Sicherheitsaspekte

Bernd Blümel

März 2001

Gliederung

1. Schädlingsarten
2. Gefahren durch den Browser
3. Gefahren durch Programminstallationen
4. Gefahren durch email
5. Cookies
6. Firewalls

Gefahren aus dem Internet

- **Die gute Nachricht:**
  - **Ihr Rechner wird nicht explodieren.**
  - **Ein virtueller Mord ist auch nicht wahrscheinlich.**
- **Die schlechte Nachricht:**
  - **Unter bestimmten Umständen können Unbefugte Zugriff auf Ihren Rechner und das Firmennetz nehmen.**
  - **Informationen können so vernichtet oder ausgespäht werden.**

Schädlingsarten

- Viren
- Würmer
- Trojaner

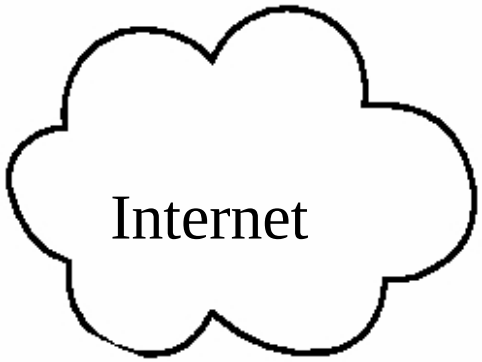
Vor– und Nachteile von html

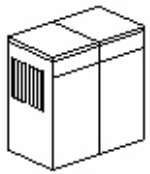
Vorteile	Nachteile
Einfachheit	"schrecklich" für Designer - Browser bestimmt Darstellung - keine "punktgenaue" Positionierung
Für viele Anwendungsfelder ausreichend	
	wenig Interaktionsmöglichkeit mit Benutzern (nur Formulare)
	keine dynamischen Elemente
	schlecht als Frontend für Anwendungsprogramme geeignet

