– Mobile Sicherheit –

Unterschiedliche Unternehmen, unterschiedliche Ansätze

Frank Pallas
Technische Universität Berlin

IT Profits 2006, Kongress Panel „Sicherheit mit IT“
Berlin, 12. Mai 2006

Was erwartet Sie hier?

Auf jeden Fall nicht:
Absolute Weisheit

Eher schon:
Nachdenkliche Anregungen

Hoffentlich nicht:
Ein Blick aus dem Elfenbeinturm

Ein aktueller Anlass

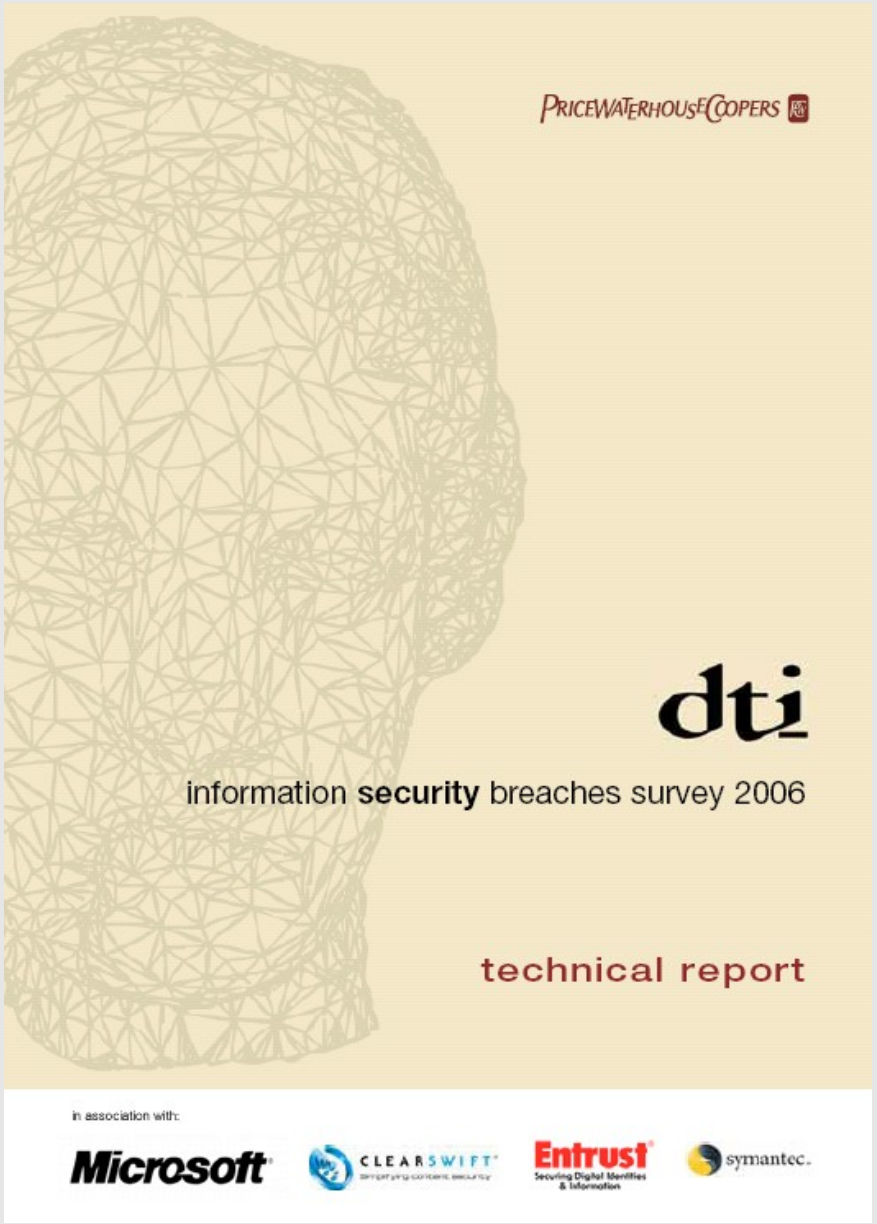
news 25.04.2006 17:17

<< Vorige | Nächste >>

Studie: Sicherheitsvorfälle in UK kosten 10 Milliarden Pfund

Der durch Viren, Spyware und Hackerangriffe verursachte Schaden in britischen Unternehmen beträgt jährlich rund 10 Milliarden Pfund. Das ist das Ergebnis einer von PricewaterhouseCoopers unter rund 1000 britischen Firmen durchgeführten Umfrage "DTI Information Security Breaches Survey". Laut der heute auf der Infosec-Konferenz in London vorgestellten Umfrage ist der Schaden im Vergleich zur 2004 erstellten Studie damit um 50 Prozent gestiegen, obwohl die Unternehmen ihre Investitionen in IT-Sicherheit von drei Prozent in 2004 auf vier bis fünf Prozent ihres IT-Budgets in 2006 erhöht haben.

Die Studie



- Information Security Breaches Survey 2006
- UK Department of Trade and Industry / PwC
- Eine der seltenen „repräsentativen“ Studien
  - Unternehmensgröße
  - Wirtschaftssektoren
- http://www.security-survey.gov.uk/

Ein Ergebnis

Kosten von Sicherheitsvorfällen in UK: insgesamt 10 Mrd. Pfund / Jahr

- Veränderung ggü. 2004 insg.: **+50%**
- Große Unternehmen: **-50%**

Woran liegt das?

These:

IT-Sicherheit in der derzeit propagierten Form ist auf zentralistische Unternehmen ausgerichtet.

Für andere Unternehmen muss daher u.U. eine andere Vorgehensweise her.

Für Mobile Sicherheit gilt dies in besonderem Maße.

Das Problem

Unternehmen

- Will / muss Informationen möglichst vertraulich halten
- Will / muss Infrastruktur schützen

➔„Hohe IT-Sicherheit“

Mitarbeiter

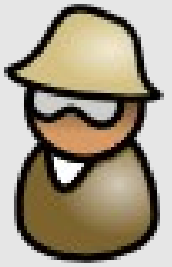
- Will / braucht Informationen zur Aufgabenerledigung
- Will / braucht Zugriff auf Infrastruktur

