Systeme II

13. Vorlesungswoche
14.07. – 18.07.2008

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Christian Schindelhauer
Sommer 2008

1

Systeme II

Sicherheitsrisiken für Netzwerke

2

SANS Institut Top 20 Internet Security Risks

- **Web-Anwendungen**
  - Datendiebstahl und Einbruch in verbundene Rechner der Web-Site
- **Leichtgläubige Computer-Benutzer und Verantwortliche**
  - befolgen falschen Anweisungen in Phishing-Anweisungen
  - Folgen: leere Bankkonten, Geheimnisverrat, Industriespionage, ...

SANS Institut Top 20 Internet Security Risks

- **Sicherheitslücken in Anwendungssoftware**
  - Web-Browser
  - Office Software
  - Email Clients
  - Media Players
- **Sicherheitslücken im Betriebssystemen und Systemsoftware**
  - Windows
  - Unix & Mac OS
  - Backup Software
  - Anti-virus Software
  - Management Softare
  - VOIP Servers

SANS Institut Top 20 Internet Security Risks

- **Eintrittsmöglichkeiten für Malware**
  - Super-User-Rechte
  - Unauthorisierte Geräte
  - Unverschlüsselte Laptops
  - Tragbare Datenträger
- **Nutzermissbrauch durch Software-Gebrauch**
  - Instant Messaging
  - Peer-to-Peer Programme
    - Preisgabe von Information, illegale Aktivitäten
- **Zero-day-Angriffe**
  - Angriffe bevor Patches verfügbar sind

Sicherheitsbedrohungen von Rechnern

CACI (http://www.caci.com/business/ia/threats.html)

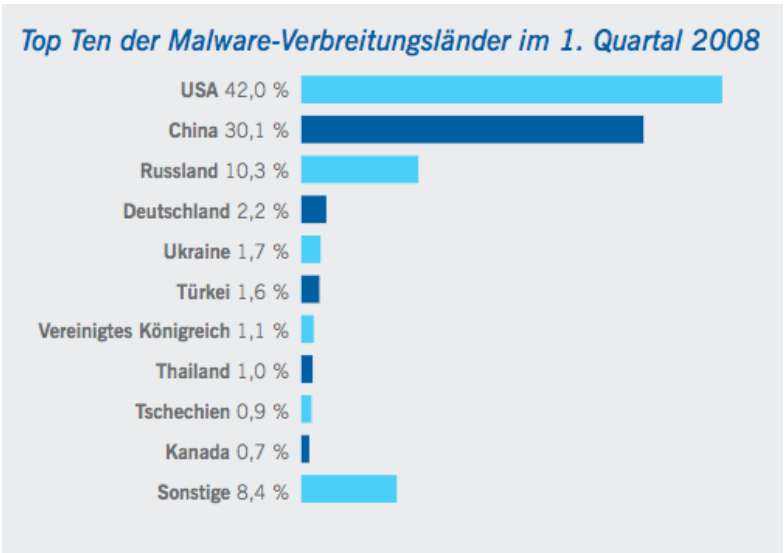
- **Absichtliche Bedrohung**
  - Bösartige Software
    - Virus, Wurm, Trojanisches Pferd, Zeitbombe, logische Bombe, Rabbit, Bacterium
  - Spoofing
    - Spoofing (IP-Klau)
    - Masquerading (Vorspielen einer Benutzer-ID)
  - Scanning (Passwort-Attacke)
  - Abhören
    - digital, physikalisch
  - Scavenging
    - Dumpster Diving, Browsing
  - Spamming (DoS)
  - Tunneln
    - Zugriff auf Low-Level-Systemkomponenten
- **Unabsichtliche Bedrohung**
  - Fehlfunktion
    - Hardware/Software-Fehler
  - Bedienfehler
    - Trapdoor, Benutzer/ Administrator-Fehler
- **Physikalische Bedrohung**
  - Feuer, Wasser, Stromausfall, Aufruhr, Kriegsschaden

