IT-Sicherheit in Meta Directories

Vortrag beim ZKI „AK Verzeichnisdienste“
15/16. Dez. 2004 in Ilmenau

Servicezentrum für
Computersysteme und
Computer-kommunikation

Übersicht

- Definitionen
- Missbrauchspotential/Schaden
- Grundsätze der UNO
- Ziele
- Maßnahmen
- Probleme
- Goldene Regeln
- Experten meinen...
- Schlussfolgerungen

Definition 1: Meta Directory

- Das Meta Directory (MD) befasst sich mit automatisierten Verwaltungsabläufen personen-bezogener Daten einer Identität, welche in den Geschäftsprozessen der Einrichtungen notwendig sind.

- Dabei bilden Provisionierung, SB Funktionalität, Aktualität und Verfügbarkeit der entsprechenden Datensätze die Kerneigenschaften des Meta Directory.

Definition 2: Identitätsmanagement

- Das Identitätsmanagement ist aus Sicht des Nutzers eine Verwaltung seiner virtuellen/digitalen Identitäten im privaten und geschäftlichem Umfeld.

- Dabei steht die Anonymisierung und Sicherheit der Kommunikation im Vordergrund.

Definition 3: IT-Sicherheit

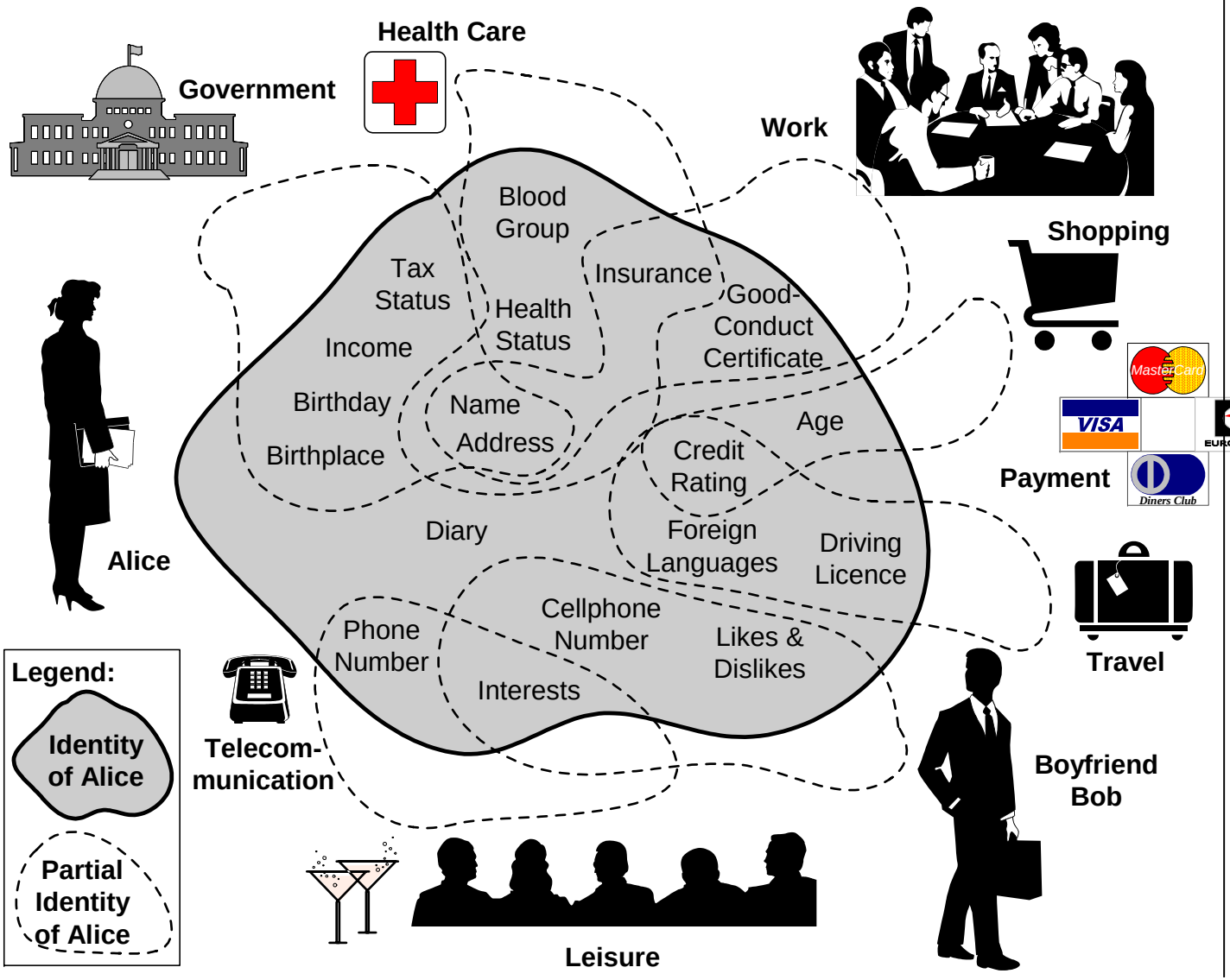
- IT-Sicherheit ist kein Status sondern der Prozess die Grundwerte der Sicherheit auf IT-Systeme und die von ihnen verwalteten Daten anzuwenden.

