Einführung in die Informationstechnik

VI – Sicherheit im Internet

Aussagen zum Thema Bedrohung

(etwas älter)

- Mit einer Wahrscheinlichkeit von rund 50 Prozent wird ein Windows-PC ohne Virenschutz und aktuelle Sicherheits-Patches innerhalb von nur 12 Minuten durch einen Internet-Wurm infiziert.
  - http://www.sophos.de/pressoffice/news/articles/2005/07/pr_20050701midyearroundup.html
- Test von BBC News: ein mit dem Internet verbundener PC mit einem Windows-Betriebssystem wird durchschnittlich alle 12 bis 15 Minuten angegriffen oder nach Sicherheitslücken abgesucht.
- Umfrage Großbritannien (2006): 21 Prozent der Befragten sagten, sie hätten Angst vor Internetkriminalität, nur 16 Prozent fürchteten sich vor einem Einbruch.
- http://www.naiin.org/de/content/phishing/v13.php
- „Chinesische Hacker dringen ins Netz des Weißen Hauses ein“, Spiegel-Meldung vom 07.11.2008, http://www.spiegel.de/netzwelt/web/0,1518,589048,00.html

Meldungen zum Thema Bedrohung

- Riesen-Botnetz identifiziert: Kriminelle kontrollieren 1,9 Millionen Zombies (22.04.2009) http://www.trojaner-info.de/news2/botnetz-ukraine-finjan.shtml
- Internetkriminalität gilt als lohnendes Geschäftsfeld für Betrüger … Die PC-Zeitschrift „Chip“ ging auf die Suche - und fand Gauner mit 800.000 Euro Einkommen. (06.05.2010) http://www.spiegel.de/netzwelt/web/0,1518,692888,00.html
- Zwei Entwickler haben die Technik zum Durchstöbern der Browser-History so weit verfeinert, dass Webseiten sogar zuletzt gelesene Artikel auf Newsseiten, die genaue Postleitzahl eines Besuchers und auf Suchmaschinen eingegebene Begriffe herausfinden können. (21.05.2010) http://www.heise.de/newsticker/meldung/History-Stealing-2-0-Ich-weiss-wo-du-wohnst-1005016.html

Aktuelle Bedrohungsmeldungen

- 01.03.2011: Attacke auf US-Großbank - Cyber-Gangster hackten Morgan Stanleys Netzwerk
- http://www.spiegel.de/wirtschaft/unternehmen/0,1518,748277,00.html
- 20.04.2010: Zeitungsbericht - China-Hacker sollen Googles Passwort-System gestohlen haben
- http://www.spiegel.de/netzwelt/web/0,1518,690005,00.html
- 03.05.2011: Sicherheitsrisiko - Hacker konnten Daten von 100 Millionen Sony-Kunden kopieren
- http://www.spiegel.de/netzwelt/games/0,1518,759830,00.html
- 28.5.2011: Cyber-Attacke gegen Lockheed Martin - Datendiebe greifen US-Rüstungskonzern an
- http://www.spiegel.de/netzwelt/web/0,1518,765422,00.html

Aktuelle Bedrohungsmeldungen

- Telekom warnt vor Schwachstelle bei drei WLan-Routern http://www.faz.net/aktuell/technik-motor/sicherheitsluecke-telekom-warnt-vor-schwachstelle-bei-drei-wlan-routern-11731141.html
- 28.05.2012 – Experten enttarnen neue Cyberwaffe http://www.spiegel.de/netzwelt/web/computerwurm-flame-von-it-experten-entdeckt-a-835604.html
- 2.6.2012 – Cyberwar: Der Wurm als Waffe http://www.spiegel.de/netzwelt/netzpolitik/experten-suchen-nach-kriegsrecht-fuer-den-cyberwar-a-836566.html
- 6.6.2012 - LinkedIn-Passwörter im Internet veröffentlicht http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/datenleck-linkedin-passwoerter-im-internet-veroeffentlicht-11776353.html

Viren-Ticker

- Passwortklau per Browser-Erweiterung: Ein neu entdeckter Schädling sammelt Anmeldedaten für Online-Dienste, auch für solche, die verschlüsselte Verbindungen nutzen. Er arbeitet dabei nicht als Keylogger sondern mit einer Firefox-Erweiterung, die gespeicherte Passwörter extrahiert. (13.11.2012)
- Neue Malware hat es auf Kassenterminals abgesehen: Ein neues Schadprogramm namens Dexter stiehlt weltweit Kreditkarten-Daten von herkömmlichen Kassenterminals. (12.12.2012)
- Malware klaut 20.000 Bilder pro PC: Ein kürzlich entdeckter Schädling betreibt Datendiebstahl der etwas anderen Art. Er kopiert nicht etwa Dokumente oder Mail-Adressen sondern Bilder. Er transferiert die ersten 20.000 Bilder, die er auf einem PC findet, auf einen FTP-Server. (08.11.2012)

Quelle: http://www.pcwelt.de/News-Sicherheit-Virenticker-7142.html

9

Übersicht

- Vergangene Wochen: Internet, Grundlagen und Dienste
- Heute:
  - Gefährdungen
    - Viren, Würmer & Co.
    - Aktive Inhalte
    - Phishing
    - Spam
    - Scareware
    - DoS, Bot-Netze
    - Dialer & Co.
  - Absicherung;
    - (Personal) Firewall, Anti-Viren Programme, Intrusion Detection
  - Schutz der Privatsphäre
  - Jugendschutz
- Orientierung am BSI-Grundschutz

10

Viren

- Original Definition von Fred Cohen (1984): A "computer virus" is a program that can "infect" other programs by modifying them to include a possibly evolved version of itself.
- Definition: Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)
- Viren schleusen sich in andere Programme ein und verbreiten sich dadurch

Bildquelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)
https://www.bsi-fuer-buerger.de/cln_174/BSIFB/DE/ITSicherheit/VirenUndAndereTiere/Virenchronik/virenchronik_node.html

11

Arten von Viren, Verbreitungswege

- Boot-Viren:
  - Booten → laden des Betriebssystems
  - Virus schreibt sich in den Bootsektor eines Datenträgers
  - Ausführung beim Starten des Rechners
- Datei-Viren:
  - Infizieren Programme, werden Teil des Programms
  - Beim Starten des Programms wird Virus ausgeführt
- Makro-Viren:
  - Makros: Skripte, die Programmschritte automatisiert ausführen
  - Beispielsweise in Word, Excel
  - Makroviren bevölkern die erzeugten Dokumente
- Skript-Viren:
  - Ähnlich Makroviren, meist auf Webseiten

12

Schäden durch Viren in der Vergangenheit

- Harmlose Schäden:
  - Der Microsoft Word-Makro-Virus WAZZU fügt bei den befallenen Dokumenten an zufälligen Stellen das Wort "Wazzu" ein.
  - MIX-1 Virus stört das Ausdrucken von Texten und Grafiken auf einem Drucker
    - Aus "Sehr geehrte Damen und Herren" wird auf dem Ausdruck dann "Rahr gaahrta Deman ond Harran„
      (Quelle: BSI, http://www.bsi-fuer-buerger.de/viren/04_0205.htm)
- Datenlöschung/-zerstörung:
  - Der Boot-Virus Michelangelo überschreibt an jedem 6. März die ersten Spuren der Festplatte mit stochastischem Inhalt und macht sie dadurch unbrauchbar (1992).
  - Der Virus Onehalf verschlüsselt maximal die Hälfte des Inhalts der Festplatte. Wird der Virus entfernt, sind die verschlüsselten Daten nicht mehr verfügbar.
  - XM/Compat-Virus: Makro-Virus, der Microsoft-Excel-Dateien befällt.
    - Durchforstet ein zufälliges Dokument aus der Bearbeitungs-History nach ungeschützten Zellen mit numerischen Werten. In diesen Zellen ändert er die Werte mit einer einprozentigen Wahrscheinlichkeit zufällig in einem Rahmen von +5 bis −5 % ab.
- Hardwarezerstörung:
  - Übertaktung von Hardwarekomponenten
  - Zerstörung von Festplatten
  - Heute eher unüblich/schwierig, auf Grund der Heterogenität der Hardware

