Security Awareness Kampagnen

GI Fachgruppe SECMGT, Workshop 12.10.2005

Dirk Fox
dirk.fox@secorvo.de

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de

Secorvo Security Consulting

- Unabhängiges Beratungsunternehmen für IT-Sicherheit

- Ausbildungszentrum für IT-Sicherheit: Secorvo College
- Ausbildungspartner von BSI, SAP und T-Systems
- Kunden: Schering, BMW, DaimlerChrysler, BASF, Heidelberger, Deutsche Bank, FinanzIT, Datev, Michelin, Toll Collect, Krones, Commerzbank, Tchibo, Bundesbank, SEW, BSI, Gardena, Bosch, Deutsche Bahn, Roland Berger, Benteler, Deutsche Post, Liebherr, SAP, EZB, Linde, ...

secorvo
security consulting

Inhaltsübersicht

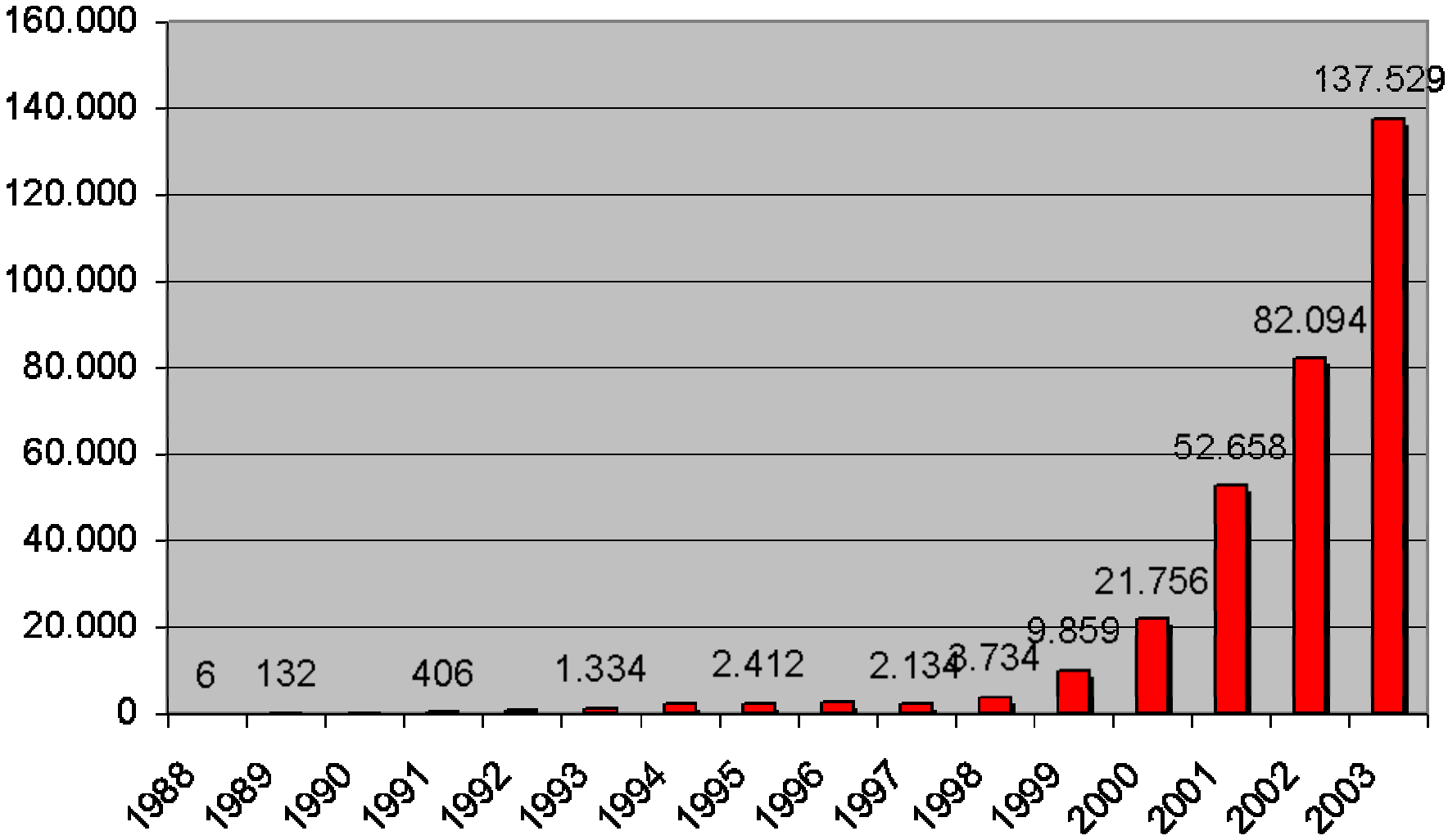
- Entwicklung der Bedrohungen
- „Risikofaktor Mensch“
- Awareness-Kampagnen
- Beispiele
- Zusammenfassung und Fazit

Inhaltsübersicht

- **Entwicklung der Bedrohungen**
- „Risikofaktor Mensch“
- Awareness-Kampagnen
- Beispiele
- Zusammenfassung und Fazit

