AdNovum

Identity & Access Management

Aktuelle Herausforderungen und Konzepte

Christof Dornbierer
CTO

22. September 2010

NEVIS

security zone
PLATTFORM FÜR INFORMATIONSSICHERHEIT


Passt Ihre Software?

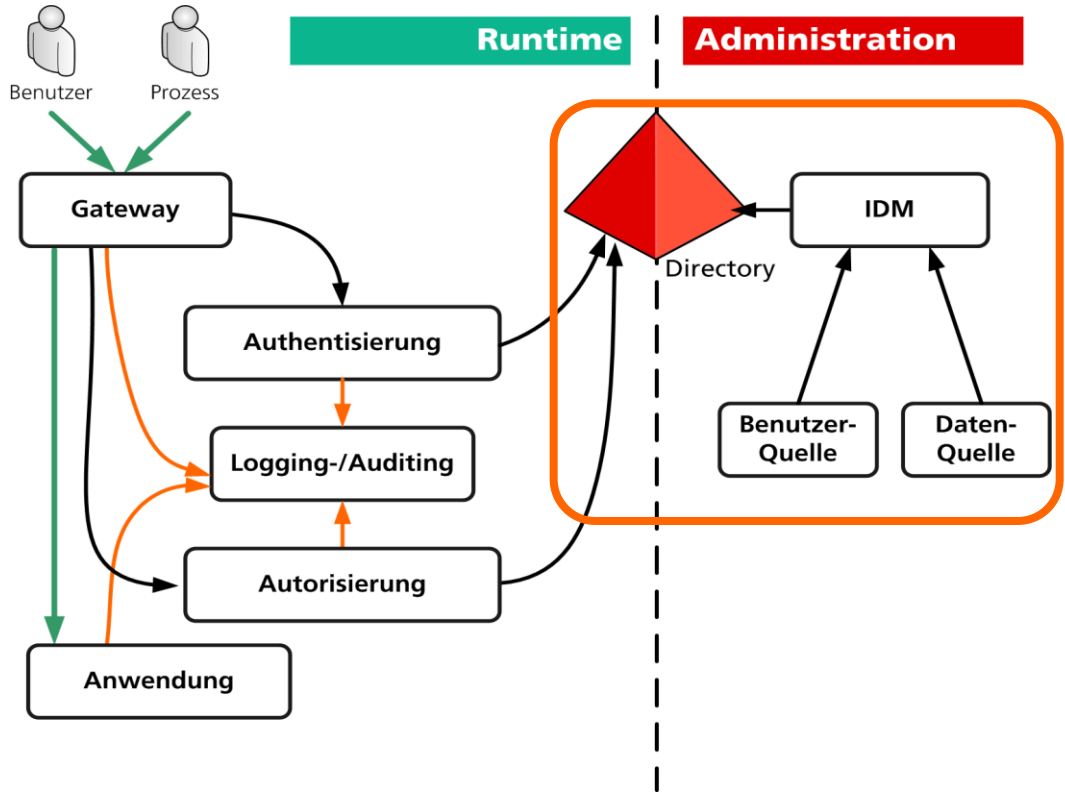
IAM & SSO – Big Picture

Online-Architektur

- Trennung **Runtime & Admin**
- Security ausserhalb Anwendung

Modulare Infrastruktur

- Gateway (Reverse Proxy & WAF) als **zentraler Einstiegspunkt**
- Authentisierung, IDM & Directory



Wazu ein Identity-Management-System?

Aktuelle Herausforderungen in verteilten Systemen I

Konsistenz

- Sind alle Benutzer in **allen Systemen** erfasst?
- Sind die Benutzerdaten **konsistent**? (Maier vs. Meier vs. Meyer)

Nachvollziehbarkeit & Compliance

- Auf **welche Systeme** dürfen die Benutzer überhaupt zugreifen?
- Wer durfte am 24. August 2005 auf das System zugreifen und eine bestimmte Transaktion ausführen?