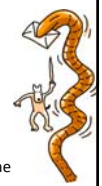
13

Trojaner

- Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen.
- Arbeiten im Hintergrund
- Ermöglichen beispielsweise Zugriff von außen
- Verbreiten sich nicht selbstständig
- Verbreitungswege:
  - ICQ, Email, Tauschbörsen, Download
- Ziel: Ausspionieren vertraulicher Daten
- Beispiel:
  - Bildschirmschoner, der Passwörter weiterleitet
  - veränderte Login-Programme

14

Würmer



- Ähnlich Viren, Verbreitung autark, ohne Wirtsprogramm
  - Benötigt aber Hilfsprogramm wie Email oder Netzwerkdienst
  - Nutzt bestehende Infrastrukturen
- Virus: Weitergabe durch infizierte Datei
- Im strengen Sinn sind Würmer sich selbst verbreitende Programme
  - Bringen oft eigene Email-Routine mit
- Verbreitung durch:
  - Email - oft als Anhängsel
  - peer to peer, Tauschbörsen
  - Instant Messaging
- Erster Wurm: Robert T. Morris (1988)
- verschleiern Ihre Existenz ähnlich den Trojanischen Pferden
- Nutzen oft gezielt Programmierfehler zur Ausführung

Bildquelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

15

Rootkit

- Root=Admin → Rootkit=Admin-Baukasten
- Ziel: (vollständige) Kontrolle über das befallene System
- Softwarewerkzeuge zum Verschleiern von Einbrüchen, ersetzen wichtiger Systemprogramme
- Klinkt sich in laufende Prozesse ein
  - Gelangt so an „interessante“ Daten
- Drei wesentliche Varianten
  - RKs die sich in den Betriebssystemkern einschleusen → Kernel Rootkits
  - RKs die sich in laufende Prozesse einhaken und deren Aufrufe auf die eigenen Programmteile umlenken → Userland Rootkits
  - Auch möglich Speicher-Rootkits
- Ziel: Kontrolle des Systems, Öffnen von Hintertüren

16

MailBombing, Archivbombe

- Mailbombe: Versenden von großen Dateien als Emailanhang → nur wirksam bei begrenztem Emailspeicherplatz
  - Oft auch mehrere Emails notwendig
- Archivbombe: gepackte Datei, die beim Entpacken sehr viel Speicherplatz benötigt
  - Problem für Antivirenprogramme
  - Bekanntestes Beispiel: 42.zip

17

Hoax

- Scherz oder Falschmeldung, Ente
- Kettenbriefe, Aufrufe zum Löschen von Dateien
- Irreführende Nachricht, die gelöscht werden kann und sollte
- Laut BSI enthalten die meisten „Hoaxes“ folgende Elemente:
  - Einen Aufhänger, der Seriosität vermitteln soll (etwa einen Bezug zu einem bedeutenden Unternehmen)
  - Eine angebliche Sachinformationen über ein Ereignis von besonderer Bedeutung (etwa das Auftauchen eines Computerschädlings) oder sensationelle Einkunftsmöglichkeiten (etwa angebliche Provisionen durch große Softwarekonzerne für die Weiterleitung von Mails), Hinweise auf Katastrophen (z. B. Tsunami) oder Verschwörungstheorien
  - Keine Daten, dafür aber Aktualität signalisierende Bezüge wie "gestern" oder "soeben"
  - Die dringende Bitte, die Information oder Warnung möglichst allen Bekannten zukommen zu lassen.
- Liste aktueller Email-Enten: http://www2.tu-berlin.de/www/software/hoaxlist.shtml
  - Aufrufe zum Tank-Boykott als Protest gegen die Preispolitik der Mineralölkonzerne

Bildquelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

18

Social Engineering

- Nutzen des Sozialen Umfeldes um an persönliche Daten zu gelangen
  - Ausspionieren des persönlichen Umfeldes
  - Ausnutzen von Verhaltensweisen
- Identity Theft: Nutzung persönlicher Daten durch Dritte.
  - Eigentlich Identitätsmissbrauch
- Social Hacking: nutzen von Social Engineering um ein ein fremdes Computersystem einzudringen
- Phishing
  - Allgemein
  - Spear Phishing
  - Dumpster Diving

19

Phishing

- Kunstwort aus password und fishing
  - „nach Passwörtern fischen“
- Ermittlung von Passwörtern und Zugangsdaten über gefälschte Emails und Webseiten
  - beeinhalten oft Link auf gefälschte Webseite
  - Falsche, versteckte Absenderadresse

Arbeitsgruppe Identitätsschutz: https://www.a-i3.org/

20

Phishing Email

Betreff: German
Von: Uni Help Desk <saeed1@ums.ac.ir>
Antwort an: Uni Help Desk <account.helpdesk48@yahoo.com.hk>
Datum: 30.07.2009 10:44
An: undisclosed-recipients:;

Wir haben Ihnen am 29. Juni 2009 beraten, dass Sie die Passwort auf Ihrem Konto, um zu verhindern, dass Unbefugte Konto Zugang im Anschluss an die Netzwerk-Anweisung wir zuvor kommuniziert werden.
Alle E-Mail-Hub-Systeme wird sich regelmäßig geplante Wartung. Zugriff auf Ihre E-Mail über das Webmail-Client wird für einige Zeit nicht verfügbar
Während dieser Gewährleistungsfrist. Wir sind derzeit die Modernisierung unserer Datenbank und
E-Mail-Konto-Center i.e Startseite.

Wir werden das Löschen alter E-Mail-Konten, die nicht mehr aktiv zur Schaffung von mehr Platz für neue Benutzer-Konten. Wir haben auch untersucht, ein Security-Audit-weit zu verbessern und unsere aktuellen Sicherheitseinstellungen.

Im Hinblick auf die Fortsetzung der Nutzung unserer Dienste werden Sie benötigen zur Aktualisierung und wieder bestätigt, Ihre E-Mail-Konto, wie unten. Um Ihr Konto wieder bestätigen, müssen Sie eine Antwort auf diese E-Mail sofort und geben Sie Ihre Kontodaten wie unten.

Benutzername: (*********)
Passwort: (*********)
Geburtsdatum:
Zukunft Passwort: (*******)(Option)

Sollte dies nicht sofort machen wird Ihr Konto deaktiviert aus unserer Datenbank und den Service nicht unterbrochen werden, wie wichtig Nachrichten können auch verloren gehen durch Ihre rückläufig wieder comfirmed Sie uns Ihre Kontonummer Details. Wir entschuldigen uns für die Unannehmlichkeiten, dass dies dazu führen, dass Sie während dieser Zeit, sondern vertrauen, dass wir sind hier, um Sie besser bedienen zu können und mehr Technologie, die dreht sich um Sichere E-Mail.