➔„Niedrige IT-Sicherheit“

Die Herausforderung

Identifikation und Durchsetzung eines „angemessenen“ Schutzniveaus

Der technische Ansatz



Unternehmen

Mitarbeiter

Schutzziele

Sicherheits-
maßnahmen

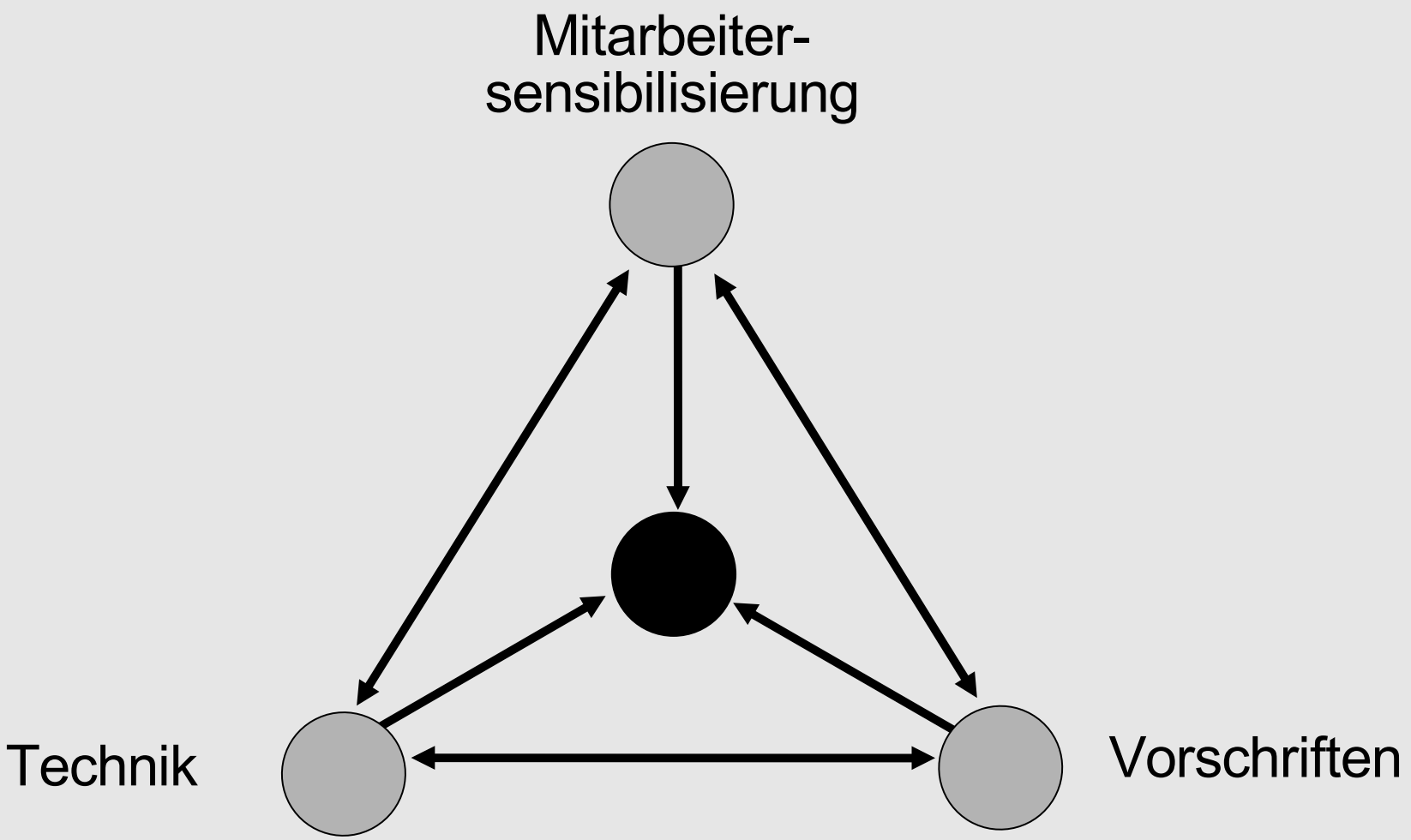
Security Management

Handlungs-
