Moderne EDV im kleinen und mittelständischen Unternehmen

EDV – Sicherheit im Zeitalter des Internet

Vortrag von Alexander Kluge-Wolf

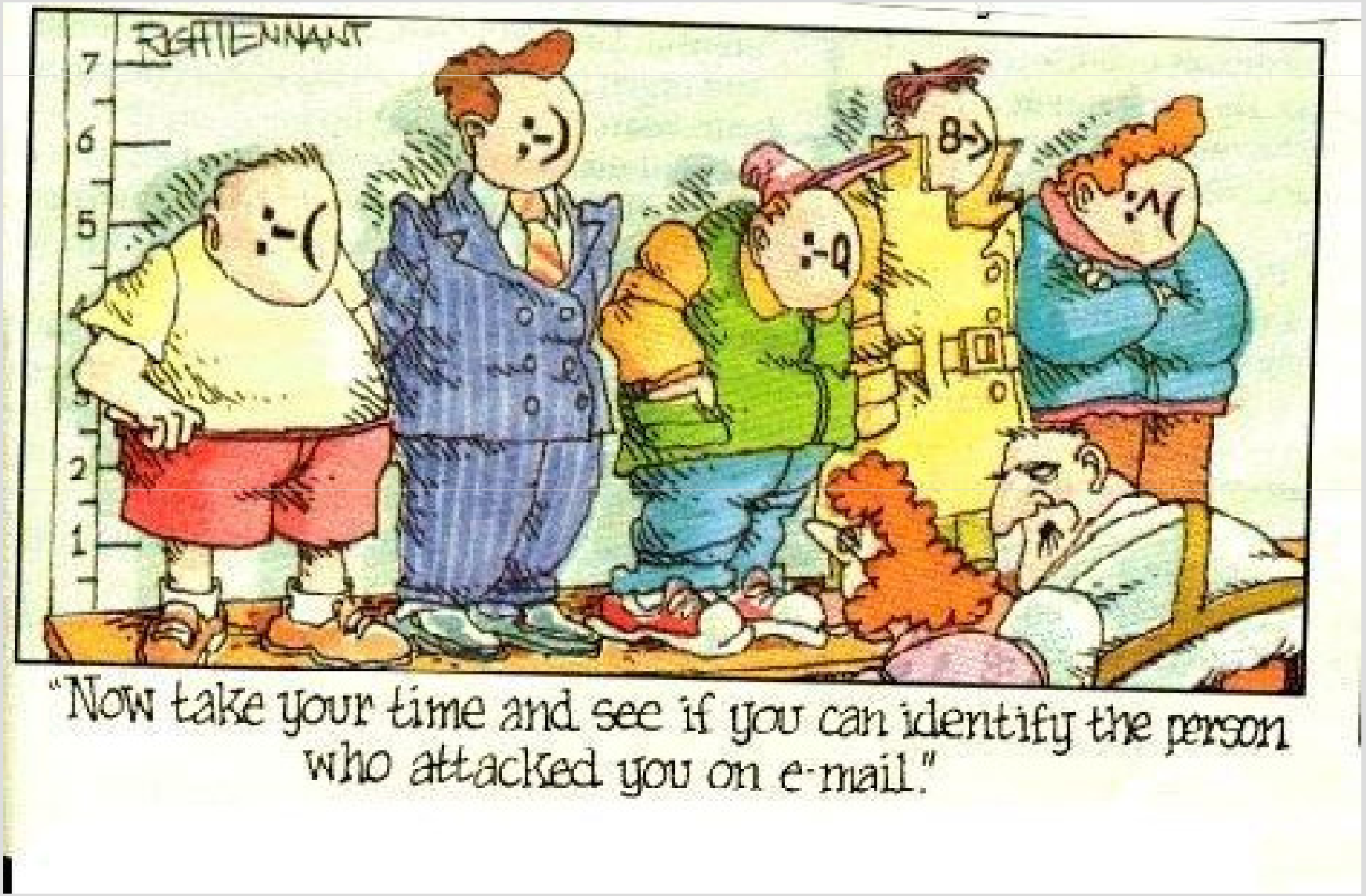
Themen

- AKWnetz, IT Consulting & Services
- „Mir kann ja nichts passieren“
- Risiken für die EDV Sicherheit
- Datensicherheitskonzepte
- praktisches Beispiel anhand von HAPAK Pro

AKWnetz, Alexander Kluge-Wolf

- Analyse
  - Prozesse
  - Ist-Zustand
  - Sicherheit
- Beratung
  - Abbildung der Geschäftsprozesse
  - Konzept zur Optimierung der EDV
  - Erstellung von Sicherheitskonzepten
- Service
  - Durchführung der Maßnahmen
  - Administration der EDV Infrastruktur
  - Hilfe in allen EDV Fragen (Support, Schulung…)

„Nehmen Sie sich die Zeit und versuchen, den zu finden, der Sie per E-Mail angegriffen hat“



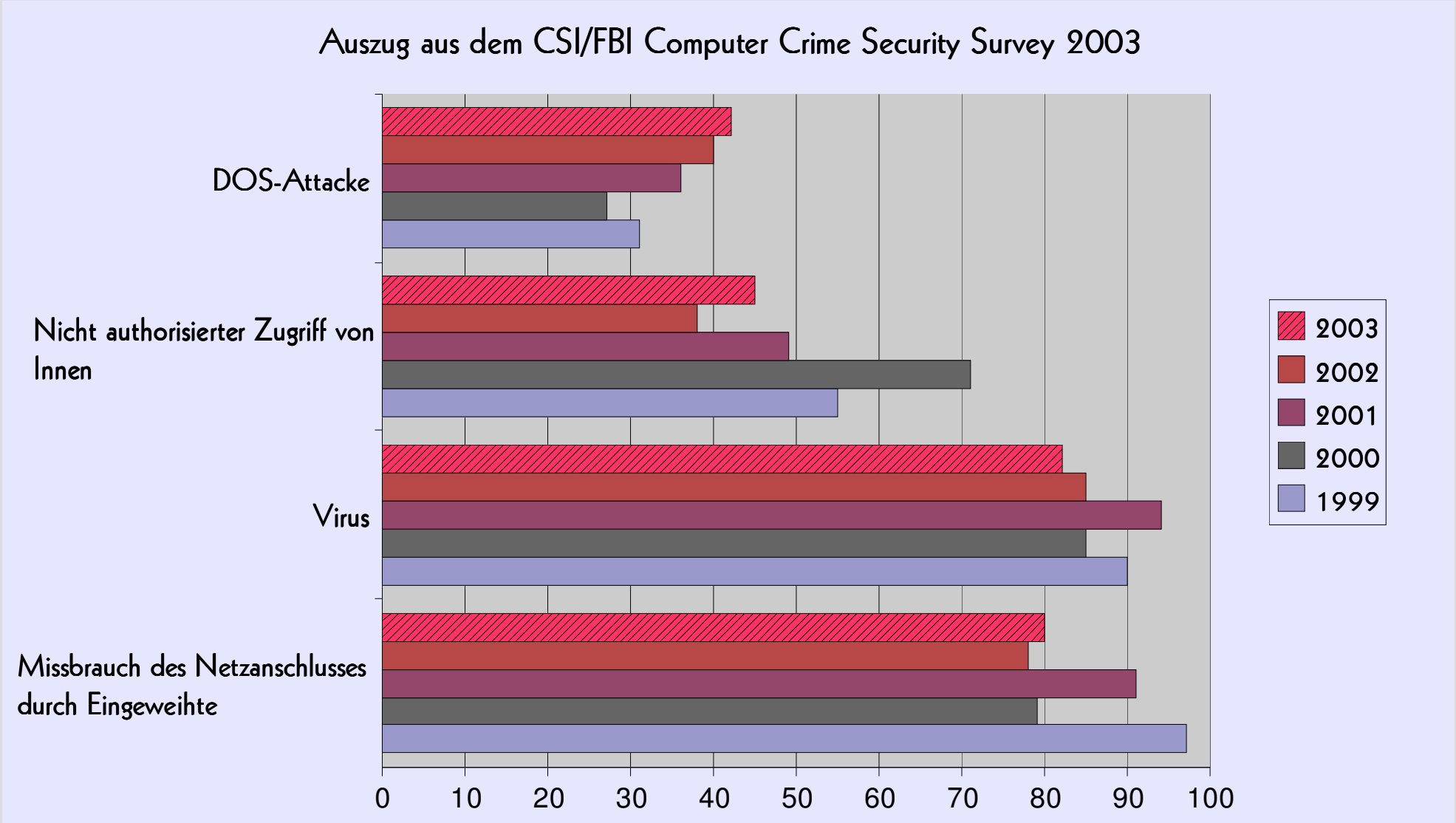
Behauptungen

- Bei uns ist noch nie was passiert
- Bei uns ist doch nichts Interessantes zu holen
- Unser Netzwerk ist sicher
- Unsere Mitarbeiter sind absolut vertrauenswürdig
- Das betrifft doch nur große Firmen

Die Realität

- 2003 sahen laut CSI/FBI Bericht fast 80% der befragten Firmen die Internet Verbindung als Hauptangriffspunkt an.
- Laut einer anderen Untersuchung sind 5% der westlichen Bevölkerung potentiell kriminell.
- Passend dazu sehen im CSI Report 77% der Befragten Firmen Ihre Mitarbeiter als Ursache für Angriffe, dies ist fast gleich auf mit Angriffen von unabhängigen Hackern (82%) von außen.
- Angriffe von Konkurrenten (Werkspionage) liegen bei 40%
- Von den nachgewiesenen Attacken/Fehlanwendungen der letzten 12 Monate liegen Virenangriffe und Missbrauch des Netzanschlusses durch Eingeweihte (Mitarbeiter,….) praktisch gleich auf.

Typen der nachgewiesenen Attacken oder Missbräuche in den letzten 12 Monaten



IT Sicherheit ist nicht nur Internet Sicherheit

- Physikalische Gefahren (Brand, Diebstahl, Vandalismus, Wasser, Blitzschlag)
- Mitarbeiter, Servicefirmen (Unwissenheit, Versehen, Frust, Rache)
- Keine oder unsichere Passworte
- Keine oder unzureichende Pflege der IT, Hard wie Software (z.B. regelmäßige Updates der Antivirensoftware und des OS)

Gibt es absolute IT Sicherheit?

Garantiert sicher nur durch

„Richards Gesetz der Datensicherheit“ :

„Kaufen Sie keinen Computer. Und wenn

Sie es doch tun, schalten Sie ihn nicht ein.“

Zitate aus „hacker‘s guide“ Seite 420

ISBN 3-8272-5931-2

Sicherheitsmaßnahmen, wie gehe ich vor

- Sicherheit ist kein statischer Zustand, sondern ein Prozess
- VVI (Vertraulichkeit, Verfügbarkeit, Integrität)
- Vorschriften und Gesetzesanforderungen
- Konsequenzen eines Ausfalls für das Unternehmen und persönlich
- Basel II und IT Sicherheit, IT Risiken des Kreditnehmers werden von Banken berücksichtigt!
- IT Grundschutz kompakt gibt einen Überblick
- IT Grundschutzhandbuch als Referenz (beides vom BSI, Bundesamt für Sicherheit in der Informationstechnik)

Praktische Erstmaßnahmen

- Datensicherung (Backup) und Rücksicherung testen!
- Datenträger unbedingt auch an einem anderen sicheren Ort aufbewahren (z.B. Bankschließfach)
- Antiviren Programm installieren, auf allen Rechnern und Updates automatisieren
- Hardware oder Softwarefirewall installieren, je nach Anbindungsart. Diese auf jeden Fall von Außen testen lassen
- Sicherheitspatches regelmäßig auf allen Systemen einspielen!
- Nur die Ports und Dienste laufen lassen die für den Betrieb erforderlich sind. Alles andere durch die Firewall sperren und im OS abschalten.
- Die Standard OS Installation dringend überprüfen! Z.B. Administrator umbenennen, Dienste die nicht benötigt werden deaktivieren.
- Möglichst sichere Passwörter wählen und Mitarbeiter durch Regeln im OS zu vernünftigen Passwörtern und regelmäßiges ändern zwingen (min 8 Zeichen mit Sonderzeichen, „$wibUbak3“

Weiterführende Maßnahmen

- Sichern Sie auch intern Ihre Daten. Will heißen, jeder Mitarbeiter bekommt im Netzwerk nur das zu sehen was er für seine Arbeit braucht!
- Überprüfen Sie Ihre Haussicherheit (Schlösser, Türen, Fenster, Alarmanlage)
- Installieren Sie für Ihre Server eine USV oder zumindest einen Überspannungsschutz.
- Dokumentieren Sie Ihre EDV möglichst genau. Diese Doku sollte unbedingt an einem wirklich sicheren Ort aufbewahrt werden.
- Achtung WLAN! Hier unbedingt alle Sicherheitseinstellungen einschalten! Sonst kann JEDER auch außerhalb Ihrer Räumlichkeiten auf Ihre Daten zugreifen.
- Nutzen Sie alle Sicherheits-möglichkeiten Ihrer Software (z.B. gesonderte Benutzer in der Warenwirtschaft oder anderen Datenbanken).

Spruch des Monats

Es gibt drei Möglichkeiten, eine Firma zu ruinieren:
mit Frauen, das ist die angenehmste;
mit Spielen, das ist die schnellste;
mit Computern, das ist die sicherste.

Oswald Dreyer-Eimbcke, deutscher Unternehmer