Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Enterprise Identity and Access Management (EIAM)

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

EIAM
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Definitionen
- Notwendigkeit
- Key Concepts
- IAMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

- **Ziele und Ergebnisse der Vorlesung**
- Definitionen
- Notwendigkeit
- Key Concepts
- IAMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Ziele und Ergebnisse der Vorlesung → EIAM

- Gutes Verständnis für die verschiedenen **Ebenen (Module)** eines „Enterprise Identity and Access Management System“
- Erlangen der Kenntnisse über die **Aufgaben**, **Prinzipien** und **Mechanismen** eines „Identity and Access Management System“
- Nachvollziehbarkeit von „Identity and Access Management“ **Prozessen** und **Workflows** anhand von praxisnahmen Beispielen erlernen

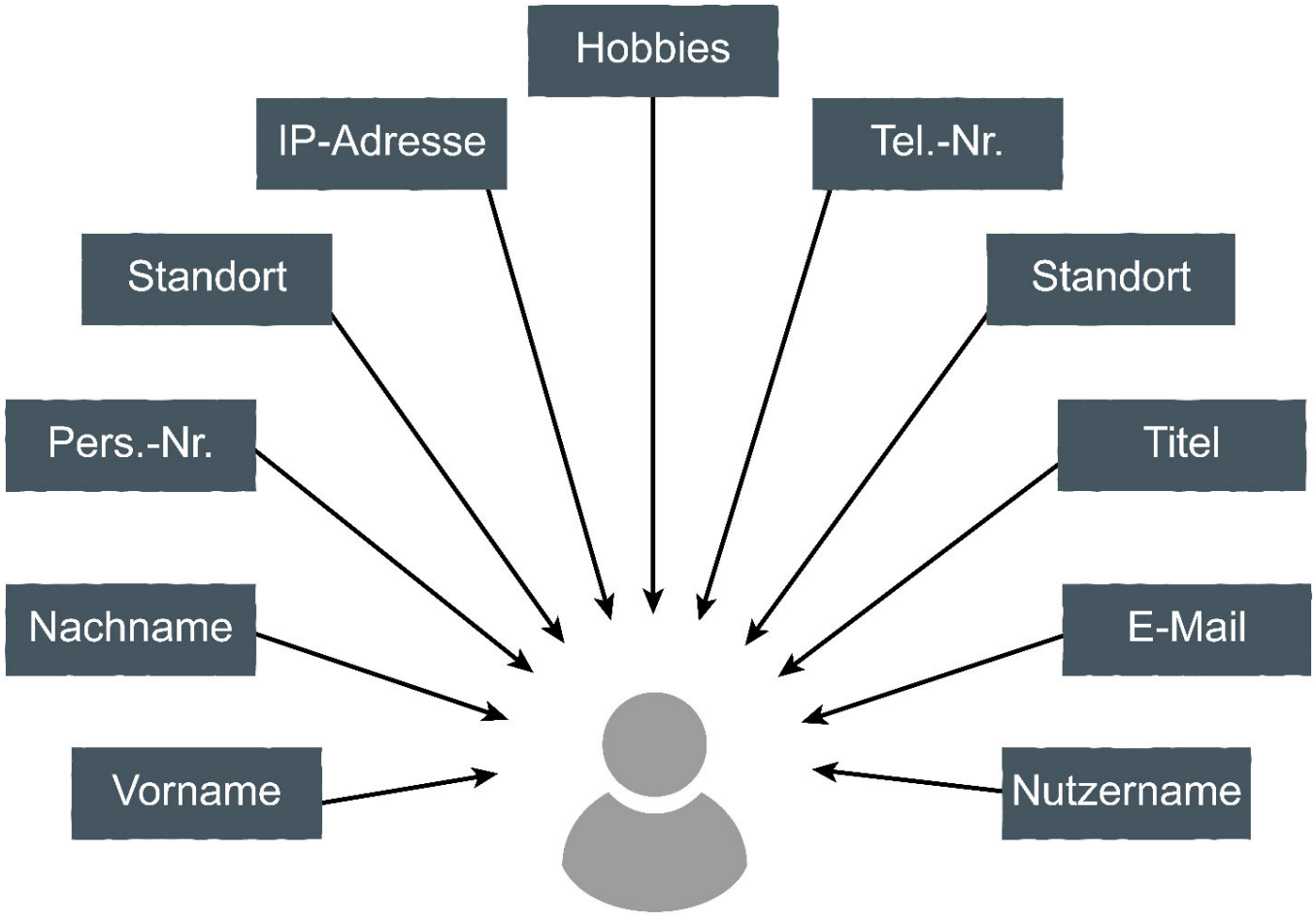
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

EIAM
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- **Definitionen**
- Notwendigkeit
- Key Concepts
- IAMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

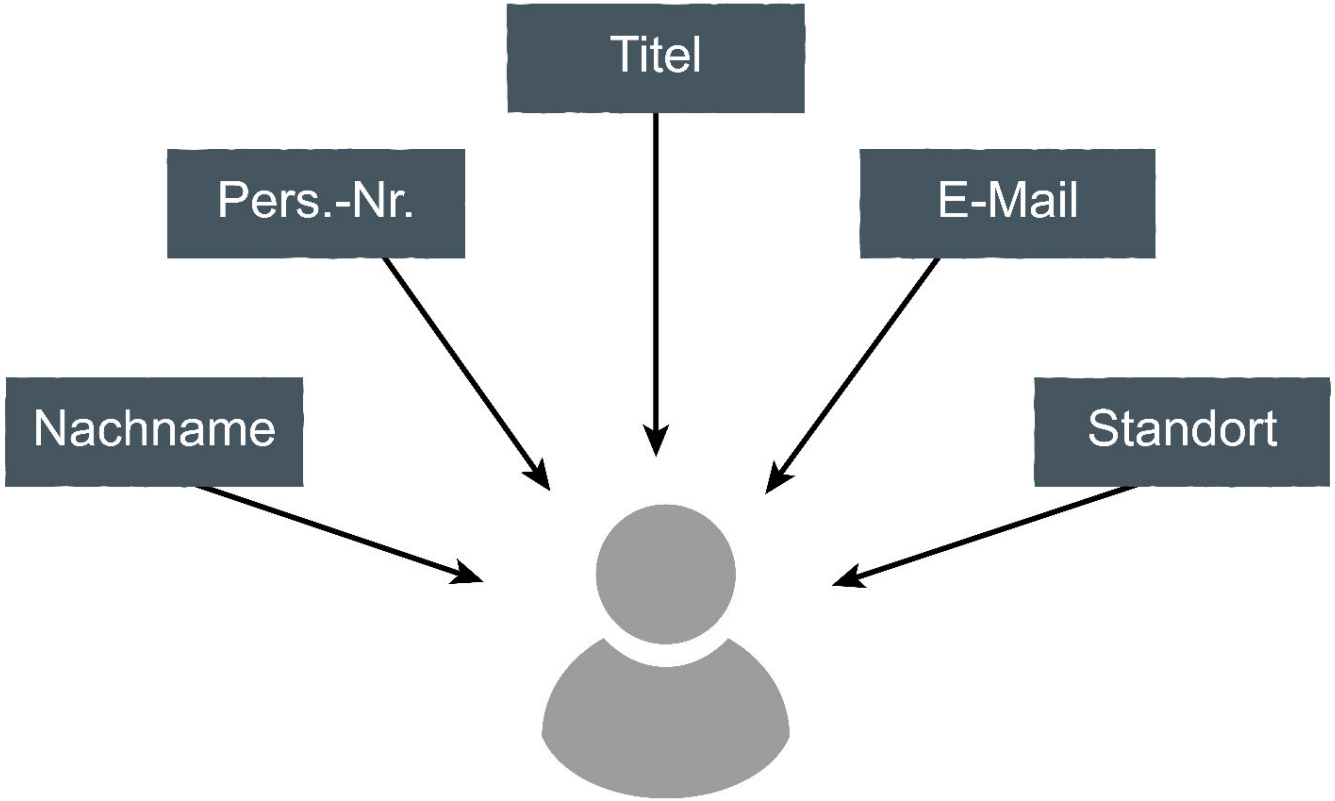
Definitionen
→ Entität



- Eine **Entität** (Person, Rechner, etc.) setzt sich zusammen aus der sie **beschreibenden Attribute**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Definitionen
→ Digitale Identität



- Eine **digitale Identität** ist die **Teilmenge der Attribute einer Entität**, welche diese Identität in einem bestimmten Kontext im Unterschied zu anderen Entitäten **eindeutig bestimmbar** machen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Definitionen
→ Identity and Access Management

- In der Fachwelt hat sich bisher keine einheitliche Auffassung, was exakt unter Identity and Access Management zu verstehen ist, durchgesetzt.
- In der Mehrheit der Definitionen bezieht sich der Begriff **Enterprise Identity and Access Management (EIAM)** im Kern auf
  - die Kombination von Verfahren der **Organisationsführung** einerseits
  - und **Technologie** andererseits,
- welche es Organisationen durch eine breite Palette von Prozessen und Funktionalitäten erlauben
  - die **Einhaltung gesetzlicher Vorschriften**
  - sowie die **Integrität, Vertrauenswürdigkeit und Verfügbarkeit von Informationen**
- gewährleisten zu können.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Definitionen
→ Identity and Access Management

- **Definition des Institut für Internet-Sicherheit – if(is):**
  - Der Begriff **EIAM** beschreibt jeglichen Einsatz von digitalen Identitäten, deren Attributen, sowie deren Berechtigungen und schließt die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein.