einschränkungen

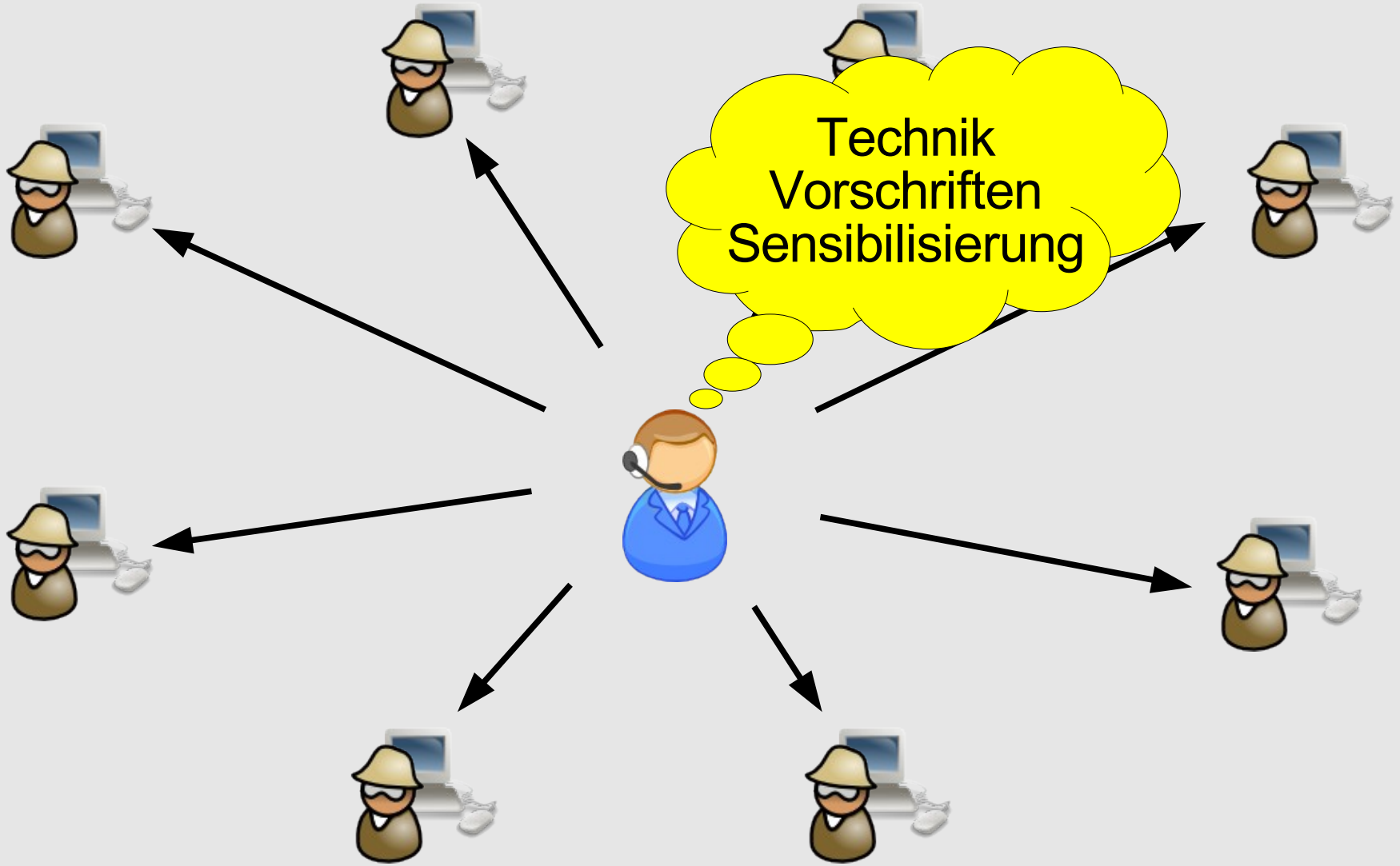
Funktions-
einschränkungen

Security Enforcement

Der – mittlerweile – übliche Ansatz