Redspin Security Report
Top Ten Netzwerkbedrohungen

- **Schlecht konfigurierte Firewalls**
- **Schlechte Netzwerkkonfiguration**
- **Web-Anwendungen**
- **Remote-Zugang**
- **Vertraulicher Information durch die Eingangstür**
- **Arbeitsplatzrechner im Netzwerk**
- **Social Engineering Bedrohung**
- **Verwechselung von Passwortschutz und Verschlüsselung**
- **Vertrauen in Partnernetzwerke**

Sophos Sicherheitsbericht 1. Quartal 2008

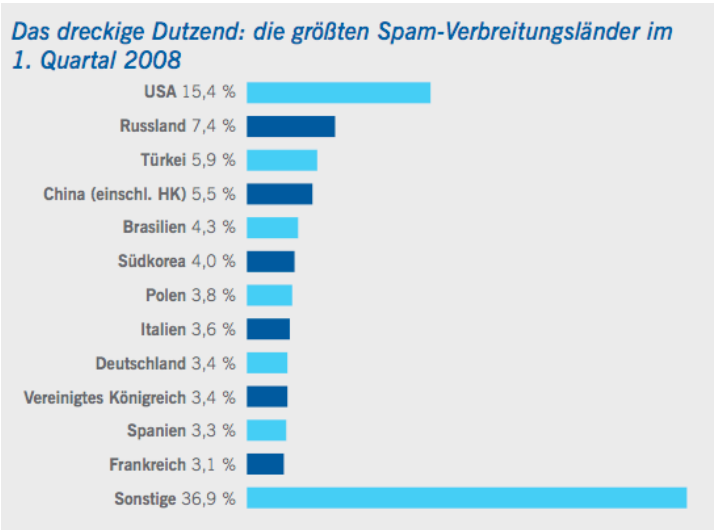
- **Infizierte Web-Seiten**
  - 15.000 Web-Seiten pro Tag
  - dreimal soviel wie 2007
  - 79% von seriösen Websites
  - selbst Websites von Sicherheitsunternehmen
- **Zunehmende Datenverluste**
  - Kundendaten (mit Kreditkarteninformation)
- **Bedrohung von E-Mails**
  - nur noch eine von 2.500 Mails
  - rückläufig: 2007: eine von 900
- **Festnahmen und Verurteilungen**
  - Botnetz-Admistratoren
  - Daten im Wert von 20 Mio. $ gestohlen
- **Malware-Hosts**



http://www.sophos.de/sophos/docs/deu/marketing_material/sophos-threat-report-Q12008de.pdf

Sophos Sicherheitsbericht 1. Quartal 2008

- **Spam**
  - Anteil: 92 % am gesamten E-Mail-Verkehr
- **Phishing**
  - 2007: 59% aller Phishing-Attacken gegen eBay oder PayPal
  - 2008: 15% PayPal, 4% eBay
- **Datenverlust**
  - Supermarktkette Hannaford Bros werden 4,2 Mio Kundenkreditkartennummern gestohlen
  - Advance Auto Parts: Finanzdaten von 56.000 Kunden
- **Neu: Mac-Malware**



http://www.sophos.de/sophos/docs/deu/marketing_material/sophos-threat-report-Q12008de.pdf

Symantec Internet Security Threats
4. Quartal 2007

Current Rank	Previous Rank	Goods and Services	Current Percentage	Previous Percentage	Range of Prices
1	2	Bank accounts	22%	21%	$10–$1000
2	1	Credit cards	13%	22%	$0.40–$20
3	7	Full identities	9%	6%	$1–$15
4	N/A	Online auction site accounts	7%	N/A	$1–$8
5	8	Scams	7%	6%	$2.50/week–$50/week for hosting, $25 for design
6	4	Mailers	6%	8%	$1–$10
7	5	Email addresses	5%	6%	$0.83/MB–$10/MB
8	3	Email passwords	5%	8%	$4–$30
9	N/A	Drop (request or offer)	5%	N/A	10%–50% of total drop amount
10	6	Proxies	5%	6%	$1.50–$30

Table 2. Breakdown of goods and services available for sale on underground economy servers[28]
Source: Symantec Corporation

