Cybercrime und Cyberwar

Wie sicher ist das Internet?

Thomas Bleier
Dipl.-Ing. MSc zPM CISSP CEH
Program Manager ICT Security
Safety & Security Department, AIT Austrian Institute of Technology GmbH

thomas.bleier@ait.ac.at | +43 664 8251279 | www.ait.ac.at/it-security

AIT Austrian Institute of Technology

- Österreichs größtes außeruniversitäres Forschungszentrum
- Fokussiert auf die Infrastrukturen der Zukunft

- **Safety & Security Department:**
  Sicherstellung der Effizienz und Zuverlässigkeit kritischer Infrastrukturen, Entwicklung und Bereitstellung zukunftsweisender Technologien

Das Problem…

- Die Komplexität von IT-Systemen steigt ständig
  - Mondlandung mit 7.500 Lines of Code
  - Heute: F-35 fighter jet: 5,7 Mio; Boeing 787: 6,5 Mio; Mercedes S-Klasse: 20 Mio; Chevrolet Volt: 100 Mio.
- Systeme werden immer mehr vernetzt
  - Internet-of-Things, Always-on, Pervasive Computing
  - M2M (Machine-to-Machine) Communication
  - Virtual Infrastrucutures (Cloud), etc.
- Industrietrend hin zu offenen Netzwerkarchitekturen
  - Offene Protokolle (e.g. All over IP)
  - Höhere Anzahl an „third parties“
- Die Abhängigkeit von IKT Systemen steigt
  - Smart Grid, Smart Home, Smart City, Smart Phone
  - eGovernment, eCommerce, eHealth, eMobility

Mehr Sicherheits-lücken

Höheres Risiko

Größere Auswirkungen

ICT Security Research @ AIT

- **Forschungsthemen**
  - Security Engineering of large and complex systems
  - Facilitating Security by Design
  - National Cyber Defense
  - Efficiently security large-scale service-oriented architectures
  - Cloud Computing for high-assurance applications
  - Security and Risk Management for Smart Grids and Critical Infrastructures
  - Next Generation Key Management for Encryption

Tools, Methodologies

+

Application Domains

=

Secure Systems

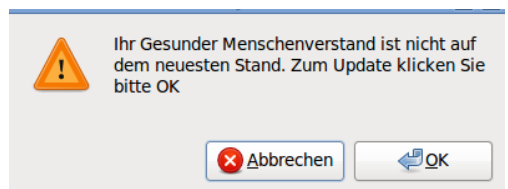
Standortbestimmung / Questionnaire

- Botnet
- Zero-Day

Die gute und die schlechte Nachricht…

Es gibt nichts was es nicht gibt!

Der erste Schutz ist der gesunde Menschenverstand!



Eine kurze Geschichte der Cyberkriminalität…

- 1969
  Start des ARPANET mit 5 Rechnern
- 1971
  Creeper - erste selbstreproduzierende Software
- 1972
  Captain Crunch – Phreaking –„Injection“ Attacken
- 1979
  Kevin Mitnick hackt Digital Equipment Corp.
- 1981
  Elk Cloner – erster Virus „in the wild“ auf Apple][
- 1987
  Stoned – weit verbreiteter Virus auf IBM PC‘s

Eine kurze Geschichte der Cyberkriminalität…

- 1988
  Morris – Wurm verbreitet sich im Internet
- 1999
  Melissa – Makrovirus, Verbreitung per E-Mail
- 2000
  Mafiaboy – Denial-of-Service – Yahoo, Amazon, ...
- 2000
  I Love You – Millionen von PC‘s infiziert
- 2001
  NIMDA – fünf verschiedene Infektionswege
- 2004
  Sasser – Firmen im Betrieb gestört

Eine kurze Geschichte der Cyberkriminalität…

- 2007
  Storm Worm – Botnet (1-10 Mio PC‘s)
- 2007
  Cyber-Angriffe auf Estland
- 2008
  Torpig – Rootkit, stiehlt Passwort, schaltet AV aus
- 2008
  Conficker – Online-Update, 9-15 Mio PC‘s infiziert
- 2009
  Aurora – Cyber-Spionage bei Google & Co.
- 2010
  Stuxnet – eine neue Kategorie von Malware

Aktuelle Vorfälle

- Anonymous „hackt“ BMI-Mail-Account *[1]*
- Twitter-Account von Nachrichtenagentur AP gehackt *[2]*
- Apple und Facebook Entwickler-PC‘s gehackt *[3]*
- Darkleech infiziert reihenweise Apache-Server *[4]*
- „Global internet slows after ‚biggest attack in history‘“ – Spamhaus DDoS [5]
- Emissionsrechtehandel wird aus Angst vor Trojaner ausgesetzt *[5]*
- …

[1] http://derstandard.at/1363708671942/Anonymous-veroeffentlicht-weitere-BMI-Mails-mit-Zugangsdaten
[2] http://www.heise.de/security/meldung/Twitter-Account-der-Nachrichtenagentur-Associated-Press-gehackt-1848272.html
[3] http://www.zdnet.com/apple-facebook-employees-hacked-via-website-malware-java-vulnerability-7000011601/
[4] http://www.heise.de/security/meldung/Darkleech-infiziert-reihenweise-Apache-Server-1833910.html
[5] http://arstechnica.com/security/2013/03/spamhaus-ddos-grows-to-internet-threatening-size/
[5] http://www.emissionshandelsregister.at/service/recent_info/items/news132.html

Warum macht jemand sowas?

- Technische Spielereien
- Beweisen was machbar ist
- Selbstdarstellung
- Wettkämpfe, Rivalitäten

Heute geht es um Geld!!!

Aktuelle Preisliste

Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 5. Goods and services advertised on underground economy servers
Source: Symantec

Quelle: Symantec Global Internet Security Threat Report XV, April 2010

Beispiel: Russian Business Network

- 150 Mio. Dollar Umsatz pro Jahr [1]

- Spam
- Malware
- Phishing
- Bulletproof hosting
- etc.

