Status Quo der Sicherheitslage

Secure Summit 2010

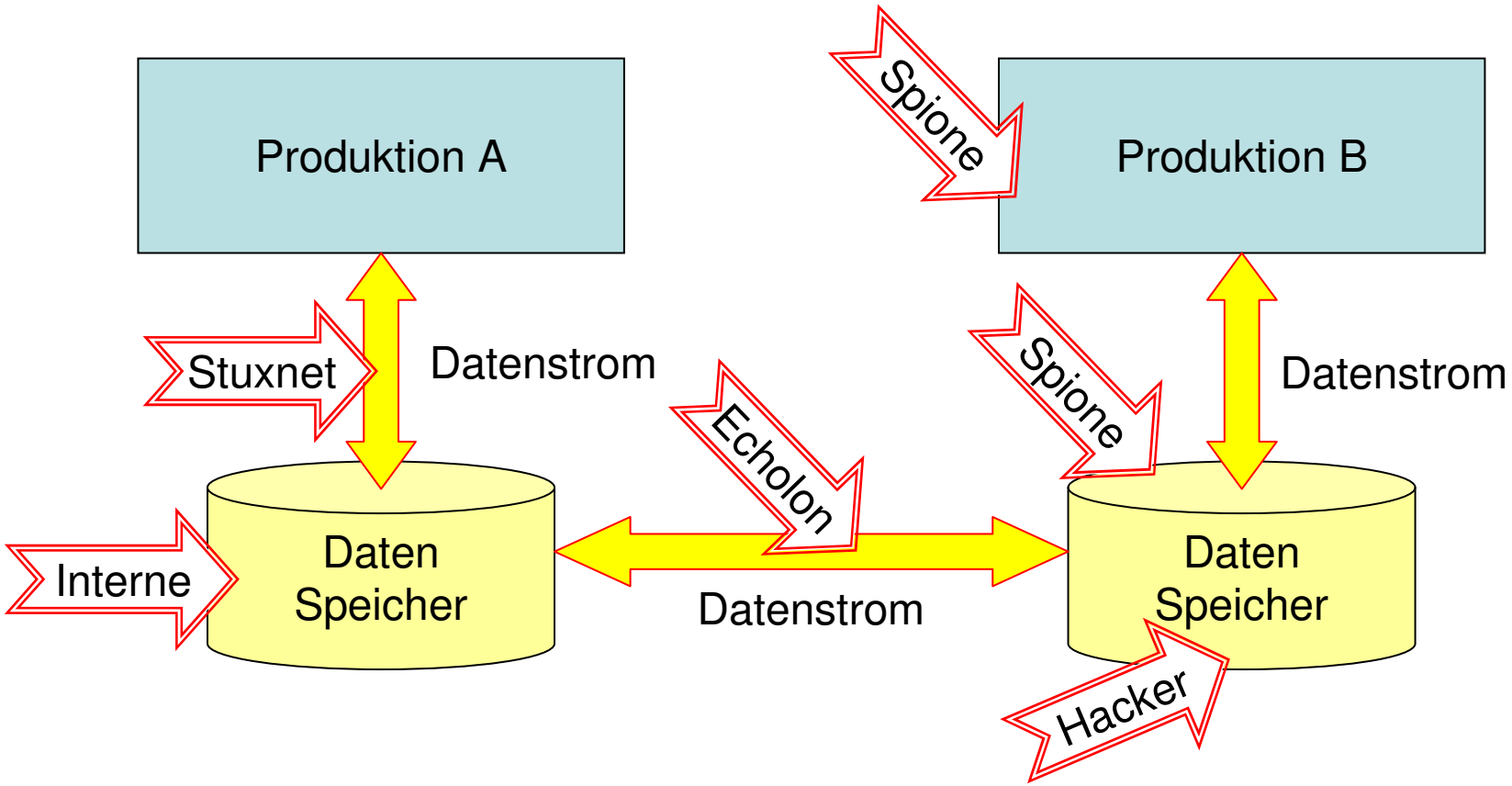
Prof. Dr. Eduard Heindl

Prof. Dr. Eduard Heindl
Hochschule Furtwangen

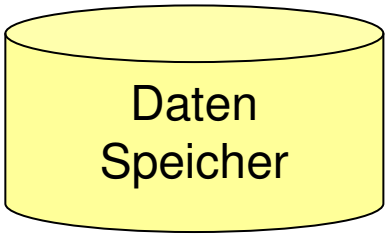
Themen

- Strategische Veränderung des Risikos
- Aktuelle Bedrohungsszenarien
- Täterformen
- Angemessene Reaktionen
- Herausforderungen für die Zukunft