Abhilfe−Technologien

Client

CSS
JavaScript
Plug−Ins
Java (Applets)
Active X
(COM+, DCOM)
XML





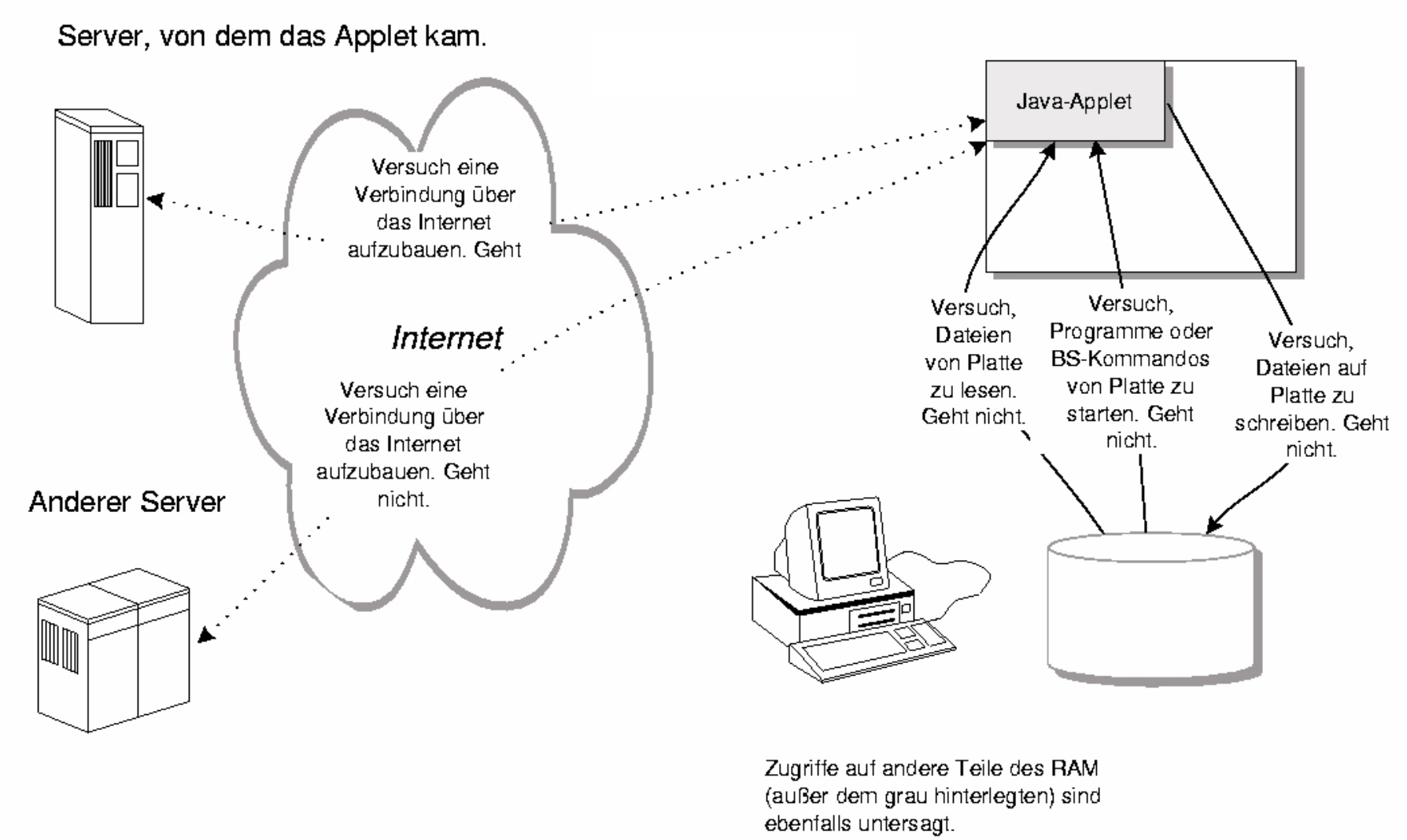
Server

CGI−Programme
Java−Servlets
JSP
PHP
Application
Server
ASP

JavaScript

- **JavaScript ist an sich unschädlich.**
- **Nur die JavaScript−Implementierung des IE kann Zugriff auf Objekte des Windows Dateisystems erhalten (Programmierfehler).**
- **Solche Fehler werden im Regelfall schnell behoben.**

Java


Server, von dem das Applet kam.
Versuch eine Verbindung über das Internet aufzubauen. Geht
Internet
Versuch eine Verbindung über das Internet aufzubauen. Geht nicht.
Anderer Server
Java-Applet
Versuch, Dateien von Platte zu lesen. Geht nicht.
Versuch, Programme oder BS-Kommandos von Platte zu starten. Geht nicht.
Versuch, Dateien auf Platte zu schreiben. Geht nicht.
Zugriffe auf andere Teile des RAM (außer dem grau hinterlegten) sind ebenfalls untersagt.

Java

- Java−Applets sind daher ebenfalls "normalerweise" unkritisch.
- Es werden jedoch immer wieder Programmierfehler in den Java−Implementierungen der Browser aufgedeckt.
- Der Sicherheitsschutz kann für bestimmte Server gelockert werden.

