Rechner existiert eine Mehrfachlizenz für das Betriebssystem und einige Sun-Compiler, die allgemein nutzbar sind. Für AIX-Rechner werden ein Basiskorb und Erweiterungskörbe mit diversen Software-Produkten auf Servern des ZIV vorgehalten.

Auf die Angabe von Versionsnummern bei den Produkten ist verzichtet worden, da es hier rasch zu Änderungen kommt. Die Händler halten meist die neueste Version bereit. Für ältere Betriebssysteme (z. B. DOS, Windows 3.x) sind gelegentlich auch ältere Versionen zu erhalten.

Wegen der ständig sich verändernden Angebotslage stellt die folgende Tabelle daher nur eine Momentaufnahme dar. Ebenso kann sie keinen Anspruch auf Vollständigkeit erheben.

		Windows-Systeme					Unix-Systeme				
Softwarekategorie Programm	DOS	Win 3.x	Win 9x	Win NT	OS/2	Mac-OS	Linux	Sola-ris2	AIX	DEC Unix	VMS
Textverarbeitung/DTP:											
Adobe Framemaker		a	a	a		a		A	A		
Adobe Pagemaker		a	a	a		a					
Caere Omnipage				b							
Corel Ventura			b	b							
Corel WordPerfect		a	b	B			a	b	B	A	
DECWrite											x
MS Publisher		a	b	b							
MS Word		a	a	A		a					
Scientific WorkPlace		a	a	a							
StarWriter		a	a	a	a	a	a	x			
TeX/LaTeX	b	b	b	B	b	b	b	x	x	x	x
TUSTEP	b		b	b			b	B	B		
Tabellenkalkulation:											
MS Excel		a	b	B		a					
StarCalc		a	a	a	a	a	a	x			
Büro-/Office-Produkte:											
Corel WordPerfect Suite		a	b	B		a	a				
IBM Lotus SmartSuite			b	b							
MS Office		a	a	A		a					
MS Project		a	a			a					
MS Schedule+		a	a								
StarOffice		a	a	a	a	a	a	x			
WP Informs		a									
Integrierte Software:											
IBM Works					a						
MS Works	a	a	a	a		a					

		Windows-Systeme					Unix-Systeme				
Softwarekategorie Programm	DOS	Win 3.x	Win 9x	Win NT	OS/2	Mac-OS	Linux	Sola-ris2	AIX	DEC Unix	VMS
Grafik und Anwendungen:											
Adobe Illustrator			a	a		a					
Adobe Photoshop			a	A		a					
Adobe Streamline		a	a	a		a					
AutoCAD / CADdiaESP	a							(x)			
AutoCAD Light		a	a	b							
Axum		b	b	B							
Corel Draw		a	b	B		a	b				
Corel WP Photohouse		a	a	a							
Corel WP Presentations		a	a	A							
Harvard Graphics		a		b							
MS Powerpoint			a	A		a					
OpenGL			a	a		a	b		x		
PV~WAVE			a	a			b	x	x	x	x
StarDraw / StarImpress		a	a	a	a	a	a	x			
xv							b	x	x		x
3D Studio				a							
Internet Tools/Multimedia:											
Adobe Acrobat Reader			a	A		a		a	a		
Adobe Pagemill			a	a		a					
Adobe Premiere			a	a		a					
Corel Web Graphics Suite			a	a							
FM Homepage			b	b		b					
MS FrontPage			b	b							
WWW-Browser		b	a	B	a		b	x	x		x
Numerik:											
Gaussian 94									x		
IBM ESSL									x		
IMSL Fortran Library								x	x	x	x
NAG Fortran Library			a	a			b	x	x	x	x

		Windows-Systeme					Unix-Systeme				
Softwarekategorie Programm	DOS	Win 3.x	Win 9x	Win NT	OS/2	Mac-OS	Linux	Sola-ris2	AIX	DEC Unix	VMS
Numerik (Forts.):											
NAG Graphics Library			a	a			b	x	x	x	x
IMSL C Library								x	x	x	
Symbolische Formelmanipulation:											
AXIOM								x	x		
MAPLE							b	x	x	x	
MATHEMATICA				b			b	x	x	x	
Datenbank:											
Corel Paradox		a	a	a							
dBase / Visual dBase			b	b		a					
DB2				a			a				
Filemaker Pro			b	b		b					
FoxPro / Visual FoxPro	a	a				a					
MS Access		a	b	B	a						
Oracle		a	a	a		a	b	(x)	x	(x)	x
Retrieval:											
Allegro	a							x			
DEC Bookreader										x	x
IBM Bookmanager	a								(x)		
IBM Searchvision									(x)		
Liman Pro (Literaturmanager)		c	c	c							
Statistik:											
S-PLUS								x			
SAS		a	a	A				x	x	a	
SPSS		c	c	C	a	a		x	x		
Archivierung/Datensicherung:											
IBM ADSM Client/Server	a	a		a	a	a	a	a	x	a	
Virenschutz											
Dr. Solomon's Antivirus Toolkit		a	a	A	a	a					

		Windows-Systeme					Unix-Systeme				
Softwarekategorie Programm	DOS	Win 3.x	Win 9x	Win NT	OS/2	Mac-OS	Linux	Sola-ris2	AIX	DEC Unix	VMS
Kommunikationssoftware:											
NetNews		b		a	a			x	x		x
X11-Server	a	a		A	a			x	x	x	x
Programmierumgebungen:											
APL2									(x)		
Borland Pascal/Turbo Pascal	a	a									
C	a			a				x	x		x
C++	a	a	b	b	a						
Delphi		a	b	B							
Fortran77	a							x	x		x
Fortran90									x		x
Java								x			
J++			b	b							
Modula-2	a										
MS Visual Basic		a	a	a							
MS Visual C++		a	a	A							
Pascal	a							x	x		x
Perl				a	a	a	b	a	a		x
PL/I					b				x		x
Editoren:											
emacs							b	x	x	x	
joe							b	x	x	x	
KEDIT	a	a	a	a	a						
THE							b	x	x	x	

Ausbau des zentralen WWW-Servers

R. Perske

Seit der Umstellung des zentralen WWW-Servers auf die Apache-Software stehen den Informationsanbietern weitere Möglichkeiten zur Verfügung.

Seit einigen Wochen läuft der zentrale WWW-Server `www.uni-muenster.de` auf einem dedizierten Rechner, gleichzeitig wurde die bislang verwendete Software der Firma Netscape durch die frei verfügbare Apache-Software mit SSL-Zusatz für abhörsichere Seiten ersetzt. Auch der der Nutzerverwaltung (Passwortänderung, Problemanalyse, E-Mail-Einstellungen usw.) dienende WWW-Server `user.uni-muenster.de` läuft jetzt auf einem eigenen Rechner. Neben der besseren Verwaltung des Servers bietet die Apache-Software viele weitergehende Möglichkeiten, einige davon stehen jetzt auch den Informationsanbietern zur Verfügung:

- Passwortgeschützter Zugriff auf WWW-Seiten, beschränkt auf einzelne Nutzer oder Gruppen, wobei sowohl mit der zentralen Nutzerverwaltung des Zentrums für Informationsverarbeitung als auch mit einer eigenen Nutzerverwaltung gearbeitet werden kann:

  `http://www.uni-muenster.de/WWW/Anbieten.html#access`

- *Server Side Includes* – Ablegen gemeinsamer Teile von HTML-Seiten in einer eigenen Datei (allerdings kein Ausführen von Programmen):

  `http://www.uni-muenster.de/apache-manual/mod/mod_include.html`

Weitere Eigenschaften des Servers können auf Anfrage freigeschaltet werden, soweit Sicherheitsbedenken dem nicht entgegenstehen. Im Testbetrieb befinden sich auch die an die zentrale Nutzerverwaltung des ZIV angepassten *Frontpage Server Extensions*.

Weitergehende Informationen für aktive und zukünftige Informationsanbieter finden Sie unter

`http://www.uni-muenster.de/WWW/Anbieten.html`

Online-Dokumentationen

Unix-Gruppe

Unter dem Stichwort *Online-Doku* können Sie verschiedene Dokumentationen im WWW abrufen.

Immer mehr Software-Dokumentationen liegen auch im WWW-Format vor und werden von uns online zur Verfügung gestellt. Der Zugriff ist allerdings in aller Regel auf Rechnersysteme und Einwahlzugänge der Universität Münster beschränkt. Sie finden die Dokumentationen auf der Titelseite des ZIV unter dem Stichwort *Online-Doku* oder direkt unter der Adresse

`http://www.uni-muenster.de/ZIV/Content--Doku.html`.

Bislang sind Dokumentationen zu folgender Software verfügbar:

- Pakete des Textsatzsystems TeX / LaTeX,
- Skriptsprache Perl 5,
- Oracle-Datenbanksysteme,
- Distributed Computing Environment DCE 2.2,
- AIX-C-Compiler Version 4.4,
- AIX-Fortran-Compiler Version 6.1,
- E-Mail-Verschlüsselungsprogramm PGP 2.6.2 / 2.6.3ia,
- Apache-WWW-Server Version 1.3,
- E-Mail-System Postfix.

Außerdem finden Sie dort:

- SelfHTML – eine umfassende HTML-Einführung,
- das IT-Grundschutzhandbuch 1998 des Bundesamts für Sicherheit in der Informationstechnik,
- Verweise auf Dokumentationen im Internet, z. B. die Internet-Standards (RFCs).

Es ist geplant, weitere Dokumentationen an dieser Stelle zugänglich zu machen.

NIC und NOC im ZIV

G. Richter

Das NIC (*Network Information Center*) und das NOC (*Network Operating Center*) im Zentrum für Informationsverarbeitung sind Anlaufstellen in allen Fragen der Verwaltung bzw. des Betriebes des Rechnernetzes der Westfälischen Wilhelms-Universität.

Im internationalen Gebrauch sind die Abkürzungen NIC und NOC, die frei als Netz-Informations-Center und Netz-Operating-Center übersetzt werden könnten. Gemeint sind damit in der Regel organisatorische Funktionseinheiten innerhalb der Organisation eines Netz- oder Netzdienste-Providers. Innerhalb der Abteilung Kommunikationssysteme des ZIV sind entsprechende Funktionseinheiten eingerichtet worden, die insbesondere die Erreichbarkeit für den Nutzer unabhängig von der persönlichen Präsenz einzelner Personen verbessern soll.

Im **NIC** können alle notwendigen Informationen, die die Verwaltung des Rechnernetzes betreffen, gezielt erfragt und koordiniert werden. Insbesondere sind hier folgende Informationen und Vorgänge gemeint:

- Beantragung von Anschlüssen an das lokale Rechnernetz (LAN),
- Anmeldung von Rechnern im LAN (Rechner-Registrierung, Vergabe von IP-Adressen und NetBios- sowie Domain-Namen etc.),
- Änderungsmitteilungen zu Rechnern im LAN (z. B. bei Umzug, Außerbetriebnahme, neuer LAN-Controller-Karte, Änderung des technisch Verantwortlichen),
- Informationsverwaltung und -koordinierung für Rechner im LAN,
- Status von LAN-Baumaßnahmen und anderen Netz-Projekten des Zentrums für Informationsverarbeitung,
- Abrechnung von Materialien und LAN-Anschlüssen,
- Datenbank des Netzes,
- CAD-Grundrisspläne mit LAN-Verkabelung.