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

Symantec Internet Security Threats
4. Quartal 2007

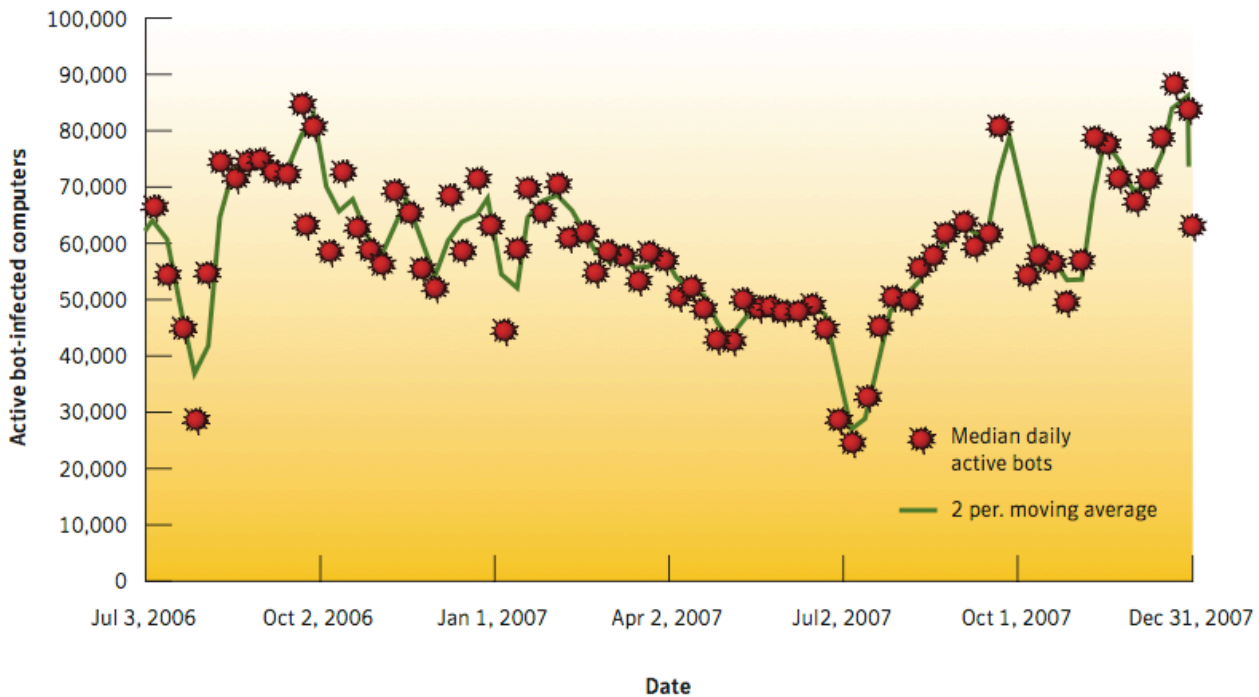


Figure 3. Active bot-infected computers by day
Source: Symantec Corporation

Symantec Internet Security Threats
4. Quartal 2007