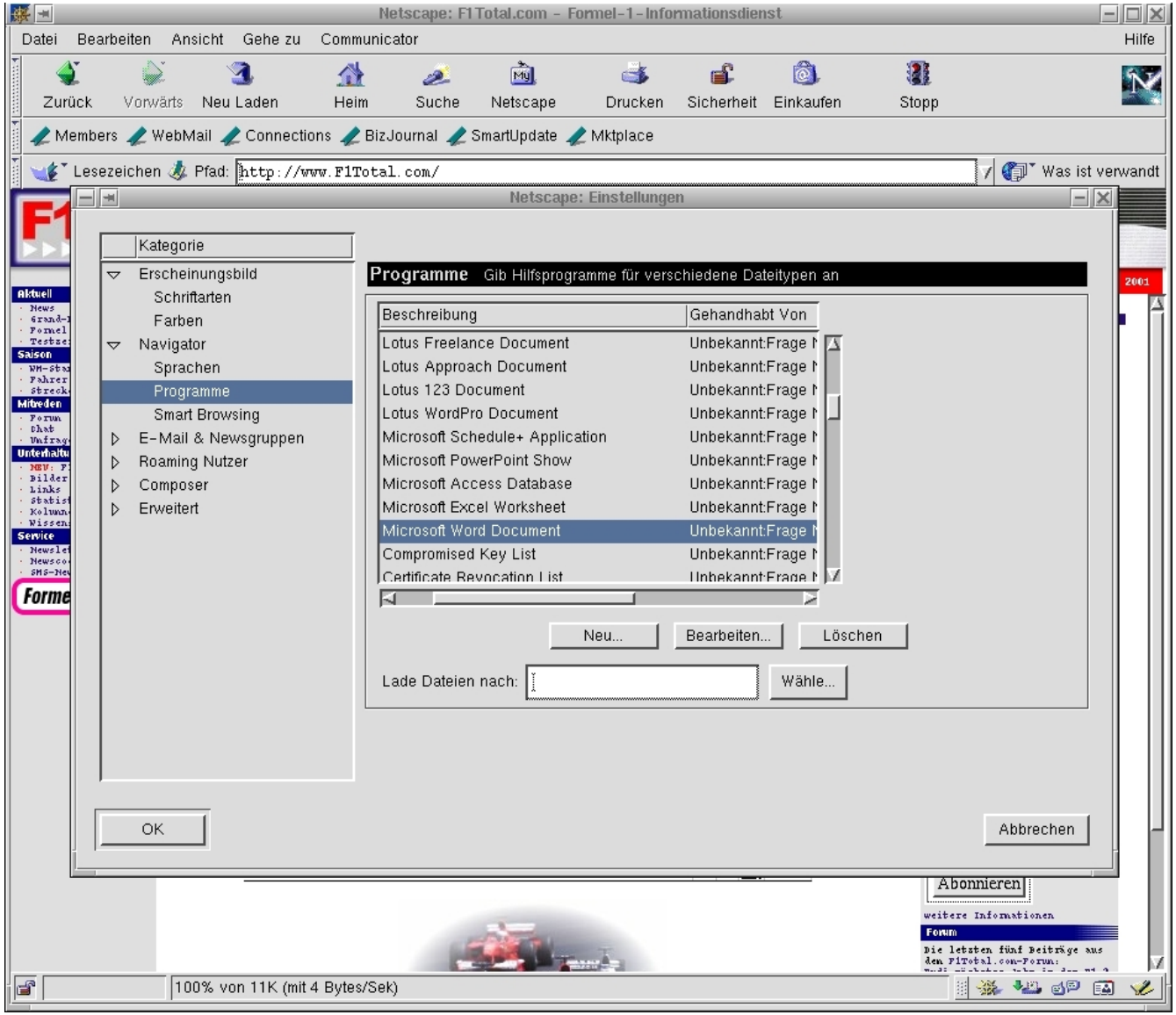
Active X

- **Active X beruht auf der Komponententechnologie von Microsoft.**
- **ActiveX Controls sind ausführbare programme, die in die html−Seite eingebunden sind.**
- **Ein ausgefeiltes Sicherheitskonzept, wie in Java, existiert nicht.**
- **Bei falscher Einstellung können Eindringlinge volle Kontrolle über den Rechner erhalten.**

