

# Praxisforum Luzern

## Forum 2: Ausbildung von Mitarbeitern in sicherheitsrelevanten Bereichen

FGSec 22. 3. 2001

Forum 2

## Inhalt

- Einleitung
- Vorstellung
- Fragestellungen
  - Ausbildung
  - Motivation
  - Dienstanweisungen
- Ergebnisse
  - Wie macht man das Problem wahrnehmbar
  - Wie erreicht man Awareness
  - Computer-based Training (CBT)
- Fazit

FGSec 22. 3. 2001

Forum 2

## Einleitung

# Human factor als grösstes Sicherheitspotential

## Vorstellung

- Marcus Holthaus, IMSEC
- Rolph Haefelfinger, Swiss Infosec
- Mark Zweiacher, plenaxx
- Thomas Kunz, BDS
- Willy Vollenweider, Digicomp
- Esther Hüsler, Swisscom

# Fragestellungen



- **Ausbildung:**
  - Awareness-Programme
  - Training / Schulung
  - Erfolgsprüfung
- **Motivation:**
  - Reglement
  - Dienstanweisungen
  - Incentives
- **Dienstanweisungen**
  - Arten & Formen
  - Organisation
  - Überprüfung der Wirksamkeit

FGSec 22. 3. 2001

Forum 2

## Fragestellungen Ausbildung / Awareness



1. Was ist der Unterschied zwischen Informationssicherheit und Informatiksicherheit? Wie vermittelt man das?
2. Wie motiviere ich Mitarbeiter, sich sicher zu verhalten?
3. Welche allgemeinen Verhaltensweisen muss ich fördern, um Awareness im Bereich Informationssicherheit voranzutreiben?
4. Wie vermittele ich, dass Informationssicherheit wichtig und relevant ist?
5. Wie überbrücke ich das Unverständnis, welches auch viele erfahrene Fachleute den Gefahren aus dem Bereich Internet entgegenbringen?
6. Wie löse ich den Konflikt, dass einerseits fast nur Microsoft-Software eingesetzt wird, diese aber andererseits einige Sicherheitslücken hat, die jedem Nutzer gefährlich werden können?

FGSec 22. 3. 2001

Forum 2

## Fragestellungen Training / Schulung:

1. Welche Ausbildungsmöglichkeiten bestehen in der Schweiz?
2. Wird in der Informatik-Ausbildung auf Stufe Grund- und Mittelschule auf Sicherheit und sicheres Verhalten hingewiesen? Hochschulbereich? Fachhochschulen? Private Schulungs-Institutionen?
3. Was spricht für fundierte, was für nutzungsorientierte Ausbildung?
4. Wie ist der Langzeitnutzen für Ausbildungen? Wie schnell veraltet das Wissen?
5. Kann man Ausbildungen in diesem Bereich auch individuell kaufen? Was spricht dafür, was dagegen?
6. Zertifikate und ihre Aussagen

## Fragestellungen Erfolgsprüfung

1. Soll überhaupt versucht werden, den Erfolg einer Ausbildung im Betrieb (d.h. nach Rückkehr der Personen an den Arbeitsplatz) zu messen?
2. Wie misst man Security Awareness?
3. Was bringen Gruppendynamische Ausbildungen?
4. Gibt es Aussagen über die Wirksamkeit von Uebungen?
5. Stufenkonzept

## Fragestellungen Motivation

1. Wie müssen Reglemente formuliert und kommuniziert werden, damit sie befolgt werden?
2. Welche Anreizsysteme sind denkbar im Bereich Informationssicherheit?
3. Wie muss die Organisation vorgenommen werden? Einbindung, Aufbau, Verteilung der Verantwortungen etc.

## Weitere Fragestellungen

- Haftung des Managements für angemessene Ausbildung der Mitarbeiter
- Verfügbarkeit von Flyern, Hinweisen, Listen von Notfallnummern und Vorgehensweisen

## Ergebnisse: Wie macht man das Problem wahrnehmbar?



- Diskussion führen: „Wieviel Sicherheit braucht's und wieviel Verantwortung nehmen wir dem Benutzer ab vs. Bekanntmachung der bestehenden Gefahren“
- Wir brauchen mehr Sicherheitvorfälle !
  - Entstehende Vorfälle sofort auf eigene Umgebung anwenden: „Könnte das bei uns auch passieren“
  - Selbst auslösen! Testen auch ohne Ankündigung
- Management Attention
  - Wieviel Information liefert man (Eigen-PR)
  - Messbarkeit nach wie vor schwierig
  - Kosten- / Nutzenrechnung
- Viel über Passwörter diskutiert
- Zertifikate wurden NICHT diskutiert... Unklar warum.
- Vieles braucht der Nutzer nicht zu wissen („Funktion des Airbags“), aber er muss sich dennoch sicher verhalten.

FGSec 22. 3. 2001

Forum 2

## Wie erreicht man Awareness?



- Mind Maps
- ½ bis 1 Arbeitstag Schulung pro Jahr und Mitarbeiter
- Schulung auch mit Externen
- Sicherheit immer mit anderen Themen kombinieren
- Sicherheit muss gelebt werden
  - Incentives, in Mitarbeiterbeurteilung berücksichtigen
- Leute wissen nicht was alles abläuft und werden es nie wissen
- IT muss so viel wie möglich an Sicherheit liefern und tut's zum Teil noch nicht -> Ressourcenfrage
- Internet an normalen Arbeitsplatz? Immer weniger...
  - Diskussionen offen führen
- Schulung mit internen und Externen

FGSec 22. 3. 2001

Forum 2

## Ergebnisse: Computer-based Training (CBT)

- Erfahrungen vorhanden, aber inkonsistent
- Messung des Erfolgs bleibt schwierig
- Leute involvieren!
- Tendenz Intranet-based
- Wichtigste Eigenschaften von CBT-Systemen
  - Unterhaltungswert
  - Bedienungsfreundlichkeit
  - Inhaltlicher Level nach Nutzer
  - Aktualität
  - Selbst- und Fremddassessment
- Zertifizierung der Fähigkeit von Personen

## Fazit

- Sicherheit ist und bleibt tricky!
- Wiederkehrende Aufgabe, wegen
  - Fluktuationen des Personal
  - Entwicklung der Technologien