TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Der Datenschutzbeauftragte

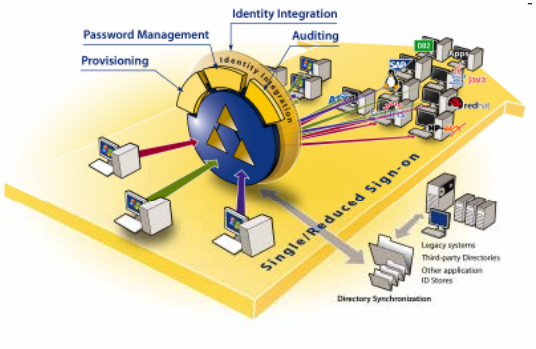
Verarbeitung personenbezogener Daten bei Errichtung und Betrieb von Verzeichnisdiensten

Matthias Herber – Datenschutzbeauftragter der TU Dresden

Kontakt: datenschutz@tu-dresden.de

Zentren für Kommunikation und Informationsverarbeitung e.V.

AK Verzeichnisdienste Duisburg, 04/05 Oktober 2010



Identity Management / ‚intelligente' Verzeichnisdienste

personenbezogene Daten ?

- benötigen personenbezogene Daten !
- ermöglichen Aufzeichnungen zum Nutzerverhalten !
- erleichtern die Verknüpfung von persönlichen Daten mit denen, die bei der Tätigkeit anfallen !

Da stellt sich die Frage:

Welche datenschutzrechtlichen Anforderungen sind an ein solches System zu stellen ?

KEINE VERARBEITUNG PERSONENBEZOGENER DATEN OHNE RECHTSGRUNDLAGE !

Die Verarbeitung personenbezogener Daten ist nur zulässig wenn,

ein Gesetz oder eine andere Rechtsvorschrift sie erlaubt

oder

die Verarbeitung dieser Daten zur Erfüllung der (vom Gesetzgeber der öffentlichen Stelle übertragenen) Aufgaben erforderlich ist und der Betroffene eingewilligt hat.

Telemediengesetz (TMG) ?????

§ 1 Anwendungsbereich

(1) Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste… . Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

Telemediengesetz (TMG)

§ 12 Grundsätze
(1)…nur erheben und verwenden …. eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt ….

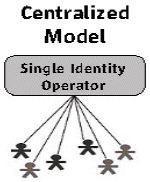
(2) … für andere Zwecke nur verwenden…. oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt ….

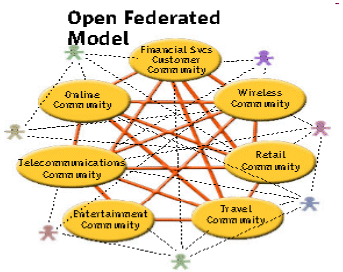
↓

Rahmenordnung für die Rechen- und Kommunikationstechnik und die Informationssicherheit an der TU Dresden / Beschluss des Senates vom 10. 12. 2008

↓

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

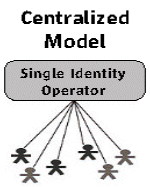


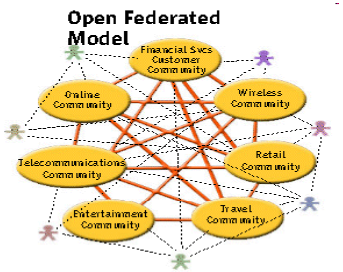


Identity Management / ‚intelligente' Verzeichnisdienste

Anforderungen

- Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten
- Erforderlichkeit
- Zweckbindung
- Datenvermeidung und Datensparsamkeit
- Datensicherheit
- Richtigkeit der Daten
- Verhältnismäßigkeit
- Transparenz
- Garantie der individuellen Mitsprache und des Zugriffsrechts für die betroffenen Personen
- Haftung
- unabhängige Überwachung und gesetzliche Sanktionsmöglichkeiten
- angemessenes Schutzniveau





Identity Management / ‚intelligente' Verzeichnisdienste

Schutzziele

Vertraulichkeit - nur Befugte personenbezogene Daten zur Kenntnis nehmen können,

Integrität - personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben,

Verfügbarkeit - personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können,

Authentizität - jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können,

Revisionsfähigkeit - festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat,

Transparenz - die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

Präambel

§ 1 Geltungsbereich und Zweck

§ 2 Begriffsbestimmungen

§ 3 Verantwortlichkeiten

§ 4 Verarbeitung personenbezogener Daten

§ 5 Zugriffsrechte

§ 6 Technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit

§ 7 Schlussbestimmungen und Übergangsvorschriften

§ 8 Veröffentlichung, Inkrafttreten

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

Präambel

Die TU Dresden strebt eine Integration ihrer komplexen und heterogenen IT-Systemlandschaft zu einer nahtlosen und redundanzfreien Umgebung im Sinne zentraler Dienste an. Zur effektiven und sicheren Nutzung zentraler Dienste ist ein einheitliches Identitätsmanagement, im folgenden IDM genannt, notwendig. Die zentrale Verwaltung der Benutzerdaten entlastet die einzelnen Dienstbetreiber von aufwendigen Routinearbeiten und erhöht das allgemeine Sicherheitsniveau durch die Möglichkeit, den Benutzern die Berechtigungen und Ressourcen automatisch zuzuweisen bzw. zu entziehen.

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

§ 1
Geltungsbereich und Zweck

Das IDM umfasst den Geltungsbereich …... Für andere …..sind mit den jeweiligen Einrichtungen gesonderte Vereinbarungen notwendig.

Die Errichtung und der Betrieb eines IDM ist ausschließlich zum Zweck der zentralen Verwaltung von Benutzerdaten für die Authentifizierung, Provisionierung und Autorisierung …. zugelassen.

Die Nutzung zu Zwecken der Personalverwaltung oder ähnlicher Aufgaben der Technischen Universität Dresden sowie zur Leistungs- und Verhaltensfeststellung und Bewertung der Mitarbeiter und Studenten ist unzulässig.

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

§ 2
Begriffsbestimmungen

Provisionierung im Sinne dieser Ordnung ist die Bereitstellung von Zugriffsrechten auf Dienste und Daten, die ein Benutzer im Rahmen seiner Tätigkeit benötigt.

Autorisierung im Sinne dieser Ordnung ist die Überprüfung von Zugriffsrechten auf Dienste und Daten.

Konsolidierung im Sinne dieser Ordnung ist die eindeutige und quellsystemübergreifende Feststellung der Identität eines Benutzers.

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

§ 3
Verantwortlichkeiten

Für den Betrieb des IDM ist das Zentrum für Informationsdienste und Hochleistungsrechnen (ZIH) der TU Dresden verantwortlich.

Für die Zulässigkeit der Errichtung und des Betriebes der zutreffenden Import- und Exportschnittstellen ist die jeweilige datenverarbeitende Stelle verantwortlich. Für den Betrieb der Import- und Exportschnittstellen ist das ZIH zuständig.

Vorrausetzung für die Zulässigkeit einer Übermittlung von personenbezogenen Daten von einem Quellsystem an das IDM sowie vom IDM an ein Zielsystem ist ein Eintrag des Quell- bzw. Zielsystems in das Verfahrensverzeichnis ...sowie der Nachweis ...der getroffenen Maßnahmen nach § 9 Abs. 2 Nr. 1 bis Nr. 6 SächsDSG.

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

§ 4
Verarbeitung personenbezogener Daten

Im IDM erfolgt die Verarbeitung personenbezogener Daten für die geschlossene Benutzergruppe ... Eine fortzuschreibende Übersicht der Art und des Umfangs der im IDM verarbeiteten Daten ist ... dokumentiert.

Die Verarbeitung personenbezogener Daten erfolgt im IDM ausschließlich zu den in § 1 dieser Ordnung genannten Zwecken.

Die im IDM gespeicherten Daten dürfen nur an Zielsysteme übermittelt werden, sofern die Übermittlung zum ordnungsgemäßen Betrieb des Zielsystems erforderlich ist und dem in § 1 dieser Ordnung genannten Zweck dient.

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

§ 4
Verarbeitung personenbezogener Daten

Beim Ausscheiden eines Benutzers aus der geschlossenen Benutzergruppe gemäß § 1 Abs. 3 IuK-Rahmenordnung wird die zentrale Benutzerkennung des Benutzers gesperrt. Die Löschung der Benutzerdaten erfolgt automatisiert nach Ablauf von 12 Kalendermonaten nach der Sperrung der zentralen Benutzerkennung.

Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der TU Dresden

§ 5
Zugriffsrechte

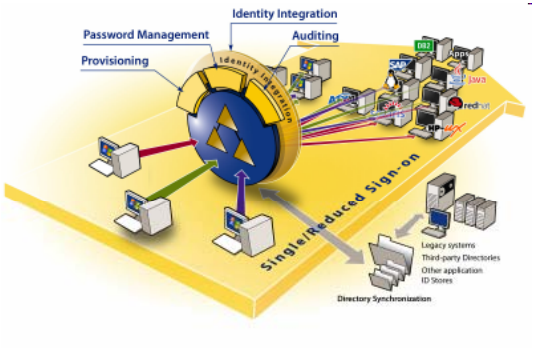
Grundlage für die Vergabe der Zugriffsberechtigungen im IDM ist ein mehrstufiges Rechtekonzept.

1. IDM-Benutzer haben Zugriff auf die über ihre Person verarbeiteten Daten
2. Zielsystem-Administratoren haben Zugriff auf die Daten der für ihren Dienst provisionierten IDM-Benutzer
3. IDM-Administratoren haben Zugriff auf die Daten aller IDM-Benutzer

Eine fortzuschreibende Übersicht der Zugriffsberechtigungen auf das IDM ist Bestandteil des Sicherheitskonzepts gemäß § 6 dieser Ordnung.

§ 6
Technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit

Maßnahmen nach § 9 Abs. 2 Nr. 1 bis 6 SächsDSG, sind im IT-Sicherheitskonzept (Anlage zur Ordnung!) beschrieben.



Was steht noch aus ?

technisch

- Schutzbedarfsfeststellung Risikoanalyse
- Sicherheits- & Rechtekonzept
- Umsetzung und Kontrolle

organisatorisch

- Verfahrensverzeichnis
- Mitbestimmung PRat ! / StuRA ?
- Senats bzw. Rektoratsbeschluss

Literatur zum Thema ?

Halbherzige Benutzerverwaltung
Klaus Scherrbacher / 20.07.2010
http://www.computerwoche.de/2349277

Datenschutzaspekte von Identitätsmanagementsystemen
Recht und Praxis in Europa / Marit Hansen, Henry Krasemann, Martin Rost, Riccardo Genghini
DuD • Datenschutz und Datensicherheit 27 (2003)

Selbstgesteuertes Identitätsmanagement
Rechtliche Möglichkeiten der Nutzung verschiedener Identitäten /Henry Krasemann
DuD • Datenschutz und Datensicherheit 30 (2006)

Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
Thema Identitätsmanagement
https://www.datenschutzzentrum.de/projekte/idmanage/uld.htm
Identity Management Systems (IMS): Identification and Comparison Study
https://www.datenschutzzentrum.de/projekte/idmanage/study.htm

Vielen Dank für Ihre Aufmerksamkeit !