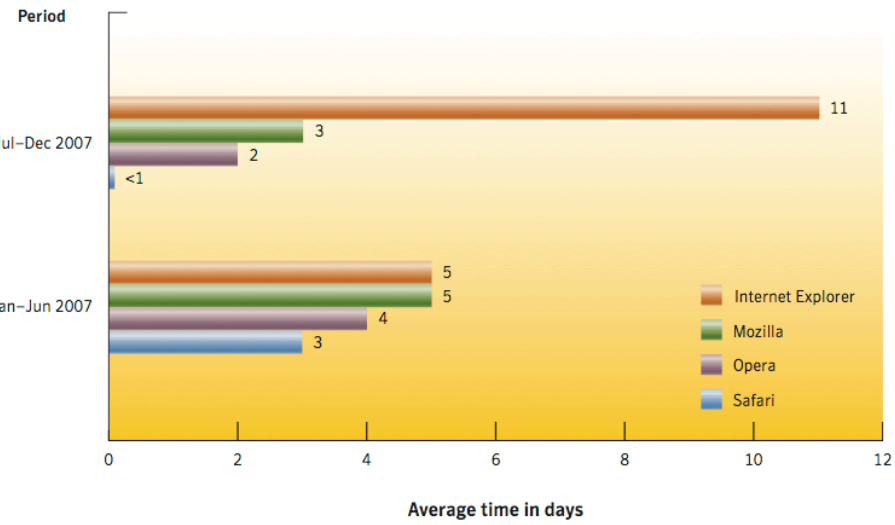


Figure 7. Window of exposure for Web browsers
Source: Symantec Corporation

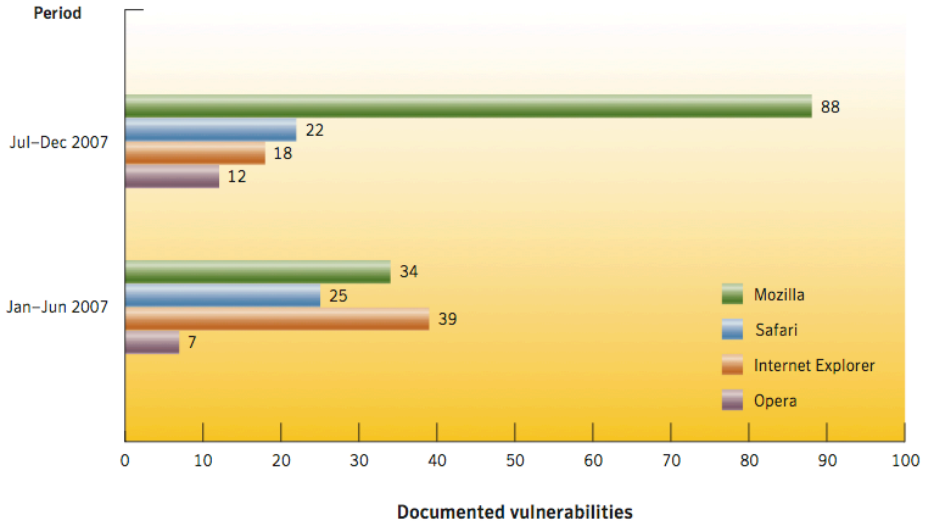


Figure 8. Web browser vulnerabilities
Source: Symantec Corporation

Symantec Internet Security Threats
4. Quartal 2007

