

Gefahren in einer vernetzten Welt

- Verbreitung eines Virus im Internet

QuickTime™ and a
GIF decompressor
are needed to see this picture.

- Über die gleichen Netzwerke....
 - werden auch Ihre Mails transferiert
 - holt sich Ihr Browser seine Daten

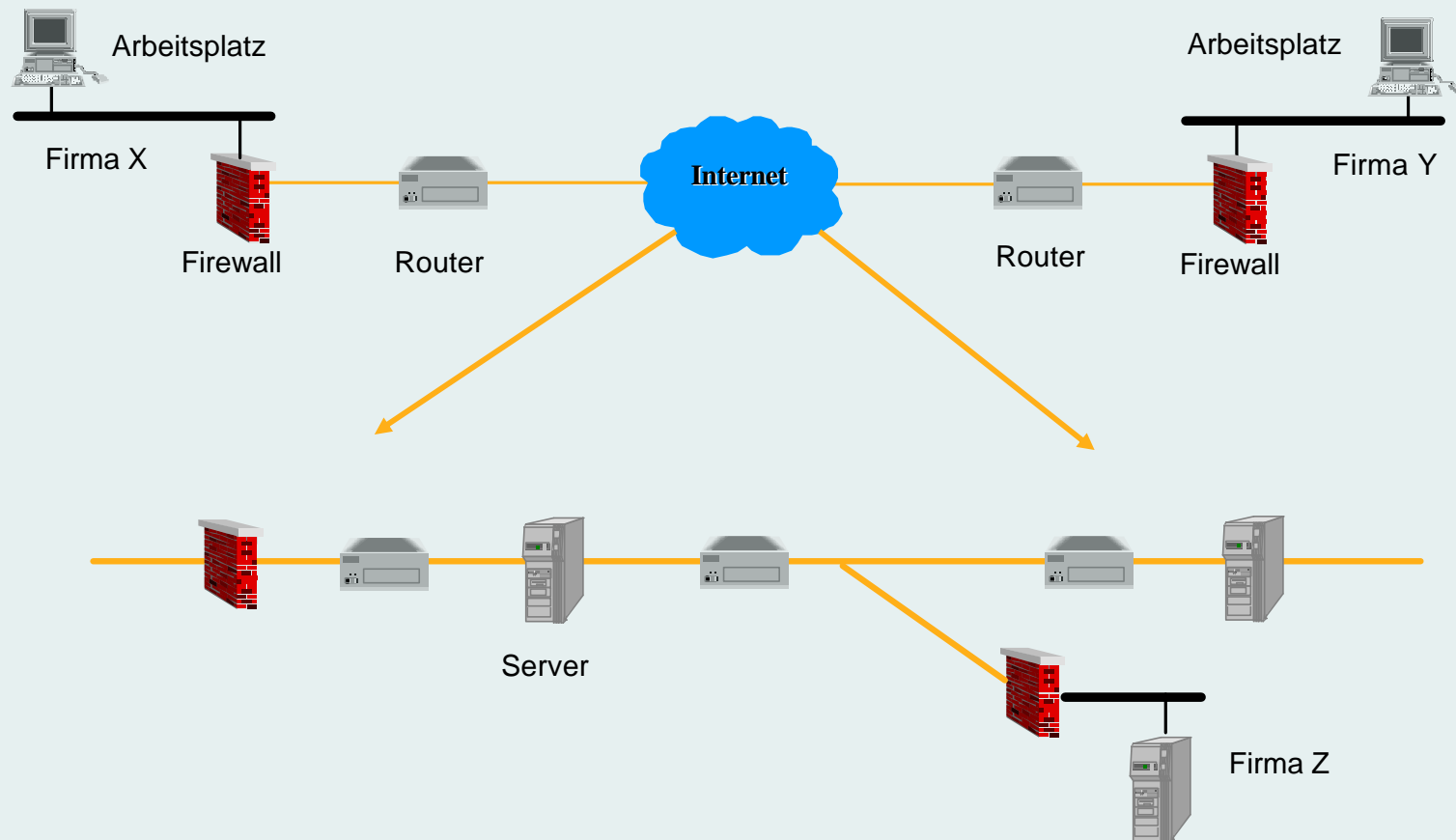
Was sind überhaupt „Spuren im Internet“ Begriffe

- Das Internet:
 - eine Ansammlung von “intelligenten” Geräten zur Verteilung von Daten
 - Diese Geräte sind alle miteinander verbunden
 - Sie werden von Organisationen kontrolliert und gewartet
 - Ihr vernetzter Arbeitsplatz ist ein Teil davon

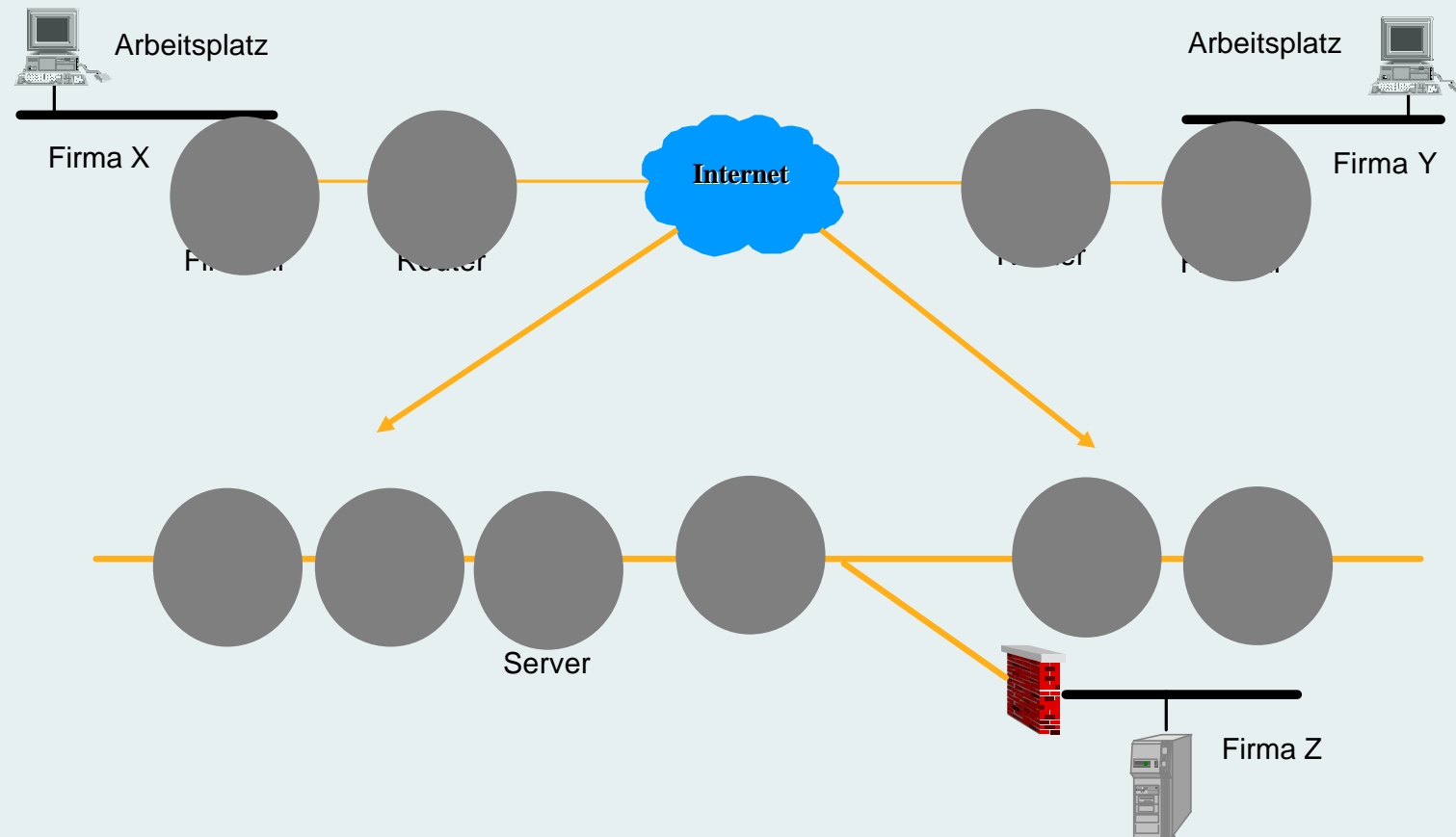
- “Geräte” sind
 - Router: Verkehrsleitsysteme
 - Firewalls: Verkehrspolizisten
 - Server: Anbieter von Diensten (Mail, WWW, andere)
 - Server: Zwischenspeicherung von Daten

- “Spuren im Sand”
 - Auf jedem dieser Geräte hinterlassen Sie Ihre Spuren
 - Protokolldateien
 - Temporäre Daten
 - Lagerung von Daten (Archivierung, Backup)
 -

Was sind überhaupt „Spuren im Internet“



Was sind überhaupt „Spuren im Internet“



Wie und wann hinterlasse ich Spuren

Der Weg einer Email

➤ Information im Header der Emails

```
Received: (from smapd@localhost) by terreactive.ch (8.11.5/8.11.5)
id g0EDvVJ20320 for <hofmann@terreActive.ch>;
Received: from host1.terreActive.ch(xxx.yyy.0.1) by tac via smap (V2.1)
Received: from host1.firma2.ch ([aaa.bbb.197.12]) by host2.terreactive.ch
via smtpd (for mailhost.terreactive.ch [172.23.1.1]) with SMTP;
Received: from outmailer1.firma2.com ([aaa.bbb.3.48]) by host1.firma2.ch
Via smtpd (for gate.terreactive.ch [xxx.yyy.202.121]) with SMTP;
Received: from qrd2172 (aaa.bbb.145.13) by pse3777.firma2.ch (MX V5.2 AnHp)
With SMTP for <hofmann@terreActive.ch>;
Received: from aaa.bbb.136,128 by qrd2172 (InterScan E-Mail VirusWall NT);
X-MimeOLE: Produced By Microsoft Exchange V6.0.5762.3
Message-ID: <8E249C7AF8BDD3119DD60000F807E9A00412AF39@twii204.firma1.ch>
From: <WG@firma2.com>
To: <hofmann@terreActive.ch>
```

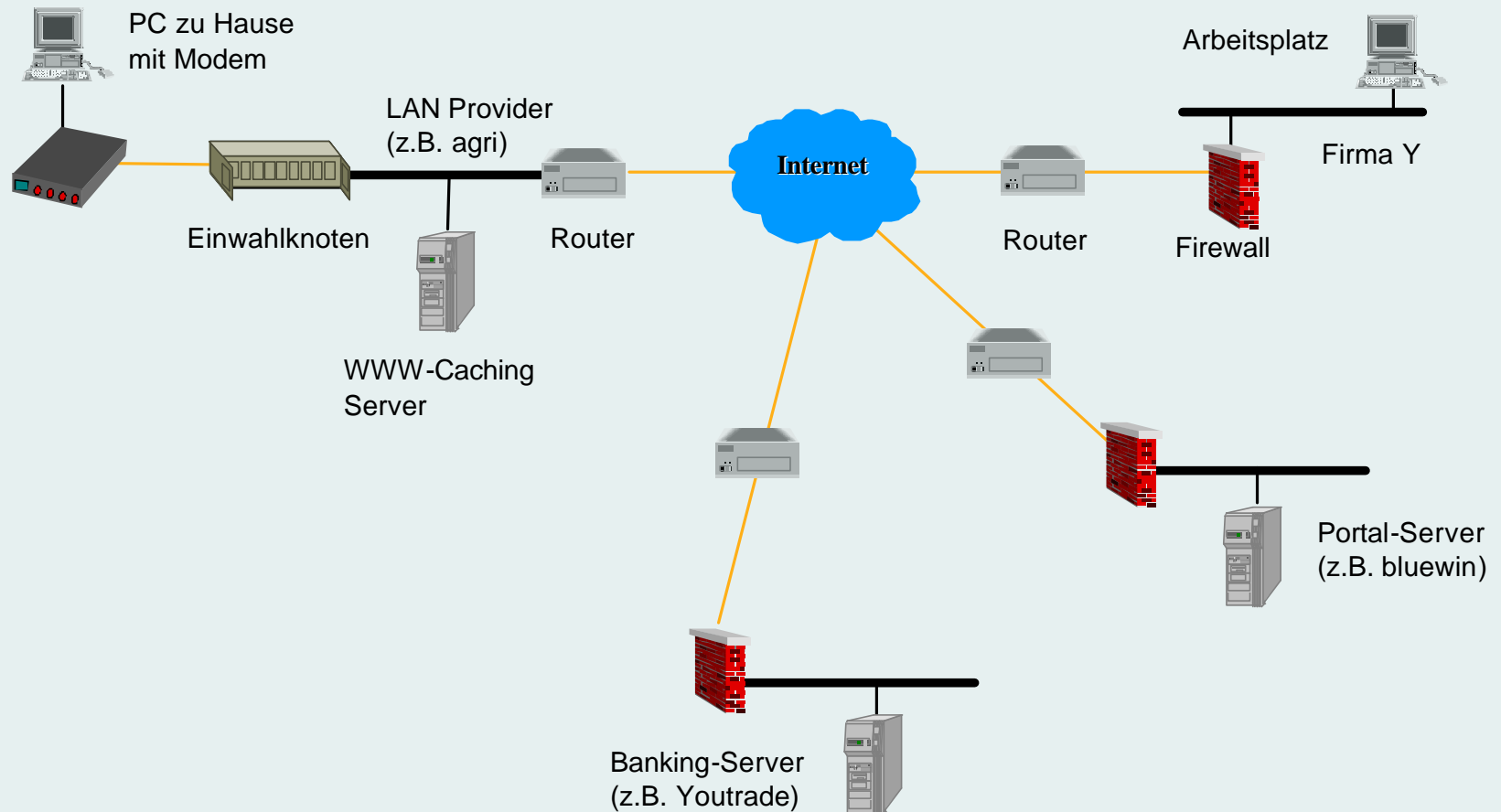
➤ Angriffspunkte und Spuren

- Systemverwalter der Server haben Zugriff
- Server wird gehackt (Hotmail, Yahoo, Bluewin,...)
- Mails werden zwischengespeichert
- Einträge in Protokolldateien auf JEDER Maschine

➤ Emails mit sensitivem Inhalt verschlüsseln (Steganos, PGP, ...)

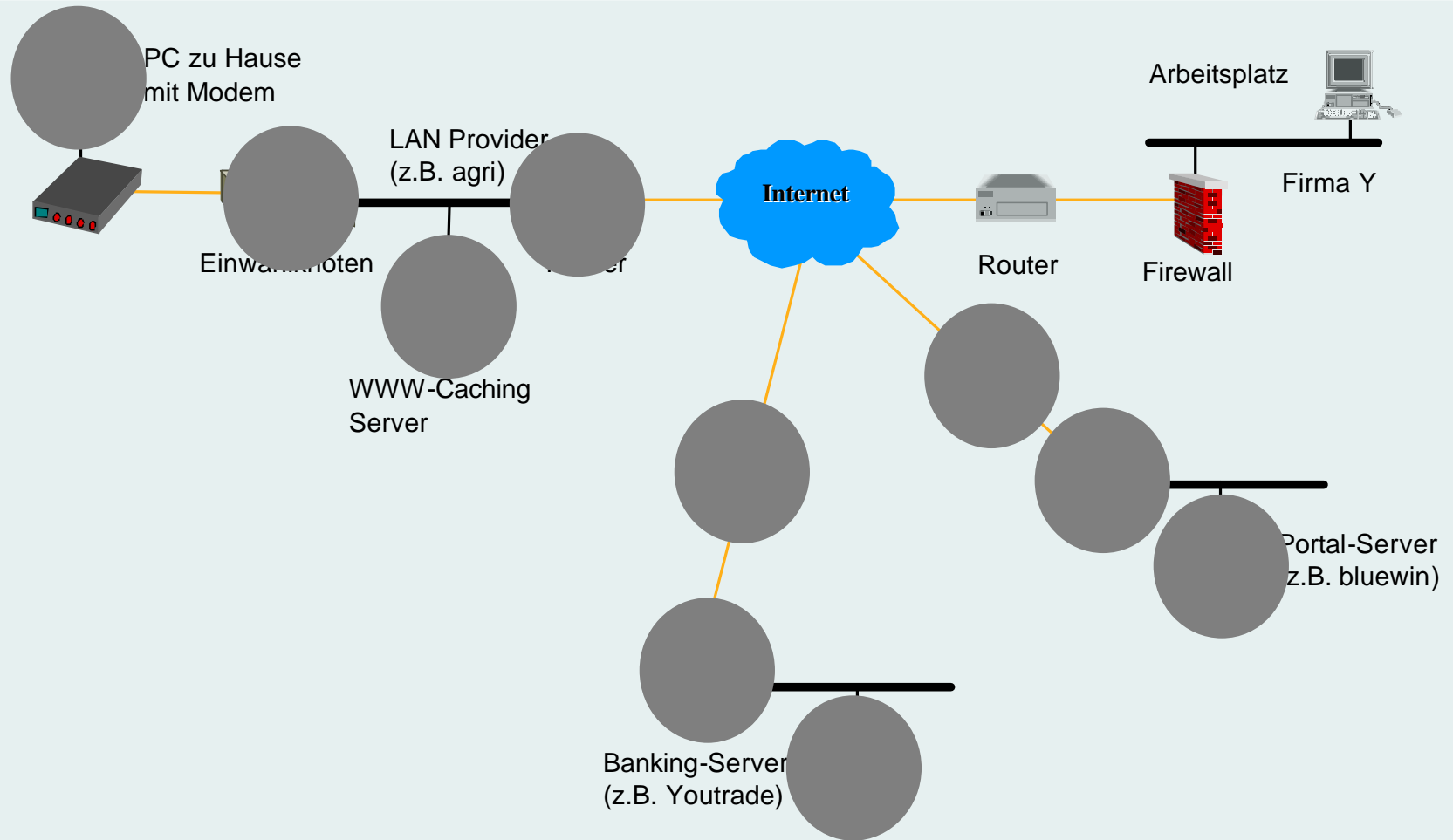
Wie und wann hinterlasse ich Spuren

Surfen im Internet vom Heim PC aus



Wie und wann hinterlasse ich Spuren

Surfen im Internet vom Heim PC aus



Wie und wann hinterlasse ich Spuren Surfen im Internet vom Heim PC aus

- Wo werden welche Informationen gespeichert
 - Einwahl beim Provider via Modem
 - Zeit, Name, Passwort, Internetadresse (IP)
 - Lokaler Browser (IE, Netscape)
 - Besuchte Seiten
 - Cookies
 - WWW-Caching Server (Zwischenspeichern von Webseiten)
 - IP, Zeit, besuchte Seiten
 - Router im Internet
 - Nur IP Adressen und Protokolle, Uhrzeit
 - Firewall beim Provider
 - Zeit, IP Adressen, besuchte Seiten
 - Server beim Provider
 - Zeit, IP Adressen, besuchte Seiten, vorher besuchte Seiten
 - Ad-Server (Bannerwerbung)
 - Zeit, IP Adressen, besuchte Seiten, vorher besuchte Seiten
- Zusätzlich beim Surfen auf Shops oder beim e-Banking
 - Persönliche Daten
 - Transaktionsinformationen
 - CC, Zahlungen, Börsengeschäfte
 - Andere an der Transaktion Beteiligte
 - Z.B. Payment Server, Lieferfirma

Wie holt der Anbieter Informationen über mich typische Portalseite

The screenshot shows a typical portal page with several banners. A red circle highlights a banner for 'IEK-Konferenz: 87 Seminare' (February 2002, Messe Zürich). Another red circle highlights a 'Sprüngli' macaron advertisement with the text 'Luxemburgerli vom Sprüngli' and 'Es ist so einfach etwas Freude zu schenken'. Blue arrows point from these banners to a computer icon on the right, indicating that these banners are loaded from an external server. A third red circle highlights the quote 'Es ist so einfach etwas Freude zu schenken' from the Sprüngli ad, with an arrow pointing to the computer icon.

○ Diese Werbebanner werden von einem externen Server geholt

➔ Meist speichern diese externen Server "Cookies" auf Ihrem PC

Cookies bleiben auf Ihrem PC gespeichert, auch wenn Sie diesen ausschalten

Wie holt der Anbieter Informationen über mich Cookies, Banner und Webbugs

- Cookies
 - Auf Ihrem PC gespeicherte Informationen
- Banner
 - Werbeeinblendungen auf den Webseiten, welche von einem anderen Anbieter geholt werden (z.B. Double Click)
- Webbugs
 - Sehr kleine, unsichtbare Bilder, welche von einem anderen Server geholt werden
- Erstellung von Profilen
 - Die Kombination von Cookies, Bannern und Webbugs erlaubt die Erstellung von Profilen, und damit personalisierter Werbung, aus den Informationen in den Protokolldateien
- Kombination mit externen Datenbanken
 - Z.B. Telefonverzeichnisse, Inkassodaten, Kreditkartenfirmen, ...
 - Zuordnung von Personen zu Surferprofilen --> Identifikation
- Big Brother is watching you!

Wie kann ich mich schützen

Tips und weiterführende Informationen

- **Browsereinstellungen anpassen:**
 - Höchste Sicherheit aktivieren
 - Active X und Java deaktivieren
 - Javascript, VBScript, JScript deaktivieren
 - Cookies nicht akzeptieren, oder nur nach Rückfrage
- Mit diesen Einstellung können Sie das Internet faktisch nicht nutzen
- Installation einer „Personal Firewall“
 - Verschiedene Produkte erhältlich, oft kombiniert mit Virens Scanner
- Wichtige Daten auf der Festplatte und Mails verschlüsseln

- **Webseiten zum Testen der vorgestellten Datenspuren**
 - <http://privacy.net/analyze/>
 - <http://www.hirnbrowser.de/ac/index.html>
 - http://www.lfd.niedersachsen.de/service/service_selbstt.html
 - <http://152.96.120.35/>
 - <http://www.datenschutz.ch/inhalt.htm>
 - <http://www.inf.tu-dresden.de/~hf2/anon/demonstrations.html>

Wie kann ich mich schützen

Tips und weiterführende Informationen

- Linksammlung
 - http://anon.inf.tu-dresden.de/ie6_privacy.html
Informationen zu Cookies, IE 6.0, Konfiguration
 - <http://anon.inf.tu-dresden.de/index.html>
JAP: Anonymisieren von Zugriffen aufs Internet
 - <http://defaced.alldas.de/>
Anzahl gehackte und „alldas.de“ gemeldete Webseiten pro TAG
 - http://www.cert.org/stats/cert_stats.html
Statistiken ueber Angriffszunahme
 - www.grc.com
Analyse einer Attacke (sehr technisch)
 - http://www.lanline.de/aktuelle-ausgabe/01_2002/lan_0102_024.html
Neue Bedrohungen mit Drahtlosen Netzwerken
 - <http://www.cert.org/>
Homepage des „Computer Emergency Response Teams“
 - <http://www.securityfocus.com/>
Sicherheits Portalseite