- Das **Ziel** ist es,
  - **vertrauenswürdige,**
  - **Identitätsbezogene und**
  - **regelkonforme Prozesse**
- durchzusetzen, die **unabhängig von Organisationen und Plattformen** standardisiert nutzbar sind.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

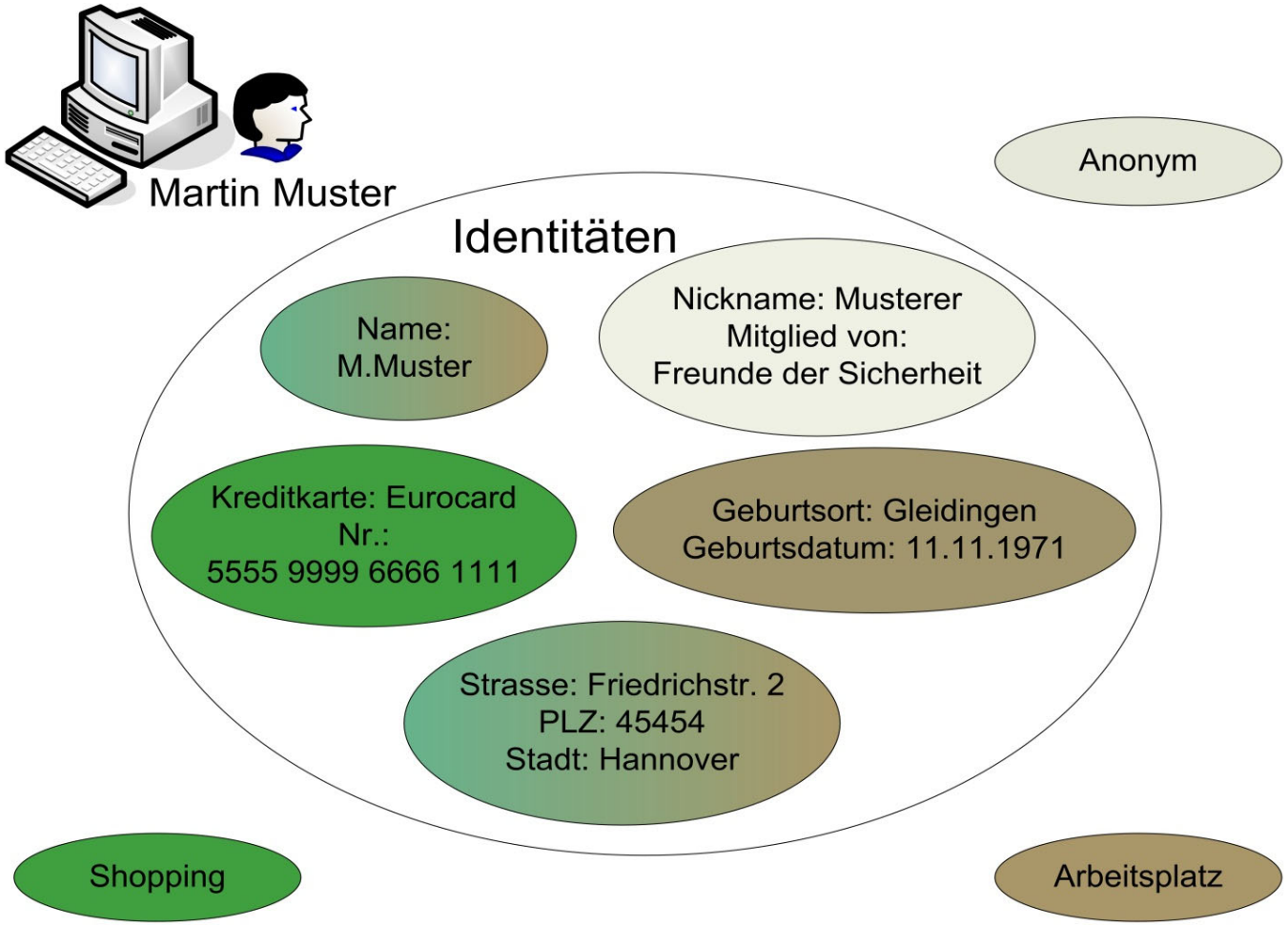
EIAM
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Definitionen
- **Notwendigkeit**
- Key Concepts
- IAMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Notwendigkeit (1/4)
→ Szenario

- Einfaches Szenario, warum Identity Management Systeme benötigt werden



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Notwendigkeit (2/4)
→ Passwörter & Nutzerkonten

- Unüberschaubare Mengen an
  - Nutzerkonten
  - Zugriffsrechten
- Passwörter & Accounts werden vergessen
- Einfache & immer gleiche Passwörter

  → Identitätskollaps

Mitgliedsname

Haben Sie Ihren Mitgliedsnamen vergessen?

Passwort

Haben Sie Ihr Passwort vergessen?

▶ Ihre Angaben zum Einloggen sind ungültig. Bitte versuchen Sie es erneut.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Notwendigkeit (3/4)
→ Folgen

- Erhöhte Kosten
- Komfortverlust
- Steigender Administrationsaufwand
- Fehlende Kontrolle
- Informations- bzw. Datenverlust
- Unüberschaubare Sicherheitsrisiken
- Sicheres organisationsübergreifendes Arbeiten unmöglich

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Notwendigkeit (4/4)
→ Zusammenarbeit mit Partnern

- Organisationen sind auf Zusammenarbeit mit Partnern angewiesen, dies verlangt nach
  - Sicherem Austausch von identitätsbezogenen Daten
  - Vertrauensverhältnissen
  - Verwendung einheitlicher Standards
  - Koppelung von Geschäftsprozessen
  - Need-to-Share Prinzip
  - Sicheres Einbinden externer Personen in interne IT-Systeme

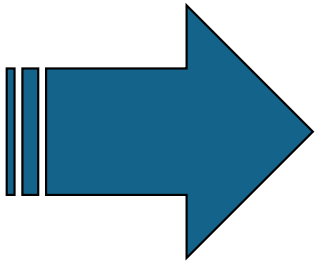
- Cloud Computing benötigt technische Aspekte zur
  - Weitergabe von Identitäten
  - Authentifizierung und Autorisierung

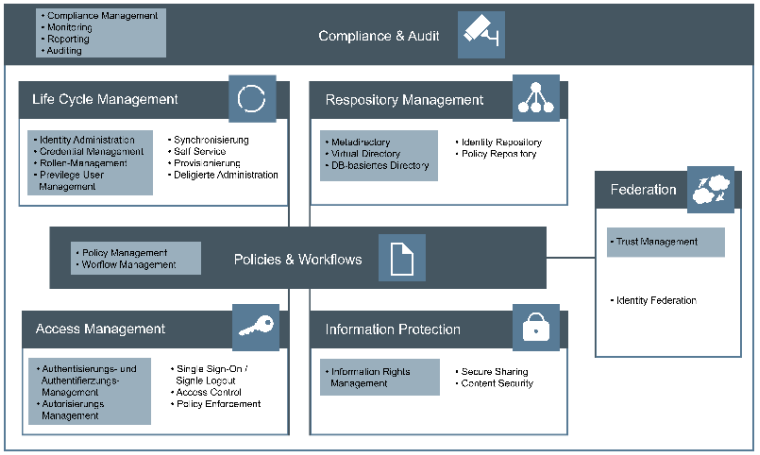
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Notwendigkeit eines EIAMs
→ Einführung durchgängiges Beispiel

- Am Beispiel des Lebenszyklus der digitalen Identität eines Mitarbeiters, soll gezeigt werden
  - warum Enterprise Identity and Access Management Systeme benötigt werden
  - und wie sie funktionieren

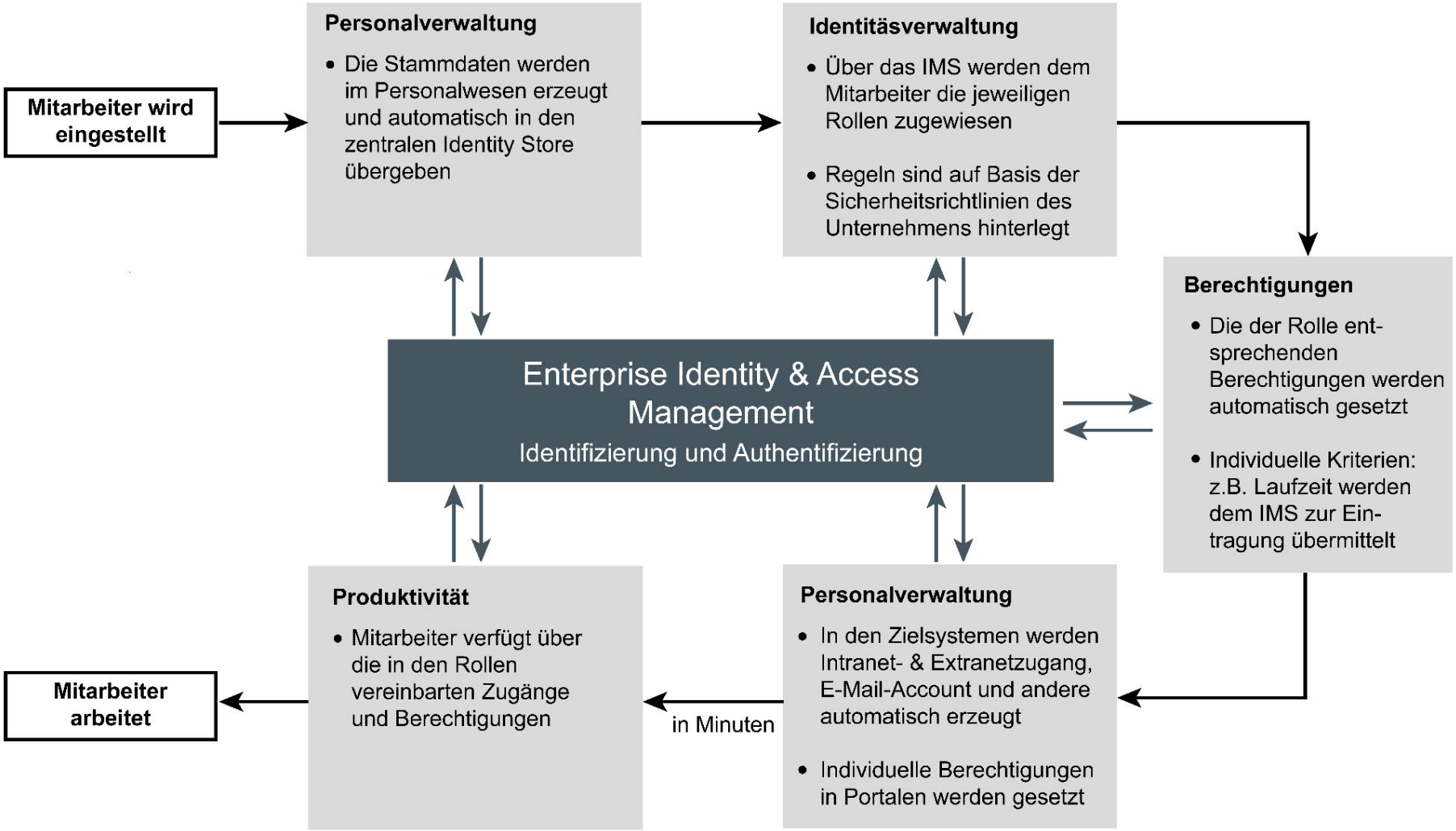
- Das Beispiel zieht sich durch die gesamte Beschreibung des Identity and Access Management Modells (siehe **Key Concepts**)





© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Notwendigkeit
→ Einführung durchgängiges Beispiel



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

EIAM
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Definitionen
- Notwendigkeit
- **Key Concepts**
- IAMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