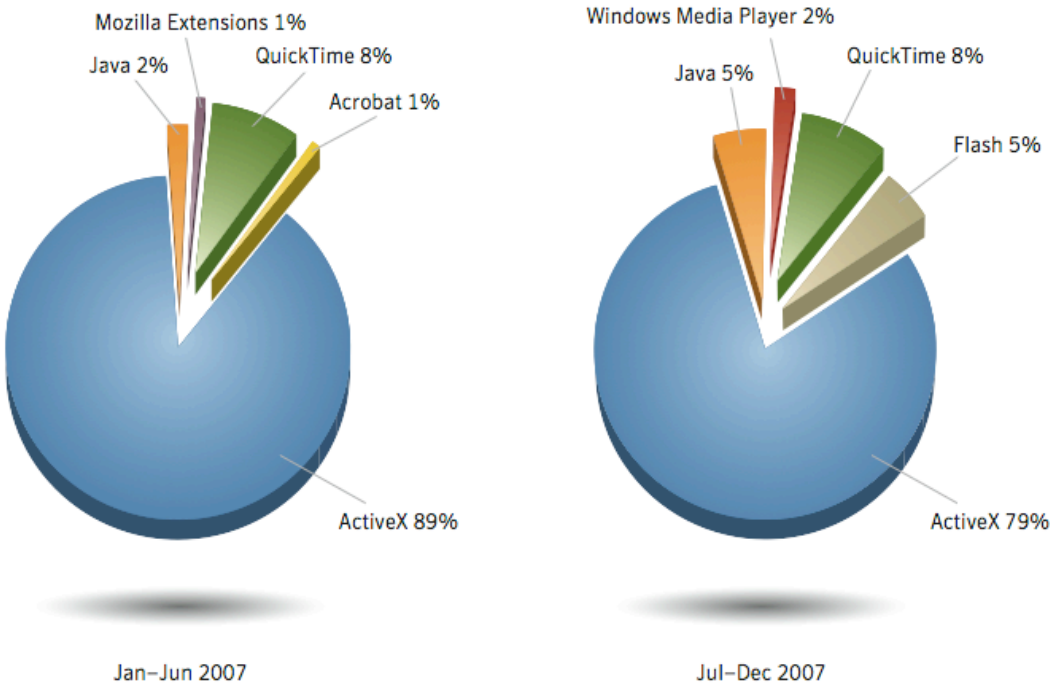


Figure 9. Browser plug-in vulnerabilities
Source: Symantec Corporation

Symantec Internet Security Threats
4. Quartal 2007

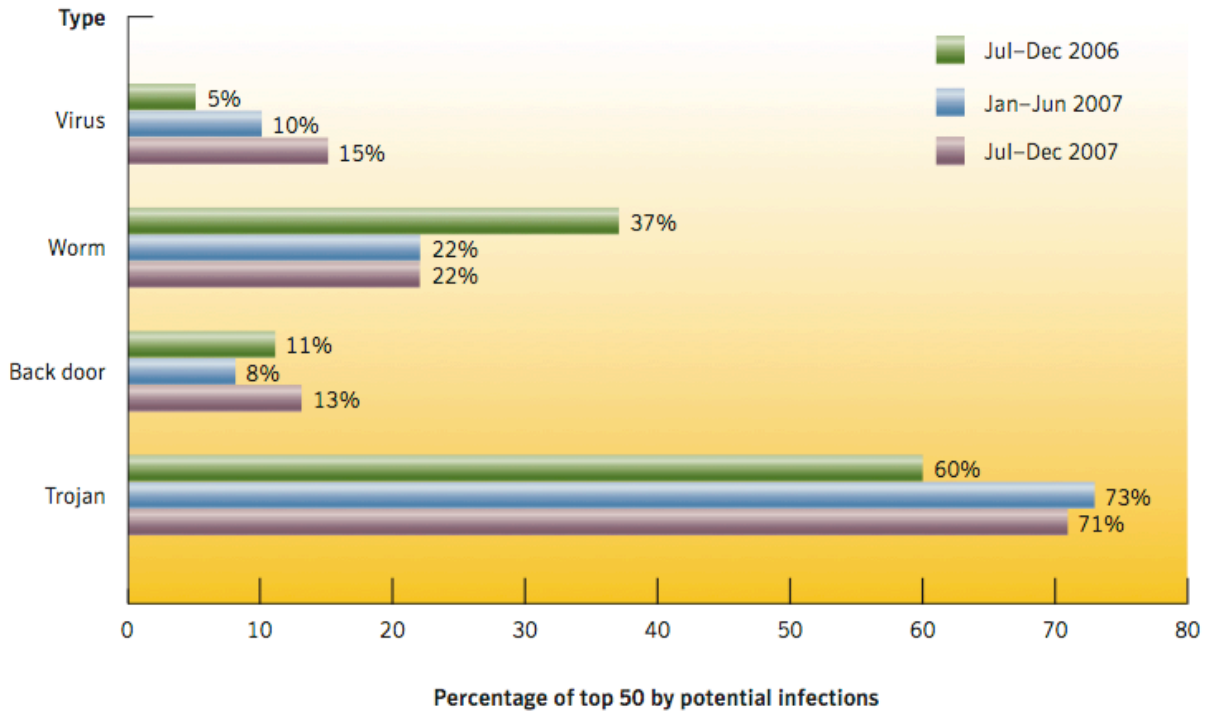


Figure 15. Malicious code types by potential infections
Source: Symantec Corporation