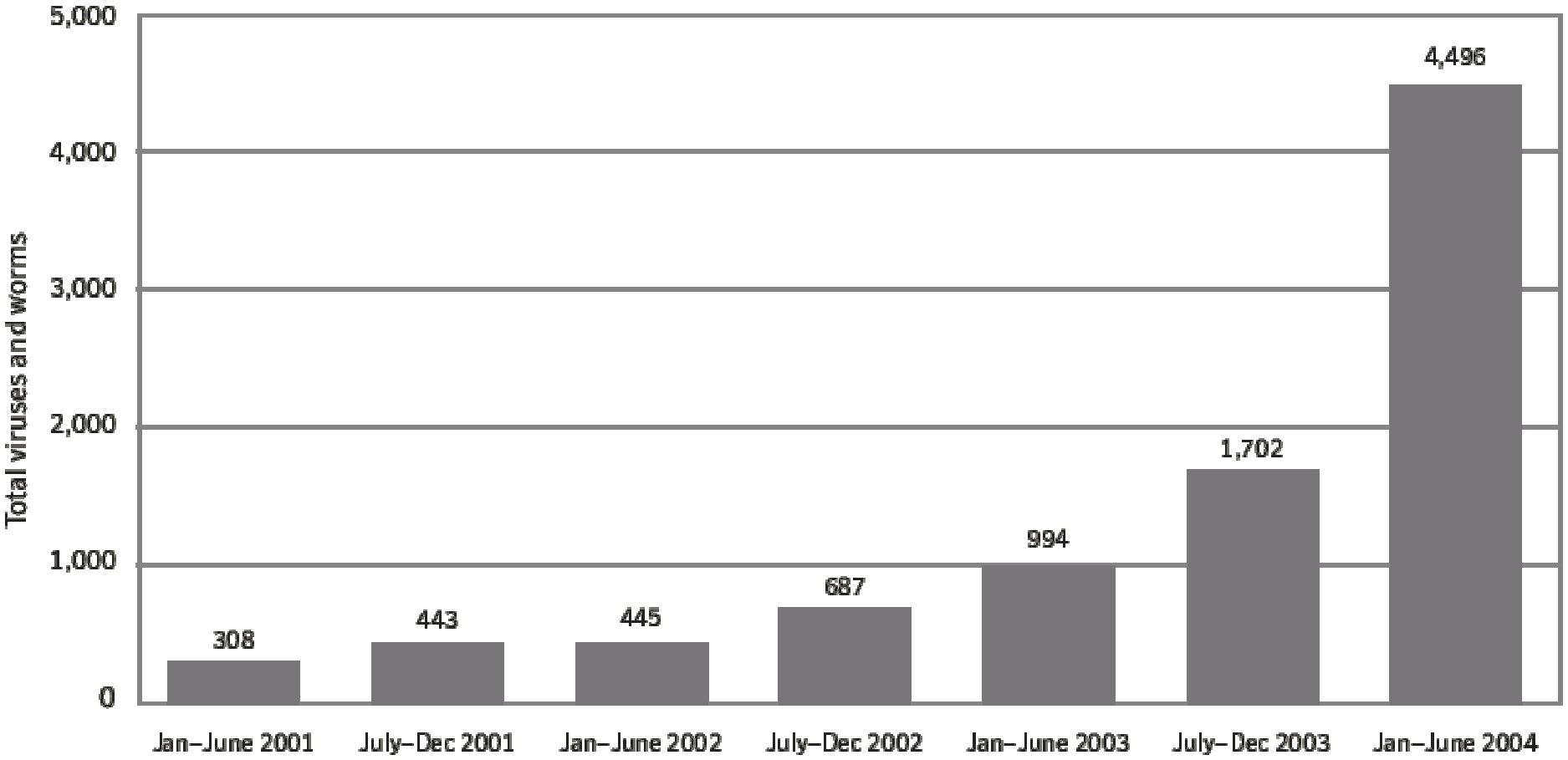
secorvo
security consulting

Angriffsstatistik des CERT/CC



secorvo
security consulting

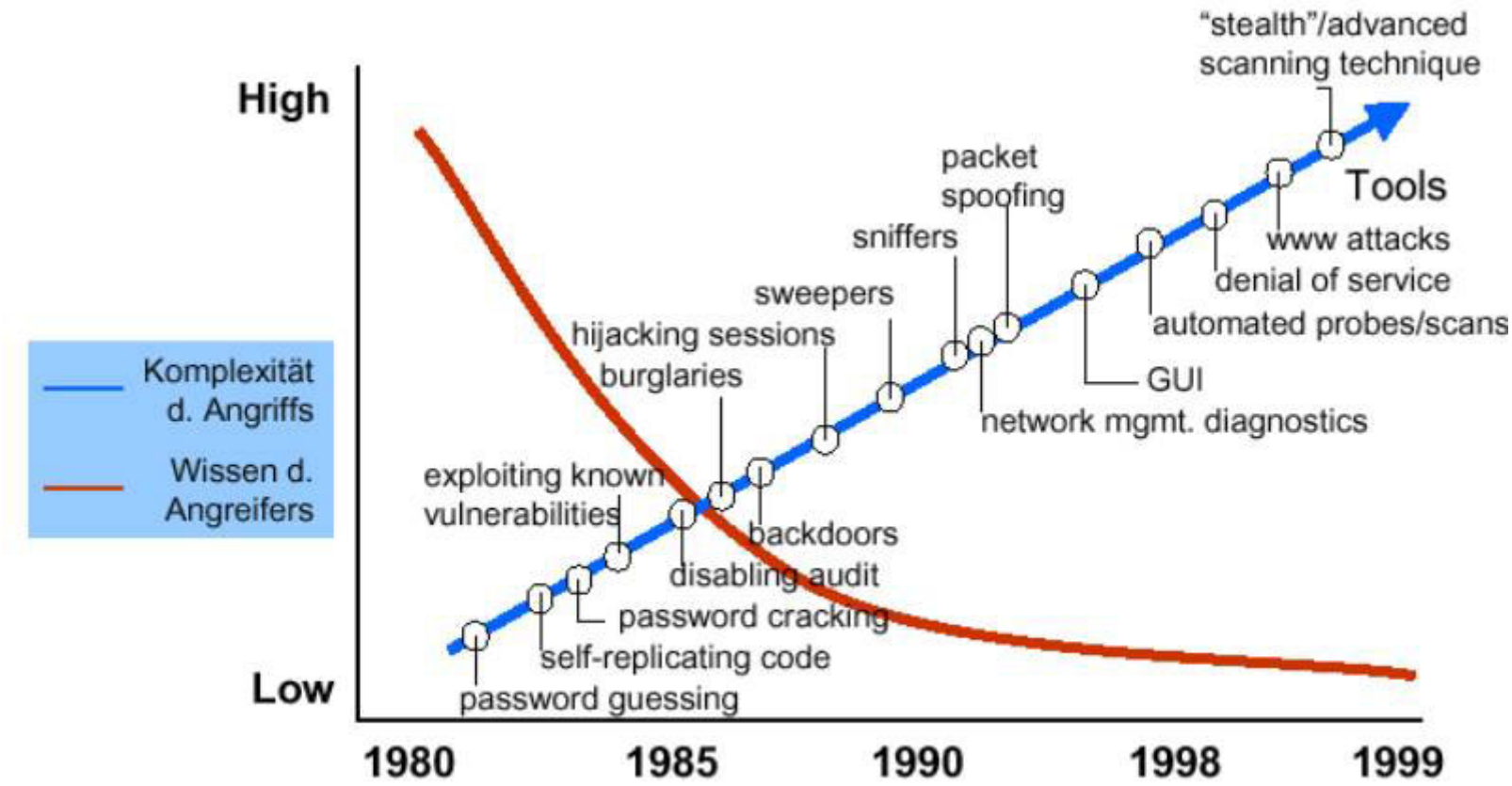
Neue Viren und Würmer



Source: Symantec Corporation

secorvo
security consulting

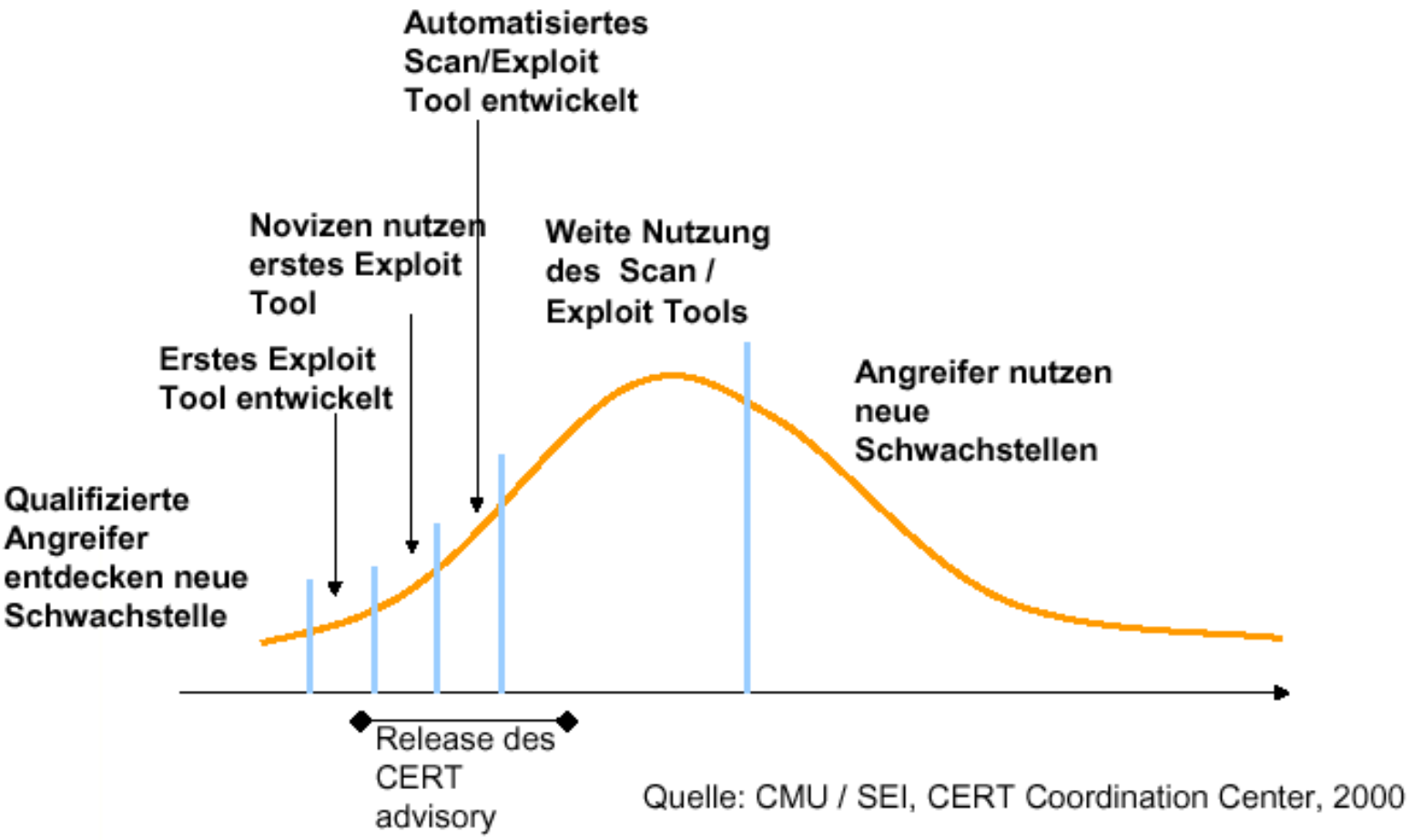
Qualität der Angriffstools



Quelle: CMU/SEI-99-TR-028

secorvo
security consulting

„Bug-Welle“



Quelle: CMU / SEI, CERT Coordination Center, 2000

secorvo
security consulting

Inhaltsübersicht

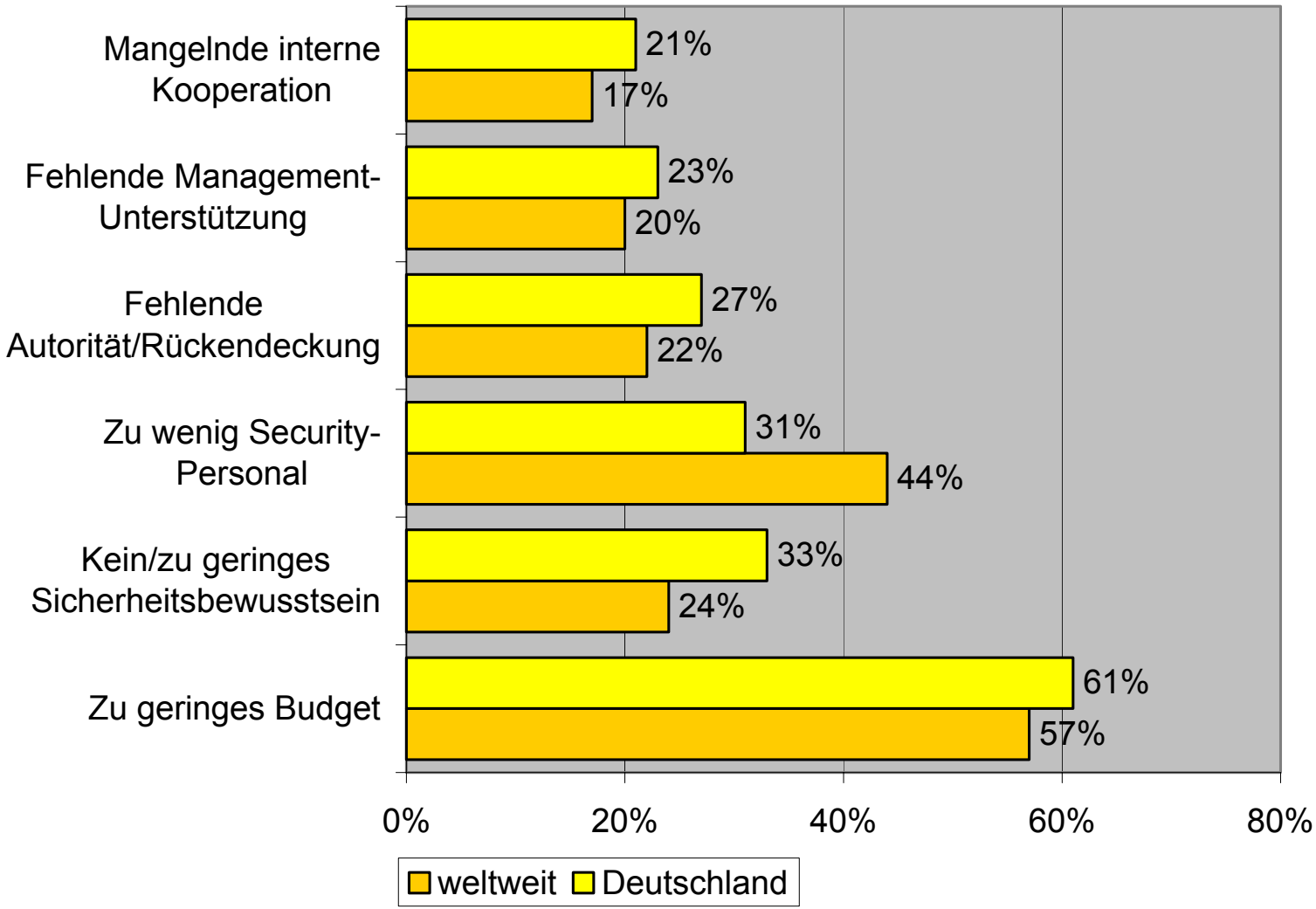
- Entwicklung der Bedrohungen
- **„Risikofaktor Mensch“**
- Awareness-Kampagnen
- Beispiele
- Zusammenfassung und Fazit

secorvo
security consulting

Top 10 Schadensverursacher

- Passworte auf Post-Its am Arbeitsplatz
- „Verlassene“ Computer ohne Schutzmaßnahme
- Öffnen von E-Mail-Anhängen unbekannter Sender
- Schlechte Passwort-Wahl
- Verlorene/gestohlene Laptops
- Ausplaudern von Passworten, Firmendaten etc.
- Installation von „Bypass“-Lösungen (z.B. Modems)