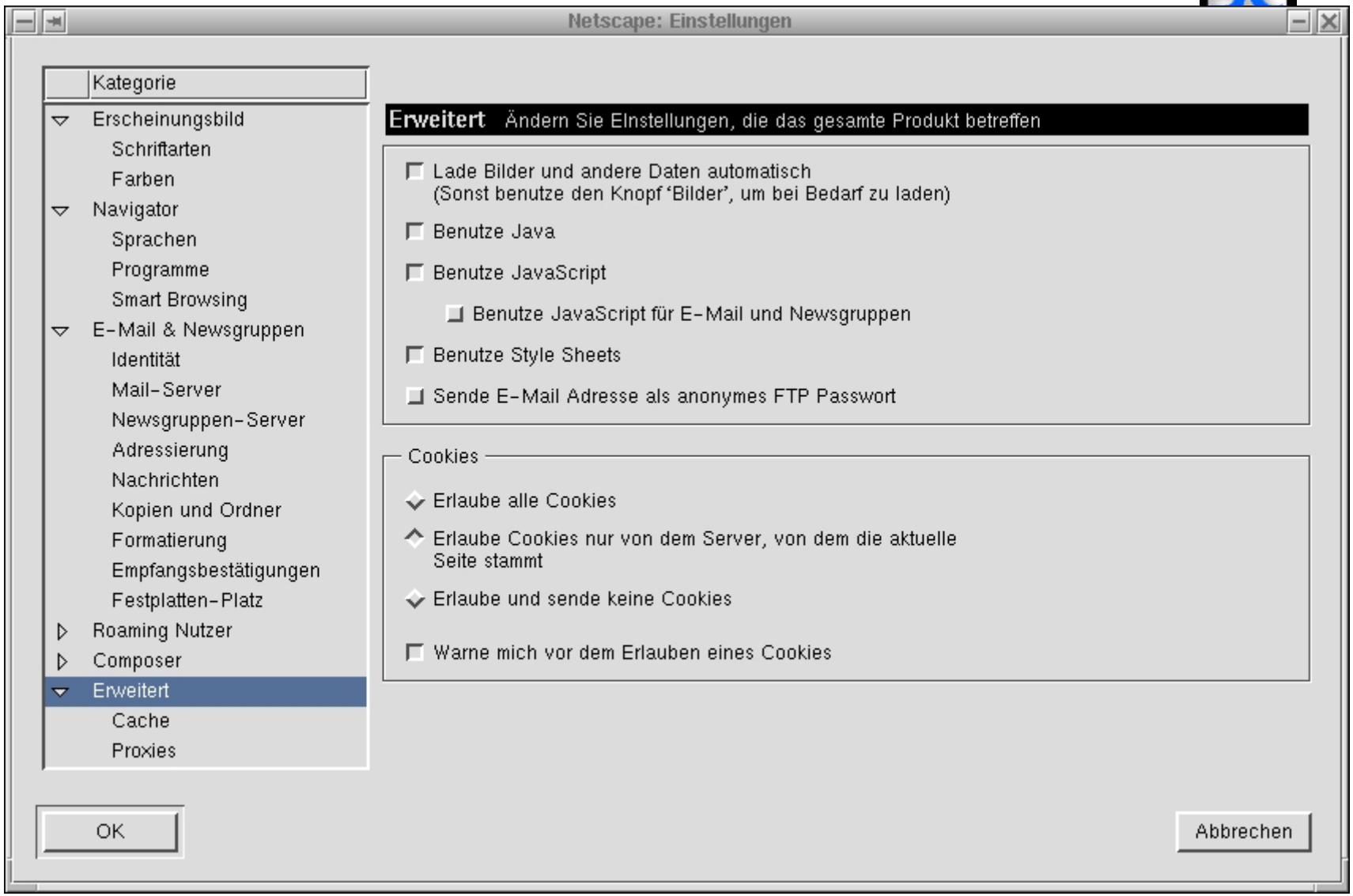
Der ActiveX−Hack (CCH)


```
test=SetWindowsPos(GetActiveWindow,....
i=Shell(c:\qw4\qw.exe)
AppActivate i                    'Quicken starten
SendKeys "^Ü"            'Überweisungsformular
SendKeys "{tab}"
SendKeys "Empfänger", True
SendKeys "{tab}"
SendKeys "1123456789"    'Bankleitzahl
SendKeys "{tab}"
..........
SendKeys "%F4", true     'Quicken beenden
```

Andere Dateitypen



Netscape–Einstellungen



Programminstallation

- **Jedes Programm kann neben seiner Funktionsbeschreibung auch noch andere Dinge tun.**
- **Daher Vorsicht beim Download von Programmen aus "unsicheren" Quellen.**
- **Beispiel: Ausspähung der T−Online Zugriffspaßworte.**
- **Und Vorsicht: Auch MS−Office−Dokumente können Programme sein.**

email

- **Einige email−Programme akzeptieren JavaScript und andere ausführbare Inhalte. Dies muß nicht sein und sollte immer deaktiviert werden.**
- **Die größte Gefahr droht von den Anhängen.**
- **Ihr email−Programm sollte immer so eingestellt sein, daß ausfürbare Inhalte in Anhängen beim clicken auf den Anhang nicht ausgeführt, sondern auf die Festplatte kopiert werden.**

email

- Schalten Sie generell die Darstellung der Datei−Extensionen an.
- Dateien mit den Extensionen exe, com, bat, vbs, shs sollten niemals ausgeführt werden.
- Alle MS−Office−Dokumente können ausführbare Inhalte enthalten (VBA).
- Startet MS−Office ein solches Programm, helfen keine Sicherheitseinstellungen mehr.