Ihre Anträge, Anfragen und Mitteilungen hierzu richten Sie bitte per E-Mail an

```
nic@uni-muenster.de
```

In dringenden Fällen erreichen Sie das NIC während der Dienstzeiten telefonisch unter (0251) 83-31598.

Im **NOC** können alle Störungen, die das Rechnernetz und seine Verbindung zur Außenwelt betreffen, gezielt an die zuständigen Stellen im Zentrum für Informationsverarbeitung gemeldet werden. Insbesondere sind hier folgende Einrichtungen des Rechnernetzes gemeint:

- Lokales Rechnernetz (LAN) mit Backbone und Gebäudeversorgung,
- LAN-Anschlusseinrichtungen (Anschlussdose, -kabel etc.),
- LAN-LAN-Kopplungen über andere Netze (z. B. ISDN),
- Einzelplatzanbindungen über Standleitungen,
- Zugang zum externen Internet (BWiN, etc.),
- Netz-Mehrwertdienste (Domain-Name-, BOOTP-/DHCP-, WINS-, TIME-Server etc.),
- Einwählzugänge über universitätsinterne und öffentliche Telefonleitungen.

Ihre Störungsmeldungen und Fragen bezüglich des Rechnernetzbetriebes richten Sie bitte per E-Mail an

```
noc@uni-muenster.de
```

Bitte machen Sie bei Ihren Störungsmeldungen möglichst erschöpfend Angaben zu Ihrer Betriebssituation:

- Absender (Name, Einrichtung, Rufnummer, E-Mail-Adresse),
- Zeitpunkt oder Zeitraum der Störung,
- Ort der Störung (z. B. LAN-Anschlussnummer, Namen der betroffenen Rechner, verwendete Rufnummer bei Einwählsystemen),
- Art und Umfang der Störung (z. B. keine Verbindung zu X, aber Verbindung zu Y; geringer Durchsatz; eingesetzte Übertragungsverfahren, z. B. FTP im LAN).

Am besten verwenden Sie jedoch bitte unsere WWW-Formulare, die Sie über die WWW-Titelseite des ZIV unter dem Punkt „Ansprechpartner - Störungsmeldungen“ finden und die ihnen helfen, alle relevanten Angaben an das NOC zu senden.

In dringenden Fällen erreichen Sie das NOC auch telefonisch unter (0251) 83-31599. Diese Rufnummer wird an Arbeitstagen zu folgenden Zeiten ständig durch das NOC bedient:

- Montag und Dienstag: 8.00h – 16.30h
- Mittwoch bis Freitag: 8.00h – 16.00h

Ab 1. Juni 1999:

- Montag bis Freitag: 7.30h – 17.30h

Falls diese Rufnummer ausnahmsweise kurzfristig nicht erreichbar sein sollte, wenden Sie sich bitte in dringenden Fällen an einen der Mitarbeiter des ZIV aus dem Bereich Kommunikationssysteme.

Die Westfälische Wilhelms-Universität richtet zum 1. Juni 1999 eine ständige Rufbereitschaft für das Rechnernetz (LAN) der Universität ein (auch nachts und an Wochenenden); so dass für diesen besonders wichtigen Netzbereich eine Erreichbarkeit „rund um die Uhr“ gewährleistet sein wird. Genauere Informationen zur Rufbereitschaft finden Sie unter

```
http://www.uni-muenster.de/ZIV/
       Content--NetzOrganisation.html
```

Bitte beachten Sie, dass die personellen Ressourcen des NOC im Verhältnis zur Anzahl der Nutzer des Rechnernetzes sehr begrenzt sind. Wenden Sie sich deshalb nach Möglichkeit zunächst an die örtlich zuständigen Betreuer (technisch Verantwortliche für Ihren Rechner im LAN, Systemadministratoren, EDV-Beauftragte der Institute, Fachbereiche oder IV-Versorgungsbereiche).

Fragen und Problem- oder Störungsmeldungen, die nicht gezielt den Betrieb bzw. die Verwaltung des Rechnernetzes betreffen, sondern etwa den Betrieb von Servern im Zentrum für Informationsverarbeitung, richten Sie bitte an die zuständigen Adressen des Zentrums für Informationsverarbeitung, im Zweifelsfall an die zentrale E-Mail-Adresse

```
ziv@uni-muenster.de
```

Neue TUSTEP-Version 1999

W. Kaspar

Seit März diesen Jahres steht bei uns die neue TUSTEP-Version 1999 für die Betriebssysteme SunOS, AIX, Linux und Windows 95/98/NT zur Verfügung. Die Unix-Varianten befinden sich wie üblich auf unserem zentralen Server und können von dort direkt aufgerufen werden. Die Windows-Variante ist auf Disketten erhältlich. Auch die Linux-Variante gibt es zusätzlich auf Disketten (Anfragen an W. Kaspar, ✆. 3 16 73, ✉ kaspar@uni-muenster.de). Die MS-DOS-Version liegt weiterhin nur in der alten Version 10/95 vor.

Fingerabdrücke

R. Perske

Dieser Beitrag enthält die kryptografischen Prüfsummen der öffentlichen Schlüssel, die vom Zentrum für Informationsverarbeitung verwendet werden.

Die PGP-Schlüssel der Mitarbeiter des ZIV finden Sie im World Wide Web zusammen mit den PGP-Schlüsseln verschiedener Zertifizierungsinstanzen unter der Adresse `http://www.uni-muenster.de/ZIV/Mitarbeiter/urzring.asc`; ich selbst agiere als Zertifizierungsstelle der Universität, siehe unter `http://www.uni-muenster.de/ZIV/PGP/`.

Bits/KeyID Date User ID

2048/EF750F1D 1997/10/14 Rainer Perske +49(251)83-31582 Certification Key
Key fingerprint = 2F 38 6E F8 DC 2E D8 5E 5B 35 DB 49 8A E4 52 AF

2048/131B72ED 1998/08/18 Rainer Altvater <altvate@uni-muenster.de>
Key fingerprint = FF 89 81 67 37 45 2B 1C 57 F5 BB DD 4A D5 04 60
1024/29A14DD1 1997/06/18 Reinhard Mersch <mersch@uni-muenster.de>
Key fingerprint = F0 AF 2B F1 FE 55 7A 3A E6 0D C7 27 29 50 22 26
1024/3D37C6E1 1997/06/19 Dr. Klaus-Bolko Mertz <mertz@uni-muenster.de>
Key fingerprint = CA 6F 8D 5C EB 67 EA 18 38 79 64 3D 64 4C 4A 8C
1024/3EBBF595 1997/02/24 "Eberhard Sturm" <sturm@uni-muenster.de>
Key fingerprint = 6C 9D B3 38 C0 8C 3C BB AF 55 2A 7B 6A C4 66 B6
1024/44C661C5 1996/12/06 Stefan Ost <ost@uni-muenster.de>
Key fingerprint = 6F DB 21 B4 67 EA C2 E0 E8 3D 78 28 7C 66 09 38
2048/456CC783 1999/03/19 Karin Giermann <giermann@uni-muenster.de>
Key fingerprint = C2 19 72 89 36 36 76 6F 4C 4E 1F 5B 2B 12 05 03
1024/51F8EA05 1997/06/18 Mathias Grote <grote@uni-muenster.de>
Key fingerprint = 0F 13 5B 2D 1D A5 9D 65 DF EA 41 6B CE E5 88 C2
1024/525140B9 1997/09/01 JOIN Project Team <join@uni-muenster.de>
Key fingerprint = 8C A9 DF 11 F5 21 89 DA 44 73 F1 FA 86 3A 1A 71
2048/7231BCE7 1999/03/17 Dr. Hilmar Pudlatz <pudlatz@uni-muenster.de>
Key fingerprint = 7B F7 C6 06 95 99 53 3A 90 7B BF FB 7D 78 03 2E
2048/8D1993F9 1998/02/27 DaWIN-Team <dawin@uni-muenster.de>
Key fingerprint = 4D 3F C7 49 F6 75 E1 AF 36 A3 F8 2C 04 86 F8 0F
2048/8D598B97 1999/03/17 Walter Bosse <bosse@uni-muenster.de>
Key fingerprint = 15 32 90 0C 3E 91 00 9A 8F 5A 82 2C D4 62 56 A3
2048/914AD795 1999/03/17 Dr. Wilhelm Held <held@uni-muenster.de>
Key fingerprint = 40 7D 68 1E C7 6A 85 CD 7D 50 57 19 E4 19 FF EB
1024/BD7873F5 1997/06/17 Jürgen Hölters <holters@uni-muenster.de>
Key fingerprint = EA CB 47 AF 3A 79 96 B5 D3 46 C8 98 53 72 3F 2B
1024/D3560AA5 1998/11/30 Guido Wessendorf <wessend@uni-muenster.de>
Key fingerprint = 46 F8 4E C0 3E 85 0D 05 10 E1 44 6E AF F1 0D 47
768/D782E369 1997/07/18 Klaus Reichel <reichel@uni-muenster.de>
Key fingerprint = 6C 35 15 A9 E3 9E 83 4E 2E 95 4A F1 47 FC 7F 58
2048/DE00243F 1999/05/05 Wolfgang Kaspar <kaspar@uni-muenster.de>
Key fingerprint = E2 38 F0 5C 58 94 C5 6F F9 D7 06 AD 17 9E A9 59
1536/E307C0B9 1997/10/14 Rainer Perske <perske@uni-muenster.de>
Key fingerprint = F3 99 93 1F AC 06 0D 17 ED 93 35 19 F6 2D A3 22
1024/8A2097A5 1997/06/13 *** KEY REVOKED ***
Rainer Perske <perske@uni-muenster.de>
Key fingerprint = AA D7 57 F5 8F 14 A7 A5 C4 E2 CF 04 95 52 25 60

Auf Wunsch zertifiziere ich auch WWW-Server. Als Herausgeber wird dabei eingetragen: Rainer Perske, perske@uni-muenster.de, Universitätsrechenzentrum, Westfälische Wilhelms-Universität Münster, Münster, Germany, DE.

Anders als bei PGP-Schlüsseln, die ich nur gegen Vorlage eines Ausweises zertifiziere, führe ich bei WWW-Servern jedoch nur eine minimale Plausibilitätskontrolle durch und halte mich an keine vorgegebene Policy. Die Ausstellung des Zertifikats hat den einzigen

Zweck, den Betreibern der WWW-Server verschlüsselte Datenübertragung zu ermöglichen, ohne dass sie gleich viel Geld an amerikanische Firmen überweisen müssen.