Symantec Internet Security Threats
4. Quartal 2007

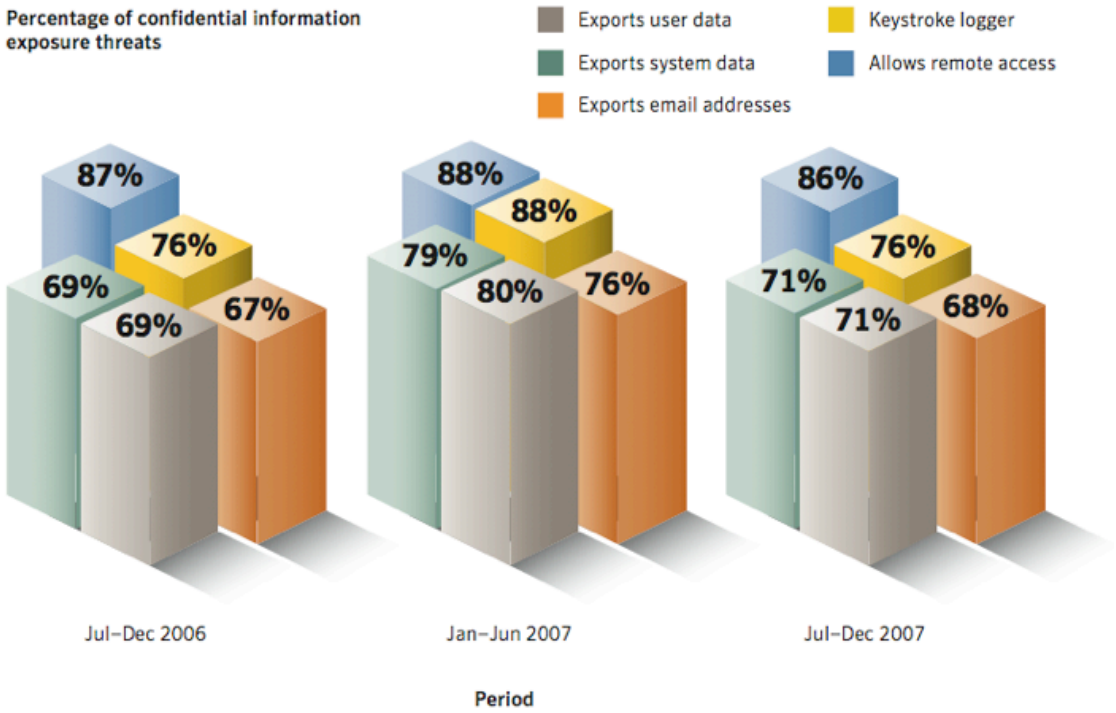


Figure 17. Threats to confidential information by type
Source: Symantec Corporation