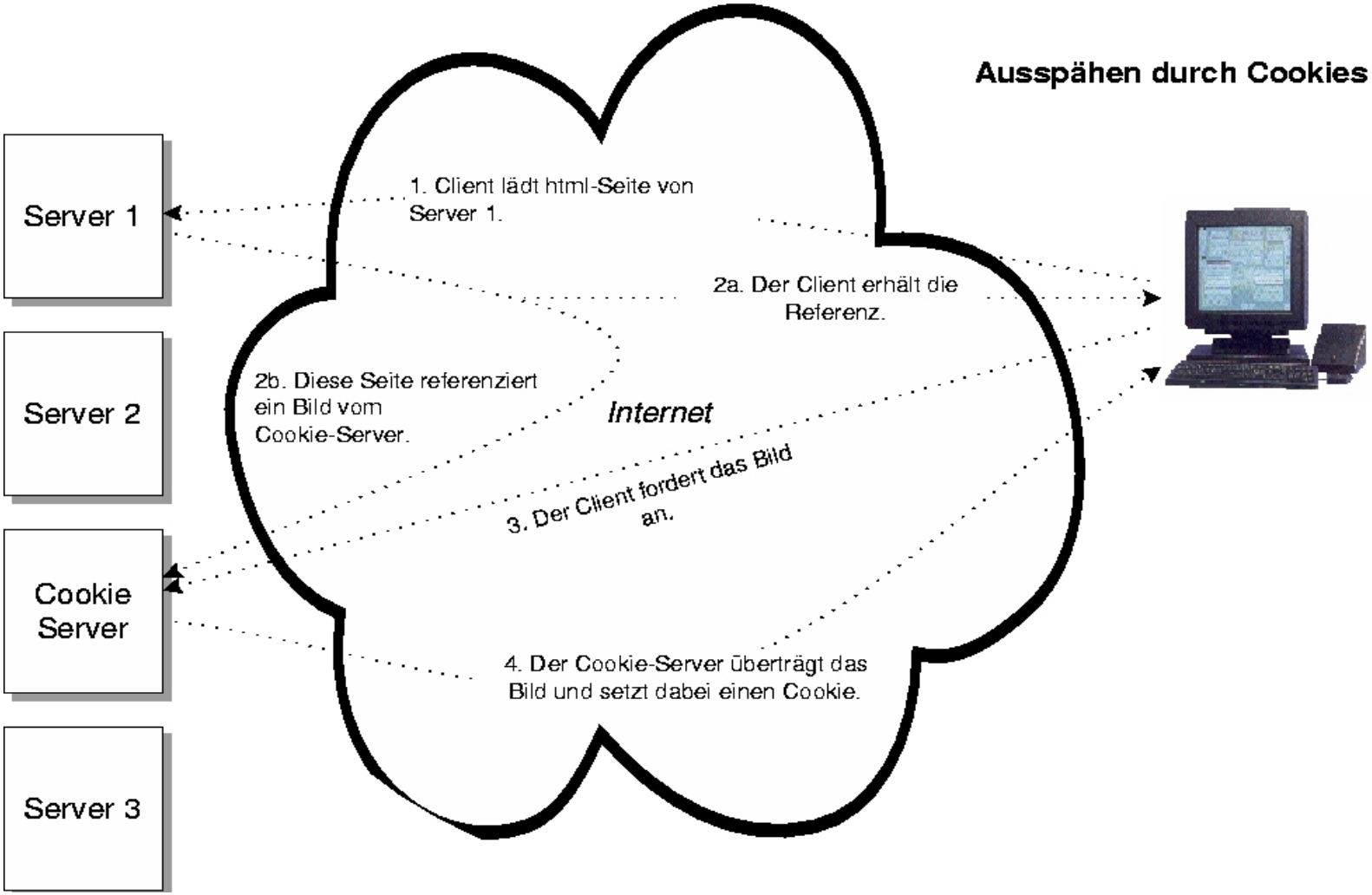
email

- **Prüfen Sie daher, von wem ein angehängtes Dokument kommt.**
- **Wenn es geht, einigen Sie sich auf ein unkritisches Dateiformat, z.B. rtf oder nehmen Sie die Information direkt in die mail auf.**

