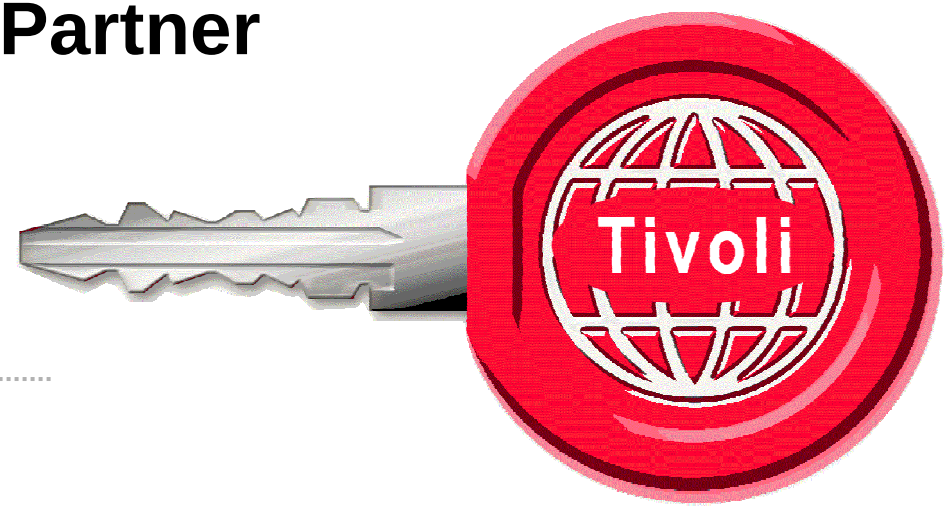
IBM Software Partner Academy Telefonkonferenz am 14.05.2010

IBM Software Business Partner Workshop



IBM Tivoli Security

Andreas Sundrum
Security Sales Leader Tivoli

IBM Deutschland GmbH

Phone +49 211 476 2997
Mobile +49 170 570 1664
Email sundrum@de.ibm.com

Tivoli software

Agenda

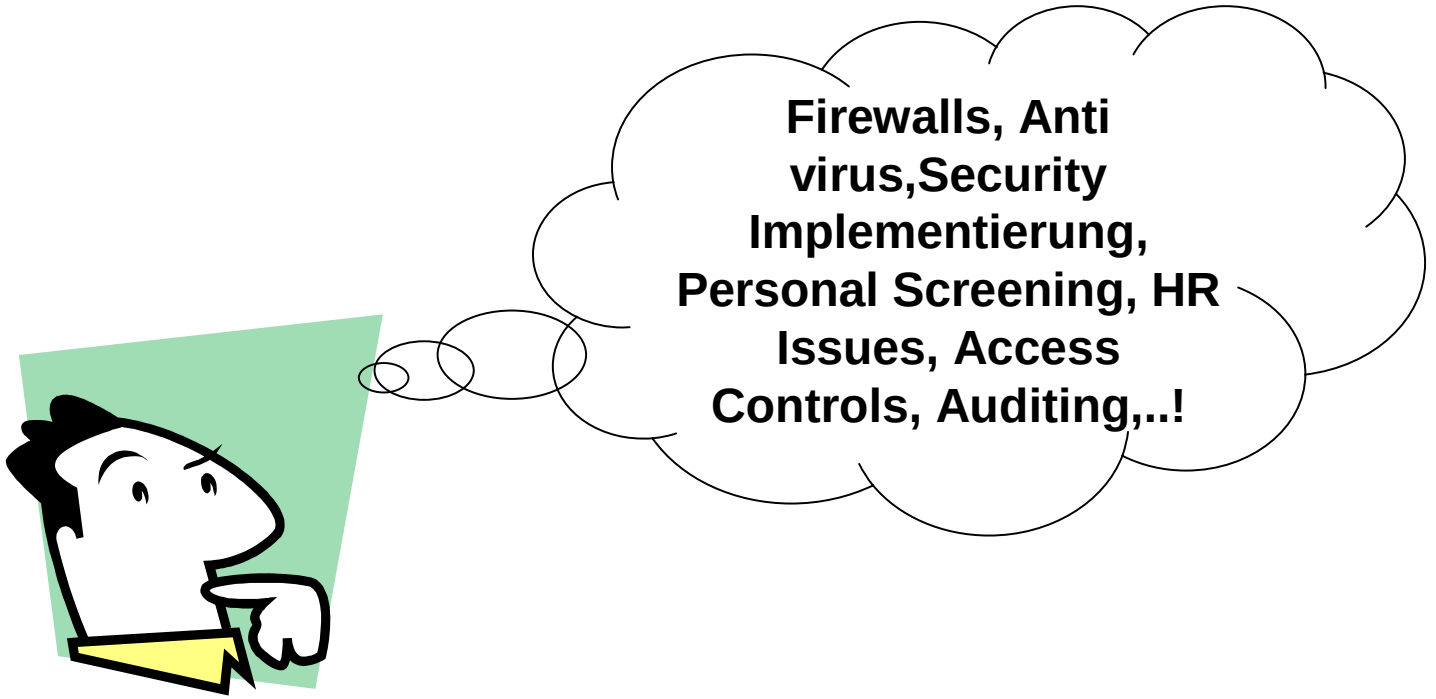
- Was ist „Security“
- Risiko Management und Policies
- Security Projekt Identifizierung
- Tivoli Security White Boarding
- Fragen ?

IBM Software Partner Academy Telefonkonferenz am 14.05.2010

Was ist Security ?

Security ?

- Security ist sehr komplex und wirkt daher abschreckend



Tivoli Security - mehr als nur Sicherheit“

- Security im typischen Sinne:
  - „Keep the bad guys out“
  - Typische Bedeutung: Virenschutz, Firewall, etc.
  - Typische Einschätzung:
    - Kostentreiber!
    - Kosten Geld, keine Ersparnis, kein Payback (ROI)
    - Werden eher belastend, störend und lästig wahrgenommen

- Tivoli Security:
  - Unser größtes Potenzial:
    - **Produktivitäts- & Kosteneinsparungen** (Automatisierte Userverwaltung (User-Lifecycle Management), keine Belastung des HelpDesks aufgrund Passwort-Resets, keine verwaisten Accounts mehr, etc.)
    - **Risikominimierung** (Zugriff für denjenigen, der ihn aufgrund seiner Tätigkeit benötigt und das Nachweisen der tatsächlichen Zugriffe)
    - **Mitarbeiterzufriedenheit** (Nur noch ein Kennwort zu verwalten)
    - **Compliance** (automatisiertes Nachweisen der Richtlinieneinhaltung)

