



© kann Schmidt / PIXELIO

Januar 2009

## Schattenseiten des Internet

Praktische Tipps zur Vermeidung von Gefahren

M. Bezold-Chatwin, Dr. E. Bötsch, V. Kokkas  
[www.lrz.de/services/security/](http://www.lrz.de/services/security/)



LRZ

2

## Grundlagen der Datenkommunikation

## DNS-Namen



3

- Beispiele: `www.heise.de`, `www.lrz.de`
- Der Name wird von rechts nach links spezifischer:

`www. lrz. de`

- Top-Level-Domain; meist Länder-Kennzeichen
- Domain
- Rechner

- Mensch: » Den Namen kann ich mir (einigermaßen) gut merken. «
- Rechner: » Zur Adressierung untauglich. «

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## IP-Adresse (Internet-Protocol-Address) + Port ①



4

- Paar `< IP-Adresse, Port >`:  
Basis für die Adressierung von Diensten
- IP-Adresse wird i.a. als Tupel von 4 Zahlen dargestellt.  
Beispiel: `129.187.254.92`
- Wird von links nach rechts spezifischer:

`129.187. 254. 92`

- IP-Netz
- IP-Sub-Netz (optional)
- Rechner

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## IP-Adresse + Port ②



5

- Wahl des Port:
  - Indirekt: http://... → 80, https://... → 443, FTP → 20 + 21, E-Mail (SMTP) → 25
  - Explizit: http://xyz.de:8080/... → 8080
- Analogie:
  - IP-Netz           ▶ Kennzahl einer (Groß-)Stadt
  - IP-Sub-Netz      ▶ Kennzahl eines Stadtviertels innerhalb einer Stadt
  - IP-Adresse       ▶ Kennzahl eines Hauses innerhalb eines Stadtviertels
  - Port               ▶ Nummer einer Wohnung innerhalb eines Hauses

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Domain-Name-System (DNS)



6

- Namens-Dienst: „Internet-Telefonbuch“
- Hauptanwendung sind folgende Abbildungen:
  - DNS-Name       → IP-Adresse
  - IP-Adresse      → DNS-Name
  - Domain-Name   → Zuständiger Mail-Server
- Sicherheitsproblem: E-Schädlinge können ...
  - DNS manipulieren → DNS liefert falsche Daten.
  - DNS umgehen     → DNS wird gar nicht erst gefragt.
  - „www.meine-bank.de“  
führt zu einer Web-Seite von Verbrechern.
  - Selbst Bookmarks sind nicht immer sicher.

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Internet-Sicherheit: Allgemeines



7

- Datenpakete durchlaufen auf dem Weg zum Ziel mehrere bis viele Zwischenstationen.
- Zwischenstationen weder bekannt noch unter eigener Kontrolle
- Keine *automatische* Verschlüsselung usw. (besser bei IPng)
- > 800 Mio. Rechner angeschlossen
- > 1 Mrd. Benutzer, d.h. 1 Mio. „Bad-Guys“ bei 1 ‰ Anteil
  - Münchner Wissenschaftsnetz:  
ca. 120 000 Benutzer, d.h. 120 „Bad-Guys“ bei 1 ‰ Anteil

⇒ **Das Internet ist unsicher !!!**

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## (Un-)Sicherheit von E-Mail ①



8

### Inhärente Probleme:

- E-Mail wird nicht verschlüsselt.
- Unsignierte E-Mail kann beliebig leicht gefälscht werden.
- Bei Fehlern (z.B. auch falsche Adresse !) erhält der Postmaster eine Fehlermeldung, die in seltenen Fällen die komplette E-Mail enthält (nicht nur die Header).
- E-Mail liegt auf *jedem* beteiligten Rechner *als Ganzes* vor.
- Nicht legitim:  
Besonderer Anreiz, fremde E-Mails zu lesen.

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## (Un-)Sicherheit von E-Mail ②



9

## E-Mail ist noch unsicherer als das sowieso schon unsichere Internet !!!

- ⇒ Rechnen Sie damit,  
dass Ihre E-Mail im schlimmsten Fall einer Postkarte entspricht, die am schwarzen Brett hängt !
- ⇒ **Verschlüsselung** bei *sensiblen* Inhalt *unverzichtbar* !  
Alternative: „Kryptischer“ Inhalt,  
den nur der *legitime* Empfänger versteht.
- ⇒ **Digitale Unterschrift** notwendig, falls Authentizität  
und/oder Verbindlichkeit erforderlich !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Gefahrenquelle „WLAN“



10

- heise Security, Meldung vom 2.1.2007 12:06:  
» Schwarz-Surfer bringt unbescholtenen  
Internetnutzer in Verdacht «
- Studie zum Schutz der WLANs im Jahr 2006:
  - 22 % **vollkommen unverschlüsselt !**
  - ca. 60 % durch WEP geschützt
  - 17 % durch WPA oder WPA-2 geschützt
- **Frei verfügbare Tools** zum
  - Abhören von WLANs
  - Knacken von WEP in weniger als einer Minute

ca. 82 % ungeschützt !
---------------------------

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Gefahrenquelle „WLAN“ – Konsequenzen für die Nutzung



11

- Privater Access-Point
  - Verschlüsselung mit WPA oder WPA-2
- Access-Point in der Firma
  - Verschlüsselung mit WPA oder WPA-2
  - Alternative: Gleichwertige Schutzmaßnahmen
- Öffentlicher Access-Point (Hot-Spot, Internet-Caffe usw.)
  - Prinzipiell ungeschützt !
  - Verschlüsselung des sensitiven Datenverkehrs, z.B.
    - VPN zur Kommunikation mit der Firma
    - SSL bei E-Mail
    - ...

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Wo geraten sensitive / wertvolle Daten in falsche Hände?



12

- ~~■ Auf dem Übertragungsweg  
im Internet → Abhören~~
- Direkt beim Menschen → Phishing
  - Im eigenen Rechner → Trojaner, Key-Logger
  - WLAN → Abhören
  - In einem Server-Rechner des Web-Shops, Info-Portals, ... → Einbruch und Diebstahl der dort gesammelten Daten

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



13

## Schutz der Privatsphäre



## Daten über mich

### – Wie kommen sie ins Internet? ①



14


- Durch mich selbst ...
  - bewusst:
    - Private Web-Seite
    - Soziale Netzwerke, Gästebücher, Kommentare, ...
    - Web-Seite der Schule, Universität, Firma, ...
    - ...
  - unbewusst:
    - E-Mail an einen Verteiler, zu dem es ein Web-Archiv gibt.
    - ...
- Durch Freunde, Bekannte
- Durch die Schule, Universität, den Arbeitgeber, ...

😊 (bis ☹)


Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Daten über mich

### – Wie kommen sie ins Internet? ②



15



- Namens-Verwechslung
- „Witzbold“
- Verlassener Partner ...
- Stalker
- Mobbing
- Identitäts-Dieb
- Wurm, der eine E-Mail fälscht und an einen Verteiler schickt, zu dem es ein Web-Archiv gibt.
- ...


Vorsorge

Regelmäßig kontrollieren, was Such-Maschinen zum eigenen Namen finden !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Schutz der Privatsphäre

### – Prinzipielle Methoden



16

- Möglichst wenig persönliche Daten veröffentlichen.
- Auswahl der persönlichen Daten sehr sorgfältig treffen.
- Sicherheits-Funktionen beim eigenen Browser, Mail-Programm, Chat-Programm usw. nutzen:
  - Sich damit vertraut machen
  - Möglichst restriktiv konfigurieren
- Zumind. lokale Spuren regelmäßig verwischen.
- Evtl. Anonymisierungs-Dienste nutzen:
  - JAP: <http://anon.inf.tu-dresden.de>
  - TOR: <http://tor.eff.org>
- Regelmäßig kontrollieren, was Such-Maschinen, Info-Dienste usw. zur eigenen Person finden.
- Evtl. professionelle Datenlösch-Dienste nutzen.

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



## Soziale Netzwerke – Probleme mit den Daten



17

### Genau überlegen, was man über sich erzählt !

An folgendes immer denken:

- Auch böse Menschen lesen mit.
- Das Internet kennt keine „Gnade des Vergessens“.
- Man kann nicht sicher sein,  
was der Anbieter mit den eigenen Daten anstellt.

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Datenvermeidung – Motivation



18

### Immer mit dem Schlimm(st)en rechnen !

- Was man einmal veröffentlicht hat,  
kann man nicht mehr zurückholen !
- Selbst wenn man den Zugriff eingeschränkt hat,  
können vertrauliche Daten in falsche Hände gelangen !
  - Man hat selbst einen Fehler gemacht  
(z.B. einen Haken zu viel oder zu wenig gesetzt).
  - Der Betreiber des Netzwerks oder Dienstes ...
    - gibt Daten widerrechtlich weiter.
    - macht einen Fehler.
  - Ein Hacker bricht in das Netzwerk / den Dienst ein.
  - Eine Vertrauensperson missbraucht Ihr Vertrauen.

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Datenvermeidung – Allgemeine Regeln



19

- Keine Daten angeben, durch die man im realen Leben gefunden werden kann !
- Nur Dinge veröffentlichen, auf die man auch noch in 3 Monaten und in 5 oder 10 Jahren stolz ist !

Folgendes sich plastisch vorstellen:  
Alles, was ich heute schreibe, lesen ...

- alle Mitschüler / Arbeitskollegen
- alle Lehrer / Vorgesetzten
- ein späterer Arbeitgeber
- die zukünftigen Schwiegereltern

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Soziale Netzwerke – Konkrete Regeln



20

- Keine Strandbilder und –filme von Kindern
- (Private) Tagebücher gehören nicht ins Internet !
- Keine unvoreilhaftigen oder (ganz) privaten ...
  - Fotos oder Filme veröffentlichen.
  - Kommentare zu Fotos / Pinnwandbeiträgen / ... schreiben.
- Diskriminierende Gruppen (z.B. rechtsradikale Themen oder Mobbing von Lehrern / Arbeitskollegen / ...):
  - Nicht beitreten !
  - Niemals gründen !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Anmelden bei einem sozialen Netzwerk, Gewinnspiel, Dienst, ... ①



21

- Impressum, Datenschutzerklärung, AGB usw. lesen:
  - Was wird mit den gesammelten Daten gemacht?
  - Wer hat Zugriff auf die Daten?
  - Werden Daten an Dritte weitergegeben / verkauft?
- Welchen Eindruck macht das Angebot?
  - Wird der Anbieter seine Versprechungen einhalten?
  - Sorgt der Anbieter für die Sicherheit der anvertrauten Daten?  
Z.B. Keine Anmeldung, falls nur eine unverschlüsselte Datenübertragung möglich ist.
- Im Zweifelsfall auf die Anmeldung verzichten !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Anmelden bei einem sozialen Netzwerk, Gewinnspiel, Dienst, ... ②



