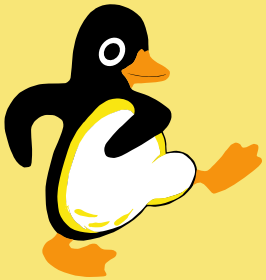


IT-Sicherheit

Dr. Ralf Schlatterbeck
Open Source Consulting

Email: office@runtux.com
Web: http://www.runtux.com
Tel. +43/650/621 40 17

Inhalt

Aktuelle Entwicklung

Zunehmend:

- Schäden durch Viren, Hackerangriffe, . . .
- Belastung durch unerwünschte Email (Spam)

Pro Virenangriff durchschnittl. Kosten von 5000.- €

Quelle: Niederösterreichische Wirtschaft Sept ’04

Umfrage

Mindestens 1 schwerer Angriff auf die IT-Sicherheit

- 2004: 58% der Unternehmen (2003: 38%)
  → bereits 1. Halbjahr 2004 mehr Angriffe als 2003!
- Nur 51% haben schriftliche IT-Richtlinien
- Nur 57% haben Disaster-Recovery-Plan

Quelle: Niederösterreichische Wirtschaft Sept ’04

→ Wie sieht es mit *Ihrer* Datensicherheit aus?

Schadprogramme

- Virus: infiziert Programme
- Wurm (Worm): infiziert Rechner
  - → Grenze zwischen Viren und Würmern verschwimmt
- Trojanische Pferde (Trojan Horse)
  - Dialler
  - Spyware
- Social Engineering (scherzhaft auch „Sozialarbeit“)
  - Hoax, Phishing

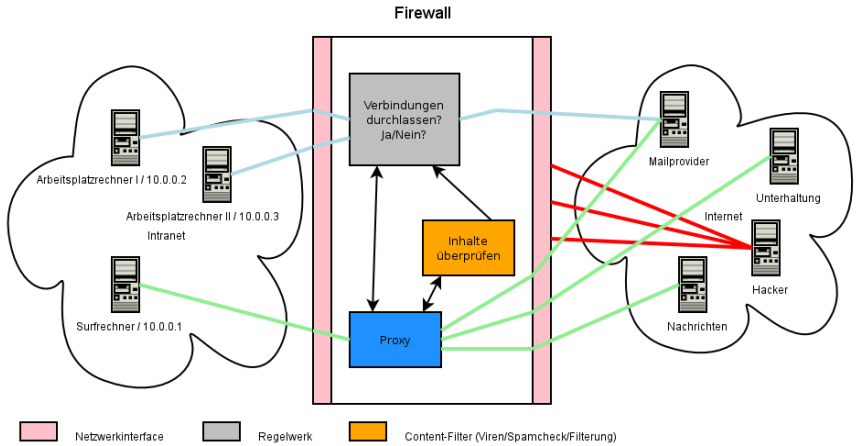
→ Zunehmend: Kriminelle Aktivitäten!

„Infektionswege“

- Email
  - gefährliche Anhänge (.exe, .com, .bat, . . .)
  - Macros in .doc, .xls, . . .
  - harmlose Anhänge (.jpg) aber Fehler in Programmen
- Direkt aus dem Internet während der Verbindung
- CD, DVD, Memory-Stick, Diskette, . . .
- Neue Verbindungstechniken: WLAN, Bluetooth

→ Zunehmend auch auf mobilen Geräten: Handy!

Schutz: Firewall Überblick



Quelle: Wikipedia, die freie Enzyklopädie wikipedia.org

Schutz: Firewall

- Schützt während Verbindung zum Internet
- Blockiert eingehende Verbindungen
- Optional Blockieren von ausgehenden Verbindungen (zum Internet)
- Braucht professionelle Wartung
  - Sicherheits-Updates
  - Analyse von Logdateien
  - Testen der Firewall

Schutz: Mail-Filter

- Filterung von gefährlichen Email-Anhängen
- Antivirus
- Filterung von unerwünschter Email
  - Spam
  - Social Engineering: Phishing
- größtes Problem: Email ist anonym

→ Lernende Filter
→ Zukunft: Authentifizierung von Mails

Schutz: Antivirus

- Schützt einzelnen Rechner
- Prüft ausführbare Dateien
- Verdächtige Aktivitäten
- Braucht regelmäßige Pflege
  - Neue Virenkennungen
  - (Automatisches) Update über Internet möglich
- Sollte auf *jedem* Rechner installiert sein!

Schutz: Datensicherung

„Das einzig sichere Kriterium einer erfolgreichen Datensicherung ist der Nachweis, dass die gesicherten Daten auch vollständig und innerhalb eines angemessenen Zeitraums wiederhergestellt werden können.“
Quelle: Wikipedia, die freie Enzyklopädie wikipedia.org

Kriterien:

- Wie, Wer, Wann, Welche Daten
- Welches Medium, Aufbewahrung: Wo, Wie lange
- Überprüfung Wiederherstellung: Wann und Wie

Open Source für Sicherheit

- Verfügbarkeit des Programm-Quelltextes (=Source)
- Geringere (Lizenz-) Kosten
- Finanzierbarkeit von Sicherheit
- Kerckhoffs[1] Prinzip: Sicherheit nicht durch Geheimhaltung der Verfahren

Open Source Experts Group der Wirtschaftskammer: opensource.co.at

[1] Niederländischer Militär-Kryptologe 1835-1903

Open Source Consulting

- Mitarbeit in IT-Security Experts Group
- Mitarbeit in Open Source Experts Group
- Beratung und EDV-Dienstleistungen
- Schwerpunkt auf Sicherheit
- Open Source auf Firewall, Server, Arbeitsplatz
- Anpassung und Erstellung von Software
- Web (Intra- und Internet) basierte Anwendungen