Kostenersparnis, bei gleichzeitiger Risikominderung und Produktivitätssteigerung

Informationssicherheit

Ziele unserer Kunden

- Es muss sichergestellt werden, dass der **Zugriff** auf Informationen ausschließlich durch **Befugte** erfolgt
- **Einheitliches Sicherheitsmanagement**, insbesondere bei abnehmender Fertigungstiefe und global integrierten Unternehmen
- **Schutz geistigen Eigentums** ist sicherzustellen
- Überwachung ordnungsgemäßen **Benutzerverhaltens** (insbesondere privilegierter Benutzer)
- Einhaltung von **Gesetzen und Regularien** muss gewährleistet sein und nachgewiesen werden können
- **Bewusstsein** bei Mitarbeitern für Sicherheit ist zu schärfen
- **Warnsystem** bei sicherheitskritischem Verhalten

IBM Tivoli Lösungen

- Einführung eines zentralen Systems zur Verwaltung von **Benutzerrechten und Zugriffsberechtigungen**
- Einführung eines Systems zum **Überwachen des Benutzerverhaltens**. Insbesondere der Aktivitäten, privilegierter Benutzer
- Einführung **automatisierter Reporting Funktionalitäten**
- Einführen eines einheitlichen **Zugriffsmanagements**
- Aufsetzen von ‚**Security Awareness**‘ Kampagnen
- Definieren und Festlegen von **Sicherheitsrichtlinien und Prozesse**

  → **Einführung eines Sicherheitsmanagements**

Fragen, der Security Verantwortlichen

- Bruch der Privatsphäre:
  - Greifen Datenbankadministratoren auf vertrauliche Daten zu?
  - Missbrauchen “trusted user” Personaldaten?
  - Begeht ein bestimmter Administrator Identitätsdiebstahl?

- Verletzung von Sicherheitsregeln:
  - Wurden unauthorisierte Systemänderungen durchgeführt?
  - Hat ein root User das Audting abgeschaltet?
  - Wann wurden die Auditlogs von den Systemadministratoren gelöscht?
  - Wer hielt ohne Berechtigung wichtige Systemprozesse an?

- Verletzung von Aufgabentrennung:
  - Hat jemand Transaktionen initiiert und genehmigt?
  - Hat ein Administrator Berechtigungen in einem System beantragt, genehmigt und konfiguriert?

Analysteneinschätzungen

- Wieviel kostet das einfache Zurücksetzen von Kennwörtern?
  - ✓ **3-4 mal im Jahr pro Benutzer und ca. € 15 pro Anruf**
- Wie lange dauert es, einen neuen Mitarbeiter mit allen notwendigen Rechten auszustatten?
  - ✓ **Bis zu 12 Tage, um den Mitarbeiter mit allen Zugriffsrechten auszustatten**
- Wieviele der früheren Mitarbeiter haben noch Zugriff auf sensitive Daten?
  - ✓ **30-60% aller Accounts sind verwaist**
- Wie sicher sind wir, das nur die richtigen Mitarbeiter Zugriff auf Kundendaten haben?
  - ✓ **70% aller Betrugsfälle mit Kundendaten werden von Insidern begangen**
- Wie lange dauert es alle Berichte für die Revision zusammenzustellen?
  - ✓ **Kann Wochen dauern und einige Unternehmen haben hierfür dedizierte Vollzeitkräfte**

Security ist nicht nur…

- Firewalls
- Anti Virus
- Encryption tools
- Smart Card Door Locks
- etc.

Security ist nicht Technologie bzw. Service getrieben, sondern es geht um das Managen bzw. Minimieren von Risiken

IBM Software Partner Academy Telefonkonferenz am 14.05.2010

Risiko Management und Policies

Wie Risko Management funktioniert

1) Nehmen Sie etwas das ihnen wichtig ist.
2) Entscheiden Sie was damit gemacht werden soll:
   a) Akzeptiere / Ignoriere das Risiko (z.B. Kometen Einschlag)
   b) Transferiere das Risiko (z.B. Kauf einer Versicherungspolice)
   c) Vermeide das Risiko (z.B. überquere die Straße nicht)
   d) Veringere das Risiko (z.B. schließe die Haustür ab)
3) Falls das Risiko transferiert oder veringert wird; ermittele die Kosten:
   a) Verlusterwartung = Verlust pro Vorfall x Anzahl der Vorfälle pro Jahr
   b) Budget <= Verlusterwartung = wir haben ein Security Projekt

Was ist eine Policy ?

- Eine Policy ist eine Ansammlung von Regeln und Standards. Das Ziel einer Policy ist Spezifizierung wie Risiken verwaltet werden

- Für Security könnte folgendes spezifiziert werden:
  - Was soll geschützt werden ?
  - Wie soll es geschützt werden ?
  - Was ist erlaubt ?
  - Was ist verboten ?
  - etc.

Policies vereinfachen Projekt Entscheidungen

- Policies begründen warum Produkte und Services implementiert werden müssen
- Policies fördern das Verständnis von Sicherheitsrisiken und der damit verbundenen Kosten
- Budget Zuweisung
  - CIO Management Unterstützung
  - LOB Support
  - CEO Support, etc.

The IBM Security Framework

- 5 Themengebiete beziehen sich auf die Security Policies einer Organisation
- Jedes dieser Lösungen hilft den Kunden die Policy Ziele zu realisieren

IBM Software Partner Academy Telefonkonferenz am 14.05.2010

Security Projekt Identifizierung

Opportunity Identifizierung und Qualifizierung

- Die Diskussion von Risiken in einer Organisation hift bei der Identifizierung von neuen Oppertunities
  - Kunden reden über Risiken und nicht über Produkte und Lösungen
  - Kunden werden nur Budget zuweisen wenn die Risiken verringert werden sollen
  - Kein Risiko = Kein Deal
- Wenn ein Kunde besorgt über ein bestimmtes Risiko ist, dann hinterfrage die Policies die hinter diesem Risiko stehen als Reaktion darauf
- Die Motivation ein Risiko zu veringern kann von einer **internen** Business Policy oder einer **externen** Compliance Anforderung kommen ☺

Welche Risiken sind für Oranisationen bedenklich

- Auf CIO, CEO Level sind alle Bedrohungen bedenklich die sich auf Vertraulichkeit, Integrität und Verfügbarkeit beziehen.
- Alle Risiken die sich auf Viren, Spyware, Malware, Hacking, etc. beziehen
- Security patching
- Gesetze und Regularien
  - Sarbanes Oxley, Basel 2
  - PCI DSS
  - Data Protection Legislation
  - Internal Audit

Welche Risiken sind für Oranisationen bedenklich

Die größten Sicherheitsbedenken sind aber interne Sicherheitsbedrohungen...

