Zielkonflikte zwischen Funktionalität, Sicherheit und Datenschutz

econique, Mainz, 13. September 2006

Martin Rost
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein, Germany
(ULD)

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Überblick

- Kurzvorstellung des ULD und ULDi
- Funktionalität, Sicherheit, Datenschutz
- Firewall/Proxy
- Anonymisierung
- Identitätsmanagement, Type 3
- Protokollierung
- Kontakt

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Kurzvorstellung ULD / ULD-i

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

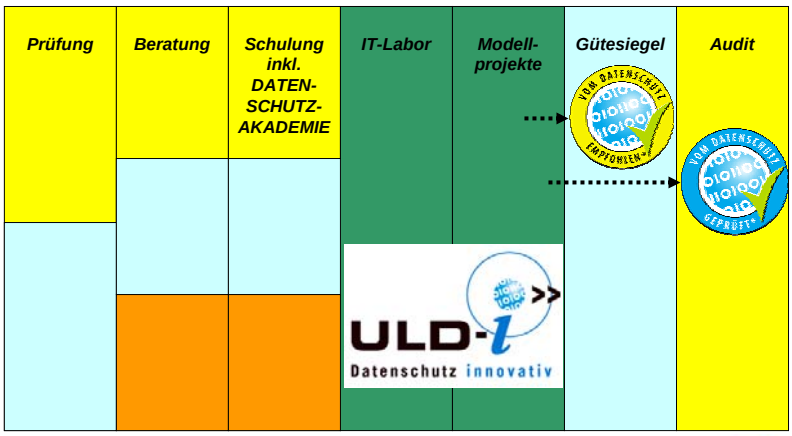
ULD-i
Datenschutz innovativ

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

3 *Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz*

Die 7 Säulen des ULD

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN



UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

4 *Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz*

Projekte im ULD
http://www.uld-i.de/projekte/

- Ubiquitäres Computing – TAUCIS
- Identitätsmanagement - Prime und FIDIS
- Nutzerorientiertes Digital Rights Management - Privacy4DRM
- Datenschutzanforderungen für die Forschung – PRISE
- Europäische Melderegisterauskunft - RISER
- Verbraucherdatenschutz und Datenschutzrecht im Scoring
- Anonymität im Internet - AN.ON

TAUCIS

Identitäts-management

RISER
Registry Information Service on European Residents

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

5 *Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz*

Projekterfahrung des ULD

Seit 1999: ULD-Projekte zu Datenschutz & Datensicherheit

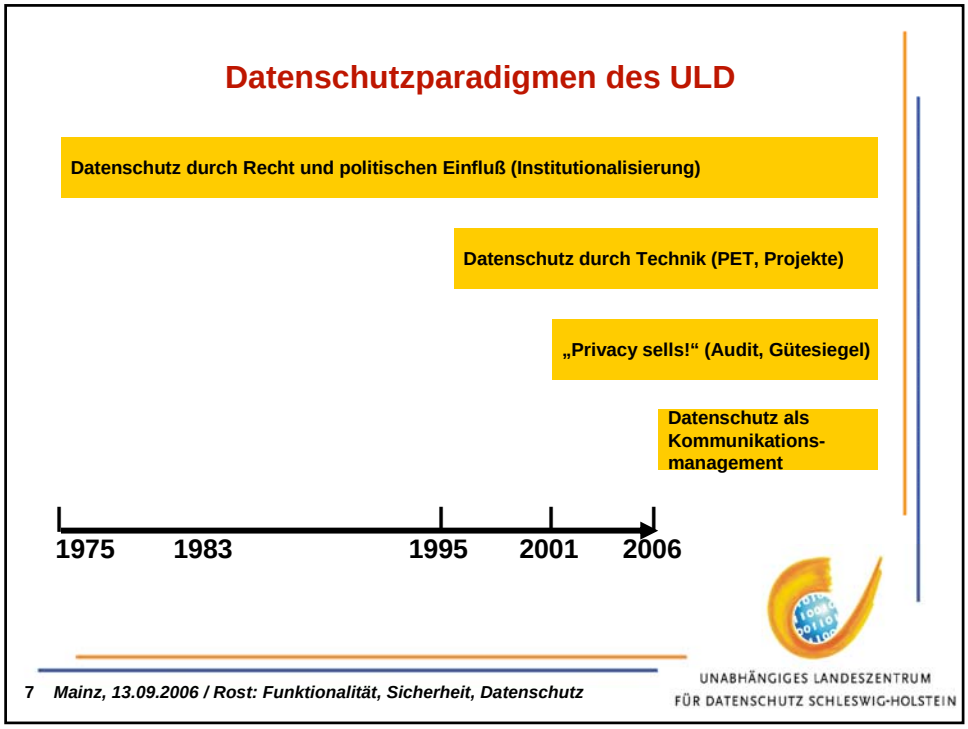
- **Unser Kooperationsnetzwerk – national & international:**