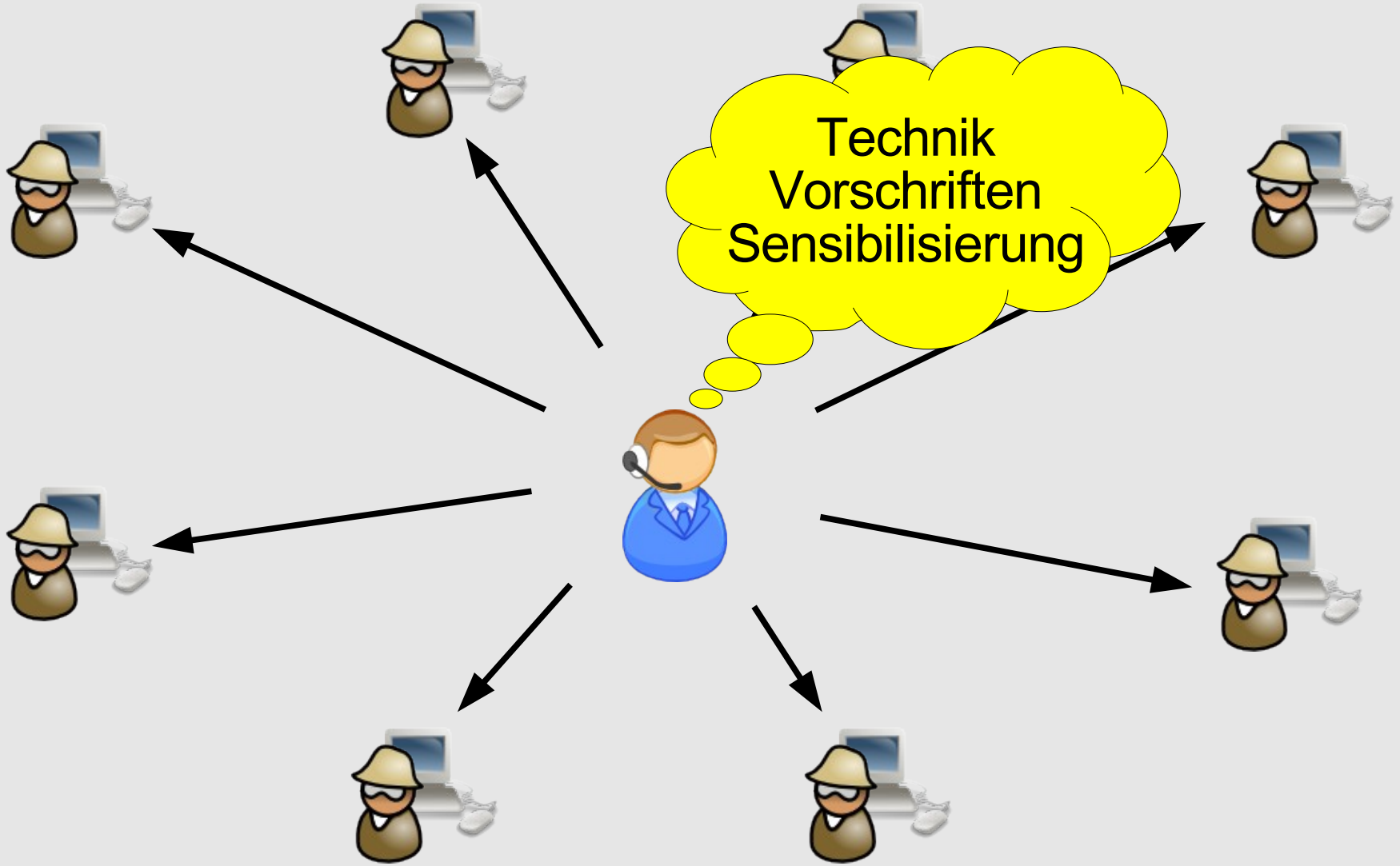
Der übliche Ansatz



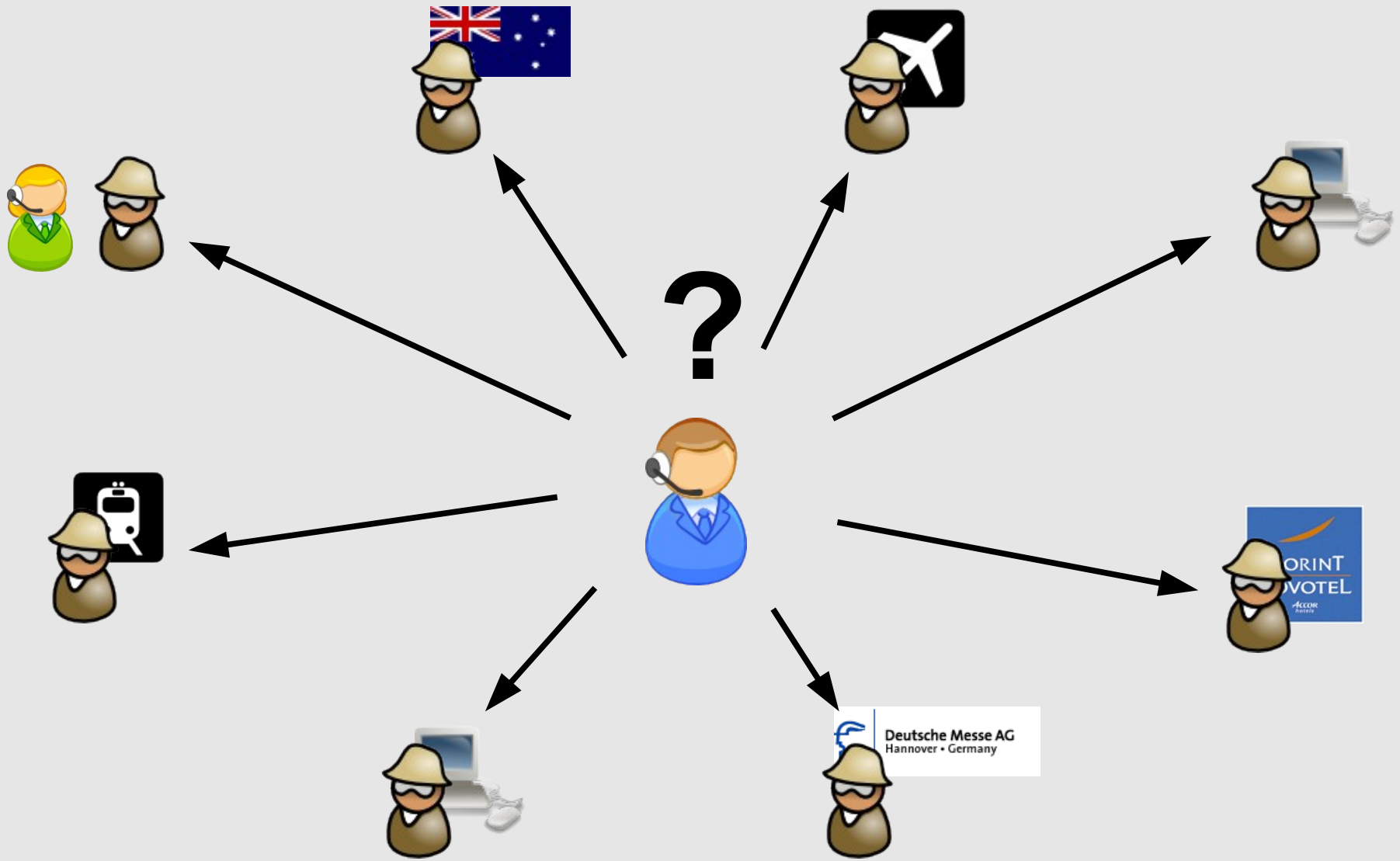
„[M]obility makes things more difficult.“

