Sicherheit in verteilten Systemen

Bedrohungen in verteilten Systemen

1) Viren, Würmer, etc., allgemein: Malware

via e-mail und via http

bedroht nicht nur durch destruktives Verhalten, sondern auch durch Missbrauch der Infrastruktur

2) Erspähen von Daten

3) Manipulieren von Daten

Abwehrmaßnahmen allgemein

1) gegen Malware:

Antivirenprogramme

traditionelle Funktionsweise: *in den erhältlichen Produkten*

- Mustererkennungsverfahren
- von schnellen Aktualisierungen abhängig
- Aktualisierung im zentralistischen push-Verfahren

verbesserte Funktionsweise: *noch im Entwicklungsstadium*

- Erkennung am Verhalten
- dezentralistische autonome Verfahren

Authentifizierung

- digitale Signatur

Abwehrmaßnahmen allgemein

2) gegen Erspähen von Daten:

Autorisierung

- Leseberechtigung

Authentifizierung

Verschlüsselung bei der Übertragung

- public-key-Verfahren

3) gegen Manipulation von Daten:

Autorisierung

- Schreibberechtigung

Authentifizierung

Verschlüsselung bei der Übertragung

- public-key-Verfahren

Abwehrmaßnahmen für verteilte Systeme

1) Firewall

Einziger Zugangspunkt zwischen Außenwelt und Intranet

Zur Kontrolle der eingehenden und ausgehenden Datenströme

- **in erster Linie für Autorisierung zuständig**

Problem:
WLAN, CD / Disketten, unpraktisch für Mitarbeiter im Außendienst

Lösung (teilweise):
Tunneling (Einrichten sicherer Kanäle in definierte Bereiche des Intranets)

Hilfstechniken:
Verschlüsselung auf allen mobilen Kanälen, Smart Cards für mobile Geräte

☹ Verschlüsselung erschwert die Malwareerkennung ☹

Abwehrmaßnahmen für verteilte Systeme

2) Webshield

Zur Kontrolle von eingehender und ausgehender Malware

- **gleich hinter Firewall**

3) Netzsegmentierung

- **Einbau von Zwischen-Firewalls im Intranet**

4) ECO-Server zur Malwareabwehr

- **on-line-Kontakt zu Herstellern von Abwehrprogrammen**
- **verteilt Aktualisierungen an alle Abwehrprogramme im Intranet**

Beispiel einer weiteren Vorsichtsmaßnahme:

e-mails sollten nicht geöffnet werden,
während eine Verbindung im https-Protokoll besteht !

sonst:

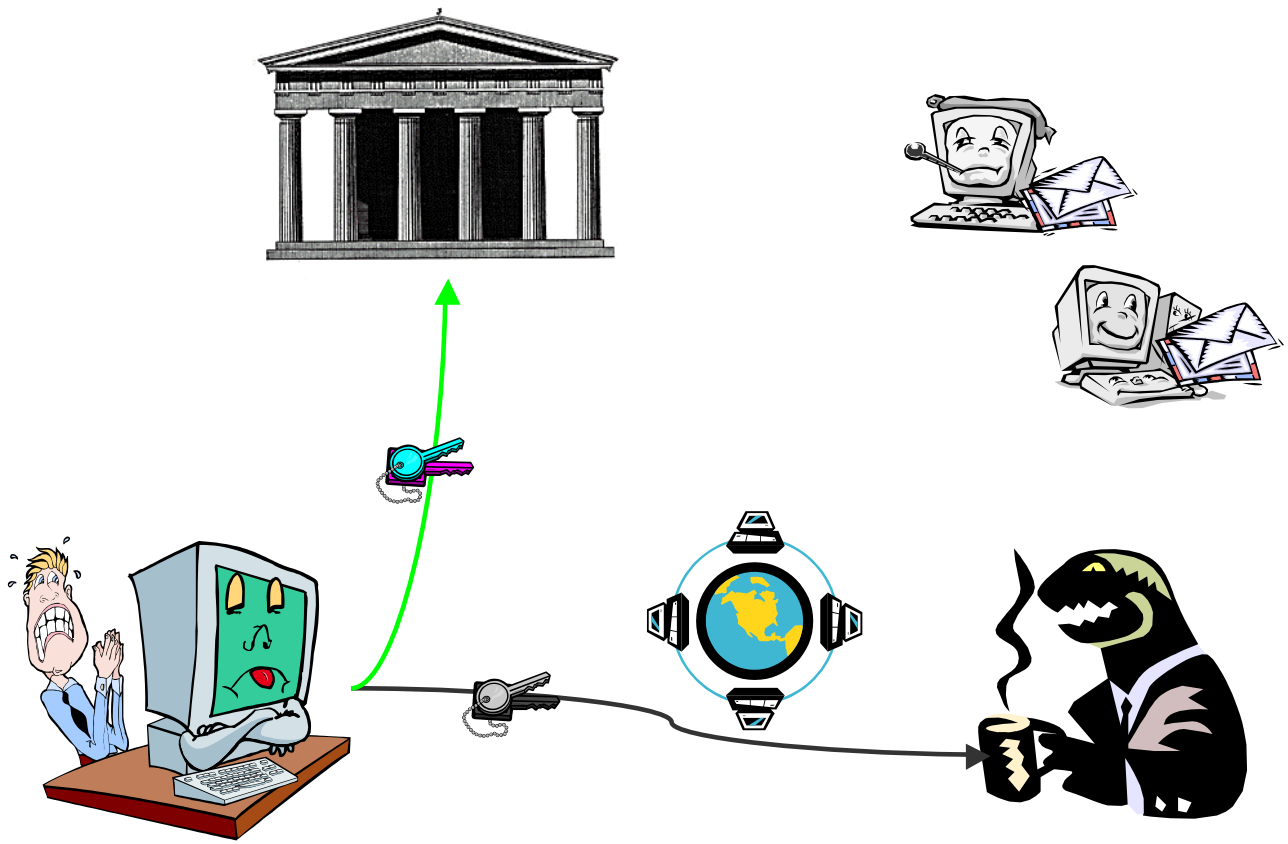

Bild aus Veranstaltung IT-Sicherheit, 17.06.2004, FH Wedel, von Jochen Brunnstein, SQS