Security Awareness
Der «Stein der Weisen» der IT Sicherheit?

Dr. Wolfgang Schnabl, CISSP
IT-Sicherheitsbeauftragter
NextiraOne Austria
September 2006

Zitate

IISA
Initiative Informationssicherheit Austria

- Bruce Schneier
  - IT Security Guru

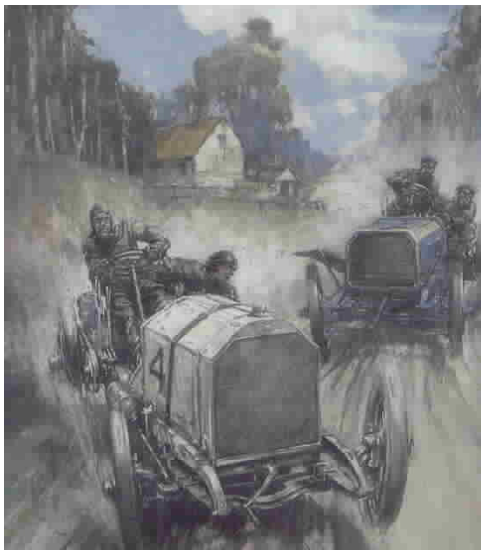
Amateure hacken Systeme...
Profis hacken Menschen

- Kevin Mitnick
  - Berüchtigter Hacker der 90er Jahre, 5 Jahre Haft

Aussage vor dem Kongress der USA
  - Ich war mit Social Engineering so erfolgreich, dass ich nur äußerst selten auf technische Attacken zurückgreifen musste.

In seinem Buch:
  - Um ein guter Hacker zu sein ist es nicht notwendig ein guter Techniker zu sein. Es reicht, wenn man ein guter Lügner ist.

Warum Sicherheit?



Warum Sicherheit?

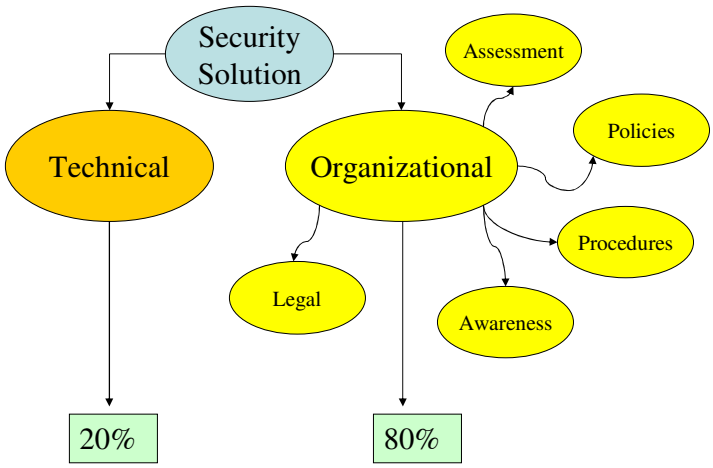
- Technische Maßnahmen:
  - Aktive Sicherheitseinrichtungen
    - ABS, ASR, ESP
  - Passive Sicherheitseinrichtungen
    - Sicherheitsgurt, Airbag, Kindersitz
- Organisatorischen Maßnahmen
  - Verkehrslenkung (Verkehrsschildern; Verkehrsleitsysteme)
  - Verkehrsüberwachung und straßenbauliche Maßnahmen
  - gesetzliche Regelungen (Gurtpflicht, Telefonierverbot)
- Persönliche Maßnahmen
  - defensives Fahren
  - korrektes Einhalten der Verkehrsvorschriften
  - Training der Fahrzeugbeherrschung (Fahrsicherheitstraining)

Warum Sicherheit?

- Technische Maßnahmen:
  - Aktive Sicherheitseinrichtungen
    - Firewall, Virenschutz, Antispam, IDP
  - Passive Sicherheitseinrichtungen
    - Identity Management, Penetration Tests, Log-Files, Redundanz
- Organisatorischen Maßnahmen
  - Policies, Awareness
  - Security Audits
  - Rechtsvorschriften, Gesetze
- Persönliche Maßnahmen
  - Verantwortungsbewusst handeln (Awareness)
  - korrektes Einhalten der Policies
  - Training des „Ernstfalls“

5 © W. Schnabl, 9/06 nextiraOne

Sicherheitsgesamtlösung



6 © W. Schnabl, 9/06 nextiraOne

Vor wem sollten wir uns fürchten?