Wenn ein Server hier genannt wird, bedeutet dies nur, dass ich ein noch gültiges Zertifikat für den Server ausgestellt habe, jedoch nicht, dass der Server läuft oder für andere als interne Zwecke des jeweiligen Instituts verwendet wird.

www.uni-muenster.de
Universitätsrechenzentrum
Serial Number: 12 (0xc) Valid Not After: Dec 17 13:42:45 2002 GMT
Fingerprint=D0:B9:D4:0A:47:C3:BE:7D:A9:2E:DA:BB:BB:56:1A:CB

mail.uni-muenster.de
Universitätsrechenzentrum
Serial Number: 14 (0xe) Valid Not After: Dec 17 14:03:35 2002 GMT
Fingerprint=91:73:A4:91:77:A0:CD:5A:BF:22:AD:C0:FE:5A:3D:67

user.uni-muenster.de
Universitätsrechenzentrum
Serial Number: 16 (0x10) Valid Not After: Dec 17 15:48:16 2002 GMT
Fingerprint=4F:D7:42:05:05:AA:EE:80:FF:35:C7:B4:53:09:6C:1F

wildcat.uni-muenster.de
Institut fuer Wirtschaftsinformatik
Serial Number: 19 (0x13) Valid Not After: Sep 1 13:48:38 1999 GMT
Fingerprint=78:CF:70:A7:81:69:AE:C4:7D:17:C5:BC:09:E1:42:6D

www-wi.uni-muenster.de
Institut für Wirtschaftsinformatik
Serial Number: 20 (0x14) Valid Not After: Sep 15 12:33:41 1999 GMT
Fingerprint=2E:6A:75:5B:A1:B5:79:2D:E3:13:E8:3B:2B:8B:C1:ED

THGMS.Uni-Muenster.DE
THG-Chirurgie
Serial Number: 21 (0x15) Valid Not After: Oct 22 12:57:49 1999 GMT
Fingerprint=EA:FA:4A:63:73:F9:83:7A:C9:D8:43:BD:81:21:82:33

asterix.uni-muenster.de
Zentrum für Informationsverarbeitung
Serial Number: 23 (0x17) Valid Not After: Oct 23 16:02:17 1999 GMT
Fingerprint=33:E1:12:C4:DF:C1:F7:5D:79:5B:6F:7A:DC:4B:89:06

user.uni-muenster.de
Zentrum für Informationsverarbeitung
Serial Number: 24 (0x18) Valid Not After: Oct 3 15:37:01 2001 GMT
Fingerprint=7D:31:D4:5A:38:10:6F:9E:4C:32:AE:42:D3:23:92:09

www.uni-muenster.de
Zentrum für Informationsverarbeitung
Serial Number: 25 (0x19) Valid Not After: Oct 8 16:17:09 2001 GMT
Fingerprint=24:D7:B8:83:93:2E:E1:A6:3A:00:96:1D:8B:F6:3D:4F

pcwi003.uni-muenster.de
Institut fuer Wirtschaftsinformatik
Serial Number: 26 (0x1a) Valid Not After: Mar 18 17:13:20 2000 GMT
Fingerprint=B6:BA:56:6D:82:CB:D3:34:53:0F:F2:08:5D:5C:88:5E

wwwunix.uni-muenster.de
Zentrum für Informationsverarbeitung
Serial Number: 29 (0x1d) Valid Not After: Apr 29 15:02:13 2000 GMT
Fingerprint=52:0D:67:00:1D:F7:FB:BE:1E:C5:2F:DA:B0:85:AA:2E

RUM-Tutorial

Spuren im Netz

L. Donnerhacke (Jena)

Surfen im Netz ist kein anonymes Unterfangen. Jeder, der sich darin tummelt, hinterlässt eine Menge Spuren. Der Autor macht auf seine lockere Art darauf aufmerksam. Wir danken für die Erlaubnis zum Abdruck im infoRUM.

Jeder, der sich bewegt, hinterlässt Spuren. Wenn Old Shatterhand und Winnetou den bösen Bleichgesichtern nachlaufen, so lesen sie die Spuren mit Sachkunde und Verstand. Analog gehen die modernen Schnüffler der Polizei und vieler privater Unternehmen vor.

Wer hat noch nicht Werbemüll im Briefkasten gefunden? Wie ein Lottoveranstalter an die Adressen kommt? Ganz einfach: Über das Einwohnermeldeamt.

Es gibt Leute, die geben bei der Beantragung Ihrer Bahncard ein Passbild ab, obwohl sie auf den umseitigen Bedingungen darauf hingewiesen werden, dass alle Daten incl. dieses Bildes zur Firma Electronic Data Systems (EDS) in die USA geschickt werden. Dies geschieht, weil die Deutsche Bahn die Kartenerstellung durch die Citibank machen lässt, während EDS für die Citibank die EDV erledigt. Die Firma verfügt über erstklassige Informationsquellen bis hin zu aufgekauften Spionagesatelliten. Durch (in Deutschland untersagte) Zusammenführung von Datenbanken kann hier ein privatwirtschaftliches Unternehmen die unglaublichsten Dinge bewegen. So wurde bspw. ein alimentenflüchtiger Engländer bei einem Inlandsflug von Neu Delhi nach Bombay verhaftet. Grund: EDS arbeitet für Air India (und weitere 23 große Fluggesellschaften) und die englische Steuerbehörde.

Wem solche Geschichten Angst einjagen, der möge sich von einem alten Sprichwort trösten lassen: „Auch wenn du nicht paranoid bist, so heißt das noch lange nicht, dass sie nicht hinter dir her sind“.

An einigen Plätzen hinterlässt man viele Spuren, an anderen weniger. Während man bei körperlicher Anwesenheit immer Spuren (Hautschuppen, Haare, ...) hinterlässt, die bspw. in der zentralen Gendatenbank des Herrn Kanther nachgeschlagen werden können, sind elektronische Medien von diesem Makel befreit.

Elektronische Medien

Auch wenn Fingerabdrücke, Blutspuren, Speichelreste oder einfache Kleidungsreste im Netz nicht zurückbleiben können, so ist doch die Kommunikation im Netz extrem formalisiert. Schließlich unterhalten sich dumme Rechner mit dummen Rechnern.

So muss jeder Rechner eine eindeutige Nummer (IP-Adresse) haben, eine Art Postanschrift. Er erreicht andere Rechner ebenfalls über diese Adressen. Jeder, der die Datenleitungen am Ende oder irgendwo dazwischen anzapfen kann, kann so ein Nutzungsprofil erstellen. Das ist einfacher, als man denkt! Auf dem Weg zum Zielsystem sind eine Vielzahl unabhängiger Kleinunternehmen involviert. Ob es der Telefonanbieter, der Provider oder dessen Telefonanbieter ist ...

Auf dem Zielsystem ist es dagegen sehr einfach. Alle Serverdienste, wie Web und Dateiserver, führen penibel Logfiles, wer wann von wo was gelesen hat. Man kann deutlich erkennen, wie `md59-072.mun.compuserve.com` alias `195.232.62.72` zuerst die ActiveX-Webseite mit allen darauf liegenden Bildern geholt hat. Vierzehn Minuten später (die Seite ist wirklich lang) wechselt er zum Ewigen Logfile und benutzt es. Übungsaufgabe: Wie schnell liest er? Liest er gern und viel? Hat er einen hohen Bildungsstand?

```
md59-072.mun.compuserve.com - - [16/Apr/1998:00:08:54 +0200]
   "GET /mitarb/lutz/security/activex.html HTTP/1.1" 200 13803
md59-072.mun.compuserve.com - - [16/Apr/1998:00:08:59 +0200]
   "GET /mitarb/lutz/security/activex.gif HTTP/1.1" 200 6176
md59-072.mun.compuserve.com - - [16/Apr/1998:00:08:59 +0200]
   "GET /mitarb/lutz/security/radioactivex.gif HTTP/1.1" 200 2904
md59-072.mun.compuserve.com - - [16/Apr/1998:00:09:01 +0200]
```

```
   "GET /pic/key.gif HTTP/1.1" 200 184
md59-072.mun.compuserve.com - - [16/Apr/1998:00:09:01 +0200]
   "GET /pic/unkey.gif HTTP/1.1" 200 196
md59-072.mun.compuserve.com - - [16/Apr/1998:00:14:07 +0200]
   "GET /mitarb/lutz/cgi-bin/logfile.pl?form HTTP/1.1" 200 949
md59-072.mun.compuserve.com - - [16/Apr/1998:00:14:25 +0200]
   "POST /mitarb/lutz/cgi-bin/logfile.pl?submit HTTP/1.1" 200 3557
```

Die Auswertung der Logfiles ist das tägliche Brot der Netzdienstleister zum Wohle Ihrer Kunden. Diese Kunden nutzen diese persönlichen Verhaltensprofile zu den verschiedensten Zwecken. Einige passen Ihr Angebot an, so dass die kleinen Angebote zugunsten eines Mainstream verschwinden. Andere leiten die Daten an Direktmarketingagenturen weiter, manchmal auch durch einfachen Verkauf.

E-Mail

Nutzt man Dienste, die ohne direkten Kontakt zum Gegenüber auskommen, wie E-Mail oder Usenet, so kann der Empfänger natürlich nicht einfach die IP-Adresse bestimmen. Jedoch schreiben alle beteiligten Systeme den zurückgelegten Weg in die transportierte Nachricht und führen darüber hinaus noch ein Logfile über alle Aktivitäten.

```
Return-Path: <news@as-node.jena.thur.de>
Received: from jengate.thur.de (uucp@jengate.thur.de
   [193.174.15.34])by avalon.iks-jena.de (8.8.8/8.8.8) with ESMTP
   id DAA19260 for <lutz@iks-jena.de>; Fri, 17 Apr 1998 03:22:22
   +0200 (MET DST)
Received: from as-node.jena.thur.de (uucp@localhost)
   by jengate.thur.de (8.8.8/8.8.8) with BSMTP id DAA09046 for
   lutz@iks-jena.de; Fri, 17 Apr 1998 03:22:20 +0200
Message-Id: <m0yPf4f-0005ZLC@as-node.jena.thur.de>
Date: Thu, 16 Apr 98 05:10 MET DST
From: news@as-node.jena.thur.de (news)
To: usenet@as-node.jena.thur.de
Subject: checkgroups by group-admin@isc.org
```

Diese Nachricht wurde (angeblich) von `news@as-node.jena.thur.de` abgesendet. Das kann natürlich gefälscht sein. In der ersten Received-Zeile ist zu lesen, woher mein Zielsystem die Nachricht bekommen hat: `Jengate.Thur.De`. Gleichzeitig schreibt er die genaue Zeit und die IP-Adresse des Einlieferers auf.

`Jengate` selbst hat sich in der zweiten Received-Zeile verewigt und behauptet, die E-Mail von `As-Node.Jena.Thur.De` per BSMTP bekommen zu haben. Vermutlich über das Datenaustauschverfahren UUCP, das ohne IP-Adressen auskommt. Die `As-Node` hat sich nicht verewigt. Das kann sein, ist aber ungewöhnlich.

Die aufgeführte Message-ID ist ideal zum Spurenverfolgen. Sie bleibt den gesamten Transportweg über fest und kann somit als Nachfrageinstrument taugen. Ein Blick auf das Logfile von `Jengate` zur fraglichen Zeit bestätigt die Angaben. Die Mail kam also wirklich von der `As-Node`.

```
Apr 17 03:22:21 jengate sendmail[9046]: DAA09046:
   from=news@as-node.jena.thur.de, size=2288, class=0, pri=32288,
   nrcpts=1, msgid=<m0yPf4f-0005ZLC@as-node.jena.thur.de>,
   proto=BSMTP, relay=uucp@localhost
```

Wer E-Mail schickt, muss also damit rechnen, dass er zurückverfolgt werden kann. Adressfälschung schützt somit nicht vor Rückverfolgung. Auch Spammer (Werbemüller) werden so zweifelsfrei identifiziert. Dies führt i. d. R. zum Account-Verlust des Spammers, oder bei großen Firmen zum Eintrag in eine schwarze Liste. Diese Listen haben normalerweise so verheerende Folgen, dass die betroffenen Provider der Spammer aktiv werden.