Strukturproblem

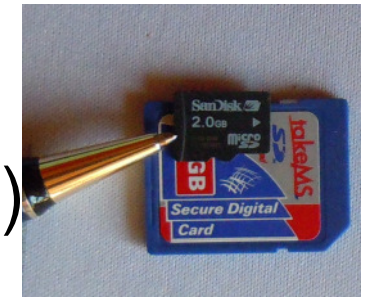


Prof. Dr. Eduard Heindl
Hochschule Furtwangen



Speicherentwicklung

- Das alte Quelle-Rechenzentrum hatte 500MB Speicher für alle Vorgänge
- Platzbedarf eine Halle
- Eine microSD Karte hat 8.000MB (8GB)
- Platzbedarf <1cm²



Alle relevanten Daten können theoretisch bei einem Besuch am Werkschutz vorbeigeschmuggelt werden

Prof. Dr. Eduard Heindl
Hochschule Furtwangen

Mobilität

- Immer mehr Unternehmen arbeiten mit verteilten Arbeitsumgebungen.
- Meetings, Schulungen, Dienstreisen, Konferenzen
- Heim-Arbeitsplätze sorgen dafür, dass auch immer mehr wettbewerbsrelevante Unternehmensdaten unterwegs sind.
- *Wie sind Ihre Daten auf Laptops, Smartphones, USB-Sticks oder in Clouds geschützt?*

Datentransfer

- Das Datentransfervolumen wächst um 40% jährlich
- 2013 werden 56 Exabyte pro Monat versendet
- 56 Exabyte = 56.000.000.000 GByte

Datentransfer durch Spionage wird immer stärker überdeckt durch normalen Transfer

Cisco, Computerwelt

Produktion A

Wissen in Daten

- Unternehmen speichern alle Daten digital ab und halten diese „online“ bereit
- Expertenwissen wird „digitalisiert“ (Wissensmanagement)
- Mitarbeiter sollen „auswechselbar“ sein

Daten in Unternehmen enthalten mehr Wissen als je zuvor

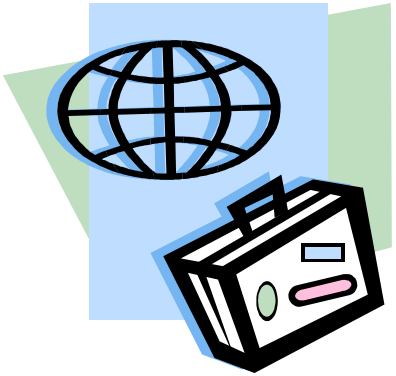
Erfolgswissen

„Der Großteil der Informationen ist heute frei verfügbar und kann somit legal erworben werden. Das strategische Erfolgswissen allerdings, das in der Regel die Existenz eines Unternehmens garantiert, bedarf auch weiterhin eines besonderen Schutzes vor Wirtschaftsspionage und Konkurrenzausspähung.“

Digitalisierung

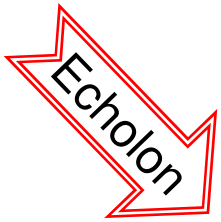
- Unser Tun und Handeln ist inzwischen fast vollständig digitalisiert.
- Planungen, Notizen, Abschlussberichte, Forecasts, Präsentationen, Konditionen, Bewertungen, Beurteilungen, Listen von Kunden, Mitarbeitern, Lieferanten ... alles Daten, alles digital, alles extrem schutzbedürftig.

Globalisierung



- Immer mehr Länder nutzen IT
- Wettbewerb wird immer schärfer
- Produkte enthalten immer mehr Information
- Bereitschaft zur Industriespionage wächst

Ungeschützte Daten werden vermehrt „abgegriffen“



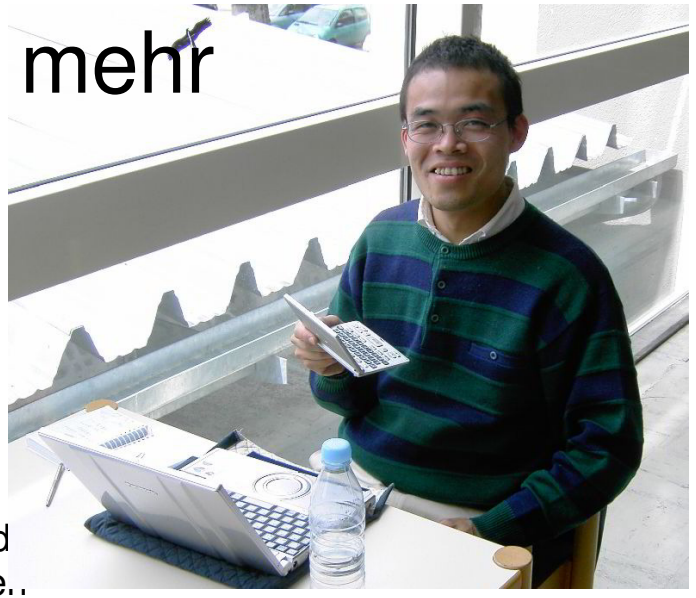
Gefährdungslage

„Die Gefährdungslage in Deutschland ist konkret. Staaten wie Russland und China betreiben mit ihren Nachrichtendiensten aktiv Spionage in den Bereichen Wirtschaft, Wissenschaft und Forschung.“

