# Sicher im Internet

PC-Treff-BB
Peter Rudolph
12.12.2015

# Risiken

- Viren
  - böswilliges Programm
  - automatische Verbreitung (Ansteckung)
  - Ziel: PC funktionsuntüchtig machen
- Trojaner
  - böswilliges Programm
  - Ziel: Rechner kontrollieren, Daten / Passwörter stehlen
- Passwortdiebstahl
- Identitätsdiebstahl
- Crypto-Ransomware
  - PC wird verschlüsselt, Lösegeld für Entschlüsselung
- Datenhunger der Werbeindustrie
  - Persönlichkeitsprofil

# Einfallstore (1)

- Mail-Anhänge
  - Scripte, Programme, Makros in Dokumenten
- Scripte in Mails
  - ActiveX, VBScript, JavaScript
  - Nicht im Thunderbird
- Scripte im Browser
  - JavaScript, Java, Flash
  - Nur Microsoft: ActiveX, VBScript
- Viren auf Datenträgern (USB-Sticks)
  - Autostart, Skripte, Programme

# Einfallstore (2)

- BadUSB-Sticks
  - Meldet sich als Tastatur an und steuert PC fern
- Offene Ports am PC
  - PC bietet Dienste an
- Schlecht gesichertes WLAN
  - schlechtes Passwort bzw. Originalpasswort
  - Verschlüsselung mit WEP
  - Vereinfachte Anmeldung mit WPS

# Vertrauensmissbrauch

- Nachgebaute WebSite (Shop, Bank, ...)
  - sieht aus wie Original ist aber auf anderem Server
- Phishing-Mail
  - Bitte um Passwortzusendung
  - Link auf nachgebaute WebSite
- Gehackte WebSite (Shop, Bank, ...)
  - Auf Original-Server eingeschleuster böswillige Funktion

# Löcher im PC

- Scripte greifen auf Platte zu
  - Browser
  - Mail
  - Office
- Offene Ports
  - Konzeptfehler in Diensten
  - Programmierfehler in Dienste
  - Angriffe (Portscans) oft schon wenige Sekunden nach Verbindung mit Internet
- Arbeiten mit Admin-Rechten

# Löcher in der Firewall

- Fernwartung
  - schlechtes Passwort
  - Programmierfehler
- Schlamperei beim Hersteller
  - Programmierfehler
  - Default-Passwörter

# Lösungen - generell

- Risiko gegen Nutzen abwägen
  - Je nach Anwendung gehen einige der Tips auf den folgenden Seiten zu weit
- Plausibilität prüfen, z.B.
  - Macht es Sinn, dass mir jemand so eine Mail schickt?
  - Welchen Nutzen hat jemand davon, wenn er mir etwas kostenlos anbietet, z.B.
    - Daten sammeln für gezielte Werbung
    - Kontolle über PC erlangen (Trojaner, SPAM-Versand)
  - Android-Handy: Braucht die App wirklich all sie geforderten Rechte?
    - z.B. Taschenlampe die Internetzugriff möchte
    - Kritisch: Identität, Adressbuch, Telefon

# Lösungen - Firewall und Betriebssystem

- Firewall (meist im Router eingebaut)
  - Zugriff von außen auf PC erst mal verboten
  - Port-Weiterleitung ermöglicht gezielte Zugriffe
  - Fernwartung ausschalten
  - UPnP ausschalten
- Betriebssystem: Linux statt Windows
  - keine Viren
  - keine Admin-Rechte beim normalen Arbeiten
  - Philosophie: Sicherheit geht vor Komfort
  - weniger verbreitet
- Windows nie ohne Antiviren-Programm und Firewall nutzen!

# Lösungen - Sicherere Software

- Browser
  - Firefox statt Microsoft
- Mail
  - Thunderbird statt Outlook
- Software nur von verlässlicher Quelle
  - Kostenlose Angebote kommerzieller Software (v.a. Spiele) sind oft mit Viren verseucht

# Lösungen - Browser

- Firefox statt Microsoft
- NoScript-Plugin
  - Scripte nur dann erlauben wenn nötig
- Flash Blocker
  - Verhindert automatisches Ausführen von Flash
- Java
  - Nur nutzen wenn benötigt
  - Quelle prüfen
- Nicht alle Passwörter speichern
  - v.a. keine die Zugang zu Rechnern, Bank, ... bieten

# Lösungen - Umgang mit Mails

- Thunderbird statt Outlook
  - Mailprogramm ohne Script (Firefox seit v3)
- Suspekte Mails löschen
  - Offensichtlich schlechtes Deutsch
  - Absender mit seltsamer Domain
  - Link auf seltsame Domain
- Links vor Klick prüfen
  - Mit Maus über Link fahren -> passt die URL zum Ziel
  - http://www.utrace.de zeigt wo die URL gemeldet ist
- Vorsicht mit Anhängen
  - "Rechnung.pdf.exe"
  - Zip-Datei mit "Dokument.doc.exe"
  - Makros in Word / Excel / PowerPoint
- Mails verschlüsseln

# Lösungen - Passwörter

- Für jeden Dienst ein eigenes Passwort
  - Passwort-Safe
  - Passwort-Algorithmus
- Keine Namen, Hobbys, Geburtsdaten
  - "social Engineering"
- Keine Wörter verwenden
  - Wörterbuchattacke
- Passphrase hilft beim merken
- Passwörter niemals verraten
  - auch keinem (scheinbaren) Techniker
  - erst recht nicht am Telefon oder per Mail
- Passwörter nie per Mail, Chat, Skype... senden

# Lösungen - Daten (1)

- Browser
  - Daten nur verschlüsselt übertragen (HTTPS)
  - Werbe Blocker nutzen, z.B. Adblock, uBlock)
  - NoScript nutzen
  - Cookies regelmäßig löschen
  - Alternative Suchmaschine nutzen, z.B. "Startpage.com"
- Mails
  - Daten nur per verschlüsselter Mails übertragen
  - Mails runter laden und nicht auf Server lassen
- Möglichst wenige Daten im Web lagern
  - Web-Mailer vermeiden
  - Cloud-Dienste vermeiden
- Handy
  - Google Search deaktivieren
  - Sprachsteuerung nicht verwenden (läuft auf Server)

# Links

- Wikipedia "Informationssicherheit"
  - https://de.wikipedia.org/wiki/Informationssicherheit
- Sicherheitschecks von Heise (c't, iX)
  - http://www.heise.de/security/dienste/
- Zuordnung URL / IP zu Weltkarte
  - http://www.utrace.de
- NoScript
  - https://noscript.net/
- Website des BSI
  - https://www.bsi-fuer-buerger.de