



Arbeitsgruppe Informationssicherheitskultur

Sicherheitsfaktor Mensch: Die Chancen der Informationssicherheitskultur

Freundlich unterstützt von: **DIGICOMP** academy

28.10.2004

Arbeitsgruppe Informationssicherheitskultur

1



Arbeitsgruppe Informationssicherheitskultur

Einleitung

28.10.2004

Arbeitsgruppe Informationssicherheitskultur

2

fg sec the information security society of switzerland Übersicht

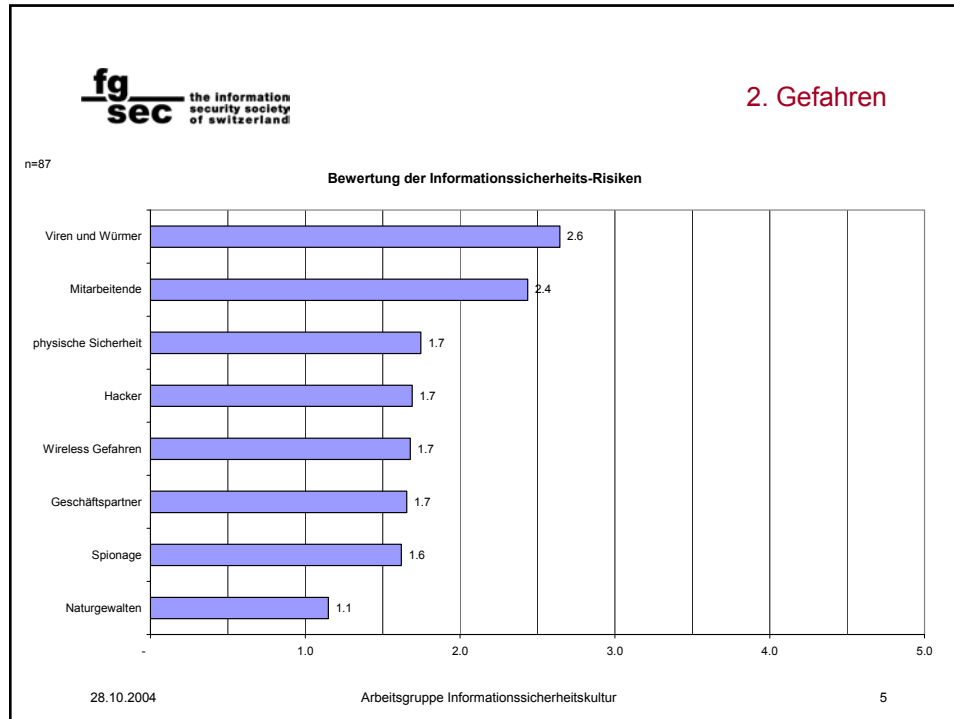
1. Vorstellung der AG-Mitglieder
2. Motivation und Ziele
3. Unsere Definition der Informationssicherheitskultur
4. Vorgehensmodell zur Analyse und Förderung der Informationssicherheitskultur
5. Was erwartet Sie weiter:
 - Situationsanalyse: wie steht es um unsere Informationssicherheitskultur
 - Management Buy-In: die Kunst des Überzeugens
 - Kommunikation: Was interessiert mich Kommunikation, ich hab eine Firewall
 - Studie Informationssicherheitskultur in CH-Unternehmen
 - Diskussion

28.10.2004 Arbeitsgruppe Informationssicherheitskultur 3

fg sec the information security society of switzerland 1. Vorstellung

Chris Baur Trivadis AG	Stefan Burau Coultts Bank von Ernst
Rafael Cruz consul&ad	Markus Herren conpro Consulting AG
Rolf Keiser Helvetia Patria Versicherung	Hans Peter Riess ixact AG
Raphael Rues Risk Resilience	Thomas Schlienger Leiter der Arbeitsgruppe iimt, Universität Fribourg
Verena Teige Syngenta Crop Protection AG	