Gesellschaftlicher Wandel

- Arbeitsplätze werden häufiger gewechselt
- Bindung zum Unternehmen nimmt ab
- Datendiebstahl ist bei jungen Menschen ein Kavaliersdelikt (Video, Audio!)
- Sorgfalt ist keine Tugend mehr

Menschen handeln heute anders als früher



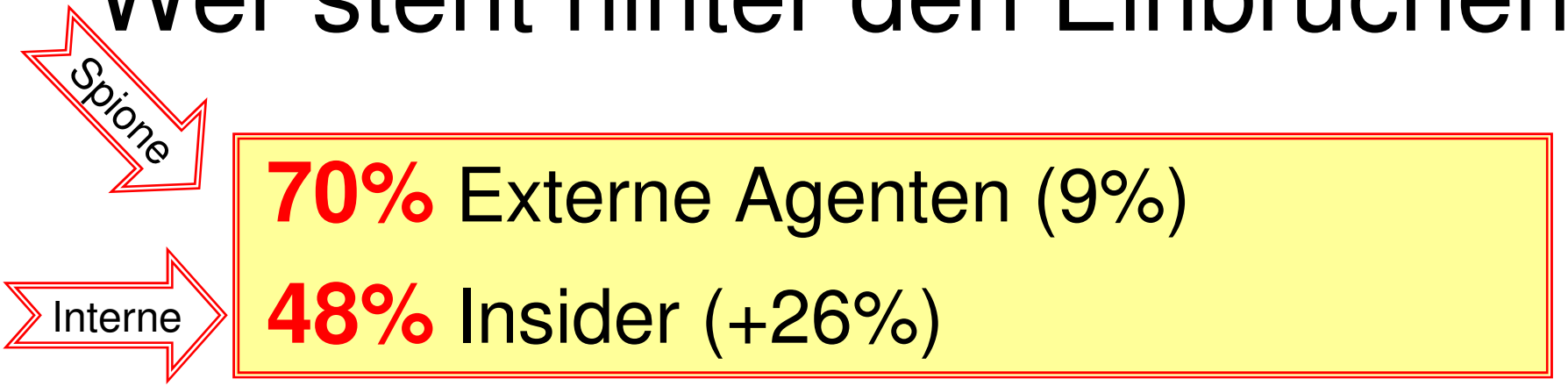
(Un)sicherheit

- Überall dort, wo viele Menschen zugreifen können, ergeben sich auch Lücken, Schwachstellen, Fehlerquellen und Möglichkeiten zum Missbrauch. Ob unabsichtlich oder gewollt,
- das Ergebnis ist ein *Schaden für das Unternehmen*

Vorbemerkung: Dunkelziffer

- Dunkelziffer 1. Art:
  - Entdeckter Datendiebstahl wird nicht den Behörden gemeldet
- Dunkelziffer 2. Art
  - Datendiebstahl kann in den Logfiles erkannt werden, bleibt aber unbemerkt
- Dunkelziffer 3. Art
  - Datendiebstahl erfolgt spurlos, indem z.B. ein unverschlüsseltes WLAN abgehört wurde

Wer steht hinter den Einbrüchen



Vorgehensweise

48% Missbrach von Rechten (+26%)

40% Hacking (-24%)

38% Schadsoftware

28% Social Hacking (+16%)

15% Physischer Angriff (+6%)