Roger Needham, Microsoft Research

Der übliche Ansatz



Grenzen des üblichen Ansatzes?



Auswirkungen von Mobilität

- Neue Risiken kommen hinzu
  - Technik kann hier sicherlich einiges tun
- Individuelle Anforderungen und Risiken unterscheiden sich weitaus stärker
  - Bestimmung des *individuell angemessenen Schutzniveaus* nahezu unmöglich

Was also tun?

Möglichkeit 1: Command and Control

- Idee:
  Zentrale Instanz legt Verhaltensregeln fest und setzt Einhaltung durch
  - Durch Technik (USB-Sticks, enforced VPN, ...)
  - Durch Vorschriften (USB-Verbot + Bestrafung, ...)
  - evtl. durch Normensetzung / Sensibilisierung
- Pro:
  Das Unternehmen kann sich „sicher“ sein
- Contra:
  Suboptimale Nutzung von Ressourcen
  - Schutzniveau „zu hoch“ → Weniger produktive Tätigkeiten möglich, ...

Möglichkeit 1: Command and Control

Vermutung:

- Vorgehen wahrscheinlich eher für hierarchisch aufgebaute Unternehmen geeignet, da notwendige Mechanismen existieren:
  - Command
  - Control
  - Sanktionierung
- Vorgehen wahrscheinlich nicht für andere Unternehmen geeignet, da maßgebliche Grundwerte verletzt werden

Möglichkeit 2: Coordinate and Cultivate

- Idee:
  Mitarbeiter sind selbst verantwortlich
  - wissen am besten, welches Schutzniveau gerade „angemessen“ ist
  - „Sicheres Verhalten“ muss **ermöglicht** werden (Schulungen, Bereitstellung von Software, ...)
  - Individualinteresse an Sicherheit wird evtl. durch **Anreize** gesteuert
- Pro:
  Weniger Einbußen durch „zu hohe“ Sicherheit
- Contra:
  Kontrollverlust, Unsicherheit, ...

