



---

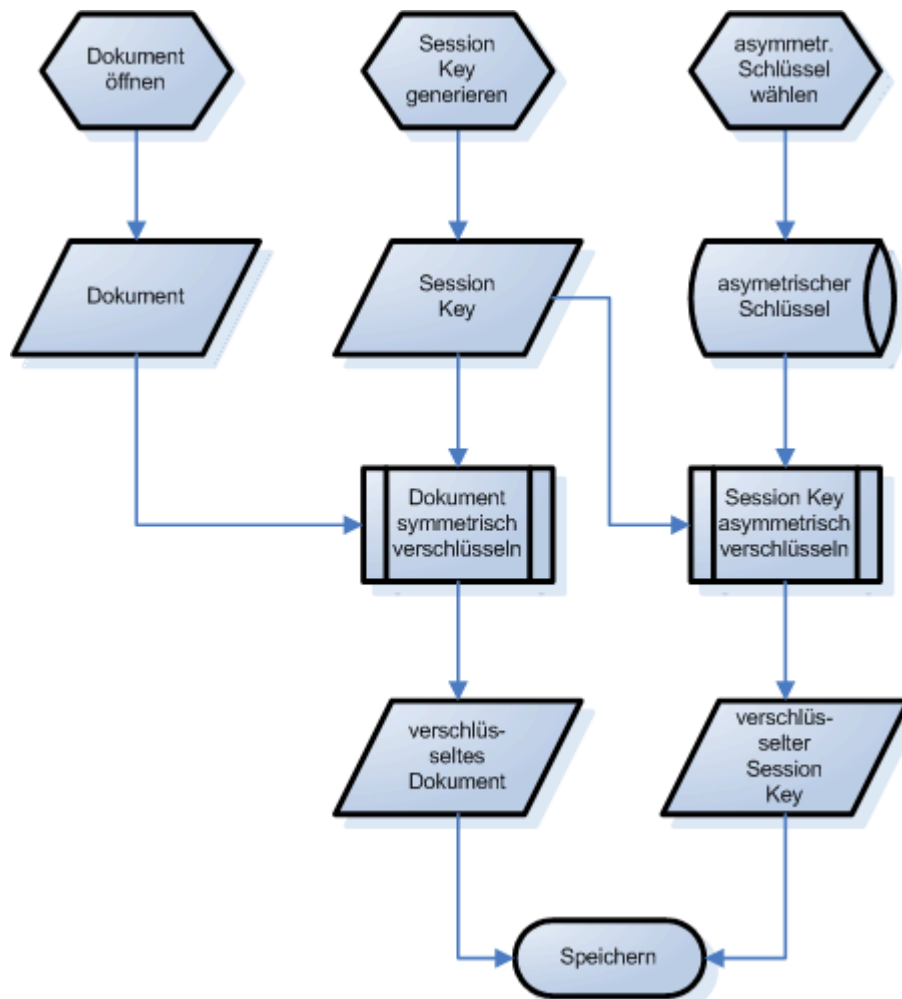
# Unternehmerische Verantwortung für Daten und Sicherheit

Vertrauen ist gut – Controlling ist besser

---



# Was ist mit IT-Sicherheit gemeint?



- Firewalls?
- Virens Scanner?
- Verschlüsselung?

# Was ist mit IT-Sicherheit gemeint?

## ■ Technik allein?

**NEIN**

## ■ Sondern?



# Haftung des Geschäftsführers

- **Basel II – Risikomanagement**
- **GdPdU – Betriebsprüfung**
- **BDSG – Datenschutz**
- **SOX – Börsenaufsicht**
  