Verschlüsselte Mail

Ein anderes Problem ist die Tatsache, dass E-Mail prinzipiell unverschlüsselt übertragen wird. Da sie auf vielen System zwischengespeichert werden muss, haben potentiell viele Menschen Zugang zum Mailinhalt. Es ist deshalb dringend anzuraten, den kompletten Mailverkehr zu verschlüsseln.

Dazu steht hauptsächlich die Software PGP zur Verfügung. PGP2.6.3in ist von den älteren Versionen die am weitesten entwickelte. Mit einigen Zusatzprogrammen kann man damit auch gut arbeiten. Die Versionen PGP5.x sind zwar leichter zu bedienen, haben aber eine Funktion eingebaut, mit der ein Dritter den Nachrichtenverkehr mitlesen könnte. Das ist zwar nicht einfach, wird aber von PGP5 aktiv unterstützt. Alle PGP-Versionen werden durch den kompatiblen Internet-Standard OpenPGP abgelöst. Dieser enthält viele Schwachstellen beider Versionen nicht mehr.

Wer verschlüsselt, muss ja dem Gegenüber irgendwie mitteilen, mit welchen Schlüsseln eine Datei codiert wurde. Diese Schlüsselnummer steht immer dabei. Man kann sie benutzen, um eine verschlüsselte Nachricht auch dann wiederzuerkennen, wenn man den Absender oder Empfänger kaum ausmachen kann. Um diese Spur zu verwischen, bietet OpenPGP an, diese Kennung auch weglassen zu können. Die Empfangsseite muss dann zwar mühsam (aber automatisch) probieren, jedoch ist dieser Angriff ausgeschaltet.

Usenet

Mit Newsartikeln ist es ganz ähnlich. Jedoch kann *jeder* die Nachricht auf diese Weise analysieren.

```
Path: news.iks-jena.de!jengate.thur.de!akk.uni-karlsruhe.de!
   riemann.iam.uni-bonn.de!fu-berlin.de!newsfeed.pop.de!
   news.hamburg.pop.de!not-for-mail
From: h.roth@mail.hh.provi.de (Hermann Roth)
Newsgroups: de.admin.net-abuse.news
Subject: Re: de.admin.net-abuse.news und Netiquette
Date: Thu, 09 Apr 1998 16:04:35 GMT
Organization: privat
Lines: 23
Message-ID: <6girja$j53$5@popnews.hamburg.pop.de>
References: <6e9i9b$nvl$1@goof.de.uu.net> [...]
   <6egqdt$2nm$1@seeadler.zwirgel.net>
   <351c8848.3159574@news.rrz.uni-koeln.de>
NNTP-Posting-Host: pop230.hh.provi.de
Mime-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 8bit
X-Newsreader: Forte Agent 1.5/32.451
```

Dieser Artikel stammt (angeblich) von einem Hermann Roth. Er wurde in die Usenet-Newsgruppe `de.admin.net-abuse.news` gepostet, die sich mit dem Usenet-Missbrauch befasst. Auch hier taucht wieder eine Message-ID auf, die für mindestens zwei Jahr weltweit eindeutig sein muss. Man kann also mit dieser ID den Artikel fast immer wiederfinden. Es sei denn, er wurde auf allen Rechnern gelöscht ...

In der References-Zeile finden sich die Message-IDs der Artikel, auf die Hermann geantwortet hatte. Fast alle dieser Zeilen kann man fälschen. Einige wenige jedoch nicht.

NNTP-Posting-Host wird normalerweise von dem Newsserver eingetragen, den Hermann genutzt hat. Über 99% aller Fälscher von Artikeln vergessen das oder können es nicht umgehen. Diese Angabe besagt, dass er auf dem Hamburger Einwahlknoten des Providers `provi.de` den Platz 230 hatte. Diese dynamische Zuordnung kann der Provider leicht auf Rückfrage durch Blick in die Logfiles auflösen. Der Absender ist so ermittelbar.

Die Path-Zeile ist das Pendant zu den Received-Zeilen der Mail. Sie listet Stück für Stück auf, welche Rechner den Artikel transportiert haben. Der IKS-Rechner hat ihn von `Jen-gate`, der wiederum hat ihn aus Karlruhe, der ihn aus Bonn, und schließlich über Berlin aus Hamburg. Es zeigt sich auch, dass `provi.de` eigentlich `pop.de` ist. Wollte man hier fälschen, so müsste man die Kette fortsetzen. Das ist alles andere als trivial und wird normalerweise schnell entdeckt. Im Zweifel geht man stückweise rückwärts, um den Absender zu ermitteln.

Ein besonderes Schmankerl ist die X-Newsreader-Zeile. Er verwendet den Forte Agent, die registrierte Vollversion eines Windows-Programms. Dies besagt normalerweise, dass

Hermann ein ehrlicher Mensch ist, denn er hat den Preis für die Shareware bezahlt, wie es sich für anständige Menschen gehört. Außerdem benutzt er Windows, also ein PC-System mit der typischen Lemming-Software. Es würde sich lohnen, ihn für passende Werbesendungen vorzumerken. Schließlich ist er ehrlich, oder?

Gefährliche Spuren im Web

Neben diesen trivialen und offensichtlichen Ansätzen gibt es auch noch ganz bösartige Fallen. So senden einige Web-Browser die E-Mail-Adresse des Nutzers mit. Wer das gefahrlos probieren möchte, schaue mal auf `http://nike.rz.uni-konstanz.de:8888/`[1]

```
Referer: https://www.iks-jena.de/mitarb/lutz/anon/linkstat.html#
User-Agent: Mozilla/3.01 (X11; U; Linux 2.0.33 i586)
Host: nike.rz.uni-konstanz.de:8888
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Via: 1.0 www-cache.iks-jena.de:3128 (Squid/1.NOVM.20)
X-Forwarded-For: unknown
Cache-control: Max-age=2592000
```

In diesem Fall besagt die Ausgabe, dass der Nutzer von der in Referer angegebenen Webseite gekommen ist. So ist eine Spurverfolgung über mehrere Rechner kein Problem. Werbung im Web wird über diese Zeile maßgeblich abgerechnet.

User-Agent gibt an, dass eine alte Version von Netscape (Mozilla) auf einem aktuellen Linux mit Pentium-PC und der graphischen Benutzungsoberfläche X11 benutzt wurde. Dies zeigt dem Marketingspezialisten, dass ich gegen den Strom schwimme. Ein komplexeres Betriebssystem im gepflegten Zustand, also Interesse in technischen Belangen. Jedoch an anderen Stellen mäkelig: Nicht die neuste Version. Vermutlich aus gutem Grund, denn das Betriebssystem ist aktuell. Werbung für Windows-Produkte ist hier verfehlt, aber so ein paar teure Gadgets könnten auf Interesse stoßen.

Der Zugriff erfolgte über einen WWW-Cache. Die ungewöhnliche Version der Software Squid zeigt, dass der Admin, der dieses System betreut, sehr sorgfältig arbeitet. Vermutlich ist also das gepflegte Linux-System auch diesem Admin zuzuschreiben. Dann ist der veraltete Browser ein Zeichen von Schlampigkeit und Widerwillen gegen Technik. Es wäre ratsam, von der Gadget-Werbung Abstand zu nehmen.

Der Cache anonymisiert leicht, denn er verrät nicht, für wen er die Anfrage ausführt. Da der Squid noch viel weitergehende Anonymisierungsmöglichkeiten enthält, ist der Admin auf der Hut, aber kommerziellen Interessen erlegen. Eine weitergehende Anonymisierung würde die Marketingspezialisten verärgern.

Ebenfalls auffällig ist, dass keine Cookies auftauchen. Der Nutzer ist also leicht bis schwer paranoid veranlagt, da er dies abgeschaltet hat. Ihm Werbung zuzusenden, könnte böse ins Auge gehen.

Cookies

Wenn die Werbeindustrie langfristige Bewegungsprofile von Nutzern anlegen will, so kann sie sich nicht auf diese Spuren verlassen. Firmen wie DoubleClick (`www.doubleclick.com`) bieten eine einfache Lösung dafür.

Besucht ein Nutzer eine Webseite, so bekommt er mit der Antwort der Servers auch eine Information `X-Set-Cookie: text`, die den Webbrowser veranlasst, sich diesen Text zu merken. Verbindet sich der Webbrowser zu einer beliebigen späteren Zeit wieder mit diesem Server, so schickt er ohne Aufforderung diesen Text zurück.

Der Server kann so erkennen, wer sich hier wie über die Informationsmenge bewegt.

---

[1] Anm. der Red.: Dieser Server existiert leider nicht mehr, aber schauen Sie mal nach unter `http://www.uni-muenster.de/exec/what`

Damit das übergreifend klappt, wird das Icon von DoubleClick immer vom DoubleClick Server geladen. Mit der Refer-Zeile kann nun DoubleClick eine sehr genaues Kundenprofil erstellen. Kauft man irgendwo ein, oder bestellt sich etwas per Mail, so hat DoubleClick den Personenbezug.

Diese Daten sind für die Direktmarketing-Agenturen so wertvoll, dass sich die Firmen wie DoubleClick eine goldene Nase verdienen können.

Das Gerücht, Cookies können auch Festplatten zerstören oder ausspionieren, ist jedoch falsch.

Gefährliche Spuren bei FTP

Dateiübertragungen werden immer noch gerne per FTP durchgeführt. Zum Anmelden auf einem FTP-Server benötigt man jedoch ein Passwort. Für den anonymen Zugang hat es sich eingebürgert, die E-Mail-Adresse zu verwenden. Damals, als die Netze noch von wenigen bevölkert, die Wiesen noch grün ... Also damals gab es die kommerzielle Nachverwertung fast nirgends und es war ein Gebot der Höflichkeit, den anonymen Zugang nicht anonym zu nutzen.

```
Fri Apr 17 01:00:15 1998 1 uranus.central.de 7787
   /pub/mitarb/lutz/teergrube/teergrube.delay.spammer b _ o a
   root@uranus.central.de ftp 0 *
Fri Apr 17 01:44:49 1998 1 rusxppp139.rus.uni-stuttgart.de 2909
   /pub/mitarb/lutz/crypt/software/pgp/pgp263in/pgp263in.changes
   b _ o a mozilla@ ftp 0 *
```

Im Logfile kann man schön erkennen, dass ein System sich an die alten Gepflogenheiten hält und die E-Mail-Adresse mitsendet. Das andere jedoch nicht. Netscape sendet stattdessen die Pseudoadresse `mozilla@`. Es gibt mittlerweile auch FTP-Server, die auf einer korrekten Adresse bestehen und diese auch überprüfen. So ist die Adresse von `Uranus` vermutlich nicht gefälscht, da die Verbindung von eben jenem Rechner kam.

```
Fri Apr 17 10:44:55 1998 2 d120.z194-58-231.relcom.ru 302
   /pub/mitarb/lutz/crypt/software/pgp/pgp263in/2.6.3in971006-971
   007.diff.asc b _ o a whoever@microsoft.com ftp 0 *
```

In diesem Fall ist die Fälschung dagegen offensichtlich, oder? Es gibt immer wieder einige Experten, die es tatsächlich hinbekommen, beim Anmelden auf einem FTP-Server ihr wirkliches Systempasswort anzugeben. Sie wurden ja nach einem Passwort gefragt! Man kann sich darüber streiten, ob es eigene Dummheit oder Überforderung ist. Die Gefahr bleibt.