[1] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2844031.ece

Ausmaß der organisierten Cyberkriminalität

- Genaue Informationen schwer ermittelbar
- Umsatz wird auf 1 Milliarde US$ pro Jahr geschätzt [1]
- In ähnlichen Größenordnungen wie Drogenkriminalität
- Jährlich 750 Mrd. Euro Schaden weltweit (Europol [2])

- Für mehr Infos zum Cybercrime-Businessmodell: http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/wp04_cybercrime_1003017us.pdf

[1] http://www.scmagazineuk.com/cyber-crime-is-a-lucrative-trade-and-its-growing/article/178317/

[2] http://derstandard.at/1293369927261/Europol-750-Mrd-Euro-Schaden-pro-Jahr-weltweit-durch-Cybercrime

Herkunft der Malware

Overall Rank 2009	Overall Rank 2008	Country	Percentage 2009	Percentage 2008	2009 Activity Rank: Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

Table 1. Malicious activity by country
Source: Symantec Corporation

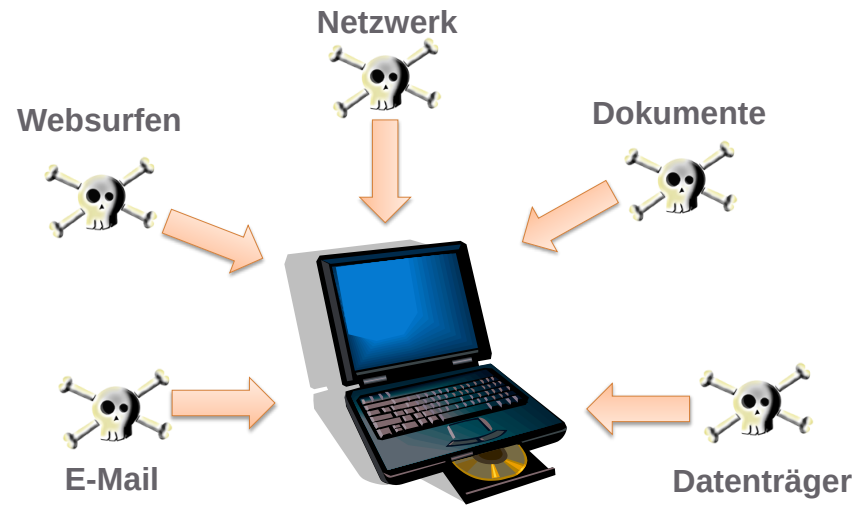
Quelle: Symantec Global Internet Security Threat Report XV, April 2010

Weitere Motive

- Spionage – Industrie, Wirschaft, Militär
  - NASA, Sandia National Labs, etc. – 2003 (Titan Rain) [1]
  - Google, Adobe, Juniper, etc. - 2009 (Aurora) [2]
  - Österreichisches Außenministerium, 2010 [3]
- Cyberwar
  - Estland, 2007 [3]
  - USA, Südkorea 2009 [4]
- **Die Technologie ist die gleiche…**

[1]http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html
[2]http://www.zdnet.de/sicherheits_analysen_aurora_angriff_mit_ie_exploit_aus_china_auf_google_und_den_rest_der_welt_story-39001544-41525729-1.htm
[3]http://kurier.at/nachrichten/2037711.php
[4]http://www.guardian.co.uk/world/2007/may/17/topstories3.russia
[5]http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm

Wie kommt das Zeug auf meinen PC?

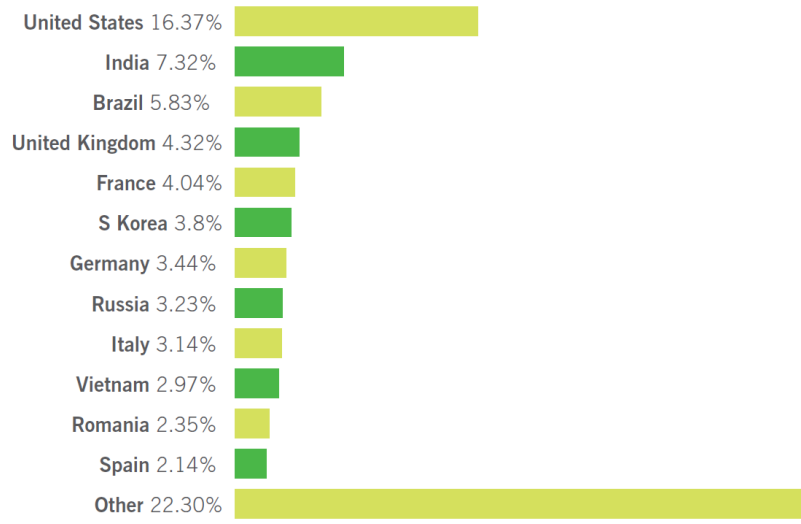


Was für Arten von Schadsoftware bzw. Angriffen gibt es derzeit?

- Spam
- Viren
- Trojaner, Adware, Spyware
- Scareware
- Drive-by Downloads
- Exploits, Zero-Day
- Phishing
- Rootkits
- Botnetze

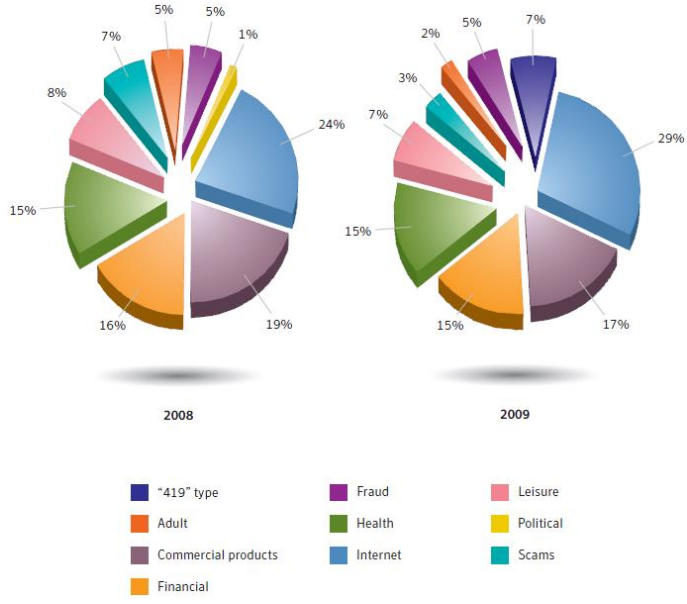
Spam

Spamversender nach Land



Quelle: Sophos Security Threat Report 2011

Spam - Inhalte



Quelle: Symantec Global Internet Security Threat Report XV, April 2010

Spam - Inhalte

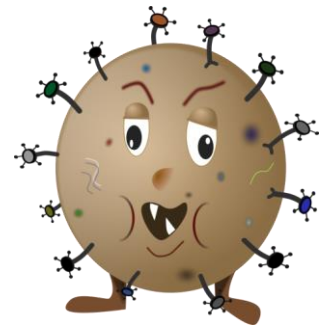
- „Angebote“
  - Die „blaue Pille“ besser nicht beim Spam-Händer kaufen
- Viren
  - I Love You
  - AnnaKournikova.jpg.vbs
- Trojaner
  - FBI / Bundeskriminalamt
  - Rechnungen

Spam - Inhalte

- Phishing
  - eBay, Paypal
    „Bitte aktualisieren Sie Ihre Account-Daten“
  - Online-Banking
  - etc.
- Betrug
  - Nigeria Connection
  - Penny Stocks
  - Money mules

Computervirus

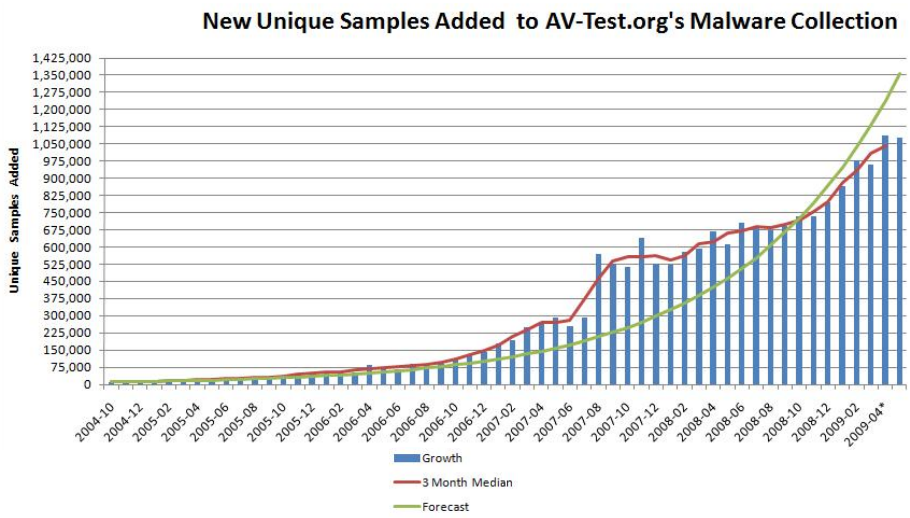
- Software, die sich in einem „Wirtsprogramm“ einnistet und so weiterverbreitet
- Diskette / Bootsektor
- Applikationsprogramm
- Dokument (Word, Excel, OpenOffice)
- USB-Stick



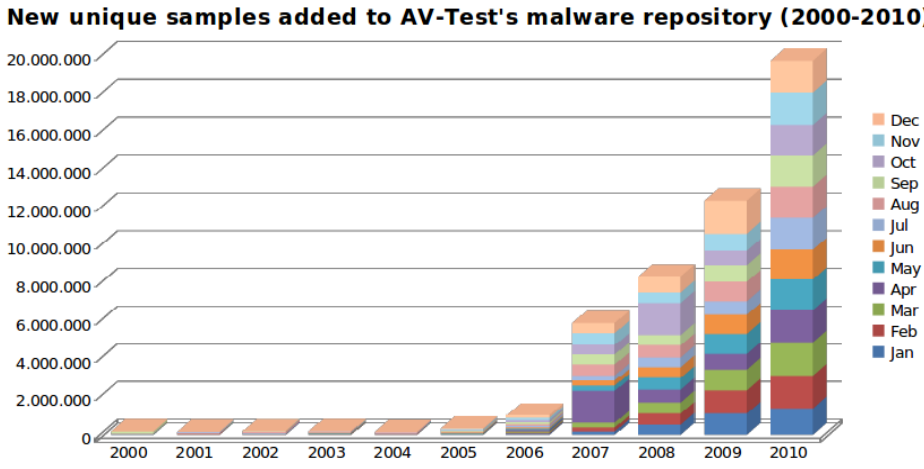
Antivirensoftware

- Zeitpunkt der Analyse
  - On-Access Wächter
  - On-Demand Scan
  - Virencheck am Mail-Gateway bzw. Web-Gateway
- Art der Erkennung
  - Signaturbasierte Erkennung – Updates!!!
  - Heuristischer Ansatz
  - Verhaltenserkennung

Anzahl der neuen Virensignaturen pro Monat!



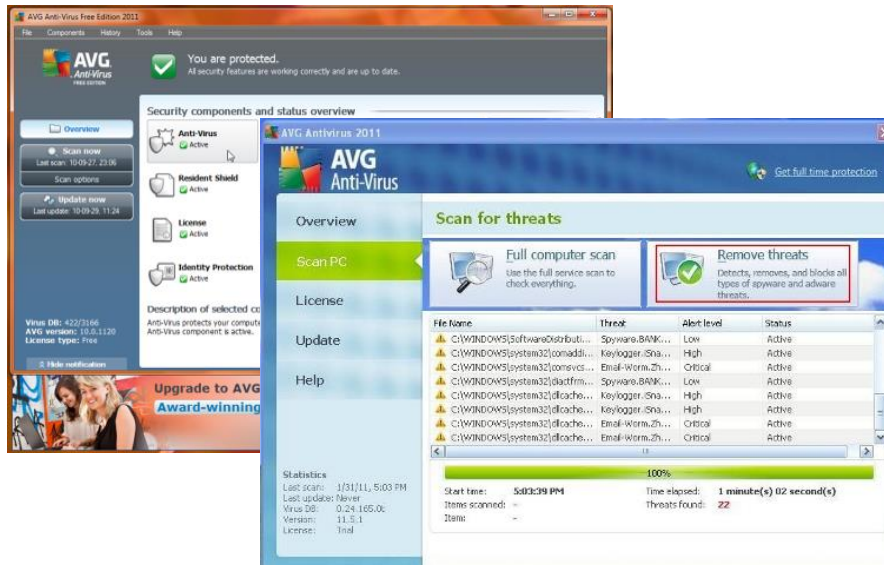
50 Mio. Viren (Jan. 2011)



Antivirus-Tools

- Diverse Hersteller - http://www.av-test.org/
- ClamAV: http://www.clamav.net/lang/en/
- Für Windows-VM‘s ☺:
  - Microsoft Security Essentials: http://www.microsoft.com/security_essentials/
  - AVG Free Antivirus: http://free.avg.com/de-de/startseite
- McAfee Stinger: http://vil.nai.com/vil/stinger/
- Virustotal: http://www.virustotal.com/
- Anubis: http://anubis.iseclab.org/

Vorsicht: Fake-AV

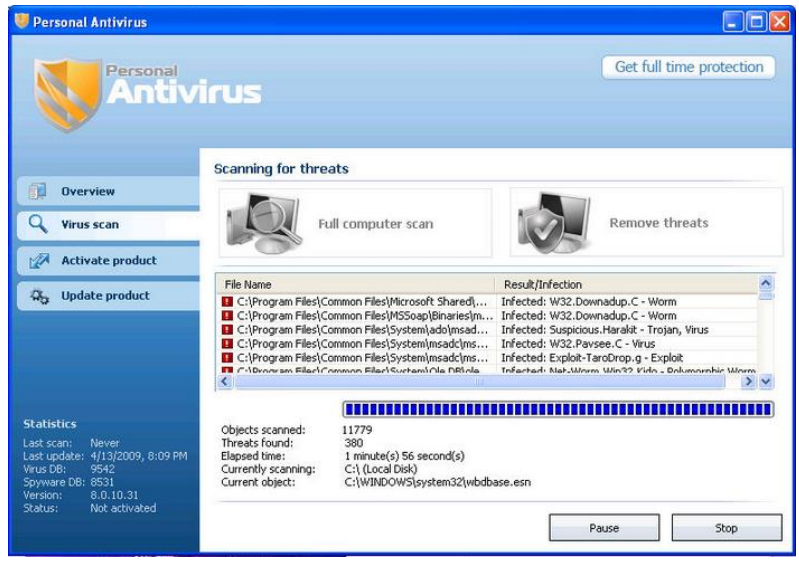


Trojaner/Adware/Spyware

- Ein Programm, das etwas anderes macht als gedacht

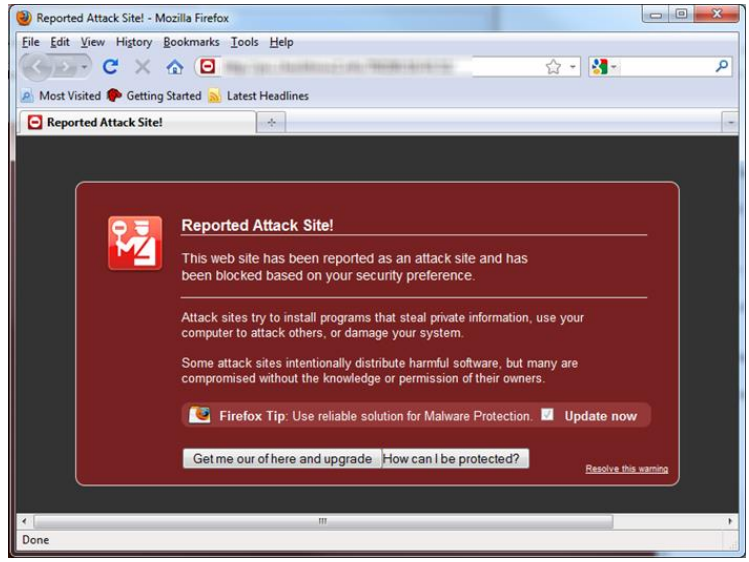
- Adware: Werbung (Desktop, Popups, etc)
- Spyware: ausspähen persönlicher Informationen (E-Mail-Adressen, Passwörter, Bildschirminhalte, etc.)
- Dialer: anrufen kostenpflichtiger Nummern
- Ransomware: Erpressung

Scareware

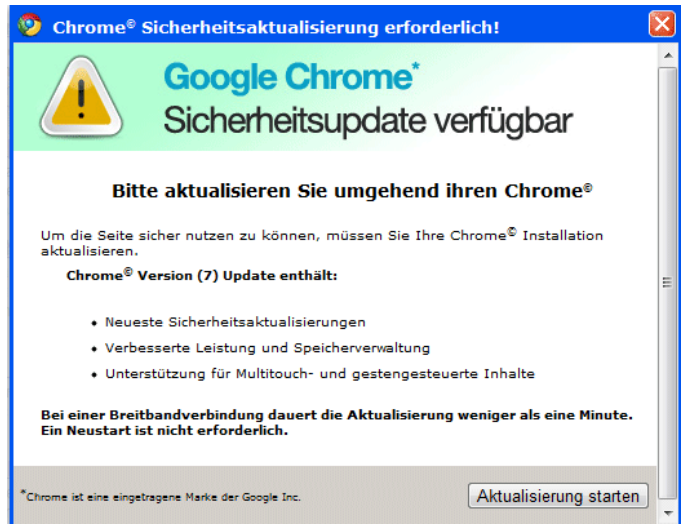


Scareware

Scareware



Scareware



Dieses Geschäftsmodell funktioniert!

- Innovative Marketing: [1]
  - Umsatz 2008: 180 Mio. USD
  - Umsatz 2010: 300 Mio. USD
- Der Entwicklungsaufwand hält sich in Grenzen
- Marketingbudget ist vorhanden…

[1] http://www.scmagazineuk.com/cyber-crime-is-a-lucrative-trade-and-its-growing/article/178317/

Drive-by download / Drive-by install

- Unbemerktes herunterladen bzw. installieren von Schadsoftware beim Surfen im Internet
- Durch Ausnützen eines Softwarefehlers in
  - Web-Browser
  - Browser-Plugins (Flash-Player, Quicktime, Java, etc.)
  - Betriebssystem (WMF)
- Auch unter Linux: xpdf, etc.

Schwachstelle Browser-Plugins

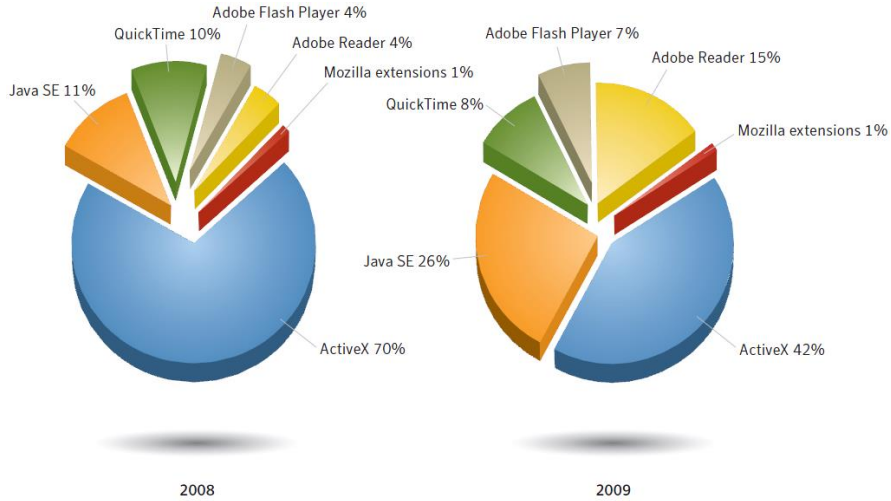
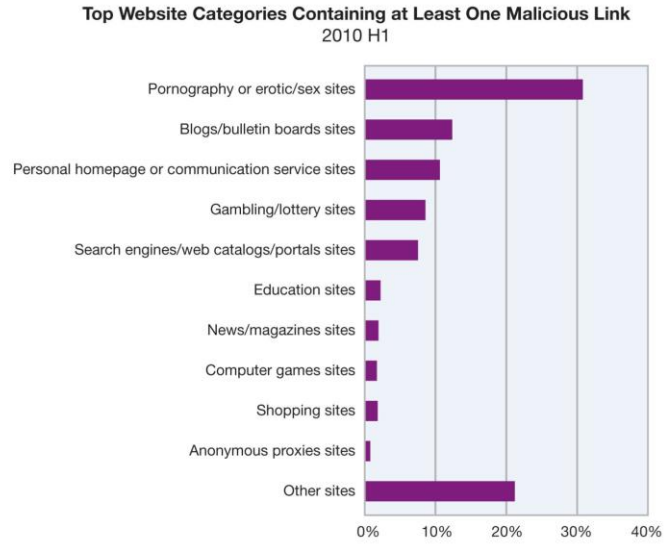


Figure 9. Web browser plug-in vulnerabilities
Source: Symantec

Gefährliche Webseiten



Source: IBM X-Force®

Nur „Vertrauensvolle“ Seiten besuchen?

Kein Schutz vor Drive-by-Downloads!

- gehackte Webseiten
- benutzergenerierter Content (Foren, etc.)
- Inhalte von Drittanbietern

- Dezember 2010:
  Google und Microsoft verteilen Malware [1]
  - Ad-networks der Unternehmen ausgetricks
  - Schadsoftware für kurze Zeit auf Drittseiten platziert
  - Führte zu Scareware-Download

- [1]http://www.computerworld.com/s/article/9200899/Google_Microsoft_ad_networks_briefly_hit_with_malware

„Manueller“ Drive-By

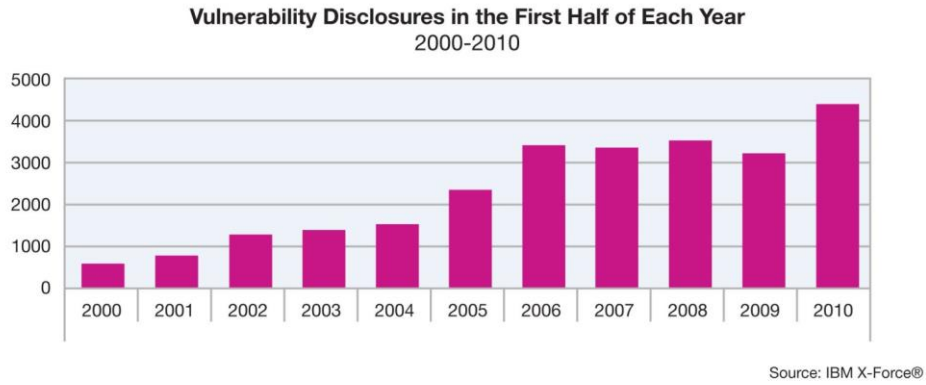
- Auch ohne direktes Ausnützen einer Software-Schwachstelle kann man Schabernack treiben…

- Demo

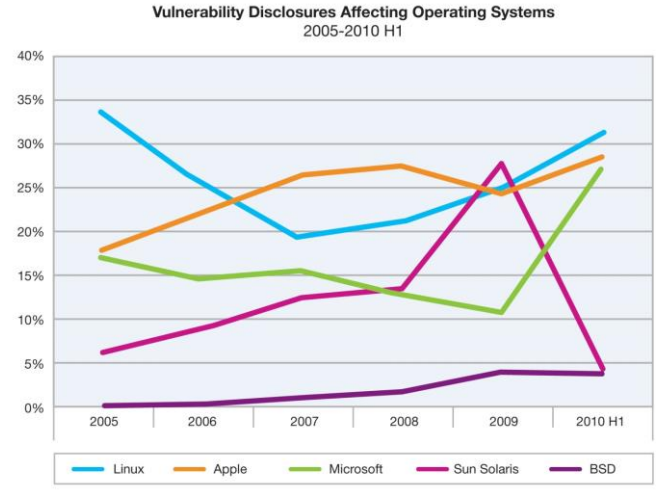
Exploits, Zero-Day-Exploits

- Fehler in der Software sind für einen Großteil der Sicherheitsprobleme verantwortlich
- Ein „Exploit“ ist eine Anleitung, um einen solchen Fehler auszunützen und eigene Programmroutinen auszuführen
- „Zero-Day-Exploits“ sind Fehler, die dem Hersteller der Software noch nicht bekannt sind, und wo es daher kein Update zur Behebung gibt

Anzahl der neuentdeckten Schwachstellen in Software

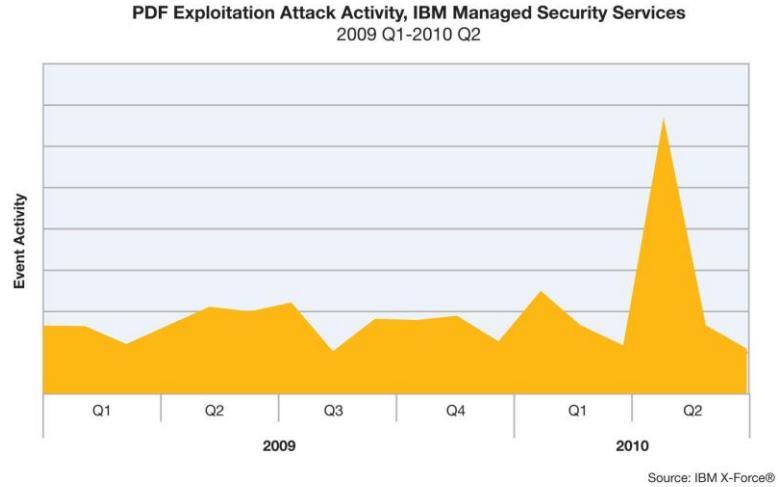


Schwachstellen in den Betriebssystemen



Source: IBM X-Force®

PDF / Adobe Acrobat Schwachstellen



Source: IBM X-Force®

Was tun als Anwender?

- Updates, Updates, Updates…
- Automatisches Update des Betriebssystems
- Ev. Updatefunktionen der Anwendungssoftware
- Manuelle Updates
- Mozilla Plugin-Check
  https://www.mozilla.org/de/plugincheck/
- Windows: Secunia Personal Software Inspector
  http://secunia.com/vulnerability_scanning/personal/

Phishing

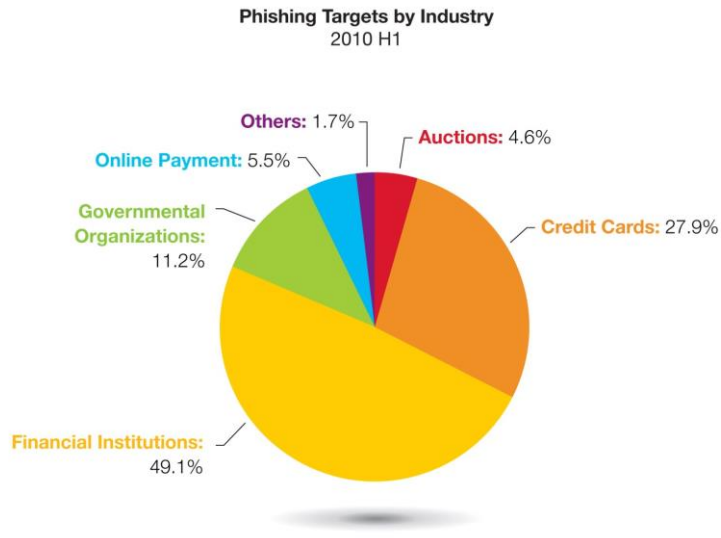
- „Fischen“ nach sensiblen Informationen (Passwörter, Kreditkartendaten, etc.)
- Identitätsdiebstahl
- Spear Phishing: gezielte Attacken auf bestimmte Personen/Firmen
- Whaling ☺

Techniken beim Phishing

- E-Mail mit manipulierten Links
  - http://www.ebay.abc.com
  - Unterschiedlicher Text und Link-URL
- Domain Squatting
- Cross-site scripting
- Trojaner manipuliert PC

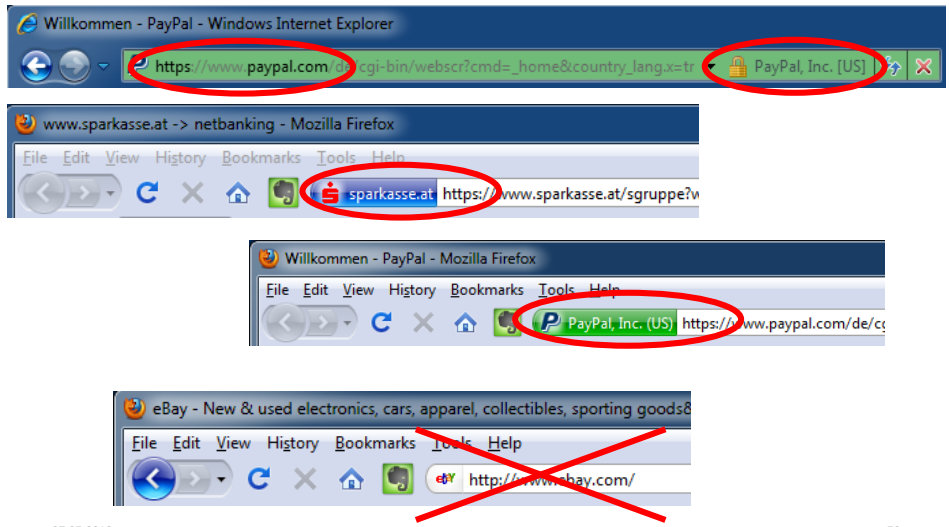
→ gefälschte Webseiten fragen Daten ab (Passwort, Kreditkarte, etc.)

Ziele der Phishing-Attacken



Source: IBM X-Force®

Verschlüsselung und Zertifkate



Rootkits

- Software, die einem Angreifer vollständigen Zugriff auf den PC gibt
- Außerdem wird die Existenz der SW versteckt
- Heute häufig in Verbindung mit anderer Schadsoftware
- Sony BMG DRM rootkit
- Linux-Rootkit manipuliert SSH-Bibliothek libkeyutils: http://www.heise.de/security/meldung/Linux-Rootkits-missbrauchen-SSH-Dienst-1810406.html

Verschiedene Arten von Rootkits

- User-mode Rootkit
- Kernel-mode Rootkit
- Virtualization Rootkit
  - Blue Pill
- Bootloader Rootkit / Bootkit
  - Evil Maid Attack
- Hardware/firmware Rootkit

Botnetze

- Ein Netzwerk von PC‘s, das unter der Kontrolle eines dritten Aktionen ausführt
- Schadsoftware wird auf dem PC aktiv
- Hinterlässt einen „Agenten“ (Bot), der im Hintergrund arbeitet
- Kommuniziert regelmässig mit seinem „Meister“, um neue Befehle, Updates, etc. nachzuladen

Dimensionen von Botnets

- 2005: Botnet mit 1,5 Millionen PC‘s [1]
- Mariposa: 12 Millionen PC‘s [2]
- Conficker: 10 Millionen PC‘s [3]
- Zeus: 3,6 Millionen PC‘s [4]
- „Bis zu einem viertel der PC‘s im Internet“ [5]
- ENISA-Studien [6] [7]

[1] http://www.v3.co.uk/vnunet/news/2144375/botnet-operation-ruled-million
[2] http://www2.canada.com/topics/technology/story.html?id=3333655
[3] http://www.f-secure.com/weblog/archives/00001584.html
[4] http://www.networkworld.com/news/2009/072209-botnets.html
[5] http://news.bbc.co.uk/2/hi/business/6298641.stm
[6] http://www.enisa.europa.eu/act/res/botnets/botnets-10-tough-questions
[7] http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

„Anwendungsbereiche“ für Botnets

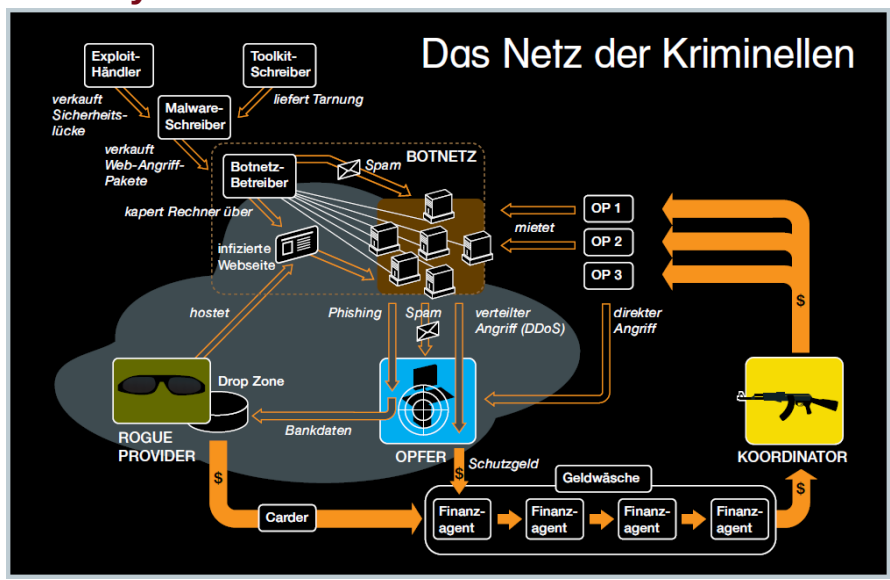
- Versenden von SPAM-Mails
  - 1,5 Millionen PC‘s versenden 1 Mail pro Minute…
- Distributed Denial-of-Service Attacken
  - 10.000 PC‘s mit ADSL (1 Mbit/s) → 10 Gbit/s
  - 1,5 Mio PC‘s mit 1 Mbit/s → 1.500 Gbit/s!!!
- Click fraud – Google Adwords, etc.
- Sammeln von E-Mail-Adressen, Passwörtern, Kreditkartendaten, etc.

Untersuchung von Botnets

- Torpig-Botnet wurde für 10 Tage von einem Forscherteam der UCSB übernommen [1]
- Ergebnis:
  - 54.090 Mailbox Account Daten (Outlook, Thunderbird, Eudora)
  - 1.258.862 E-Mail Adressen
  - 11.966.532 Datensätze aus Formularen inkl. URL‘s
  - 411.039 Webserver-Accounts
  - 415.206 POP Mail-Accounts
  - 1.235.122 Windows-Passwörter
  - …
- Zeus Tracker: https://zeustracker.abuse.ch/

[1] http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf

Die Cybercrime-Industrie



Quelle: Heise Technology Review April 2008

Schutzmaßnahmen

Gesunder Menschenverstand

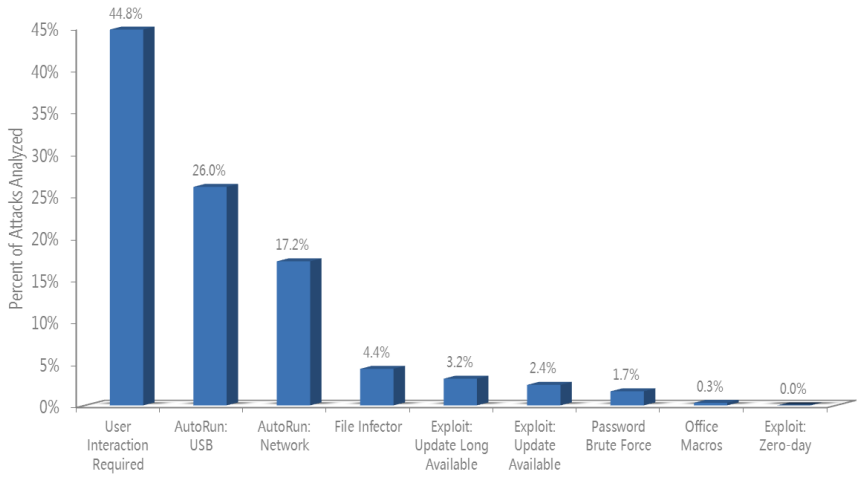
Information und Weiterbildung

Awareness und Vertrauen

Technische Maßnahmen

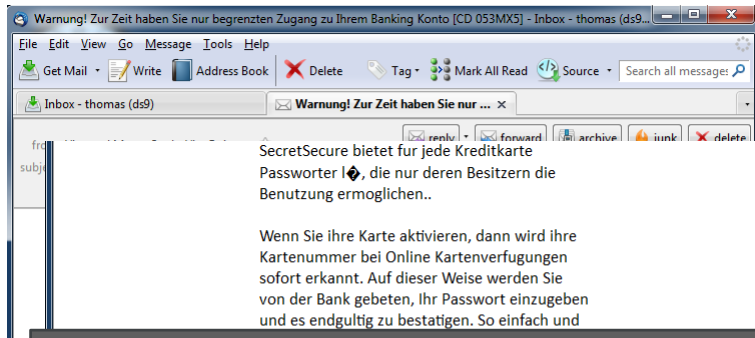
Infektionswege

- Fast die Hälfte aller Infektionen erfolgen mit „Mithilfe“ des Benutzers



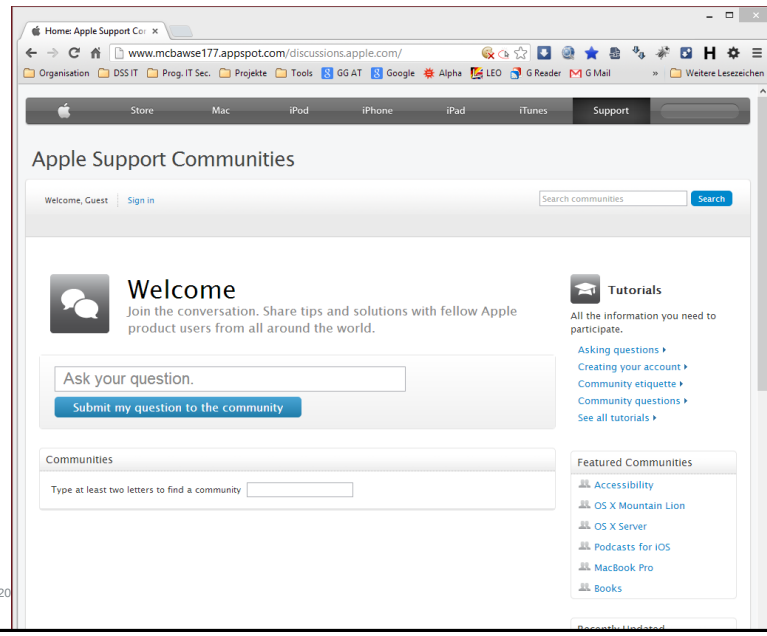
Quelle: Microsoft Security Intelligence Report 2011, Daten aus 1. HJ. 2011, http://www.microsoft.com/security/sir/default.aspx

Gesunder Menschenverstand



http://www.visa.at.de.visa-und-mastercard.bankkonto.verified.by.visa.gibt.ihnen.5zusatzlichen.schutz.und.seelenfrieden.wenn.sie.online.durch.einfuhrung.einer.neuen.sicherheit.secure.code.sicherheit.hawaiicoffeeandtea.com/.https-/Visa-AT/

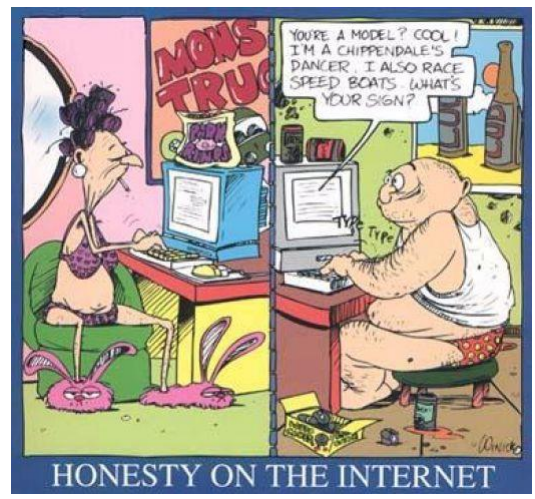
Nicht immer so offensichtlich…



Informationsquellen

- Saferinternet.at: http://www.saferinternet.at/
- Heise Online News / Heise Security
  http://www.heise.de/newsticker/
  http://www.heise.de/security/
- CERT AT: http://www.cert.at/
- Bürger-CERT: https://www.buerger-cert.de/
- SANS: http://www.sans.org/

Awareness - Vertrauen

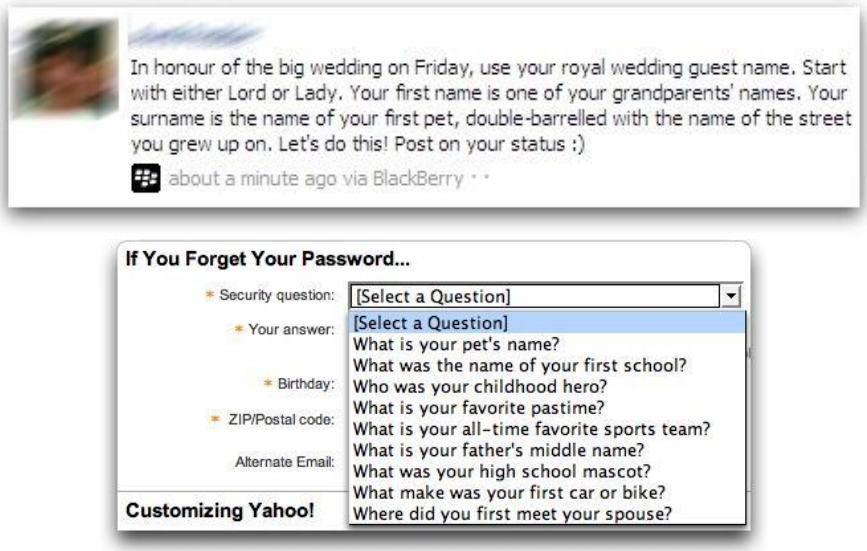


Awareness und Social Networks

- „Getting in Bed with Robin Sage“ [1]
  - 28 Tage Experiment von Thomas Ryan
  - Fiktiver Account auf Facebook, LinkedIn, Twitter, etc.
  - „Friend“ von 300 Personen in der IT Security Industrie, inklusive NSA, DoD, etc.
- YourOpenBook: http://youropenbook.org/
- Please Rob Me: http://pleaserobme.com/

[1] http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
[2] http://www.krone.at/Digital/Cyberkriminelle_nehmen_verstaerkt_Firmen_ins_Visier-Mehr_zu_holen-Story-224374

„Royal Wedding Guest Name“



Technische Schutzmaßnahmen

- Filter – Antivirus, Firewall, etc.
- Updates!
  - Betriebssystem
  - Webbrowser, E-Mail-Client
  - Browser-Plugins
  - Anwendungsprogramme – Office, PDF
- Intrusion Detection / Intrusion Prevention Systeme
- …

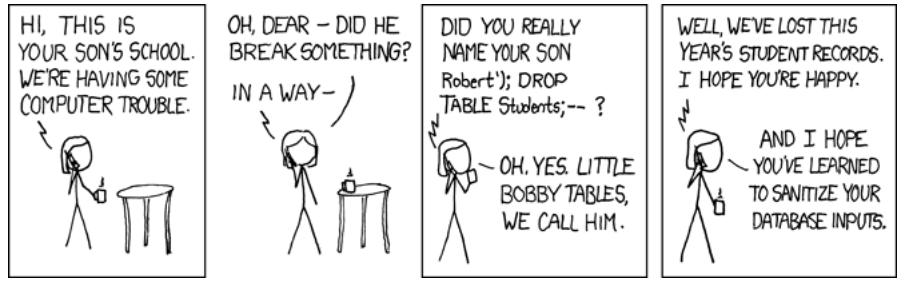
Ein Trend in der Zukunft: Mobile Schadsoftware?

- Talking Tom [1]
- Android Market - über 50 infizierte Apps entfernt [2]
- Soundminer [3]
- Smartphone Keylogger via Accelerometer [4]
- Zeus und SpyEye mit Android-Modul [5]

[1] http://www.heise.de/ct/artikel/Inkasso-auf-Fingertipp-1102753.html
[2] http://www.heise.de/security/meldung/Google-entfernt-ueber-50-infizierte-Apps-aus-dem-Android-Market-1200662.html
[3] http://www.cs.ucdavis.edu/~hchen/paper/hotsec11.pdf
[4] http://www.airdemon.net/soundminer-nds.pdf
[5] http://threatpost.com/en_us/blogs/zeus-banking-trojan-comes-android-phones-071211

Sicherheit ist ein kontinuierlicher Prozess

- Es reicht nicht, ein System sicher zu machen, man muss es auch sicher halten!
- Gerade in diesem Moment werden Methoden entwickelt, die derzeit sichere Systeme angreifbar machen, über Wege, an die bisher niemand gedacht hat…



Quelle: „Exploits of a Mom", http://xkcd.com/327/

Sicherheit kostet etwas

Sicherheit ⟺ **Bequemlichkeit**
Funktionalität
Geschwindigkeit

Der richtige Mittelweg ist wichtig!

Danke für die Aufmerksamkeit!

Fragen?

Thomas Bleier
Dipl.-Ing. MSc zPM CISSP CEH
Senior Engineer, Program Manager IT Security
Research Area Future Networks and Services
Safety & Security Department
thomas.bleier@ait.ac.at | +43 664 8251279 | www.ait.ac.at/it-security