- **Organisationsverschulden**
- **Produkthaftung**



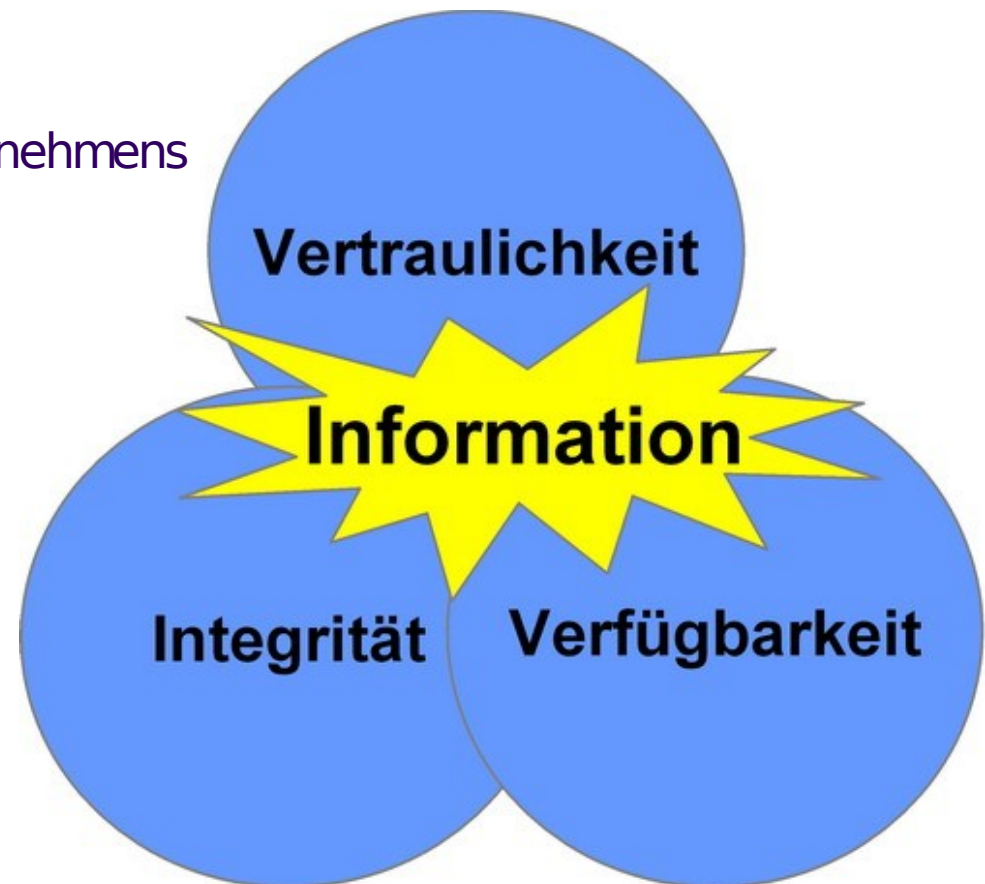
# Was heißt Informationssicherheit?

Unter Informationssicherheit verstehen wir den Schutz

- der Unternehmensziele,
- der Daten und Prozesse des Unternehmens
- der technischen Infrastruktur

gegen den Verlust

- der Verfügbarkeit
- der Vertraulichkeit
- der Integrität

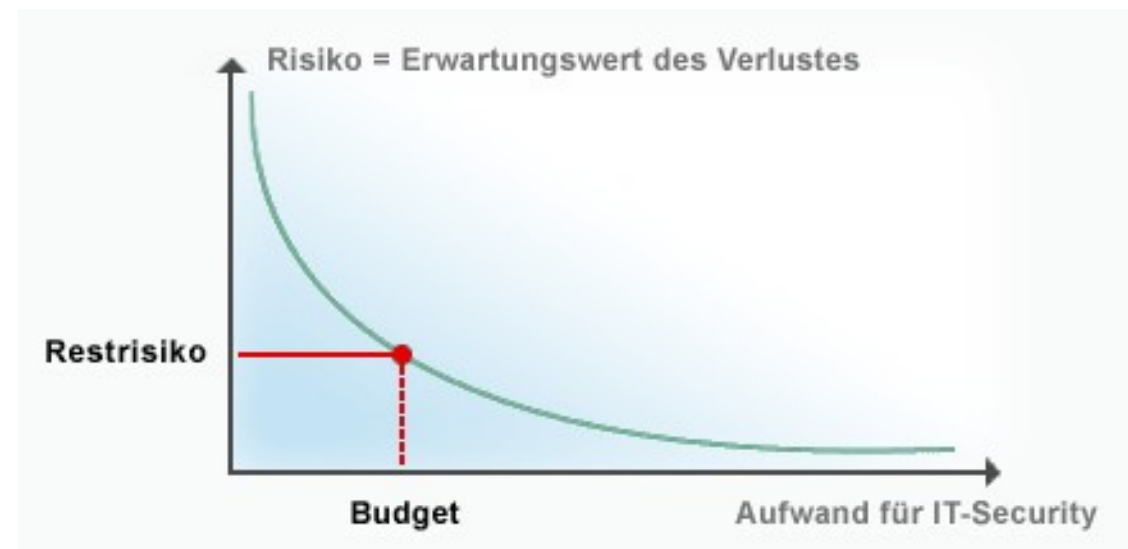


# Was will IT-Sicherheit?

**Ziel der IT-Sicherheit ist es, Risiken,**

- die aufgrund realistischer Bedrohungen vorhanden sind,
- durch wirtschaftlich angemessene Maßnahmen
- auf ein akzeptables Maß

**zu beschränken.**



# Was Sie erwartet

- Warum schützen?
- Warum ich?
- Was schützen?
- Wovor schützen?
- Wie schützen?

