

# Technische Grundlagen der IT-Security

Dr. Gerhard Laga

E-Center der WKÖ

Verstehen. Denken. Handeln.



# Die Bedrohung im IT-Umfeld

- Offenes Netzwerk, wo sich „Gute“ und „Böse“ (ungewollt) treffen
- Kein greifbarer „Gegner“
- Rechtsproblematik, da weltweites Phänomen
- „Kavaliersdelikt“ Hacking entwickelt sich zu illegalem „Businessmodell“

# Massenhaft verschickte E-Mail-Werbung (Spam)

- Zumindest 70 Prozent des E-Mailverkehrs ist massenhaft ungezielt versendete Werbung
- Tendenz stark steigend
- Das Aussortieren bindet Mitarbeiter und deren Arbeitskraft
- Spamming-Verbot in Österreich greift international nicht
- Technische Maßnahmen sind nötig!

# Phishing und Dialer

- **Phishing**
  - Mittels gefälschten E-Mails soll den Empfängern Passworte oder PIN/TAN Kombinationen entlockt werden
  - Technische Vermischungsgefahr, wenn mehrere Browserfenster geöffnet sind
  - Abhilfe:
    - Aktuelle Browserversion verwenden
    - Telebanking nur über eigene Bookmarks starten
    - Banken werden Digitale Signaturen einsetzen und ermöglichen
- **Dialerprogramme** können den Wählleitungszugang auf eine kostenpflichtige Telefonnummer umleiten

# Viren und Schadprogramme

- **Computerviren** können die gesamte Softwarelandschaft eines Unternehmens zerstören
  - Sie werden hauptsächlich via E-Mail verbreitet
  - Nur ein zumindest wöchentlich aktualisiertes Anti-Virenprogramm kann schützen
- **„Trojanische Pferde“** nisten sich in PCs (meist unbemerkt) ein
  - Sie zerstören nichts und verhalten sich meist unauffällig, Dritte können den PC aber ohne Ihr Wissen fernsteuern!
  - Diese Rechen- und Netzleistung wird illegal verkauft zB für
    - Spamversand
    - Verteilte Netzangriffe (DDOS-Attacken)
  - Eine aktuelle Firewall kann Ihren PC dagegen schützen

# „Soft Facts“ mit gravierenden Auswirkungen

- Fehlende Wartung und Aktualisierung der Software
- fehlende Datensicherung
- mangelndes Notfallkonzept
- Schäden werden - oft auch unbewusst - durch eigene (Ex-) Mitarbeiter verursacht

# Verantwortung der Geschäftsführung

- IT-Sicherheit ist mittlerweile geschäftskritisch!
  - Überlegen Sie den Schaden, der durch den Verlust aller Ihrer elektronischen Daten entstehen würde!
- Der Geschäftsführer hat die Haftung für Datensicherheit nach § 33 Datenschutzgesetz zu tragen!
- Eine sichere IT-Infrastruktur wird bald kreditrelevant (Basel II)!

# VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

- Initiativen der WKÖ
  - Fachverband UBIT: It-Security Experts Group  
[www.ubit.at/expertsgroups](http://www.ubit.at/expertsgroups)
  - Initiative Informationssicherheit Austria  
[www.iisa.at](http://www.iisa.at)
- Weitere Informationen finden Sie unter
  - [wko.at/it\\_security](http://wko.at/it_security)
  - Hotline der Sicherheitskampagne: 0800 221 221