IT Sicherheitstrends in der nächsten Zeit

Alexander Tsolkas

CISO Schenker AG

Unternehmertag FH Hof

Agenda

- Interner Antrieb
- Externer Antrieb
- Weniger Perimetersicherheit
- Mobilität
- Web Dienste
- Was kommt als nächstes?

Interner Antrieb

- Integrierte Geschäftsprozesse mit Partnern, Zulieferern und Kunden
- Dynamisches Geschäftsfeld und IT-Umgebung
- Wachsendes e-Business
- Mobilisierung der Arbeitskräfte
- Budgetkürzungen
- Grenzenloser Informationsfluss wird gefordert
- … you can‘t do business behind a wall (Jericho Forum)

Externer Antrieb

- **EU Corp. Governance Proposal (Gov2003)**
- **Basel II**
- **BAFin**
- **KontraG**
- **SOX 404**
- **Neue Technologien**
  - WI-Max (**W**orldwide **I**nteroperability for **M**icrowave **Acc**ess)
  - UMTS
  - ……

Raffinierte Attacken

- Modularer bösartiger Programmcode
- Anstieg der bot Netzwerke
- Sicherheitsrisiken in der Wireless Umgebung
- Sicherheitsrisiken bei VoIP

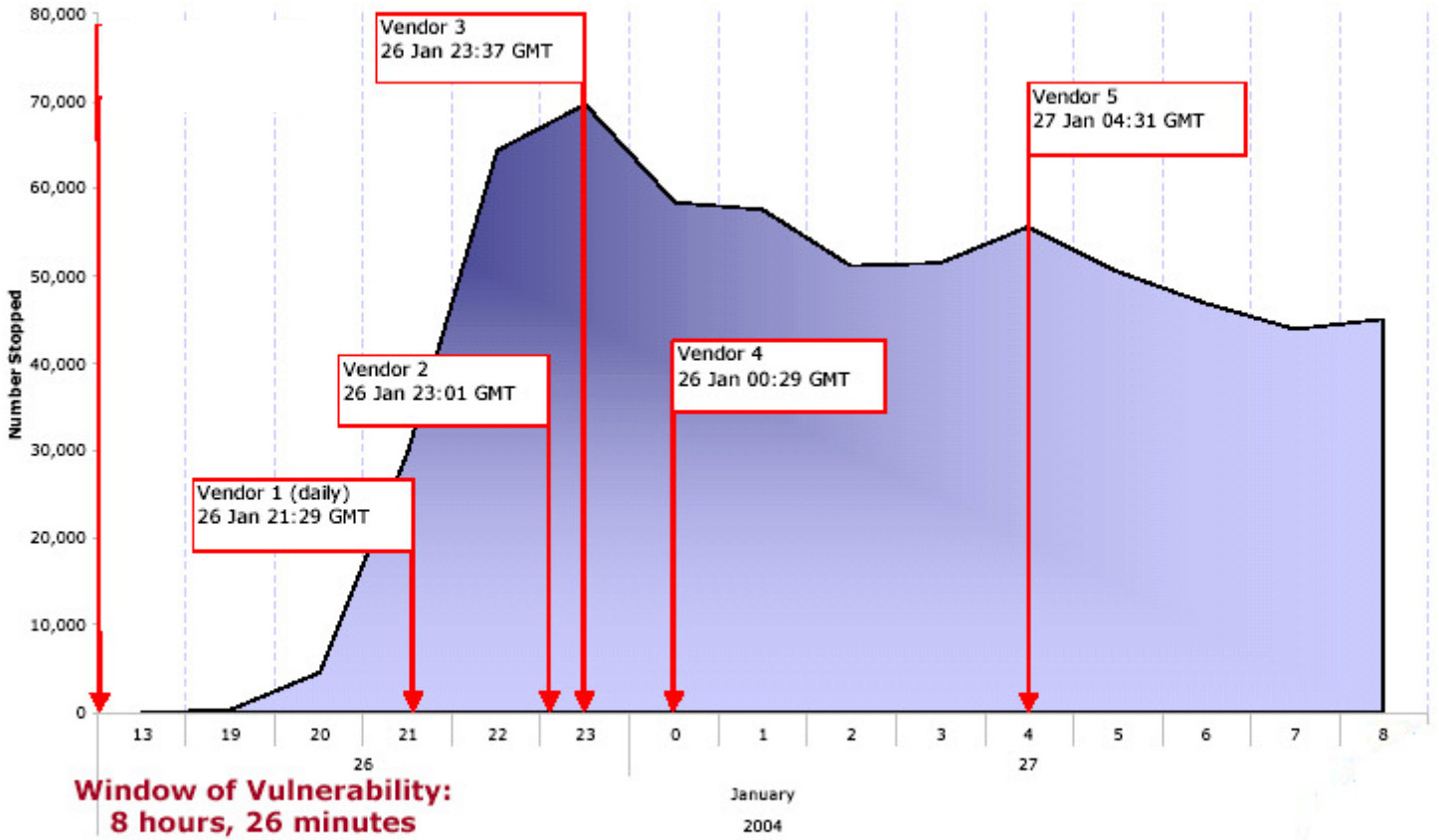
Der Sapphire Wurm bzw. “Slammer”

- Die Zahl der infizierten Computersysteme verdoppelte sich alle 8.5 Sekunden
- Infizierte 75,000 Computersysteme in den ersten 11 Minuten!
- Netzwerkausfälle, Systemausfälle, verspätete Flüge etc. ...