Gefährliche Spuren bei T-Online

Wer über T-Online angeschlossen ist, hat es besonders schwer. T-Online als Tochter des ehemaligen Monopolisten Deutsche Bundespost arbeitet an sehr vielen Stellen sehr bürokratisch. So werden auf allen Homepages ein Impressum zwangsgesetzt. Wer auf einer Webseite ist, braucht nur die Seite `.impressum.html` abzufragen. Dort findet sich

- der volle Name des Nutzers,
- die komplette Anschrift,
- die Telefonnummer,
- die E-Mail Adresse.

Die zusätzlichen AGBs, die das beschreiben, sind in einer defekten PDF-Datei, also nicht leicht einsehbar, versteckt.

Auch in den Usenet-News passieren die seltsamsten Dinge. Hier ein Ausschnitt aus einer Diskussion in `de.org.ccc`:

```
From: Corny_K@t-online.de (Nikkon)
Subject: Experiment!
```

```
Date: 12 Apr 1998 19:30:25 GMT

Hi
Mich würde mal sehr interessieren was man so auf legaler
weise über mich und meine Daten herausfinden kann.
IP,...
```

Die Antworten kamen stakkatoartig.

```
Hmm... mal sehen.
Also, Dein Internet Provider ist schon mal T-Online.
Du benutzt als Nickname das Kuerzel "corny_k", und gibst
vor, dass Dein Realname "Nikkon" sei.

Außerdem hast Du Deine Nachricht am 12. April 1998 ge-
schrieben. Also Du online warst, warst Du auf Port
news02.btx.dtag.de Online. Anhand der Message ID koennte
man dann mit Hilfe der T-Online Logdateien vermutlich
einiges herausfinden.
Aber es geht auch so.

Dein Mailreader ist der "Forte Free Agent" in der Versi-
on 1.11/32.235.

Dein Name ist vermutlich Michael Korn.

Deine Adresse ist wohl: Rebbergblick 15, 77960 Seelbach,
Schutter.

Die Telephonnummer koennte die 07823 432 sein.

  ------------------------------

Deine Nachbarn heißen Catharina Kolb, Armin Roth und
seine Frau Anne Roth-Ohnemus. In der gleichen Straße,
nur auf der anderen Seite, hat Dr. Gerhard Baran seine
Tierartzpraxis.

  ------------------------------

DejaNews AuthorProfile verraet noch allerhand mehr ..

Homepage http://home.t-online.de/home/07823432-0001/
noch schwer im Aufbau ...
```

Wie die erste Antwort zustande kam, ist bereits erklärt worden, aber wie geht der Rest? Die Telefonnummer schreibt T-Online automatisch und zwangsweise in den Nachrichtenkopf!

```
X-Sender: 07823432-0001@t-online.de
```

Damit ist es leicht, entweder eine Telefonbuch-CD zu befragen, oder ganz einfach das Impressum der Homepage abzurufen. Die Nachbarn stehen im Adressbuch. Man kann sogar auf den sozialen Status schließen, indem man die Einwohner pro Hausnummer zusammenzählt.

DejaNews

Es wurde DejaNews erwähnt. Was ist das? DejaNews ist ein Suchdienst, der versucht alle Artikel in allen Newsgruppen recherchierbar zu halten. Was bei Geheimdiensten Normalität ist, wird so dem normalen Nutzer ebenfalls ermöglicht. DejaNews bietet so ziemlich alle Suchmöglichkeiten, die man sich wünscht. Leider ist die kostenlose, öffentliche Datenbank etwas eingeschränkt. Für einige Dollar ist das aber leicht zu ändern.

Befolgt man den Rat und erstellt ein Autoren-Profil für `Nikkon`, so zeigt Dejanews folgendes an:

```
99%  de.org.ccc
42%  de.newusers.questions
42%  fido.ger.win95
36%  de.alt.hoerfunk
```

```
36%  de.rec.tv.misc
30%  de.talk.jugend
24%  de.alt.geschichten
24%  de.alt.radio-scanner
17%  de.etc.bahn.eisenbahn
17%  de.talk.jokes
11%  de.comm.mobil.pager
11%  de.etc.bahn.stadtverkehr
11%  de.rec.motorroller
11%  fido.ger.ccc
11%  fido.ger.isdn
11%  z-netz.fundgrube.gratis
11%  z-netz.rechner.ibm.windows.win95
11%  z-netz.telecom.telefon
11%  z-netz.wissenschaft.technik
```

Es ist leicht zu sehen, dass die betreffende Person in letzter Zeit vornehmlich in `de.org.ccc`, `de.newusers.questions` und Win95er-Gruppen aufgetaucht ist. Fasst man die Kategorien zusammen, so ergibt sich die Interessenlage zu:

- Hacken = Kreativer Umgang mit Technik
- Motorroller fahren
- Win95 und ISDN
- Geschichten und Filme

Nebenbei ist er noch jung (vermutlich unter 18) und neu im Medium.

Obwohl die Daten nicht sehr aussagekräftig sind, denn dazu ist eine längere Netzteilnahme notwendig, sollte es doch zum Nachdenken anregen. Was wäre, wenn das letzte Ablehnungsschreiben diesen Hintergrund hatte?

Wie prüfe ich mich selbst? `http://www.dejanews.com/home_if.shtml`

Neben DejaNews gibt es auch noch viele andere News-Archive. Die meisten sind nicht öffentlich und werden von Geheimdiensten oder Firmen betrieben. Als Kuriosität gelten die Babylonischen Purpurdaten. Dieses News-Archiv wird von Ralph Babel im Taunus betrieben. Um Daten aus den Purpurdaten abzufragen, muss man Ralph öffentlich so bedrängen, dass er nur durch Zitieren des gewünschten Artikels die Anschuldigung von sich weisen kann. Normalerweise wird er jedoch nur die Message-ID zitieren. Dann hilft nur noch, hartnäckig zu bleiben.

Das vermutlich am weitesten zurückreichende Archiv liegt bei Heiko Schlichting in Berlin: Als zu Beginn der Neunziger eine Newsverbindung zwischen der TU und der FU aufgebaut werden musste, fuhr man mit dem Fahrrad Streamer-Kassetten hin und her. Für diese Exabyte-Bänder ist heute jedoch kein Lesegerät mehr aufzutreiben.

Suchmaschinen

Wer im Netz länger aktiv ist, wird auf irgendeiner Webseite auftauchen, ob zitiert oder selbstgeschrieben. Wer eine Suchmaschine wie Altavista, Hotbot oder sonstige nach seinem Namen befragt, kann Erstaunliches zutage fördern.

Praktisch jede geschäftliche Begegnung wird in den ersten Kontakten von derartigen Suchaktionen begleitet. Schließlich möchte man ja nicht an einen Scharlatan geraten. Es ist so einfach, zu suchen... aber die Interpretation ist sehr sehr schwer.

Es kommt häufiger vor, dass man bei der Suche in die Irre läuft. Einige kleinere Firmen gestalten Ihre Webseiten so, dass man auf der Suche nach einer Konkurrenzfirma zu ihnen gelangt. Die Tricks sind einfach, aber wirkungsvoll: Weiße Schrift auf weißem Grund, spezielle Keyword-Kopfzeilen auf der HTML-Seite etc. pp.

Wenn man in einer bestimmten Situation sich über eine Ablehnung durch einen Geschäftspartner wundert, so sollte man selbst mal schauen, wie die Suchmaschinen das eigene Selbst darstellen. Inzwischen ist das World Wide Web schon so weit kommerzialisiert,

dass der Verursacher juristisch belangt werden kann.

Diese juristischen Schritte werden aber vorwiegend gerne von den Haien und Hechten im Geschäft angestrengt. So kann es dem Durchschnittsbenutzer schon mal passieren, dass er eine Abmahnung erhält. Die Gründe können so vielfältig wie dumm sein. Es genügt manchmal schon, einen bekannten Firmennamen (in einem ganz anderen Zusammenhang und keinesfalls mit Hintergedanken) auf der Webseite zu haben. Wenn diese Webseite bekannt ist, also von vielen anderen verlinkt wurde, dann kann sie in der Wertung der Suchmaschine die eigentlichen Firmenseiten übertrumpfen. Das lässt sich kaum eine große Firma bieten.

Es gibt allerdings auch Fälle, in denen man vorsätzlich persönlich angegriffen wird. So führen Linksextreme in den USA eine Liste von Leuten, die sie für Nazis halten. Da ich irgendwann einmal in einer Abstimmung für die Newsgruppe rec.music.white-power gestimmt habe (um die Gruppe rec.music.misc zu entlasten), stehe ich auch auf dieser Liste. Gegen Dummheit ist einfach kein Kraut gewachsen. Allerdings können nur wenige Personalchefs das wirklich begreifen. Es bleibt nur die Hoffnung auf einen Generationswechsel in diesen Büros.

Chat und IRC

In der Werbung heißt es stets: „Anarchie und Freiheit. Spaß im Netz.“ Dieser Spruch hat in keinem Bereich so viel Wirkung gezeigt wie im IRC, dem Internet Relay Chat. Da Chat eine live, also online, Angelegenheit ist, ist dem Chat-Server die IP-Adresse bekannt.

Darüberhinaus erhält der Chatserver auch die E-Mail-Adresse und den Namen. Da diese Daten aber jedem Chat-Teilnehmer zur Verfügung stehen, ist es selbstverständlich, dass auch hier Firmen diese Daten auswerten.

Deshalb und weil die E-Mail-Adresse technisch nicht notwendig ist (im Gegensatz zu Mail und News), findet man hier viele gefälschte Adressen. Mit einem Pseudonym sinkt aber gleichzeitig die Hemmschwelle der von der Werbung geköderten Neulinge, so dass das Medium Chat stark verkommen ist. Es geht zu wie im Kindergarten.

Da aber die IP-Adresse bekannt ist, bleibt die Anonymität im Chat ein Traum.

Trojaner

Wer kennt nicht die blinkenden und tönenden Webseiten, die man kaum ohne Kopfschmerzen ertragen kann? Ein besonderes Gimmick sind jedoch die aktiven Inhalte, also Java, JavaScript oder ActiveX-Programme. Diese können den Browser um völlig neue Funktionen erweitern.

Während JavaScript nur wenige Zusatzfunktionen des Browsers ansprechen kann und Java in einer gesicherten Umgebung („Sandbox“) abläuft, haben *ActiveX Controls* völlig freien Zugriff auf alles, was im Rechner passiert.

ActiveX Controls sind also richtige Programme, die man per Browser und Mausklick auf das System lädt, installiert und startet. Sie können ungehindert die Platte auslesen, Seriennummern von Software an den Hersteller schicken, die Finanz- und Bankensoftware fernbedienen usw. usf.

Damit nun dieses Scheunentor nicht allzu weit offen steht, werden normalerweise nur zertifizierte *Controls* geladen. Das bedeutet, der Programmierer unterschreibt, dass das sein *Control* ist. Die Identität des Programmierers wird von einer Zertifizierungsinstanz bestätigt. Im Zweifel kann man ihn also verklagen.

Da jedoch für Europa keine Zertifizierung verfügbar ist, die von Microsoft akzeptiert wird, erstellen die meisten Programmierer unzertifizierte *Controls*. In vielen Browsern sind deswegen die sowieso fragwürdigen Sicherheitsprüfungen abgeschaltet.

