

# Nutzen- und Sicherheitsaspekte des Identity-Management

Michael Rogulla, SIZ

# Agenda

---

- Die Sparkassen-Finanzgruppe
- Gesetzliche Rahmenbedingungen:
  - Basel II
  - KWG §25a
  - Kontrollmöglichkeiten mit IdM Systemen
- Provisioning Systeme als Directory Enabled Applications
- Erfahrungen aus Umsetzungsprojekten
- Sicherheits- und Nutzenaspekte von Provisioning und Identity Management (IdM) Systemen
- Federated Identity Management
- Empfehlungen, Schlusswort

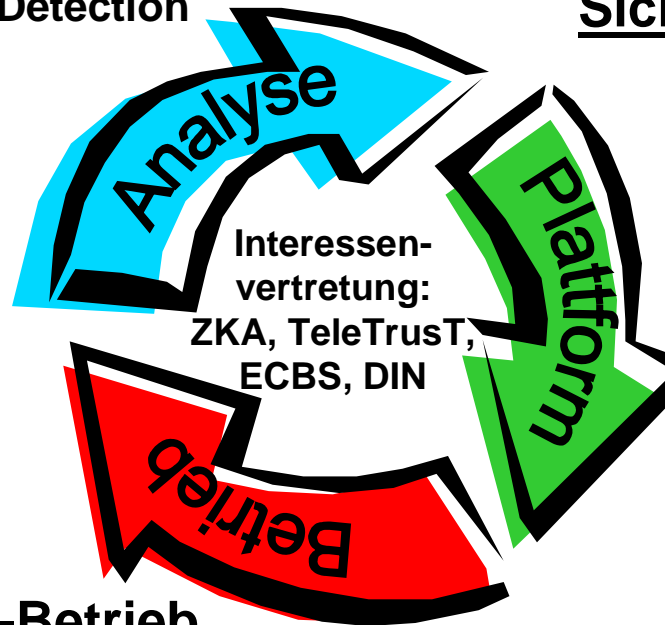
# Die Sparkassen-Finanzgruppe

- Die Sparkassen-Finanzgruppe ist föderalistisch organisiert. Stand Ende 2001 gibt es
  - 540 Sparkassen mit über 16.000 Zweigstellen in Deutschland
  - Regional und überregional operierende Verbände
  - 12 international operierende Landesbanken
  - 3 Rechenzentren in Deutschland
  - Weitere Unternehmen wie
    - Deka, Landesbausparkassen, Provinzial Versicherung u.v.m.
  
- Das SIZ ist ein marktorientierter IT-Dienstleister in der Sparkassen-Finanzgruppe
  - Sitz in Bonn
  - 69 Mitarbeiter (Stand 01/2003)
  - Zentrales Thema: Beratung und Komponenten für die Zusammenarbeit der IT in der gesamten Sparkassen-Finanzgruppe und darüber hinaus.