- Arbeitnehmer mit legitimiertem Zugriff auf wichtige Systeme und Daten
- Weiche Policies für Administratoren
- Mißbrauch von Passwörtern
- Einschleppen von Malware, Spyware, Würmern, Trojanern, etc...
- Infrastruktur Security, Server Protection, Desktop Protection, Network Infrastrukture Schutz, etc.
- Data Loss Prevention, getrieben von Medien Berichten und Datenverlusten (Kto. Daten, Kd Daten, Telemarketing, Webpages, etc.)

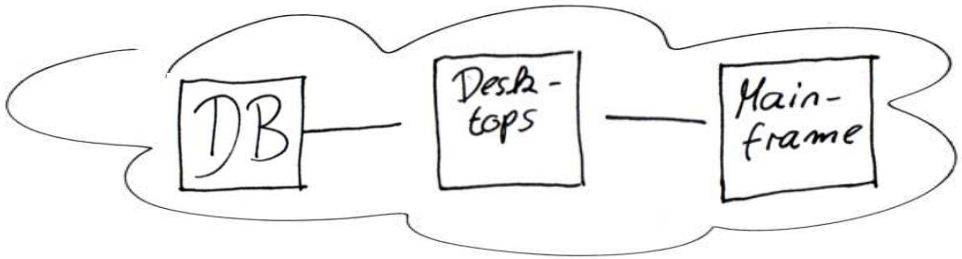
Security Entscheider und Beeinflusser

- Heutzutage sind die **Ansprechpartner** zu Security Themen weit verteilt in den Unternehmen.
- **Budget** Verantwortlicher wird auf das ROI fokusieren.
- **CEO** wird auf die Compliance Regelungen und Haftungsrisiken achten
- **Marketing** wird auf die Reputation des Unternehmens fokusieren
- **IT Verantwortlicher** wird auf die internen operativen Risiken fokusieren (Malware, Spyware, etc.)
- **Datenschutzbeauftragter** wird auf den Datenschutz achten
- **End User** wird auf die Benutzerfreundlichkeit achten

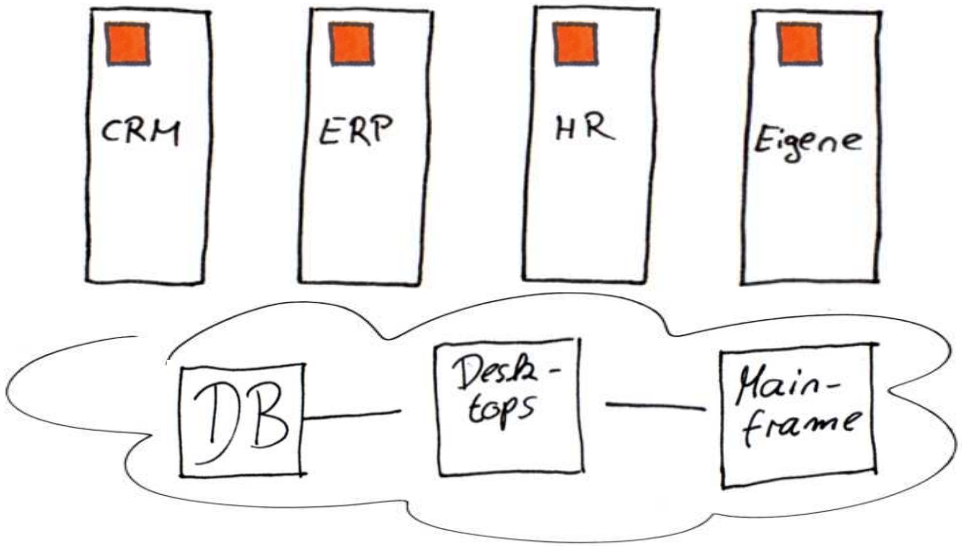
IBM Software Partner Academy Telefonkonferenz am 14.05.2010

Tivoli Security White Boarding

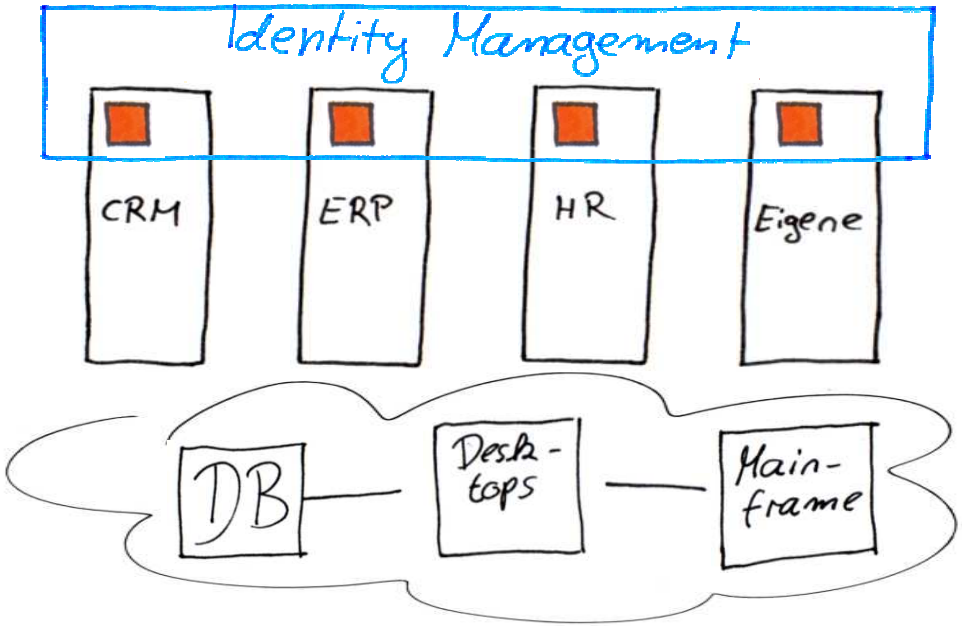
Zu Beginn betrachten wir als Beispiel Ihre Datenbanken, Desktops
und den Mainframe, welche Ihre unternehmenseigene IT-Infrastruktur bilden!