Minuten nach dem Auslösen

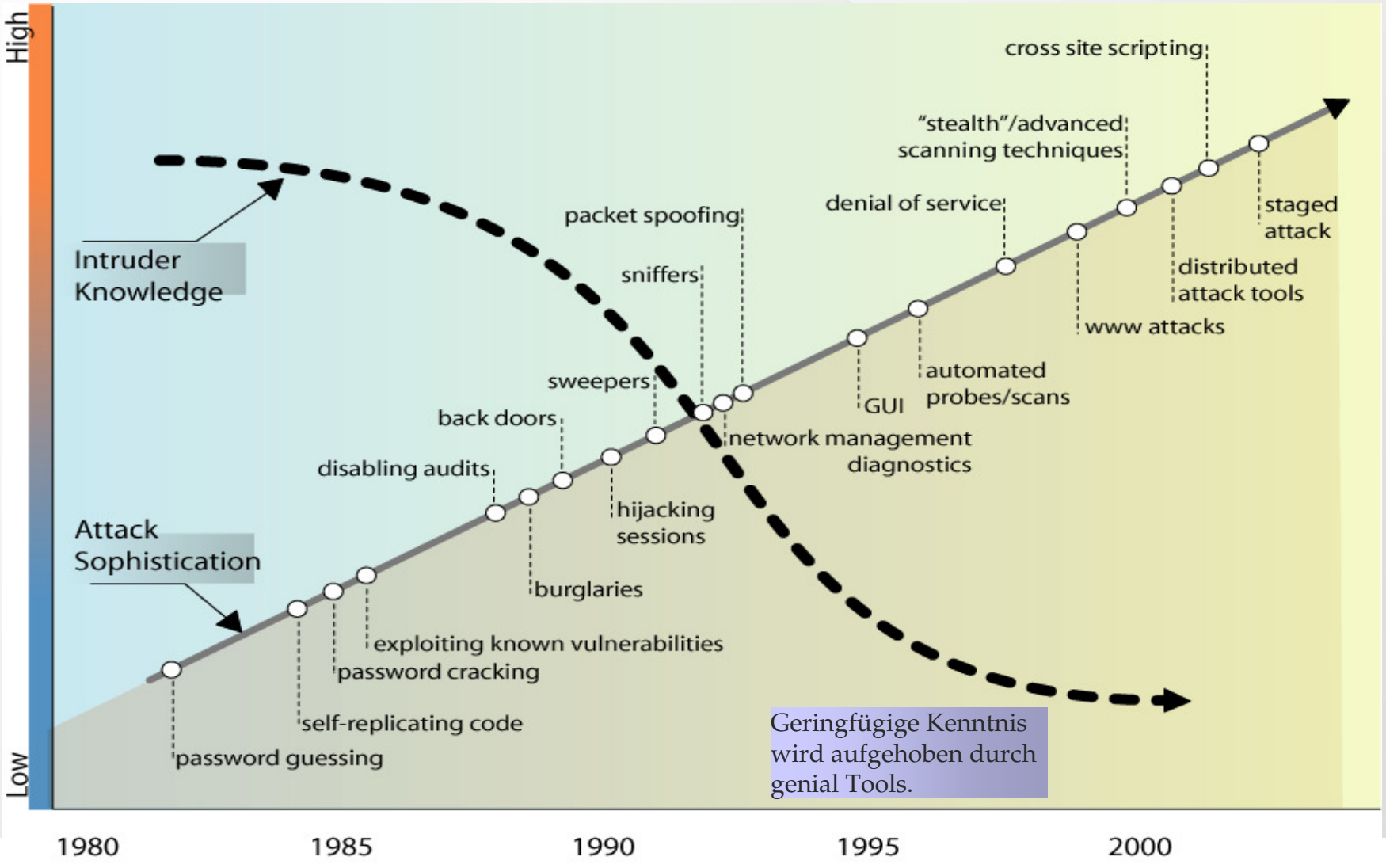
11

Infektionsgeschwindigkeit “MyDoom-A”