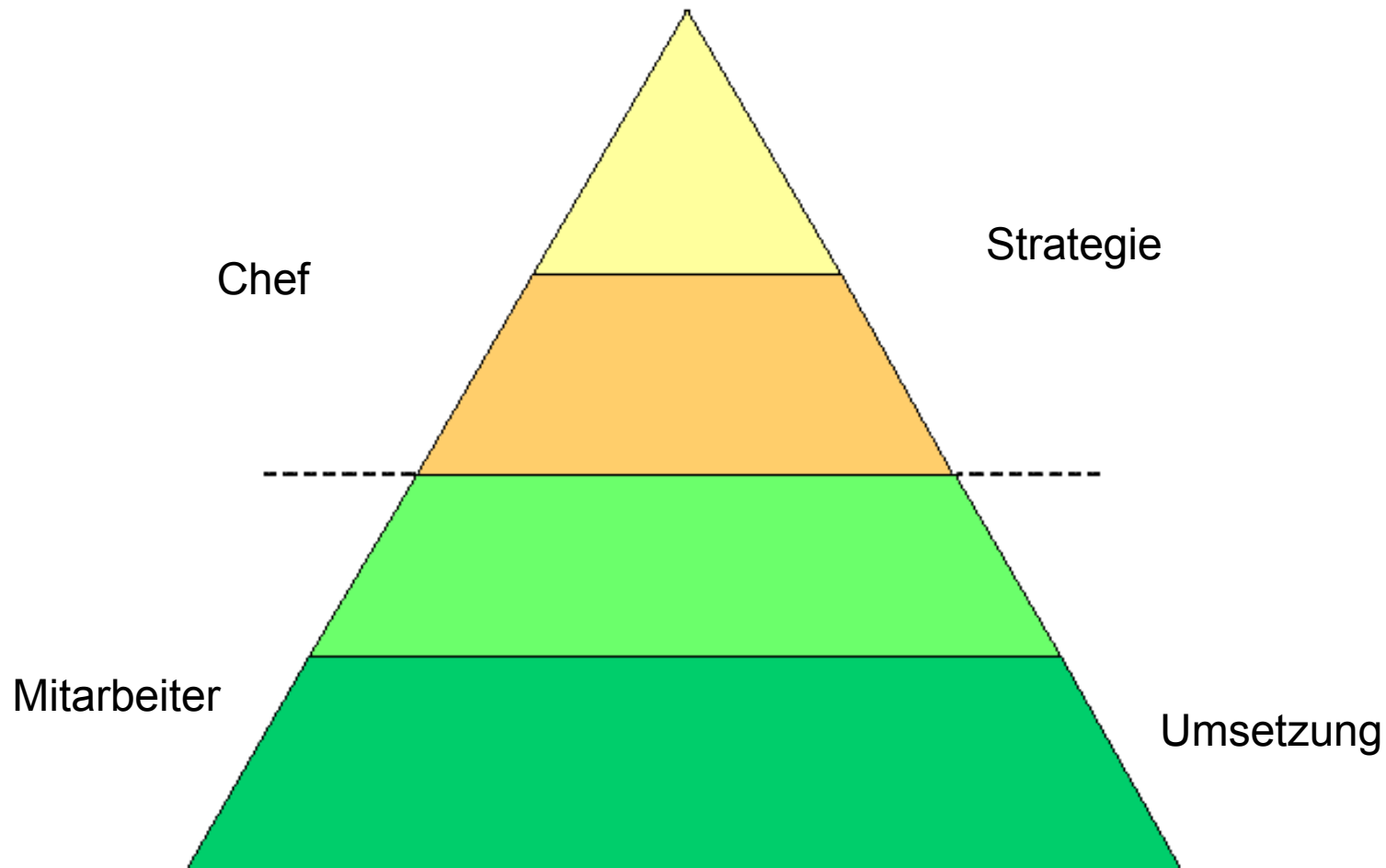


# Wandel IT und Sicherheit

- **komplexe interne und weltweite Netzwerke**
  - Wie leicht lassen sich Daten (weg)transportieren?
- **Integration der IT in zentrale Unternehmensprozesse**
  - Was läuft, wenn meine IT nicht mehr läuft?
- **Ganzheitliche Architektur**
- **IT-Sicherheit heißt heute  
Schutz der Funktionsfähigkeit des Unternehmens**



# Organisation der Sicherheit



# Sicherheit ist Chefsache

- **Delegation ist ein Zyklus aus Beschreiben (Verantwortung), Warten und Verantwortung wieder übernehmen (Kontrolle)**
  - Führung durch Zielvereinbarung
  - Führung durch Abweichungskontrolle
- **Nicht delegierbar sind**
  - Formulierung der Unternehmensziele
  - Verantwortung für Unternehmensprozesse
  - Kontrolle der Maßnahmen
- **Delegierbar sind**
  - technische, organisatorische und personelle Beratung
  - Planung und Umsetzung der Maßnahmen



# Warum nicht der Administrator?

## ■ Der Admin hat keine Ahnung

- welche Prozesse die Ziele meines Unternehmens realisieren
- welchen Wert meine Daten in meinem Unternehmen haben

## ■ Der Admin kann nicht selbst kontrollieren

- ob er seine Aufgaben ordnungsgemäß ausübt

## ■ Der Admin muss nicht den Kopf hinhalten

⇒ Ich muss meine Verantwortung  
selbst wahrnehmen!



# Was schützen?

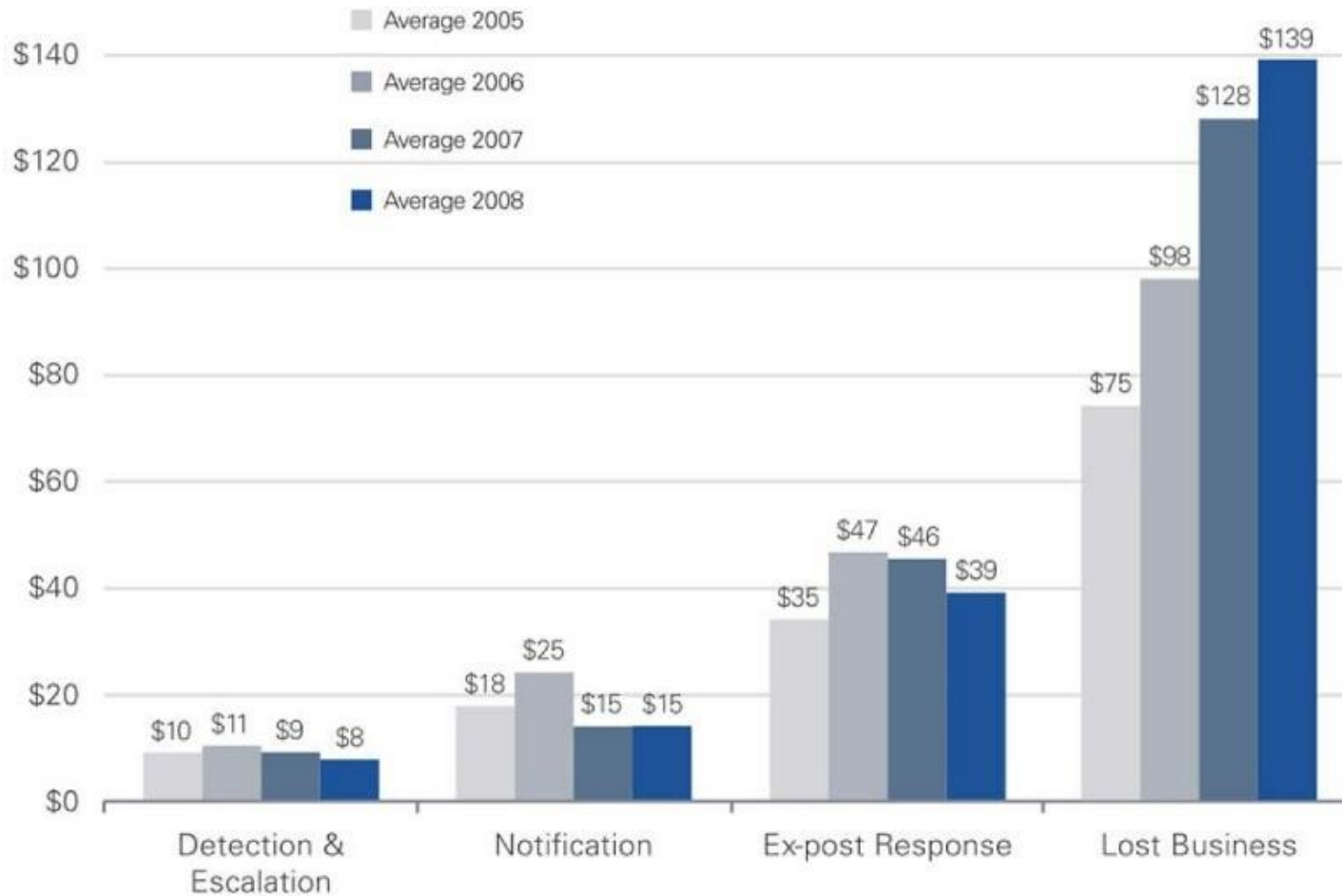
## ■ Informationen

- Know-How, eigentliche „Werte“
- auch nicht IT-mäßig erfasste Informationen
- Datenschutz aus Sicht des Betroffenen

## ■ Datenverarbeitung

- kein Datenschutz ohne sicheres System
- Prozesse von IT abhängig
- Hintertüren nicht vergessen

# Kosten je verlorenen Datensatz



# Personenbezogene Daten



**Imageverlust** ⇒ **Kundenverlust**

# Privatsphäre



## Persönliche strafrechtliche Konsequenzen

# Beispiele

## ■ Datenschutz-Problem

- Strafzahlungen bis zu 1,4 Mio €
- teure Anzeigenkampagne
- „Negativ-Beispiel“



⇒ Lange Nachwirkungen



# Alles schützen?

## ■ Ziele

- Haftungsrisiko ausschließen
- finanzielle Risiken vermindern

## ■ Auswahlkriterien

- Wert der Information für das Unternehmen
- Notwendigkeit aus Sicht des Betroffenen

# Wovor schützen?

## Gefahr erkannt – Gefahr gebannt?



# Betrachtung der Risiken



## Liste von Gefahren erstellen

- Was kann eintreten?
- Welcher Schaden entsteht?