- Script Kiddies
  - beinahe keine Erfahrung, Schulwissen über IT & Netzwerke
  - benutzen Dokumentationen & Tools vom Internet
  - meistens keine Beziehung zum Opfer
  - Aktionen sind nicht wirklich geplant
  - endet oft mit Zerstörungen beim attackierten System
- Spezialisten & professionelle Hacker
  - gutes bis sehr gutes IT Know-How
  - gutbezahlte Jobs (Systemadministratoren, Softwareentwickler, …)
  - ehemalige Mitarbeiter
  - lebt über seine Verhältnisse, hat hohe Schulden
  - Vorsatz: finanzieller Vorteil, Rache, Spionage, …
  - verwischen ihre Spuren und versuchen so lange als möglich ein Backdoor geheim & offen zu halten

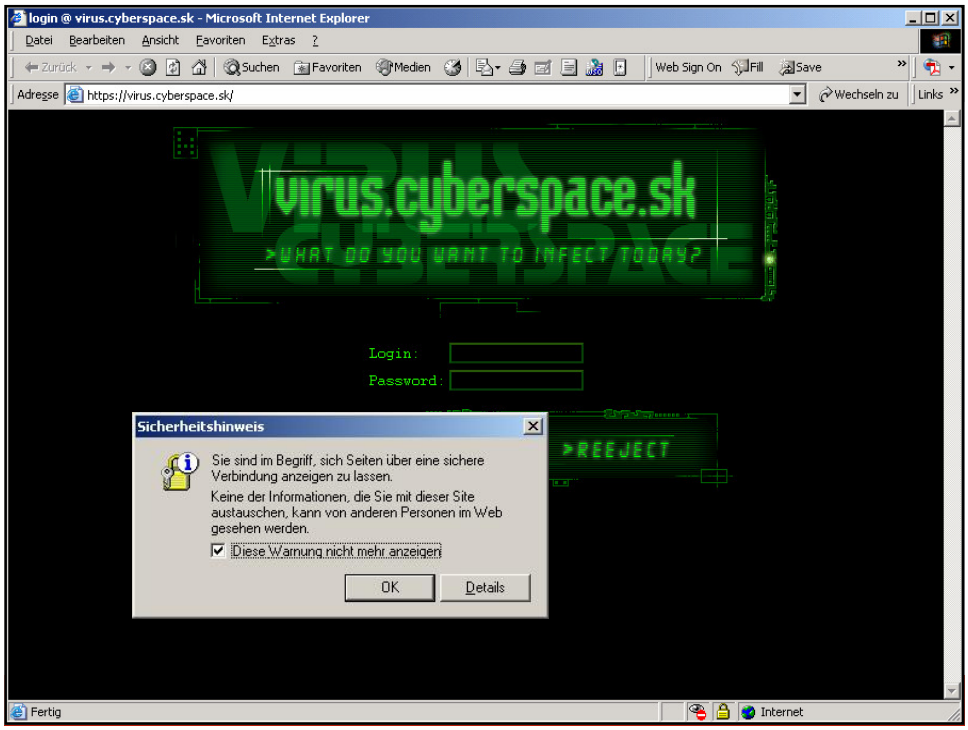
7 © W. Schnabl, 9/06

Vor wem sollten wir uns fürchten?

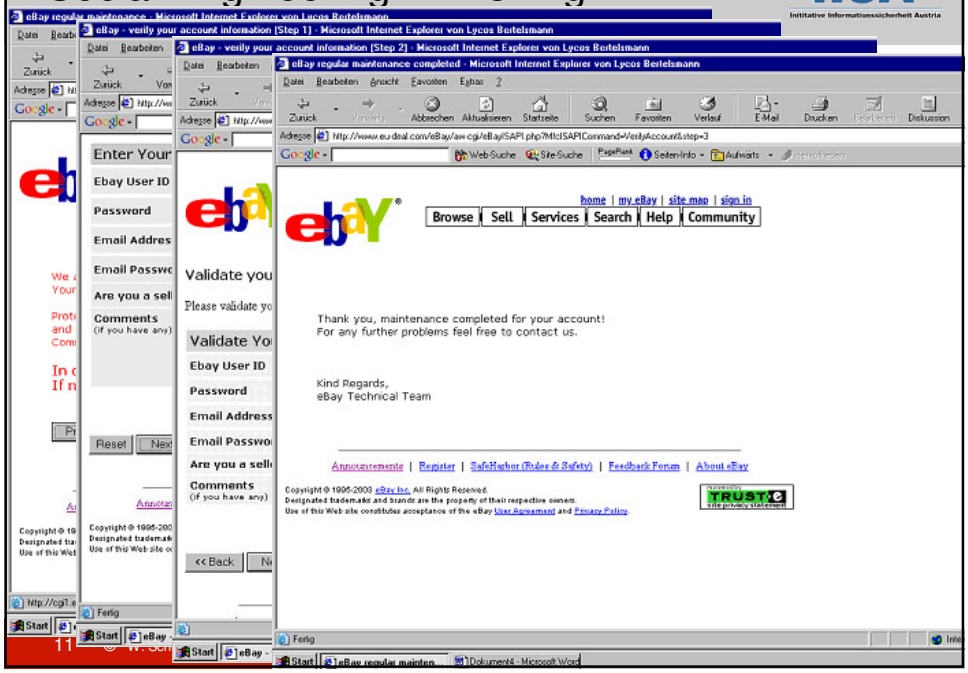
- Harmloser Benutzer
  - Unzureichend gesicherter
    - Heim-PC
    - Firmen Laptop
    - UMTS Benutzer
    - WLAN Benutzer
- Liefern die Plattform für
  - kriminelle Aktivitäten
  - automatisierte Angriffe
  - SPAM Versand