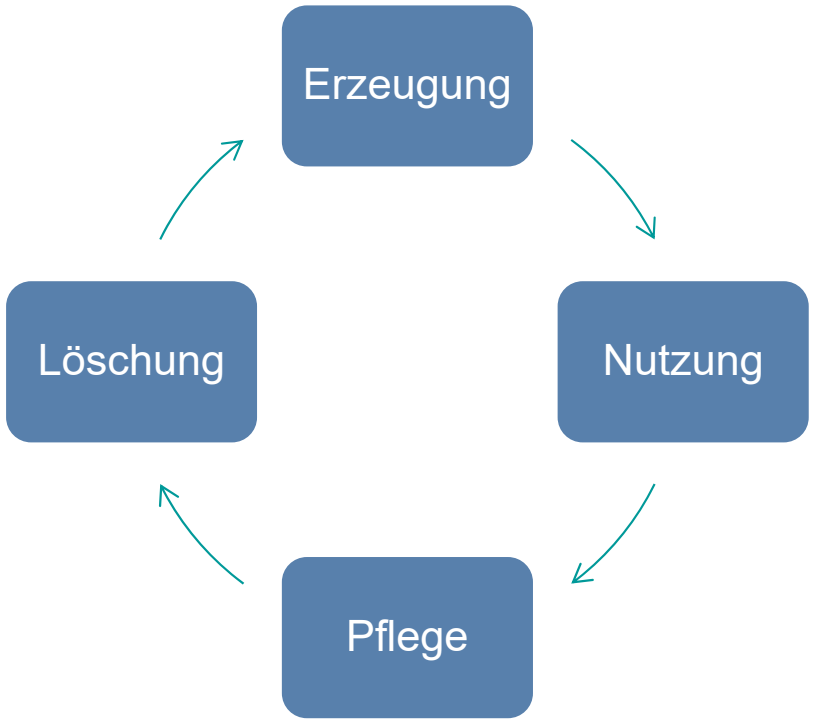
Key Concepts
→ Anforderungen

- Sichere und komfortable Authentifizierung
- Strukturierte Identitäts-Datenspeicherung und –verwaltung
- Zusammenführung von Identitätsdaten
- Identitäten über ihren gesamten Lebenszyklus begleiten
- Vermeidung von Überberechtigungen
- Schutz von Informationen und Zugriffen
- Organisationsübergreifende Nutzung von Identitäten
- Vertrauen zwischen Dienstanbietern herstellen

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Anforderungen

- Enterprise Identity and Access Management soll:
  - digitale Identitäten und ihren gesamten Lebenszyklus verwalten
  - insbesondere, deren vertrauenswürdige Attribute sowie Berechtigungen



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Aufbau eines Enterprise IAM

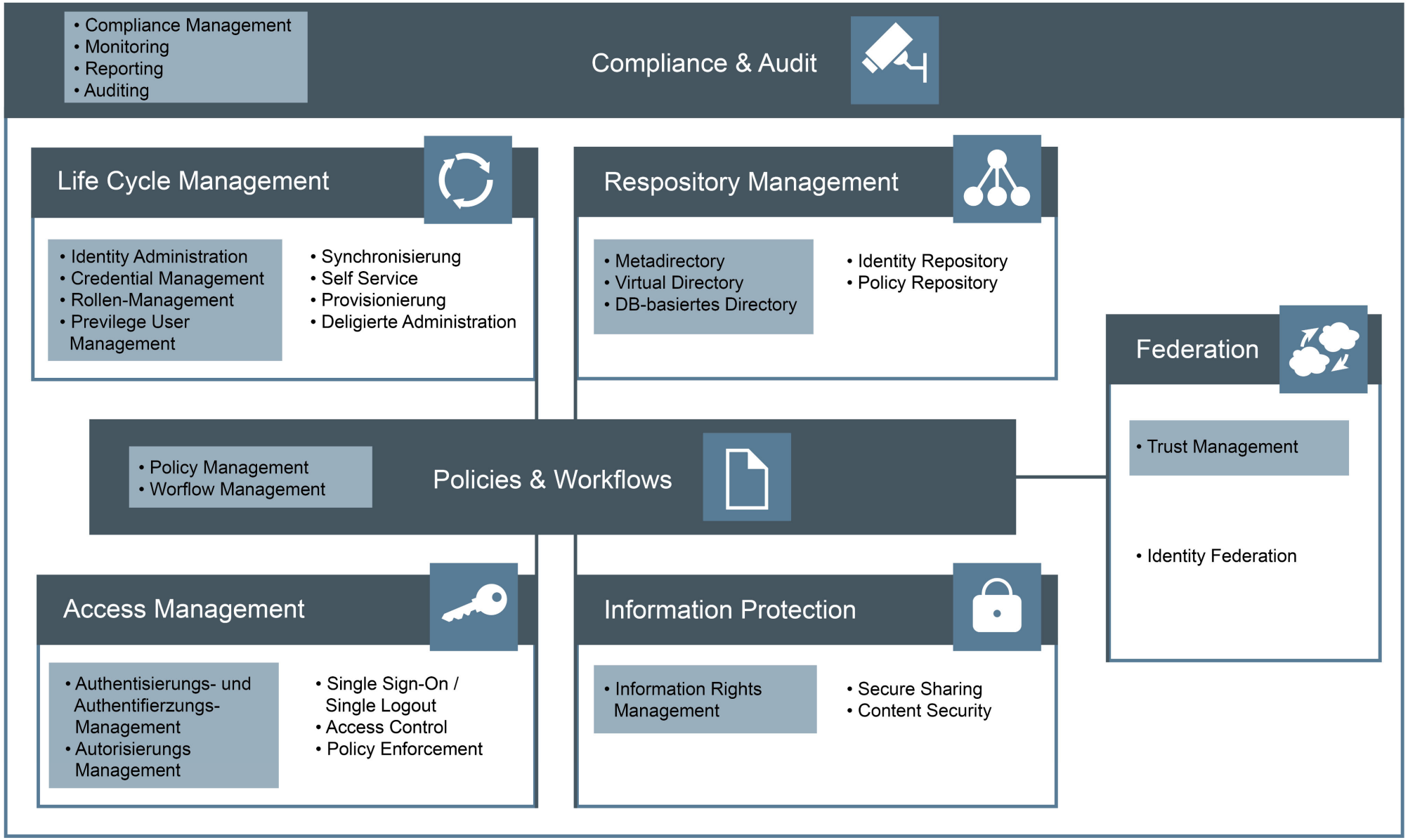
- Strukturierung eines IAM-Modells in sieben Module:
  - Policies & Workflows
  - Repository Management
  - Life Cycle Management
  - Access Management
  - Information Protection
  - Federation
  - Compliance & Audit

  } Typische Struktur für die Anwendung in Unternehmensnetzwerken

  - Diese Module bestehen aus Komponenten und diese enthalten wiederum (technische) Funktionen

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Ein Enterprise-IAM-Modell



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Policies & Workflows (1/4)

- **Basis des Identity Managements:**
  - Die Verwaltung von Richtlinien und automatisierten oder organisatorischen Arbeitsabläufen ist zentral für den Erfolg des IdM.

- **Policies (Richtlinien):**
  - Definieren den Anspruch und die zu erreichenden Ziele (Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit).
  - Policies können global für das ganze System oder servicespezifische für eine bestimmte Ressource definiert werden.
  - Eine servicespezifische Policy (z.B. für die Lohnbuchhaltung) hat Vorrang vor den globalen Policies.
  - Policies müssen in einem Repository zur Verfügung gestellt werden.
  - Jeder Komponente lassen sich Policies zuordnen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Policies & Workflows (2/4)

- **Workflow (Arbeitsablauf):**
  - Ein Workflow bezeichnet die Verwaltung eines Prozesses.
  - Er unterstützt die Erstellung und Verarbeitung von Geschäftsprozessen.
  - Dabei können von den Workflows vordefinierte Ablaufstrukturen festgelegt werden, die die Prozesse zwischen den Entitäten in viele kleine automatische Teilprozesse zerlegen.
  - Dazu gehören auch die Koordination und Fehlerbehandlung bzw. die integrierte Datenverwaltung oder der Transfer von Daten.
  - Workflows sind sehr flexibel und können auch für komplexere Prozesse eingesetzt werden. Damit wird erreicht, dass Arbeitsvorgänge mit Workflows halb-/automatisiert werden können.
  - Workflows sind nicht nur technischer Natur.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Policies & Workflows (3/4)

- **Beispiel für Policies & Workflows:**
  - Ein Mitarbeiter (def. als Entität) kommt neu in ein Unternehmen.
  - Eine Richtlinie für die Personalverwaltung regelt, welche Stammdaten zur Erzeugung einer neuen digitalen Identität benötigt werden und wie diese jeweils geprüft werden müssen.
  - Ein Workflow gibt vor, wie diese Daten in das System der Personalverwaltung eingepflegt werden müssen.
  - Eine weitere Richtlinie regelt in welchen Abständen die Daten in ein Directory übernommen werden müssen.
  - Zuletzt beschreibt ein Workflow wie die Daten in das zuständige Directory hinzugefügt/kopiert werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Policies & Workflows (4/4)

- **Policy Management:**
  - Ein zentrales Policy Management stellt sicher, dass die erstellten Richtlinien eingehalten werden.
  - Hierfür werden Werkzeuge für die Erstellung, Deaktivierung und Zuweisung zur Verfügung gestellt.

- **Workflow Management:**
  - Zentrale Verwaltung aller Workflows. Dies ist notwendig, da Workflows die Komponenten des IaM verbinden.
  - Jegliche Aufgaben, um Workflows zu definieren, zu spezifizieren, zu simulieren, auszuführen und zu steuern.
  - Die Koordination von Workflows erfolgt durch ihren Aufbau. Dabei stellen sich die Fragen der Verantwortlichkeit (wer, was, wann und wie).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Repository Management (1/2)

- Zentrale Speicherung von Informationen:
  - Ziel: Eine einzige digitale Identität pro Nutzer/Entität.

- Directory Services:
  - Die Daten werden hierarchisch in einer Baumstruktur, dem Directory Information Tree (DIT), gespeichert.
  - Diese Baumstruktur ähnelt oder entspricht oft einer realen organisatorischen oder geografischen Struktur.
  - Die eingesetzte Datenbank ist im Normalfall für ihre speziellen Aufgaben (die Suche, das Einfügen und Löschen) optimiert.
  - Verteilte Speicherung und Daten-Replikation.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Repository Management (2/2)

- Beispiel für Repository Management:
  - Die digitale Identitäten eines Mitarbeiters, genauer deren Attribute, werden beim Zugriff auf Applikationen im Rahmen seiner Tätigkeit im Unternehmen benötigt.
  - Die strukturierte Identitäts-Datenspeicherung und –verwaltung in einem Metadirectory erlaubt eine Authentifizierung anhand der jeweils aktuellen Attributwerte (von überall im Unternehmen).
  - Ebenso wird die Richtlinie zur Bestimmung der korrekten Stärke einer Authentifizierung aus einem zentralen Repository abgerufen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: DB-basiertes Directory (1/2)

- Alternativ zu einem Directory Service mit Baumstruktur kann zur Datenspeicherung eine relationale Datenbank verwendet werden.