⇒ Risiken erkennen

# Einflussfaktoren

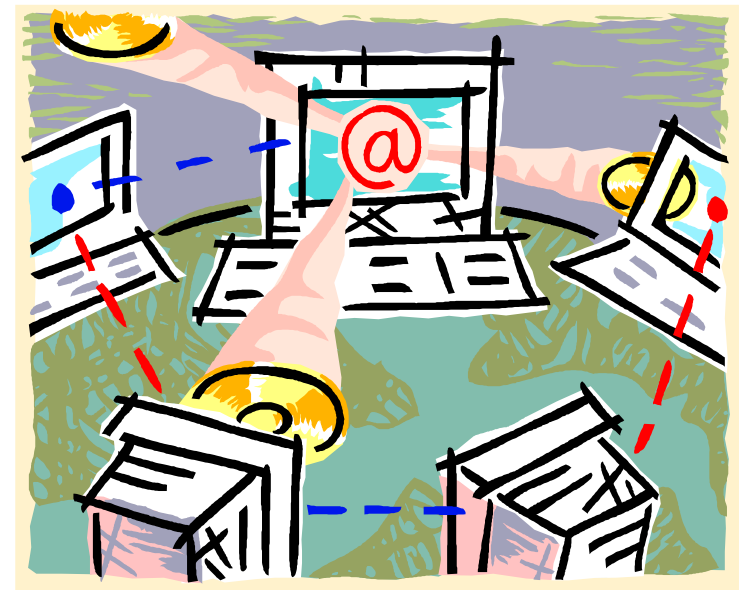


## Mensch

- **Das „größte“ Risiko**
- **unabsichtliche Fehler**
  - vertrauliche Information auf Schreibtisch liegen lassen
- **absichtliche Fehler**
  - Informationen aus dem Unternehmen entwenden

# Einflussfaktoren

- **Ausfall von Geräten**
  - defekte Harddisk
- **Fehler in Systemen**
  - Sicherheitslücke im Betriebssystem
- **Fehler in Programmen**
  - falsche Berechnung
- **Stromausfall**



## Technik

# Einflussfaktoren



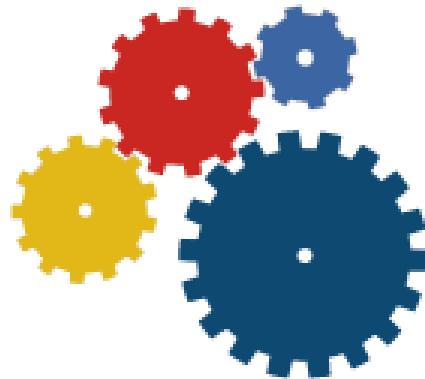
## Benutzung

- **Surfen im Internet**
  - Trojanische Pferde
  
- **Versand von E-Mail**
  - Schadsoftware im Anhang
  
- **Mitnahme von Notebook**
  - Diebstahl

# Ergebnis der Risikoerkennung

- **Auflistung erkannter Gefahren im Risiko-Katalog**
  - mit Angaben zur Eintrittswahrscheinlichkeit
  - und möglichem Schaden für das Unternehmen

⇒ **Hilfsmittel:**



**BSI Grundschutz - Gefahrenkataloge**

# Umgang mit Risiken



- Rechenzentrum im Keller wird überflutet
- ⇒ Rechenzentrum in den 2. Stock verlegen

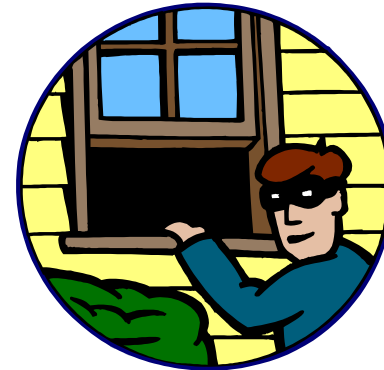
**Risiko - Vermeidung**

# Umgang mit Risiken

## ■ Ungeschützte Fenster

- Dieb dringt ein

⇒ Fenster vergittern



## Risiko - Verminderung

# Umgang mit Risiken



■ **Notebook wird gestohlen**

⇒ **Versicherung abschließen**



**Risiko - Überwälzung**

# Umgang mit Risiken



**Rest-Risiko  
muss / will man selbst tragen**

# Wo ist meine Verantwortung?

- **Vorgehen zu Risiken festlegen**
- **Klassifizierung von Schäden festlegen**
  - Was ist ein niedriger / mittlerer / hoher Schaden für das Unternehmen?
- **Rest-Risiken akzeptieren**
- **Kontrolle ausüben**
- **Prozess „in Gang halten“**

# Was kann ich delegieren?

- **Risiken / Gefahren für das Unternehmen erheben**
  - auch externe Vergabe
- **Bewertung der Risiken vornehmen**
  - Zusammenarbeit intern / extern
- **Maßnahmen ausarbeiten / umsetzen**
- **Überprüfung der Maßnahmen**
  - Bericht an Verantwortlichen (an Sie)

# Wie sehen Schutz-Vorkehrungen aus?

## ■ Wirksamer Schutz erfordert T O P -Maßnahmen

- Technische Einrichtungen
- Organisatorische Regelungen
- Personelle Qualifizierungsprozesse



# Was kann ich zur Wirksamkeit beitragen?

## ■ Technische Einrichtungen

- schützen höchstens vor technischen Bedrohungen

## ■ Merke

- **T** allein ersetzt nicht das **OP**erative Geschäft



# Beispiel: Angriff über USB

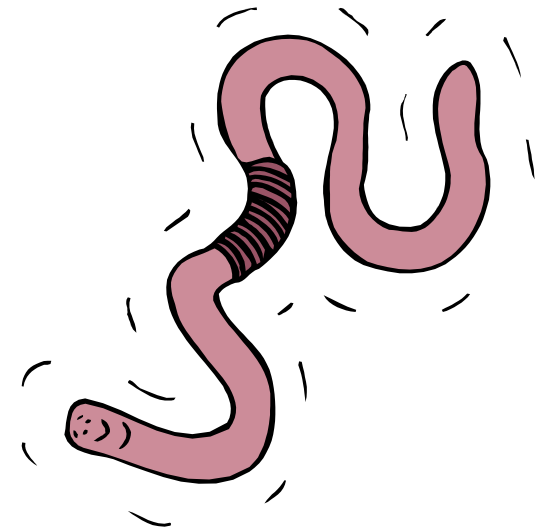
## ■ erfolgt via Autoplay-Funktion

- auf vielen Windows-Systemen ist die Autoplay-Funktion aktiviert

## ■ Infektion erfolgt in beide Richtungen

- USB-Stick verseucht PC
- PC verseucht USB-Stick

## ■ Dies ist ein Hauptverbreitungsweg des bekannten Conficker-Wurms

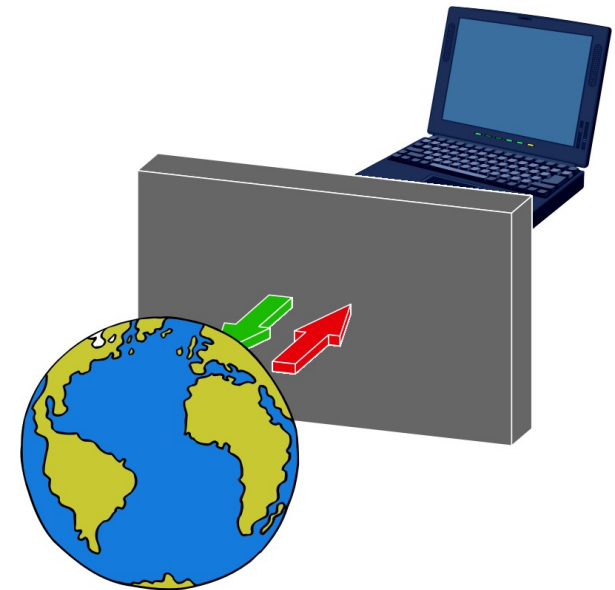


# Schutz durch Hard- und Software

## ■ Eine Hardware Firewall

- funktioniert wie ein **Rückschlagsventil:**

Verbindungsversuche sind nur in einer Richtung möglich, nämlich von innen nach außen



- ist üblicherweise im **DSL-Router** eingebaut, nicht jedoch in einem Telefon / ISDN -Modem

# Schutz durch Hard- und Software

## ■ Schützt mich eine Firewall?

- Bei Infektion via USB hilft die Firewall nicht, weil sie nur die Schwelle zum Internet bewacht, aber nicht den USB-Anschluss.
- Schadsoftware versucht, weitere Funktionen aus dem Internet nachzuladen.
- Dies lässt die Firewall zu, weil die Verbindung von innen heraus erfolgt.



# Schutz durch Hard- und Software

## ■ Schützt mich ein Virens Scanner?

- Gezielte Angriffe auf Unternehmen werden nicht erkannt.
- Neue Schadsoftware wird nur mit einer gewissen Verzögerung erkannt.
- Virens Scanner muss ständig aktualisiert werden.
- Virens Scanner werden von Schadsoftware abgeschaltet.
- Schadsoftware versteckt sich mit einem sogenannten Rootkit.



# Wirksame Abwehr

## ■ Software auf dem neuesten Stand halten!

- Hersteller beseitigen laufend bekannt gewordene Schwachstellen
- Die von Conficker ausgenutzte Autoplay-Schwachstelle wurde 2009 in Windows XP beseitigt.

## ■ Nicht mit Administrator-Rechten arbeiten

- Schadsoftware hat es dann schwerer sich „einzunisten“
- Nicht immer „ja“ klicken!



# Wirksame Abwehr durch Technik?

- **Wie wird die Software immer auf dem neuesten Stand gehalten?**
  - Dokumentation des Software-Einsatzes und daraus abgeleiteter Prozesse
- **Wer braucht Administrator-Rechte?**
  - Regelung von Benutzergruppen und Anwenderprivilegien
- **Dokumentation und die Regelung von Prozessen gehören zur IT-Organisation**



# Der wirksamste Schutz besteht hier darin,

eine Regelung zum Umgang mit USB-Datenträgern zu schaffen, diese allen zu vermitteln und deren Einhaltung durchzusetzen.

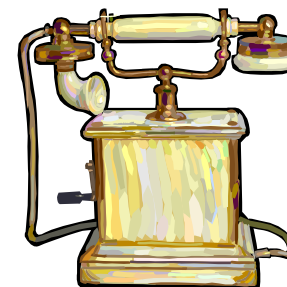


⇒ Ein **wirksamer Schutz** entsteht (auch hier) nur durch das **Operative Sicherheit-Geschäft**

**Chefsache**

# Überprüfung der IT-Dokumentation

- **Ist sie allgemeinverständlich gegliedert?**
  - Management Summary
- **Spiegelt sie die aktuelle Organisationsstruktur des Unternehmens wider?**
  - Lokationen, Abteilungen, Prozesse
- **Spiegelt sie die aktuelle Kommunikationsstruktur des Unternehmens wider?**
  - Medienkanäle, Datenaustausch



# Sicherheitsmaßstab

## ■ Die IT-Dokumentation muss

- eine fachkundige, firmenfremde Person

### **in die Lage versetzen,**

- die wichtigen Daten und Systeme nach einer IT-Katastrophe zu retten
- einen ausgefallenen Administrator zu ersetzen
- sicherheitsrelevante Prozesse und Regelungen nachzuvollziehen



# Überprüfung der IT-Dokumentation

- Gibt es ein **Betriebshandbuch**, in dem festgelegt ist, **was wo wann wie** in der IT passiert?



- Gibt es einen **Notfallplan** für vorhersehbare Katastrophen?



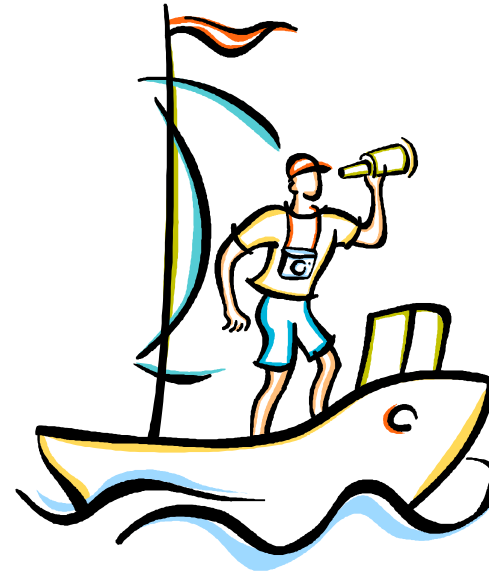
# Überprüfung der Verantwortlichkeiten

- Wer ist bisher verantwortlich für die **Pflege der Dokumentation**?
- Bestehen zwischen internen und externen Verantwortlichen **klar abgegrenzte Verantwortungsbereiche**?
- Wer ist verantwortlich für die **IT-Schulung**?

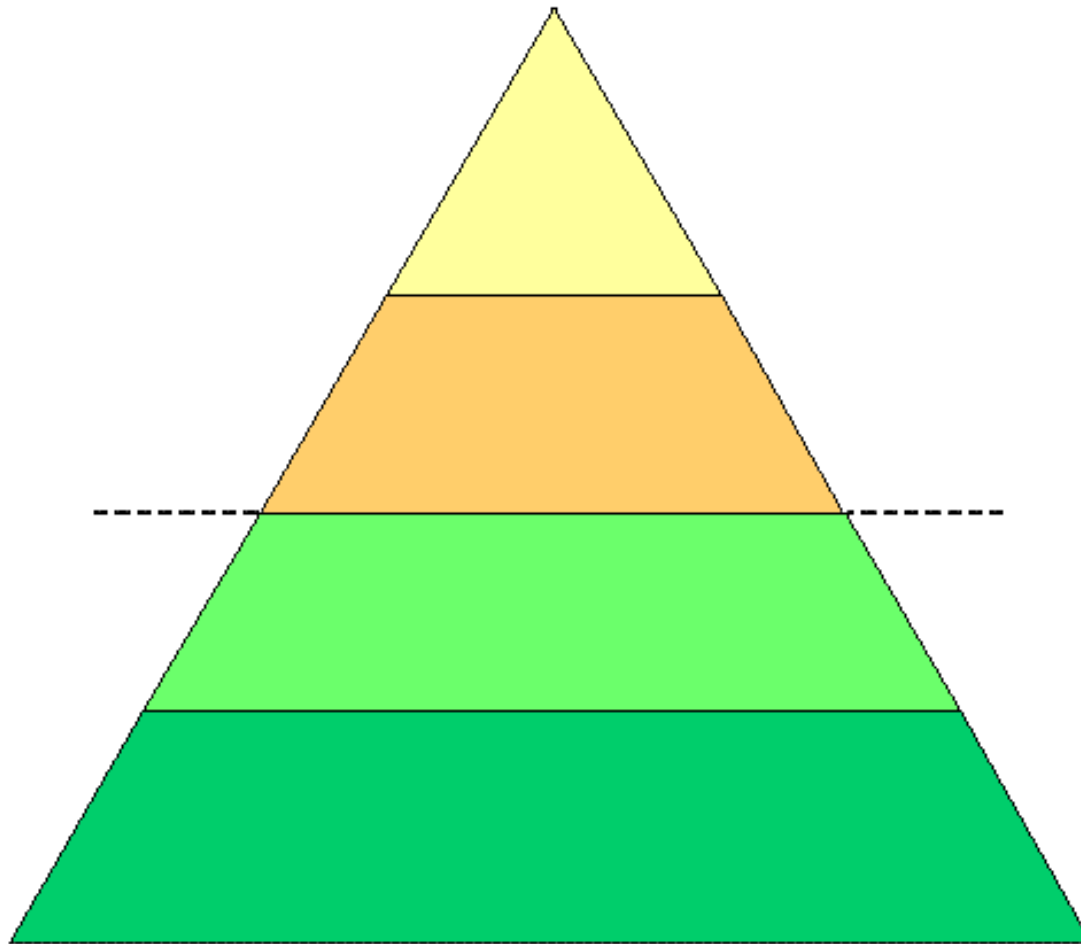


# Der Faktor Mensch

- Welche **Fähigkeiten** und welche **Sensibilität** sollten *Ihre* ideale Mitarbeiter/innen haben, um wirkungsvoll zum Datenschutz beizutragen?



# Entwicklung eines Sicherheitskonzepts



# Entwicklung eines Sicherheitskonzepts

## ■ Beschreibung des Ist-Zustands

- Erfassen der Lücken, Schwachstellen und Risiken

## ■ Formulierung von Zielen

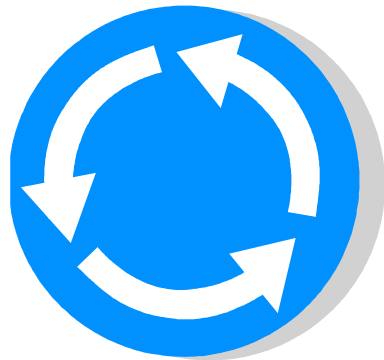
- zur Verbesserung des aktuellen Status

## ■ Konzeption von Massnahmen

- zur schrittweisen Zielerreichung



# Nach dem Spiel ist vor dem Spiel



## ■ Zyklische Prüfung der an die IT-Technik delegierten Aufgaben

- Controlling
- Reviews

## ■ Begleitung der Verantwortlichen durch neutrale Sachverständige

- Begutachtung
- Audit



# Zusammenfassung



# Veranstalter

- **medien forum freiburg**

Fachgruppe IT und Sicherheit

<http://www.mff.net/>

<http://www.fritsi.de/>

# Referenten

- **Hansjörg Pfister**  
**Alcatraz Softwareentwicklung**

<http://www.alcatrazplus.de/>

- **Jürgen Bader**  
**B+R Secure**

<http://www.brsecure.de/>

- **Meinrad Rombach**  
**CALL**

<http://www.lernbegleiter.de/>

- **Ralf Steinemann**  
**iTernity / PYRAMID Computer**

<http://www.iternity.com/>

- **Olav Seyfarth**  
**Datenschutz individuell**

<http://www.datenschutz-individuell.de/>

- **Richard Gertis**  
**VivaSoft**

<http://www.vivasoft.de/>