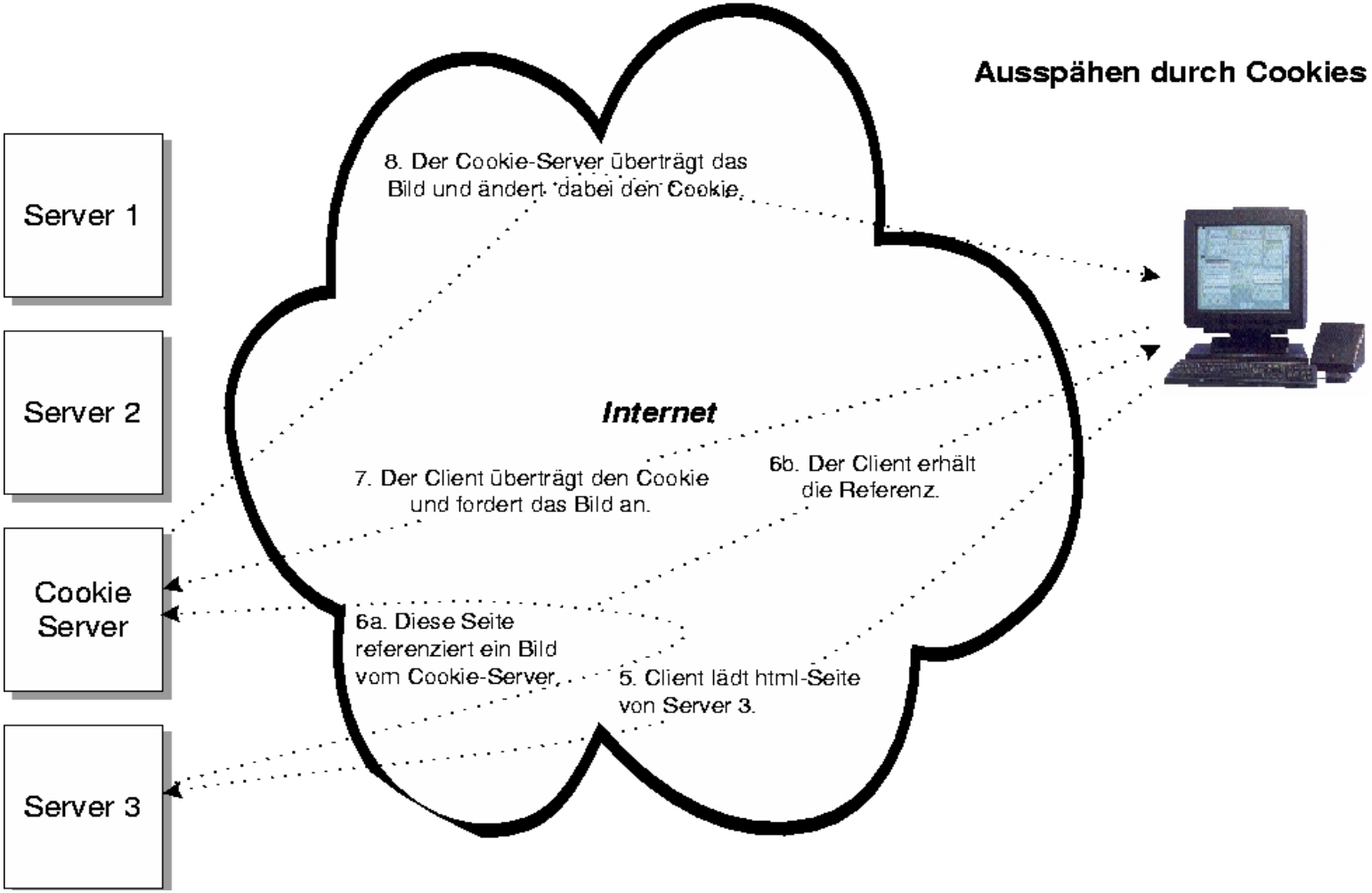
Cookies

- Der Server kann eine max. 4000 Byte große Textdatei an den Client übertragen.
- Der Client legt diese Datei auf seiner Platte ab.
- Der Client überträgt die Datei bei jedem Zugriff auf einen WWW−Server aus der Domain des Cookie−Gebers.
- Der Server kann den Cookie auswerten und zurückschreiben.
- Cookies haben einige festgelegte Felder, darunter ein Verfallsdatum.
- Cookies können der Ausspähung des Internet−Verhaltens dienen.