8 © W. Schnabl, 9/06


A new device has been found
Device:Airbus A310
Run Auto-configuration?
Start
Cancel
Bluetooth
Bluetooth
9


login @ virus.cyberspace.sk - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Adresse https://virus.cyberspace.sk/
virus.cyberspace.sk
>WHAT DO YOU WANT TO INFECT TODAY?
Login:
Password:
Sicherheitshinweis
Sie sind im Begriff, sich Seiten über eine sichere Verbindung anzeigen zu lassen.
Keine der Informationen, die Sie mit dieser Site austauschen, kann von anderen Personen im Web gesehen werden.
Diese Warnung nicht mehr anzeigen
OK
Details
>REEJECT
Fertig
Internet

Social Engineering - Phishing



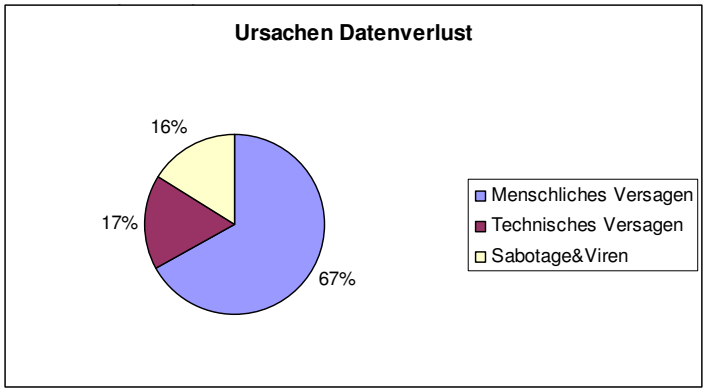
11 © W. Schnabl, 9/06

Social Engineering Specialist

12 © W. Schnabl, 9/06

Warum Sensibilisierung für IT-Sicherheit?

- Etwa 70% der sicherheitsrelevanten Vorfälle durch Mitarbeiter im Unternehmen ausgelöst
  - In den wenigsten Fällen geschieht dies absichtlich



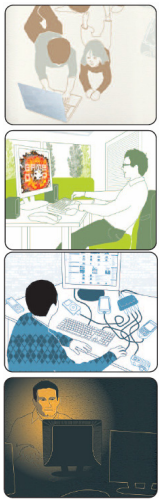
Menschliche Schwächen

Menschliche Schwächen, die für Sicherheitsvorfälle verantwortlich sind

- Vergesslichkeit
- Unachtsamkeit
- Mangelndes Problembewusstsein
- Überforderung
- Unzureichende Risiko-bewertungsmechanismen
- Zu geringe Phantasie

Gängige Anwendertypen

- **Der Unbedarfte** (der Sicherheits-Softie)
  - geringe Sicherheitskenntnisse
  - geringes Problembewusstsein
- **Der Technikinteressierte** (der Gadget-Freak)
  - verbindet alles mit allem – private mit betrieblicher IT und umgekehrt
- **Der Eigennützige** (der Illegale)
  - bricht Regeln, ohne primär andere schädigen zu wollen
- **Der Böswillige** (der Saboteur)
  - handelt vorsätzlich und mit Schädigungsabsicht



15 © W. Schnabl, 9/06 nextiraOne

Der Unbedarfte

- Zwei Drittel der User kaum Wissen über IT-Sicherheit
- Ein Viertel lässt Notebook tw. durch Familie nutzen (Italien: 42%)
- Fühlen sich nicht für ihre Geräte verantwortlich

Wie gut kennen sich die europäischen Angestellten mit IT-Sicherheit aus?

Wie viel Prozent der Angestellten geben an, dass sie von IT-Sicherheit überhaupt keine oder nur geringe Kenntnisse haben?

Europäischer Durchschnitt:	62%
Deutschland:	66%
Spanien:	62%
Niederlande:	62%
Frankreich:	56%
Großbritannien:	46%

Geben an, wenige Kenntnisse zu besitzen

Wie viel Prozent der Angestellten übernehmen selbst die persönliche Verantwortung für die Aktualisierung des Virenschutzes auf einem unternehmenseigenen Laptop oder PC?

Europäischer Durchschnitt:	22%
Spanien:	34%
Italien:	22%
Niederlande, Deutschland, Großbritannien, Frankreich:	19%

Übernehmen die meiste Verantwortung

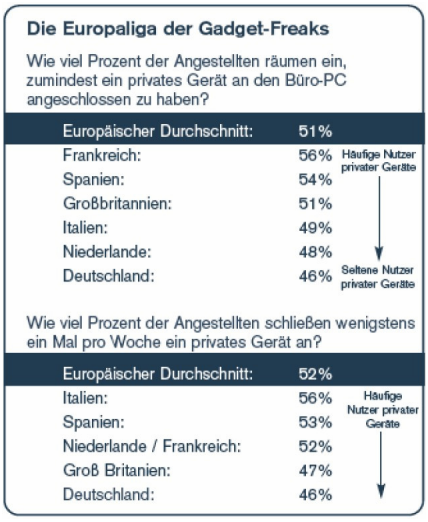
Übernehmen die geringste Verantwortung

Quelle: McAfee Studie Dez.05 „The Threat within“

16 © W. Schnabl, 9/06 nextiraOne

Der Technik-Interessierte

- Verwenden PDAs, Mobil-telefone, MP3-Player, Digitalkameras etc. ständig
- 25% schließen diese auch am Arbeitsplatz an
  - Firmengeräte
  - Netzwerk
- Diese Benutzer verursachen verstärkt Sicherheitsprobleme
  - individuelle Software
  - Aufrüstung der Standard-PCs



Quelle: McAfee Studie Dez.05 „The Threat within“

Der „illegale“ Anwender

- Verwenden betriebliche IT zu privaten Zwecken, obwohl verboten
  - Speichern private Daten
  - Verletzen z.B. Urheberrechte
  - „importieren“ Schadprogramme
  - Beeinträchtigen Leistungsfähigkeit des Netzwerk (Audio, Video, Spiele)
- Verursachen Haftungsrisiko für Unternehmensführung

Quelle: McAfee Studie Dez.05 „The Threat within“

Der „böswillige“ Anwender

IISA Initiative Informationssicherheit Austria

- Sehr geringer Anteil der Mitarbeiter (1-2%)
  - Datendiebstahl
  - Unautorisierte Dateneinsicht
  - Betrug
  - Sabotage
- Durch zunehmenden Subunternehmereinsatz verschärft sich das Problem

Nach Informationen der High Tech Crime Unit:

- 75 % aller Verunstaltungen von Websites sind das Ergebnis der Bemühungen von eigenen Mitarbeitern.
- 38 % aller Betrugsdelikte werden von eigenen Mitarbeitern begangen.
- 20 % der nicht autorisierten Zugriffe auf Unternehmenssysteme werden von innen ausgeführt.
- 68 % aller Datendiebstähle werden von Mitarbeitern begangen.[10]

5 % der Angestellten geben an, in den IT-Systemen ihrer Unternehmen auf Bereiche zuzugreifen, für die sie nicht autorisiert sind (z. B. Konten- oder Personaldaten).

Quelle: McAfee Studie Dez.05 „The Threat within“

19 © W. Schnabl, 9/06 nextiraOne

Mitarbeitersensibilisierung – Der Stein der Weisen der IT Sicherheit?

IISA Initiative Informationssicherheit Austria

20 © W. Schnabl, 9/06 nextiraOne

Mitarbeitersensibilisierung – Erstellung eines Konzepts I

- Unterstützung durch Geschäftsführung
- Erarbeitung eines individuellen Konzepts
  - Ausarbeitung mit IT-Mitarbeitern, Security Verantwortlichen
  - Beispiele aus Unternehmen
    - Statistiken
    - Erklärung der Policy
    - Security-Verletzungen
  - Beispiele von „Zu Hause“
    - Home Firewall-Logs
    - Passworte, Admin-Rechte
    - Email, Spam, Phishing
    - Telebanking, Ebay, Peer2Peer
    - UMTS, WLAN

21 © W. Schnabl, 9/06 nextiraOne

Mitarbeitersensibilisierung – Erstellung eines Konzepts II

- Durchführung in Gruppen
  - Ähnlicher Wissensstand
    - IT Personal, Techniker
    - Administration
    - Management
  - Interaktivität
    - Nicht zu viele Teilnehmer
- Zeit für persönliche Gespräche
  - Pausen und im Anschluss
- Ansprechstelle bei Problemen
  - Email und Tel.-Durchwahl

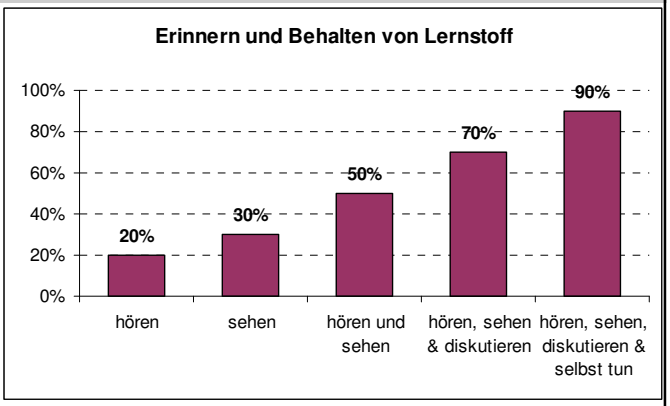
22 © W. Schnabl, 9/06 nextiraOne

Möglichkeiten für Training

Verschiedene Lernformen

Wir behalten von dem, was wir

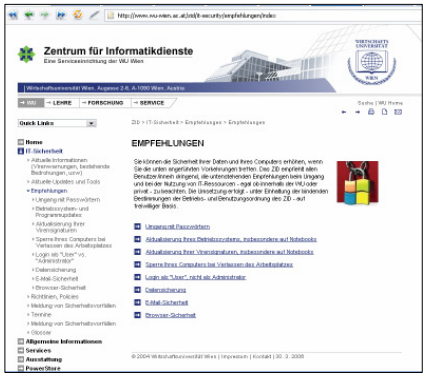
- nur hören 20%
- nur sehen 30%
- hören und sehen 50%
- hören, sehen und darüber zusätzlich diskutieren 70%.
- hören und sehen und diskutieren und auch selbst tun 90%



nach Franz Decker, 1985

Möglichkeiten für Training

- Merkblatt
- Intranet
- Webbased Training
- Schulung/Workshop
- Firmenkultur

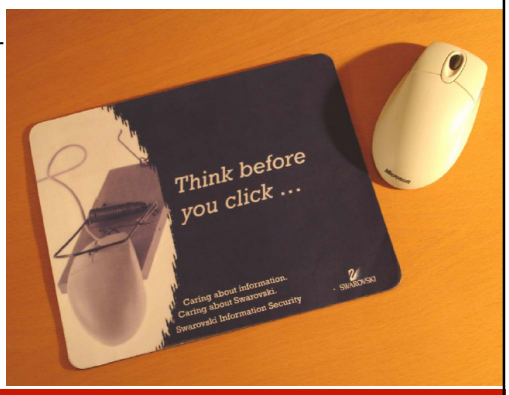


- Messbarkeit
  - Computer-unterstützte Tests
  - Hotlineanfragen (weniger, anspruchsvoller)
  - Audits
  - Gelebte Praxis

Mitarbeitersensibilisierung – Erfolgsfaktoren

IISA Initiative Informationssicherheit Austria

- Effektive Sensibilisierung
  - Anhaltender Lernprozess
  - Sinnvoll aus der Sicht des Mitarbeiters
  - Messbare Wirkung
  - Langfristige Verhaltens-änderungen
- Ziel:
  Hausverstand benutzen



25 © W. Schnabl, 9/06 nextiraOne

IISA Initiative Informationssicherheit Austria

Watch out

Was tun, wenn Sie etwas bemerken?

Meldung an:

IT Abteilung
help@eigene-firma.at
Tel DW: 333

26 © W. Schnabl, 9/06 nextiraOne