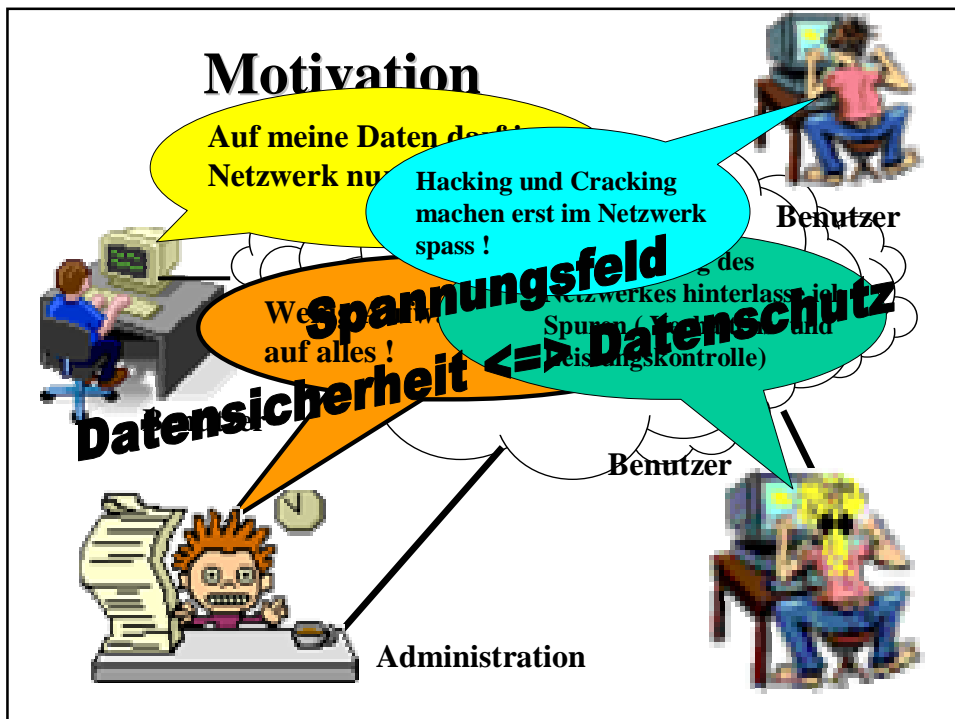


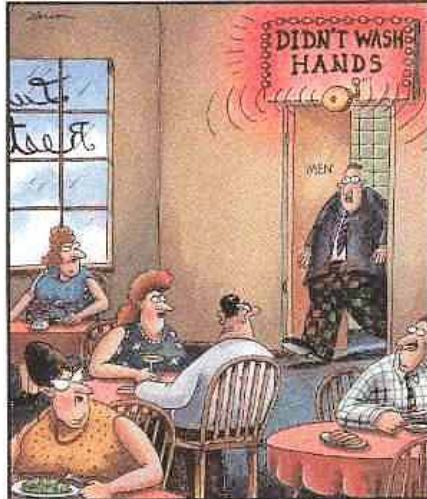
Datenschutz in Rechnernetzen

Regierungsdirektor W. Ernestus
Bundesbeauftragter für den Datenschutz
Referat VI
(Technologischer Datenschutz)