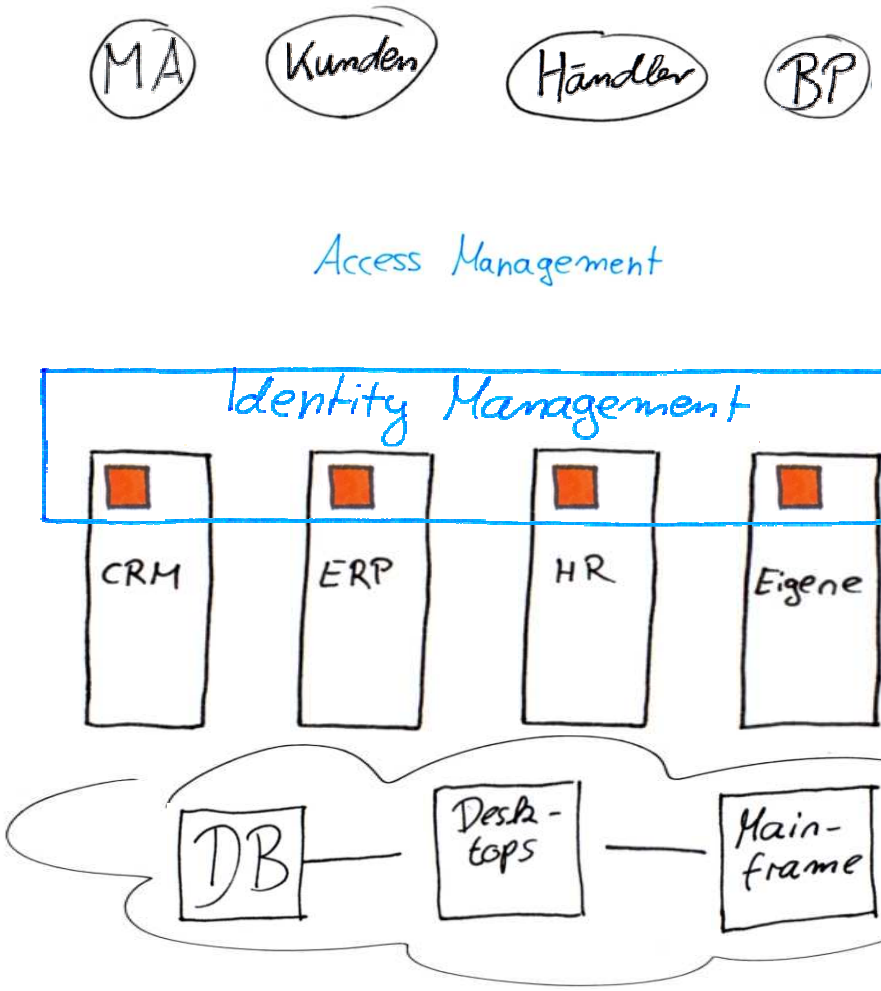
Zudem laufen bei Ihnen eine vielzahl von Systemen, wie CRM, ERP, HR oder auch eigene Applikationen, welche allesamt eigene Benutzerverwaltungen durchführen.



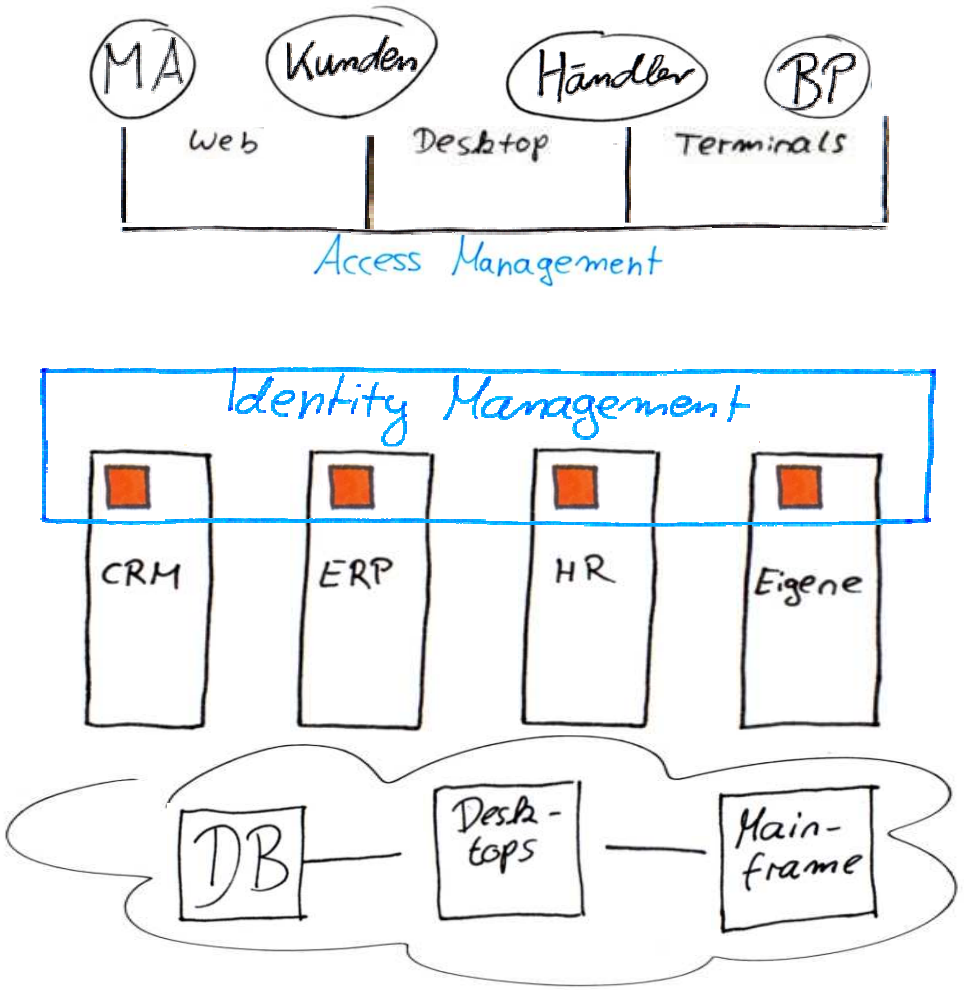
Dieser Administrationsaufwand wird mithilfe des Identity Managements durch eine automatische, zentrale Benutzerdefinition und Bereitstellung von Benutzerdiensten minimiert. Dadurch werden Kosten gespart.



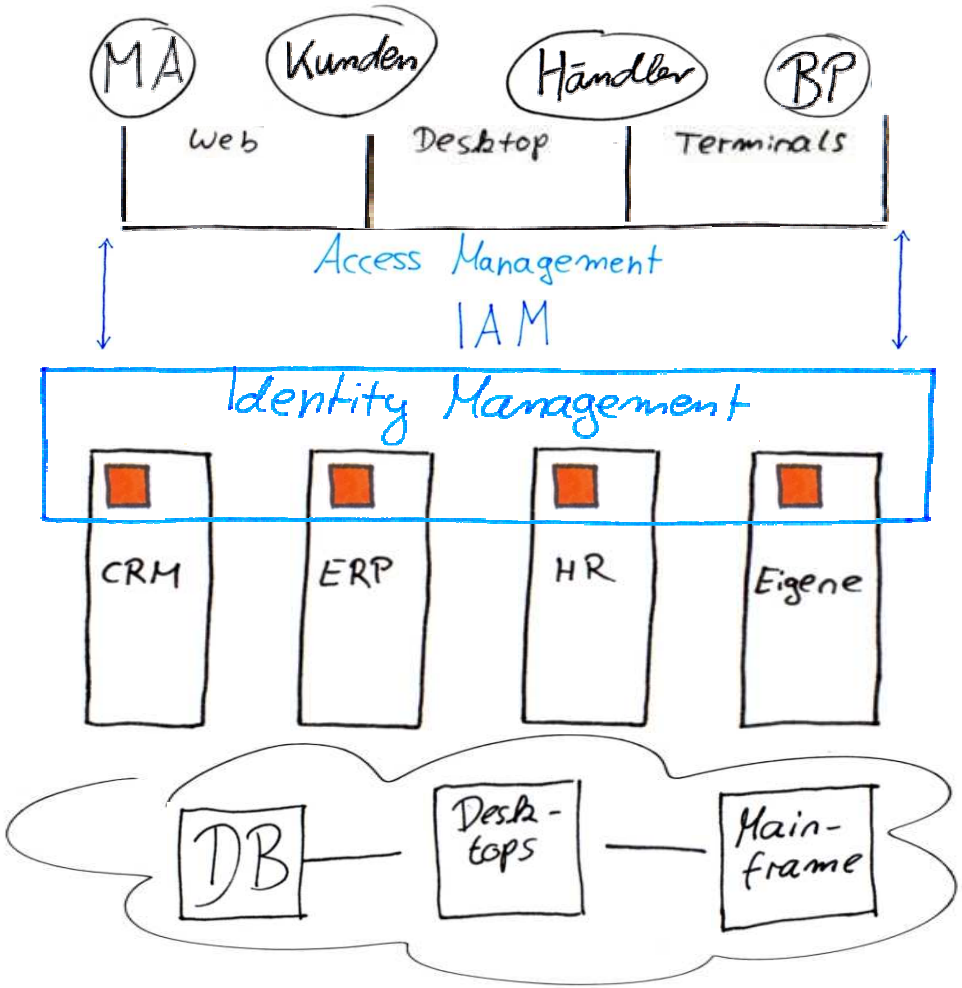
Der Zugang von z.B. Ihren Mitarbeitern, Kunden, Händlern und Business Partnern erfolgt über das Access Management…



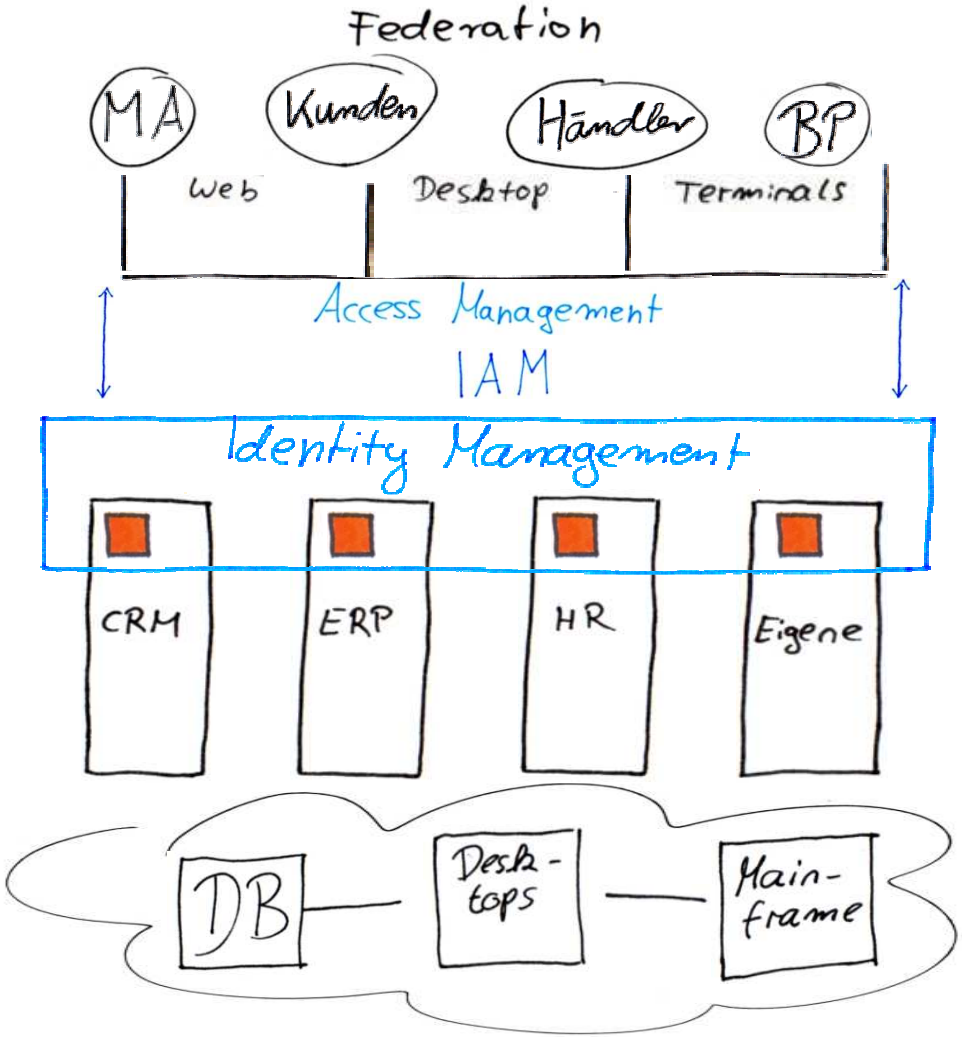
Als Zugangswege bieten sich hier beispielsweise Desktops, Terminals und das Web an