# Produkte des SIZ, Bereich Sicherheitstechnologie

## Aktive Sicherheit

- **S**CERT
- Tiger Team / Sicherheits-Audit
- Intrusion Detection
- Antiviren



## Sichere IT-Plattform

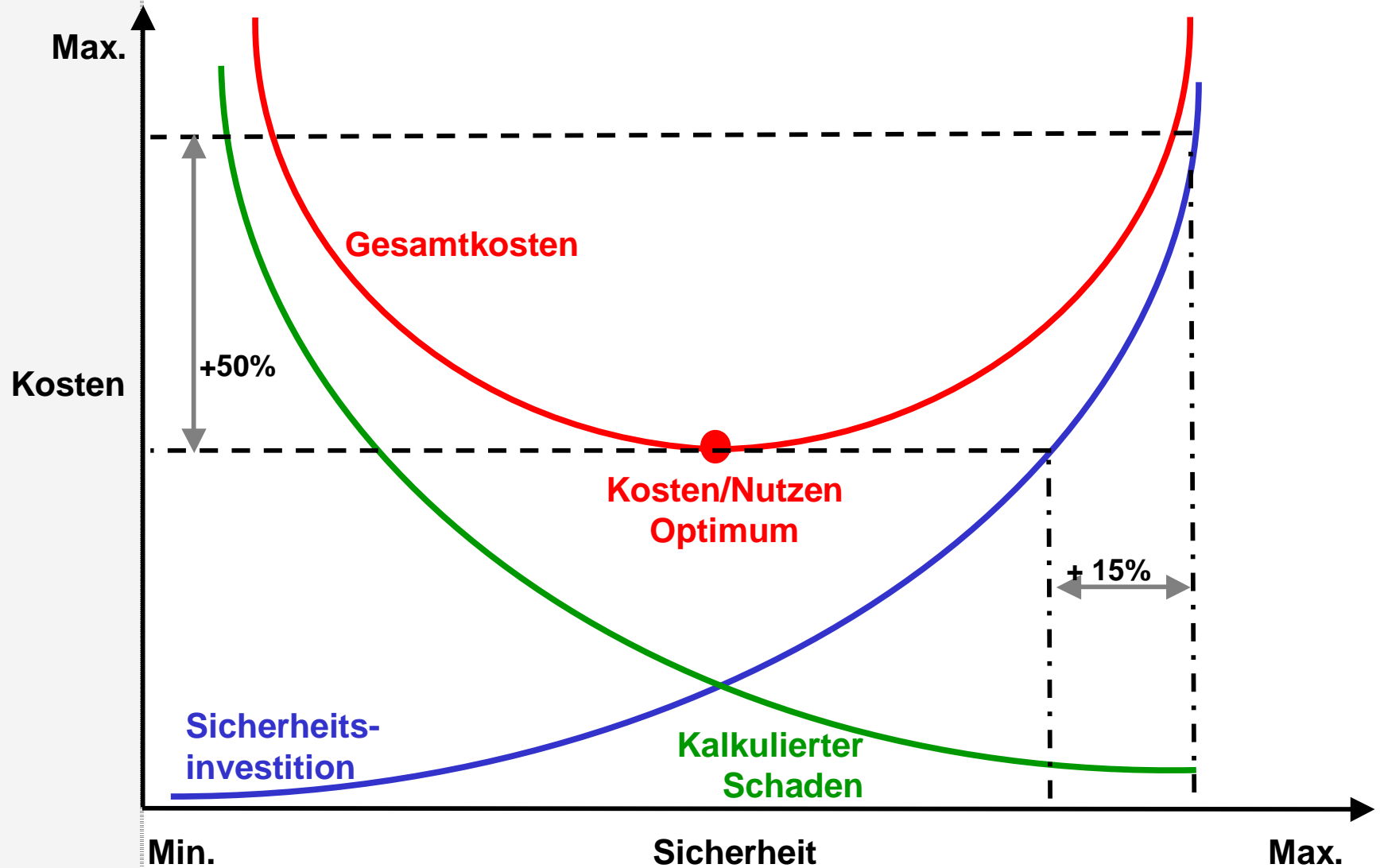
- Infrastruktursicherheit
- Systemtechnische und kommunikationstechnische Infrastruktur
- Sourcing, Rahmenverträge
- Nationales und internationales Sicherheitsrecht

## Sicherer IT-Betrieb

### *Sicherheit – Verfügbarkeit – Betrieb*

- Sicherheitspolicies
- Service Level Management, KWG § 25a
- Prüfungs- und Revisionsanforderungen, BAFin, Basel II, OPDV
- Betriebskostenoptimierung, TCO

# Kostenaspekte der IT-Sicherheit



# Empfehlung zur Etablierung von Sicherheit in der IT

---

- Herstellung und Aufrechterhaltung von IT-Sicherheit ist für ein Unternehmen fundamental und sollte daher ganzheitlich betrachtet werden. Es ist eine Aufgabe der Geschäftsleitung.
  
