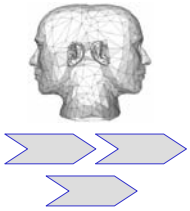
Strategische Ansätze und Best-Practices für Identity Management



Dr. Horst Walther, Vorsitzender des Kompetenzzentrums Identity Management der Nationalen Initiative für Informations- und Internet-Sicherheit (NIFIS), Deutschland

Expert Talk @ devoteam consulting

Radisson SAS Palais Hotel, 1010 Wien

Version 0.9

Ernste Warnung

Stoppen Sie mich – bevor es zu spät ist.

- Akute Powerpoint-Vergiftung ist eine weit verbreitete aber weithin unbekannte Zivilisationskrankheit.
- Sie tritt besonders bei ehrgeizigen Führungskräften und den durch sie Geführten auf.
- Sie ist durch eine Therapie aus frischer Luft, Sonne, absoluter Ruhe und einem Gläschen Wein leicht heilbar.

Synopse

11:20 - 12:00
Strategische Ansätze und Best-Practices für Identity Management
Dr. Horst Walther

- Die Aufgaben eines unternehmensweiten Identity Managements sind nicht neu.
- Die Verankerung in der organisatorischen Infrastruktur steht jedoch am Beginn.
- Der Vortrag erläutert, welche Strategie Unternehmen zur Lösung der vielfältigen Anforderungen verfolgen sollten.
- Dabei wird deutlich, dass Identity Management vielfach mit der prozessmäßigen Neuorientierung beginnt.
- Die technische Implementierung folgt als zweiter Schritt.

Agenda

Agenda

Was ist die NIFIS?

Nationale Initiative für Informations- und Internet-Sicherheit

Die NIFIS im Überblick

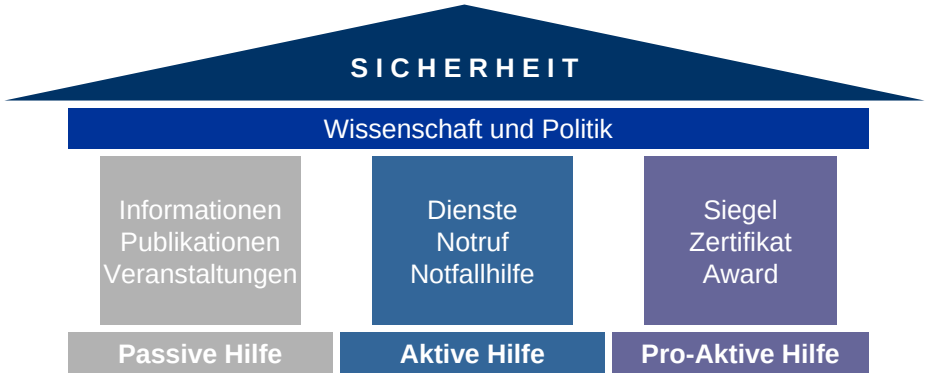
- Nicht gewinnorientierter, eingetragener Verein
  - Motto - „aus der Wirtschaft für die Wirtschaft“
  - Position - „neutrale, herstellerunabhängige Institution“
- Gegründet im Juni 2005 mit Sitz in Frankfurt am Main
- Mitglieder (Auszug):

Fraport, SIEMENS, DEKRA, OKI PRINTING SOLUTIONS, KPMG, interxion, Magirus IT advisorygroup, COMPUWARE, controlware communicationssystems, EVANGELISCHES KRANKENHAUS HAMM, clara.net, PHYSECURE

GenericIAM

Der Sicherheitsbedarf in Unternehmen

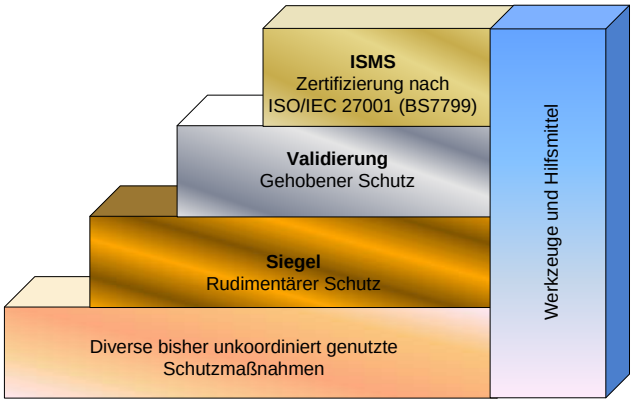
Sicherheit beginnt nicht erst beim Virenscanner und hört auch nicht an der Firewall auf:



GenericIAM

Die Sicherheitsstufen

Zwischen „keinem Schutz“ und einem „optimalen Schutz“ muss kein Vakuum sein:



Aufbau der NIFIS

Exekutivbeirat
- Fr. Dr. Krogmann MdB, CDU
- Hr. Otto MdB, FDP
- Fr. Stokar von Neuforn MdB, BÜNDNIS 90 DIE GRÜNEN
- Hr. Tauss MdB, SPD

Vorstand
Peter Knapp (Vors.)
Dr. Thomas Lapp (stellv. Vors.)
Brad Chapman
Mathias Gärtner

Wissenschaftlicher Beirat
- Hr. Prof. Dr. Heckmann
- Hr. Prof. Dr. Herberger
- Hr. Prof. Dr. Merle

Mitgliederversammlung

NIFIS ist primär Kompetenzzentrum für

- Informations-Sicherheits-Management-Systeme
- Identity Management
- Business Continuity Management
- Datenschutz
- Flächendeckende CERT-Infrastruktur
- Förderung sicherer IP-Kommunikation in Unternehmensnetzwerken
- Sicherheit von Rechenzentren und Informationstechnologie
- Sicherheit von Software-Anwendungen
- Sicherheit von VoIP

Agenda

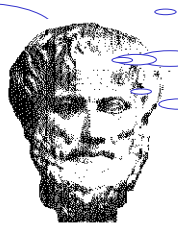
Wer ist die NIFIS?

Was verstehen wir unter Identity Management?

Vor welchen Herausforderungen steht das Identity Management?

Wer sollte im Unternehmen für Identity Management zuständig sein?

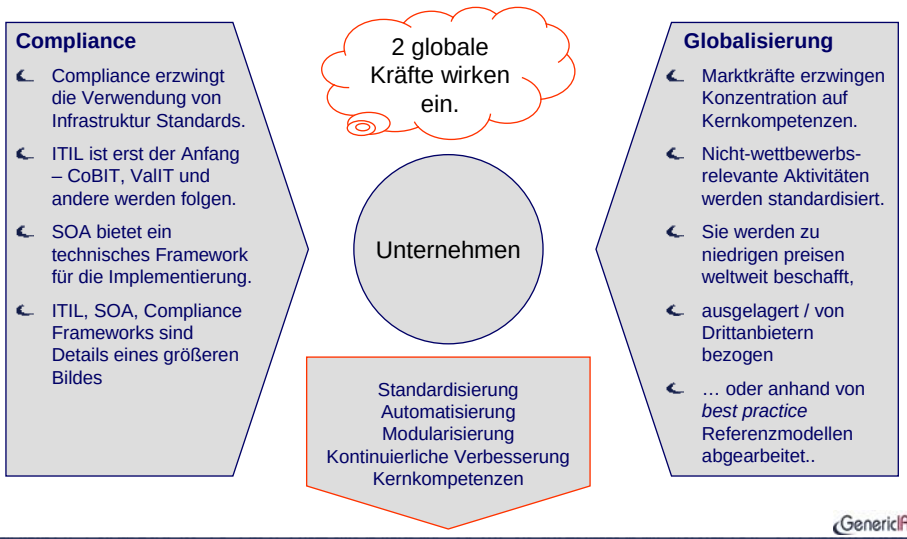
Was sind die größten Hindernisse für IdM-Projekte?



Welche Trends sind erkennbar?

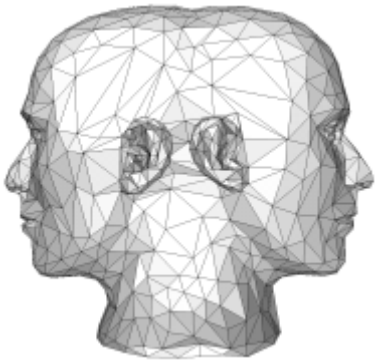
Was bleibt noch zu tun?

Vorab : Der Kontext
Die Industrialisierung der Dienstleistung



Begriffe rund um das Identity Management

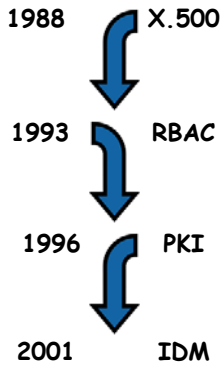
Definition
Identity Management – Was ist das?



- **Identity Management** (IdM) ist die ganzheitliche Behandlung digitaler Identitäten.
- **Identity & Access Management** (IAM) schließt auch die Verwaltung von Zugriffsrechten ein.
- Die Aufgaben des IAM sind **nicht neu** – sie sind seit Anbeginn mit den betrieblichen Abläufen fest verbunden.
- Neu ist die **übergreifende** Betrachtung …
  - Der einzelnen Disziplinen und
  - Über das gesamte Unternehmen hinweg
- IAM ist eine **Infrastrukturaufgabe** mit zu etwa gleichen Teilen …
  - Einer **fachlich** organisatorischen Komponente
  - Einer **technischen** Komponente und
- Dafür gibt es im klassischen Unternehmens-aufbau keine definierte „**Ownership**“

Die Wurzeln des Identity Managements
Erst die ganzheitliche Sicht führte zum Identity Management.

3 Unabhängige Quellen …



Historisch 3 unabhängige Strömungen ...

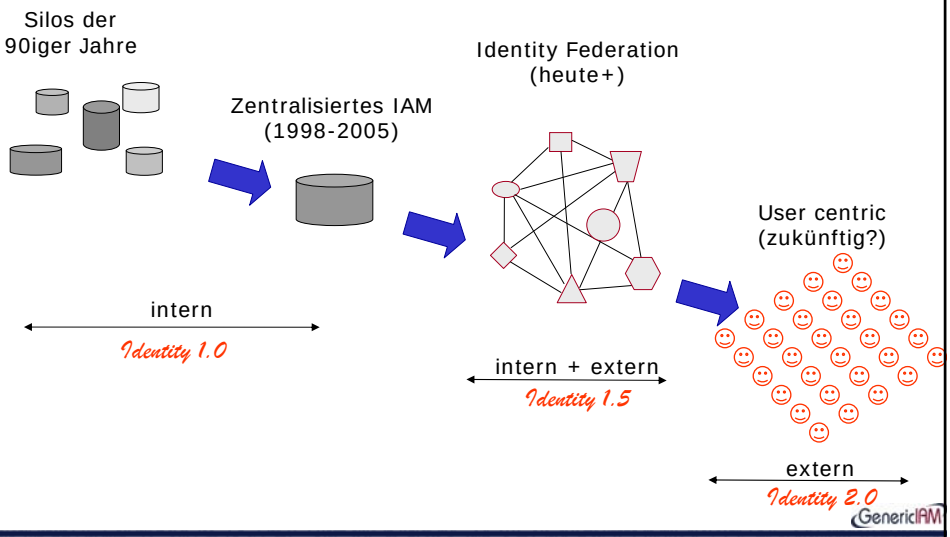
- Die Idee der public key infrastructure (**PKI**) für eine zertifikatsbasierte starke Authentisierung kann bis in das Jahr **1976** zurück verfolgt werden,
- Die CCITT[1] heute ITU-T[2] hat ihre 1. Spezifikation eines **X.500**- Verzeichnis-dienstes **1988** veröffentlicht.

  Die heute üblichen Verzeichnisdienste sind durch diese Entwicklung beeinflusst.
- 5 Jahre später startete das NIST[3] seine Arbeiten am *role based access control* (**RBAC**)[4].

[1] Comite Consultatif Internationale de Télégraphie et Téléphonie
[2] International Telecommunications Union-Telecommunication
[3] National Institute of Standards & Technology
[4] RABC: Role Based Access Control

➔ **Die verfügbaren Komponenten zeigen eine deutliche funktionale Überlappung und ergänzen sich nicht problemlos zu einer Identity Management Infrastruktur.**

Entwicklung des Identity Managements
Seither findet eine permanente Evolution statt.



Welchen Nutzen bringt Identity Management?

- Die Wirkung lässt sich in 3 Kategorien bewerten …
  1. Direkter Nutzen über die Amortisationsdauer
  2. Schadenvermeidung bei äußerem Zwang (z.B. Compliance)
  3. Risikobegrenzung bei potentiellen Schäden (Risiken)
- Direkter Nutzen entsteht durch …
  - Vermeidung unproduktiver Zeiten bei den Mitarbeitern
  - Verringerung der Kosten für die Belegarchivierung.
  - Verringerung von Administrationsaufwänden
- Schadenvermeidung ergibt sich …
  - Aus einem verbesserten *Rating* aufgrund verringerter operativer Risiken.
  - Vermeidung negativer Folgen von *Compliance-Überprüfungen*
  - Vermeidung von Totzeiten bei Übernahmen, *Mergers* und Kooperationen.
- Risikobegrenzung durch die erhöhte Sicherheit …
  - Entsteht vor allem durch ein schnelles und vollständiges *De-Provisioning*.
  - Eine modellbasierte und feingranulare Zugriffssteuerung
  - Die Möglichkeit einer vorbeugenden Risikoerkennung durch eine zentrale und schnelle Berechtigungsevidenz.

Agenda

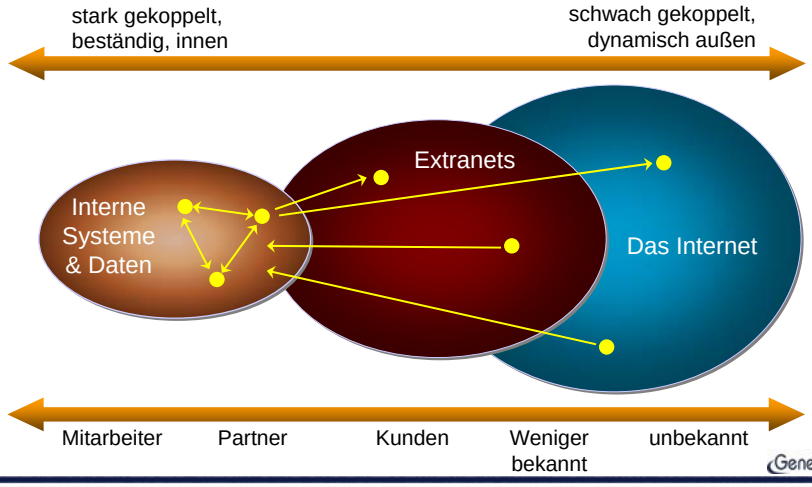
Warum ist Identity Management sinnvoll?

Treiber für die intensive Beschäftigung mit dem Thema.

- Das Denken in **kompletten Geschäftsprozessen** verlangt eine einheitliche Infrastruktur.
- Die **verschwimmenden Unternehmensgrenzen** machen eine neue Sicherheitsarchitektur erforderlich.
- Eine **unternehmensübergreifende** automatisierte Zusammenarbeit lässt sich nicht mit internen technischen Lösungen unterstützen.
- **Ressourcenvirtualisierungen** (SOA, Web-Services, Grid-Computing erfordern eindeutige digitale Identitäten und automatisierte Rechteprüfungen.
- Durch eine **steigende unternehmerische Dynamik** steigt der Bedarf nach Rollen- und Rechteänderungen stark an.
- Ein generell höheres **Sicherheitsbewusstsein** verbietet „gut gemeinte“ *workarounds* der Vergangenheit..
- **Externe Auflagen** wie SOX, „EuroSOX“, Basel II, … versuchen den Risiken elektronisch verketteter Geschäftsprozesse zu begegnen.
- Die **Industrialisierung der Dienstleistung** kommt nicht ohne digitale Identitäten aus.

Die e-Business-Herausforderung
Traditionelle Netzarchitekturen reichen nicht mehr aus.

- Interoperabilität *und* Portabilität: Im e-Business müssen Unternehmen ihr Inneres nach außen kehren



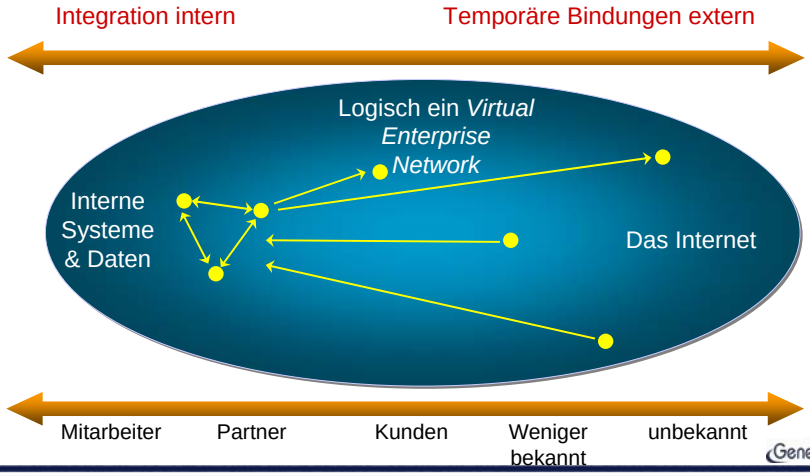
Die e-Business-Herausforderung
Die neuen Anforderungen erfüllen wir (noch) nicht.

- Die verschwimmenden Grenzen kehren das Innere nach außen …
  - Der Bedarf, das Netz zu „öffnen“ bescheren uns zwei **gegenläufige Erfordernisse** flexibleren Zugang und höhere Sicherheit
  - Sicherheitsmaßnahmen **über** logische und physische **Grenzen hinweg**.
  - Anwendungen, Datenbanken und Betriebssystemen **fehlt ein** skalierbarer und ganzheitlicher Mechanismus, um Identitäten, Zertifikate und Geschäftsregeln über alle Grenzen hinweg zu verwalten.
  - **Wireless-** und andere Endgeräte erhöhen die Komplexität
  - Von falsch verstandenem “**SSO**” gehen Gefahren aus.
  - Die unvermeidbare **Überschneidung** von öffentlichen und privaten Identity Strukturen kompliziert diesen komplexen Fall weiter.
  - Traditionelle Netzwerkarchitekturen **behindern das Geschäft**:
    - „Der Firewall ist tot!“

Die Antwort – *Virtual Enterprise Network*

Geschützte Assets anstelle von Burgmauern.

- Die Antwort: Eine identitätsbasierte flexible Infrastruktur



Das Festungsdenken reicht nicht mehr

Das Festungsdenken ist dem e-Business nicht mehr angemessen

- Es versagt in dem Maße, wie Anwendungen für Partner und Kunden geöffnet werden.
- Firewalls allein reichen nicht mehr aus
- Vergabe (und Entzug) von Schlüsseln für den Zutritt im Hotel
- Gesicherte Safes mit begrenztem Zugriff “hinter dem Tresen”
- Sicherheitspersonal patrouilliert.

Gestern
Festungs-Modell

Heute
Hotel-Modell

Geht es nur um Sicherheit?
Die Barings Bank – ein Beispiel.

- 1995 ging die Barings-Bank zum Preis von **einem Pfund** an den holländischen ING-Konzern.
- Die Bank der britischen Könige war seit war seit 1762 eine der feinsten Londoner Adressen.
- Bis 1992 Nick Leeson in Singapur begann Preisdifferenzen zwischen japanischen Derivaten auszunutzen.
- Es entstand ein Verlust von **1,4 Milliarden** Dollar.
- Leeson wurde wegen Urkunden-fälschung, Untreue und Betrugs zu **6 ½ Jahren Haft** verurteilt.
- Leeson hatte den Handel mit Finanzderivaten in Singapur **und** die Back-Office Funktionen wo die Trades kontrolliert wurden, geleitet.

  - ein **katastrophaler Mix.**

➢ **Eine rollenbasierte Aufgaben-trennung hätte weniger gekostet.**

10 top compliance issues
Was Wirtschaftsprüfer am häufigsten bemängeln

1. Nicht erkannte oder nicht gelöste **segregation of duties** (SOD) **Verletzungen.**
2. Betriebssystem Zugriffsmöglichkeiten zu Finanzanwendungen oder zum Portal nicht gesichert - **lassen Hintertüren offen.**
3. Datenbank- (e.g. Oracle) Zugriffsmöglichkeiten zu Finanzanwendungen (z.B.: SAP, Oracle, Peoplesoft, JDE) nicht gesichert - **lassen Hintertüren offen.**
4. **Entwickler** können fachliche Anwendungen in der Produktion laufen lassen.
5. Eine zu große Zahl an Berechtigungen für "**super user**" Transaktionen in Produktion.
6. Ehemalige Angestellte oder Berater **haben noch Zugriff.**
7. **Erfassungszeiten** in FiBu-Anwendungen **nicht beschränkt**.
8. Add-ons, Parametrisierungen, Tabellen & Interfaces sind **nicht gesichert.**
9. **Verfahren** für manuelle Prozesse **existieren nicht** oder werde nicht eingehalten.
10. Die System-**Dokumentation** beschreibt nicht den aktuellen Prozess.

Nutzen von Identity Management
Was sagen die Analysten?

„Der eigentliche Nutzen von Identity Management ist nicht IT-Sicherheit, sondern die Fähigkeit, Geschäftsprozesse, Workflows, Kundenbeziehungen, Menschenführung und Schutz des Privaten zu verbessern und dynamisch an veränderte Situationen anzupassen.

Management by Identity schafft Vertrauen – die Grundlage der Wirtschaft in einer digitalen Welt.“

Martin Kuppinger, KCP

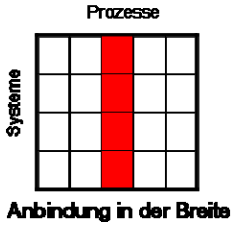
Projektproblematik – wo beginnen?
Ein schrittweises Vorgehen ist erforderlich

- **Operative** Bereiche fordern Komfortverbesserung ...
  - Single-sign-on
  - Self-Service
  - (schnelles) Provisioning
- Revision, Security, Compliance fordern ...
  - Transparenz (**Evidenz**)
  - Report & Analysen
  - Incident alerts
  - Sauberes & schnelles De-Provisioning
- Berechtigungssituation oft nicht bekannt ...
  - Befragungen helfen oft nicht weiter
  - Analysen sind erforderlich
  - Sie „enthüllt ihr Gesicht“ oft erst im Umsetzungs-Projekt.
  - Risiken für die Umsetzung

➔ Identity Management Projekte können sehr komplex werden. Risiko begrenzende Maßnahmen sind von Beginn an erforderlich.

Einführung Tiefe vs. Breite

Welches Vorgehen verspricht den höchsten Nutzen?



- Durchstich in der Tiefe wenn ...
  - Einige wenige Systeme gut angebunden
  - Rechtesituation gut bekannt
  - bidirektionale Anbindung technisch vorhanden
  - Wichtige Massensysteme:
    - Windows
    - Exchange
    - Lotus NOTES
  - Systemneueinführung
- Evidenzbildung in der Breite wenn ...
  - Eine zentrale Benutzerverwaltung aufgebaut werden soll
  - Sicherheits- und Compliance-Erwägungen im Vordergrund stehen.
  - Viele wichtige und wenig bekannte Altsysteme angebunden werden sollen.

➔ Bei gewachsenen Systemlandschaften lassen sich nicht alle Systeme in einem Schritt einbinden.

Evidenzbildung – Einführung in der Breite

- Vorteile
  - Aufbau eines Benutzermanagement möglich.
  - Schneller Überblick über viele Systeme
  - Auskunftsfähigkeit
  - *Compliance* schnell erreichbar
  - Gut schrittweise einbindbar (viele kleine Erfolge → geringes Projektrisiko)
  - Enthüllt Berechtigungs- und User-Mapping-Komplexität in dispositiven Prozessen.
  - Macht den Erfolg nachfolgend eingeführter operativer Prozessunterstützung messbar transparent.
  - Macht die Revision zum Verbündeten

➔ ... schaltet „das Licht ein“.

Evidenzbildung – Einführung in der Breite

- Nachteile
  - Es sind noch keine operativen Prozesse automatisiert
    - Kein single sign-on
    - Kein Provisioning
    - Keine einheitliche ID
  - Abbildungsregeln sind oft sehr aufwändig
    - Unterschiedliche ID-Konventionen HMeyer, MeyerH, Hans.Meyer, ...
    - Unterschiedliche Schreibweisen Möller, Moeller, Møller, ...
    - Unterschiedliche Verlässlichkeit der Quellen
    - Behandelte Ausnahmen ausblenden
  - Abgleich mit Soll-Beständen erforderlich
    - HR-Daten, Soll-Berechtigungen, Lizenzen,
    - Zur Erkennung von Ausnahmen (Schattenkonten, Unter-, Überberechtigungen)
    - Erst dann der volle Nutzen
  - Die Mapping-Regeln sind sehr unternehmensspezifisch

➔ **... schafft einen ordnungsmäßigen Zustand – aber nicht mehr.**

Agenda

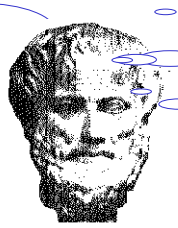
Wer ist die NIFIS?

Was verstehen wir unter Identity Management?

Vor welchen Herausforderungen steht das Identity Management?

Wer sollte im Unternehmen für Identity Management zuständig sein?

Was sind die größten Hindernisse für IdM-Projekte?



Welche Trends sind erkennbar?

Was bleibt noch zu tun?

6 Ursachen für das Scheitern von IAM-Projekten
Wie sie Wirtschaftsprüfer berichten

Identity- und Access Management Projekte schlagen fehl weil …

- die Beteiligten **unterschiedliche Sprachen** sprechen,
- in **Organisationen** ist oft nicht klar, wer …
  - verantwortlich und
  - operativ zuständig ist,
- Referenzmodelle wie COSO einen **top-down**-Ansatz verfolgen, die meisten Organisationen aber **verteilt** arbeiten,
- technische **Inkompatibilitäten** der meisten heutigen Systeme es schwer die machen gesamte Autorisierungslandschaft zu managen,
- **Segregation of duty** (SOD) mit der aktuellen *state-of-the-art*-Technik nur schwer zu erreichen ist,
- Die **geringe Sichtbarkeit** des IAM es erschwert, ausreichende Budgetmittel zu erhalten.

Komplexitätsfaktoren ...
Was macht IdM-Projekte so schwierig?

- Bestehende Lösungen
  - Je **mehr bestehende** Lösungen für das Identity Management existieren, umso höher wird der Aufwand, sie zu harmonisieren und zu ersetzen.
  - **Je reifer** die existierenden Lösungen sind, umso schwerer finden neue Ansätze Akzeptanz.
- Querschnittscharakter
  - Identity-Management Prozesse sind typischerweise **bereichsübergreifend**.
  - Es sind **viele** gleichberechtigte **Stakeholder** in ein Projekt involviert.
  - 3 bis 5 mal höhere **Kommunikationskomplexität** zu „normaler“ SW-Entwicklung.
  - Typischer **Change** Management Prozess: Macht-Sponsor erforderlich!
- Prozessreife
  - Je höher die **Reife** der Management-Prozesse (z.B. nach CMMI) umso leichter fällt die Einführung von IAM-Prozessen, -Regeln, -Rollen, -Policies.
  - Reife IAM-Prozesse in einem **unreifen Prozess-Umfeld** finden wenig Akzeptanz (Aufwandstreiber).
- Projektzuschnitt
  - SW-Implementierungsprojekte sind **überfordert**, wenn sie die organisatorischen Voraussetzungen erst schaffen müssen
  - Prozess- und Rollen-Definitionen erfordern eigene **Definitionsprojekte** vor der oder parallel zur Implementierung.
- Marktkonsolidierung
  - Mergers & Acquisitions führen zu wenig kompatiblen **Produktsammlungen**.
  - Die Software übernommener Unternehmen wird häufig nicht mehr optimal **unterstützt**.

… Komplexitätsfaktoren
Was macht IdM-Projekte so schwierig?

- Technische Risiken
  - IAM-SW-Suiten sind **komplex** und schwer zu handhaben.
  - Ohne **Implementierungs-erfahrung** in exakt der geforderten Umgebung sind die Projektrisiken nicht kalkulierbar.
  - Hinter „harmlosen“ Versions-sprüngen (z.B.: 5.6 auf 6.0) stecken oft komplette **Neuent-wicklungen**.
  - Die Matrix der vom Hersteller unterstützten **Komponenten** vs. Version ist of sehr dünn besetzt.
  - Ersatz von Infrastruktur-Komponenten führt oft zu hohem **Aufwand**.
- Verfügbarkeit von Fachspezialisten
  - Verfügbarkeit von Fachpersonen mit **Domänen-Wissen** ist oft der Engpass-Faktur bei Rollen- und Prozess-Definitionen.
  - Sie werden in der **Anforderungs-definition** und der **QS** benötigt.
  - Wartezeiten (auf Spezialisten) sind Aufwandstreiber.
- From scratch vs. Templates
  - Nur ein Teil der IAM-Prozesse ist wirklich **unternehmensspezifisch**.
  - Die **Übernahme** von Prozessen und / oder Rollen aus generischen Modellen kann Projekte beschleunigen.

Die Motivation für NIFIS GenericIAM
Gesucht: ein Baukasten für Standardprozesse des IAM

Die Idee hinter GenericIAM

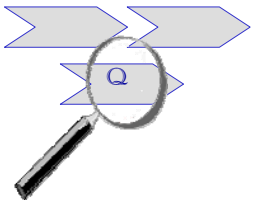
- Prozesse verursachen den meisten Aufwand.
  - so gehen bei PKI-Projekten 2/3 des Aufwandes in die Prozesse.
- Warum mit einem weißen Blatt Papier beginnen?
- Warum, das Rad immer wieder neu erfinden?
- Gibt es nicht auffällige fachliche Ähnlichkeiten?
- Sollten wir uns nicht lieber auf die Unterschiede konzentrieren?
  - ... Und das Gemeinsame „von der Stange“ verwenden?

Agenda

Mission von NIFIS GenericIAM

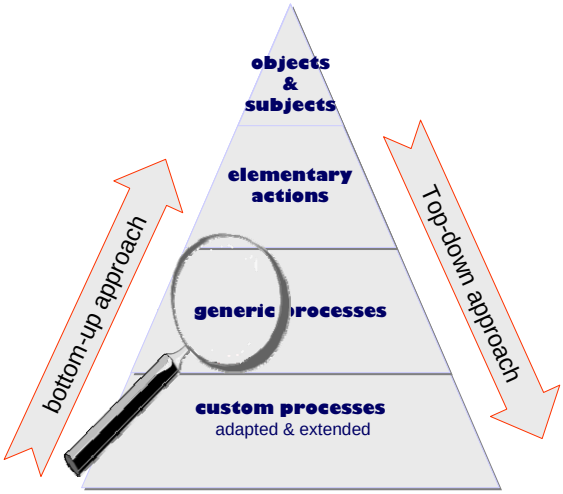
Welchen Auftrag haben wir uns gegeben?

- Wir haben das **Ziel**, für das Identity- und Access Managements (IAM) ein allgemein verwendbares (generisches) **Prozessmodell** zu entwickeln.
- Es soll als Vorlage für unternehmensspezifische **Prozesse** dienen.
- Es soll in manchen Fällen auch unmittelbar **implementiert** werden können.
- Diese Prozesse sollen eine definierte, hohe und angemessene **Qualität** aufweisen.
- Sie sollen zu den gängigen regulatorischen Anforderungen "**compliant**" sein.



Der NIFIS GenericIAM Modellierungsansatz

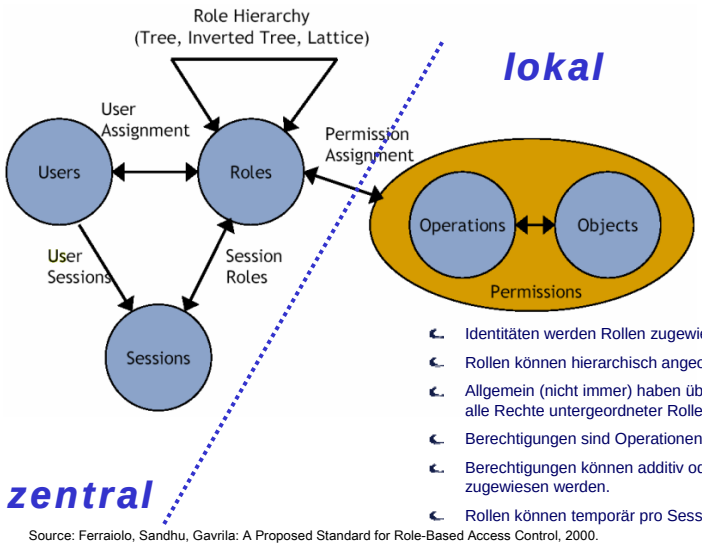
bottom-up- und top-down-Ansatz führen zu einem generischen Modell



GenericIAM

Zentral vs. Lokal

IDs & Rollen haben zentralen, Berechtigungen lokalen Charakter.

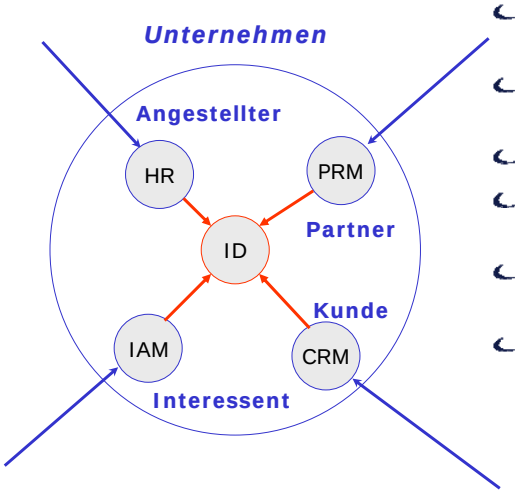


- Identitäten werden Rollen zugewiesen
- Rollen können hierarchisch angeordnet sein.
- Allgemein (nicht immer) haben übergeordnete Rollen alle Rechte untergeordneter Rollen
- Berechtigungen sind Operationen auf Objekte.
- Berechtigungen können additiv oder subtraktiv zugewiesen werden.
- Rollen können temporär pro Session gelten.

Source: Ferraiolo, Sandhu, Gavrila: A Proposed Standard for Role-Based Access Control, 2000.

Die zentrale digitale Identität

Wann immer ein Individuum die Unternehmensgrenze passiert …



- Wird seine digitale Identität erzeugt
- Unabhängig ob es als *User* wirkt oder nicht.
- User bedeutet bereits eine Rolle.
- Die digitale Identität ist sein digitales Abbild
- Seine Lebenszeit bestimmt auch die seiner digitalen Identität.
- Seine digitalen Identität ist global und eindeutig.
  - Bereits die Wirkung der Biometrie bedenken!

Trends des Identity Managements

Welche wesentlichen Entwicklungen sind zu erwarten?

- Service Orientierung
- End-to-end-auditing
- User centric Identity Management
- Verschmelzung von klassischer und *federated* IdM
- Standardisierung über Referenzmodelle
- IdM etabliert sich auf Business Ebene

➔ **Der große Kontext heißt: „*Industrialisierung der Dienstleistung*“.**

Agenda

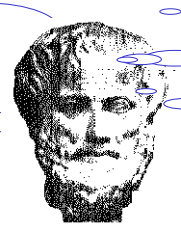
Wer ist die NIFIS?

Was verstehen wir unter Identity Management?

Vor welchen Herausforderungen steht das Identity Management?

Wer sollte im Unternehmen für Identity Management zuständig sein?

Was sind die größten Hindernisse für IdM-Projekte?



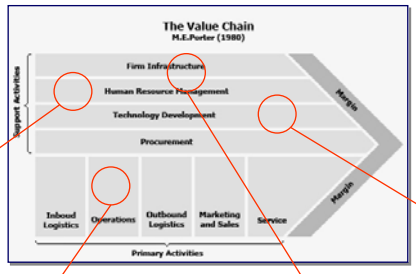
Welche Trends sind erkennbar?

Was bleibt noch zu tun?

GenericIAM

Verantwortung

Wer sollte im Unternehmen für Identity Management zuständig sein?



HR

- ✓ hat eine natürliche Affinität zu Personen
- \- Relativ businessfern
- \- Zeitverhalten nicht gerade real time.

Business

- ✓ Verantwortung und Aufgaben decken sich.
- \- Nicht Unternehmens-übergreifend
- \- Spezialwissen fehlt.

neue Funktion

- \- Noch ohne Beispiel
- • Muss für Identitäten, Rollen & Prozesse zuständig sein
- • Braucht organisatorisches und technisches Wissen
- • Braucht Gestaltungsmandat
- ✓ Chance für ein maßgeschneidertes Design

IT

- ✓ Technisches Umsetzungswissen ist vorhanden
- \- Mandat für Unter-nehmensgestaltung fehlt.
- \- Organisation ist nicht Technik.

Agenda

Vorgaben für das Identity- & Access Management

Wie sollte die IAM-Landschaft aussehen.

- **IAM-Strategie** – Es ist eine verbindliche und gelebte IAM-Strategie nötig. Sie muss konkret und umsetzungsorientiert formuliert sein.
- **zentrale Identity** - Die *digital identity* sollte unternehmenszentral geführt werden. Das entspricht dem Unternehmensinteresse und ermöglicht zentrale Forderungen zu erfüllen.
- **zentrale Rollen** - Rollen (in der geeigneten Definition) drücken die Beziehung einer Person zum Unternehmen aus. Sie sind von zentralem Interesse
- **dezentrale Berechtigungen** - Access-Informationen drücken das aus, was eine Rolle pro System darf. Sie haben (eher) lokalen Charakter. Sie müssen aber für Compliance- und Security-Zwecke zentral auswertbar sein.
- **zentrale IAM-Ownership** - Damit Prozesse, Definitionen, Schnittstellen des IAM sich nicht auseinanderentwickeln ist eine definierte Zuständigkeit erforderlich.
- Unternehmensweit **hohe Prozessreife** schaffen: Sie können keine Inseln der Ordnung in einem Meer von Chaos schaffen.

Questions - comments – suggestions?

GenericIAM

Lunch break

GenericIAM

Caution Appendix

Here the notorious back-up-slides follow ...