Wer sich diese Dinge mal praktisch ansehen will, kann auf

`http://www.iks-jena.de/mitarb/lutz/security/activex.html` vorbeischauen. Es sind auch aktive Beispiel-*Controls* verfügbar, die ein wenig von ihren Schnüffelvorgängen berichten.

Was tun?

So schlimm es klingt, was kann man nun wirklich tun? E-Mail sollte man immer verschlüsseln. Will man anonym Mail versenden, so muss man anonyme Remailer benutzen.

In den Usenet News sollte man immer daran denken, dass man einem öffentlichen Medium angehört, und sich entsprechend verhalten. Will man trotzdem etwas Kritisches oder Heikles ansprechen, so benutzt man auch hier anonyme oder pseudonyme Remailer.

Wer im World Wide Web nicht alles herausposaunen will, sollte seinen Provider nach einem anonymisierenden Proxy fragen. Der Squid hat standardmäßig die Einstellungen `Anonym Ja/Nein` und `Paranoid`.

Dieser Text unterliegt der GNU Public License.

Sichere Nutzung des World Wide Web

B. Brandel (Eichstädt)

Diesen Beitrag drucken wir mit Genehmigung des Autors nach leichter Anpassung an die hiesigen Gegebenheiten.

Das World Wide Web ist ein dichter Dschungel von netzartig miteinander verbundenen Hypertext-Dokumenten. Wer sich im WWW bewegt, muss wissen, dass auf Schritt und Tritt Gefahren lauern. Diese einschätzen und meistern zu helfen ist Ziel dieses Artikels, der auch auf verschiedene an deutschen Rechenzentren veröffentlichte Artikel zurückgreift (siehe Literatur).

Die Anfänge des WorldWideWeb

In der ursprünglichen Form des WorldWideWeb bewegten sich die Benutzer relativ gefahrlos, aber ohne Interaktionsmöglichkeiten von Verweis zu Verweis in den Dokumenten im Hypertext-Raum. Man konnte lediglich die dort abgelegten Informationen empfangen, ohne selbst direkt den Betreibern der gerade betrachteten Seiten auf dem WWW-Server Informationen zurücksenden zu können.

CGI

Um dem Wunsch der WWW-Nutzer nach Interaktivität nachzukommen, wurde die Sprache des WWW um Formularbefehle und um das Common Gateway Interface (CGI) erweitert. Damit kann der Besucher einer WWW-Seite beispielsweise ein dort abgelegtes Formular im Browserfenster auf seinem PC ausfüllen (z. B. das Suchformular einer Suchmaschine). Danach werden die Formulardaten über das Internet zurück zum WWW-Server transportiert. Auf dem Server wird dann ein Programm gestartet, das in mehreren Schritten die Weiterverarbeitung der Daten durchführt. z. B.:

1. Abfrage der zur Suchmaschine gehörenden Suchdatenbank,
2. dynamische Erzeugung von HTML-Code mit den Suchergebnissen,
3. Übertragung dieser HTML-Daten an den aufrufenden WWW-Browser,
4. Anzeige der Suchergebnisse im Browserfenster.

Da CGI-Scripte auf dem Server und nicht auf dem lokalen PC des Benutzers ablaufen, gibt es für den lokalen PC i. Allg. keine großen Sicherheitsprobleme. Als Benutzer sollte man allerdings bedenken, dass eingegebene Formulardaten meist ungeschützt oder schlecht verschlüsselt über das Netz transportiert werden. Es besteht daher durchaus die Möglich-

keit, dass sie auf ihrem Weg durchs Internet von Dritten gelesen und manipuliert werden! Speziell bei finanziellen Transaktionen mit Kreditkartennummern sollten Sie zuvor mit Ihrem Kreditkartenvertreiber genau abklären, wer im Schadensfall haftet!

Die eigentlichen Sicherheitsprobleme bei CGI-Scripten treten dagegen vor allem auf dem Server auf und werden von den Webmastern sorgfältigst überwacht:

Während an der Domäne `ku-eichstaett.de` die Seitengestaltung i. Allg. den inhaltlich Verantwortlichen (Lehrstühlen etc.) überlassen ist, gilt dies aus Sicherheitsgründen nicht für CGI-Scripte. Diese benötigen auf dem WWW-Server zur Ausführung zwingend Administratorrechte, was bedeutet, dass ein bösartiges CGI-Script ohne Überprüfung durch das Betriebssystem alle Daten auf dem Server kompromittieren und löschen könnte!

Daher werden WWW-Server so konfiguriert, dass CGI-Scripte nur dann ablauffähig sind, wenn sie in einem ganz bestimmten Verzeichnis des Servers abgelegt sind, in dem nur die Webmaster Schreibrechte besitzen. Alle CGI-Scripte der Nutzer werden dann nach Rücksprache handverlesen von den Webmastern in diesem Verzeichnis abgelegt. Nur so kann sichergestellt werden, dass keine gefährlichen CGI-Scripte den Server lahmlegen können.

Auf `www.uni-muenster.de` wird ein anderer Weg beschritten: Auf Antrag wird den Informationsanbietern ein eigener, mit abweichenden Rechten versehener virtueller WWW-Server nur für CGI-Programme eingerichtet.

Java, JavaScript und ActiveX

Während CGI-Scripte nur auf der Serverseite Programme starten können, erlauben die WWW-Erweiterungen Java, JavaScript und ActiveX den Start von Programmen auf dem lokalen WWW-Client. Wenn derartige Programme in HTML-Dokumente eingebunden sind, werden sie beim Aufruf der entsprechenden WWW-Seite vom WWW-Server zum lokalen Rechner transportiert und dort – meist ohne Rückfrage – gestartet. Dies birgt natürlich die Gefahr, dass Sie auf diese Weise durch bloßes Anklicken einer Seite des WWW auf Ihrem PC Programme ausführen, deren Funktionsweise sie gar nicht kennen und die Funktionen enthalten können, die Ihren PC schädigen oder vertrauliche Informationen über Sie weitergeben. In den nächsten Abschnitten werden die Besonderheiten der Sprachen Java, JavaScript und ActiveX hinsichtlich ihrer Konzeption und Sicherheitsmechanismen dargestellt.

Java

Java ist eine objektorientierte Programmiersprache, die von der Firma Sun Microsystems entwickelt wurde. Java wurde mit dem Ziel der Plattformunabhängigkeit entwickelt, d. h. dass Javaprogramme auf fast allen Rechnerplattformen direkt ohne weitere Übersetzung abgearbeitet werden können. Dazu wird der Quellcode in einen rechnerunabhängigen Code (Bytecode) übersetzt und zur Ausführung bereitgestellt.

Beim Betrachten von WWW-Dokumenten, in die Java-Programme eingebunden sind, auch Applets genannt, werden diese vom Server heruntergeladen und von einem virtuellen Rechner (Java Virtual Machine), der im WWW-Browser eingebaut ist, interpretiert und abgearbeitet. Da Java eine universelle Programmiersprache und nicht auf die Verwendung im WWW eingeschränkt ist, ist es vom Sprachkonzept her Javaprogrammen nicht verboten, beliebige Funktionen im Computer auszuführen, insbesondere ist der Zugriff auf die lokalen Ressourcen (lokale Festplatte, Netzwerk u. a.) i. Allg. durchaus sinnvoll und erwünscht. Für Javaprogramme unbekannter Herkunft aus dem Internet sind Zugriffsrechte dieser Art aus Sicherheitsgründen völlig indiskutabel. Deshalb wurden Java-Applets in WWW-Dokumenten folgende Beschränkungen auferlegt:

- Applets dürfen keine Dateien auf dem lokalen Rechner lesen oder schreiben.
- Applets können keine Netzwerkverbindungen aufbauen außer zu dem Rechner, von dem sie geladen wurden.
- Applets können keine Programme starten.

- Applets können keine Programmbibliotheken laden.
- Applets haben nur begrenzten Zugriff zu den Systeminformationen des lokalen Rechners.

Diese auch als „Sandbox“ bezeichnete Methode soll dazu führen, dass die von unbekannter Quelle aus dem WWW geladenen Programme keinen Schaden auf dem lokalen Rechner anrichten können. Die Überwachung der oben genannten Einschränkungen übernimmt der Java-Interpreter im WWW-Browser. Damit hängt aber die Sicherheit der Java-Applets völlig davon ab, wie sorgfältig diese Überwachungsfunktionen im Browser implementiert wurden! Die Vergangenheit hat gezeigt, dass immer wieder Sicherheitslücken in einzelnen Browserversionen aufgetreten sind, die dazu führen konnten, dass spezielle Applets Zugriff auf die lokale Festplatte erhielten oder andere unerwünschte Funktionen ausführten.

Die Sandbox-Methode hat aber auch den Nachteil, dass eventuell nützliche Funktionen mit Applets nicht realisiert werden können, wenn dazu Zugriffe auf die lokalen Ressourcen des Rechners benötigt werden. Deshalb hat die Firma Netscape für ihren Browser der Version 4 (Communicator 4.x) die Sicherheitsstrategie geändert. Die Applets können eine digitale Unterschrift vom Hersteller erhalten. Diese Unterschrift wird aus einer Art Prüfsumme vom Programm und einem persönlichen Schlüssel des Unterzeichners gebildet. Dadurch kann ein unterschriebenes Programm nachträglich nicht unbemerkt geändert werden. So unterschriebene Applets können dann einen erweiterten Zugriff auf lokale Ressourcen mit konkreter Angabe derselben (z. B. Leserecht auf der lokalen Platte) anfordern. Der Browser erkennt bei der Sicherheitsprüfung diese Funktionen und meldet sie dem Benutzer, wobei gleichzeitig eine Information zur Unterschrift und zum Unterzeichner angezeigt wird. Der Benutzer kann dann entsprechend seinem Vertrauen zum Programmierer entscheiden, ob diese Funktion ausgeführt werden soll. Der Vorteil dieser Methode besteht darin, dass es unwichtig ist, auf welchem Server sich das Objekt befindet und auf welchem (unsicheren) Wege es zum Benutzer gelangt, da es durch diese Unterschrift vor Veränderung geschützt ist. Die Schwierigkeit für den Leser besteht darin einzuschätzen, welchem Programmierer von Applets er vertrauen kann.

Da Java aber immerhin ein brauchbares Sicherheitskonzept besitzt, ist es trotz aller bekannten Sicherheitslücken nach der persönlichen Meinung des Autors weitaus sicherer als die anderen Formen aktiver Inhalte wie JavaScript oder gar ActiveX ist, die Sie unbedingt beide in Ihrem WWW-Browser deaktivieren sollten!

Nähere Informationen zum Thema *Java Security* sowie Beispiele für Killer-Applets finden Sie unter [4], [3], [2], [1].

JavaScript

Trotz der Namensverwandtschaft hat JavaScript mit Java nicht allzu viel zu tun. JavaScript, entwickelt von der Firma Netscape, ist eine objektbasierte Sprache, die die Einbindung von Programmen in HTML-Dokumente ermöglicht. Der Microsoft Internet Explorer versteht ebenfalls JavaScript, verwendet dafür allerdings den Namen „JScript“.