Viele Passwörter & Benutzerkonten

- Jedes System hat seine eigenen Passwort-Richtlinien

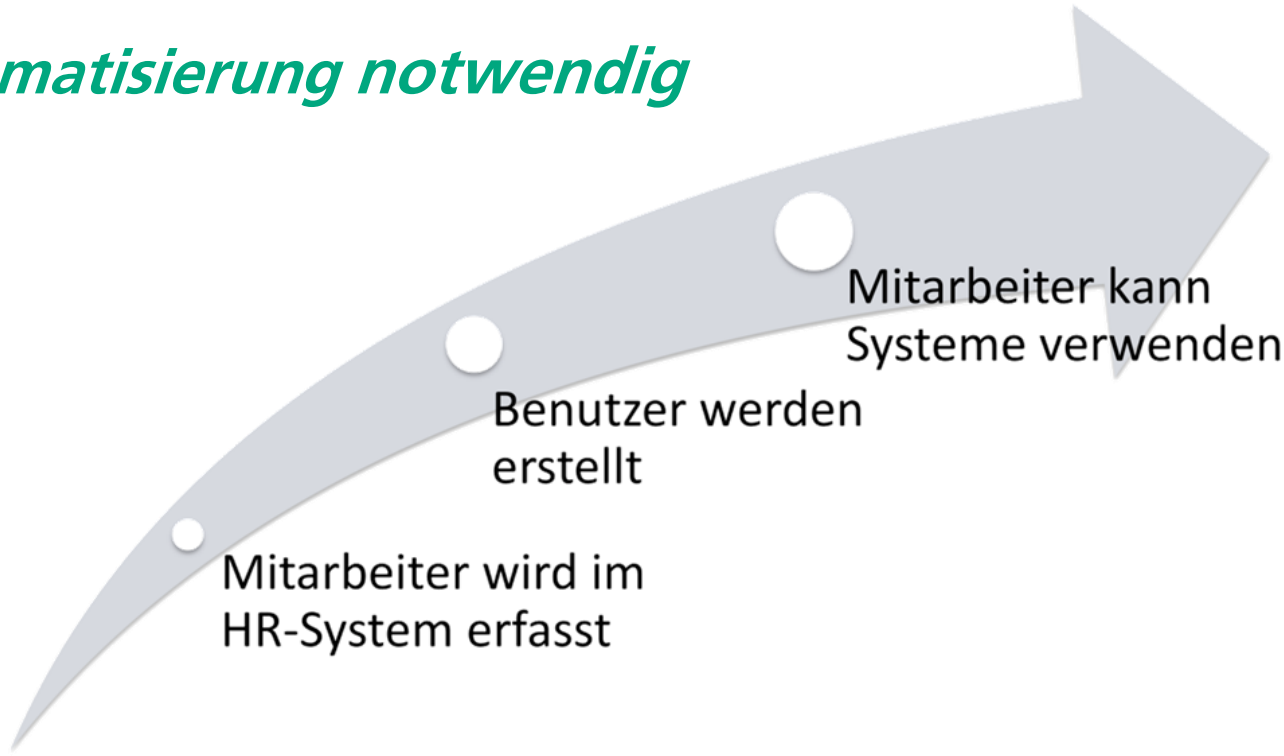
→ Benutzer muss sich **diverse Passwörter** und Benutzernamen merken.

Aktuelle Herausforderungen in verteilten Systemen II

Keine Einbindung in Unternehmensprozesse

- Wurde der Benutzer nach dem Austritt aus der Firma auch in allen Systemen deaktiviert?
- Kann ein Mitarbeiter **ab Tag 1** in der Firma auf die benötigten Systeme zugreifen?

→ ***Automatisierung notwendig***

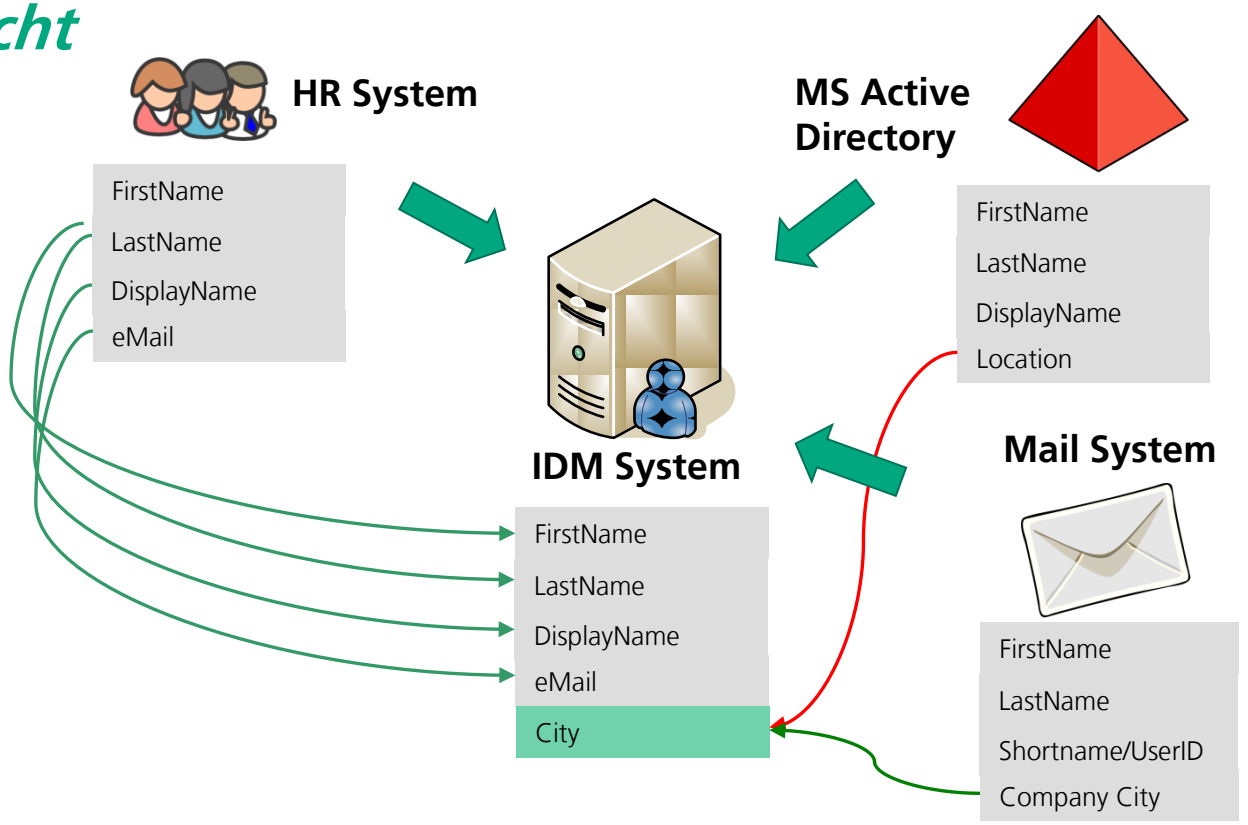


Identity-Management-Konzepte I

Identitätskonsolidierung

- Sammlung und Abgleich von Identitätsinformationen
- Klare Definition von Master-Systemen pro Attribut

→ *Konsolidierte Sicht*

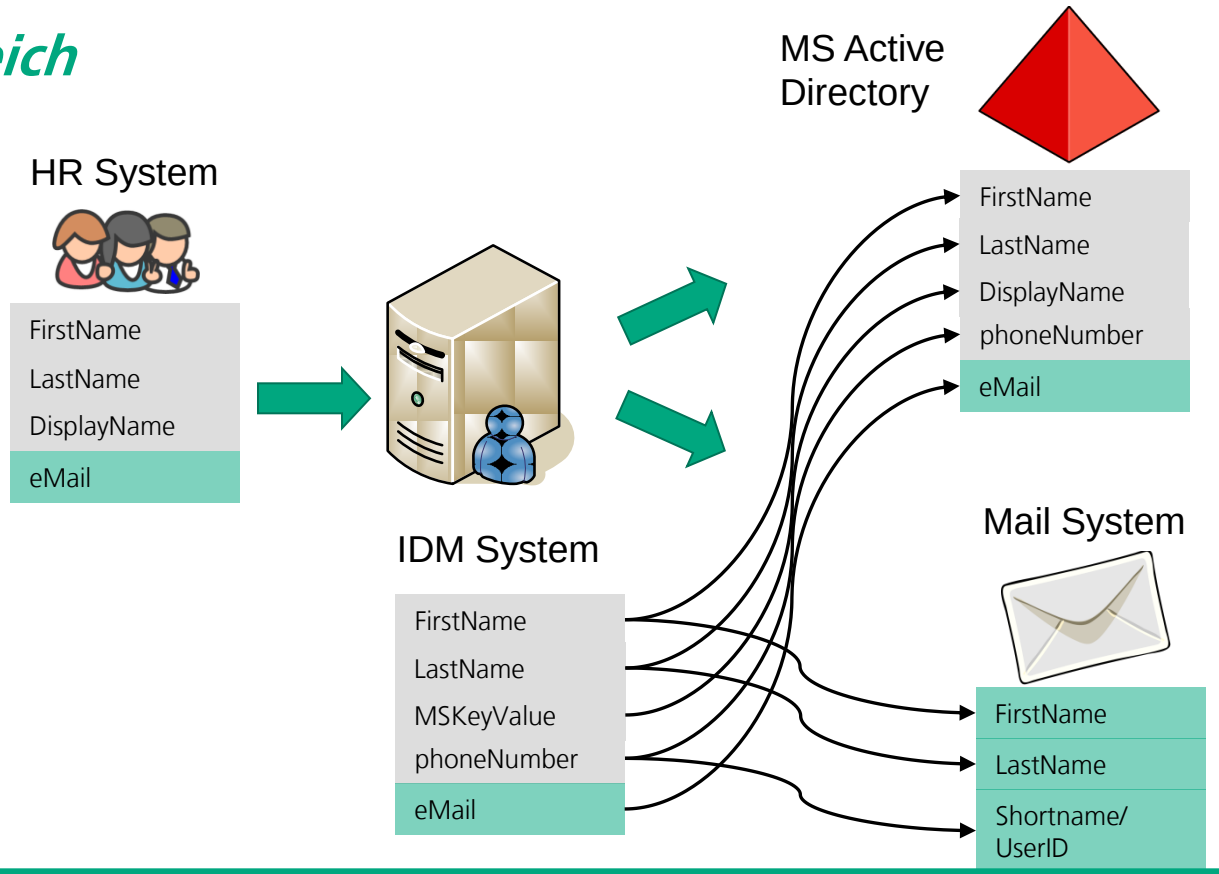


Identity-Management-Konzepte II

Provisionierung / De-Provisionierung von Informationen

- Automatisches Erstellen/Deaktivieren von Benutzern in Systemen
- "Push" von anderen Informationen zu Zielsystemen

→ ***Automatisierter Abgleich***

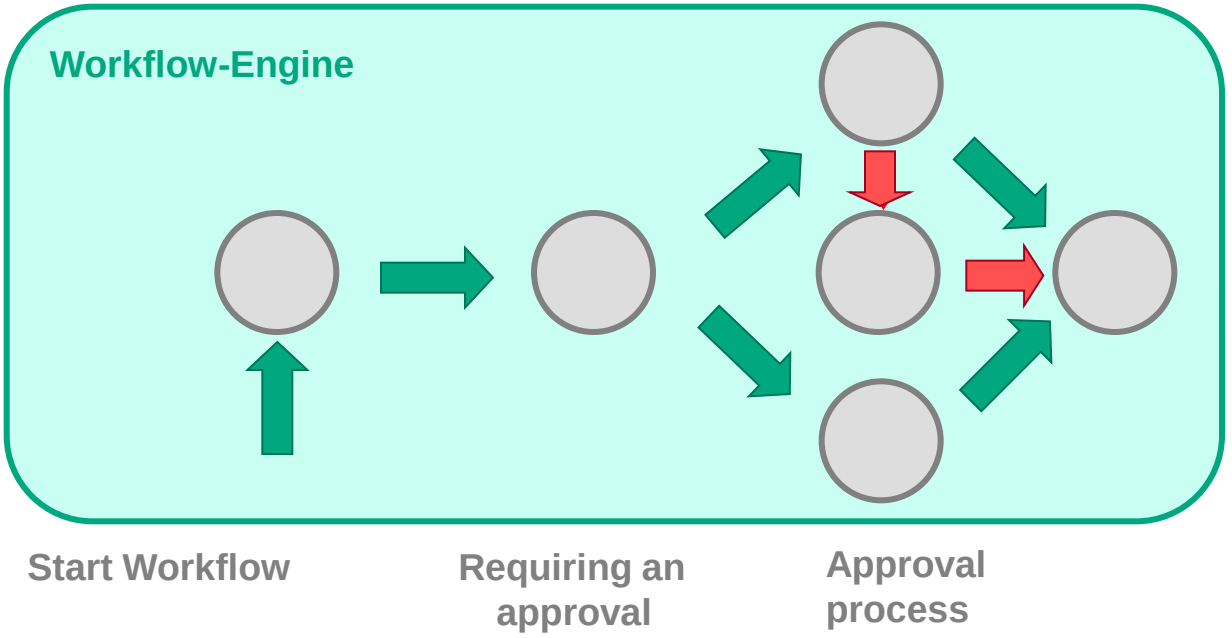


Identity-Management-Konzepte III

Provisionierung / De-Provisionierung von Informationen

- Elektronische Unterstützung von internen Prozessen rund um Identitäten
- Ersetzt zum grossen Teil papierformular-basierte Prozesse
- Beispiele: Freigabe von Rollen, Bestätigung von Berechtigungen, …