- Kein Bericht bei Sicherheitsvorfällen
- Verwendung veralteter (fehlerhafter) Software
- Unterschätzung der Bedrohung durch „Innentäter“

Hindernisse für IT-Sicherheit



The State of Information Security 2004
CIO-Magazin, PWC 9/2004; 8.000 Teilnehmer

secorvo
security consulting

Grenzen der Technik

- **Benutzer sind häufig Schadensursache**
  - **52% der IT-Schäden werden durch Mitarbeiter verursacht (KES/KPMG-Studie 2002)**
  - **Technische Sicherheitslösungen sind selten erfolgreich, wenn Benutzermitwirkung erforderlich**
- **Vision technischer Beherrschbarkeit**
  - **Technische Schutzmaßnahmen überwiegen (Firewalls, Virenscanner, Intrusion Detection, ...)**
  - **Regeldurchsetzung wird meist technisch erzwungen**

➢ **Eine Erhöhung des Sicherheitsniveaus ist nur mit Anhebung des Sicherheitsbewusstseins möglich**

Immanente Schwächen

- **Rechtfertigungszwang: Maßnahmen der IT-Sicherheit sind fast immer Fortschrittsbremsen**
- **Ungewissheit: Sicherheitsvorfälle sind fast immer unerwartete Ereignisse**