- Top-Down Ansatz:
  1. Schritt: Unternehmenspolitik
    - Geschäftsführung beschließt und unterstützt die Einführung und den Betrieb eines Sicherheitsmanagementsystems
  
  2. Schritt: Organisation
    - Einführung und fortlaufende Pflege eines Sicherheitsmanagementsystems
    - Analyse und Dokumentation von Prozessen, Anwendungen, Systemen, Infrastruktur
  
  3. Schritt: Technik
    - Nutzung entsprechender technischer Maßnahmen wie Firewalls, Proxies oder Provisioning Systeme

# Gesetzliche Rahmenbedingungen: Basel II

---

- Basel II ist ein Rahmenwerk in der Finanzwelt, welches durch das „Baseler Komitee der Bankenaufsicht“ entwickelt wird. Start: 2006
  
- Kreditinstitute werden durch Basel II zukünftig stärker angehalten
  - Risiken quantitativ zu bewerten
  - Risiken differenzierter zu beleuchten
  - Risikovorsorgen (=Eigenkapitalvorsorge) zu treffen
  
- Die Eigenkapitalquote wird sich in Basel II nach der individuellen Höhe des Risikos richten. Das Gesamtrisiko wird berechnet aus:
  - Kreditrisiko
  - Marktrisiko
  - Operationelles Risiko                      ← **NEU**

# Gesetzliche Rahmenbedingungen: Basel II: Operationelles Risiko

---

- Im Vergleich zur bestehenden Baseler Eigenkapitalvereinbarung ist das Operationelle Risiko neu hinzugekommen.
- Operationelles Risiko ist die Gefahr von Verlusten, die in Folge der Nichteinhaltung oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge externer Ereignisse eintreten.
- Operationelle Risiken können durch Maßnahmen im Bereich der IT-Sicherheit reduziert werden.

# Gesetzliche Rahmenbedingungen: §25a Kreditwesengesetz (KWG)

---

- §25a KWG regelt die organisatorischen Pflichten der Kreditinstitute im Bereich des Bankenaufsichtsrechts.
- §25a Absatz 1 KWG verpflichtet die Kreditinstitute, bestimmte organisatorische Vorgaben hinsichtlich ihrer Tätigkeit im Kreditgeschäft zu erfüllen:
  - Steuerung
  - Überwachung
  - Und Kontrolle der vorhandenen Risiken
- §25a Absatz 2 KWG behandelt die Problematik der Auslagerung von bestimmten Funktionsbereichen auf andere Unternehmen (Outsourcing).

# Eine Auslagerung entbindet nicht von den Pflichten aus §25a KWG

- Gesamtverantwortung bleibt immer beim auslagernden Kreditinstitut
- umfangreiches Vertragswerk erforderlich mit SLAs und Sicherheitsvereinbarungen
- Institutseigene, dokumentierte IT-Sicherheitsrichtlinien sind Voraussetzung für geeignete vertragliche Regelungen
- Einrichtung eines wirksamen Kontrollsystems für Auslagerungsunternehmen entsprechend den Vorgaben der BaFin



# Gesetzliche Rahmenbedingungen für AGs und GmbHs

- Die vorgestellten Themen Basel II und KWG §25a betreffen Unternehmen aus dem Finanzdienstleistungssektor.
- Das seit dem 1. Mai 1998 in Kraft getretene KontraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) verpflichtet auch Kapitalgesellschaften wie AGs und GmbHs zur Einführung eines wirksamen Risikosteuerungsmanagements  
→ Parallele zu §25a KWG, hier können Provisioning Tools bei der Reduzierung von (operationellen) Risiken unterstützen.
- AktG §91 (Aktiengesetz) verpflichtet alle Handelsunternehmen (nicht nur AG sondern auch GmbH) zur Einrichtung eines Überwachungssystems, um frühzeitig Entwicklungen zu erkennen, die den Fortbestand des Unternehmens gefährden können  
→ hier können Reverse Provisioning Tools unterstützen.
- MaH (Mindestanforderungen an das Betreiben von Handelsgeschäften)

# Umsetzung der gesetzlichen Rahmenbedingungen

---

- Provisioning / Identity Management (IdM) Systeme sind technische Maßnahmen, die bei der Erfüllung der gesetzlichen Forderungen Unterstützung liefern können.
  - Steuerung
  - Überwachung
  - Und Kontrolle der vorhandenen Risiken
  
  - Statusbildung auch von zurückliegenden Zeitpunkten (z.B. für Audits)
  
  - Kontrollmöglichkeit über zentrale Daten wie z.B. Zugriffsrechte auch auf ausgelagerte Systeme (Outsourcing)

# Provisioning Systeme als „Directory Enabled Applications“

- Provisioning gehört zu den technischen Maßnahmen und ist ein Funktionsbereich aus dem übergeordneten Identity Management.
- Die organisatorischen Maßnahmen müssen vor der Umsetzung der technischen Maßnahmen abgeschlossen sein:
  - Analyse, Dokumentation und ggf. Anpassung der Prozesse, Anwendungen, Systeme, Rollen und Rechte im Unternehmen
  - Zuständigkeiten für Anwendungen
- Technische Aspekte sollten anschließend geklärt werden:
  - Z.B. Anbindung der Anwendungen über Konnektoren möglich?
- Besonders in der Definition und Abstimmung von Mitarbeiterrollen im Unternehmen kann erheblicher Aufwand stecken.