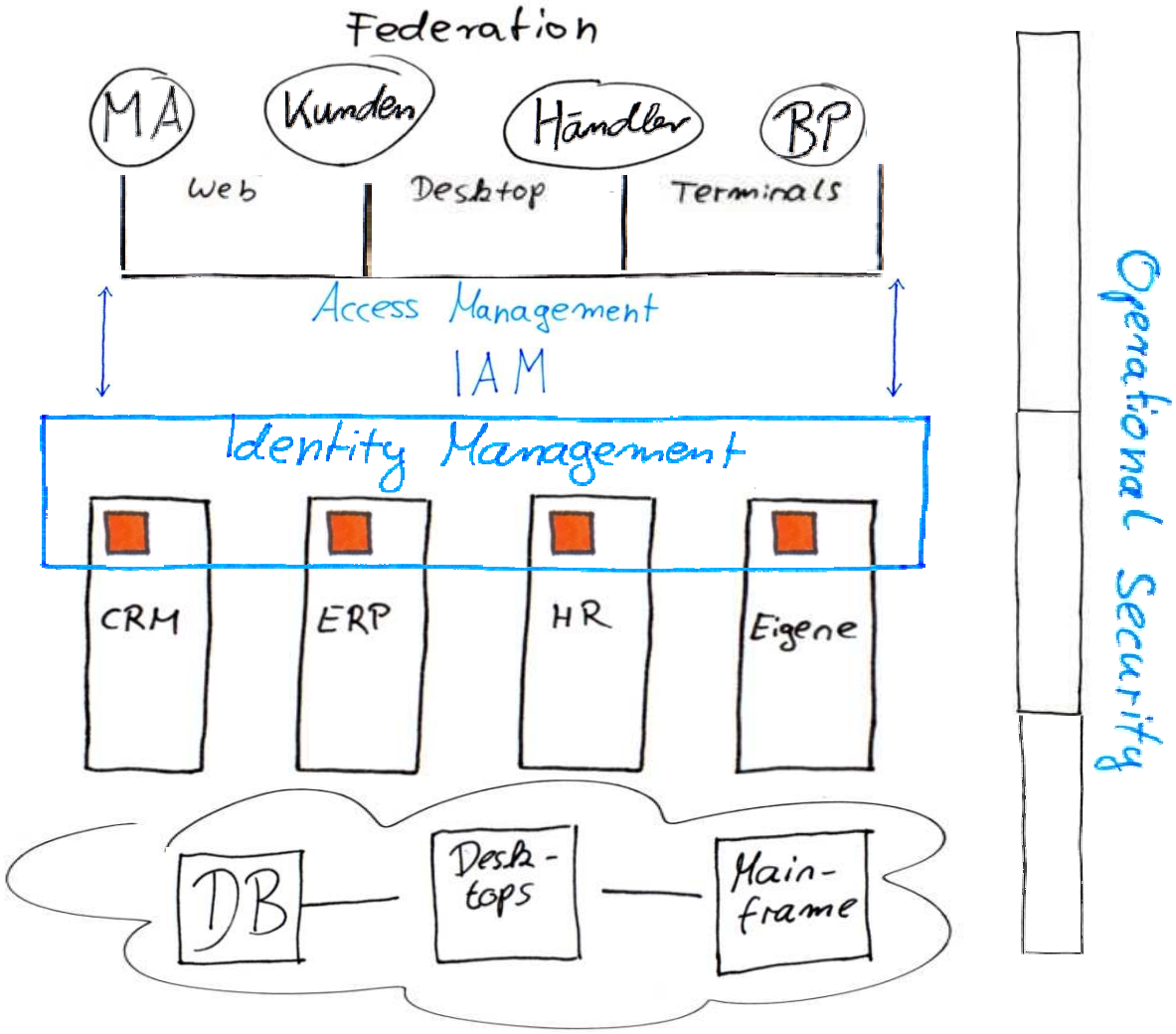
Der gesamte Themenkomplex wird als Identity & Access Management, kurz IAM bezeichnet.



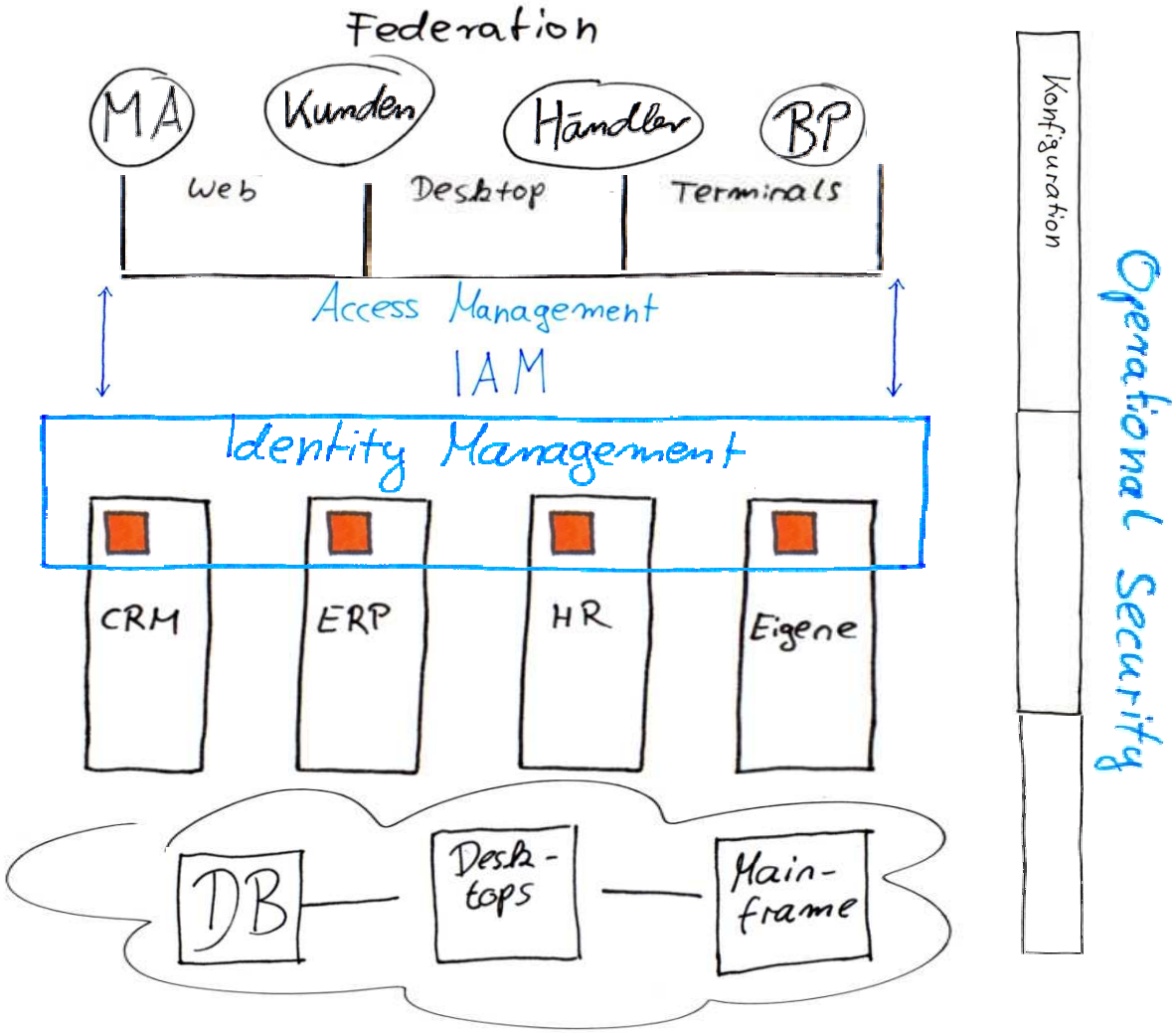
Soll IAM über Unternehmensgrenzen hinweg zum Einsatz kommen (z.B. bei Herstellern, Zulieferern, Händlern), so spricht man von Federation.