Kenntnis über Angriffe

Komplexe Systeme versus unwissende Angreifer



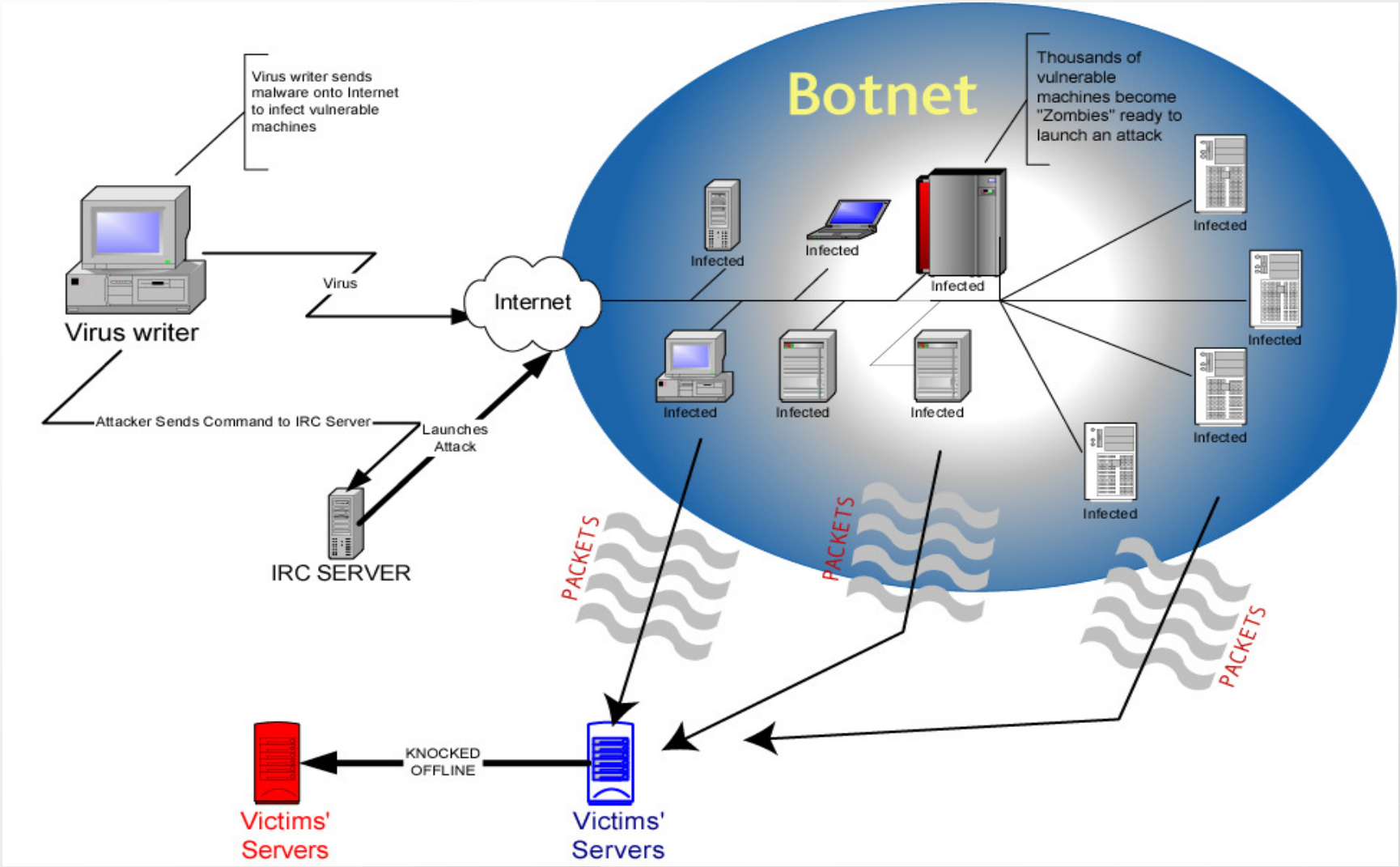
CERT/CC

Virenschutzprodukte

82% der Firmen berichteten Vireninfektionen, obwohl 99% von ihnen Antivirensoftware einsetzte.

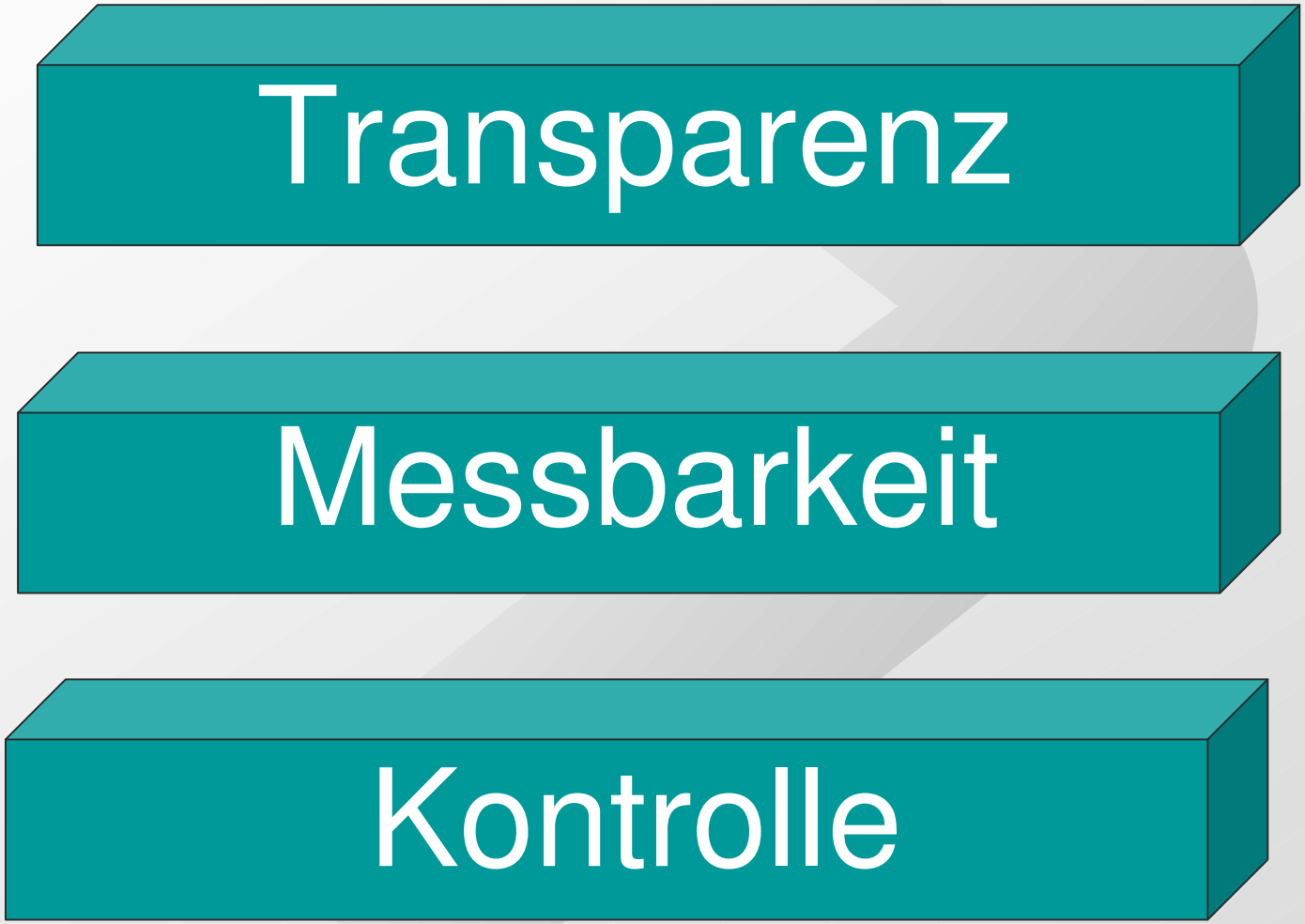
The 2003 CSI/FBI Computer Crime and Security Survey