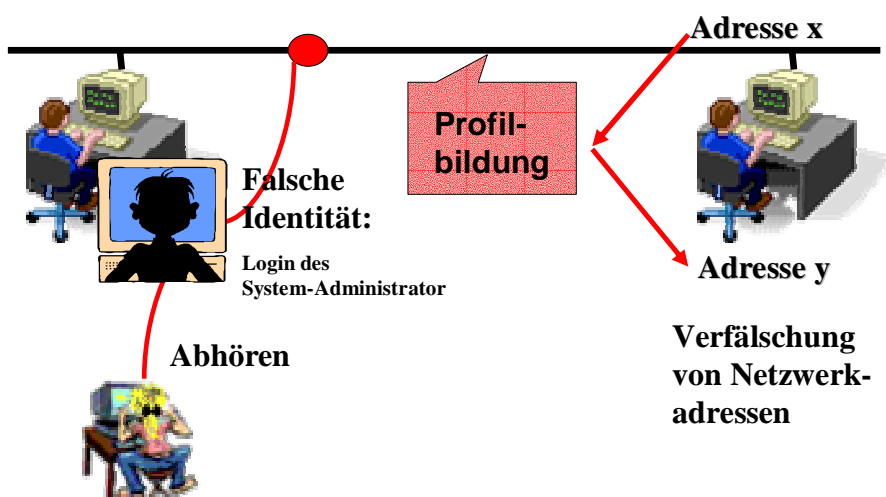
Technisch-organisatorische Maßnahmen

Datei:OMW1.ppt



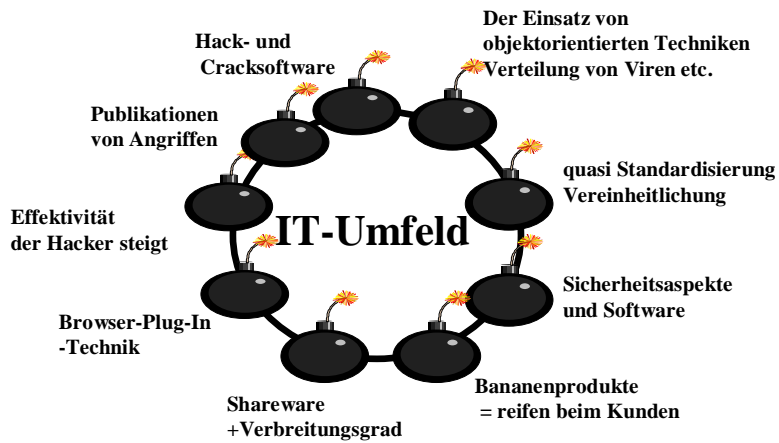
- Grundgedanke des Datenschutzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten **und beim Technikeinsatz** in seinem Persönlichkeitsrecht beeinträchtigt wird.
- Bei allen heute schon möglichen Verarbeitungsvorgängen nimmt nicht nur die Zahl der erfassten und verarbeitenden personenbezogenen Daten zu, die Rückschlüsse auf Personen zulassen, sondern auch deren Sensibilität. Es geht nicht mehr nur um die Tatsache, dass eine sichere Verarbeitung stattfindet, sondern immer öfters auch darum, "was" dabei passiert.

Bedrohungen im Netzwerk



Datei: Netzwerkbedrohungen

Gefahren für den Netzwerk-Arbeitsplatz



Datei: Gefahren-Internet-Arbeitsplatz

Datenarten in Netzen

Benutzer-Stamm-daten



(Benutzername, Funktion, Arbeitsplatz, Berechtigungen etc.)

Inhalts-daten



Wir über uns:
240 Jahre Erfahrung in der Druck-Produktion
 bringen allein CYBER DRIVES 35 Senior Ingenieure die volle Entwicklung unserer Laufwerke für die beste Qualität zu marktgerechten Preisen und klaren Absatzzweigen bestimmen das Firmenprofil der CYBER DRIVE Technology GmbH. In der Rubrik **Vertrieb** finden Sie Informationen über die Vertriebswege und Bezugsquellen von CYBER DRIVE. Unter **Marketing** informieren wir Sie über Anzeigen, Testergebnisse und allgemeine Informationen von CYBER DRIVE.

(Inhalte, Bilder, Töne)

Protokoll-daten

WER ARBEITET, MACHT FEHLER.
VERMEIDE FEHLER!



(Daten über Verhalten, der Mitarbeiter, Administratoren)

Benutzerverhalten

Eventuell bewusste
Falscheingaben machen !!

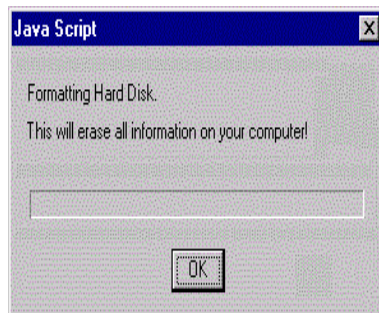
Nur notwendige
Angaben machen !



Alle Eingaben von mir,
können gegen mich und
weiter verwendet werden

Vortäuschen einer
höheren Arbeits-
leistung

Datensicherung



Zulässigkeit/Erforderlichkeit



"Ich habe in deinem Zimmer Zigaretten gefunden ..."

Verpflichtungen verantwortlichen Stellen

Datei: Datensicherung01.ppt

Grundsätze bei der Verarbeitung personenbezogener Daten

Personenbezogene Daten dürfen ohne Einwilligung nur und in dem Umfang erhoben, verarbeitet und genutzt werden, wie dies gesetzlich erlaubt und im Einzelnen erforderlich ist

Dabei sind angemessene technische und organisatorische Maßnahmen zur **Datensicherung** zu treffen



Datei: Grundsaeetze.ppt



§ 9 BDSG nebst Anlage



Datei: Para9BDSG

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die Acht Gebote der Datensicherung



Beispiel: Weitergabekontrolle

Vorschrift:

zu gewährleisten, dass personenbezogene Daten **bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können**, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Kritik:

Hier fordert das BDSG technisch unmögliches ! Bei der elektronischen Übertragung kann zwar die Vertraulichkeit gesichert werden, das kopieren und verändern der Daten nicht !!!

Datei: BeispielZugriffskontrolle

Beispiel: Zugriffskontrolle

Vorschrift:

zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und **nach der Speicherung** nicht unbefugt gelesen, kopiert, verändert oder **entfernt** werden können.



Vorschrift zielt auf die Vertraulichkeit und Integrität !

Aber:
Was bedeutet Daten entfernen?

Begriff **entfernen** ist im BDSG nicht definiert !

Datei: BeispielZugriffskontrolle

Beispiel: Zutrittskontrolle



Vorschrift:

Unbefugten ist der Zutritt zu Datenverarbeitungslagen zu verwehren, wenn dort personenbezogene Daten verarbeitet werden !

Kritik:

Ist die Regelung im Zeitalter des Internets noch durchsetzbar ?
Ist diese Vorschrift in Zeiten der Netzwerktechnik überhaupt durchsetzbar ?

IT-Sicherheit

Datei: IT-Sicherheit

Was bedeutet
IT-Sicherheit ?

IT-Sicherheit ist der
Zustand eines Systems
einer Systemkomponente
oder eines Verfahrens,
der ein vorher bestimmtes
Maß an Vertraulichkeit,
Integrität und Verfügbarkeit
für die Daten garantiert.

Verfügbarkeit

Integrität

Vertraulichkeit

Systeme/Systemkomponenten/Verfahren

Was ist zu tun?

- Es müssen technisch-organisatorische Maßnahmen ergriffen werden zur Gewährleistung der Datensicherheit
- Nützlich ist die Entwicklung eines Datenschutzkonzepts
- Regelmäßig Überprüfung der ergriffenen Maßnahmen
- Überprüfung der Wirksamkeit der ergriffenen Maßnahmen
- Maßnahmen müssen dem Stand der Technik berücksichtigen
- Für den Netzwerkbetrieb ist eine Policy zu entwickeln



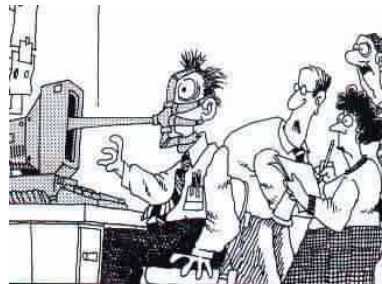
Datensicherung ist die Gesamtheit aller



← **Regelungen und**

Maßnahmen, →

zur Herstellung und Erhaltung der Datensicherheit, die erforderlich sind, um einen wirksamen Datenschutz zu gewährleisten



"ALRIGHT, STEADY EVERYONE. DEBBY, GO OVER TO KEN'S PC AND PRESS 'ESCAPE' VERY CAREFULLY!"

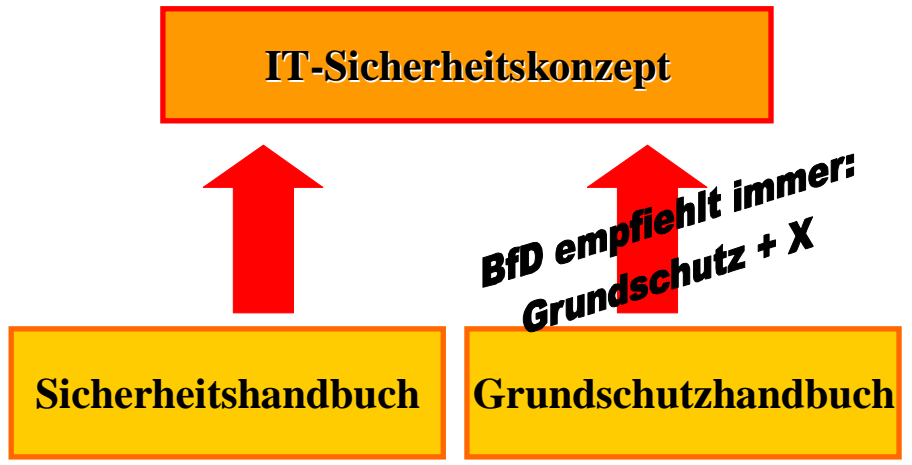
Datei: Datensicherung02

Privacy Policy

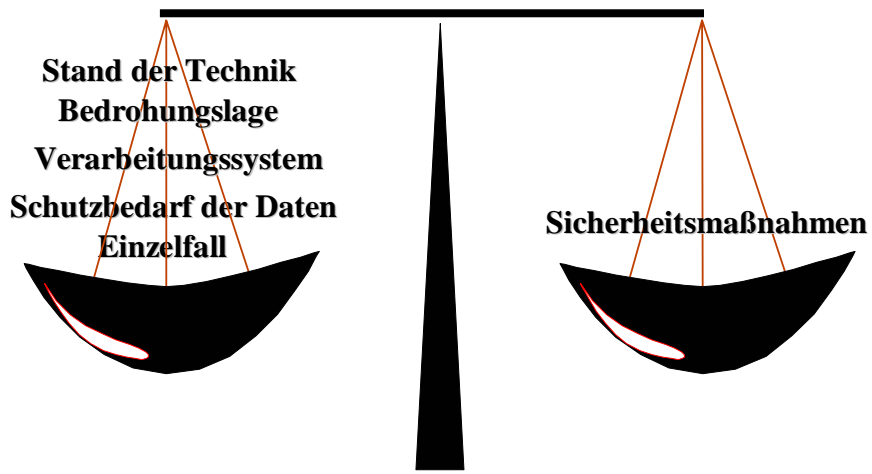


- Welche Daten werden gesammelt?
- Wo werden Daten genutzt?
- Was wird mit Daten gemacht? (Verhaltens- und Leistungskontrolle?)
- Können eigene Daten eingesehen werden? **Vorsicht sehr schwieriges Authentisierungsproblem !!!**
- Versteht der Benutzer (Normalbürger die (Ihre) Privacy Policy?
- Wurde die Policy überprüft?
- Was passiert bei Verstößen?!!

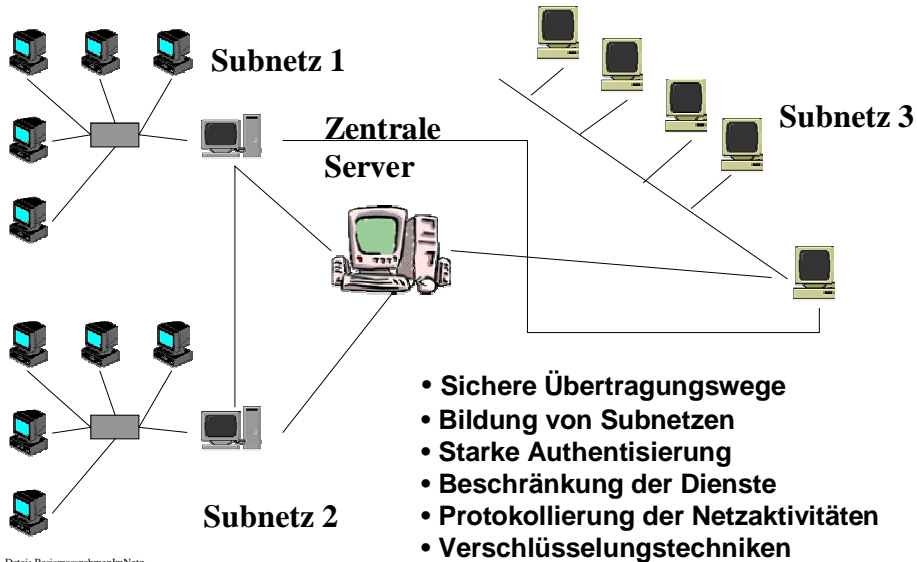
Methoden zur Erstellung eines IT-Sicherheitskonzepts



Abhängigkeiten der Sicherheitsmaßnahmen



Basismaßnahmen in lokalen Netzwerken



Gestaltung von Protokollen!

1. Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?

2. Wer hatte von wann bis wann welche Zugriffsrechte?

Randbedingungen:

- Umfang der Protokolldatei
- geeignete Tools zur Auswertung

Natürlich beachten wir das Datenschutzgesetz und treiben keinen Missbrauch mit Ihren Daten, Sie altes Ferkel, Sie!



Morgens beim System-Admin.

Datei: Gestaltung von protokollen

Aufbewahrungsdauer



- Allg. Löschregeln des BDSG
Löschungspflicht § 20 Abs. 2 BDSG
- Aufbewahrungsdauer richtet sich nach der Wahrscheinlichkeit, daß Unregelmäßigkeiten offenbar werden können
- Erfahrungsmäßig sollte 1 Jahr nicht überschritten werden
- bei gezielten Kontrollen schon früher
- Verwendung von Ringspeichern

Quelle: Aufwaahr

Datenvermeidung und Datensparsamkeit



Nach § 3a BDSG Gestaltung und Auswahl von DV-Systemen an dem Ziel so wenig wie möglich personenbezogene Daten zu erheben, verarbeiten oder zu nutzen

Welche Prüfungsmöglichkeiten gibt es?

- Datenschutzaudit
- Zertifizierung durch das ULD in Kiel
- Quid! GmbH (Ver.di)
- Aber.....

Kiss me...
I'll be your
Queen



(c) WWW.OHMYGOODNESS.COM

Freiwillige Selbstkontrolle !??

Hilfsmittel:

Programme zur
automatisierten Kontrolle
von Sicherheitsein-
stellungen

Beispiele:
USEIT (BSI)



oder für das Internet

<http://sad.inf.fh-rhein-sieg.de/>



Mitbestimmung

Datei: Mitbestimmung01

- Verhaltens- oder Leistungskontrolle mit technischen Einrichtungen -



Mitbestimmungspflicht gemäß §75 Abs. 3 Nr.17 BPersVG oder §87 Abs. Nr.6 BetrVG erstreckt sich auf:
„...die Einführung und Anwendung technischer Einrichtungen, die dazu **bestimmt** sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.....“

Rechte des Betroffenen



- **Auskunft**
- **Berichtigung**
- **Sperrung**
- **Löschung**
- **Schadensersatz**
- **(Anrufung des BfD)**

Datei: Rechte-des- Betr.