# Erfahrungen aus Umsetzungsprojekten (1)

---

- In der Sparkassen-Finanzgruppe wurden bereits sehr frühzeitig Projekte zur Evaluierung und Pilotierung von Provisioning und Identity Management Systemen aufgesetzt.
  
- Die ersten Projekte wurden aus einem technischen Blickwinkel begonnen. Typische Fragestellung war dabei:
  - Welches Produkt muss ich verwenden?
  - Welche Performance ist zu erwarten [=Sizing] ?
  - Kann ich meine bestehende Anwendungslandschaft an die neuen Systeme anbinden?
  
- Bei einer technischen orientierten Herangehensweise können organisatorische Fragen (Dokumentation der Prozesse sowie Rollen und Rechte, Klärung der Zuständigkeiten) übersehen werden und den Projektaufwand nachträglich enorm vergrößern.

# Erfahrungen aus Umsetzungsprojekten (2)

---

- Projekte, welche zunächst in einer Fachabteilung begonnen wurden, betrafen - wegen der Querschnittsfunktion von Verzeichnisdiensten - größere Unternehmenseinheiten als geplant. Daraus resultieren neue Fragestellungen bzgl. der Verantwortung und Finanzierung dieser Aktivitäten.
  
- Es tritt leicht eine Zwickmühle auf:
  - Man sollte zunächst mit einem begrenzten Projektziel arbeiten, möglichst mit nachweisbarem Return of Investment (RoI). Dazu bietet sich das Thema Provisioning an.
  
  - Aber auch Teilbereiche aus dem Identity Management (IdM) (wie z.B. Provisioning) haben bereits Auswirkungen auf die Architektur der IT, so dass man eigentlich mit der Umsetzung der „großen“ Idee beginnt. Dann jedoch werden Aktivitäten mit ursprünglich begrenztem Umfang schnell sehr ressourcenaufwändig.

# Sicherheits- und Nutzenaspekte von Identity Managementsystemen (1)

- Sicherheit von IT-Systemen umfasst zwei Aspekte:
  - Sicherheit, die durch den Einsatz des jeweiligen IT-Systems entsteht
  - Sicherheit, die für den Einsatz des jeweiligen IT-Systems gewährleistet sein muss.
  
- Provisioning / Identity Management (IdM) Systeme sind kritische Komponenten der Infrastruktur einer Organisation, da diese unter anderem den Zugriff auf zum Teil kritische Systemressourcen regeln.
  - Provisioning / IdM Systeme müssen daher entsprechend sicherheitstechnisch geschützt werden.
  - Eine hohe Verfügbarkeit muss gewährleistet sein.

# Sicherheits- und Nutzenaspekte von Identity Managementsystemen (2)

- Einsatzbereich von Provisioning bzw. Identity Management Systemen vorrangig bei der Benutzerverwaltung
- Sicherheitskritisch sind
  - Fehler bei der Zuweisung von Benutzerrechten
  - Verzögerungen bei der Änderung / Löschung von Zugriffsrechten
- Nutzenaspekte:
  - Reduzierung der manuellen Eingriffe durch Automatisierung von Vorgängen, dadurch geringere Fehlerhäufigkeit
  - Geringere Wahrscheinlichkeit, dass Änderungen verzögert durchgeführt oder vergessen werden.
  - Möglichkeit zur Einbindung in einen Workflow, dadurch Beschleunigung von unternehmensinternen Vorgängen (Vergleich: Umlaufmappe o.ä.)