- Unter Sicherheit eines IT-Systems versteht man eine Eigenschaft eines IT-Systems, bei der Maßnahmen gegen die im jeweiligen Einsatzumfeld als bedeutsam angesehenen Bedrohungen der Integrität, der Verfügbarkeit und der Vertraulichkeit in dem Maße wirksam sind, dass die verbleibenden Risken tragbar sind.

Definitionen: Zusammenfassung

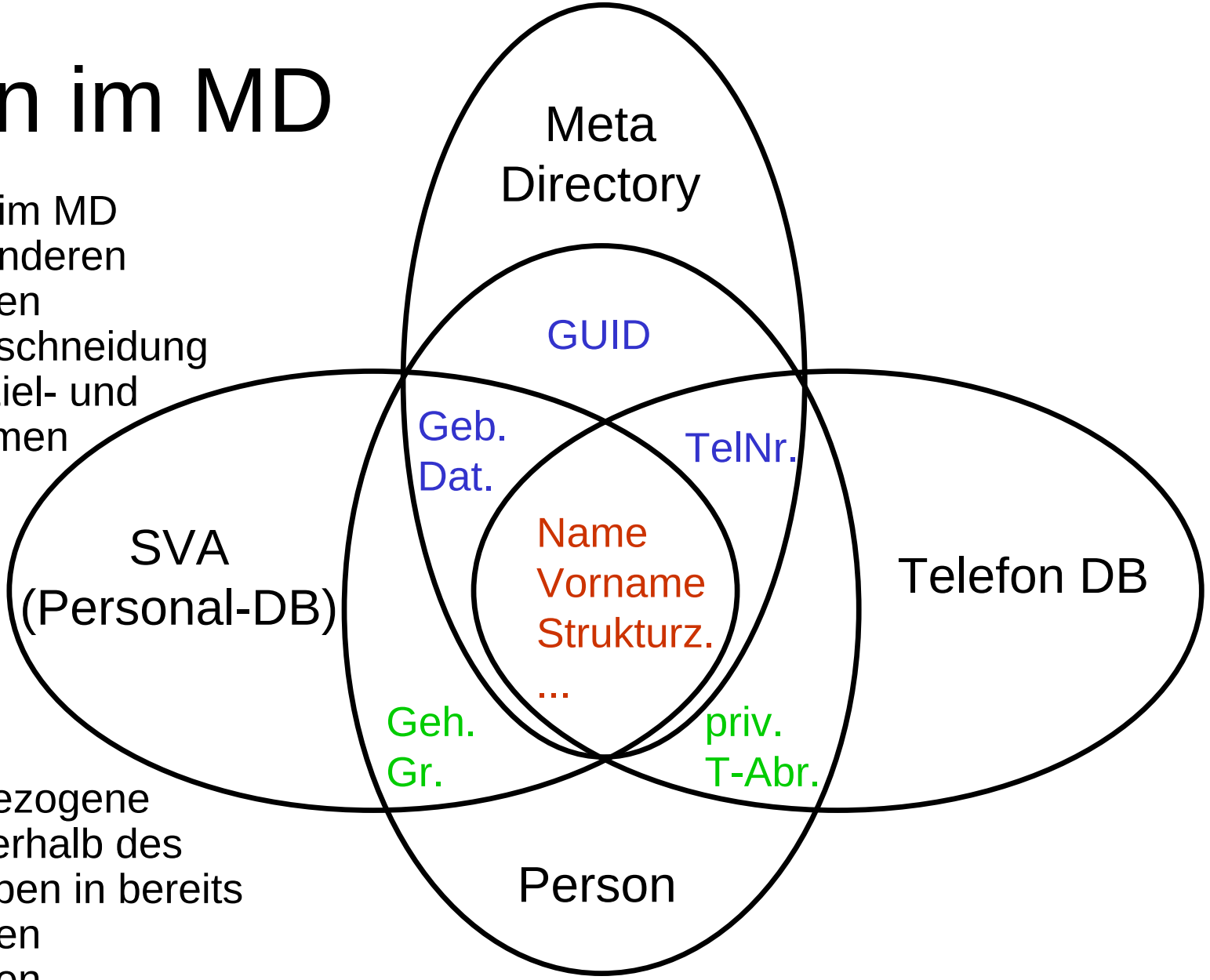
- MD:
  - Verwaltung statischer personenbezogener Daten aus Sicht der Einrichtung.
- IDM:
  - Schutz der persönlichen Daten (digitale Identitäten) aus Sicht der Nutzer.
- IT-Sec:
  - IT-Sicherheit ist erreicht, wenn die IT-Systeme so reagieren, wie man es von ihnen erwartet.

Blick auf die Daten - IDM



Daten im MD

- Alle Daten im MD stehen in anderen Datenbanken
- keine Überschneidung zwischen Ziel- und Quellsystemen ohne MD



- personenbezogene Daten außerhalb des MD verbleiben in bereits existierenden Datenbanken

Missbrauchspotential und Schaden

- Identitätsmissbrauch
  - Authorisierung gebunden an Identität?
- rechtliche Verstöße (gegen Datenschutz)
  - führen zu Regressforderungen
- Störung der Prozesse
  - z.B. durch Sabotage: mit oder ohne vorhandene Berechtigung im System → Verwundbarkeit der DV Prozesse einer Hochschule
- Imageschaden in der Öffentlichkeit
  - entsteht durch nicht sachliche Diskussion

Ursachen der Schäden

- Fehler der eigenen Mitarbeiter
- Mängel in der Projektplanung und/oder Organisation
- Fehler bei der Implementierung oder den verwendeten Produkten
- Lücken im Sicherheitskonzept

Grundsätze der UNO

- Grundsatz der Rechtmäßigkeit und der Ehrlichkeit
- Grundsatz der Richtigkeit
- Grundsatz der Zweckbestimmung
- Grundsatz der Möglichkeit des Betroffenen zur Einsichtnahme
- Grundsatz der Nichtdiskriminierung
- Grundsatz der Sicherheit
- Ausnahmebefugnisse, Überwachung / Sanktionen, Grenzüberschreitender Datenverkehr, Geltungsbereich

Grundsatz der Sicherheit

Zitat: *"Geeignete Maßnahmen sollten ergriffen werden, um die Dateien sowohl gegen Naturgefahren, wie zufälligen Verlust oder Zerstörung, als auch gegen Gefahren durch menschliche Einwirkungen, wie unerlaubten Zugang oder vorsätzlichen Missbrauch von Daten, zu schützen."*

Ziele

- Schutz der Grundwerte
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- Einhaltung der gesetzliche Regelungen
- Zusammenfassung:

  Unterschiede MD - IDM – VD

Ziele: Schutz der Grundwerte

- Vertraulichkeit (confidentiality, privacy) kennzeichnet einen Zustand von Daten, in dem eine Informationsgewinnung aus sensiblen Daten nur berechtigten Personen und den für sie agierenden informationstechnischen Prozessen möglich ist.

Ziele: Schutz der Grundwerte

- Integrität (integrity) kennzeichnet einen Zustand von Daten, in dem die Korrektheit (Unversehrtheit) der Daten selbst und die korrekte Funktionsweise von Systemen sichergestellt sind.

Ziele: Schutz der Grundwerte

- Verfügbarkeit (availability) kennzeichnet einen Zustand von Daten, in welchem sie durch berechtigte Personen (eingeschlossen den für sie tätigen informations-technischen Prozessen) zum geforderten Zeitpunkt nutzbar sind.

Ziele: Einhaltung der gesetzliche Regelungen

- Richtlinie der vereinten Nationen
- Konvention des Europarats
- Datenschutzgesetze des Bundes
- Datenschutzgesetze der Länder
- Teledienstedatenschutzgesetz
- Mediendienste-Staatsvertrag
- Signaturgesetz
- ...

Ziele – Unterscheidung MD/IDM/VD

- Welches Risiko besteht für die verarbeiteten Daten: statisch/dynamisch/personenbezogen
  - z.B.: Schlüsselmanagement - Datendosen – Accounts – Name/Adresse/Telefonnummer
- MD: Verwaltung der Personendaten der Angehörigen der Institution
- IDM: Bündelung der verschiedenen (anonymen) Identitäten
- VD: verschiedene sächliche Ressourcen - Accounts

Maßnahmen

- **technisch:** Authentisierung, Authorisierung, Protokollierung, sichere Datenübertragung

- **organisatorisch:** Sicherheitsordnung und Sicherheitskonzept, Verantwortlichkeit, informationelle Selbstbestimmung, Beteiligung des Datenschutzes und der Personalvertretungen

technische Maßnahmen

- Authentisierung
  - Einsatz von Smartcards oder -token
- Authorisierung
  - rollenbasierte Rechtemanagement
- Protokollierung
  - Logfiles, Transskripts, Histories...
- sichere Datenübertragung
  - SSL-Datenverschlüsselung
  - Firewall / Portfilter

organisatorische Maßnahmen

- IT-Sicherheitsordnung (Guideline)
  - Zielsetzung, Organisationsform, Verantwortung
- IT-Sicherheitskonzept (Standards)
  - Definition der Sicherheitstechnologien und Prozesse zur Erzielung der Vorgaben
- informationelle Selbstbestimmung
  - Einsicht und ggf. Steuerung des Verbreitungsgrads
- Beteiligung des Datenschutzes
  - Mitsprache bei Definition des erforderlichen Sicherheitsniveaus
- Beteiligung der Personalvertretungen
  - Mitsprache bei Gestaltung der Arbeitsprozesse

Maßnahmen zum Schutz der Vertraulichkeit

- Nur authorisierte Personen und Prozesse haben Zugriff auf definierte Teile der Daten
- Feststellung Identität → Authentifizierung
- Zweckbindung einhalten
- Definition des Datenflusses
- Die administrativen Vorgänge dokumentieren und beschränken
- Schutz der Logfiles und Teilinformationen
- Schutz und Trennung von Test- und Entwicklungs- vom Produktivsystem

Maßnahmen zum Schutz der Integrität

- Schutz vor Manipulation → Prüfsummen
- Funktionsfähigkeit durch Qualitätssicherungsmaßnahmen
- Fehlertoleranz
- Logging
- Zugang zu den Systemen definieren
- Berechtigungsmanagement: Lese- und Schreibberechtigungen
- MD: Nur eine Identität pro Person !

Maßnahmen zum Schutz der Verfügbarkeit

- Synchron (online) – Asynchron (offline)
- Bewertung der Zeitskala: Wie lange sind Daten verfügbar? → gesetzliche Regelungen → Interaktion mit Grundwert Integrität (Richtigkeit)
- Tests zum Nachweis der Verfügbarkeit
- Testkonzept mit Planung und Durchführung

Probleme

- Einbettung in schon existierende, heterogene IT-Strukturen
- Selten existieren bereits umfassende IT-Sicherheitsordnungen/-leitlinien oder -konzepte/-standards
- Unklare Bewertung des Risikos
- Probleme sind i.d.R. nicht neu: d.h. sie sind menschlicher und/oder organisatorischer Art
  → technische Probleme sind selten!

Goldene Regeln

... zum Umgang mit personenbezogenen Daten:

- Einhaltung der Zweckbestimmung
- Speichern und kommunizieren der notwendigen Daten
- Schutz der Persönlichkeitsrechte und die Privatsphäre von Personen
- Sicherung von Aktualität und Richtigkeit
- Gewährung der Einsichtnahme
- Einhaltung der Sicherheitsvorschriften im Umgang mit den Daten
- nachvollziehbare Prozesse erhöhen die Transparenz

Experten meinen...

in einer Studie des unabhängigen Landeszentrum für Datenschutz (ULD) Schleswig-Holstein (Sep. 03):

*"Thereby experts expect complicated usability of Identity Management Applications, an **inadequate level of computer security and privacy**, and also lengthy standardisation processes as main bottlenecks for developing a society-wide Identity Management System."*

Schlussfolgerungen

- technische und organisatorische Maßnahmen aus dem IT Umfeld greifen auch bei MD
- klare Verantwortung und Kommunikation erleichtert das Geschäft
- Lösungen von der Stange gibt es nicht – die jeweilige Situation vor Ort ist entscheidend
- Beteiligung von IT-Sicherheitsbeauftragten, Datenschutz und Personalrat ist unerlässlich bei der Einführung und dem Betrieb von MD

Kommentare - Fragen ?

Markus.von.der.Heyde@scc.uni-weimar.de