- **Dauerbaustelle: Sicherheitskonzepte müssen ständig an IT- und Ablauf-Änderungen angepasst werden**
- **Mitarbeiterkreativität: Für jede kreative Schutzmaß-nahme findet man eine noch kreativere Umgehung**
- **Transparenzbedarf: Maßnahmen werden nachlässig umgesetzt, wenn Motivation unbekannt**
- **Didaktische Herausforderung: Wirksame IT-Sicherheit ist vor allem erlerntes Verhalten**

Wahrnehmung von Sicherheit

- **Arbeitsbehinderung**
  - IT-Sicherheitsmaßnahmen verlängern Prozesse
  - Zugangspasswörter müssen gemerkt werden
  - Daten sind nicht unmittelbar zugänglich
- **Risikoannahmen „realitätsfern“**
  - Bedrohungen erscheinen unrealistisch („Das kann bei uns nicht vorkommen“, „Bisher ist noch nie etwas passiert“)
  - Sicherheitsmaßnahmen erscheinen überzogen (z.B. Passwortlänge, Passwortwechsel)
- **Verantwortung wird Dritten zugeordnet**
  - Lösung des Schutzproblems = Aufgabe der IT-Abteilung
  - Betroffenheit durch Vorfälle wird nicht gesehen
  - Bedeutung des eigenen Verhaltens wird unterschätzt