Es ist auch relevant, Sie verstehen, dass unser primäres Anliegen ist die Sicherheit für unsere Kunden, und für die Sicherheit ihrer Daten und Dateien. Bestätigungs-Code: / 93-1A388-480 Technische Support-Team Grüße UNI Help Desk Support / Maintainance Team TSRa

21

Erkennen von Phishing-Emails

- gefälschte Absenderadressen – im Header nachsehen
- unpersönliche Anrede („lieber Kunde der ...-Bank“)
- dringender Handlungsbedarf signalisiert (sonst Datenverlust)
- es wird gedroht ("Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren…")
- Vertrauliche Daten (z. B. PINs und TANs) werden abgefragt
- Die Mails enthalten Links oder Formulare, die vom Empfänger verfolgt bzw. geöffnet werden sollen
- manchmal in schlechtem Deutsch verfasst
- E-Mails enthalten kyrillische Buchstaben oder falsch dargestellte bzw. fehlende Umlaute

http://www.bsi-fuer-buerger.de/phishing/beispiele.htm

22

Erkennen von Phishing-Webseiten

- oft fehlt Sicherheitshinweis im Browser (https://), kann aber auch gefälscht werden
- Domainnamen enthalten unübliche Zusätze, sehen den tatsächlichen aber ähnlich
  - www.x-bank.servicestelle.de
  - banking.postbank.ru
- Sicherheitszertifikat fehlt, erkennbar durch das Schlosssymbol
  - in Statusleiste
  - in Eingabezeile

http://www.bsi-fuer-buerger.de/phishing/beispiele.htm

23

Phishing Webseiten - Beispiel

http://www.bsi-fuer-buerger.de/phishing/beispiele.htm

24

Phishing Webseiten - Beispiel

http://www.bsi-fuer-buerger.de/phishing/beispiele.htm

25

Identitätsmissbrauch

- Vorgeben falscher Identität für verschiedene Zwecke
  - Einen Betrug durchzuführen: Bestellungen bei Versandhäusern
  - Um in Rechnersysteme einzubrechen
  - Dienstleistungen kostenlos zu nutzen
  - Weitere Daten zu erhalten
- Nicknapping: Benutzen fremder Nicknames
- Anlegen von Accounts unter fremdem Namen
  - Kann genutzt werden, um Person zu schaden
  - Kann dazu führen, dass betroffene Person keinen Account mehr anlegen kann → echter Identitätsdiebstahl

26

Netzbasierte Manipulationen

- Pharming, Spoofing, Poisoning: Manipulation der DNS-Abfragen
  - Ziel:
    - Umleitung von Nutzern auf alternative Webseiten
    - Obwohl die richtige URL eingegeben wurde
    - Verschleierung der eigenen Identität
  - Angriffsziele: DNS-Server, hosts-Dateien
- Man-in-the-middle-Angriff: im LAN, WLAN
- Cache-Poisoning

https://www.bsi.bund.de/cln_165/ContentBSI/grundschutz/kataloge/g/g05/g05078.html

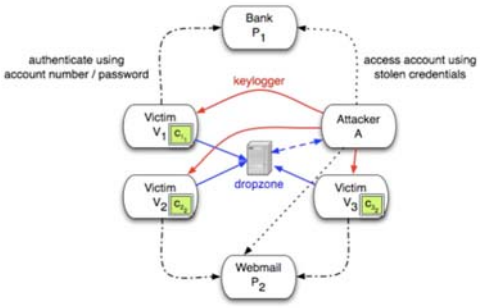
27

Spyware

- Software, die das Verhalten von Nutzern ausspioniert
- ähnlich Phishing, allerdings passiv
- kann auf Rechner gelangen über:
  - Aktive Inhalte auf Webseiten
  - Freeware oder Shareware
- gefährlich: keylogger, können auch Passwörter ermitteln

28

Methoden des Ausspähens



Spiegel-Artikel: Cyber-Verbrecher gehen IT-Forschern in die Falle, http://www.spiegel.de/netzwelt/tech/0,1518,600971,00.html

29

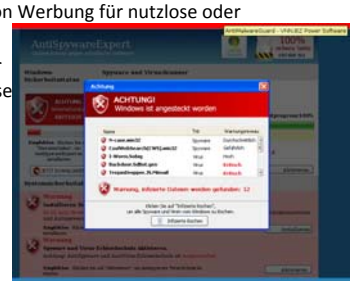
Spam

- Spam ist dem Dosenfleisch SPAM (Spiced Porc and Ham) entliehen (deutsch: Frühstücksfleisch)
- Als Spam, Spamming oder Junk Mail (Müllpost) bezeichnet man:
  - Massenversand nichtangeforderter Werbe-EMails
  - Werbebeiträge in Newsgroups, die nichts mit dem Thema der Newsgroup zu tun haben.
  - Kettenbriefe
- Voraussetzung: Email-Adressen

30

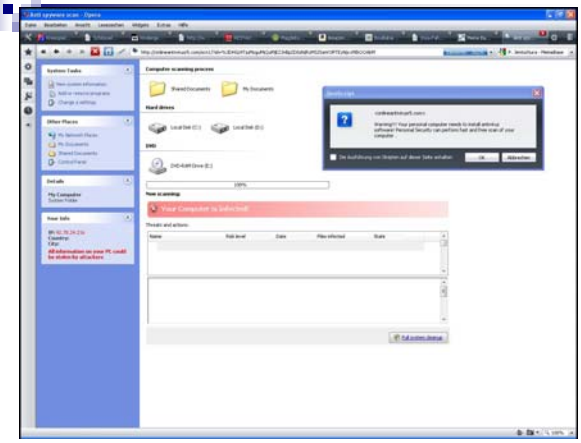
Scareware

- Werbung, die die Angst von BenutzerInnen ausnutzt → Trickbetrug
- gezielte Platzierung von Werbung für nutzlose oder gefährliche Software
- auch Vorgaukeln einer Schadsoftwarediagnose
- Betroffen u.a.: New York Times, Microsoft



http://www.heise.de/security/artikel/Zweifelhafte-Antiviren-Produkte-270094.html

31



32

Aktive Inhalte auf Webseiten

- Browser können kleine Programme innerhalb der Webseite ausführen
  - Java-Applets, JavaScript, ActiveX, VBScript
- benötigt, um Inhalte dynamisch zu aktualisieren
- Gefahrenpotential, da Programme auf Rechner ausgeführt werden
  - Ausführung sollte vom Browser kontrolliert werden
  - Schwachstelle bei:
    - fehlerhafter Programmierung
    - gezieltem Angriff

34

DoS – Deny of Service

- Außer Betrieb setzen von technischen Einrichtungen
- bombardieren von Servern mit Anfragen → Überlastung
- oft verteilte Angriffe – distributed DoS
  - Verbreitung der Angriffsprogramme vorher als Wurm
  - Nutzung von Bot-Netzen

35

Bots

- Ro(bot-Net), ferngesteuertes Netz von gekaperten Rechnern
  - Zombie-PCs
- Jeder Rechner kann einzeln ferngesteuert werden oder
- Im Verbund arbeiten
  - genutzt für Spam, DoS