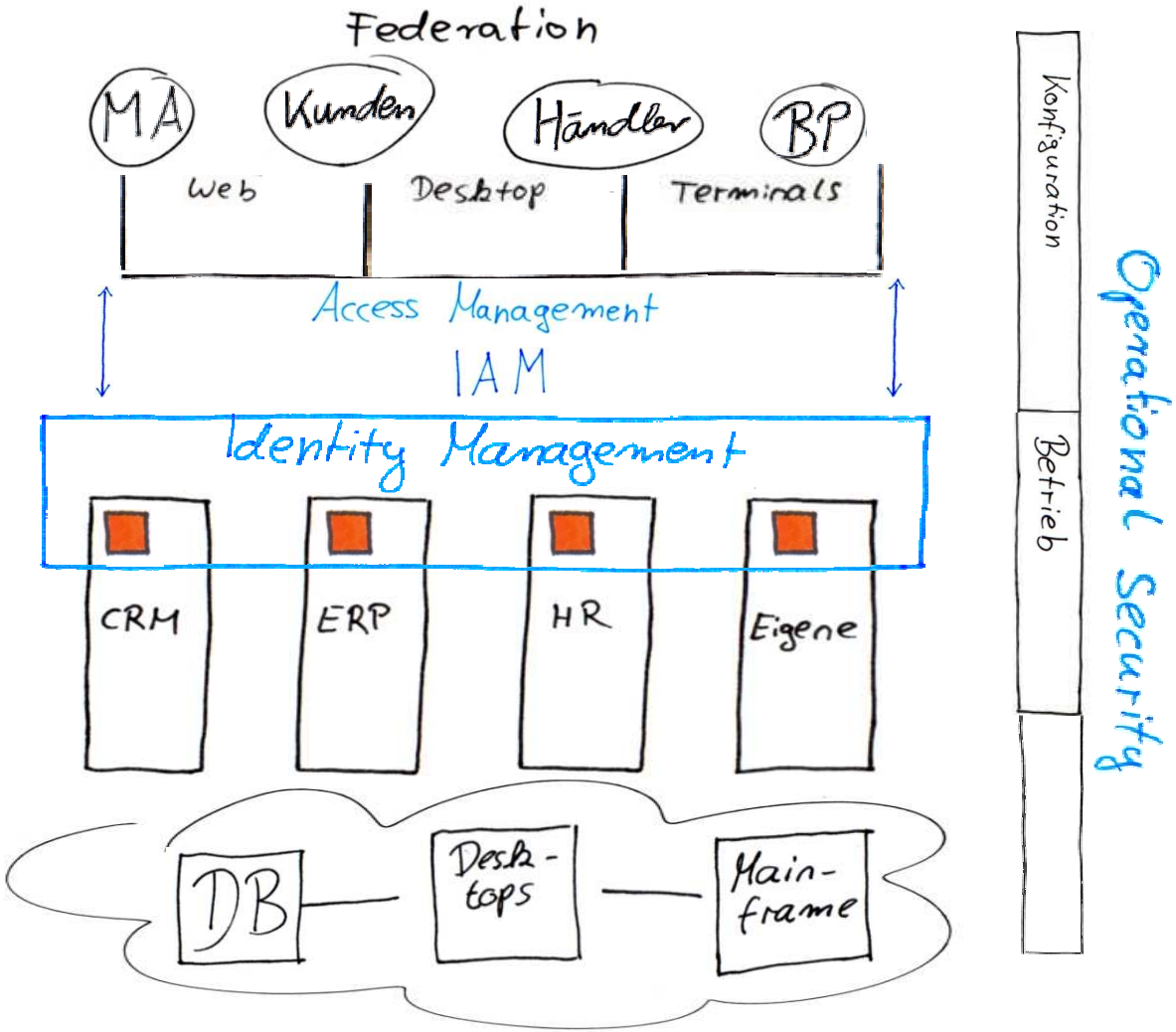
Neben IAM ist Operational Security ein weiterer Themenkomplex, der sich aus 3 Bestandteilen zusammensetzt