28.10.2004 Arbeitsgruppe Informationssicherheitskultur 4



- fg sec** the information security society of switzerland
2. Massnahmen
- **Technik**
 - Technische Massnahmen wie ACL, Firewalls etc.
 - “Sicherheit ist ein technisches Problem welches durch technische Massnahmen von IT-Fachleuten gelöst werden muss”
 - **Organisation**
 - Einbezug des Managements
 - Institutionalisierung: Sicherheitspolitik, Sicherheitsorganisation, Sicherheitskonzeption
 - **Mensch**
 - Sensibilisierung
 - Sicherheitskultur
- 28.10.2004 Arbeitsgruppe Informationssicherheitskultur 6

2. Unsere Überzeugung

- Der sogenannte „Faktor Mensch“ ist für die Informationssicherheit auf verschiedene Weise von **grosser Bedeutung**
- Dieser Faktor wird vielfach **unterschätzt und vernachlässigt**
- Es steht noch viel **zu wenig Wissen** und Informationen zu dieser Thematik zur Verfügung

2. Ziele der Arbeitsgruppe

- In welcher Weise beeinflussen das **Wissen**, die **Einstellungen** und **Überzeugungen** der betroffenen Personen unsere Arbeit zur Verbesserung der Informationssicherheit?
- Wie können wir die zu erwartenden Einflüsse dieser Art **beschreiben, erfassen** und in unserer Arbeit **berücksichtigen**?
- Wie können wir das **Wissen** und **Verhalten**, aber auch die **Einstellungen** und **Überzeugungen** der Mitarbeitenden in Bezug auf die Informationssicherheit im positiven Sinn **beeinflussen**?

3. Definition der Organisationskultur

Definition:

„Kultur ist ein **Muster von Grundannahmen**, die von einer Gruppe während des Lernprozesses zur Bewältigung ihrer Anpassungs- und Integrationsprobleme erfunden, entdeckt oder entwickelt wurden und die sich soweit **bewährt** haben, dass sie als gültig betrachtet und neuen Mitgliedern als die **richtige Haltung für das Wahrnehmen, Denken und Fühlen** im Umgang mit diesen Problemen vermittelt werden.“

[Schein, E. H. (1985). Organizational Culture and Leadership: A Dynamic View. San Fran-cisco, Jossey-Bass.]

3. Vorteile einer geeigneten Informationssicherheitskultur

- **Koordinationsfunktion:**
 - verringert den Bedarf an **formalen Regelungen** und administrativen Anweisungen
 - erlaubt vor allem in **nicht vorhersehbaren Situationen**, Entscheidungen auf einen gemeinsamen Kern von einheitlichen kulturellen Werten abzustellen, welche Zeit sparen und somit die Reaktionszeit verkleinern und die Widerstandsfähigkeit vergrössern.
- **Integrationsfunktion:**
 - eine Informationssicherheitskultur muss dezentralisiert und überall in der Organisation gelebt werden. Selbst wo starke Subkulturen vorhanden sind, muss eine **einheitliche Sicherheitskultur** gelebt werden.
 - Eine solche Integration macht möglich, dass die Sicherheitskultur ein **übergeordnetes Element** ist. Diese Voraussetzungen ermöglichen dem Unternehmen, aktiv die Sicherheitsförderung voranzutreiben.

„in these [starke Kultur] companies, people way down the line know what they are supposed to do in most situations because the handful of guiding values is crystal clear“

[Peters, T. J. and R. H. Waterman (1982). In search of excellence: lessons from America's best-run companies. New York, NY, Harper and Row]

- **Massnahmen zur Aneignung von Fertigkeiten**
 - zur korrekten Anwendung von technischen und organisatorischen Sicherheitsmassnahmen
 - und zum geeigneten Umgang mit sensitiven Informationen zu befähigen
 - Erklären und Einüben
- **Massnahmen zur Bewusstseinsbildung (Awareness)**
 - Notwendigkeit von Sicherheitsmassnahmen zu verdeutlichen
 - Aufzeigen der bestehenden Bedrohungen
 - Schulungsmassnahmen, Drucksachen, offiziellen Äusserungen
- **Massnahmen zur Normenbildung**
 - Eingang in die tägliche Praxis
 - unbewussten, eher langfristigen Prozess
 - nicht kurzfristig und nicht direkt steuerbar