T-Mobile · Microsoft IBM · W3C World Wide Web consortium · Lufthansa Konzerndatenschutz · hp invent · EUROPEAN COMMISSION DIRECTORATE-GENERAL Joint Research Centre · IETF

- **Projektvolumina: 20.000 € – 16 Mio €**
  Partner: 1 – 24

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

6 *Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz*

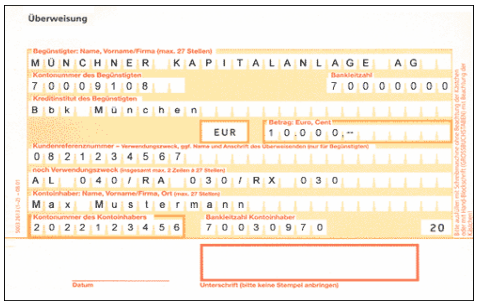

Datenschutzparadigmen des ULD
Datenschutz durch Recht und politischen Einfluß (Institutionalisierung)
Datenschutz durch Technik (PET, Projekte)
„Privacy sells!“ (Audit, Gütesiegel)
Datenschutz als Kommunikations-management
1975
1983
1995
2001
2006
7 Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz
UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN


Funktionalität, Sicherheit, Datenschutz
8 Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz
UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Funktionalitätsanforderung

Anforderung:

Es sollen netzgestützte Transaktionen stattfinden können.
(Recherchen, Bestellungen, Überweisungen, Buchungen, Ummeldungen, Formularausfüllungen, Server- bzw. Systemmanagement, ...)



UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Sicherheitsanforderungen

- **Integrität von Daten**
  - **Daten davor schützen, dass sie unbefugt verändert wurden bzw. werden können.**
    - **Schutz durch Signieren**
- **Vertraulichkeit von Daten**
  - **Keine Einsichtnahme in Daten durch Unbefugte möglich.**
    - **Schutz durch Verschlüsselung**
- **Verfügbarkeit**
  - **Redundanz**
- **Authentizität von Daten**
  - **Daten überprüfen können, ob sie aus der angegebenen Quelle stammen.**
    - **Schutz durch Signieren**
    - **Authorisierung/Zugriffe nach Login/ Passworteingabe**

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

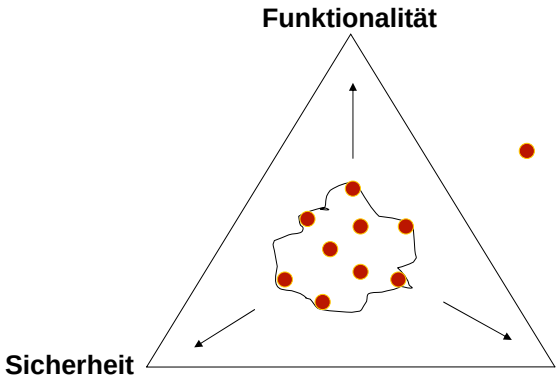
Datenschutzregeln

- **Zweckbindung**
  - Engst möglicher Zuschnitt auf die wesentlichen Daten.
- **Datenminimierung**
  - Bei jedem Einzelschritt weitest möglich auf Daten verzichten/ löschen.
- **Löschung**
  - Einhaltung von Speicher- bzw. Löschfristen
- **Einwilligung**
  - Wenn möglich, Zustimmung der Betroffenen einholen
- **Pseudonymisierung / Anonymisierung**
  - Wenn möglich, so früh wie möglich personenbezogene Daten anonymisieren/ pseudonymisieren.