Im Unterschied zu Java werden JavaScript-Programme als Quelltext (Script) in die HTML-Dokumente eingebunden. Diese Scripte werden nach dem Einlesen des Dokuments vom Browser interpretiert und abgearbeitet. Die Sicherheitsstrategie besteht darin, dass die Sprache keine Elemente enthält, die einen Zugriff auf die lokale Festplatte ermöglichen. Trotzdem sind auch hier Sicherheitslücken aufgetreten. Im Unterschied zu bösartigen Java-Programmen, die potentiell Daten auf den Festplatten des Benutzers verändern können, betreffen die Sicherheitslücken von JavaScript vor allem die Vertraulichkeit der Benutzerdaten, d. h. es können aus dem Internet unbemerkt Informationen über den lokalen Rechner oder über den Nutzer abgerufen werden. Im Juli 1998 wurde ein Fehler in den Browsern von Microsoft und Netscape entdeckt, der bösartigen JavaScript-Programmen auf einer WWW-Seite ermöglicht, selbst nach Verlassen dieser Seite die jetzigen und zukünftigen Surf-Aktivitäten des Besuchers zu protokollieren und an den bösartigen WWW-Server zurückzusenden. Außerdem können auch noch bei den neuesten Browser-

versionen von Netscape und Microsoft beliebige Dateien auf den lokalen Festplatten ausgespäht werden, siehe dazu [5], [6], [7].

Genauso unsicher vor Internetspionen sind Ihre Browser-Präferenzdateien im Netscape Communicator (bis Version 4.04) mit Ihrer E-Mailadresse und eventuell sogar leichsinnigerweise abgespeicherten Passwörtern, beschrieben in:

```
http://www.mygale.org/~nando
```

Genauso gefährlich ist aber, dass auch das Ausfüllen von HTML-Formularen überwacht werden kann. Da dies direkt auf dem lokalen Rechner des Nutzers geschieht, kann dieser Eingriff auch nicht durch einen Firewall-Rechner oder durch Verschlüsselung der Formulardaten während der Datenübertragung verhindert werden. In den neueren Versionen der Browser (Netscape 3.x und 4.x) wurde dieser Fehler beseitigt. Nähere Informationen können Sie ebenfalls unter [1] nachlesen.

ActiveX

ActiveX wurde von der Firma Microsoft entwickelt, um Software über das Internet zu verteilen. Wie *Java Applets* kann ein *ActiveX Control* in eine WWW-Seite eingebunden werden und erscheint dort typischerweise als nette interaktive Grafik. ActiveX wird ausschließlich vom Microsoft Internet Explorer unterstützt.

Im Gegensatz zum plattformunabhängigen Java werden *ActiveX Controls* als ausführbare Binärfiles verteilt und müssen zuvor für jedes Betriebssystem separat compiliert werden. Das Sicherheitsmodell ActiveX unterscheidet sich ebenfalls völlig von Java. Wie bereits beschrieben, erreicht Java Sicherheit durch die Beschränkung von Applets auf einen Satz von sicheren Aktionen. In Ausnahmefällen können digital signierte Java-Applets um die Erlaubnis zu konkreten, eigentlich nicht erlaubten Zusatzaktionen (z. B. Leserecht auf lokalen Platten) bitten. Im Gegensatz dazu sind *ActiveX Controls* in ihren Aktionsmöglichkeiten nicht im geringsten eingeschränkt. Sie sind zwar auch digital signiert, aber der Benutzer wird vor ihrer Ausführung bestenfalls pauschal gewarnt, ohne genau zu erfahren, welche Rechte auf seinem PC sich das *ActiveX Control* nehmen wird. Schreiben Sie sich also vor der Ausführung den Autor des *ActiveX Control* gut auf, damit Sie wissen, wer danach Ihre Festplatte gelöscht oder mit Viren verseucht hat, oder verwenden Sie einfach einen Nicht-Microsoft-Browser! Was mit ActiveX möglich ist, können Sie ausführlich auf den WWW-Seiten des Chaos Computer Clubs nachlesen [9].

Gefährdung der Privatsphäre im WWW

Die meisten WWW-Server protokollieren jeden Zugriff aus aller Welt mit. Die Protokolldateien (Logfiles) enthalten üblicherweise die IP-Adresse und den Rechnernamen, an dem Sie sitzen, die Zeit des Zugriffs, eventuell sogar Ihren Benutzernamen, Name und Größe des angeforderten URL, u. U. auch von Ihnen ausgefüllte Formulardaten (nur bei GET-, nicht bei POST-Methode). Manchmal wird auch der zuletzt betrachtete URL, Ihr Browser und Ihre E-Mail-Adresse notiert.

Wenn Sie einen Proxy-Server verwenden, werden sogar alle URLs, die Sie betrachten, mitprotokolliert. Obwohl die Betreiber der WWW-Server zumindest in Deutschland per Gesetz dazu verpflichtet sind, die Privatsphäre Ihrer Besucher zu respektieren, ist es technisch kein Problem, mit Hilfe von CGI-Scripten Adressen zu sammeln und an Massenmailer weiterzuverkaufen. Wundern Sie sich also nicht, wenn Sie ab und zu Werbemail irgendwelcher Art erhalten; in diesem Fall hat irgend jemand Ihre Mailadresse meist illegal gesammelt und weiterverkauft.

Cookies (siehe [10])

Wohl nichts außer ActiveX Controls verbreitet im Web solchen Schrecken wie Cookies, wenn es um Systemsicherheit und Schutz der Privatsphäre geht. Während die Horror-

geschichten über erstere meistens wahr sind, befinden wir uns bei letzteren oft im Bereich urbaner Legenden.

Zunächst einmal sind Cookies eigentlich keine schlechte Idee, kann man mit ihnen doch einen Mangel von HTTP umschiffen. HTTP ist das Protokoll, durch das sich WWW-Browser und WWW-Server miteinander unterhalten. HTTP hat ein Problem, es ist *stateless*, d. h. jeder Request, den ein Browser einem Server schickt, ist für diesen ein einzigartiges Ereignis, ohne jeden Zusammenhang zu früheren Requests, die vom selben Browser kamen. Bestimmte Dienste benötigen aber Informationen darüber, was ein Browser schon alles vom Server wollte. Dazu gehören sogenannte Einkaufskörbe oder Tutorien, die es dem Benutzer erlauben, dort wieder einzusteigen, wo er aufgehört hatte, oder auch Dienste, die sich der Benutzer nach persönlichen Bedürfnissen selbst anpassen kann wie „My Yahoo“.

Cookies werden vom Server generiert und dem Client als Teil der Antwort auf einen Request mitgeschickt. Der speichert sie dann in einer speziellen Datei. In der dürfen maximal 300 Cookies stehen, jedes bis zu vier Kilobyte groß, wobei nicht mehr als 20 Cookies von einem Server, bzw. einer Domain stammen dürfen. Dies sind die Spezifikationen des Cookie-Erfinders Netscape. Die Implementierung ist dem Browserhersteller überlassen, der sich nicht an diese Zahlen halten muss. Für einen Juristen beginnt hier schon die Frechheit: „Wie kommen Anbieter von WWW-Seiten auf die Idee, sie dürften nach Belieben den Platz auf meiner Festplatte verwenden?“

Bei jedem Request, den der WWW-Browser an einen Server schickt, durchsucht er zuerst die Cookie-Datei nach Cookies, die für diesen Server bestimmt sind und schickt sie dann als Teil des Requests mit. D. h. nicht der Server verlangt die Herausgabe der Cookies, der Browser schickt sie vielmehr freiwillig[2]. Er schickt sie aber nicht an beliebige Server, sondern nur an den, von dem er auch das Cookie bekommen hat. Jedes Cookie hat also einen Gültigkeitsbereich, der spätestens an der Domänengrenze des setzenden Servers endet. Ein Cookie, das von einem Server in der Domain `ku-eichstaett.de` gesetzt wurde, wird also nie an einen Server in der Domain `uni-konstanz.de` geschickt. Ausserdem kann der cookie-generierende Server seinen Cookies auch noch eine Lebenszeit mit auf den Weg geben, nach deren Ablauf sie verfallen. Seltsam, dass so wenige Websites, die mit Cookies arbeiten, diese Möglichkeit auch nutzen ...

Was sind die Gefahren durch Cookies?

Profiling

Der Betreiber einer Website kann anhand von Cookies nachvollziehen, welche seiner Seiten Sie wie lange und in welcher Reihenfolge angesehen haben. Er kann diese Daten für sich nutzen, um auf die Seiten, die Sie ansehen, zur Laufzeit auf Sie maßgeschneiderte Werbung ohne große Streuverluste zu zaubern. Besonders aussagekräftig ist es, wenn verschiedene Netsites sich zu einem Verbund zusammenschließen und ihre Cookies zentral von einer darauf spezialisierten Firma, z.B. der DoubleClick Corporation, verwalten lassen, dann kann auch ein WWW-Server-übergreifendes Benutzerprofil von Ihnen angelegt werden: Z. B. kann man so in Erfahrung bringen, dass Sie sich nicht nur für Persil, sondern auch für Babynahrung und Handfeuerwaffen interessieren. Wenn in Ihrer Cookie-Datei beispielsweise eine Zeile

```
ad.doubleclick.net FALSE / FALSE 942195440 IAA d2bbd5
```

enthalten ist, sind Sie „Kunde“ der DoubleClick Corporation. Wenn Sie darauf aber keinen Wert legen, sollten Sie dann diese Zeile besser per Hand löschen oder die ganze Cookie-Datei entsorgen.

[2] Anm. d. Red.: Dies geschieht ohne Rückfrage und ohne den Anwender zu informieren selbst dann, wenn das Akzeptieren von Cookies zwischenzeitlich ausgeschaltet wurde.

Belästigung durch lästige Werbe-Mails (Spam)

Man kann Cookies auch nutzen, um Ihnen ebenfalls maßgeschneiderte Werbe-E-Mail zu schicken: Sie haben sicher irgendwo in die Einstellungen Ihres Browsers Ihre E-Mail-Adresse eingegeben, ja? Haben Sie auch JavaScript aktiviert? Dann ist es kein Problem, sie mit einem kleinen Script herauszufiltern. Zu guter Letzt kann Ihre Adresse zusammen mit Ihrem Benutzerprofil dann auch noch weiterverkauft werden.

Sensible Informationen

Ein Cookie kann beliebige Informationen enthalten, z. B. Kreditkartennummern (damit Sie nächstes Mal noch einfacher einkaufen können) oder Benutzerkennungen und Passwörter (damit Sie nächstes Mal ohne Anmeldeprozedur in die *Site* kommen). Diese Daten liegen unverschlüsselt auf Ihrer Platte in einem Unterverzeichnis Ihres Browsers, z. B. in

```
C:\Programme\Netscape\Users\Ihr_Name\cookies.txt
```

oder in

```
H:\Netscape\cookies.txt.
```

Des weiteren werden Cookies, sofern keine besonderen Vorkehrungen getroffen werden, unverschlüsselt übertragen, auch bei „Secure Servern“!

Von wegen sicher!

Inzwischen sind Fälle bekannt, in denen es gelungen ist, die gesamte Cookie-Datei zu lesen, also nicht nur den Teil, der „rechtmäßig“ zum Server geschickt wurde. Auch hier war wieder das notorisch unsichere JavaScript beteiligt.

Wie wehren?