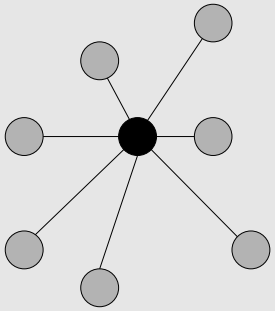
Möglichkeit 2: Coordinate and Cultivate

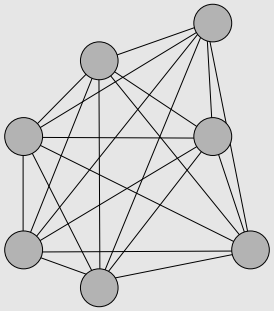
Vermutung:

- Vorgehen wahrscheinlich eher für nicht-hierarchisch aufgebaute Unternehmen geeignet, da Grundwerte gleich sind:
  - Eigenverantwortung
  - Autonomie
  - Kooperation
- Vorgehen wahrscheinlich nicht für extrem hierarchische Unternehmen geeignet, da
  - Mitarbeiter opportunistischer sind
  - Zentralinstanzen Macht abgeben müssten

IT-Sicherheit: Zentral oder dezentral?

Was für ein Unternehmen sind Sie?





Zentrale Hierarchien	**Lose Hierarchien**	**Demo-kratien**	**Märkte**
Militär, klassische Produktion	Universität, Kreativunter-nehmen	Kleinst-unter-nehmen	Business Networks

Grafik nach:
Malone (2004), S. 6: The Future of Work

„As soon as you have distributed systems, you have people responsible for security in all sorts of places,

and they have to apply rules which in general terms they don't understand.“

Roger Needham, Microsoft Research

Über den Referenten

Frank Pallas

Technische Universität Berlin - Informatik und Gesellschaft

pallas@cs.tu-berlin.de

http://ig.cs.tu-berlin.de/ma/fp/

http://ig.cs.tu-berlin.de/forschung/mobile/

Bonusfolien

Und die Presse?

Mobile (Un)-Sicherheit in Unternehmen

Symantec 12|4|2006

Für Unternehmen sind Sicherheitsbedenken das größte Hindernis bei der Einführung mobiler Technologien. So setzen über 60 Prozent aller Unternehmen die neuen Technologien nur begrenzt ein, da sie keine zusätzlichen Sicherheitsrisiken

Studie: IT-Verantwortliche vernachlässigen die mobile Sicherheit

Mobile Security gewinnt immer mehr an Bedeutung. Zahlreiche CeBIT-Aussteller widmen sich dem Thema an ihren Ständen. Aufklärung tut Not: Nur 19,4 Prozent aller deutschen Unternehmen haben bereits Vorkehrungen zum Schutz ihrer mobilen Informationssysteme getroffen.

Firmen sollten effektive IT-Richtlinien für den Umg

Lost a BlackBerry? Data Could Open A Security Breach

By Yuki Noguchi
Washington Post Staff Writer
Monday, July 25, 2005; Page A01

The ability to carry vast amounts of data in small but easily misplaced items such as computer memory sticks and mobile e-mail devices has transformed the way Americans work, but it has also increased the risk that a forgotten BlackBerry or lost cell phone

Securing the (Increasingly) Mobile Client

By James L. Bindseil, Global Technical Director Symantec
Tuesday, 26 October 2004 11:00 EST

Enterprise deployments of notebook PCs, tablet PCs, and PDAs continue t leaps and bounds. In fact, researcher Gartner Inc. recently predicted that year 2010, 80 percent of key business processes will involve the exchang real-time information involving mobile workers.

Small wonder, then, th emerged as Priority Nc business risks that toc and the need for a pro

Europas Sicherheitsagentur will sich um mobile Gefahren und Identitätsklau kümmern

Die European Network and Information Security Agency (ENISA) wird sich im laufenden Jahr unter anderem mit den wachsenden Gefahren in mobilen Netzen und mit dem Thema Identitätsklau beschäftigen. Das sagte der Direktor der ENISA, Andrea Pirotti, auf Anfrage von heise online. Für beide Themen sollen ENISA-Arbeitsgruppen eingerichtet werden, erklärte Pirotti. Vor den Informations- und Kommunikationstechnik-Treffen auf Einladung der österreichischen EU-Ratspräsidentschaft hatte die ENISA sich mit ihrer Expertengruppe (Permanent Stakeholder Group aus Vertretern von Industrie und Wissenschaft getroffen.