Anatomie eines Botnet



Anatomie eines Botnet

Und man muß dennoch .....



.....gewährleisten

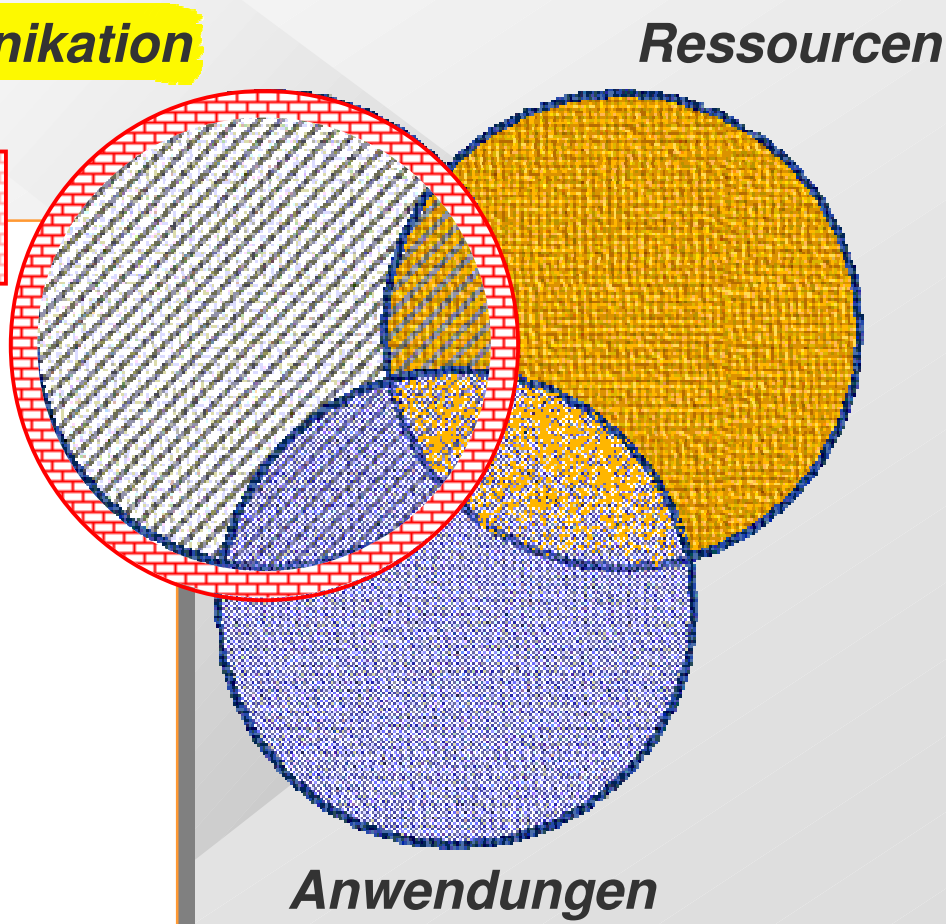
Erfolgsfaktoren einer Sicherheitsstrategie

- **Menschen**
- **Prozesse**
- **Technologien**

Perimetersicherheit – Das mittelalterliche Modell

- **Versuchen Sie einmal e-Business in einer mittelalterlichen Burg**
  - Firmen schützen sich mittels Firewalls, Virenscanner, etc.
  - Sicherheitsmaßnahmen setzen auf Trennung des “Inneren” vom “Äußeren”
- **Vorteile:**
  - Leicht einzurichten und zu verwalten; Unabhängig von Anwendungen
  - Klar definierte Kosten; Sicherheitsmaßnahmen können quantifiziert werden

Sicherheit innerhalb eines Unternehmens



Perimetersicherheit

- Sicherheit als Teil der Infrastruktur: Trennung von Sicherheitsmechnismen und Anwendungen
- Defensives Verständnis: Das BÖSE kommt von außen…

ABER:

- Mobile Geschäftstätigkeit ?
- Kollaboratives e-Business ?
- Web Dienste (.NET, J2EE) ?
- Durchgreifende IT / P2P Anwendungen ?