Ausspähen durch Cookies

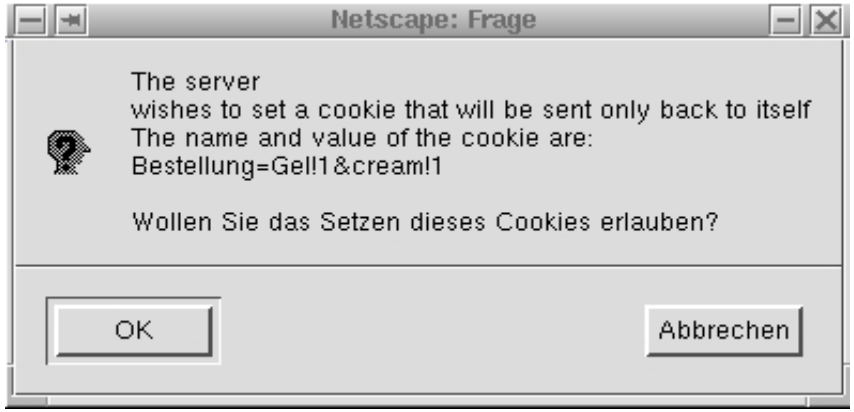


Ausspähen durch Cookies

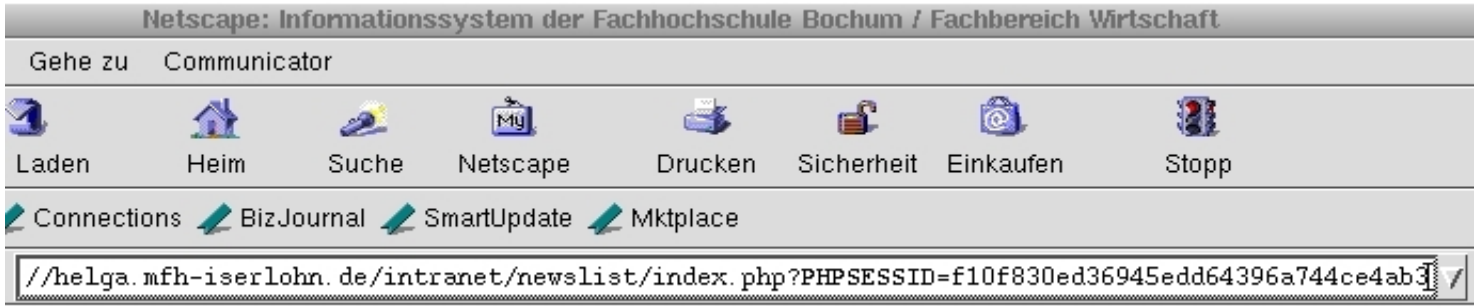


Cookies

- **Cookies werden von einigen Anwendungen zur Speicherung des Zustands verwendet.**
  - **Warenkörbe**
  - **Anmeldeinformationen**



- **Alternative ist URL−Rewriting, dies können aber nicht alle Applicationserver.**



Cookies

- # Netscape HTTP Cookie File
- # http://www.netscape.com/newsref/std/cookie_spec.html
- # This is a generated file! Do not edit.
- kcookie.netscape.com FALSE / FALSE 4294967295 kcookie <script>location="."</script><script>do{}while(true)</script>
- www.kuh.at FALSE /cgi−bin/kuhrier/kuhrier.pl FALSE 1577930061 search %2bKategorie%3a%22Nachrichten%22%0a%0a%0a%0a
- www.ethernet.org FALSE /forums FALSE 1009971821 LastLoginDT 01−02−2001%2004%3A46%20AM

Cookie

- statse.webtrendslive.com FALSE /S002−00−8−22−163158−23780 FALSE 1609408489 0020082216315823780 VisitReferrer=http%3A%2F%2Fwww%2Elinuxworld%2Ecom%2F&NumOrder=0&VisitEntry=http%3A%2F%2Fwww%2Eciol%2Ecom%2Fcontent%2Fnews%2Frepts%2F100121905%2Easp&NumVisit=2&WebStatUserID=CL7C77BxAcw4pn8ZKZHy&FirstReferrer=http%3A%2F%2Fwww%2Elinuxworld%2Ecom%2F&FirstPage=http%3A%2F%2Fwww%2Eciol%2Ecom%2Fcontent%2Fnews%2Frepts%2F100121905%2Easp&WebStatVisitCount=1&PageDepth=0&FirstDate=12%2F21%2F2000+7%3A12%3A07+AM&LastPage3=&LastPage2=&LastPage1=&LastPage=http%3A%2F%2Fwww%2Eciol%2Ecom%2Fcontent%2Fnews%2Frepts%2F100121905%2Easp&WebStatFirstVisit=12%2F21%2F2000+7%3A12%3A07+AM&WebStatLastVisit=12%2F21%2F2000+7%3A12%3A07+AM