- Mögliche Technologien sind z.B. PL/SQL von Oracle, MySQL oder PostgreSQL. Der Zugriff erfolgt mittels jeweiliger Datenbanksprache.

- Dabei ergeben sich folgende Vorteile gegenüber einem Directory Information Tree (DIT):
  - Transaktionsfähigkeit - Änderungen an der Datenstruktur erweisen sich einfacher als in einer Baumstruktur
  - Referenzielle Integrität
  - Accounting - Datenbank-Sprachen wie SQL nutzen kaufmännische Funktionen, die bei Verwendung von Baumverzeichnissen wegen geringer Typensicherheit nicht einsetzbar sind.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: DB-basiertes Directory (2/2)

- Relationale Datenbanken haben den Nachteil, dass ihre Performance nicht in jeder Situation optimal und im Fall von Directories eher schlecht ist.

- Des Weiteren fehlt der relationalen Datenbank im Gegensatz zum DIT die Möglichkeit zur Vererbung.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Metadirectory

- Ein Metadirectory (engl. für Metaverzeichnisdienst) synchronisiert Datenbestände aus verschiedenen anderen Verzeichnisdiensten.
- Voraussetzung dafür ist, dass alle zu synchronisierenden Daten im Verzeichnisdienst abbildbar sind.
- Das entsprechende Schema muss standardisiert sein, damit verschiedene Anwendungen darauf zugreifen können.
- Durch die Integration von Workflows und Policies wird die Synchronisierung der Einträge und Berechtigungen in den Repositories geregelt.
- Daten werden z.B. bei Änderungen automatisch weitergeleitet und aktualisiert.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Virtual Directory

- Virtual Directory ist eine hierarchisch aufgebaute Technologie, die eine Sicht auf digitale Identitäten, ihre Attribute, Daten und die dazugehörigen Berechtigungen bietet, ohne ein komplett eigenes Verzeichnis aufzubauen (im Gegensatz zu einem Metadirectory).

- Der Aufbau eines Virtual Directory gleicht dem eines normalen LDAP-Directories, der Datenzugriff erfolgt jedoch per Referenz.

- Erhält das Virtual Directory eine Anfrage, so werden die Daten beim Zugriff in Echtzeit aus dem jeweiligen Repository (Datensilo) gelesen und an die zuständige Datenquelle weitergeleitet, d.h. sie werden nur referenziert.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Identity Repository

- Ein Identity Repository (engl. für Identitätsspeicher) ist ein Verzeichnisdienst oder eine Datenbank zur Speicherung von digitalen Identitäten.

- Mittels Synchronisierung, durch ein Metadirectory oder ein Virtual Directory werden die Einträge unterschiedlicher Identity Repositories abgeglichen.

- Die Daten im Identity Repository werden durch die Identity Administration verwaltet.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Policy Repository

- Ein Policy Repository dient der zentralen Speicherung von Policies.
- Es erlaubt IT-Systemen, Policies bei Bedarf abzurufen.
- Oft ist das Policy Repository mit anderen Repositories (bspw. Role und Entitlement Repository) in einem umfassenden Repository konsolidiert.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Life Cycle Management (1/3)

- Das EIDM behandelt den kompletten Life Cycle von digitalen Identitäten und den mit ihnen verknüpften Prozessen.
- Der Life Cycle einer Entität beginnt mit der Erstellung und Administration von digitalen Identitäten und deren Attributen in entsprechenden Datensätzen sowie deren Zuteilung in entsprechende Repositories.
- Die Zugriffsrechte der digitalen Identitäten werden durch eine Rollenverteilung eingeschränkt.
- Die Änderung bzw. Aktualisierung von Identitäts-bezogenen Daten und Credentials erfolgt im Rahmen der Provisionierung, der De- und Reprovisionierung und durch Synchronisierung aller Repositories mit dem jeweils führenden System (z.B. ein Metadirectory).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Life Cycle Management (2/3)

- Durch einen Self Service haben Nutzer selbst die Möglichkeit (wenn auch eingeschränkt) z.B. ihre Daten zu aktualisieren und zusätzliche Rechte bzw. Rollen anzufordern.

- Der Life Cycle einer Entität endet mit der endgültigen Löschung einer digitalen Identität.
  - Eine Reprovisionierung ist dann unmöglich.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Life Cycle Management (3/3)

- Beispiel für Life Cycle Management:
  - Der Mitarbeiter benötigt durch die Zuordnung (siehe Workflow) zu einem neuen Projekt Rechte zum Zugriff auf Applikationen (siehe Access Management) auf die er zuvor nicht zugreifen konnte (bspw. über eine neue Rolle).
  - Er beantragt diese Rechte in einem Webfrontend (Self Service).
  - Der Projektleiter hat sein Recht zur Genehmigung dieser Rechte an einen Vertreter delegiert.
  - Dieser genehmigt dem neun Projektmitarbeiter diese Rechte nach Prüfung in seinem Webfrontend.
  - Das System provisioniert diese Rechte anschließend in die Applikationen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Identity Administration

- Der eigentliche Fixpunkt in einem EIDM-System ist die digitale Identität.
- Sie ist eine Ansammlung von Attributen einer Entität (z.B. einer Person oder einem IT-System), die diese von anderen Entitäten in einem bestimmten Kontext unterscheidbar macht.
- So ist jede Entität eindeutig identifizierbar und alle Datenanforderungen oder -übermittlungen können einer bestimmten Entität zugeordnet werden.
- Die Identity Administration erstellt und verwaltetet die digitalen Identitäten.
- Sie unterstützt deren Erzeugung und Bearbeitung und sorgt für eine Synchronisierung identitätsbezogener Daten.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
Funktion: Provisioning (1/2)

- Provisioning:
  - Automatisierung aller Prozesse bezüglich der Erstellung, Verwaltung, Deaktivierung sowie Löschung von digitalen Identitäten.

- Deprovisionierung:
  - Berechtigungen einer digitalen Identität (ggf. gesamte Identität) in allen betroffenen IT-Systemen automatisiert deaktivieren.
  - Dies geschieht z.B., wenn ein Mitarbeiter das Projekt wechselt oder das Unternehmen verlässt.
  - Der Mitarbeiter hat dann keinen Zugang mehr zu den Organisationsressourcen und den Diensten des EIAM-Systems.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
Funktion: Provisioning (2/2)

- Reprovisionierung:
  - Reaktivierung von Daten und die jeweiligen Berechtigungen, sofern sie noch vorgehalten wurden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Rollenmanagement (1/2)

- Erstellung, Verwaltung und Zuteilung von Rollen an eine digitale Identität (Nutzer oder IT-System).
- Eine Rolle ist eine Art Baustein eines Zugriffsmodells und wird benötigt, um digitalen Identitäten Berechtigungen zu erteilen.
- Die verschiedenen Berechtigungen in einem Unternehmen müssen je nach Prozess in entsprechenden Rollen abgebildet werden.
- Einer digitalen Identität können mehrere Rollen für verschiedene Teilbereiche zugeordnet werden.
- Die Einstellungen werden per Hand vom Administrator zugewiesen.
- Der Nutzer hat eine stark eingeschränkte Möglichkeit, Rollen zu verwalten (Self Service).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Rollenmanagement (2/2)

- Technische Rolle:
  - Spezifische (technische) Aufgabe, wie z.B. ein Backup-Administrator oder ein DB-Administrator mit den nötigen Rechten.
- Geschäftsrolle:
  - Zusammenfassung von mehreren technischen Rollen (z.B. „Mitarbeiter“ oder „Projektleiter“).
- Role Mining:
  - Bestehende Berechtigungen für den Zugriff auf Ressourcen in einem Unternehmen automatisiert analysieren und daraus Rollen ableiten.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts

→ Komponente: Privileged User Management

- Privilegierte Nutzer (wie z.B. Administratoren von IT-Systemen) besitzen durch ihre weitreichenden Rechte die potentielle Macht, jederzeit und an jedem Ort Veränderungen an Informationen durchführen zu können.
  - Genaue Kontrolle der privilegierten Nutzer, verbunden mit zusätzlichen Sicherheitsmaßnahmen, notwendig.
  - Nur die Rechte und Zugänge erteilen, die unbedingt für die Erfüllung ihrer Aufgaben notwendig sind.

- Das PUM ermöglicht die Datenschutz- und Richtlinien-konforme kontinuierliche Überwachung von Aktivitäten privilegierter Nutzer.
  - Integriert in das Monitoring und Reporting des EIAM-Systems.
  - Risikominimierung durch automatisiert versandte Reports bei Verdacht auf kriminelle Handlungen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Delegierte Administration

- Weitergabe von Rechten/Privilegien (im Idealfall auf Rollen basierend) nach Bedarf von einer digitalen Identität an eine bisher nicht privilegierte Identität.
  - Automatisierung durch zuvor festgelegte und in einem Policy Repository bereitgestellte Richtlinien möglich.
  - Mit diesem automatisierbaren Prozess soll ein möglichst fortwährender Arbeitsbetrieb gewährleistet werden (z.B. bei Urlaub oder Erkrankung).
  - Jegliche Weitergabe von Rechten wird zu jedem Zeitpunkt durch das EIAM-System protokolliert und ist somit vollständig nachvollziehbar.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Synchronisierung

- Daten jeglicher Art nach einer Veränderung automatisch an alle beteiligten IT-Systeme (z.B. Repositories bzw. Directory Services) weiterleiten und abgleichen.
- Notwendigkeit:
  - Berechtigungsänderungen im Rahmen der Provisionierung in den betroffenen IT-Systemen.
  - Vermeidung von Inkonsistenzen von Datenbeständen in unterschiedlichen Verzeichnissen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Self Service

- Die Funktionen des Self Service sind:
  - Anmeldung an Diensten
  - Änderung eigener Daten sowie Passwortbearbeitung
  - Zurücksetzen vergessener Passwörter (z.B. anhand von vorher festgelegten Antworten auf definierte Fragen)
  - Beantragung von Rollen für sich selbst
  - Überprüfen des Status der eigenen Anträge
  - Genehmigung sowie Delegation von Zugriffsrechten oder Teilen davon für die Nutzer- und Rollenverwaltung an andere Nutzer

- Datenschutzkonforme Protokollierung aller Aktivitäten:
  - Gewährleistung der Nachvollziehbarkeit und Prüfbarkeit im Rahmen des Auditing.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Credential Management

- Verwaltung aller Credentials einer Entität.
  - Credentials sind Nutzernamen, Passwörter, Zertifikate, biometrische Merkmale, kryptographische Schlüssel und weitere Nachweise, die als Authentisierungsmerkmale dienen können.
  - Diverse Kombinationen aus diesen Credentials ergeben wieder eigene Credentials, bspw. das Paar Nutzername + Passwort.