22

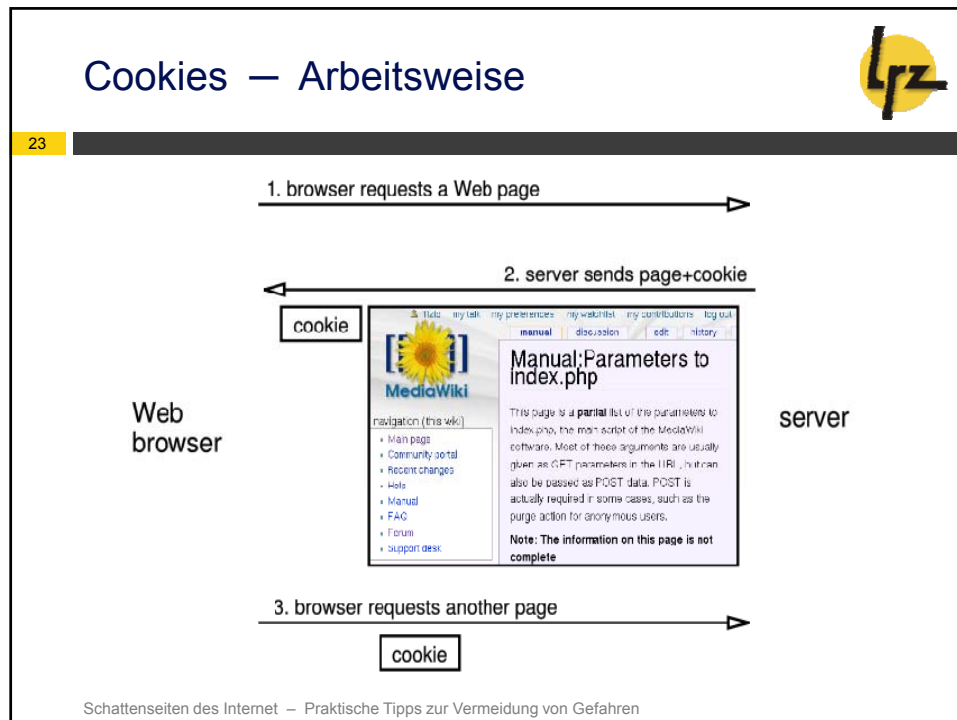
- Optionale Datenfelder leer lassen.
- Falls man den Zugriff einschränken kann:  
Dies auch so weit wie möglich nutzen.
  - Sind alle relevanten „Häkchen“, Auswahl-Boxen usw. entsprechend gesetzt?
- Auf unerwünschte Voreinstellungen achten !
  - Wurden alle entsprechenden „Häkchen“ entfernt?
  - Wurden alle relevanten Auswahl-Boxen verändert?
- Vor dem Abschicken der Anmeldung einen Ausdruck / Screenshot zur Beweissicherung machen von ...
  - dem ausgefüllten Anmeldeformular
  - Impressum, Datenschutzerklärung, AGB usw.

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Cookies – Arbeitsweise



23



## Cookies – Aufgaben



24

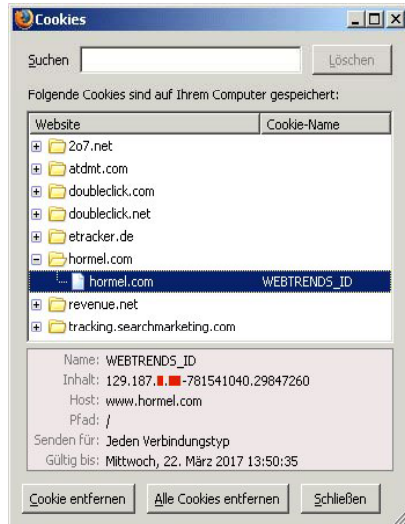
- Identifizierung des Surfers
    - Nicht als “Hänschen Müller”, sondern “nur” als “Surfer 129”
  - Session-Management (z.B. Web-Mail)
  - Persönliche Einstellungen (Inhalt, Oberfläche, ...)
  - Zugangskontrolle
    - Cookie enthält sensitive bzw. wertvolle Daten !
  - Erstellung von Bewegungsprofilen innerhalb eines Web-Servers
  - Erstellung von Nutzungsprofilen
    - Werbung
- } Potentiell gefährlich für die Privatsphäre !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Cookies – Aufbau



25



- Name
- Inhalt
- Gültigkeitsbereich
  - Rechner oder Domain
  - Pfad
- Ablaufdatum
- ...

Wikipedia:  
 .../HTTP\_cookie (En),  
 .../HTTP-Cookie (De)

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Nutzungsprofile durch server-fremde Cookies



26



cia.gov  
mediawiki.org  
**HTTP\_REFERER** → QUERY! asdsadasdsa! asdsada! FREE TRIAL! → lotofbanners.com

Anderer Namen:

- Tracking-Cookies
- 3<sup>rd</sup>-Party-Cookies

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Individualisierte URLs



27

- Beispiele:
  - [www.my-webshop.com/?id=k12slksdf.90abegf.edfd](http://www.my-webshop.com/?id=k12slksdf.90abegf.edfd)
  - [www.my-game.org/members/a98ef560be12/start/](http://www.my-game.org/members/a98ef560be12/start/)
- Aufgabe: Ähnlich wie bei Cookies
- Probleme: Ähnlich wie bei Cookies
  - Potentiell **wertvolle** Daten
  - Potentiell **gefährlich für die Privatsphäre**

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Spuren – Lokaler Rechner / Web-Browser



28

- Passwörter, Formularinhalte → Nicht speichern
- Smart-Browsing (Internet-Keywords) → Deaktivieren
- History-Liste → Regelm. löschen (?), kurze Gleitlöschung
- Bookmarks } **Keinesfalls weitergeben**
- Cookies } **Keinesfalls weitergeben**
  - Keine *automatische* Entgegennahme
  - Keine server-fremden Cookies
  - Unerwünschte Cookies regelmäßig löschen
  - Evtl. Black-List konfigurieren
- Location-Bar-, Download-History → Regelmäßig löschen
- Platten-Cache von gelesenen Seiten → Regelmäßig löschen

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Spuren – Lokaler Rechner / Sonstiges



29

- Log-File eines Personal-Firewalls
- Sonstige System-Log-Files
- Konfigurationsdateien, Caches usw. diverser Anwendungen
- Sich informieren
- Regelmäßig löschen
- Überwachungs-Programme
  - Key-Logger
  - Regelmäßiger Screen-Shot



Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Spuren – Beim Provider



30

- Log-Files von Firewalls, Web-Proxies, Mail-Server usw.
- Abhören in Netzkomponenten
- Telekommunikations-Überwachungsverordnung (TKÜV)  
(Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation)
- Nutzung von Anonymisierungs-Diensten

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Spuren – Log-Files der Web-Server