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

1 *Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz*
1

Datensicherheit ungleich Datenschutz



IT-“Arbeitspunkt“
einer Organisation

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

1 *Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz*
2

3 Beispiele für Zielkonflikte zwischen Funktionalität, Sicherheit und Datenschutz

1 3 *Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz*

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Firewall/Proxy

Vorrang der internen Sicherheitsanforderungen?

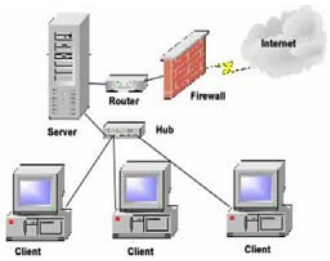
1 4 *Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz*

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Der Firewall/Proxy-Konflikt

Der FW- oder Proxy-Admin kann / muss / will aus Gründen der **sicherheitstechnischen Systemanalyse** in Prinzip jederzeit sämtliche Päckchen einsehen bzw. loggen können, die die FW passieren.

Aus Gründen des innerbetrieblichen **Datenschutzes** soll der Administrator der FW oder des Proxy keinen Zugriff auf E-Mails oder Webabrufe haben. Ihn geht es nichts an, wofür sich einzelne Mitarbeiter, das Management, der Betriebsrat, die Marketing- und Forschungsabteilung interessieren.



UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Lösung des FW-Konflikts

Betriebsvereinbarung schließen, unter welchen Bedingungen an der Firewall oder auf dem Proxyserver geloggt werden darf. Es müssen Aussagen getroffen werden darüber:

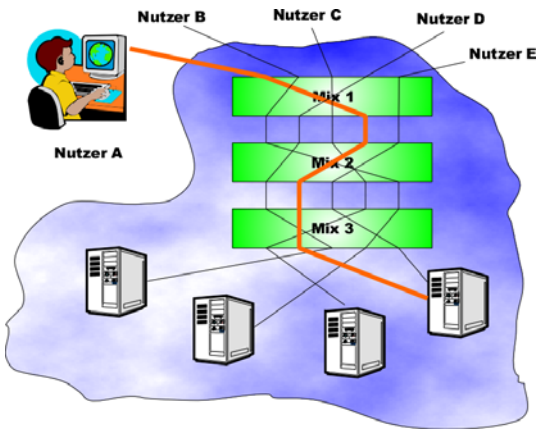
- **zu welchen Anlässen protokolliert werden darf. (Anlaßbezogen oder dauerhaft?)**
- **was protokolliert wird. (Zweckbindung, Datenminimierung, Pseudonymisierung der Daten)**
- **wie der Zugriff auf die Logdaten geregelt ist. (Vier-Augenprinzip, Einbezug von Management, betrieblicher Datenschützer, Betriebsrat, Einwilligung durch den Betroffenen)**
- **dass kommuniziert wird, dass das Mitprotokollieren angeschaltet ist. (organisationsweite Kommunikation)**

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Anonymisierung
Vorrang des Datenschutzes?

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

ANONymisierung,
die auch vor dem Betreiber schützt



http://anon.inf.tu-dresden.de/

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Lösung der Nutzung von Schutzdiensten

Betriebsvereinbarung schließen darüber, unter welchen Bedingungen ein Schutzdienst - wie Anonymisierung oder rechner-/personenbezogene Verschlüsselung (bspw. Abruf von per https geschützten Mails) - nicht genutzt werden darf.