36

veraltet: Dialer

- Programme, die unbemerkt die Einwahl ins Internet übernehmen
  - meist über so genannte Mehrwertdienst-Nummern
    - 0190 – mittlerweile verboten, 0137, 118x, oder Ausland
- funktionieren nicht bei DSL
- ersetzen die „normale Einwahl“ unbemerkt
- als Schadsoftware aber noch üblich

37

Andere Formen des Missbrauchs

- Podslurping: Nutzung von USB-Sticks, IPods, oä. Massenspeichern zum Datenklau
  - Prinzip: Schlürfen am Rechner
    - Nutzen der Autostart-Funktion zum Starten von Software, die „interessante“ Daten auf den Stick kopiert
- Snarfing: Angriffe auf Drahtlosgeräte (WLAN), Bluesnarfing (Bluetooth)
- Bluejacking

38

Abzocke

- Nutzung von Kontaktdaten im Netz zur Zustellung von Rechnungen
- Datenermittlung durch dubiose Angebote im Netz
  - Beispiele: Berechnung des zu erwartenden Lebensalters, Senkung des Energieverbrauchs,
- oder: Nutzung erschlichener Kontaktdaten
- oft unter Vortäuschung eines seriösen Absenders wie Single.de, Web.de, etc.

39

Überwachung allgemein

- Vorratsdatenspeicherung: EU verlangt 6 Monate
  - Spuren im Internet: Internetprovider speichert Verbindungsdaten
  - Telefondaten
- Handy:
  - Positionsbestimmung problemlos möglich
- Videoüberwachung: öffentliche Plätze, Bus & Bahn
- Auto: Blackbox, Telemetrie
- Reisen: Flugbuchungen
- Rabattkarten, Kreditkarten
- RFID-Chips: für Waren, Tiere, Menschen

40

RFID

http://de.wikipedia.org/w/index.php?title=Datei:134_2khz_rfid_animal_tag.jpg&filetimestamp=20100108234403

41

Wireless LAN

- Gefahren:
  - Fremdnutzung des eigenen WLANs
  - Mithören des WLAN-Verkehrs: Man in the middle-Angriff
- Sicherheitstipps:
  - WLAN nur bei Gebrauch einschalten
  - Verschlüsselte Verbindung aktivieren
  - Nur öffentlicher Hotspots mit sicherer Verschlüsselung verwenden
  - Eigenen WLAN Hotspot nicht über WLAN konfigurieren

42

Einführung in die Informationstechnik

SICHERHEIT IM INTERNET-SCHUTZMÖGLICKEITEN

43

Schutzmaßnahmen, BSI empfiehlt:

1. Installation eines Virenschutzprogramms – regelmäßige Aktualisierung
2. (Personal) Firewall installieren und aktualisieren
3. Sicherheitsupdates für Betriebssystem und andere Software durchführen
4. nicht als Administrator arbeiten
5. Zugangsdaten unter Verschluss halten
6. Email-Anhänge nicht bedenkenlos öffnen
7. Downloads überprüfen (Quelle vertrauenswürdig?, gefälscht?)
8. keine persönlichen Daten weitergeben
9. Verschlüsselung der Kommunikation (WLAN, VoIP, Email)
10. Sichungskopien

44

Datensicherung

- Auslagerung von Daten auf sichere Datenträger
  - Vorsicht bei mobilen Datenträgern
- Backup
  - vollständig
  - Inkrementell
  - Software:
    - ab Windows Vista Bestandteil von Windows
    - alternativ: Personal Backup, …
- Prioritäten bei der Sicherung:
  1. Sicherung von persönlichen und Anwendungsdaten
  2. Betriebssystem und Anwendungen

45

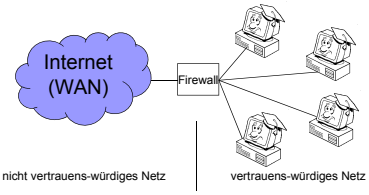
Virenschutzprogramme

- durchsuchen Speicher nach Viren
- zwei Betriebsarten:
  - transient: durch den Benutzer gestartet, läuft nur auf Anweisung
  - resident: mit dem Rechner gestartet, läuft permanent im Hintergrund
- wird Virus gefunden → Sperrung/Löschung der betreffenden Datei
- Software für Windows: bspw. Microsoft Security Essentials, Avira Antivir (nur private Nutzung), Campuslizenz Sophos (URZ)

46

Firewall

- auch Sicherheitsgateway genannt – eigenständige Netzwerkkomponente
- untersucht die Datenpakete - Filter
- unterbindet unerlaubte Zugriffe auf sicheres Netz und umgekehrt



47

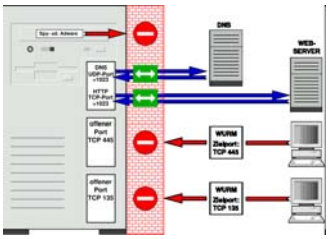
Firewall – Technologien

- **Paketfilter:** verwirft oder lässt Pakete passieren - zum Beispiel Untersuchung Quell- und Zieladresse, Port
  - ganze IP-Bereiche können gesperrt werden
- **Content Filter**:überprüft Inhalt von Paketen
  - Filtert: aktive Inhalte, Spam, Viren,
- **Intrusion Prevention**: sperren von Ports
- **Firewall Policy**: Regeln für das Verhalten einer Firewall

48

Personal Firewall

- nicht zwischen Netzwerken sondern zwischen Computer und „Außenwelt“
- kontrolliert Zugriffe von außen und von innen
- IDS/IPS
- Paketfilter
- beobachtet Programme
  - Schutz vor Angriffen von innen
- lernfähig



http://de.wikipedia.org/wiki/Personal_Firewall

49

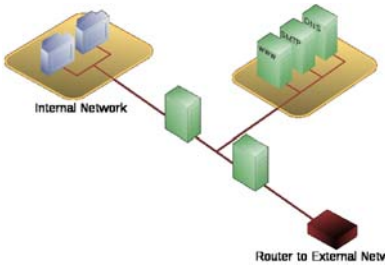
DMZ – Demilitarized Zone

- Ent- oder demilitarisierte Zone
- Problem: Rechner, die aus dem Internet erreichbar sind (sein müssen)
  - Bsp.: Mailserver, Webserver, Tauschbörsensauger
  - Ermöglichen Zugang zum lokalen Netz
- Lösung: Schaffung einer Pufferzone, die aus dem Internet erreicht werden kann, von wo aus aber das Heimnetz sicher ist
- Technisch: Errichtung von zwei Firewalls

http://www.heise.de/netze/artikel/DMZ-selbst-gebaut-221656.html

50

DMZ - Prinzip



51

Firewall: Software

- FLI4L: Floppy ISDN for Linux
  - Eigentlich ein Router, trennt aber internes Netz und Internet und bietet Funktionen wie:
    - IP-Masquerading, DMZ, Logging
  - gut kombinierbar mit Eisfair-Server

http://www.fli4l.de/

- IPCop: ähnlich FLI4L,
  - einfachere Konfiguration insbesondere bei mehreren Netzen
    - Drei Netze sind vorkonfiguriert, DMZ möglich
  - größere Hardwareanforderungen

http://www.ipcop.org/

- ähnlich: pfSense

52

Schutz der Privatsphäre

- Allgemein: Speicherung, Verarbeitung, weitergabe, etc. von personenbezogenen Daten benötigt eine Zustimmung der betreffenden Person
- E.T. Programme: wollen nachhause telefonieren, übermitteln Daten
- Internetspuren: Transparenz beim Surfen
  - Provider vermerkt mindestens IP-Adresse
  - Cache enthält angesehene Webseiten
  - History enthält URLs besuchter Webseiten
- Unverschlüsselte Email: auf jedem Rechner, den die Email durchläuft kann geschnüffelt werden
- Cookies: speichert persönliche Einstellungen (auf Webseiten)
  - Idee: Einstellungen nur einmal vornehmen