31

- IP-Adresse des eigenen Rechners
    - DNS-Name
    - WHOIS-Information
  - Verlangte URL
  - URL des Dokuments, in dem die verlangte URL steht (→ HTTP\_REFERER)
  - Informationen über den Browser
    - Hersteller, Version, Betriebssystemvariante, unterstützte MIME-Types, ...
  - Datum, Uhrzeit, Zeitzone
  - ...
- <http://browserspy.dk/>

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Spuren – Was der Browser verrät ☹



32

### Beispiel: Übertragene HTTP-Header

```

HTTP_ACCEPT          text/xml, application/xml,
                    application/xhtml+xml, text/html,
                    text/plain, image/png, */*
HTTP_ACCEPT_CHARSET  ISO-8859-1, utf-8, *
HTTP_ACCEPT_ENCODING gzip, deflate
HTTP_ACCEPT_LANGUAGE en, de
HTTP_CONNECTION      close
HTTP_HOST            browserspy.dk
HTTP_REFERER         http://browserspy.dk/
HTTP_USER_AGENT      Mozilla/5.0 (X11; U; Linux x86_64;
                    en-US; rv:1.8.1.19) Gecko/20081213
                    SUSE/1.1.14-3.1 SeaMonkey/1.1.14
HTTP_VIA             1.0 nc2 (NetCache NetApp/5.3R2D5)
HTTP_X_FORWARDED_FOR 129.187.***.***
QUERY_STRING
REMOTE_ADDR          129.187.254.12
REMOTE_PORT          34997
REQUEST_METHOD       GET
REQUEST_URI          /headers.php
REQUEST_TIME         1232309964

```

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



## Peer-to-Peer-Dienste



33

Potentielle Sicherheitsprobleme bei Peer-to-Peer-Diensten (P2P), wie z.B. Napster, Gnutella, KaZaA:

- Dateien aus unbekanntenen Quellen können grundsätzlich problematisch sein !
- Eigener Rechner ist gleichzeitig Server !
  - ⇒ Bei fehlerhafter Konfiguration ...
    - werden ungewollt private Daten (z.B. Liebesbrief, Steuererklärung) weltweit zur Verfügung gestellt; schlimmstenfalls sogar die komplette(n) Platte(n).
    - wird die eigene Platte für weltweite Schreibzugriffe geöffnet !!!

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



34

## Spam-Mails und Botnets



© Paul-Georg Meister / PIXELIO

## Fähigkeiten moderner E-Schädlinge ①



35

### Eigen-Schutz

- Verbergen vor Entdeckung (→ root-Kit, VM-Monitor)
- Nachladen von neuen Software-Modulen über das Internet
- Entgegennahme von Anweisungen über das Internet
- Deaktivieren von Viren-Scannern, Personal-Firewalls
- Schließen von Software-Lücken
- Tunen des Rechners zur Performance-Verbesserung

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Fähigkeiten moderner E-Schädlinge ②



36

### Schad-Funktionen

- Fernsteuern des Rechners
- Mitprotokollieren sämtlicher Tastatur-Eingaben
- Periodische Erzeugung von Screen-Shots
- Ausforschen der lokalen Platte
- Abhören des lokalen Netzes
- Verschicken von Spam-Mails
- Angriff fremder Rechner (→ DoS: Denial of Service)
- Infektion weiterer Rechner

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

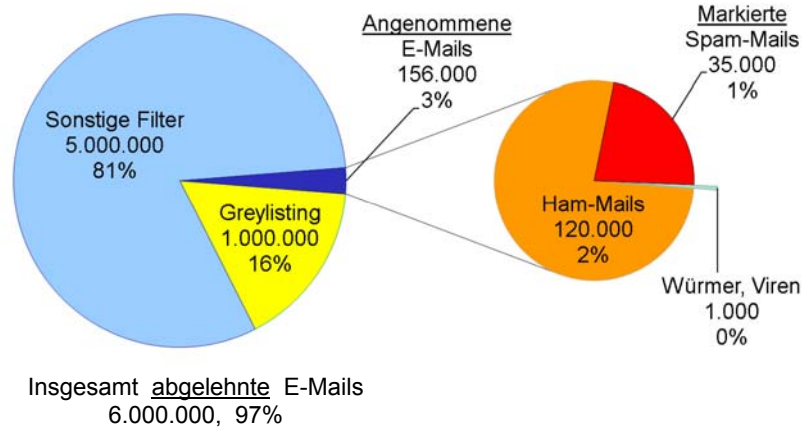
## Spam-Abwehr am LRZ



37

### Von den Mail-Relays pro Tag bearbeitete E-Mails

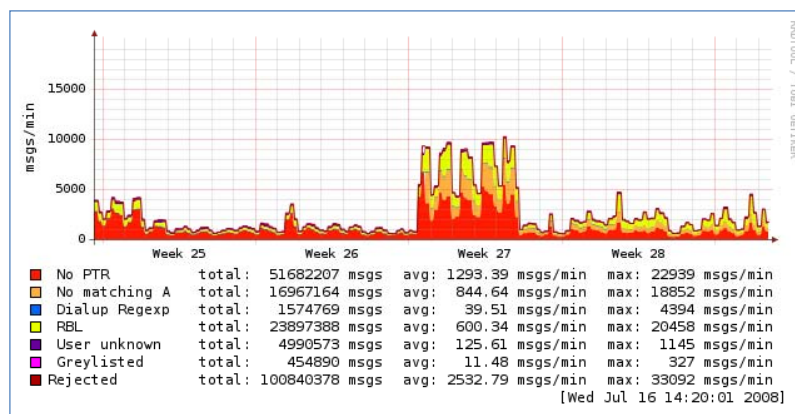
(Peak: 20.000.000 (!) E-Mails)



## Beispiel einer Spam-Welle am LRZ

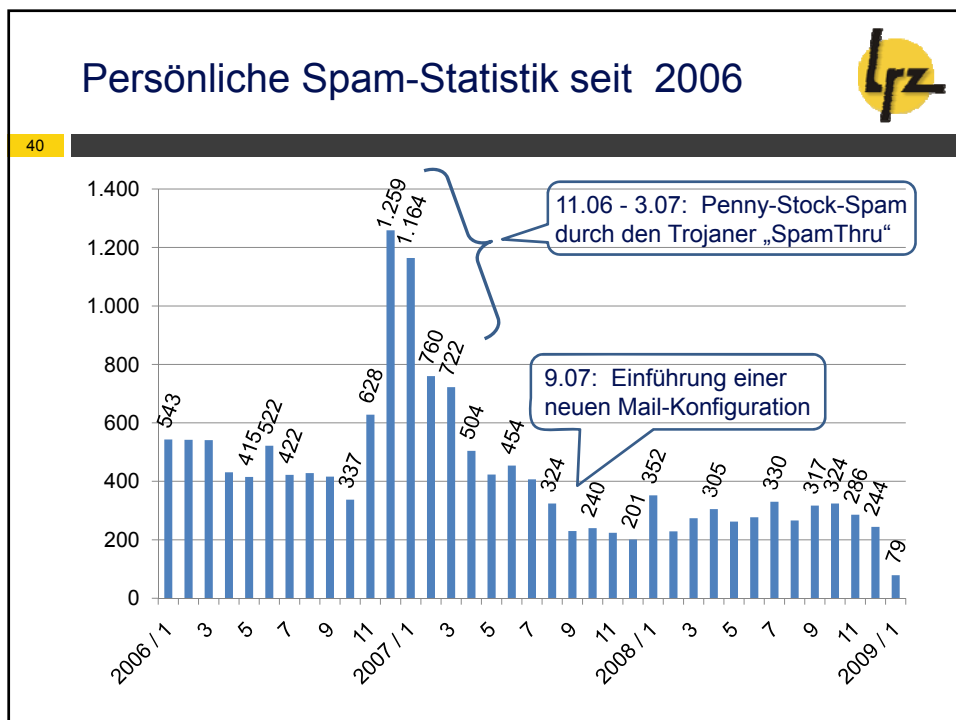
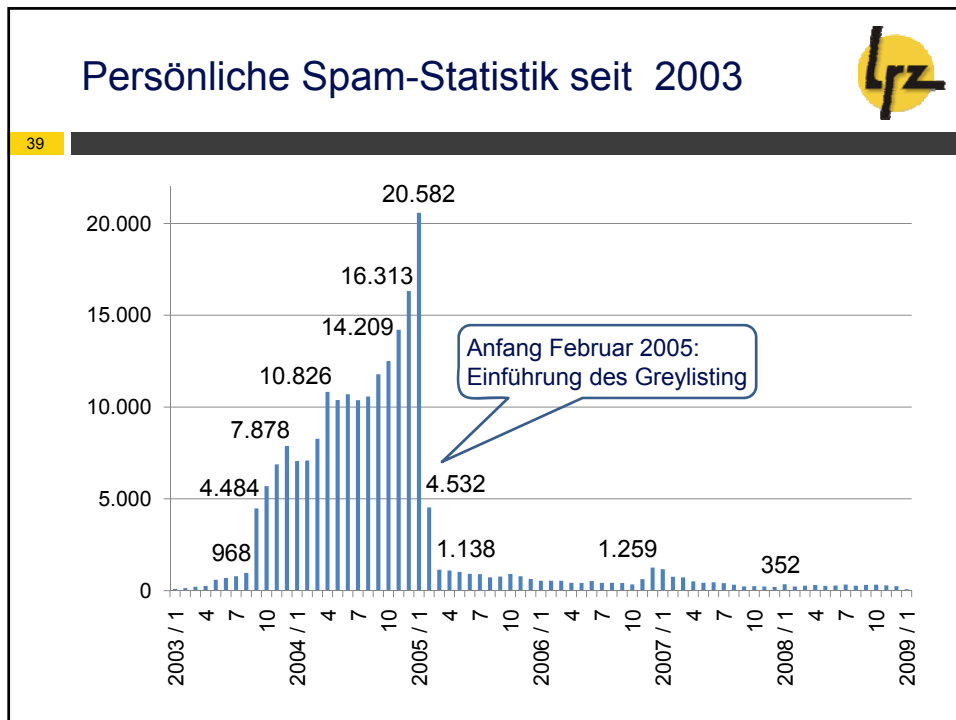


38



Dauer: Mo. 30.6.08, 12:00 Uhr bis Fr. 4.7.08 24:00 Uhr  
 Spitzenwert: 33.092 abgelehnte E-Mails pro Minute

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



## Schutz gegen Spam – Im Vorfeld ①



41

### Hintergrund:

Spammer sammeln Mail-Adressen von Web-Seiten, aus News-Gruppen, aus Foren usw.

### Deshalb die eigene primäre Mail-Adresse ...

- nur vertrauenswürdigen Personen geben.
- möglichst nicht allgemein veröffentlichen.
- in Web-Seiten usw. „verfremdet“ darstellen.

### Beispiele:

- erwinX@Xdomain.de [ Alle „X“ bitte entfernen ]
- erwin\_hier\_ät\_domain\_hier\_dot\_de
- Aus der Mail-Adresse ein GIF erzeugen und dieses verwenden.

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Schutz gegen Spam – Im Vorfeld ②



42

- Zur Anmeldung jeweils eine neue, individuelle Mail-Adresse verwenden (→ Free-Mailer).
  - Bei Missbrauch einfach aufgeben
- Evtl. ein Kontaktformular anbieten:
  - 👍 Mail-Adresse kann nicht gesammelt werden (nur bei richtiger Implementierung)
  - 👎 Unbequem für die Nutzer
  - 👎 Kostet Aufwand
  - 👎 Kann bei Implementierungsfehlern zum Spammen missbraucht werden !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Schutz gegen Spam

### – Nach Erhalt einer Spam-Mail



43

- Spam-Mail möglichst nicht lesen.
  - Spam-Mails enthalten manchmal „Web-Bugs“ (d.h. Links auf unsichtbare 1-Pixel-Bilder, durch die der Spammer das Lesen registrieren kann).
  - Die Mail-Adresse gewinnt für den Spammer an Wert !
- Falls möglich:
  - Mail-Programm konfigurieren, dass beim Ansehen verlinkte Bilder nicht (automatisch) angezeigt werden.
- Hyper-Links in Spam-Mails nicht verfolgen.
  - Die Mail-Adresse gewinnt für den Spammer weiter an Wert !
- Niemals, niemals, niemals ein mit Spam beworbenes Produkt kaufen !
  - Die Mail-Adresse gewinnt für den Spammer weiter an Wert !

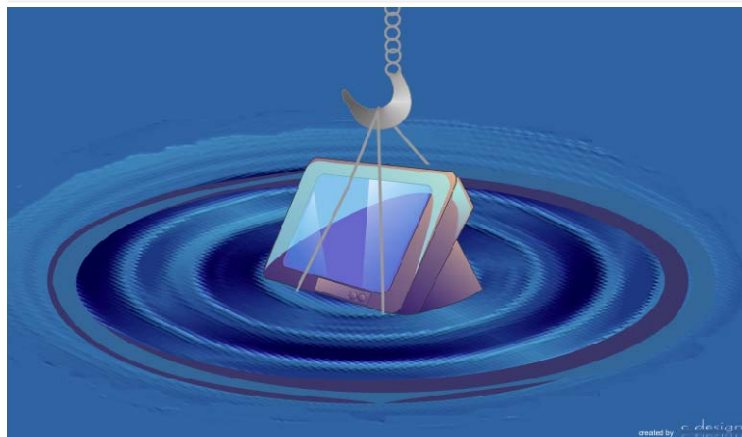
Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



44



## System-Sicherheit (z.B. der eigene PC)



## Ziele von Angriffen



45

- Benutzer als *Person*
  - Social Engineering → „Aushorchen“:  
Persönlich / per Telefon /  
per E-Mail (Phishing)
  - Trashing → „Putzkolonnen“
- *Rechner* des Benutzers
  - Via Inter-/Intra-Net oder persönlich
- *Netzkomponenten* (praktisch nie Datenleitungen)
- *Zwischenstationen* im Internet auf dem Weg zum Kommunikationspartner
  - Z.B. Lesen fremder *unverschlüsselter* E-Mails

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## „Waffen“ der Angreifer



46

- Würmer, Botnet-Drohnen
- Trojanische Pferde
  - Programme,
    - die neben ihrer *offensichtlichen* Funktion (z.B. Screen-Saver, Spiel, Sound-Generator, Home-Banking-Tool)
    - auch noch eine *versteckte* Nebenfunktion haben (z.B. Ausspähen von Kennungen und Passwörtern).
  - Beispiele
    - Adware → „Zwangsbeglückung“ mit Werbung
    - Spyware → Ausforschen von Passwörtern, Surf-Verhalten usw.
- **Überwiegende Verbreitung durch Web-Seiten**  
⇒ Firewalls sind kein Schutz



Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Angriffspunkte (absteigende Bedeutung)



47

- **Security-Lücken** in der Software
  - Hersteller, Administratoren und Benutzer reagieren zu langsam oder überhaupt nicht
- **Ungenutzte Security-Mechanismen**
  - z.B. veralteter oder gar kein Viren-Scanner, nicht eingespielte Patches
- **Schlechte Passwörter** ☹ ☹ ☹
- Konfigurationsfehler → Administratoren und Benutzer
- Abhören des Datenverkehrs → Rechner (praktisch nie Leitungen)
- Benutzer als Person
- Diebstahl von Hardware → Notebook / PDA / Handy

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Die wichtigsten Regeln ①



48

### ■ Menschliche Firewall:

- Sich der Gefahr bewußt werden
  - Sich kontinuierlich informieren
  - Gesunder Menschenverstand
  - Vorsicht, Vorsicht, Vorsicht, Vorsicht ...
- **Sicheres Verhalten:**
    - Sicherer Umgang mit Kennungen
    - **Gute** Passwörter
    - Regelmäßige Kontrolle der Technik

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



## Die wichtigsten Regeln ②



49

### Technik:

- Aktuelle Programmversionen
  - Alle Service-Packs, Security-Patches, ...
  - Viren-Scanner
    - Aktuelle Version + Signaturen
    - On-Access-Scanning
    - Alle Dateitypen
  - Regelmäßiger Backup wichtiger Daten
  - Personal-Firewall: Nur etwas für Profis (?)
- } Möglichst automatischer Update

**In vielen Fällen reicht dies vollkommen aus !**

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Viren-Scanner – Prinzipielle Probleme



50

- Ein Schädling ist neu.
  - Er wird i.a. erst nach mehreren Stunden bis evtl. sogar Tagen (!) erkannt.
- Riesige Zahl an neuen Schädlingen und Varianten
  - Nur etwa die Hälfte der Schädlinge wird erkannt !
  - ⇒ Vorsicht + Security-Patches usw. *nicht* überflüssig !
- Immer wieder Probleme mit Malware in Archiven
- Malware in verschlüsselten Archiven wird *meist nicht* erkannt !
- Oft Probleme mit Spyware und Adware
  - ⇒ Eigenes Tool sinnvoll


Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Personal-Firewall (?)

51

Vorteil:

- ⊕ Schutz gegen einige Arten von Angriffen:
  - Zugriffe von außen auf im Hintergrund laufende Server-Dienste
  - Kommunikation lokaler E-Schädlinge (nur bedingt)



Nachteile:

- ⊖ Zusätzliches System, das Fehler enthalten kann
- ⊖ Gefahr der Fehl-Konfiguration
- ⊖ Sinnvoller Betrieb erfordert ...
  - Know-how
  - kontinuierliche Überwachung
- ⊖ Titanic-Effekt

} Schutz oft nur **subjektiv** vorhanden !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Personal-Firewall – Titanic-Effekt

52

- Andere bewährte Sicherheits-Mechanismen werden vernachlässigt.
  - Verspätetes Einspielen von Security-Patches, Service-Packs, Updates ...
- Unvorsichtiges Verhalten wegen vermeintlichem Schutz
  - Kritikloses Anklicken von Mail-Anhängen
  - Besuch von wenig vertrauenswürdigen Web-Seiten
- Falsche Anwendung der neuen Technologie
  - Kritikloses Öffnen von Ports



Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Weitergabe von Datenträgern

### – Schutz der Daten? ①



53

#### Arten der Weitergabe

- Unabsichtlich → Verlust, Diebstahl
- Absichtlich → Verkaufen, verschenken, wegwerfen

#### Prinzipielle Probleme

- Vielfalt der Datenträger:  
Platten, USB-Sticks, Karten für Kameras, ...
- „Versteckte“ Datenträger (z.B. Platten in Druckern)  
→ Oft nur physische Zerstörung möglich
- Unzählige Kopien im Laufe der Bearbeitung:  
Temporäre Dateien, Backups, automatisch erzeugte  
Wiederherstellungsdateien, Schattenkopien,  
Auslagerungsdateien, ...

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Weitergabe von Datenträgern

### – Schutz der Daten? ②



54

#### Schutzmechanismen

- Verschlüsselung:
  - Schutz bei allen Arten der Weitergabe
  - Umfang: Einzelne Dateien ↔ **Komplette Laufwerke / Partitionen**
  - Wichtig: Qualität der Software und des Passworts
- Löschen von Daten:
  - Kein Schutz bei unabsichtlicher Weitergabe
  - „Einfaches“ Löschen durch das Betriebssystem reicht nicht aus !
    - Nur der Verzeichniseintrag wird gelöscht.
    - Daten selbst bleiben erhalten und können wiederhergestellt werden.
  - ➔ Einmaliges Überschreiben erforderlich (möglichst mit Spezialprog.)
  - ➔ Kopien-Problematik: Möglichst komplette Laufwerke überschreiben

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Unachtsamer Umgang mit Kennungen



55

- **Weitergabe eines Passworts**
  - Meist durch Benutzerordnung untersagt
- Wahl eines **schlechten** Passworts
- **Unkritische Verwendung** von fremden Programmen, Profiles usw.
- Verschicken eines Passworts über *unverschlüsselte* E-Mail
- Einräumen von zu großzügigen Rechten
- Unbeaufsichtigtes Verlassen einer Dialogsitzung (v.a. in öffentlich zugänglichen Räumen)
  - Sitzung locken oder beenden
- „Freundlicher, flüchtiger Bekannter“, der einem kurz hilft, und man versteht nicht, was er tut

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Wie kommen Hacker an Ihr Passwort?



56

- **Schlechte Passwörter !** ☹ ☹ ☹
- Trojanische Pferde
  - Falsches Login-Programm, Key-Logger
- Abhören von Rechnern (praktisch nie von Leitungen)
- Beibehalten allgemein bekannter Default-Passwörter
- Aufgeschriebene Passwörter
  - Zettel verloren oder hängt am Rechner
- (Leichtsinnige) Weitergabe von Passwörtern
- Lesen fremder *unverschlüsselter* E-Mails

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Sicherer Umgang mit Passwörtern ①



57

- **Das Passwort niemals weitergeben !**
  - Weitergabe meist durch Benutzerordnung untersagt
  - Geben Sie einem flüchtigen Bekannten Ihre Wohnungsschlüssel oder Ihre Scheck-Karte?
- **Nur „gute“ Passwörter verwenden !**
  - Für verschiedene Tätigkeiten mit unterschiedlichen Sicherheits-Anforderungen auch verschiedene Passwörter verwenden !
    - Administrator ↔ Normaler Benutzer
    - Beruf ↔ Privat
    - Homebanking ↔ Spiel

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Sicherer Umgang mit Passwörtern ②



58

- Passwörter nie **unverschlüsselt** per E-Mail verschicken !
- (Allgemein) bekannte Default-Passwörter sofort ändern !
- Passwörter regelmäßig ändern !
  - Systemverwalter: Alle 1 - 6 Monate
  - Benutzer: Alle 3 - 12 Monate
- Passwörter aufschreiben / abspeichern?
  - Ja, aber mit Verstand !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Aufschreiben von Passwörtern – Regeln



59

- Nach Verlust des Zettels usw. Passwörter sofort ändern !
- Nach Möglichkeit ...
  - Kennung und Passwort nicht zusammen aufschreiben.
  - Passwort „verfälscht“ aufschreiben.  
→ Leicht zu merkender Algorithmus
  - nicht (unverschlüsselt) auf einem Rechner speichern.
- Zettel für Notfall / Vertretungsfall / Backup:
  - Sicher aufbewahren !
  - Nach Nutzung des Zettels Passwort evtl. ändern.
- Zettel als Gedächtnisstütze:
  - Zettel **immer** bei sich tragen !

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Passwörter – Faustregeln



60

- “Wertvolle” Passwörter (z.B. Admin.-Passwörter)
  - Möglichst gut
  - Sicher aufschreiben
  - Möglichst häufig ändern
- Selten verwendete Passwörter
  - Möglichst gut
  - Sicher aufschreiben
- Häufig verwendete Passwörter
  - Einigermaßen gut (→ schnelles Eintippen)
  - Häufiger ändern

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Qualität von Passwörtern

61

The diagram shows a horizontal arrow pointing to the right, representing the quality of passwords. The arrow is divided into three sections: a red section on the left labeled 'Fahrlässig schlecht', a red section in the middle labeled 'Schlecht', and a green section on the right labeled 'Gut'. A vertical dashed line separates the 'Fahrlässig schlecht' and 'Schlecht' sections. A vertical solid line separates the 'Schlecht' and 'Gut' sections.

- Fahrlässig schlecht**
  - Kürzer als 8 Zeichen
- Schlecht**
  - Wahrscheinlich von > 1 Person verwendet
- Gut**
  - Mindestens 8 Zeichen lang
  - Mindestens: 1 Klein-, 1 Großbuchstabe, 1 Ziffer, 1 Sonderzeichen
  - Ziffer / Sonderzeichen nicht nur am Anfang / Ende
  - Wahrscheinlich nur von 1 Person verwendet

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Unverantwortlich schlechte Passwörter

62

- Eigenschaften:
  - Kann mit *wenigen* Versuchen erraten werden !
  - Angreifer muss die gehashten Passwörter **nicht besitzen**, da Ausprobieren durch Einloggen möglich.
- Kriterien:
  - Wörter aus dem **Kennungs-Kontext** (z.B. bei UNIX /etc/passwd)
    - Kennung selbst, Kommentarfeld, ...
  - Wörter aus dem **persönlichen Umfeld**
    - Eigener Name / Vorname, Vorname des Partners / eines Kindes, ...
  - Eines der **fünf häufigsten** Passwörter (z.B. "geheim")

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Schlechte Passwörter



63

- Eigenschaften:
  - Kann mit Wörterbuch-/Brute-Force-Angriff erraten werden.
  - Angreifer muss die gehashten Passwörter besitzen.
- **Bereits 1 (!!!)** der folgenden Kriterien reicht aus:
  - (Spitz-)Name, Person, Ort, ... → Schnurzi, Gandalf
  - Wort einer (natürlichen) Sprache → Sittich
  - *Bekanntes* Akronym → siehe später
  - Kürzer als 8 Zeichen → Brute-Force-Angriff
  - Nur Buchstaben oder nur Ziffern → Brute-Force-Angriff
- Einfache Transformationen bieten keinen zusätzlichen Schutz! (z.B. rückwärts schreiben,  $i \leftrightarrow 1$ ,  $o \leftrightarrow 0$ )

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Gute Passwörter



64

- Alle (!!!)** folgenden Kriterien müssen erfüllt sein:
- Erfüllt kein Kriterium eines schlechten Passworts.
  - Länger als 7 Zeichen
    - Achtung: Manchmal werden nur die ersten N Zeichen ausgewertet!
  - Enthält Groß- und Kleinbuchstaben.
  - Enthält mindestens eine Ziffer oder ein Sonderzeichen.
  - Die Ziffer / das Sonderzeichen steht nicht am Anfang oder am Ende.
  - Man kann sich das Passwort leicht merken.
  - Man kann das Passwort schnell tippen.
    - „Blick über die Schulter“

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



## Collage-Methode



65

- ① 2 Wörter wählen (evtl. aus verschiedenen Sprachen)
- ② Hieraus jeweils 3 Buchstaben wählen (z.B. die ersten oder letzten 3)
- ③ Es sollten sowohl Groß- als auch Kleinbuchstaben dabei sein.
- ④ 2 Ziffern und/oder Sonderzeichen wählen
- ⑤ Alle Bestandteile zusammensetzen. Dabei die Ziffern und/oder Sonderzeichen nicht *nur* am Anfang und/oder Ende.

### Beispiel:

„haus“ + Hausnr. 23 + „HOUSE“ → hau23HOu

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Akronym-Methode



66

- ① Auswahl eines Satzes, der **keinesfalls allgemein bekannt** sein darf
- ② Auswahl von 6 - 7 Wörtern aus diesem Satz
- ③ Anfangsbuchstaben der ausgewählten Wörter verwenden
- ④ Es sollten sowohl Groß- als auch Kleinbuchstaben dabei sein.
- ⑤ 2 - 1 Ziffern und/oder Sonderzeichen wählen, sofern sie sich nicht unmittelbar aus dem Ausgangssatz ergeben
- ⑥ Alle Bestandteile zusammensetzen, dabei die Ziffer(n) und/oder Sonderzeichen nicht nur am Anfang und/oder Ende

Beispiel: „AeS,dkab“ (siehe Punkt ①)


Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren



67 **Fazit**



© S. Hofschlaeger / PIXELIO

Sie tun es zum **eigenen** Schutz ! 

68

Es kann viel auf dem Spiel stehen !

- Ihre Gesundheit
- Ihre Unbescholtenheit
- Ihr guter Ruf
- Ihr Geldbeutel
- Ihre Privatsphäre

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## „Botschaften“ des Vortrags



69

- Das Internet hat leider einige Schattenseiten.
- Dennoch nicht erforderlich:
  - Panik
  - Prinzipielles Vermeiden des Internet
- Mit einigen relativ einfachen Maßnahmen kann man vielen Gefahren aus dem Weg gehen.

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Wichtigster Schutz gegen die Gefahren



70

### Menschliche Firewall:

- Sich der Gefahr bewusst werden
- Sich **kontinuierlich** informieren
- Sicheres Verhalten
- Gesunder Menschenverstand
- Vorsicht, Vorsicht, Vorsicht, Vorsicht, ...



Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren

## Quellen des Vortrags



71

### Vielen Dank für Folien, Anregungen, Bilder usw.

- Bayerisches LKA, Sachgebiet 513 Ha:  
Gefahren im Internet – » Worauf ich unbedingt achten sollte ! «.  
[www.lrz.de/services/security/vortraege/lka.gefahren.2007-03.pdf](http://www.lrz.de/services/security/vortraege/lka.gefahren.2007-03.pdf)
- Margret Bezold-Chatwin:
  - Vortrag: Girls' Day – Ohne Gefahr ins Internet
  - Folien-Style, Grafiken und Smileys
- Dr. Ernst Bötsch, Dr. Petra Einfeld, Vasilios Kokkas:  
Einführung in die System- und Internet-Sicherheit.  
[www.lrz.de/services/security/benu-kurs/](http://www.lrz.de/services/security/benu-kurs/)
- Dr. Ernst Bötsch: Security-Bausteine für das MWN.  
[www.lrz.de/services/security/vortraege/](http://www.lrz.de/services/security/vortraege/)
- Bilder von [www.pixelio.de/](http://www.pixelio.de/)

Schattenseiten des Internet – Praktische Tipps zur Vermeidung von Gefahren