# Sicherheits- und Nutzenaspekte von Identity Managementsystemen (3)

- ... Nutzenaspekte:
  - Entlastung der Administratoren von Routinetätigkeiten wie
    - Zurücksetzen des Passwortes
    - Änderung von Gruppenzugehörigkeiten
  - Single Point of Administration
  - Es kann jederzeit ein Status sowohl über die aktuelle als auch vergangene Berechtigungssituation hergestellt werden.
  
  - Identity Management bietet auch Funktionen, die für das Risikomanagement nutzbar sind.

# Kontrollmöglichkeiten mit Identity Management Systemen (1)

---

- Ein Auslagernder ist neben der Verwaltung der Zugriffsrechte auf interne Systeme auch verantwortlich für die Zuweisung solcher Rechte auf Systeme, die bei einem Dienstleister stehen.
- Installation und Betrieb der Identity Management (IdM) / Provisioning Systeme können durch den Dienstleister vorgenommen werden.
- Inhaltliche Definition der Berechtigungsprofile auf Basis der Geschäftsprozesse und Zuweisung jedes Mitarbeiters zu diesen Profilen gehört zu den hoheitlichen Aufgaben des Auslagernden.
- Die Auslösung des Prozesses zur Berechtigungsvergabe und die gesonderte Zustimmung zur Vergabe von Einzelrechten darf ebenfalls nur durch den Auslagernden erfolgen.

# Kontrollmöglichkeiten mit Identity Management Systemen (2)

---

- Aus Sicherheitsgesichtspunkten muss eine Provisioning-Lösung mindestens folgende Funktionen unterstützen:
  - Policy-basierte Berechtigungsvergabe. Der Auslagernde gibt die Regeln vor, nach denen der Dienstleister zu verfahren hat.
  - Berechtigungsevidenz: Der Auslagernde hat jederzeit die volle Transparenz der aktuellen Berechtigungssituation
  - Flexibler Genehmigungs-Workflow: Die Aktivierung einer Berechtigungsvergabe an einen Mitarbeiter des Auslagernden durch direkte oder höhere Vorgesetzte muss möglich sein.
  
- Der Einsatz von Provisioning Systemen erleichtert also die Kontrolle über den Dienstleister.
  
- Das Engagement von IBM verdeutlicht, dass dieses Marktsegment auch von den Großen der Branche für bedeutend gehalten wird.

# Federated Identity Management (1)

---

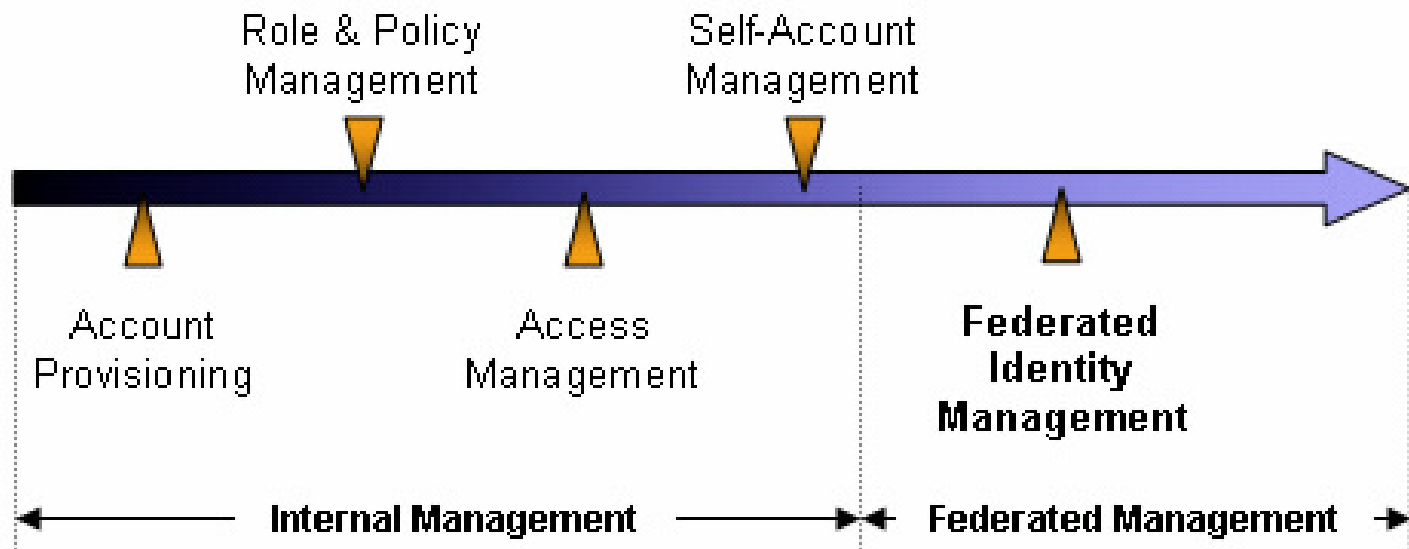
- Unter „Federated Identity Management“ (FIM) wird Identity Management über Unternehmensgrenzen hinweg verstanden.
- Es wächst heutzutage mehr und mehr der Anspruch an Unternehmen, nicht nur Mitarbeitern, sondern auch Partnern und Kunden (z.B. bei Supply Chain Management) Zugriff auf interne IT-Ressourcen zu gewähren.
- Eine starre Trennung zwischen „innen“ und „außen“ weicht einer mehrstufigen Sicherheitshierarchie.
- Neue Ansätze wie Webservices beschleunigen diese Entwicklung.