→ ***Nachvollziehbarkeit / Vereinfachung***

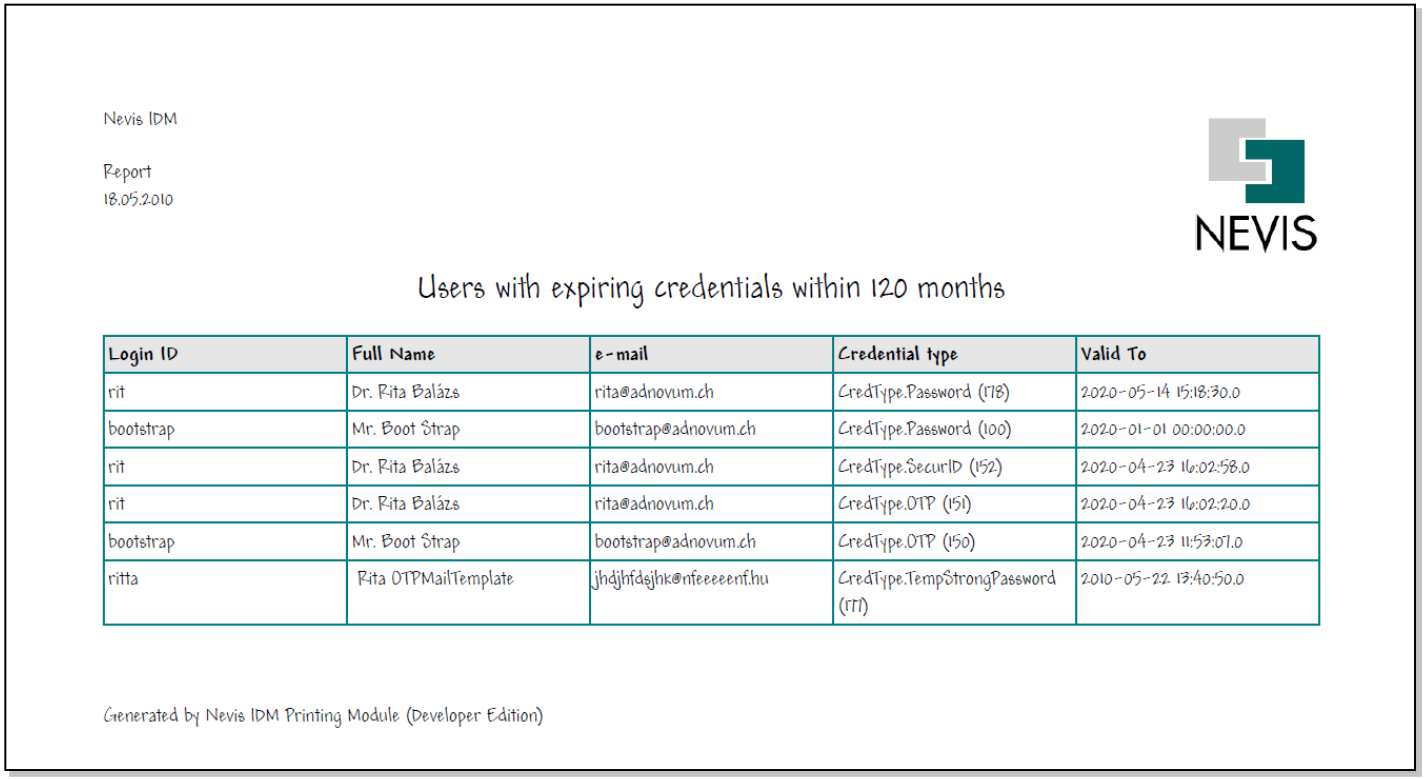


Identity-Management-Konzepte IV

Rollenmanagement & Reporting

- Verwalten von Rollenhierarchien
- Automatische Zuweisung von Rollen und Berechtigungen
- Reporting bzgl. Rollenzuweisungen und Berechtigungen

→ ***Auditfähigkeit***



Nevis IDM

Report
18.05.2010

NEVIS

Users with expiring credentials within 120 months

Login ID	Full Name	e-mail	Credential type	Valid To
rit	Dr. Rita Balázs	rita@adnovum.ch	CredType.Password (118)	2020-05-14 15:18:30.0
bootstrap	Mr. Boot Strap	bootstrap@adnovum.ch	CredType.Password (100)	2020-01-01 00:00:00.0
rit	Dr. Rita Balázs	rita@adnovum.ch	CredType.SecurID (152)	2020-04-23 16:02:58.0
rit	Dr. Rita Balázs	rita@adnovum.ch	CredType.OTP (151)	2020-04-23 16:02:20.0
bootstrap	Mr. Boot Strap	bootstrap@adnovum.ch	CredType.OTP (150)	2020-04-23 11:53:01.0
ritta	Rita OTPMailTemplate	jhdjhfdsjhk@nfeeeeenf.hu	CredType.TempStrongPassword (111)	2010-05-22 13:40:50.0

Generated by Nevis IDM Printing Module (Developer Edition)

Aktuelle Themen und Umsetzung

Aktuelle Themen

- Nachvollziehbarkeit / Audit-Fähigkeit / Reporting
- Automatisierung → Konsistenz der Daten
- Self Service / Delegated Administration
- Role Management / Segregation of Duties

Umsetzungen

- Diverse Produkte verfügbar, aber:

→ **IDM-Projekt ist nur zu einem kleinen Teil Tool-Integration**

→ **Prozesse und Zuständigkeiten zentral (Business Projekt!)**


Passt Ihre Software?

AdNovum Informatik AG

Christof Dornbierer, CTO

Röntgenstrasse 22, 8005 Zürich

christof.dornbierer@adnovum.ch, www.adnovum.ch

T +41 44 272 6111