Cookies wurden von Netscape mit Version 2 des Browsers eingeführt, und zwar ohne dies groß bekannt zu geben oder zu dokumentieren. Eine Möglichkeit dieses „Feature“ zu deaktivieren fehlte ebenfalls. Die Reaktionen in der Netzgemeinde waren darum heftig, und wie üblich kursierten bald die wildesten Verschwörungstheorien im Netz. Seit Version 3.x und 4.x kann man darum Cookies kontrollieren bzw. ganz abschalten, sehen Sie mal in Ihren Optionen nach. Das gleiche gilt für den Internet Explorer von Microsoft. Wenn Sie möchten, können Sie auch unerwünschte Zeilen in Ihrer Cookie-Datei entfernen oder die ganze Datei komplett löschen.

Näheres über Cookies können Sie [10] und [11] entnehmen.

Empfohlene WWW-Browser-Einstellungen und Verhaltensweisen

Keines der drei Produkte Java, JavaScript und ActiveX bietet absolute Sicherheit vor Missbrauch durch ungebetene Zaungäste aus dem Internet. Während Java an sich ein gutes Sicherheitskonzept besitzt und nur durch Implementierungsfehler im lokalen Java-Interpreter Gefahren für den Benutzer drohen, sind die Sicherheitslöcher von JavaScript, das durch Einschränkungen in seinem Sprachumfang wenigstens etwas geschützt ist, deutlich größer. Bei ActiveX, das unbekannte Zugriffe ohne Einschränkung erlaubt, hat das Sicherheitsloch sogar die Größe eines Scheunentors. Daher möchte Ihnen der Autor folgende Empfehlungen ans Herz legen:

Wer sicherheitsrelevante Daten auf seinem Rechner aufbewahrt, sollte Java mit Vorsicht benutzen und JavaScript und erst recht ActiveX in seinem WWW-Browser deaktivieren. Bei Netscape müssen Sie Bearbeiten → Einstellungen → Erweitert → „Java aktivieren“ ankreuzen sowie „JavaScript aktivieren“ auskreuzen. Beim Internet Explorer ist die Deaktivierung von JavaScript seit Einführung des „Security Zones“-Features, das eigentlich das Internet sicherer machen sollte, schwierig geworden. Wie Sie es trotzdem schaffen, können Sie unter [1] nachlesen. AktiveX vermeiden Sie am besten, indem Sie den Microsoft Internet Explorer deinstallieren, sofern Ihr Betriebssystemhersteller dies erlaubt,

und den Netscape Communicator verwenden, der durch Unkenntnis perfekt vor AktiveX geschützt ist. Notfalls können Sie auch den Microsoft Internet Explorer in der höchsten Sicherheitsstufe benutzen. AktiveX ist dann deaktiviert.

Wer trotzdem JavaScript nutzen muss, sollte immer die neueste Version seines Browsers installieren, damit dann zumindest die älteren Sicherheitslücken beseitigt sind. Dann sollte bei konkretem Bedarf JavaScript aktiviert und baldmöglichst wieder deaktiviert werden.

Jede Warnung oder Meldung Ihres Browsers sollte aufmerksam gelesen werden, bevor sie akzeptiert wird. Installieren Sie nie ohne Virentest „unbedingte Tools“ aus dem WWW!

Wenn Sie Mails im HTML-Format erhalten, können diese genauso wie normale WWW-Seiten Applets, Scripten etc. enthalten. Wenn Sie diese Mails dann mit Ihrem WWW-Browser lesen, gelten die üblichen Risiken und Sicherheitseinstellungen Ihres Browsers!

Deaktivieren Sie Cookies und lassen Sie sie von Fall zu Fall nur kurzzeitig zu!

Abschließend darf der Hinweis auf eine interessante Quelle im WWW nicht fehlen: Unter [12] finden Sie nämlich eine Suchmaschine, die eine Volltextsuche in den Mitteilungen fast aller deutschen Hochsschulrechenzentren ermöglicht. Dort können Sie weitere interessante Artikel zum Thema DV-Sicherheit finden.

Literatur

Dieser Artikel wäre nicht möglich gewesen ohne die folgenden hervorragenden, im WWW zur Verfügung stehenden Quellen:

Security allgemein:
[1] http://www.w3.org/Security/Faq/www-security-faq.html

Java:
[2] http://java.sun.com/sfaq/
[3] http://www.eyeone.no/KillerApp/KillerApp.htm
[4] http://www.hu-berlin.de/inside/rz/rzmit/rzm15/7.html

JavaScript:
[5] http://www.geocities.com/ResearchTriangle/1711/b6.html
[6] http://pages.whowhere.com/computers/cuartangojc/.
[7] http://www.microsoft.com/security/bulletins/ms98-015.asp
[8] http://www.mygale.org/~nando

ActiveX:
[9] http://www.ccc.de/radioactivex.html

Cookies:
[10] http://www.uni-konstanz.de/ZE/RZ/KM/148/148-03.html
[11] http://www.rz.uni-augsburg.de/connect/9801/cookies.html

Volltextsuche in den Mitteilungen der deutschen Hochschulrechenzentren:
[12] http://webmania.rz.hu-berlin.de/Newsletter/

Anmerkung der Reaktion:

Seit der Erstveröffentlichung dieses Artikels sind weitere Fehler in den hier beschriebenen Browsern bekannt geworden. Ständig aktualisierte Informationen dazu sowie weitere Tipps zur Vermeidung von Gefahrenquellen finden Sie in

`http://www.uni-muenster.de/WWW/Sicherheit.html`.

Wir bitten Sie in Ihrem eigenen Interesse, diese Informationen zu beachten sowie sich regelmäßig die von den Herstellern der WWW-Browser herausgegebenen Korrekturen zu besorgen.

RUM-Lehre

Lehrveranstaltungen des ZIV

Veranstaltungen im laufenden Sommersemester

260081	Kommunikation und Information im Internet Mo 13–15 Hörsaal: Raum 107, Einsteinstr. 60	Mertz, K.-B.
260096	Programmieren in Java Mi 10–12 Hörsaal: M4	Sturm, E.
260100	Datenbankprogrammierung mit Delphi Di 15–17 Hörsaal: Raum 107, Einsteinstr. 60	Pudlatz, H.
260115	Statistische Datenanalyse mit dem Programmsystem SPSS Do 11–13 Hörsaal: Raum 107, Einsteinstr. 60	Nienhaus, R.
260120	Einführung in Windows NT Do 14–16 Hörsaal: Raum 206, Röntgenstr. 13	Kamp, M./ Lange, W.
260134	Rechnernetze: Technische Grundlagen Do 10–12 Hörsaal: Raum 206, Röntgenstr. 13	Richter, G./ Schulze, D./ Speer, M./ Wessendorf, G.
260149	Kolloquium des Zentrums für Informationsverarbeitung Fr 13–15	Held, W.

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11–12, Tel. 83-3 15 61

Nähere Angaben über den Inhalt und die Voraussetzungen der folgenden Veranstaltungen werden vor Semesterbeginn vom Zentrum für Informationsverarbeitung bekanntgegeben, siehe die WWW-Seite `http://www.uni-muenster.de/ZIV/Lehre/`.

Veranstaltungen in der vorlesungsfreien Zeit

260013	Programmieren in C [4] vom 30.8. bis 10.9.1999, ganztägig 10 – 12 und 13 – 15 Hörsaal: M4 und Raum 107, Einsteinstr. 60	Hölters, J.
260028	Statistische Datenanalyse mit dem Programmsystem SPSS [4] vom 30.8. bis 10.9.1999, vormittags 9 – 13 Hörsaal: Raum 107, Einsteinstr. 60	Zörkendörfer, S.
260032	Programmieren in Fortran [4] vom 13.9. bis 24.9.1999, vormittags 8 – 12 Hörsaal: Raum 107, Einsteinstr. 60	Reichel, K.
260047	Windows NT Systemadministration [3] [4] für Mitarbeiter in IV-Versorgungseinheiten vom 13.9. bis 24.9.1999, ganztägig 9 – 11 und 13 – 17 Hörsaal M4 und Raum 107, Einsteinstr. 60	Kämmerer, M

[3] Für diese Veranstaltung kann eine Anmeldung von anderen Interessenten erfolgen, sofern noch freie Plätze vorhanden sind.

260051	Programmieren in Java für Fortgeschrittene [4] vom 20.9. bis 1.10.1999, vormittags 10 – 12 Hörsaal: Seminarraum B Institut für Wirtschaftsinformatik	Süselbeck, B.
260066	Kommunikation und Information im Internet [4] vom 27.9. bis 8.10.1999, ganztägig 10 – 12 und 13 – 17 Hörsaal: M4 und Raum 107, Einsteinstr. 60	Perske, R.

Veranstaltungen im Wintersemester 1999/2000

260070	Kommunikation und Information im Internet [4] Mo 13 – 15 Hörsaal: Raum 107, Einsteinstr. 60	Mertz, K.-B.
260085	Publizieren im Internet mit HTML und XML Mi 15 – 17 Hörsaal: M4 und Raum 107, Einsteinstr. 60	Neukäter, B.
260090	Programmieren in Java Mi 9 – 11 Hörsaal: M4	Sturm, E.
260104	Programmieren in Pascal unter Delphi [4] Mi 14 – 16 Hörsaal: Raum 107, Einsteinstr. 60	Pudlatz, H.
260119	Objektorientiertes Programmieren in C++ Di 13 – 15 Hörsaal: M4	Mersch, R.
260123	Programmieren in Perl Mo 13 – 15 Hörsaal: Raum 206, Röntgenstr. 13	Ost, St.
260138	Statistische Datenanalyse mit dem Programmsystem SPSS [4] Mi 11 – 13 Hörsaal: Raum 107, Einsteinstr. 60	Nienhaus, R.
260142	Einführung in Unix Mo 15 – 17 Hörsaal: Raum 206, Röntgenstr. 13	Grote, M.
260157	Einführung in Windows NT Do 14 – 16 Hörsaal: Raum 206, Röntgenstr. 13	Kamp, M./ Lange, W.
260161	Rechnernetze: Technische Grundlagen Do 10 – 12 Hörsaal: Raum 206, Röntgenstr. 13	Richter, G./ Schulze, D./ Speer, M./ Wessendorf, G.
260176	Kolloquium des Zentrums für Informationsverarbeitung Fr 14 – 16 Hörsaal: Raum 206, Röntgenstr. 13	Held, W.

[4] Wegen der Begrenzung der Teilnehmerzahl ist für diese Veranstaltung eine Anmeldung am Service-Schalter des Zentrums für Informationsverarbeitung, Einsteinstraße 60, erforderlich.

Liebe Leserin, lieber Leser,
wenn Sie **infoWWW** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **infoWWW** nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.
Bitte haben Sie Verständnis dafür, dass ein Versand außerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.
Vielen Dank!
Redaktion **infoWWW**

☐ Ich bitte um Aufnahme in den Verteiler.
☐ Bitte streichen Sie mich/den nachfolgenden Bezieher aus dem Verteiler.
☐ Mir reicht ein Hinweis per E-Mail nach dem Erscheinen einer neuen WWW-Ausgabe.
Meine E-Mail-Adresse:

_____

An die
Redaktion **infoWWW**
Zentrum für Informationsverarbeitung
Röntgenstr. 9–13
48149 Münster

☐ Meine Anschrift hat sich geändert.
Alte Anschrift:

_____

_____

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

Außerhalb der Universität:

_____

(Bitte deutlich lesbar in Druckschrift ausfüllen!)
Ich bin damit einverstanden, dass diese Angaben in der **infoWWW**-Leserdatei gespeichert werden (§ 4 DSG NW).

_____ _____

Ort, Datum Unterschrift