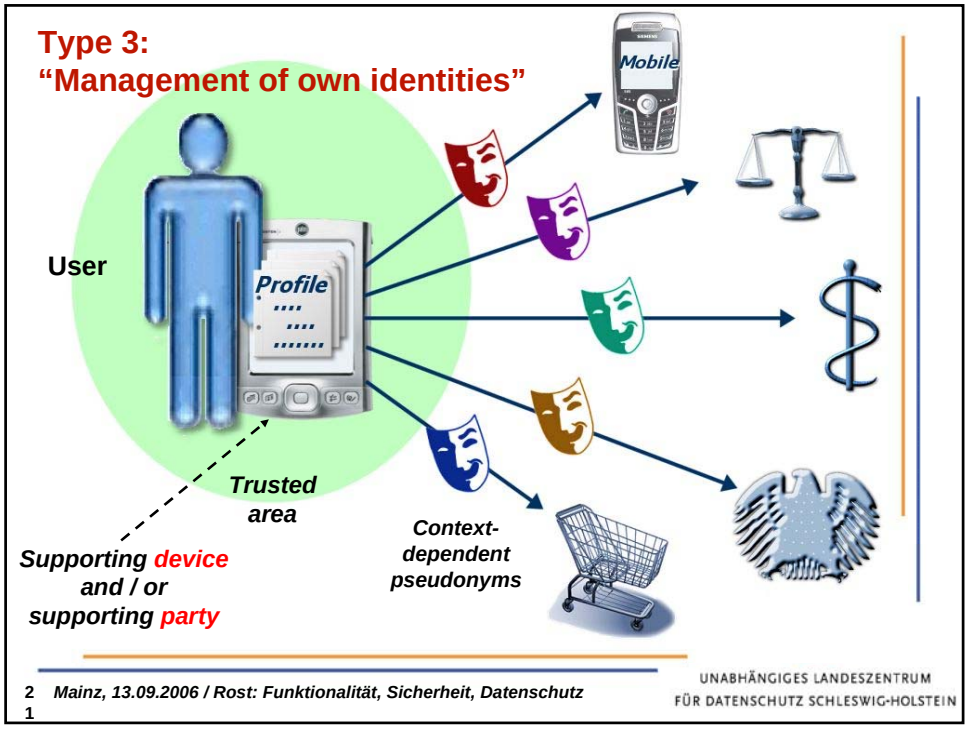
Kommunikation, dass ein bestimmter Dienst am Port der Firewall unter Angabe eines Grunds gesperrt ist und wann mit der Aufhebung zu rechnen ist.

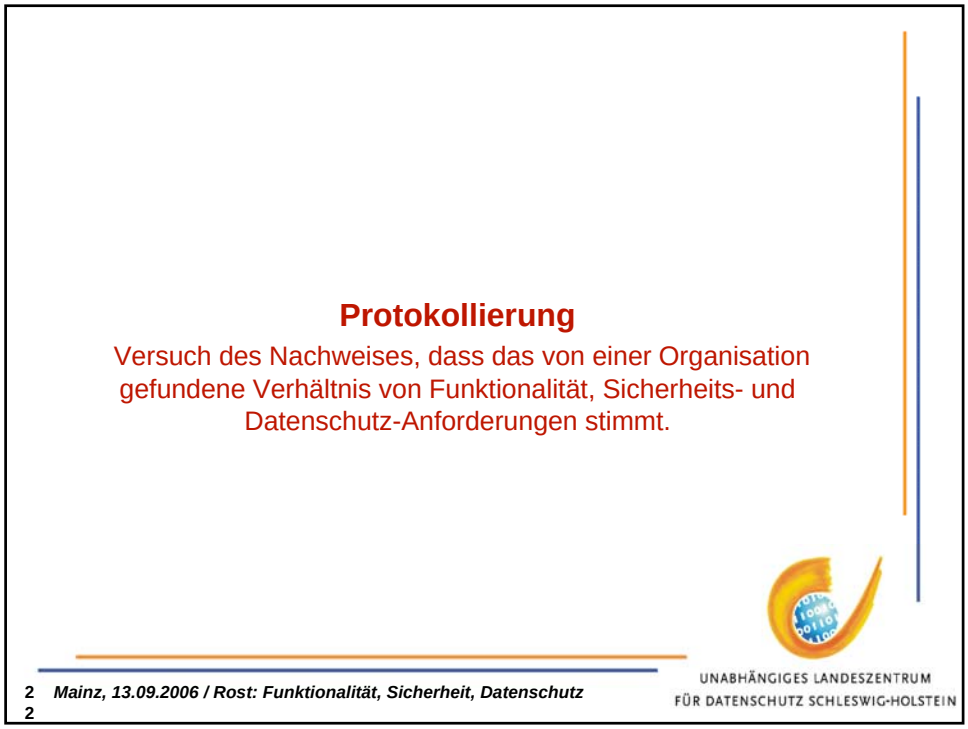
UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Identitätsmanagement

Nichtverkettbarkeit durch Pseudonymverwaltung

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN


Type 3:
"Management of own identities"
Mobile
User
Profile
Trusted area
Supporting device and / or supporting party
Context-dependent pseudonyms
2 Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz
1
UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

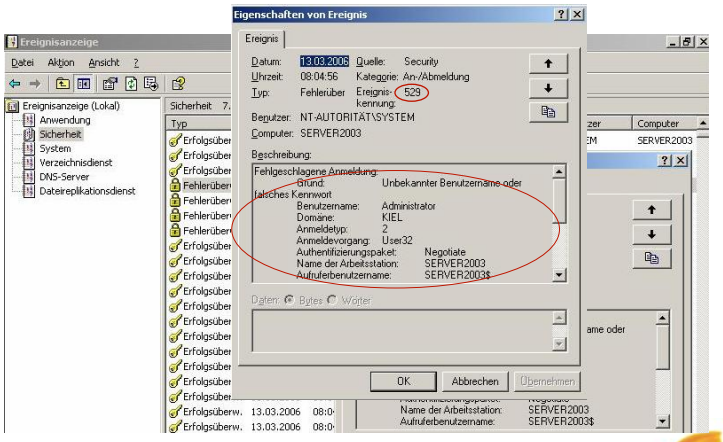

Protokollierung
Versuch des Nachweises, dass das von einer Organisation gefundene Verhältnis von Funktionalität, Sicherheits- und Datenschutz-Anforderungen stimmt.
2 Mainz, 13.09.2006 / Rost: Funktionalität, Sicherheit, Datenschutz
2
UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Das Protokollierungsproblem

- Automatisierte Protokoll/Logdaten sind leicht, in der gegenwärtigen Praxis allerdings unkontrollierbar ohne Zweckbindung und Datensparsamkeit, herausgeschrieben. Und genau so einfach sind sie **unterdrück-, manipulier- oder löschbar**.
- Administratorentätigkeiten sind auf Standardbetriebssystemen **nicht beweisfest** protokollierbar.
- Die **Kontrolle von Protokollen** geschieht ungeregelt und findet in der Praxis – insbesondere auch in Bezug auf Nachweisbarkeit, dass die Auftragsdaten-verarbeitung bzw. das Outsourcing korrekt erfolgt, praktisch nicht statt.

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Protokollierungspraxis unter Windows2003



http://www.datenschutzzentrum.de/sommerakademie/2006/somak06_infb07_rost.pdf

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Kontakt

Martin Rost
Mail: LD32@datenschutzzentrum.de
Tel: 0431 988 1391

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein,
24103 Kiel, Holstenstraße 98
Mail: mail@datenschutzzentrum.de
Tel: 0431 988 1200
Fax: 0431 988 1223
Web: www.datenschutzzentrum.de

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN