PC-Sicherheit

Georg Schöbel

Chaostreff
Göttingen

26. Mai 2008

Gliederung

Warum?

- Grundlagen
- Aspekte der Sicherheit:
  - Verlust der Vertraulichkeit
    Bsp.: Ihr Arbeitgeber sieht ihre Bewerbung bei der Konkurrenz.
  - Verlust der Integrität
    Bsp: Bei ihrer Onlineüberweisung wird das Zielkonto geändert.
  - Verlust der Verfügbarkeit
    Bsp.: Alle ihre digitalen Fotos sind gelöscht.
- Prävention
- Technische Maßnahmen

Für wen und was?

- für den Standard-Privat-Nutzer
- Windows
- mit Bordmitteln
- bzw. kostenfreien oder kostengünstigen Lösungen
- praxisorientiert
- zahlreiche Alternativen
- „80:20-Regel“

Das Wichtigste:

Gesunder Menschenverstand

BACKUPS!

Motivation:

Festplatten-Versagen [Google-Paper]

- 23% in 3 Jahren
- 36% in 5 Jahren

Verdoppelung bei Temperaturunterschieden von über 15°C.

Nicht nur deshalb: Backups

- regelmäßig
- getestet
- sicher gelagert

Paranoia ist (hier) gut!

Methoden und Medien

- Was sichern?
  - Betriebssystem und Programme
  - Anwendungsdaten
- Wie sichern?
  - Vollsicherung
  - Differentielle Datensicherung
- Worauf sichern?
  - Festplatte
  - CD/DVD/Blu-ray
  - USB-Stick
  - Bandlaufwerk
- Einfache Anleitung zum Anwendungsdaten-Backup der Uni Bonn
- c't Ausgabe 9/2006, S. 104 ff. und Ausgabe 12/2007, S. 158 ff.

Nutzerverwaltung

Normale Installation unsicher:

- Meist nur ein Konto mit Administratorrechten
- => Schadprogramme (Viren etc.) haben Vollzugriff
- Komfort vs. Sicherheit

Abhilfe bis Windows XP:

- Administrator-Konto nur für Verwaltungsaufgaben
- Nutzerkonten für Surfen, Emailen, Office etc.
- Sichere Passwörter verwenden

ab Vista: Benutzerkontensteuerung, User-Account-Control (UAC)

Nutzerverwaltung

Nutzerverwaltung

Neue Konten anlegen:

Systemsteuerung -> Benutzerkonten -> Konto ändern -> neues Konto erstellen

Kontentyp ändern:

Systemsteuerung -> Benutzerkonten -> Konto ändern -> (eigenen) Kontotyp ändern

Passwort setzen:

Systemsteuerung -> Benutzerkonten -> Konto ändern -> Kennwort erstellen

- Welche Probleme gibt es?
- Lösungen: suDown, MachMichAdmin (s. c't 5/07 S.138)

Passwörter

- Setzen!
- Mehrere, unterschiedliche Passwörter
- Sichere Passwörter wählen:
  - mindestens 8 Zeichen
  - Groß- und Kleinschreibung
  - Zahlen
  - Sonderzeichen

Mein Namenstag ist der 23. April!

MNid23.A!

- Passwort-Safe: KeePass von Bruce Schneier.

Firewall

- Windows Firewall blockt eingehende Verbindungen

Windows Firewall

START - Systemsteuerung - Netzwerkverbindungen

rechte Maustaste->Eigenschaften

Reiter Erweitert

- *Internetverbindungsfirewall* aktivieren

- erst ab Windows XP SP2 standardmäßig aktiviert
- Kein Schutz bei abgehenden Verbindungen
- ab Vista verbessert: Standorte

Alternative Firewall: ZoneAlarm

pro:

- kostenfrei für Privatanwender
- für Windows 2000, XP und Vista
- blockt auch abgehende Verbindungen

contra:

- Störung des Normalbetriebs
- aufwändigere Konfiguration/Lernphase
- Fachwissen nötig

Allgemeine Anmerkung:

- Schadprogramme umgehen Firewalls oft
- trügerische Sicherheit

Updates

- Jede Software enthält Fehler
- Behebung durch Updates
- Mircosoft: Hotfixes => Servicepacks

Maßnahmen:

- Servicepacks einspielen
- Automatische Updates aktivieren
  - Windows Vista, XP, Me, 2000 => Windows Update
  - Microsoft Office => Office Update
  - Windows + Office => Microsoft Update (ab Office 2003)
  - Sonstige: Flash, Quicktime, Java etc.
- Aktualitätsprüfung für über 4000 Programme:
  Secunias Personal Software Inspector (PSI)

Antivirus

Was ist ein Virus?

- selbstverbreitendes Programm
- häufig mit Schadfunktion
- umgangssprachlich auch für Würmer und Trojaner genutzt

Prävention:

- Aktualität der Virenerkennung
- häufige, automatische Updates
- Kostenlose Antiviren-Programme
  - AntiVir Personal - Free
  - AVG Anti-Virus Free

Wenn der Virus schon da ist:

- Knoppicillin
- Ausleihe der CD z.B. bei Stadtbibliothek Göttingen
  Titel: „c't 2007,26. Software-Kollektion 8“

Spyware/Malware

Was ist Spyware?

- Spyware: Kann z.B. ihre persönlichen Daten weiterleiten
- kann die Systemleistung deutlich einschränken

Prävention:

- Microsofts Echtzeitschutz:
  - Windows Defender
- für Windows XP kostenlos; in Vista bereits vorhanden

- Weitere kostenlose Anti-Spyware/Malware-Programme
  - Spybot Search&Destroy
  - Lavasoft Ad-Aware
  - Microsofts Tool zum Entfernen bösartiger Software

Festplattenverschlüsselung

Problem:

- Physischer Zugriff umgeht alle Sicherungen

Abhilfe:

- Verschlüsselung der gesamten Festplatte
- insbesondere für Notebooks
- TrueCrypt
  - kostenlos
  - Open Source
  - einfache Anwendung
  - sicher (selbst bei Stromausfall)
  - AES-Verschlüsselung
  - hohe Performance
  - Notfallmedium
- ausführlicher c't Artikel

Anmerkung: Ohne Passwort keine Daten

Sicheres Löschen

Löschen einer Datei:

- nur Verzeichnis gelöscht
- Inhalte noch da

Abhilfe:

- Inhalte gezielt überschreiben: SDelete
- oder alle ungenutzten Plattenbereiche: Eraser

Anmerkung: Reserve-Sektoren

WLAN

Unsichere Funknetzwerke:

- weite Verbreitung: Notebooks, Router, etc.
- häufig unsicher ab Werk
- Übertragung im Klartext

Abhilfe:

- Verschlüsselung
- Methoden: WEP, WPA, WPA2
- WEP ist gebrochen (Aktiver Angriff <5min)
- WPA2 mit sicherem Passwort nutzen

Systemwiederherstellung

- für Microsoft Windows ME, XP und Vista
- früheren Zustand wiederherstellen
- Wiederherstellungspunkt
  - automatisch => Systemprüfpunkt
  - manuell => Wiederherstellungspunkt

Systemwiederherstellung

Start - Programme - Zubehör - Systemprogramme - Systemwiederherstellung

Verhaltensregeln

„Die üblichen Verdächtigen“

- Vorsicht bei Email-Attachments
- Absender von Emails ist leicht fälschbar
- Downloads/Attachments nur mit aktuellem Virenscanner öffnen
- WWW: Active-X und Freunde => Vortrag „Sicher im WWW“
- Datei-Typen (Endungen) beachten
- Autostart => Kafu
- Autorun (CDs, Macros) => Shift-Taste

Danke für Ihre Aufmerksamkeit!

FRAGEN?