53

Einschub: Flash-Cookies

- von Flash-Player (Adobe) geschriebene Daten
- nur an Flash Player gebunden → browserübergreifend verfügbar
- Cookie-Größe:
  - „normale“ HTTP-Cookies: 4KB
  - Flash-Cookies: 100KB, mehr nach Zustimmung durch Nutzer möglich
- Normalerweise dürfen nur Einstellungen einer Webseite beinhalten
- Problem: werden nicht vom Browser verwaltet
  - → nicht sichtbar
  - → schlecht löschbar
  - → längere Lebensdauer

54

Schutz der Privatsphäre

- Einkaufen im Internet:
  - Hinterlegen von Adressen
  - Kreditkartendaten
  - Vorlieben, Verhalten, „der gläserne Kunde“
- Instant Messaging: gesamte Kommunikation kann und wird vom Provider gespeichert
- Angaben zur eigenen Person auf Webseiten: wird von Suchmaschinen gespeichert
- Metadaten in Bildern

55

Schutzmöglichkeiten

- Cookies löschen oder nicht akzeptieren
- Browser-Cache löschen
- History löschen
- Personal Firewall so einstellen, dass ausgehende Verbindungen gemeldet werden
- Emails verschlüsselt versenden: PGP – Pretty Good Privacy
- auf sichere Verbindung achten: „https://“

56

Passwörter

Wann ist ein Passwort sicher?

- Was meinen Sie?
- je länger desto besser, min. 8 Zeichen
  - Ziel: Brute-Force-Methode ausschalten
  - Aber: Passwortknacker sind clever
    - Vergleich mit Wörtern aus Lexika
- Komplexität erhöhen: Sonderzeichen, Satzzeichen, Zahlen, Buchstaben kombinieren
  - Schlecht: Substitution von Buchstaben durch Zeichen und Zahlen: E→3, i → 1, i →!, l→!, o →0, A→4, S →5, usw.
  - Auch schlecht: Jq4d3i oder 0qww2945

http://www.microsoft.com/security/online-privacy/passwords-create.aspx

57

Passwörter

Wann ist ein Passwort sicher?

- Wie bekommt man ein sicheres Passwort?
  - Das man sich auch noch merken kann ☺
  - Möglichkeit 1: WrssdNuW#EidVmsK;6
  - Möglichkeit 2: WerraitetsospäddurchWachtundNind2012?
    - Wer reitet so spät durch Nacht und Wind?
    - WerreitetsospätdurchNachtundWind?
    - WerraitetsospäddurchWachtundNind?
    - WerraitetsospäddurchWachtundNind2012?
- Öfter Passwörter ändern
- Verschiedene Passwörter für verschiedene Zwecke

http://www.microsoft.com/security/online-privacy/passwords-create.aspx

58

Kinder- und Jugendschutz

- Ungeeignete Inhalte: Gewalt, Pornographie, Rassismus
- Missbrauch von Chatrooms:
  - sexueller Kontakt zu Minderjährigen
  - Drogenverkauf
  - Verbreitung von ethisch und moralisch verwerflichen Informationen
  - Vorbereitung von Aktionen
- teure Downloads, Spam, Viren, Dialer

59

Schutzmaßnahmen

- geeignete Startseiten verwenden
- Technische Möglichkeiten:
  - Filterprogramme gegen jugendgefährdende Inhalte, Spam, Viren
  - Firewall mit Contentfilter (bspw. SquidGuard)
- Aufklärung:
  - allgemein über Gefahren im Internet: Spam, Viren
  - Bewusstsein über Gefahren entwickeln
  - persönliche Daten niemals preisgeben
  - keine Verabredungen außerhalb von Chatrooms

60

Zusammenfassung

- Bedrohungen „von außen“: Viren & Co., Spam, Spyware
- Bedrohungen „von innen“: eigenes Verhalten, Sorglosigkeit, Unwissenheit
- Schutzmaßnahmen: regelmäßiges Backup, Installation Virenschutz, Personal Firewall, Aufmerksamkeit
- Gefährdung von PDAs, Handys nicht vergessen

61

SCHADSOFTWARE AUF HANDYS

62

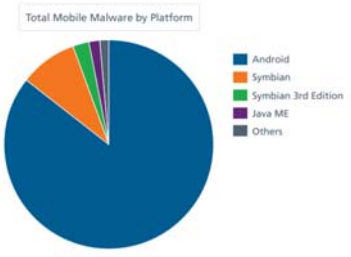
Handyschadsoftware

- erster Handyvirus: 2004 für SymbianOS: Cabir
  → Verbreitung über Bluetooth
- Ab Herbst 2004 Trojaner
  - Mosquit.a: getarnt als Spiel versendet SMS zu Nummern aus dem Telefonbuch
  - Skuller.a: Tauscht Icons gegen Totenschädel und löscht Dateien des Betriebssystems, Telefon startet nach Abschaltung nicht wieder
- Anfang 2005: Würmer, die sich über Smartphoneprotokolle und -dienste verbreiten
- Heute hauptsächlich Android (Quelle: McAfee Threats Report)

http://www.securelist.com/en/analysis?pubid=200119916

63

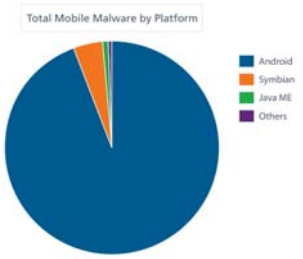
Mobile Schadsoftware



McAfee Threats Report: First Quarter 2012
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf

64

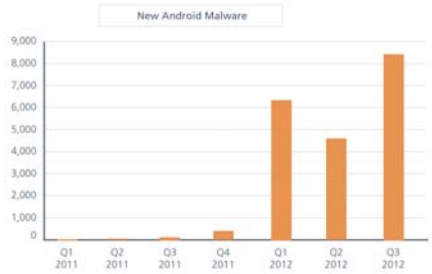
Mobile Schadsoftware



McAfee Threats Report: Third Quarter 2012
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf

66

Mobile Schadsoftware



McAfee Threats Report: Third Quarter 2012
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf

67

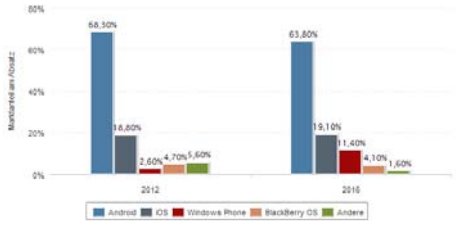
Handyschadsoftware

Wer ist gefährdet? Und warum?

- Handys, die eine populäre (weit verbreitete) Softwareplattform haben
- Handys zu deren Betriebssystem ein SDK bereitsteht, oder die ein OpenSource OS haben (gut dokumentiert)
- Handys deren Betriebssystem Fehler enthält
- iOS populär aber nicht offen
- Schutz: Antivirensoftware, Updates
- Jüngste Pressemitteilung: 8% von 13.500 untersuchten Android-Apps enthalten Sicherheitslücken (Quelle: Spiegel-Online, http://www.spiegel.de/netzwelt/web/viele-android-apps-von-sicherheitsluecke-betroffen-a-862613.html)

69

Handybetriebssysteme – Marktanteile



http://de.statista.com/statistik/daten/studie/182363/umfrage/prognostizierte-marktanteile-bei-smartphone-betriebssystemen/

70

Handyschadsoftware - Verbreitung

- selbstständig per Bluetooth: suche nach Handys in der Nähe deren Bluetooth aktiviert ist
  - auffällig: Verringerung der Akkulaufzeit
- klassisch:
  - Download von Dateien aus dem Internet
  - per Email
- per SMS/MMS (teilweise auch in Bildern versteckt)
- Aufruf zum Download (Bsp.: wie bei Zeus)
- Near Field Communication (NFC)-Angriffe

71

Handyschadsoftware

Arten von Schadsoftware/Angriffen

- Dialer für Handys
  - frei herunterladbare Programme können sich als Dialer erweisen: verschicken unbemerkt SMS an teure Mehrwert-dienste
    http://www.spiegel.de/netzwelt/web/0,1518,671924,00.html
- Viren fürs Handy
- Trojaner:
  - Beispiel Zeus: Diebstahl von mTANs
- Manipulierte SMS: Antwort an gefälschte Telefonnummer
  - teure Mobilfunknummer
  - andere „interessierte“ Person

http://www.spiegel.de/netzwelt/mobil/0,1518,555019,00.html

72

Handyschadsoftware – (weitere) Schäden

- Verschicken von SMS, MMS
  - Datenklau: können auch Adressbuch-Daten beinhalten
  - Spam
- Löschen des Adressbuchs und/oder von Systemdateien
- Sperren des Handys, bspw. Verhindern das Einschalten
- Datenklau: Verschicken des Adressbuchs per Bluetooth

73

Schadsoftware im Auto

- Ziele:
  - Überwinden der Wegfahrsperre
  - Kontrolle über das komplette System
- Möglichkeiten des Zugangs:
  - Fernbedienbare Zugangssysteme
  - Infotainmentsysteme, insbesondere Android-basiert
- Daraus resultierende Probleme: Versicherung

74

GOOGLE = DATENSAMMLER?

76

Google = Datensammler?

- Was weiss Google?
  - kommt darauf an ☺
- Suchmaschine nur einer von vielen Diensten
  - Google = etwa 50 Dienste
- Oft behauptet: Google bietet massenhaft kostenlose Dienste – Nutzer revanchiert sich mit einem Einblick in seine Privatsphäre

77

Suchmaschine

Google Deutschland

- sehr gute Suchergebnisse durch PageRank Verfahren
- Problem: Speicherung
  - IP-Adresse - neun Monate lang, freiwillige Anonymisierung
  - welcher Browser benutzt wird
  - die Suchanfrage selbst
  - Datum
  - Hinterlassen von Cookies zur Identifizierung
  - außerdem Spartensuche: Produkte, wiss. Artikel, Landkarten, Bücher, Videos

78

interessenbasierte Werbung

- Partnerseiten liefern Daten darüber, was sich ein Surfer anschaut + IP des Surfers
- Google erstellt Profil und liefert passende Werbung
- meist verdeckte Nutzung
- Transparenz unter: http://www.google.com/ads/preferences

79

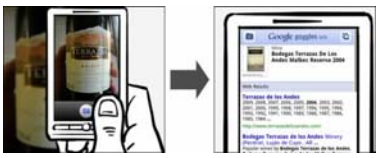
GMail – Account

- Name des Nutzers/der Nutzerin
  - wenn Kontoname = Nutzername
- Durchsuchen der Emails nach Stichwörtern zur gezielten Einblendung von Werbung
- viele Dienste mit Account verknüpft
  - Terminkalender, Docs, Health, Fotos, Blogger, Talk
- von Email abhängiger Dienst (ohne Anmeldung nutzbar): Alerts
  - Angabe einer Emailadresse notwendig

80

Google Goggles

- Suche über Bilder
- Prinzip: mit Handykamera Photo zu Google senden → Antwort: Informationen zum photographierten Objekt



- Problem: Personensuche
- Vorlieben, Interessen, Standorte

81

Google Chrome

- Googles Browser
- Probleme:
  - Omnibox – Adresszeile als Eingabefeld für URLs und Suchbegriffe
    - Autovervollständigung → sendet ständig Daten an Google
  - Jede Installation enthält eine eindeutige Identifikationsnummer
    - wird an Google gesendet, bspw. bei Aktualisierungsprüfung
  - Senden von Programmfehlern an Google:
    - ID, momentan offene Dateien und Programme sowie Dienste und Dateiinhalte werden an Google gesendet
- viele „problematische“ Dienste sind abschaltbar

82

Google Toolbar

Erweiterung von Firefox, IE und Chrome

- erlaubt direktes Suchen bei Google auch andere Suchdienste wie Bildersuche, Scholar, usw.
- Popup-Blocker
- Durchsuchen der aktuellen Webseite
- Infos zur aktuellen Seite: u.a. ähnliche Seiten, Seiten die auf diese verweisen
- Synchronisierung mit Google-Konto
- Rechtschreibkorrektur in Formularfeldern
- SideWiki
- Hervorhebung von Suchwörtern
- Webprotokoll: Protokoll der eigenen Webaktivitäten
- Mein Standort: Ortsbezogene Informationen bekommen

http://toolbar.google.de/
http://de.wikipedia.org/wiki/Google_Toolbar

83

Probleme: Google Toolbar

- Rechtschreibkorrektur erfordert das Senden der Daten zu Google
- SideWiki: Kommentare werden bei Google gespeichert
- Synchronisierungsfunktion: speichert Browsereinstellungen. incl. Autofill-Infos im Googlekonto
- Autofill sendet: Daten über Struktur der Seiten die das Webformular enthalten und deren Gliederung
- Webprotokoll speichert Verlaufsdaten im Googlekonto
- Mein Standort sendet Infos über: MAC-Adresse, SSIDs des WLANs, ID des Routers (MAC-Adresse), Signalstärke des Routers

http://www.google.com/support/toolbar/bin/static.py?page=privacy.html&hl=de&v=

84

Google Desktop

- Indizierung von Dokumenten auf dem lokalen PC
  - Office-Dokumente, Textdateien, PDF, Musik, Bilder, Videos, Emails, Webseiten, History
- Vorteil: lokale Dokumenten können durchsucht werden
- Problem: Suchfunktion über mehrere Rechner
  - erfordert Zwischenspeicherung von Daten bei Google → Suchindex der Dokumente
  - erlaubt Zugriff auf private Dokumente

85

Google Talk

- Instant Messaging
  - auch für Handy wie iPhone, Android, Blackberry
- VoIP - Funktionalität
- Problem: alle Nachrichten werden über Google-Server geleitet

86

Google Health

- zentrales Abspeichern von Gesundheitsdaten
  - Befunde, Allergien, Laborergebnisse, Medikamente
- Überprüfung von Wechselwirkungen mit anderen Medikamenten
- Backup für Befunde
- Suche nach Ärzten und Krankenhäusern
- Problem: alle Daten landen bei Google auf dem Server

87

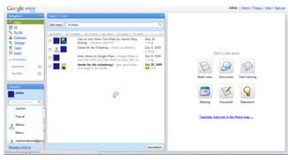
Google Docs

- gemeinsames Bearbeiten von Dokumenten
  - Textverarbeitung, Tabellenkalkulation, Präsentationen
- Problem: Dokumente liegen bei Google auf dem Server

88

Google Wave

- das gruppenenarbeits-, projektbarbeitungs-, photosharing-, brainstorming-, interactive games tool ☺
- Gruppenarbeit unter Benutzung von Photos, Karten, Videos, Textverarbeitung
- Problem: alle arbeiten online → alle Daten bei Google



89

Anonym bleiben?

- ist möglich
  - fiktiven Benutzernamen wählen
  - nicht über Google surfen: nicht anmelden
  - Nutzung von Anonymisierungsdiensten
  - Nutzung alternativer Suchmaschinen wie: http://www.ixquick.com → speichert keine Daten
  - Googles Suchmaschine nicht benutzen
  - Transparenz: Google Dashboard
  - http://www.google.com/ads/preferences
- aber schwierig:
  - siehe interessensbasierte Werbung
    - selbst wer nicht über Google surft wird an Google gemeldet
  - Google Analytics: Webseitenbetreiber können analysieren lassen, wer sich wofür interessiert → Weiterleitung an Google → Profilerstellung

90

Google-Analytics

- Browser-Erweiterung – erlaubt es, Google Analytics das Datensammeln zu verbieten
- Für Chrome, Firefox, IE
- Alternative: Webseitenbetreiber können IP-Adressen verkürzen

http://www.spiegel.de/netzwelt/web/0,1518,696816,00.html

91

Zusammenfassung

- Google erschafft ein virtuelles Gedächtnis
- Ziel: auf alle Fragen die eine richtige Antwort zu geben
- Problem: richtige Antwort auf alle Fragen verlangt viel Wissen über denjenigen der fragt
- bisher versichert Google, dass die angebotenen Dienste nichts voneinander wissen
- theoretisch möglich: Zusammensetzen aller Informationen aus verschiedenen Quellen
  - anhand von IP-Adressen, gesetzten Cookies, angegebenen Nutzernamen (auch von Werbepartnern)
  - Worst case: Abgleich mit anderen Quellen wie Amazon, Paypal
- Vision: online über Google, Browser als Plattform für alle Anwendungen, Speicher → Google, Stichwort cloud computing

92

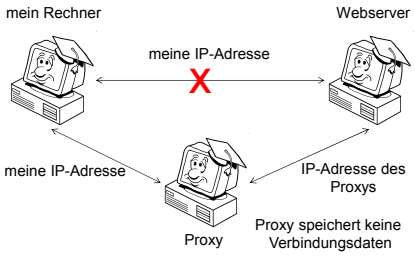
Einführung in die Informationstechnik

ANONYM IM INTERNET

93

Anonym im Internet

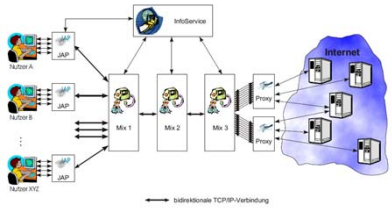
- Benutzung von Proxy-Servern
  - öffentliche Proxy-Listen verfügbar



94

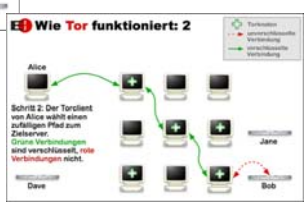
Verschleierung der Identität: JAP

- JAP arbeitet als lokaler Proxy
- Kommunikationsverbindungen verschlüsselt über einen Umweg mehrerer Zwischenstationen – Mixe
- mehrere (tausend) Benutzer kommunizieren über Mixe
- Mixe protokollieren nicht



95

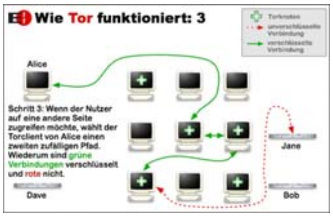
Verschleierung der Identität: TOR



http://www.torproject.org/overview.html.de

96

Verschleierung der Identität: TOR



- Unterschied TOR, JAP:
  - Tor wählt Route zufällig
  - JAP hat festgelegte Route

http://www.torproject.org/overview.html.de

97

Anonym im Internet: Rewebber

- Nutzung von Anonymisierungswebseiten
- ohne Installation anonym surfen
- Anonymität aber nicht gesichert
- URL muss in Formular eingetragen werden

98

99

PGP – Pretty Good Privacy

- Verschlüsselung von Emails
- Public-Key-Verfahren, asymmetrisch
- Prinzip:
  - privater Schlüssel zum Entschlüsseln
  - öffentlicher Schlüssel zum Verschlüsseln

100

Zusammenfassung

- mit etwas Aufwand kann man anonym im Netz bleiben
- Nutzung von Verschleierung:
  - Proxys
  - Anonymisierung durch Routen
  - Rewebber
- Emailverschlüsselung: PGP
- Test, welche Daten ermittelbar sind: http://www.anonym-surfen.com

101

Links

- Sicherheit im Internet beim BSI: http://www.bsi.bund.de/fachthem/sinet/index.htm
- Sehr gute Übersicht zum Thema „Sicherheit im Internet“: http://www.bsi-fuer-buerger.de/
- Schutz der Privatsphäre: http://www.privacy.gov.au/internet/internet_privacy/
- Arbeitsgruppe Identitätsmissbrauch im Internet: https://www.a-i3.org/

102

Einführung in die Informationstechnik

CYBERWAR

103

Cyberwar - Begriff

- Cyberwar: Zusammensetzung aus Cyberspace und War
  Hans Fleischhack, Michael Lübke, Kai-André Pancratz et al.(Hrsg.): „Der Wandel in der Informatik in den vergangenen 25 Jahren", 2011, http://www.informatik.uni-oldenburg.de/~iug10/war/texte/einleitung.html
- Hintergrund: Verwundbarkeit moderner Infrastrukturen da (immer) mehr Abhängigkeit von Computern besteht
  - Im zivilen Bereich (Vernetzung von Dingen, Internet of Things)
  - im industriellen Bereich (Fernwartung, Steuerung von Großanlagen)
  - Im militärischen Bereich (vernetzte Kriegsführung)
- Grundlage: IT-Systeme sind tief in gesellschaftliche, politische und wirtschaftliche Strukturen eingedrungen
  - Angriff auf vernetzte IT-Strukturen hat großen Schaden zur Folge
- Andere Begriffe: Cyberwarfare, Computernetzwerkattacke (CNA), militärisch: Computernetzwerkoperationen (CNO)

104

Cyberwar - Definition

- Cyberwar ist somit definiert durch eine **Attacke im Internet**, die **beträchtliche Auswirkungen** meist finanzieller Art auf das System des Angegriffenen hat. Dies kann zwischen Staaten, Unternehmen oder auch mit Beteiligung von Privatpersonen geschehen. Wichtig ist hier, dass **die Auswirkungen ernst zu nehmen sind**.
  Hans Fleischhack, Michael Lübke, Kai-André Pancratz et al.(Hrsg.): „Der Wandel in der Informatik in den vergangenen 25 Jahren", 2011, http://www.informatik.uni-oldenburg.de/~iug10/war/texte/einleitung.html

105

Cyberwar

- Der Begriff Cyberwar ist aus den Begriffen **War** und **Cyberspace** zusammengesetzt und bezeichnet die **kriegerische Auseinandersetzung** mit den **Mitteln** der **Informationstechnologie**. In der Praxis meint dies den Angriff auf Computer und die in ihnen enthaltene Information, die Computernetzwerke und die von den Computern abhängigen Systeme (aus Saalbach, 2012).

106

Cyberwar - Definition

- Ergänzend: Das Thema ist eng verbunden mit dem der Sicherheitslücken im Internet. Wer sich mit Cyberwar befasst, muss sich auch um Sicherheitslücken kümmern, denn vor Cyberwar kann man sich schützen.
  Hans Fleischhack, Michael Lübke, Kai-André Pancratz et al.(Hrsg.): „Der Wandel in der Informatik in den vergangenen 25 Jahren", 2011, http://www.informatik.uni-oldenburg.de/~iug10/war/texte/einleitung.html

http://www.informatik.uni-oldenburg.de/~iug10/war/texte/einleitung.html

107

Cyberwar: Vorgehensweise

- Erlangen von Zugang zu Rechnersysteme
  - Bspw. Social Engineering, Zero-Day-Exploits, Hacken von Passwörtern
- Installation von Schadsoftware: siehe vorvergangene Vorlesung
- Manipulation und Spionage
  - Rechner übernehmen, manipulieren
- Cyberwar: bspw. durch Distributed Deny of Service (DDoS)-Angriffe

(Saalbach, 2012)

108

Cyberwar– Beispiel: Morris Wurm

- Erste Form des unbeabsichtigten Angriffs
- Robert T. Morris programmiert 1988 Software, die sich selbst verbreitet
  - Ziel: so viele Rechner wie möglich infizieren und von dort eine Nachricht schicken
  - Wurm richtet im System keinen Schaden an
- Problem: Mehrfachinfektionen – Rechner wurden lahm gelegt
- Geschätzte Anzahl: 6000 (ca. 10% des Internets)
- Finanzieller Schaden: ca. 10-100Mill. $

109

Cyberwar – Beispiel: Stromnetz USA

- Versuch, in das amerikanische Stromnetz einzudringen
- 2003 konnte Wurm Slammer in Atomkraftwerk David-Besse in Ohio eindringen
- Seit 2006 mussten zweimal Atomkraftwerke wegen Cyberangriffen abgeschaltet werden
- 2009 eindringen von Hackern in die Stromnetzkontrolle
  - Sie hinterliessen Software, die die Unterbrechung bei Bedarf erlaubten

(Saalbach, 2012)

110

Cyberwar – Beispiel: Kampfdrohnen

- 2009 irakischen Aufständischen ist es gelungen in US-Drohnen einzudringen
  - → Konnten Videos mit ansehen
- 2011 Virus in der Creech Air Force Base
  - Steuerzentrale für Drohnen

(Saalbach, 2012)

111

Cyberwar – Beispiel: Estland

- Großangriff auf Estland 2007
- Ursache: Verlegung eines sowjetischen Kriegerdenkmals aus Tallinn
- Mehrwöchige DDoS-Angriffe auf die IT-Infrastruktur von Russland aus (Saalbach, 2012)
  - Server der estn. Regierung, Banken, Zeitungen, politischer Parteien und Unternehmen
  - Zahl der Anfragen auf Rechner stieg von 1000 p. Tag auf 2000 p. Sekunde (Saalbach, 2012)
- Folge: Verärgerung/Repressalien seitens Russland

http://www.informatik.uni-oldenburg.de/~iug10/war/texte/vorfaelle.html

112

Cyberwar – Beispiel: Stuxnet (2010)

- Art der Schadsoftware: Wurm für Windows
- Geschätzte Entwicklungskosten: ca. 1 Millionen US-$
- Verbreitet sich autonom und sucht eigenständig nach geeigneten Systemen zur Infektion
  - Nutzt Zero-Day-Exploit
- Angriff auf Industrieanlagen, sehr spezialisiert
  - betroffen: Siemens-Steuerungssysteme (SPS) die unter Windows laufen
  - Beeinflussung von Frequenzumrichtern
- Löscht sich nach bestimmter Zeit selbst
- Eingebracht in abgeschottete Systeme über USB-Sticks

http://www.informatik.uni-oldenburg.de/~iug10/war/texte/vorfaelle.html#w32
(Saalbach, 2012)

113

Cyberwar – Beispiel: Flame

- Stuxnet Nachfolger??
- Wurm/Trojaner für Windows-Rechner
  - Sehr umfangreiche Funktionalität, sowohl Wurm als auch Trojaneraktivität
- Fernsteuerung und Ausspionierung von Rechnern, Auswertung von
  - Tastatureingaben
  - Mikrofon
  - Screenshots
  - Hintertür zum Nachladen weiterer Module
- Infektion nicht über öffentl. Internet

114

Cyberwar – Beispiel: Flame

- Ablauf der Erstinfektion nicht klar
- Wahrscheinlich per Email und/oder Webseite
- Verbreitung laut Kaspersky hauptsächlich im Nahen Osten
- Sehr gute Verschleierung der Entstehung, zeitpunkt kaum bestimmbar
- Schadsoftware löscht kann sich selbst löschen

115

Cyberwar: Schutz

- In Deutschland verantwortlich: BMI → BSI
- Bundeswehr hat eigene Cyberwar-Einheit gebildet
  - Seit 2006 im Aufbau
  - Militärstrategisches Ziel: Überlegenheit im Cyberspace → Beherrschung des Cyberspace im Konfliktfall
- Cybersoldaten aus den Informatik-Fakultäten der Bundeswehr-Unis
- Ziel: in fremde Netzwerke eindringen, sie auskundschaften, manipulieren und ggf. zerstören.
- Probleme: Kriegsrecht für Cyberwar
  - Parlamentsvorbehalt
  - NATO-Bündnisfall?

http://www.spiegel.de/netzwelt/netzpolitik/experten-suchen-nach-kriegsrecht-fuer-den-cyberwar-a-836566.html

116

Cyberwar: Probleme

- Wann ist eine Computerattacke ein "bewaffneter Angriff"?
- Wer schützt die Opfer?
- Wie kann und wird man sich verteidigen?
- Ist ein Wurm eine letale Waffe?
- Darf mit konventionellen Waffen auf einen Angriff im Cyberspace geantwortet werden?
  - Obama sagt ja -> Spiegel-Online, 1.6.2011
- Oder nur mit einem Computer Networt Defence?
- Darf ein Cyberkrieg nur im Cyberspace stattfinden?

117

Cyberwar – Literatur

(aufgerufen: 30.06.2012)

- http://www.spiegel.de/netzwelt/web/trojaner-flame-so-arbeitet-der-virus-a-835652.html
- Saalbach, 2012: Cyberwar, Grundlagen-Methoden-Beispiele, Version 4, 25.03.2012, Universität Osnabrück, Fachbereich 1, URL: http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-grundlagen-geschichte-methoden.pdf
- http://www.spiegel.de/netzwelt/netzpolitik/experten-suchen-nach-kriegsrecht-fuer-den-cyberwar-a-836566.html
- http://www.informatik.uni-oldenburg.de/~iug10/war/index.html
- http://www.fas.org/sgp/crs/terror/RL32114.pdf
- http://www.spiegel.de/netzwelt/netzpolitik/ist-ein-cyberkrieg-ein-krieg-a-841096.html