Symantec Internet Security Threats
4. Quartal 2007

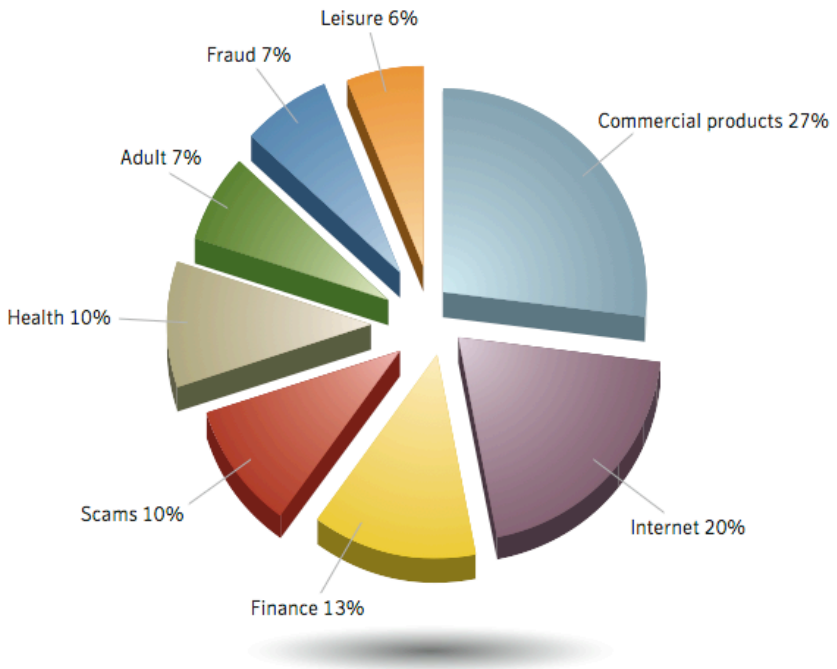


Figure 24. Top spam categories
Source: Symantec Corporation

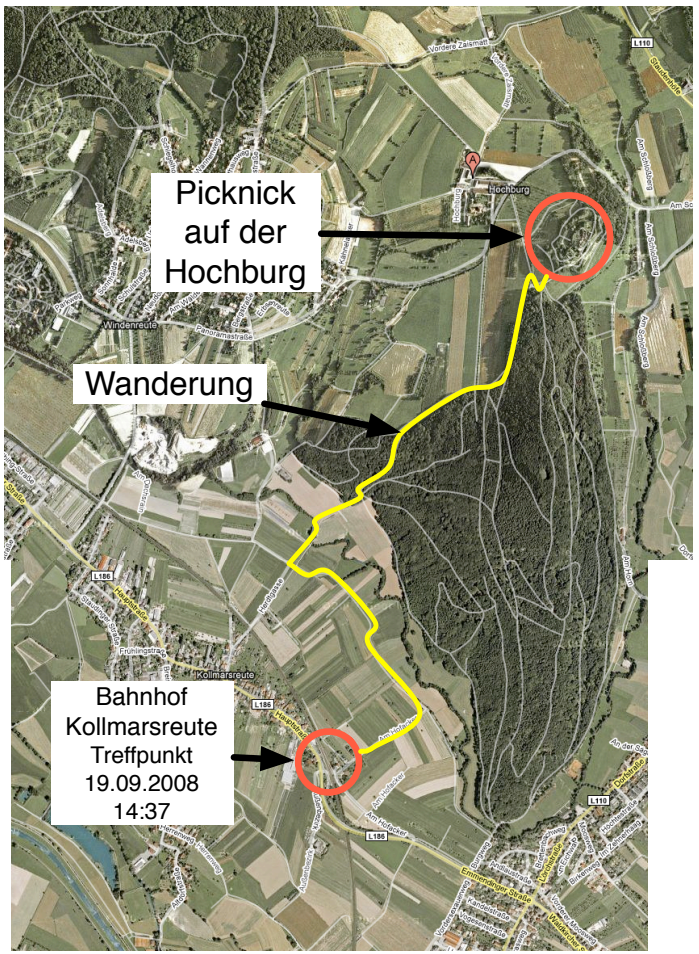
Symantec Internet Security Threats
4. Quartal 2007

Rank	Propagation Mechanism	Current	Previous
1	File sharing executables	40%	14%
2	File transfer/email attachment	32%	30%
3	File transfer/CIFS	28%	15%
4	File sharing/P2P	19%	20%
5	Remotely exploitable vulnerability	17%	12%
6	SQL	3%	<1%
7	Back door/Kuang2	3%	2%
8	Back door/SubSeven	3%	2%
9	File transfer/embedded HTTP URI/Yahoo! Messenger	2%	<1%
10	Web	1%	1%

Table 9. Propagation mechanisms
Source: Symantec Corporation

Picknick auf der Hochburg

- **Freitag 19.09.2008 14 Uhr**
- **Abfahrt 13:56**
  - S-Bahnstation Freiburg-Messe
- **Ankunft 14:37**
  - Bahnhof Kollmarsreute
- **Wanderung auf die Hochburg**
  - Ankuft 16:00
- **Picknick auf der Hochburg**
  - Getränke im Forum bestellen
  - Anlieferung per auto
  - Essen selbst mitbringen
- **Abreise per Wanderung nach Kollmarsreute**



Systeme II

Ende der 13. Vorlesungswoche

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Christian Schindelhauer
Sommer 2008

19