Inhaltsübersicht

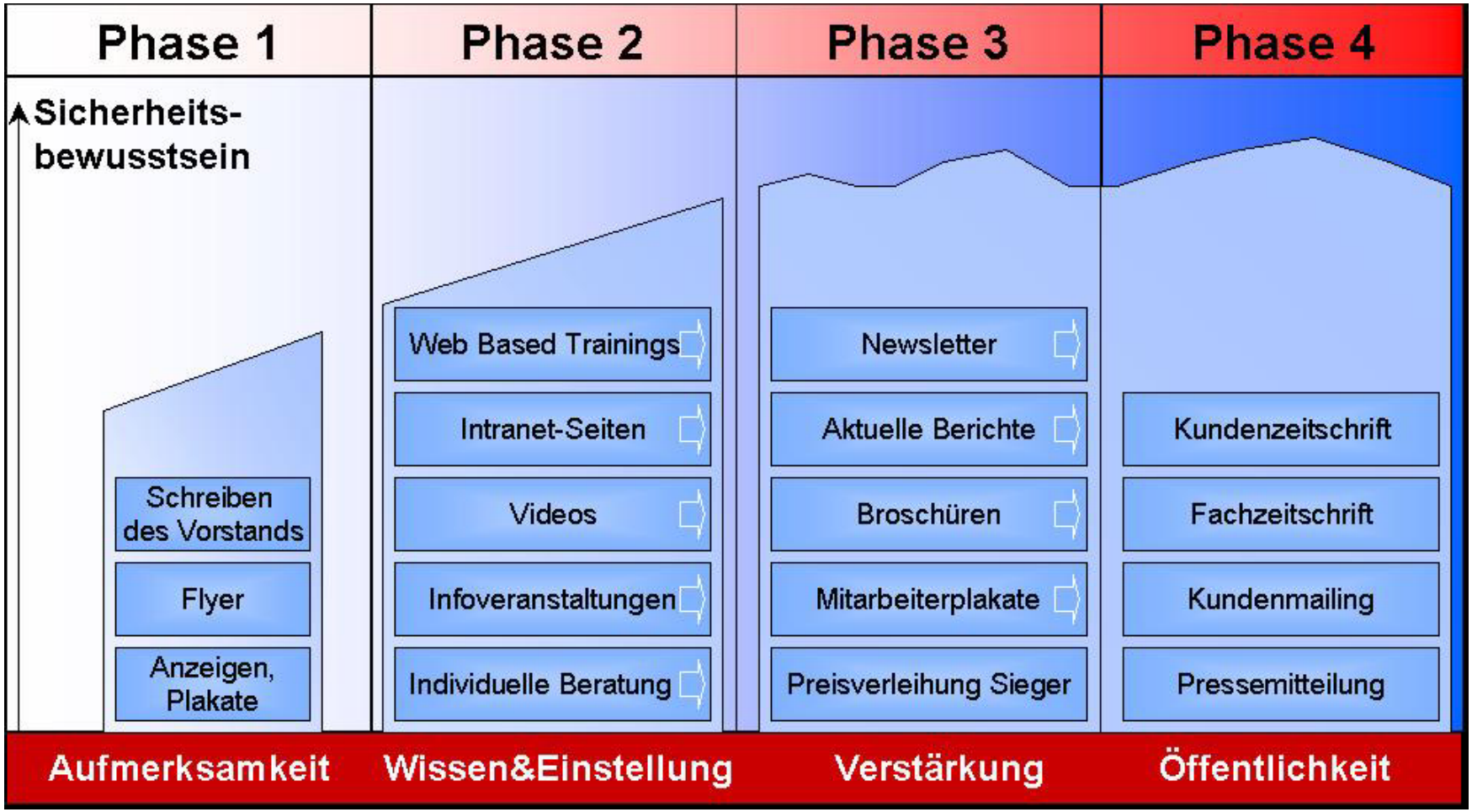
- Entwicklung der Bedrohungen
- „Risikofaktor Mensch“
- **Awareness-Kampagnen**
- Beispiele
- Zusammenfassung und Fazit

Zielsetzungen

- Erhöhung der Sensibilität für Sicherheitsbelange bei allen Mitarbeitern
- Schaffung von Verständnis durch Transparenz der Motivation und der getroffenen Maßnahmen
- Etablierung eines positiv besetzten Sicherheitsbegriffs
- Verankerung von Informationssicherheit als Qualitätsmerkmal
- Steigerung der realen Sicherheit und damit Verringerung der tatsächlichen Risiken