Sicherheit innerhalb eines Unternehmens

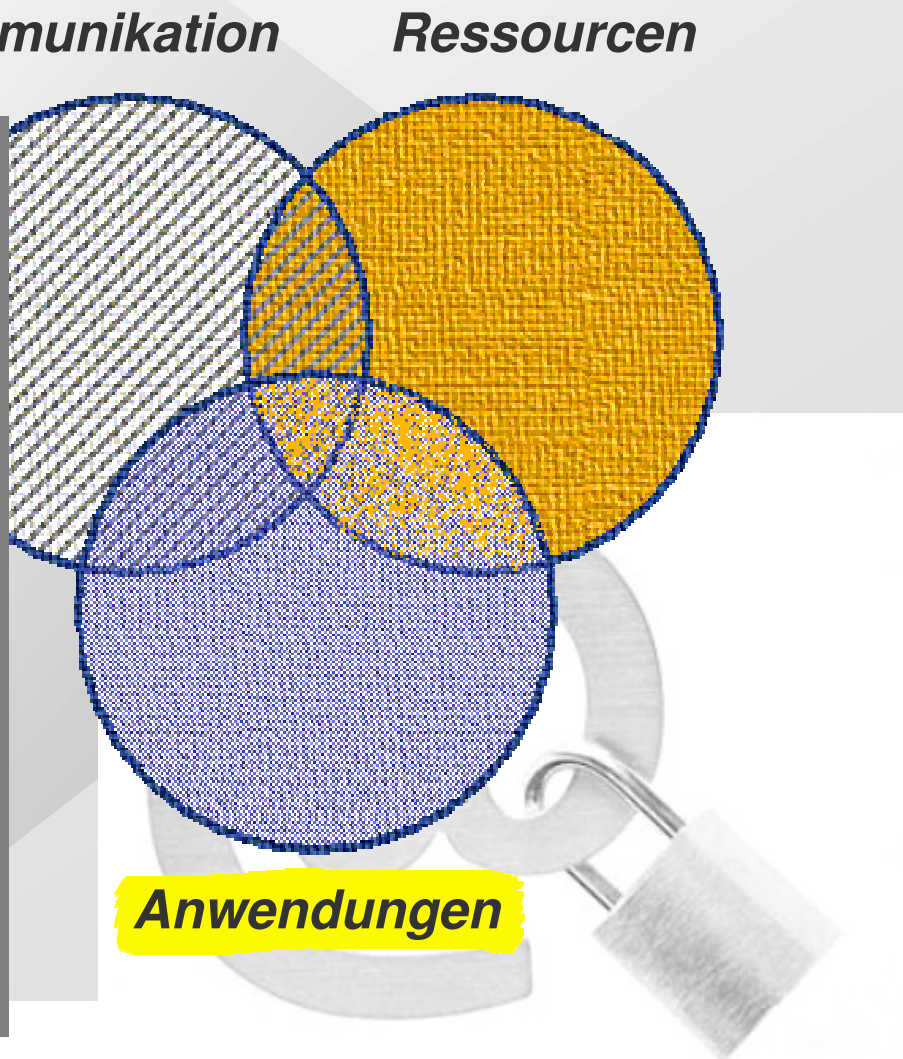
Secure e-services

Proaktive Sicherheit:

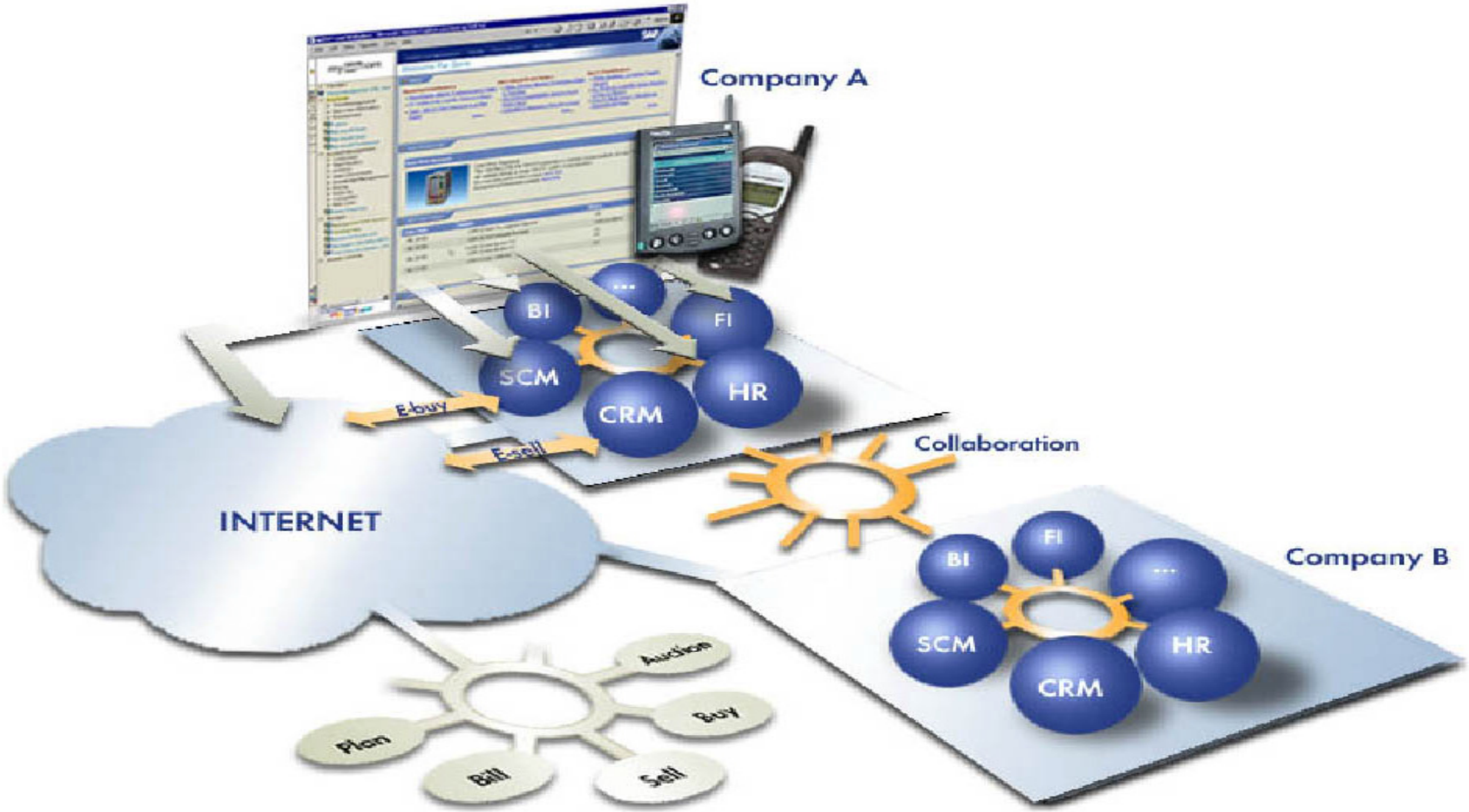
- **Sicherheit ist die Qualität der Lösung**
- **Soviel Sicherheit wie möglich auf der Anwendungsebene bieten**

Vision: Sicheres e-Business ohne Firewalls

- **Austausch, Portale, und Anwendungsserver bieten sichere e-Dienste**
- **Föderalisierte Identitäten**
- **Firmenweites Single Sign-On, Authorisierung, und Richtlinien-verwaltung**



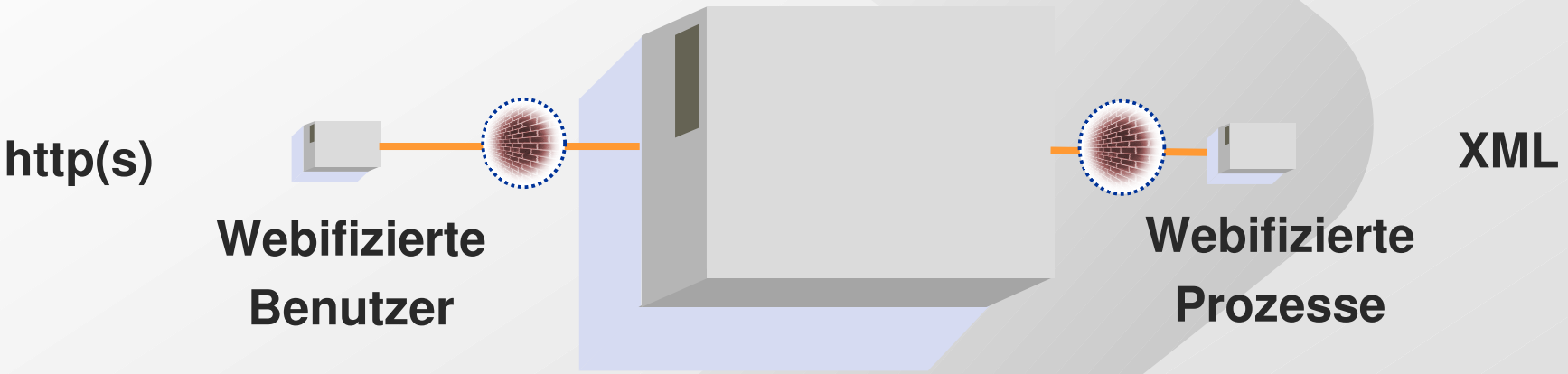
Weniger Barrieren ... dennoch mehr Sicherheit…



…heißt … große Änderung bei Web Diensten

Ehemalige Architektur

Eine Stufe der Integration:
Anwendungsserver



Benutzer-zentrierte Integration: Rollen

Prozess-zentrierte Integration: Als Source Code

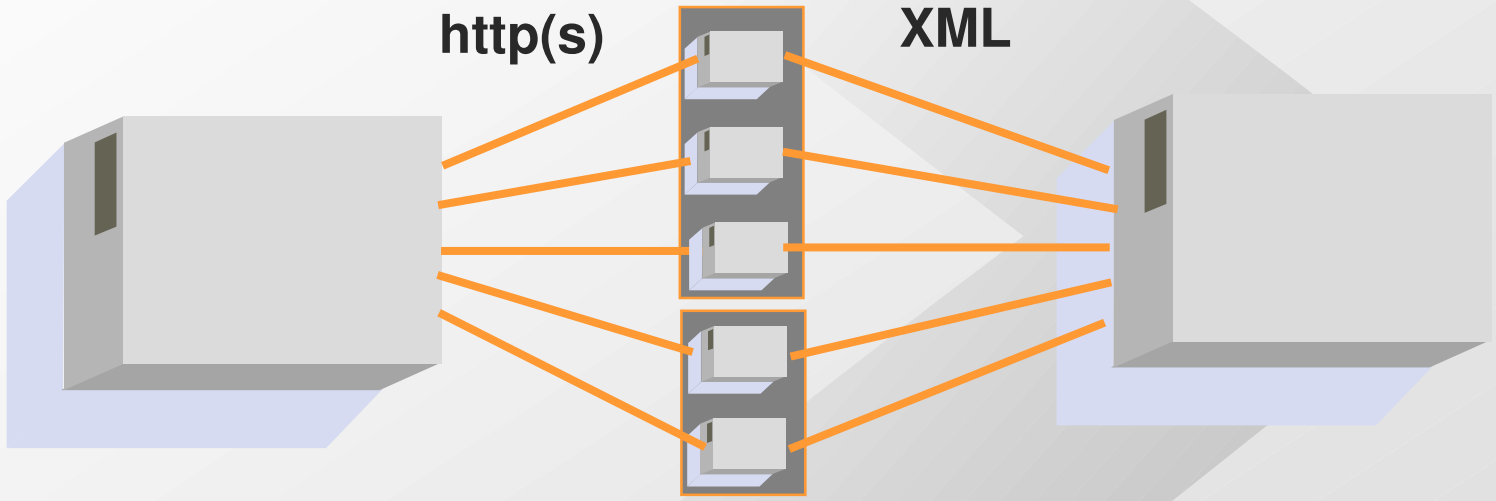
(“Abruftransaktion” oder besser “call transaction”)

Große Änderung bei Web Diensten

Neue Architektur

Zwei separate Stufen der Integration

Keine Firewall!



Benutzer-zentrierte Integration: Portal

Web Dienste

Prozess-zentrierte Integration: Austausch

Konsequenzen

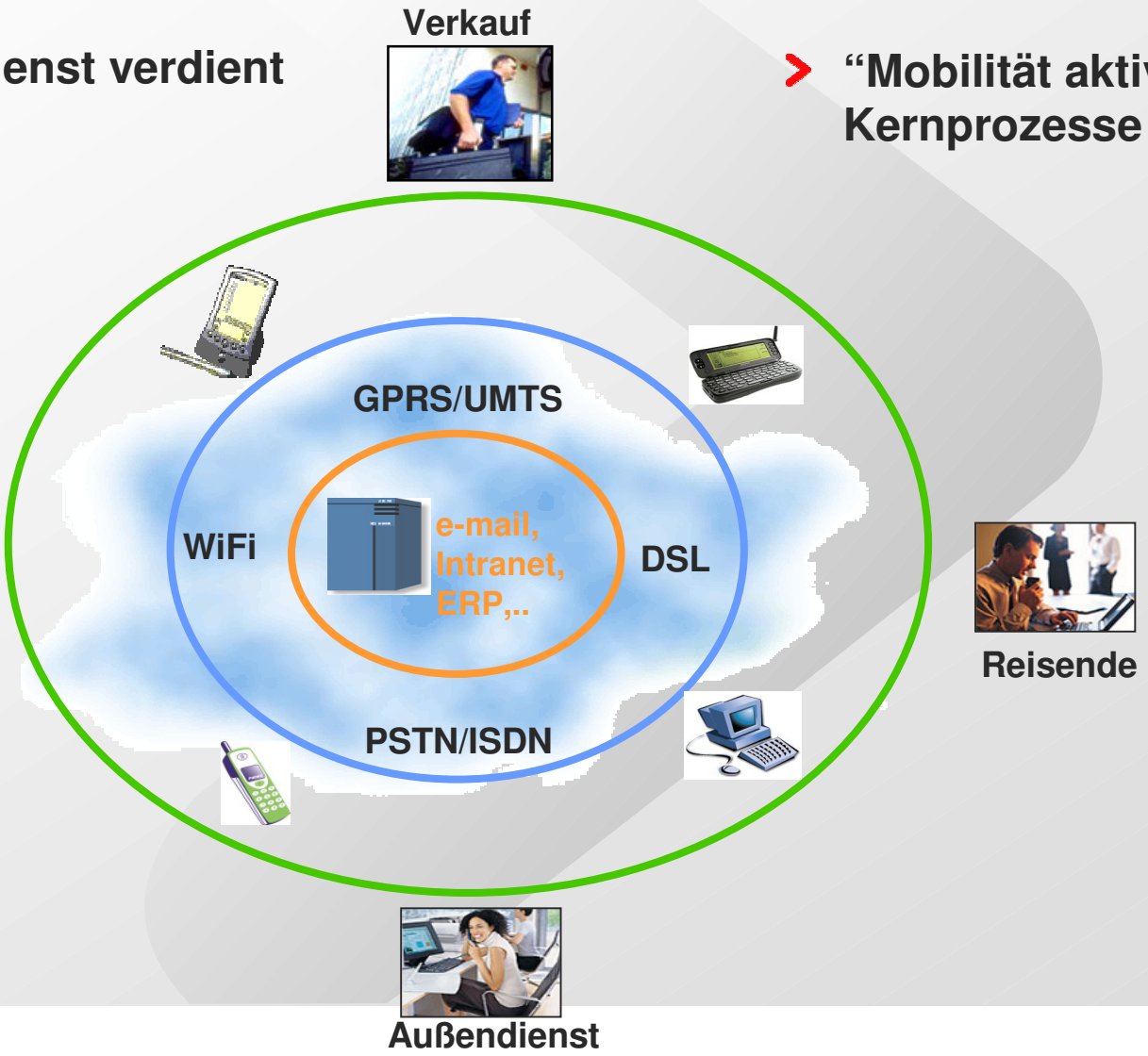
- **Keine Benutzerverwaltung innerhalb von Web Diensten**
  - Externes, zentralisiertes Benutzermanagement → Föderierte Identitäten
  - Externe Autorisierungsverwaltung → Provisioning Dienste
  - Protokoll für Autorisierungsbereitstellung → Nachvollziehbarkeit
- **Keine Prozessintegration innerhalb der Web Dienste**
  - Sicherheit von Dokumenten → WD Security Exits
  - Revisonssichere Exchange-Infrastruktur → Sichere Exchanges
  - Audit von verteilten Prozessen und Szenarien → Auditgerüst

Perimetersicherheit ist nicht länger ausreichend

Mobilität – der nächste daraus folgende Schritt

- “Der Außendienst verdient das Geld”

- “Mobilität aktiv in die Kernprozesse integrieren”



Sichere Mobilitätslösung durch Mehrstufigkeit

- Detaillierte Mobilitätslösung
- Definierte Strategie & Zweckmäßigkeit
- Definierte KPI's und Kontrollen
- Identifiziert spezifische Mobilitäts-möglichkeiten
- Passt Sicherheitsrilis mobilen Er-fordernissen an
- Auf Basis einer globalen Infrastruktur und Architektur

Mobilitätsstrategie

- Definition der geschäfts-bezogenen Architektur
- Front-End Anwendungs-lösungsdesign
- End-2- End Anwendungs-kommunikation
- End-2-End Anwendungsverwaltung

Prozesse & Anwendungen

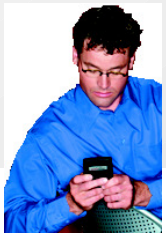
- AAA Lösungsdesign & Implementierung
- PKI Lösungsdesign & Implementierung
- Front-end VPN Zugriffs-lösung
- Front-End Datenschutz-lösung
- Zugriffskostenverwaltung
- End-2-End Kommunikations-verwaltung

Infrastruktur Globales Intranet

- Globale Zugangslösung
- Providerverwaltung

Infrastruktur Globales Internet

Hugo



GSM
UMTS
GPRS
WiFi
xDSL

Internet

Was erwartet uns als nächstes ?

- **Formalisiertes Risiko und Compliance Management (COSO)**
- **Identity & Access Management über organisatorische Grenzen hinweg (Liberty Alliance project)**
- **Höherer Fokus auf anwendungsbezogene Sicherheit bei Secure Web Services**
- **Managed Endpoint Security**
- **Starke Authentifizierung wird immer häufiger benötigt**
- **Single Sign-On**
- **Eingebaute anstatt angehängte Sicherheit**
  - ie. VoIP secured with IPSEC

Quellen

- PITAC (Presidents Information Technology Advisory Committee) “Cyber Security: A Crisis of Prioritization” *US Government* February 2005 http://www.itrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf
- Alan Lawson “A World without Boundaries” *Butler Review Journal Article* April 2005 http://www.butlergroup.com/research/DocView.asp?ID={BD1E4C70-F644-42F1-903E-CDBC09A38B8D}
- Paul Stamp, & Robert Whiteley mit Laura Koetzle & Michael Rasmussen “Jericho Forum Looks To Bring Network Walls Tumbling Down” *Forrester* http://www.forrester.com/Research/Document/Excerpt/0,7211,37317,00.html
- Joanne Cummings "Security in a world without borders" *Network World* 27 September 2004 http://www.networkworld.com/buzz/2004/092704perimeter.html
- http://www.jerichoforum.org
- http://www.opengroup.org
- http://wirelessman.org
- SAP Deutschland GmbH (Dr. Sachar Paulus)
- … und natürlich CISCO, Forrester research, Gartner Group, Burton Group u.v.a.


Am Ende dreht sich alles nur um …
Vertrauen
Integrität
Vertraulichkeit

IT Sicherheitstrends in der nächsten Zeit

Alexander Tsolkas

CISO Schenker AG

Unternehmertag FH Hof