# Federated Identity Management (2)

- Erste Aktivitäten wie „Passport“ von Microsoft oder die „Liberty Alliance“ unter der Federführung von SUN verdeutlichen FIM als wichtigen Trend:
  - „Passport“ von Microsoft ist ein Produkt. Sein Einsatz wird vornehmlich im Segment der Endkunden gesehen
  - „Liberty Alliance“ unter der Federführung von SUN ist eine Sammlung von Spezifikationen. Erste Produkte und Rahmenwerke auf deren Basis wurden entwickelt. Der Einsatz wird im B2B (Business-to-Business) Bereich gesehen.
  
- Die Liberty Alliance hat in ihren Spezifikationen die Koexistenz mit „Passport“ berücksichtigt.

# Federated Identity Management (3)

## Evolution of Identity Management



# Federated Identity Management (4)

---

- Federated Identity Management (FIM) ist eine Notwendigkeit für eBusiness über Unternehmensgrenzen hinweg.
- FIM wird die Komplexität und die Kosten (Einführung, Abstimmungen, laufender Betrieb, Überwachung) im Vergleich zu Identity Management Systemen steigern.
- Bei der Nutzung von FIM müssen Unternehmen akzeptieren, dass Teile ihrer Sicherheitsinfrastruktur und Prozesse außerhalb des eigenen Hoheitsgebietes gepflegt werden.
- Dadurch müssen neue sicherheitstechnische Aspekte beleuchtet werden.

# Empfehlungen (1)

---

- Provisioning und Identity Management (IdM) Systeme haben Marktreife erlangt. Ihr Einsatz kann empfohlen werden.
- Es ist dringend anzuraten, vor der Einführung von Provisioning und IdM Systemen insbesondere Fragen der Organisation des Unternehmens (Prozesse, Rollen und Rechte) zu klären. Ist dies nicht der Fall, kann der Projektumfang stark anwachsen.
- Neue gesetzliche Rahmenbedingungen machen die Einführung eines Systems notwendig, mit dem Risiken
  - gesteuert
  - überwacht
  - und kontrolliert werden können

Es sollte geprüft werden, inwieweit in dem eigenen Unternehmen diese Maßnahmen bereits umgesetzt wurden und ggf. Maßnahmen aufsetzen, falls dies noch nicht geschehen ist.

## Empfehlungen (2)

---

- Die Einführung eines IdM oder eines Teilbereiches (Provisioning Systeme o.a.) hat starken Einfluss auf die Architektur der IT des Unternehmens und sollte aus einer gesamtheitlichen Perspektive betrachtet werden. Ein Kommitment und aktive Unterstützung durch die Geschäftsführung wird empfohlen.
- Identity Management Systeme sind als Teil der sicherheitstechnischen Infrastruktur besonders zu schützen, da sie an zentraler Stelle den Zugriff auf viele andere, teils kritische, Systeme gewähren.
- Bereits existierende Federated Identity Managementsysteme wie „Passport“ von Microsoft weisen laut Experten noch Sicherheitslücken auf. Ihr Einsatz kann im B2B Umfeld nicht ohne ausreichende Risikoabschätzung empfohlen werden.