➢ Bewirkung nachhaltiger Verhaltensänderungen

Planung Awareness-Kampagne

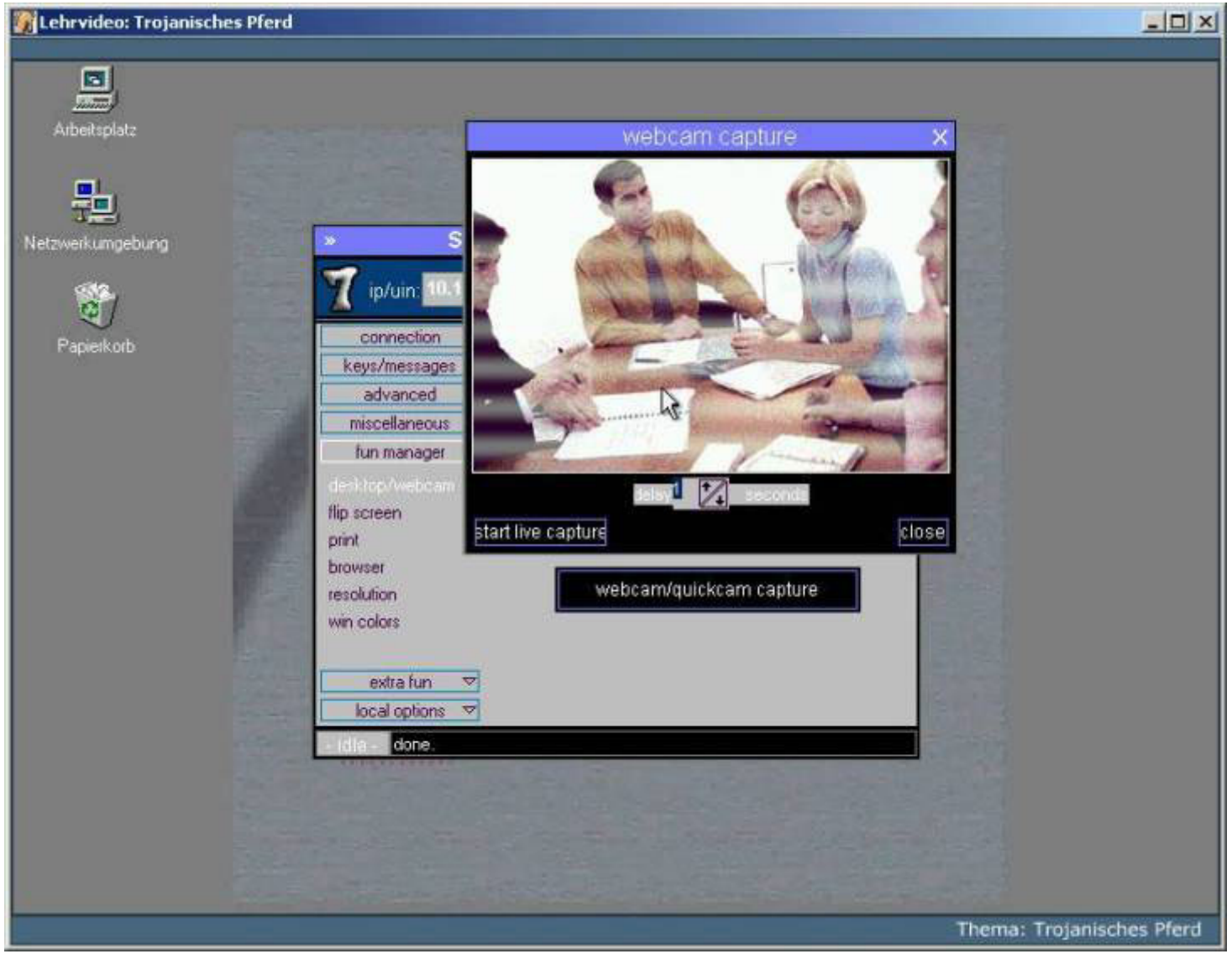


secorvo
security consulting

Aufbau Awareness-Kampagne

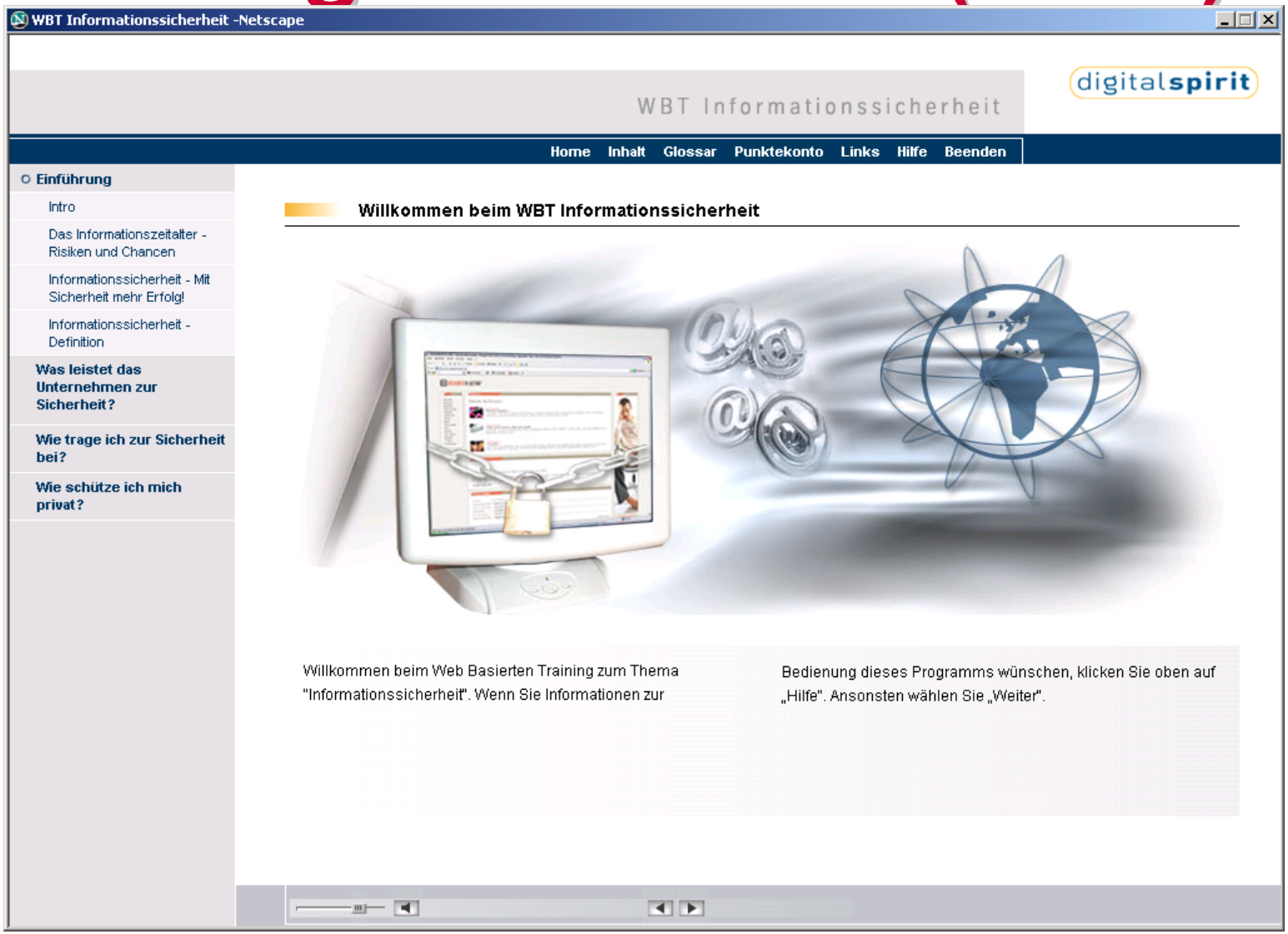
- **Phase 1: „Aufmerksamkeit gewinnen“**
  - **Ziel: Motivation der Mitarbeiter zur aktiven Mitwirkung**
  - **Maßnahmen: Plakate, Vorstands-E-Mail, Logo, Hauszeitschrift**
- **Phase 2: „Wissen vermitteln, Einstellungen verändern“**
  - **Ziel: Grundwissensvermittlung, Verhaltensänderung**
  - **Maßnahmen: WBT, Informationsveranstaltungen, Videos, ggf. Evaluation des Sicherheitsbewusstseins, Give-Aways**
- **Phase 3: „Verstärkung“**
  - **Ziel: Dauerhafte Verhaltensänderung, positive Identifikation**
  - **Maßnahmen: interner Newsletter, Broschüren, Intranet-Portal**
- **Phase 4: „Öffentlichkeitsarbeit“**
  - **Ziel: Verankerung von IT-Sicherheit als Qualitätsmerkmal**
  - **Maßnahmen: Interne und externe Publikationen**

Videos zur Sensibilisierung



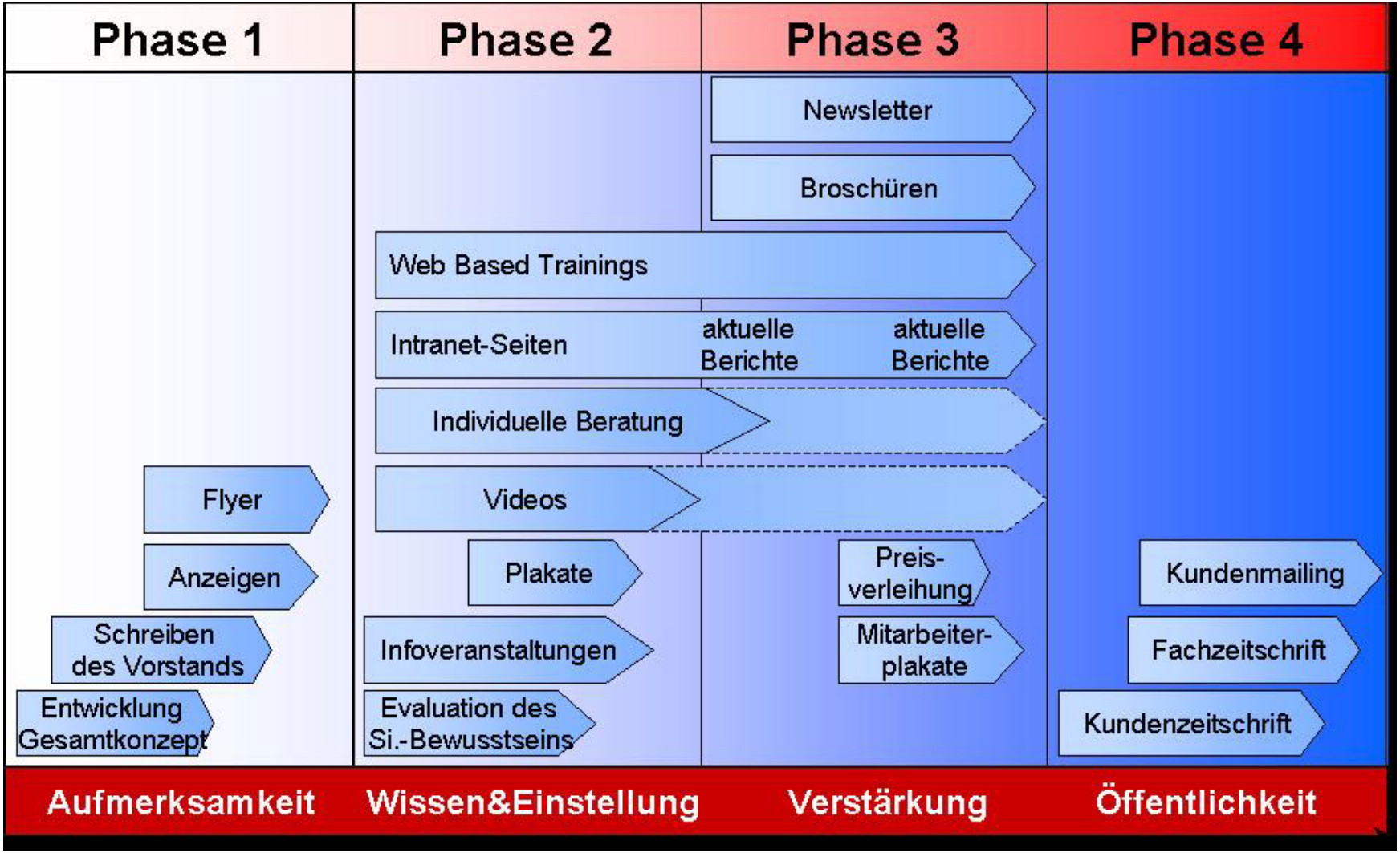
secorvo
security consulting

Hintergrundwissen (WBT)



secorvo
security consulting

Ablauf Awareness-Kampagne



secorvo
security consulting

Inhaltsübersicht

- Entwicklung der Bedrohungen
- „Risikofaktor Mensch“
- Awareness-Kampagnen
- **Beispiele**
- Zusammenfassung und Fazit

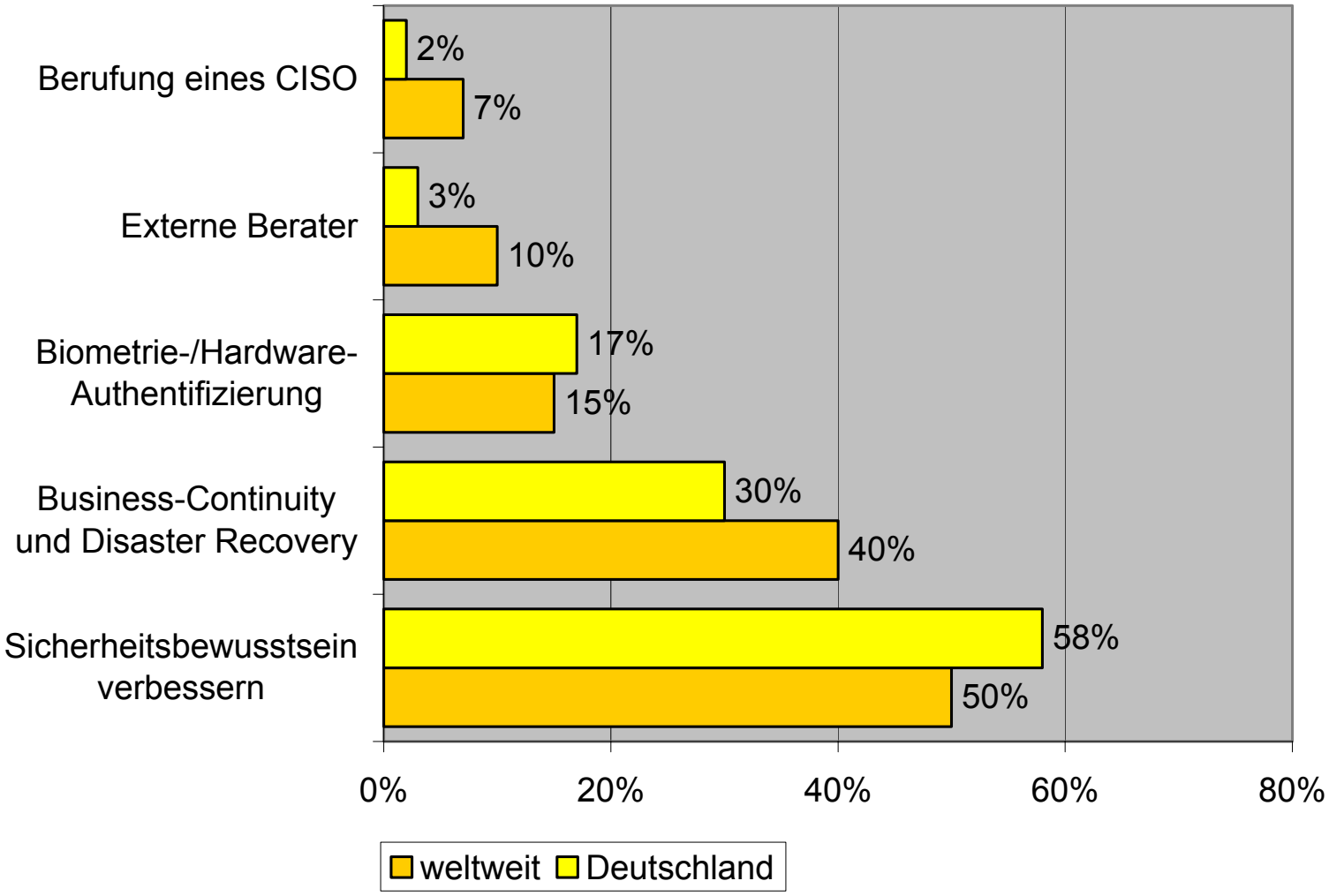
secorvo
security consulting

Inhaltsübersicht

- Entwicklung der Bedrohungen
- „Risikofaktor Mensch“
- Awareness-Kampagnen
- Beispiele
- **Zusammenfassung und Fazit**

secorvo
security consulting

Maßnahmenplanung 2005



The State of Information Security 2004
CIO-Magazin, PWC 9/2004; 8.000 Teilnehmer

secorvo
security consulting

Erfolgsfaktoren

- **Einbindung der Führungskräfte**
  - Vorab-Information
  - Führungsverantwortung: Vorbild, Motivation und Kontrolle
- **Konzentration auf das Wesentliche**
  - Welche Themen und Regelungen sind am Wichtigsten?
  - Nur ein Thema je Maßnahmen-Modul
- **Integration verschiedener Unternehmensbereiche**
  - Modularer Aufbau der Kampagne (Themenmodule)
  - IT-Sicherheit, Risiko-Management, Unternehmenssicherheit, Werksschutz, Arbeitsschutz
- **Nutzung eines kommunikativen Maßnahmen-Mixes**
- **Positive emotional-affektive Ansprache**

Die Alternative...

secorvo
security consulting

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de

Ausgewählte Referenzen

- **Awareness-Kampagnen und WBT Informationssicherheit**
  - BASF AG
  - CCBank AG
  - DekaBank
  - Fiducia IT AG
  - Framatome ANP
  - Linde AG
  - Robert Bosch GmbH
  - RWE Systems AG
  - Schweizerische Nationalbank
  - Siemens AG
  - T-Systems International GmbH
  - ThyssenKrupp AG

- **Sensibilisierungs-Videos (u.a.)**

  ABB, Allianz, Altana, Audi, Aventis, AXA, BASF, Badenia, Benteler, Bosch, BMW, Boehringer-Ingelheim, BP, Bundesbank, Commerzbank, Daimler-Chrysler, DAK, DATEV, DEKRA, Degussa, Deutsche Bank, EnBW, FinanzIT, Framatome, Henkel, HVB, Hochtief, INA, Keiper, LB-BW, L-Bank, Liebherr, Linde, Merck, Michelin, Microsoft, Pfalzwerke, RAG, RWE, SEW, Siemens, STEAG, T-Systems, Telekom, Thales, Vattenfall, Voith, ...