- Regelung der Nutzung von Hilfsmitteln die für den sicheren Umgang mit Credentials notwendig sind.
  - z.B. eine Smartcard, die als sicherer Container für Zertifikate dient, oder ein Security Token mit ähnlicher Funktionalität.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Access Management (1/2)

- Entscheidung über Zugriffsberechtigungen auf der Basis von Nutzeridentitäten, -rollen und Zugriffsrechten.

- Es beschreibt die notwendigen Sicherheitsmechanismen für
  - den Zugriff auf ein EIAM-System sowie
  - die Kontrolle (Access Control) und
  - das Durchsetzen des Zugriffs (Enforcement).

- Zugangslösungen sind z.B.:
  - Sicherheitsprotokolle
  - Virtual Private Networks (VPNs)
  - Authentifizierungstechniken

Access Management

- Authentisierungs- und Authentifierzungs-Management
- Autorisierungs-Management

- Single Sign-On / Signle Logout
- Access Control
- Policy Enforcement

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Access Management (2/2)

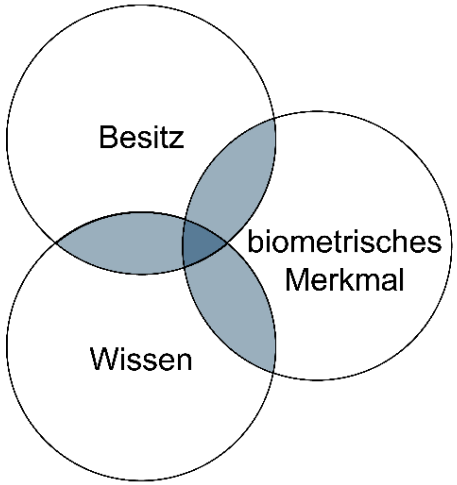
- Beispiel für Access Management:
  - Der Mitarbeiter benötigt Zugriff auf viele unterschiedliche Applikationen.
  - Er bekommt eine SmartCard mit einem Personenzertifikat der unternehmenseigenen PKI.
  - Hiermit meldet er sich Morgens an der Domäne und dadurch gleichzeitig an einem Single Sign-On System an.
  - Dieses sorgt dafür, dass er beim Zugriff auf eine Applikation automatisch authentifiziert wird, ohne sich erneut anmelden zu müssen.
  - Am Ende seines Arbeitstages meldet er sich von der Domäne ab, wodurch ein Single Logout Mechanismus ihn an allen Applikationen abmeldet.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

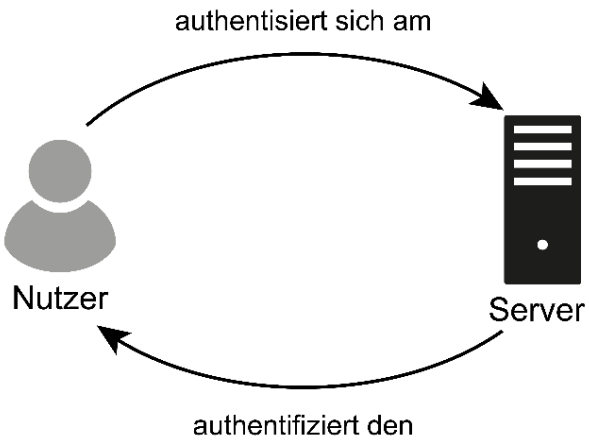
Key Concepts

→ Komponente: Authentifizierungs-Management (1/2)

- Die Authentifizierung beschreibt die Verifizierung der Echtheit der Identität einer Entität (z.B. Nutzer oder IT-System).
  - z.B. durch ein Passwort (Wissen), den Fingerabdruck (Sein), durch Hardware-Sicherheitsmodule (Besitz).



- Eine Entität (z.B. ein Nutzer) authentisiert sich an einer Instanz, indem sie den Nachweis der eigenen Identität erbringt.
- Die Instanz authentifiziert die Entität in der Folge.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts

→ Komponente: Authentifizierungs-Management (2/2)

- Das Authentifizierungs-Management definiert und kontrolliert
  - den Vorgang der Verifizierung sowie
  - die zu verwendenden Authentisierungstechniken.

- Mit diesem Prozess wird die
  - Datenintegrität und Vertraulichkeit gewahrt,
  - und es wird zum Schutz von Informationen beigetragen.

- Der Authentifizierung folgt im Normalfall die Autorisierung für definierte und an Rechte gebundene Zugriffe.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts

→ Komponente: Autorisierungs-Management

- Das Autorisierungs-Management muss Richtlinien, Prozesse und Verfahren zur Festlegung von Zugriffsrechten vereinen.
  - Anwendungsübergreifende Berechtigungs- und Richtlinienverwaltung.
  - Gewährleistung einer sicheren, effektiven und effizienten Steuerung und Verwaltung.
  - Modul zum Review der Berechtigungen für Audits benötigt.
- Voraussetzung: Eine erfolgreiche Authentifizierung.
- Mehrwerte:
  - Automatisierung der Vorgänge und
  - die Vermeidung von Überberechtigung.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Access Control

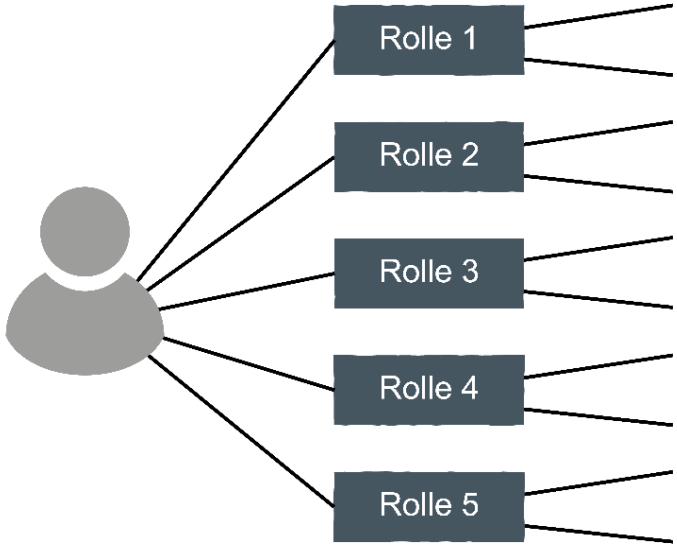
- Netzwerkweiter Zugriffsschutz auf unternehmensspezifische Ressourcen und Services durch Entitäten.
  - Um einen Zugriff auf solch einen Dienst zu gewährleisten, werden vorab technische und organisatorische Vorbereitungen getroffen.
  - Dazu werden Entitäten authentisiert, authentifiziert und autorisiert.
  - Die Kontrolle erfolgt meist durch Passwörter, Gewährung von Privilegien und Bereitstellung von Attributen.

- Unterschiedliche Ressourcen erfordern unterschiedliche Zugriffskontrollen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Role-Based Access Control

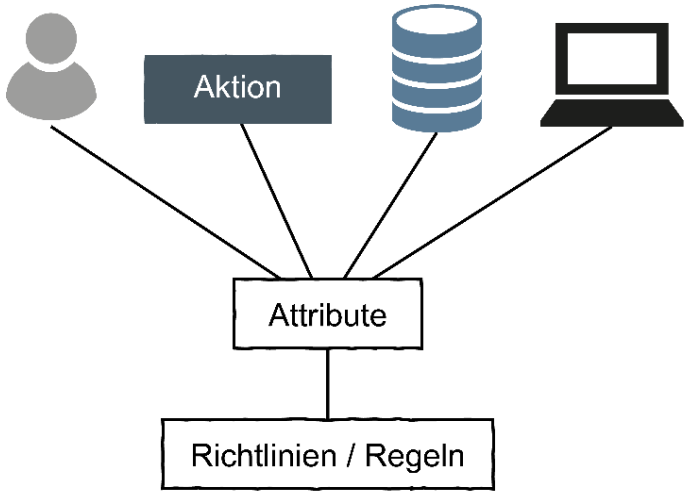
- Bei der rollenbasierte Zugriffskontrolle werden den Nutzern des IT-Systems oder Netzwerks Rollen zugeordnet.
  - Die Nutzer können dabei mehrere Rollen besitzen.
  - An eine Rolle sind entsprechende Berechtigungen gebunden.
  - Je nach Rollenzuordnung des Nutzers erteilt oder sperrt das IT-System dann das Zugriffsrecht auf Betriebsmittel.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Attribute-Based Access Control

- Bei der attributbasierten Zugriffskontrolle wird der Zugriff auf eine Ressource gesteuert durch:
  - Attributen des Nutzers (Entität),
  - der Ressource,
  - dem Zustand der Systemumgebung,
  - sowie auf diese Attribute angewendeten Sicherheitsregeln.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

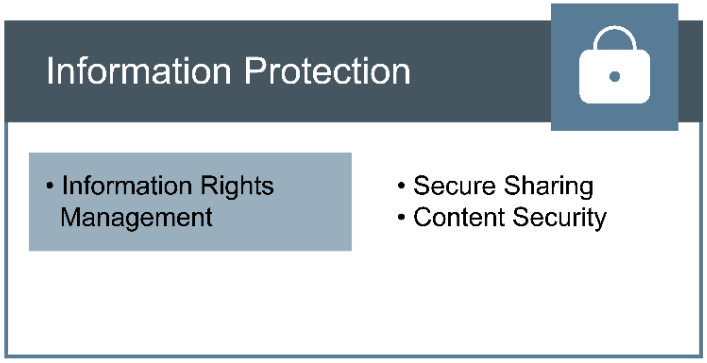
Key Concepts
→ Funktion: Policy Enforcement

- Das Policy Enforcement ist dafür verantwortlich,
  - Anfragen an einen Dienst entgegen zu nehmen und
  - basierend auf einem Regelwerk die angefragten Aktionen durchzusetzen oder effektiv zu verhindern.
- Die technische Umsetzung wird meist als Policy Enforcement Point (PEP) beschrieben.
- Policy Enforcement ist keine zentrale Funktion, sondern muss in allen IT-Systemen und Anwendungen umgesetzt werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Information Protection (1/2)

- Über Policies werden Informationen nur Personen mit entsprechenden Berechtigungen zugänglich gemacht.
- Eine Information Rights Management (IRM) Infrastruktur sorgt für Verschlüsselung der Daten und regelt den Zugriff.
  - In keiner Phase der Existenz verlässt die Information das Schutzlevel.
- Nachverfolgbarkeit wird über spezielle Dienste gewährleistet.
- Mehrwert:
  - Durchgängig angemessenes Schutzlevel.
  - Schutz von Informationen, auch über Organisationsgrenzen hinweg.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Information Protection (2/2)

- Beispiel für Information Protection:
  - Ein Mitarbeiter generiert im Rahmen seiner Tätigkeit unternehmens-kritische Informationen.
  - Er muss diese Mitarbeitern und externen Partner zugänglich machen, jedoch sicherstellen, dass keine unbefugten Personen Zugriff erhalten.
  - In seiner Office-Applikation wählt er bei Abspeicherung des Dokumentes die Personen aus, die dieses später lesen können sollen.
  - Er kann sicher sein, dass das Dokument nun in verschlüsselter Form vorliegt und nur mit Hilfe einer IRM-Infrastruktur geöffnet werden kann.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Secure Sharing

- Secure Sharing beschreibt einen Sicherheitsmechanismus, der die Schutzlevel-konforme Verarbeitung von Informationen unter dem Zugang von mehreren Identitäten gewährleistet.

- Eine Information ist bei der Weitergabe innerhalb einer definierten Gruppe über ihren gesamten Lebenszyklus geschützt.
  - Sie ist nur von den Rechte-abhängigen definierten Identitäten (z.B. einer Rolle unter den entsprechenden Schutzmechanismen) bearbeitbar.
  - Durchgehende Transport- und Ende-zu-Ende-Verschlüsselung bei der Verarbeitung eines Dokuments.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts

→ Komponente: Information Rights Management

- Information Rights Management (IRM) bildet die logische Ergänzung zum Secure Sharing.

- Das IRM bewahrt sicherheitskritische Daten vor unkontrollierten Veränderungen oder Verarbeitungen, indem den Identitäten eindeutige automatisierte Rechte vergeben werden.

- Die korrekte Zuweisung von Rechten an Nutzer oder Nutzergruppen bzw. Rollen beinhaltet individuell einstellbare Lese-, Schreib- und Ausführungsrechte, immer in Bezug auf eine Identität.

- Identitäten mit entsprechenden Rechten dürfen die Informationen evtl. verändern und drucken, während andere Identitäten die Informationen lediglich sichten dürfen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Content Security

- Content Security beschreibt den Schutz von Informationen durch die Absicherung der Infrastruktur und der verarbeitenden Hard- und Software.

- Ergänzung des IRM und Secure Sharing durch Abwehrmaßnahmen gegen potenzielle Angreifer und absichtliches oder versehentliches Fehlverhalten.
  - z.B. durch Anti-Malware-Programme, Verschlüsselung und Data Leakage Prevention (DLP).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Federation (1/2)

- Austausch von Identitäts- und Authentifizierungsinformationen zwischen unterschiedlichen Organisationen.
  - Föderierte Autorisierung von Identitäten.

- Aufbau von Vertrauensverhältnissen auf partnerschaftlicher Basis.
  - Gemeinsames, sicheres und vertrauenswürdiges Arbeiten auch über Organisationsgrenzen hinweg.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Federation (2/2)

- Beispiel für Federation:
  - Der Mitarbeiter muss für einige Zeit mit Applikationen eines Projekt-partners arbeiten
  - Bei dem Zugriff auf die Applikationen muss er sich wie gewohnt mit seiner SmartCard authentifizieren
  - Anschließend kann er wie gewohnt auf die fremde Applikation zugreifen

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Trust Management

- Organisatorische und technische Maßnahmen für die Abbildung des Vertrauensverhältnisses:
  - Organisation ←→ Föderations-Partner
- Organisatorische Maßnahmen:
  - Policies, Workflows und vertragliche Aspekte.
- Technische Maßnahmen:
  - Sicherheit der gesamten EIAM-System-Infrastruktur, Einhaltung von technischen Spezifikationen, PKI-Infrastruktur.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Funktion: Identity Federation

- Gesicherter Abgleich von Identitäts- bzw. Authentifizierungsinformationen von Entitäten über System- und Unternehmensgrenzen hinweg.
  - Möglichkeit der Pseudo- und Anonymisierung.
  - Grundlegend ist die Authentifizierung des Nutzers an der Organisations-internen Domäne.
  - Anschließend werden die Nutzerinformationen (Claims) an die andere Organisation übergeben (z.B. Rollen, Berechtigungen oder Nutzereigenschaften).
  - Ein Authentifizierungsmerkmal pro digitaler Identität nötig.

- Beispiele für Standards: Security Assertion Markup Language (SAML), WS-Federation und Liberty Alliance.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Compliance & Audit (1/2)

- Dienste und Prozesse zur Überwachung und Überprüfung aller Vorgänge im Identity and Access Management System.

- Einhaltung von Vorschriften (Compliance):
  - Schutz unternehmenskritischer Daten.
  - Rechtskonformität (z.B. durch Dokumentation von Prozessen und Archivierung von Vorgängen in IT-Systemen).
  - Definition eines Ist-Zustandes für spätere Audits.

- Vergleich eines Soll-Ist-Zustandes (Audit):
  - Erkennung und Bewertung von Risiken.
  - Maßnahmen für die Erreichung der Compliance.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Modul: Compliance & Audit (2/2)

- Beispiel für Compliance & Audit:
  - Der Mitarbeiter hat während seiner Tätigkeit weisungsgemäß zwei Transaktionen durchgeführt die eine Verletzung einer Richtlinie bedeuten.
  - Seinem Vorgesetzten fallen diese Vorgänge auf und er möchte den Gründe hierfür erfahren.
  - Anhand einen hierfür vorgesehenen Dienst gesendeten Logdateien der Applikation, mit deren Hilfe die Transaktionen ausgeführt wurden, lässt sich die Situation nachvollziehen und der Vorgang durchgängig verifizieren.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Compliance Management

- Ein Compliance Management definiert und verwaltet Vorschriften für Prozesse und Prozessergebnisse.

- Ein Unternehmen kann die Vorgaben festlegen, während Audits tatsächliche oder mögliche Verstöße gegen die Vorgaben identifizieren sowie einschätzen und gegebenenfalls dem Compliance Management berichten.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Monitoring

- Systematische Überwachung von Systemen und eine Protokollierung aller relevanten Daten bzw. Vorgänge innerhalb eines EIAM-Systems.
  - z.B. Zugriff, Delegierte Administration, Self Service, Änderungen von Credentials, Protokolle des Privileged User Managements.
  - Erkennung und Auswertung von Fehlern bei Konfiguration, Kommunikation und Anwenderaktivitäten.
  - Gegenmaßnahmen bei kritischen Vorkommnissen anstoßen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Komponente: Reporting

- Kontinuierliche Berichterstellung und Auswertung von vergangenen und aktuellen Aktivitäten im EIAM-System.
  - z.B. Informationen über Zustände von Identitätsdaten oder Berechtigungen.
- Meldung kritischer Vorkommnisse
  - z.B. automatisierbar per E-Mail, Instant-Messenger oder SMS.
- Zuständiges Personal erhält eine klare Übersicht über den Zustand verschiedener Prozesse und kann feststellen, ob Aktivitäten vorschriftsmäßig durchgeführt wurden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

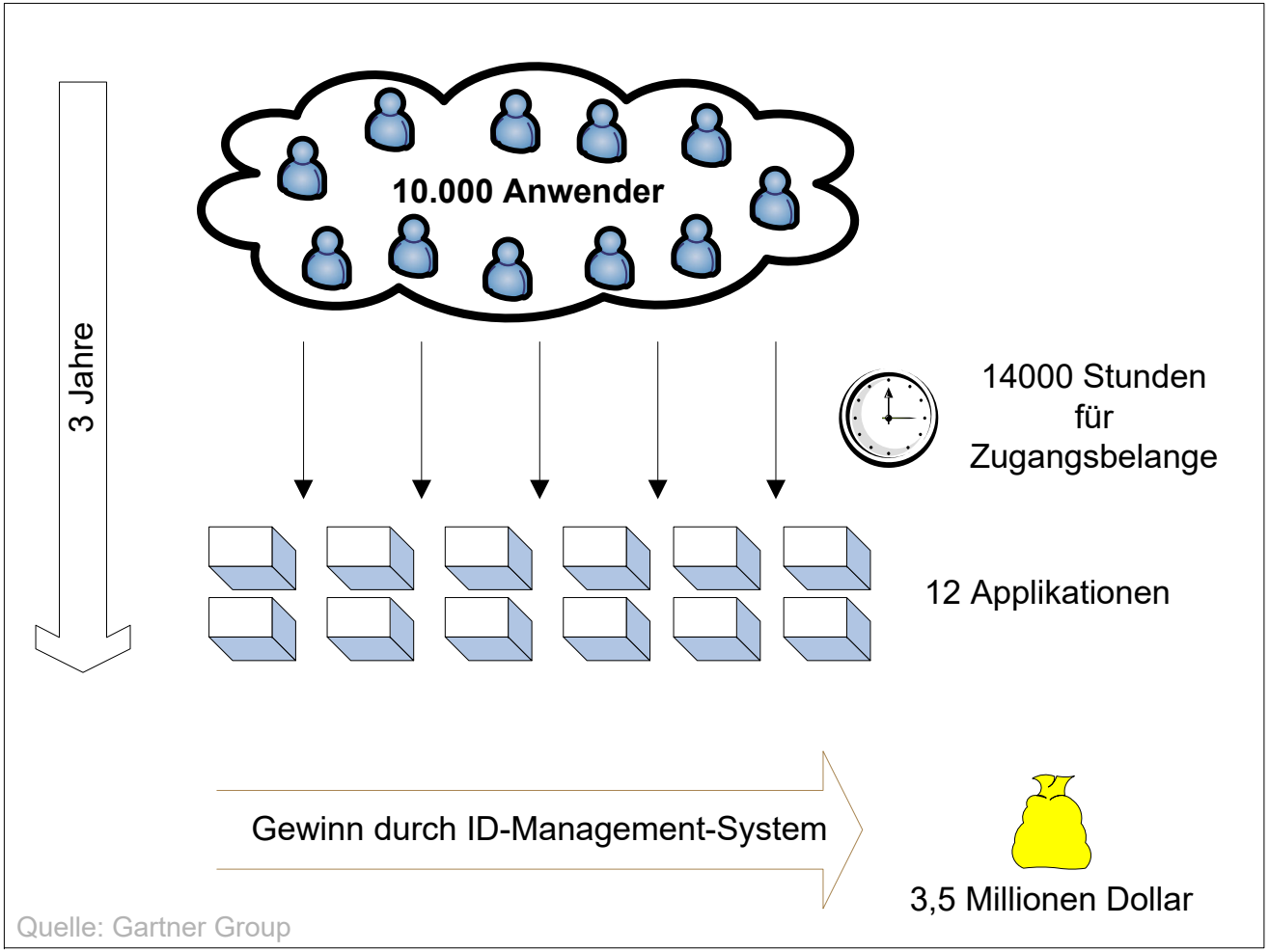
Key Concepts
→ Komponente: Auditing

- Prüfung aktueller und vergangener Rechte und Aktionen einer Entität mit Bezug auf die IT-Systeme und IT-Ressourcen.
  - Dabei werden relevante Informationen über einen Prozess erstellt, gespeichert und dem Auditor zur Verfügung gestellt.
  - Das Reporting kann das Auditing entsprechend unterstützen.
- Wichtige Fragestellungen beim Auditing:
  - Welche Aktionen wurden wann und von wem ausgeführt?
  - Welche Anwendungen wurden genutzt und auf welcher Ressource wurden sie ausgeführt?
  - Wer hat wann welche Berechtigungen vergeben?
- Datenschutz muss beachtet werden (z.B. bei personenbezogenen Daten).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Kostenszenario

- **Kostenersparnis durch Identity Management Systeme**

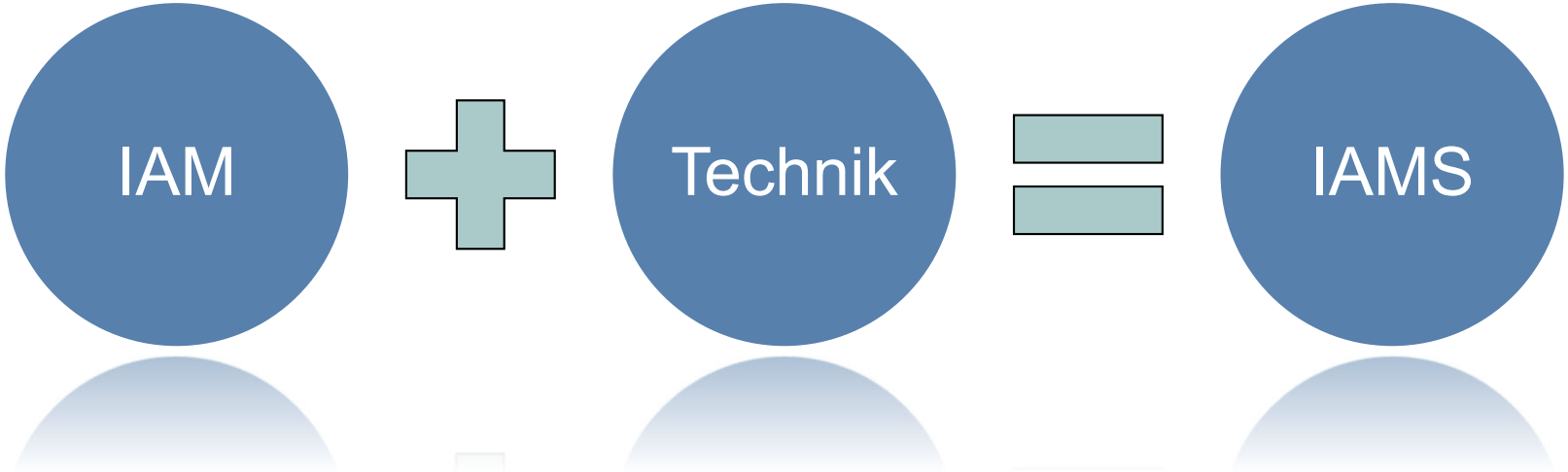


© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Key Concepts
→ Technologie

- Technologien eines Identity and Access Managment System (IAMS)
  - Verzeichnisdienste
  - Single Sign-On / -Logout
  - Circle of Trust
  - Föderation oder zentrale Datenhaltung
  - Einbindung von Webservices

} Typische Struktur für die Anwendung in Firmennetzwerken



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

EIAM
→ Inhalt

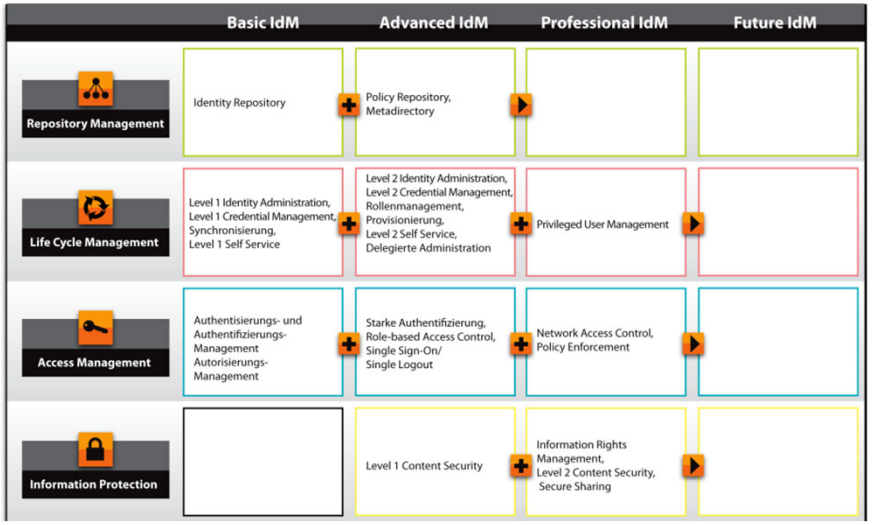
- Ziele und Ergebnisse der Vorlesung
- Definitionen
- Notwendigkeit
- Key Concepts
- **IAMS-Lebenszyklus**
- Single Sign-On
- Circle of Trust
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

IAMS-Lebenszyklus

- Umsetzung eines IAMS, gleichzeitig Langzeit-Roadmap für ein umfassendes IAMS
- Schrittweises Vorgehen anhand von Reifegraden, eingeteilt in vier Abstufungen
- Komponenten und Funktionen werden mit unterschiedlichen Reifegraden, sog. Leveln, dargestellt
  - Bestimmte Komponenten und Funktionen nur schrittweise eingeführt werden können oder sollten
  - Vorgeschlagene Umsetzung ist in keinem Fall abschließend
- IAM := konstanter, nie endender Prozess

  → alle Module durchlaufen immer wieder den Prozess der Überprüfung, Anpassung und Erneuerung



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

IAMS-Lebenszyklus
→ Reifegradbetrachtung Teil 1

	Basic IdM	Advanced IdM	Professional IdM	Future IdM
Repository Management	Identity Repository	Policy Repository, Metadirectory		
Life Cycle Management	Level 1 Identity Administration, Level 1 Credential Management, Synchronisierung, Level 1 Self Service	Level 2 Identity Administration, Level 2 Credential Management, Rollenmanagement, Provisionierung, Level 2 Self Service, Delegierte Administration	Privileged User Management	
Access Management	Authentisierungs- und Authentifizierungs-Management Autorisierungs-Management	Starke Authentifizierung, Role-based Access Control, Single Sign-On/ Single Logout	Network Access Control, Policy Enforcement	
Information Protection		Level 1 Content Security	Information Rights Management, Level 2 Content Security, Secure Sharing	

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

IAMS-Lebenszyklus
→ Reifegradbetrachtung Teil 2

	Basic IdM	Advanced IdM	Professional IdM	Future IdM
Policies & Workflows	Level 1 Policy Management, Level 1 Workflow Management	Level 2 Policy Management, Level 2 Workflow Management	Level 3 Policy Managment, Level 3 Workflow Management	
Federation			Trust Management, Identity Federation	
Compliance & Audit	Level 1 Monitoring, Level 1 Reporting, Level 1 Auditing	Compliance Management, Level 2 Monitoring, Level 2 Reporting, Level 2 Auditing	Level 3 Monitoring, Level 3 Reporting, Level 3 Auditing	

- Zyklische Reifegradbetrachtung
  - Ebenso wie IdM / IAM ein dynamischer Prozess ist, so ist auch das technische System einer ständigen Erneuerung unterworfen

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

EIAM
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Definitionen
- Notwendigkeit
- Key Concepts
- IAMS-Lebenszyklus
- **Single Sign-On**
- Circle of Trust
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Single Sign-On
→ Überblick (1/2)

- Einmalige Authentifizierung → Nutzung weiterer Dienste ohne erneute Authentifizierung
- Sicherheitsgewinn, da nur noch ein Passwort genutzt werden muss, dass komplexer gewählt werden kann
- Komfortgewinn für den Nutzer

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

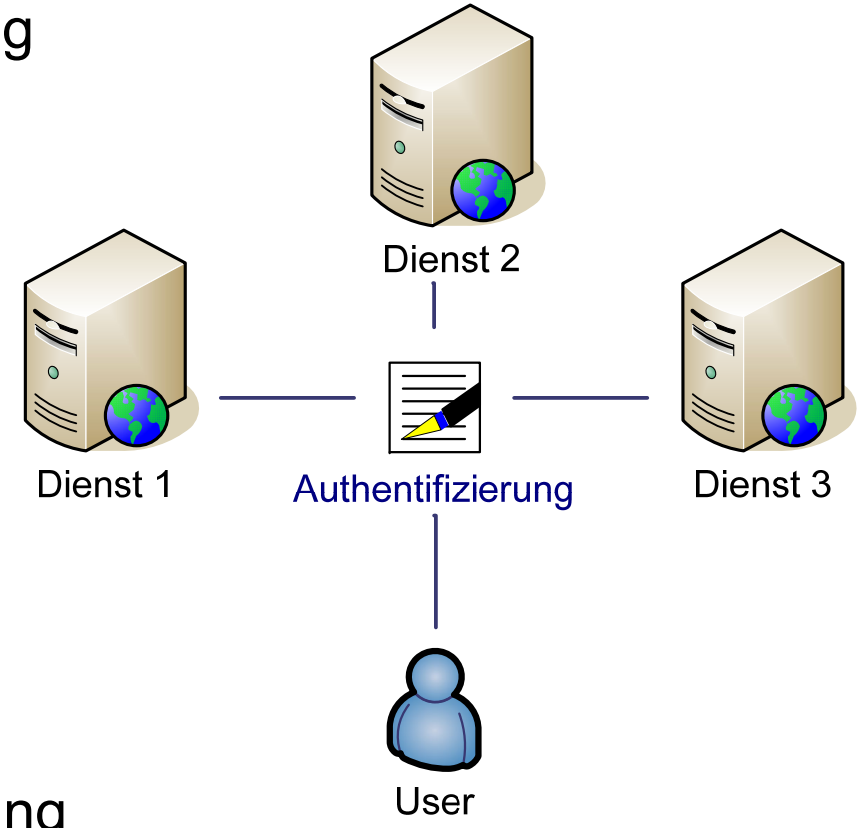
Single Sign-On
→ Überblick (2/2)

- Unterschiedliche Interpretationen:
  - Portallösung
    - Nutzung mehrerer Dienste innerhalb eines Portals
    - Nutzung von Cookies
    - Verbreitung besonders in Intranet Systemen
  - Ticketingsystem
    - Nutzer erhält Daten (Ticket) welche bei den angeschlossenen Servern bekannt sind
  - Lokale Lösung
    - Siehe "Unechtes SSO“

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Single Sign-On
→ Echtes SSO

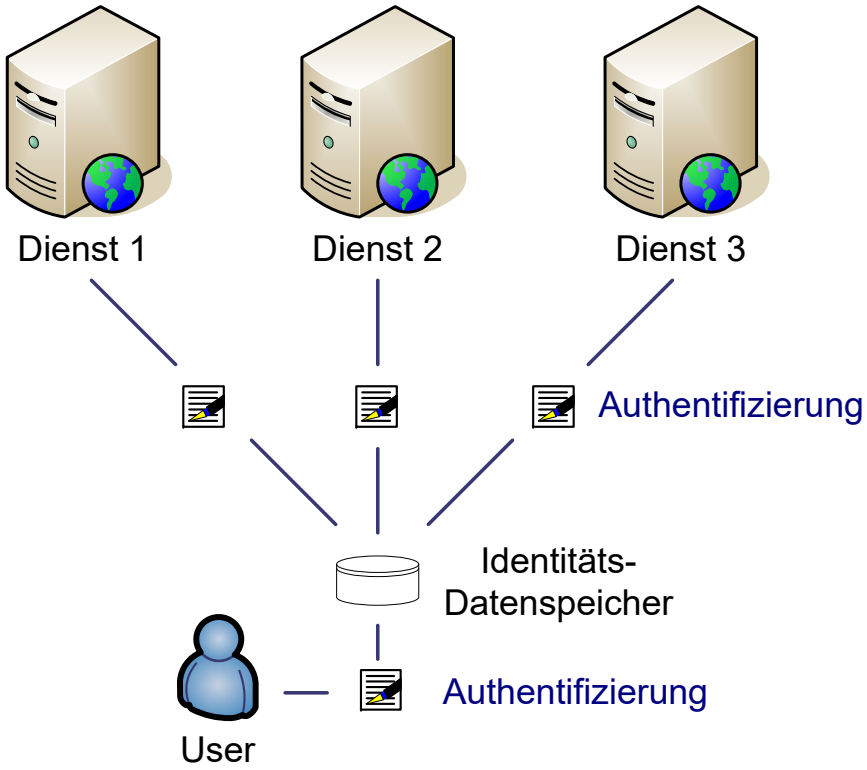
- Serverseitig implementiert
- Kommunikation der Server untereinander → Identity Federation
- Vorausgehende vertragliche Vereinbarung → Trust Management
- Vorteile:
  - Hoher Komfort
  - Hohe Sicherheit
  - Volle Mobilität
- Nachteile:
  - Aufwendige, komplexe Implementierung



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Single Sign-On
→ Unechtes SSO

- Identitätsdaten-Eingabe-Automatismus
- Einmalige Authentifizierung an einem Identitätsdatenspeicher (Software, USB-Stick)
- Clientseitig implementiert
- Anbieterunabhängig



- Vorteile:
  - Sofort einsetzbar
  - Technischer Aufwand gering
- Nachteile:
  - Plattform- & betriebssystemabhängig
  - Eingeschränkt mobil

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

EIAM
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Definitionen
- Notwendigkeit
- Key Concepts
- IAMS-Lebenszyklus
- Single Sign-On
- **Circle of Trust**
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Circle of Trust
→ Konzept (1/2)

- Konzept, um echtes Single Sign-On und weitere vernetzte Dienste anzubieten
- Basierend auf geschäftlichen Vereinbarungen zwischen Diensteanbietern (Einigung auf Technologie notwendig)
- Identity Providern
  - Stellt Authentifizierungsinfrastruktur
  - Vertrauenswürdigste Instanz innerhalb des Circle of Trust (CoT) für den Nutzer, da vom Nutzer gewählt
  - Kennt alle angeschlossenen Service Provider
  - Verwaltet die Identitätsinformationen des Nutzers

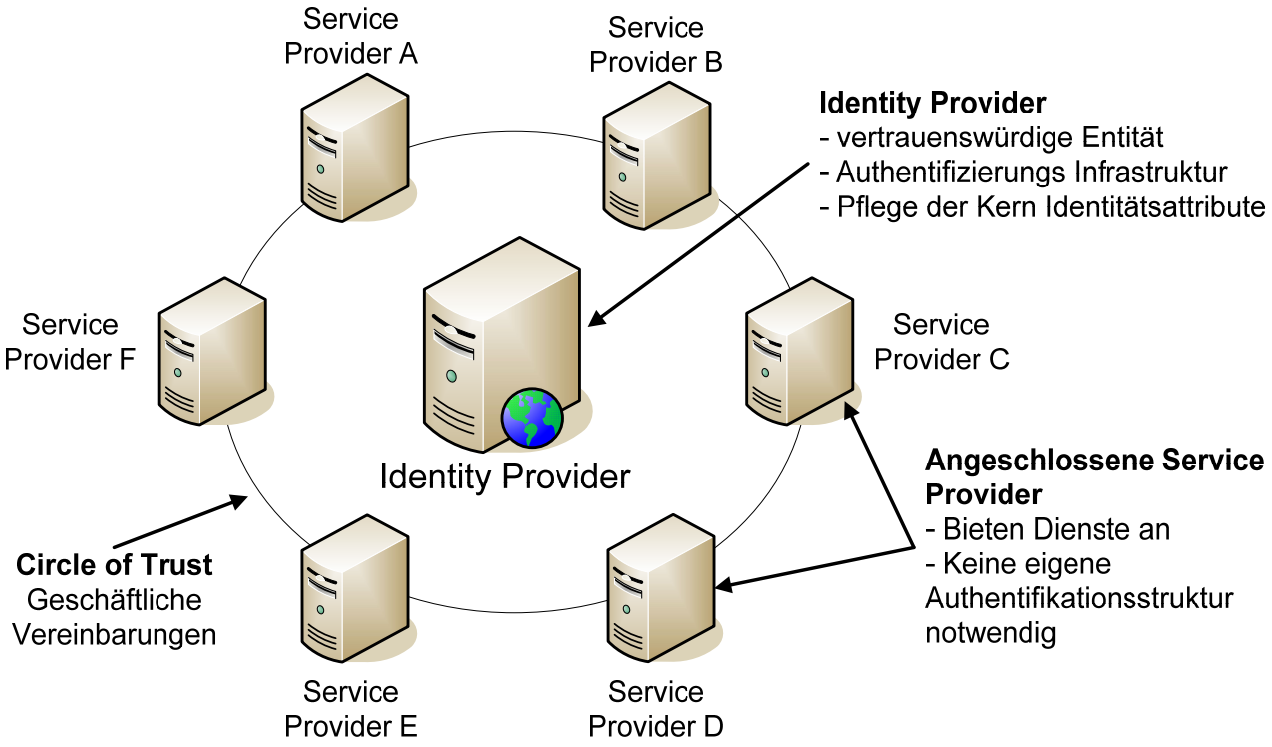
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Circle of Trust
→ Konzept (2/2)

- Service Providern
  - Diensteanbieter
  - Authentifizierungsinfrastruktur nicht notwendig
  - Kennt in der Grundform nur den Identity Provider

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Circle of Trust
→ Schema



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

EIAM
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Definitionen
- Notwendigkeit
- Key Concepts
- IAMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- **Zusammenfassung**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

EIAM
→ Zusammenfassung (1/2)

- Identity and Access Management Systeme (IAMS) vereinfachen den Umgang mit digitalen Identitäten, ihren Attributen und Berechtigungen enorm

- IAM ist ein sehr komplexes Thema – Ein Modell bring unterschiedliche Module in Einklang

- Zunehmend wird es wichtiger, Authentikationsverfahren zu verwenden, die in der globalen handelnden Gesellschaft über staatliche Grenzen und Verantwortungsbereiche hinaus verwendet werden können.
  → Dieser Anspruch aus der Vorlesung Authentikation wird durch IdMS unterstützt

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

EIAM
→ Zusammenfassung (2/2)

- Die Einführung und der Ausbau von IAMS und Ihrer Konzepte, wie Single Sign-On, sind aufgrund der stetig steigenden Anzahl von Identitäten unausweichlich
- Identitätsföderation ermöglicht sicheres organisationsübergreifendes Arbeiten von digitalen Identitäten
- Der Reifegrad des IAMS muss beachtet werden

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Enterprise Identity and Access Management (EIAM)

Prof. Dr. (TU NN)
Norbert Pohlmann

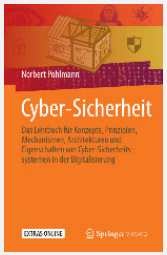
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Anhang / Credits

Wir empfehlen

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022
  https://norbert-pohlmann.com/cyber-sicherheit/



- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum

CYBER SCHUTZRAUM

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

MASTER internet-sicherheit.

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

https://twitter.com/ProfPohlmann

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Literatur
→ Artikel / Bücher

N. Heibel, M. Linnemann, N. Pohlmann: „Dokumente sicher im Griff: Sicheres Enterprise Rights Management“, IT SECURITY, März/April, 02/2008
https://norbert-pohlmann.com/wp-content/uploads/2015/08/220-Dokumente-sicher-im-Griff-Sicheres-Enterprise-Rights-Management-Prof-Norbert-Pohlmann.pdf

S. Feld, N. Pohlmann: „Security analysis of OpenID, followed by a reference implementation of an nPA-based OpenID provider”. In Proceedings of the ISSE 2010 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2010 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Vieweg-Teubner Verlag, Wiesbaden 2010
https://norbert-pohlmann.com/wp-content/uploads/2015/08/264-Security-analysis-of-OpenID-followed-by-a-reference-implementation-of-an-nPA-based-OpenID-provider-Prof-Norbert-Pohlmann.pdf

O. Achten, S. Feld, N. Pohlmann: „Identity Management als fortwährender Prozess – Mit Sicherheit zum Ziel“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 1/2010
https://norbert-pohlmann.com/wp-content/uploads/2015/08/253-Identity-Management-als-fortwährender-Prozess-Mit-Sicherheit-zum-Ziel-Prof-Norbert-Pohlmann.pdf

M. Gröne, N. Pohlmann: „Föderierte Autorisierung und ein Umdenken im Privilegienmanagement – Organisationsübergreifend arbeiten – aber sicher!“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 5/2010
https://norbert-pohlmann.com/wp-content/uploads/2015/08/267-Föderierte-Autorisierung-und-ein-Umdenken-im-Privilegienmanagement-–-Organisationsübergreifend-arbeiten-–-aber-sicher-Prof-Norbert-Pohlmann.pdf

N. Pohlmann: "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, ISBN 978-3-658-25397-4; 594 Seiten, Springer-Vieweg Verlag, Wiesbaden 2019
https://norbert-pohlmann.com/cyber-sicherheit/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen