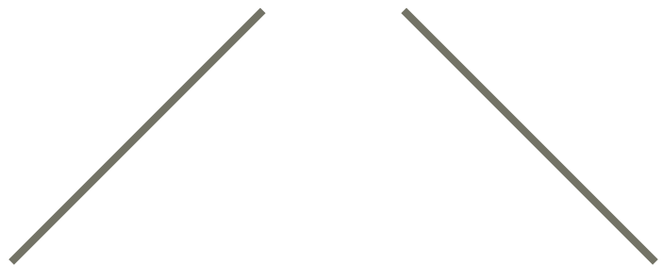
Carl Friedrich von Weizsäcker Friedensvorlesung

Cyber Security · Cyber War · Cyber Peace

Soziale Sicht

Prof. Dr. Tobias Eggendorfer

Cyber



Internet?

Computer?

Cyber-War

Kriegsführung durch Angriffe auf IT-Systeme

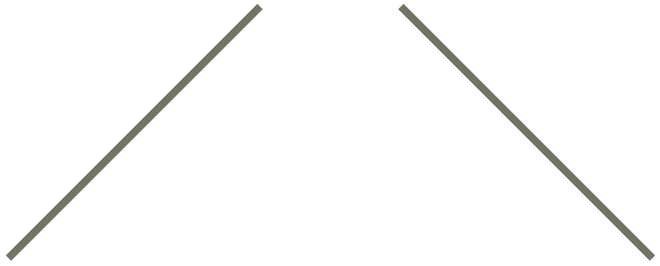
Cyber-Security

Schutz von IT-Systemen vor Angriffen

Cyber-Peace

IT-Frieden?
Abrüstung im Cyber-War?

Soziale Sicht



Gesellschaftlich

Gemeinnützig

Soziale Sicht

Gesellschaftlich

Verantwortung?

Gemeinnützig

Soziale Sicht

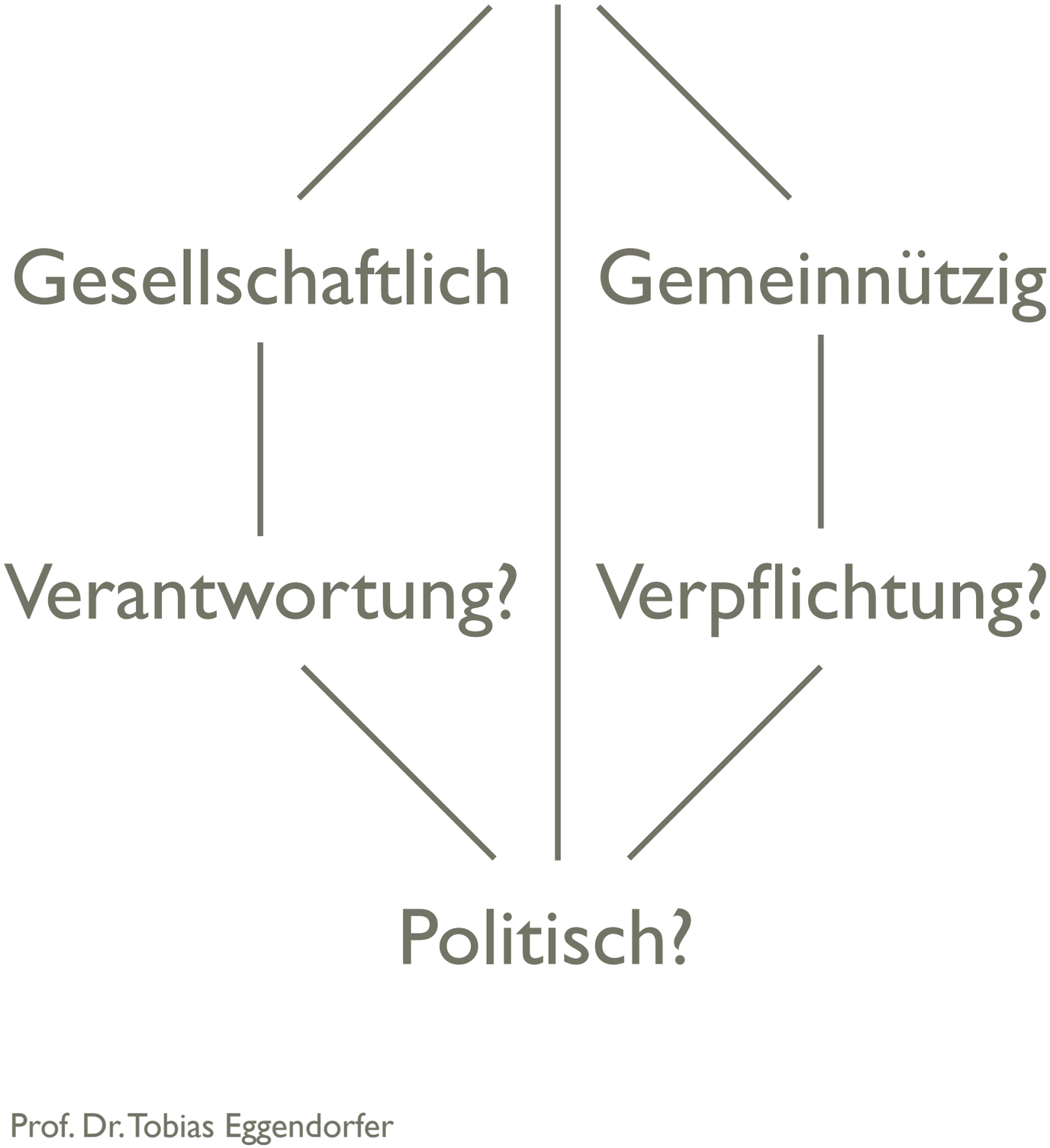
Gesellschaftlich

Verantwortung?

Gemeinnützig

Verpflichtung?

Soziale Sicht



Neue Gefahren?

1947

1962

- Mariner 1 Rakete
  - Berechnung Flugdaten statt mit Durchschnittsweten mit aktuellen Werten
    - Hektische Manöver ➜ Zwangsexplosion
- Handschriftliche Notiz in Quelltext

1978

- NASA entdeckt Ozonloch - theoretisch: Software hält Meßwerte für Fehler und korrigiert sie

1983 - 1987

- Therac-25 - tödliche Strahlenüberdosis
- Außer der Therapeut war Anfänger...

1984

1984

1984 - 1986

- 1984: Dissertation von Fred Cohen
- 1986: Erste Infektion an der FU Berlin

1985 - 1986

1985 - 1986

1988

- Rob Morris' Wurm infiziert 10% des Internet
- Buffer Overflow in fingerd
- Experiment - mit fatalem Ausgang

1995

- Ping of Death
- Fragmentierte Ping-Pakete falsch zusammengesetzt
- System stürzt ab

1997

2004

- Hartz IV-Überweisung kommen nicht an.
- Umstellung auf Scheck-Versand:
  Briefe kommen zurück

2005

- 5 Milliarden Schaden beim A380
- zu kurze Kabel
- Ursache:
  - CATIA v5 in Toulouse
  - CATIA v4 in Hamburg
  - Fehlerhafter Converter

2007

2008

2009

2011 - Datendiebe

SM

PLAYSTATION®
Network

2011 - Datendiebe

2011 - Datendiebe

2011 - Datendiebe

The Ritz-Carlton®

2011 - Datendiebe

2013 - Geheimdienste

Fazit:

Computer nicht fehlerlos.

Aber:

Zu großes Vertrauen in Computer

„Laut dem Computer ist das so.“

Beispiel: SZ vom 14.10.2013

In Hamburg-Neuengamme ist es zu einem kuriosen Unfall gekommen. Weil ihr Navigationsgerät sie offenbar in die falsche Richtung führte, fuhren zwei Männer mit ihrem Kleinbus in einen Seitenarm der Elbe.

Paradox:
„Ist mein Online-Banking sicher?“

Cyber-War: „Hacking“

- Ursprünglich:
  Friedliches,
  kreatives
  Umnutzen
- Heute oft:
  Destruktives
  Eindringen

Unterscheidungen

- Cracker ↔ Black Hat
- Hacker ↔ White Hat

  „ethisches Hacken“
- Grey Hat
- Skript Kiddie

Stören von Systemen

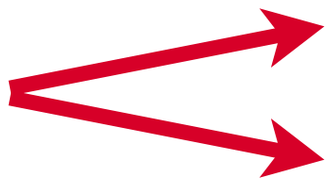
- Angriffe auf
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität

Stören von Systemen

- Angriffe auf
  - Verfügbarkeit → Denial of Service
  - Vertraulichkeit
  - Integrität

Stören von Systemen

- Angriffe auf
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität

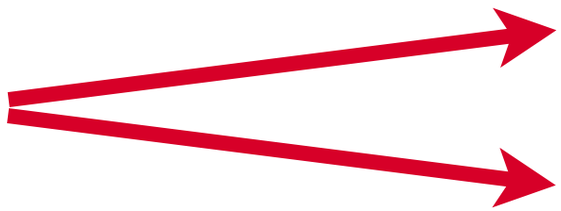


Sniffen

Einbrechen

Stören von Systemen

- Angriffe auf
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität



Einbrechen

Manipulation während Übertragung

Angriffe: Verfügbarkeit

- Distributed Denial of Service Angriff
- Provozierte Systemabstürze

Provozierter „Absturz“?

- Ping of Death
- Code Injection z.B. durch Buffer Overflow
- Fehlerhafte Programme durch
  - Unzureichende Tests
  - Unzureichende Qualitätssicherung

Angriff: „Sniffen“

- Mitlesen von übertragenen Daten
- Ursache:
  - Fehlende Verschlüsselung
    ➜ Anforderung „übersehen“
    ➜ Qualitätsmangel

Standard: Unverschlüsselt

- SMTP / POP3 / IMAP
- SIP / RTP
- DNS
- FTP
- Telnet

} Viel zu aufwendig - damals.

Gestern auf heise.de

05.11.2013 08:15

« Vorige | Nächste »

XMPP soll durchgehend verschlüsselt werden

vorlesen / MP3-Download

Eine Gruppe von Programmierern und Betreibern von XMPP-Systemen hat ein Manifest veröffentlicht, nach dem der XMPP-Standard ab dem 19. Mai 2014 nur noch mit durchgehender Verschlüsselung eingesetzt werden soll. An diesem Tag ist der Open Discussion Day, an dem seit 2006 offene Protokolle und Standards gewürdigt werden.

Mit dem Manifest haben die Entwickler einen Zeitplan vorgelegt, was bis zum 19. Mai alles verändert und getestet werden muss, damit die durchgängige Verschlüsselung funktionieren kann, beginnend mit dem Einsatz der neuesten TLS-Verschlüsselung. Dabei wollen sie sich durchweg an die IETF-Empfehlungen zu TLS halten.

Angriff: „Einbruch“

- Ausnutzen einer Sicherheitslücke
- ➜ Übernahme des Systems
- Ursache:
  Unzureichender Schutz?

Wie „einbrechen“?

- Code Injection durch
  - SQL-Injection
  - Cross-Site-Scripting
  - PHP-Injection
  - Shell-Injection
  - Shell-Code-Injection

SQL-Injection

SQL-Injection

ImmoSky AG – INFORMATION

immosky.de/webagent_deactivate.php?int_id=77794 or 1=0&ccode=49

update tbl_interessent set int_emailagent = 0 where int_id = 77794 or 1=0

DEUTSCHLAND

ALLE ANGEBOTE | SERVICES | ÜBER UNS | KONTAKT | JOBS

ORMATION

-Mail-Agent wurde erfolgreich deaktiviert.

Ursache?

- Programmfehler:
- Unzureichende Kontrolle der Eingabe
- Fehlendes „Escaping“

Cross-Site-Scripting

- Einschleusen von JavaScript in fremde Seiten
  - Ausspähen von Daten
  - Manipulieren von Daten
  - u.v.m.
- Ähnlich: HTML-Injection

Cross-Site-Scripting

- Ursache:
  - Fehlerhafte Eingabekontrolle
  - Unzureichendes Escaping der Ausgabe

PHP-Injection

- PHP: Serverseitige Script-Sprache
- Einschleusen von PHP in PHP
- Ziele:
  - Übernahme des Servers
  - Ausspähen von Daten
  - u.v.m.

PHP-Injection

- Ursache:
  - Fehlerhafte Eingabekontrolle
  - Nutzung „gefährlicher“ Funktionen wie
    - eval
    - exec

Shell-Injection

- Einschleusen von Kommandozeilen-Befehlen, z.B. rm -rf /
- Ziele:
  - Denial of Service
  - Manipulation / Ausspähen von Daten
  - u.v.m.

Ursache

- Ursache:
  - Fehlerhafte Eingabekontrolle
  - Nutzung „gefährlicher“ Funktionen wie
    - exec

Shell-Code-Injection

- Einschleusen von Maschinen-Code in laufendes Programm
- Ziele:
  - Übernahme des Rechners
  - Denial of Service
  - u.v.m.

Ursache

- Fehlerhafte Eingabekontrolle führt z.B. zu
  - Format String Fehler
  - Stack Overflow
- Fehlerhafte „Pointer-Operationen“

Und es gibt viel noch mehr...

Immer dieselben

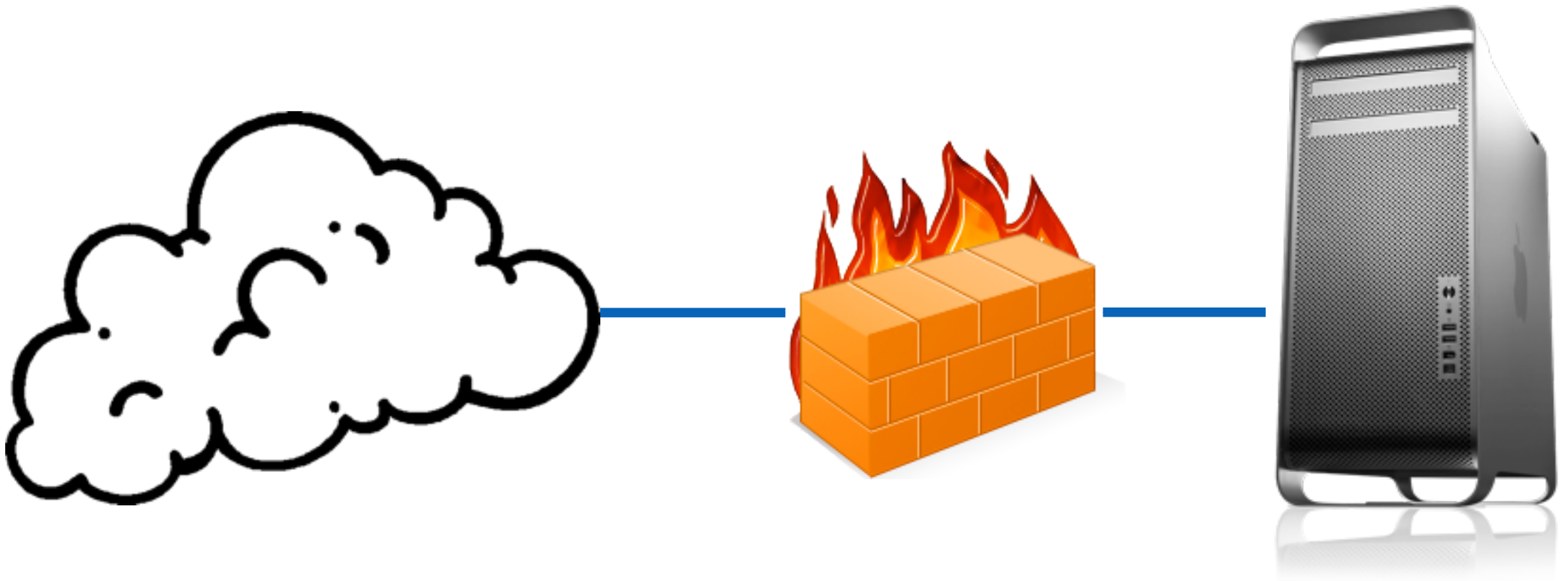
Ursachen.

Schlampige
Programmierung.

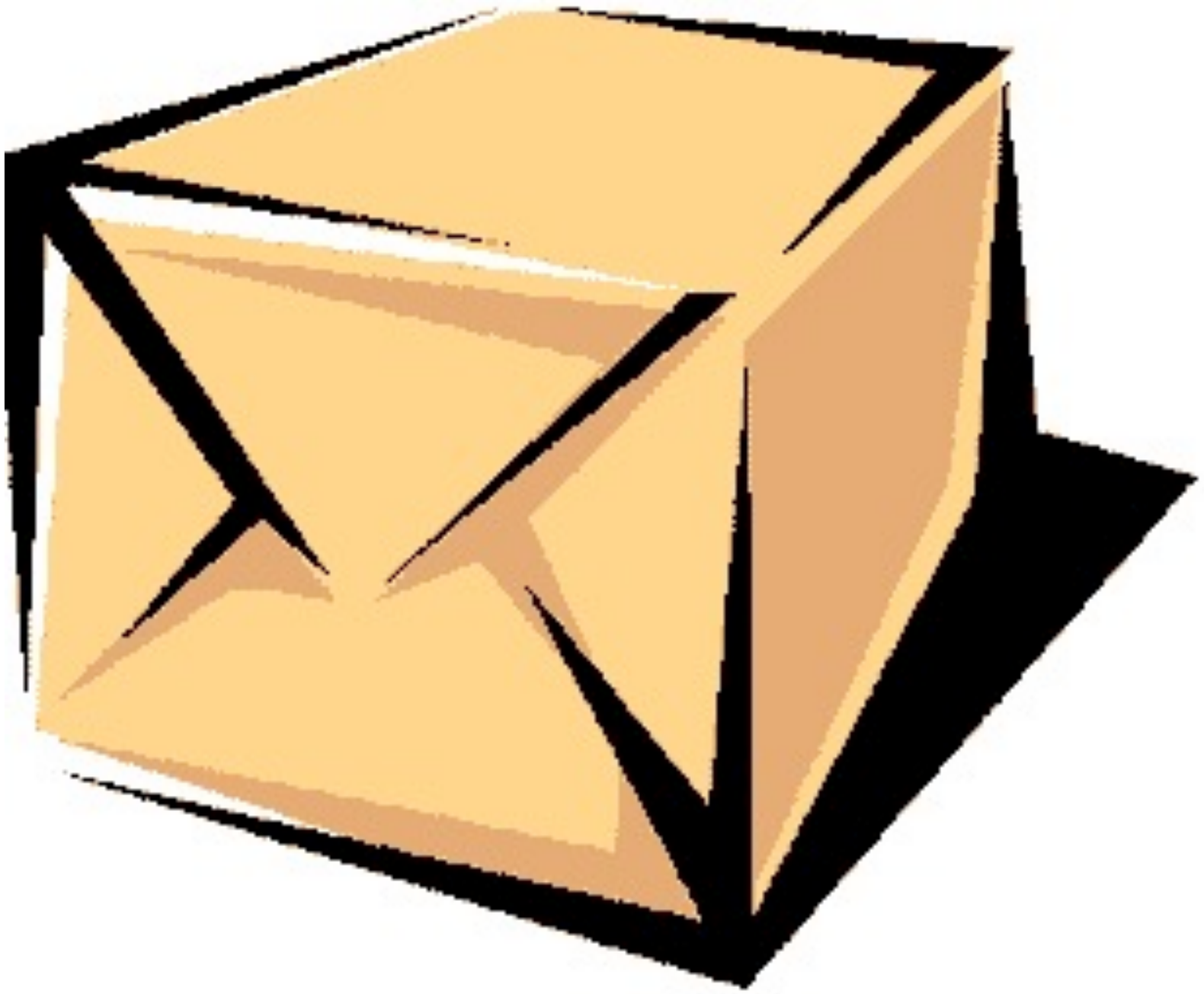
Fehlende Qualitätskontrolle

Unbeholfene Schutzmaßnahmen

Firewalls



Was eine Firewall sieht:



Was sie nicht kann:

Encarta Enzyklopädie, Photo Researchers, Inc./Scott Camazine

Application Level Firewall?

Ja, gibt es, aber:

- Erkennt nur bekannte Angriffe
- Heuristik für Anomalien

Intrusion Detection System?

Ja, gibt es, aber:

- Erkennt nur bekannte Angriffe
- Heuristik für Anomalien

Intrusion Prevention System

Intrusion Prevention System

- Koppelt Firewall mit IDS
- Gleiche Mängel

Ergebnis:

Single-Point-Security

Single-Point-Security

Single-Point-Security

PLEASE
CLOSE
GATE

PLEASE
CLOSE
GATE

Ursache

Ursache

IT-Sicherheitsmaßnahme

IT-Sicherheit scheitert:

- Nicht an:
  - Kreativität von Sicherheitsmaßnahmen
  - Know How der „Experten“
- Aber an:
  - miserabler Softwarequalität
  - fehlender Qualitätssicherung

Warum das so ist:

- Softwareeinkauf derzeit nach:
  - Schön bunt
  - Billig
  - Kenne ich schon
  - One Size fits all

Bohren Sie damit Löcher in Beton?

Umdenken dringend nötig.

Was wir ändern müssen:

Qualität einfordern

Das ist nicht normal:

Wissen Sie noch?

Wir haben die Sicherheit neu erfunden .
Die neue A-Klasse.

Was wir noch ändern müssen:

Qualität einfordern.

Qualität einfordern.

Qualität einfordern.

Und dann noch:

- Klare Anforderungen definieren
- IT-Sicherheit ab 1. Semester
- Sachmängel- / Produkthaftung korrigieren
- Qualität bezahlen

Und was hat das mit CyberWar & -Peace zu tun?

Angreifer nutzen Qualitätsmängel

Danke für Ihre Aufmerksamkeit.

http://www.eggendorfer.info