Gemeinsame Eigenschaften

98% Server betroffen

85% Angriff nicht sehr schwierig

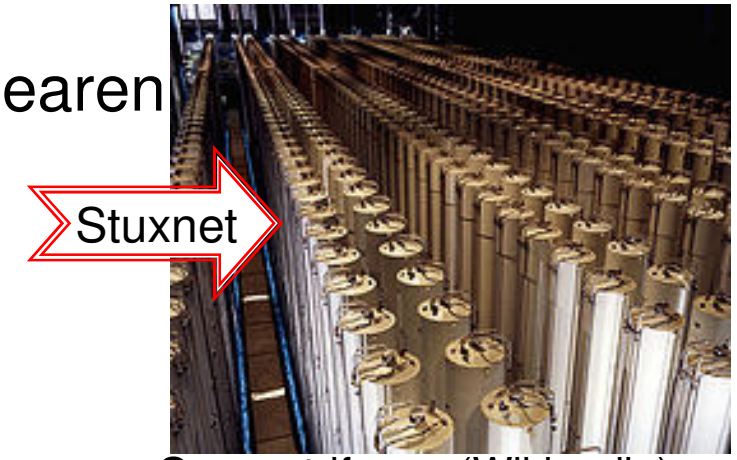
61% Entdeckung durch Dritte

86% Hinweise im Logfile vorhanden

96% Vermeidbar durch relativ einfache Vorsorge

Stuxnet

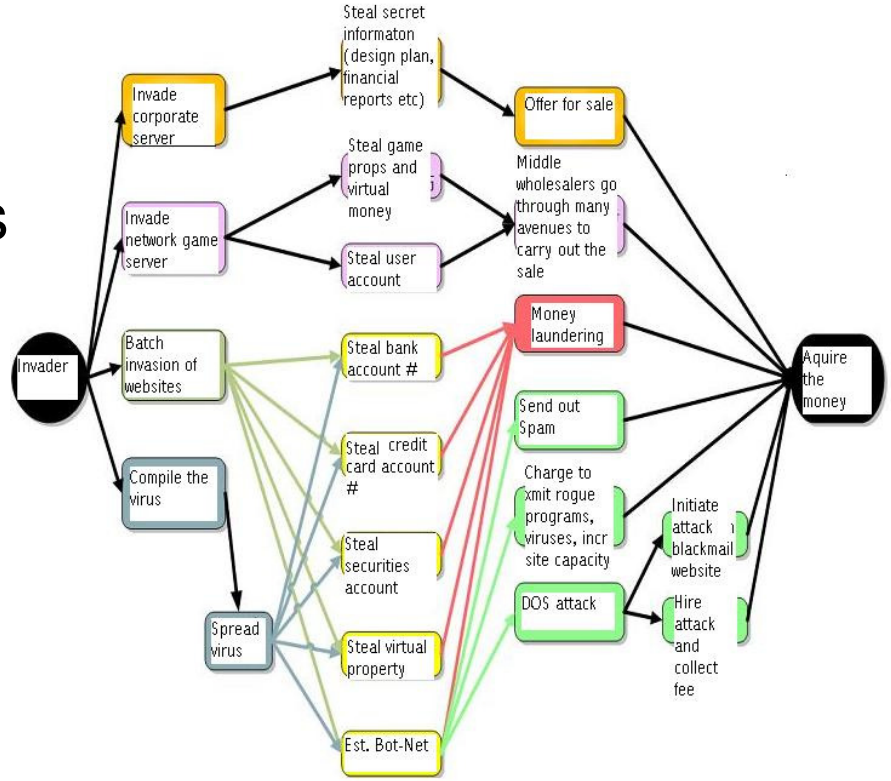
- Der digitale Erstschlag ist erfolgt (FAZ)
  - Stilllegung der iranischen nuklearen Anreicherung
  - Trojaner per USB übertragen
- Digital gesteuerte Produktionsanlagen können prinzipiell zerstört werden
- Angriff erfordert massives IT Know How
- Einsatz von US Software problematisch



Gaszentrifugen (Wikipedia)

GhostNet

„Im April 2009 veröffentlichte das kanadische Institut Munk Centers for International Studies eine Studie über ein als „GhostNet“ bezeichnetes Computerspionagenetzwerk, das mutmaßlich von China unterhalten wird“

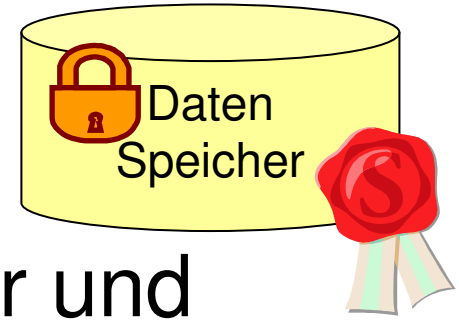


www.darkgovernment.com/news/chinas-ghostnet/

Verfassungsschutzbericht 2009

Mögliche Lösungen

- Daten müssen bereits auf dem Datenträger verschlüsselt sein
- Zugriff nur über digitale Signatur und biometrische Kennung
- Schulung der Mitarbeiter
- Anzahl unternehmensfremder Personen mit digitalen Rechten begrenzen
- Sorgfältiges Rechtemanagement



Herausforderungen I

- Intelligente Viren
  - Schadsoftware wird sehr viel spezifischer nach Dokumenten suchen
  - Verbesserte Tarnung
- Mobilfunk
  - Multimedia Handys sind optimale Plattform für Spionage
  - Neue, schnelle Transportkanäle
- Qualität digitaler Zertifikate
  - Herausgeber
  - Interface

Herausforderungen II

- Miniaturisierung
  - Kameras
  - Speichermedien
- Delokalisation
  - Cloud Computing
  - Outsourcing
- Komplexität
  - Systemgröße
  - Integration von IT in Alles „embedded“
  - Kommunikationsnetzwerke SAS