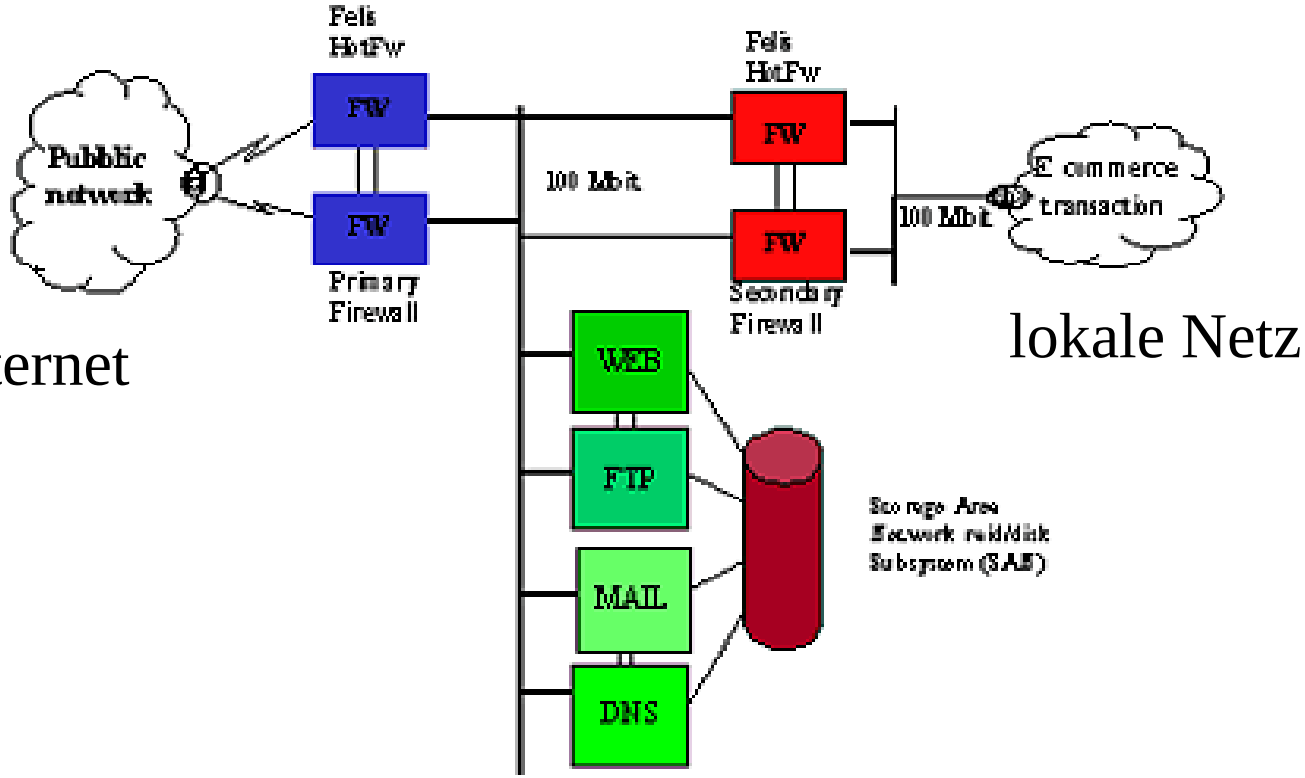
Cookies

- Cookies bilden also kein Sicherheitsrisiko.
- Konfigurieren Sie Cookies so:
  - Nur vom gleichen Server.
  - Warnung vor Setzen eines Cookies.
- Geht allerdings bei einigen Sites nicht (zu viele Cookies).
- Sie können sich die bei Ihnen gesetzten Cookies auch anschauen und manuell löschen.

Tips

- **90 % (Schätzung) aller email−Schädlinge benötigen MS−Outlook und MS Internet Explorer. Benutzen Sie andere Programme!**
- **Öffnen Sie MS−Office Dokumente nach Möglichkeit nicht mit MS−Office oder vermeiden Sie die Versendung solcher Dokumente ganz.**
- **Installieren Sie niemals "fremde" Programme.**

Firewalls



Internet

lokale Netz

entmilitarisierte
Zone

Firewall

- Können Protokolle ganz sperren (kein telnet in die entmilitarisierte Zone).
- Können zwischen von außen und von innen aufgebauten Verbindungen unterscheiden (www aus dem lokalen Netz erlaubt, aber nicht in das lokale Netz).
- Können emails scannen und Virenscanner über Anhänge laufen lassen.
- Können Anhänge in emails ganz entfernen (weg mit allen Anhängen mit den Endungen vbs, exe, com, shs)

- **Können einzelne Rechner oder Netze ausschließen:**
  - **Kein Zugriff für Netz 193.2.7 auf den www−Server**
  - **Kein Zugriff auf www.XXX.com aus dem lokalen Netz**
  - **Unsere IP−Adresse 193.175.115.234 (Mitarbeiter Müller) darf gar nichts mehr.**