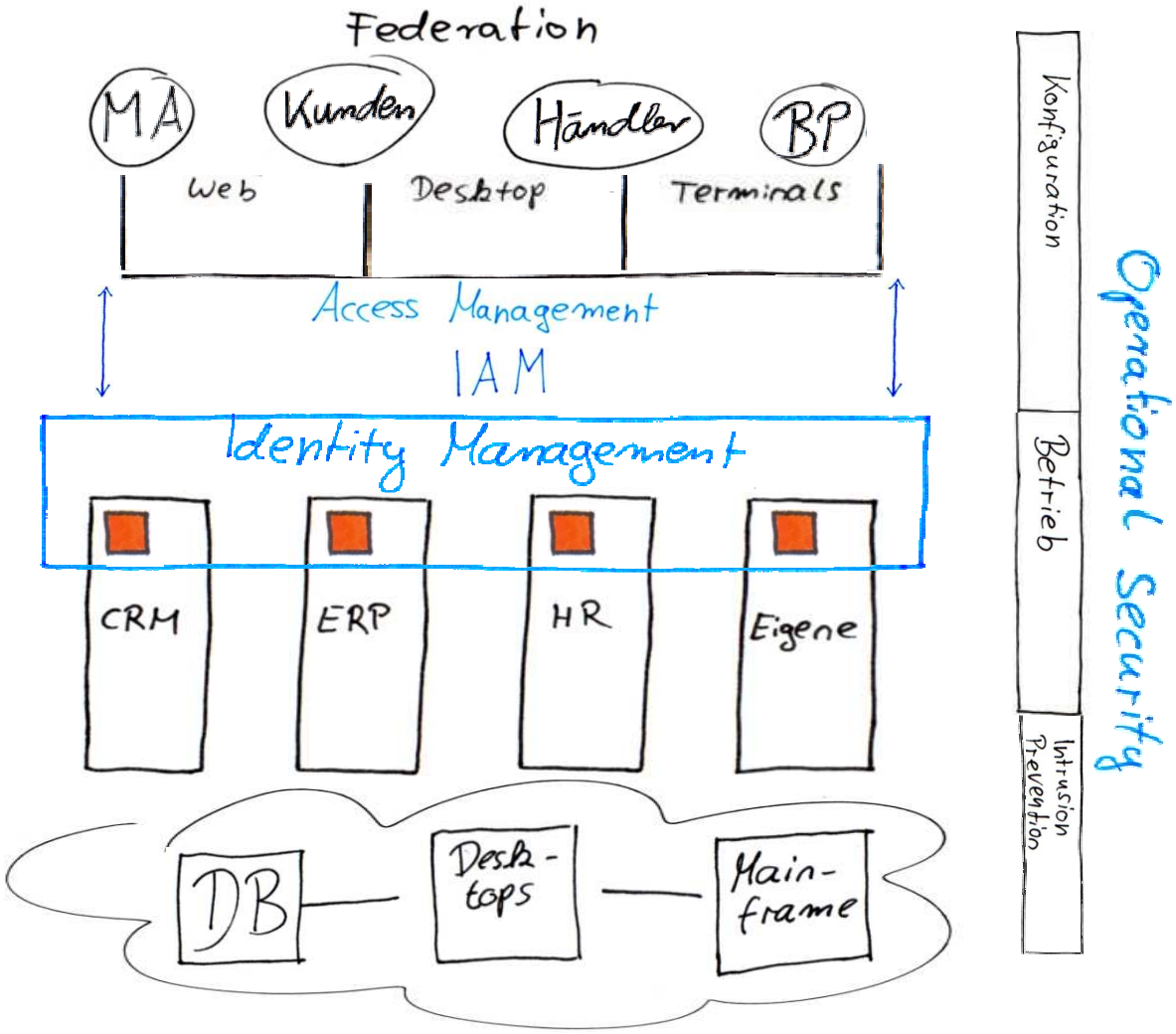
In Ihrem IT-Umfeld sollte Ihre Konfiguration in Hinblick auf die Erfüllung von Sicherheitsrichtlinien beurteilt werden…



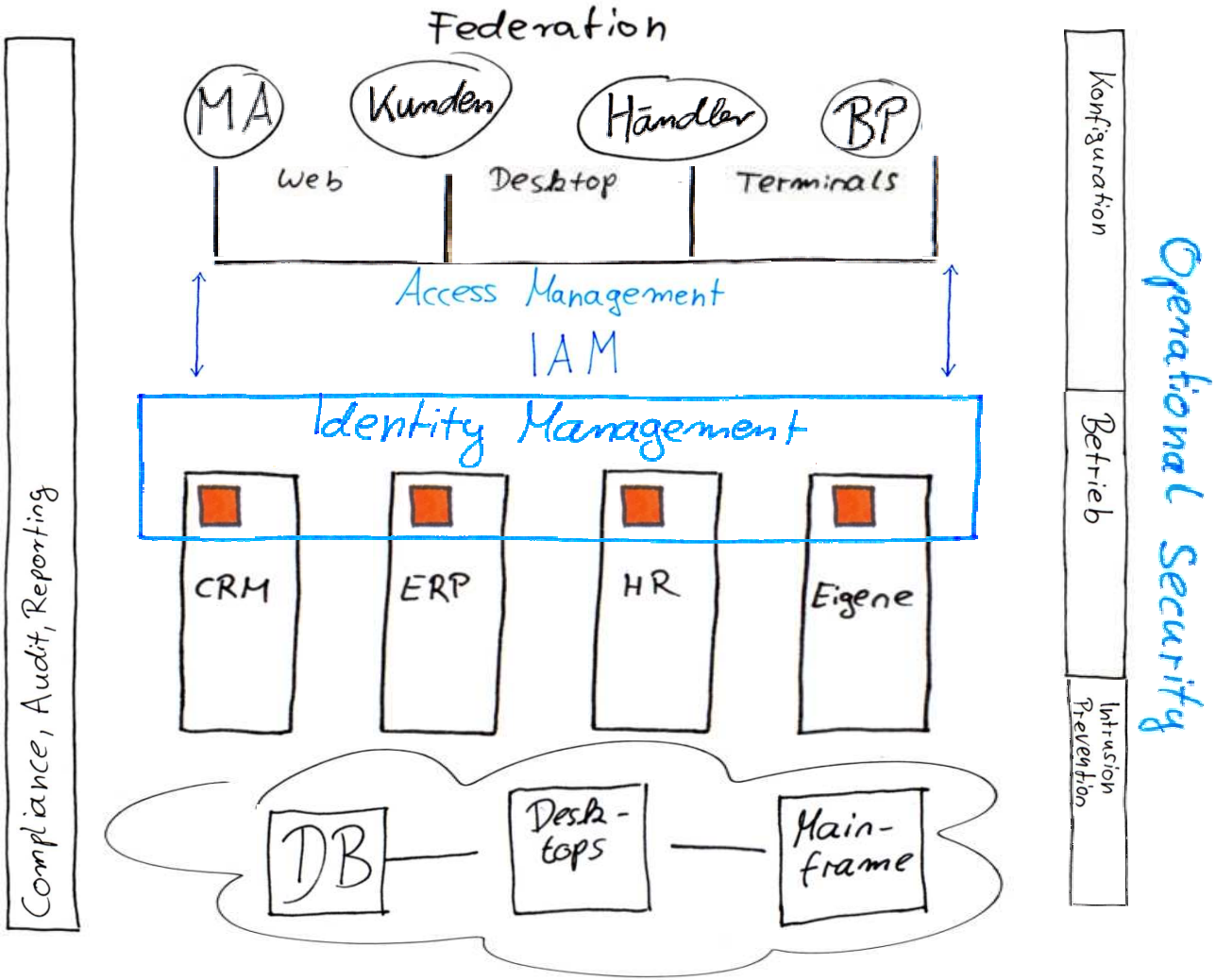
…Kritische Sicherheitsinformationen sollten in Echtzeit überwacht werden (Security Event Logs)…



Mit Hilfe von Intrusion Prevention werden kritische Sicherheitslücken in Systemen aufgedeckt und geschlossen



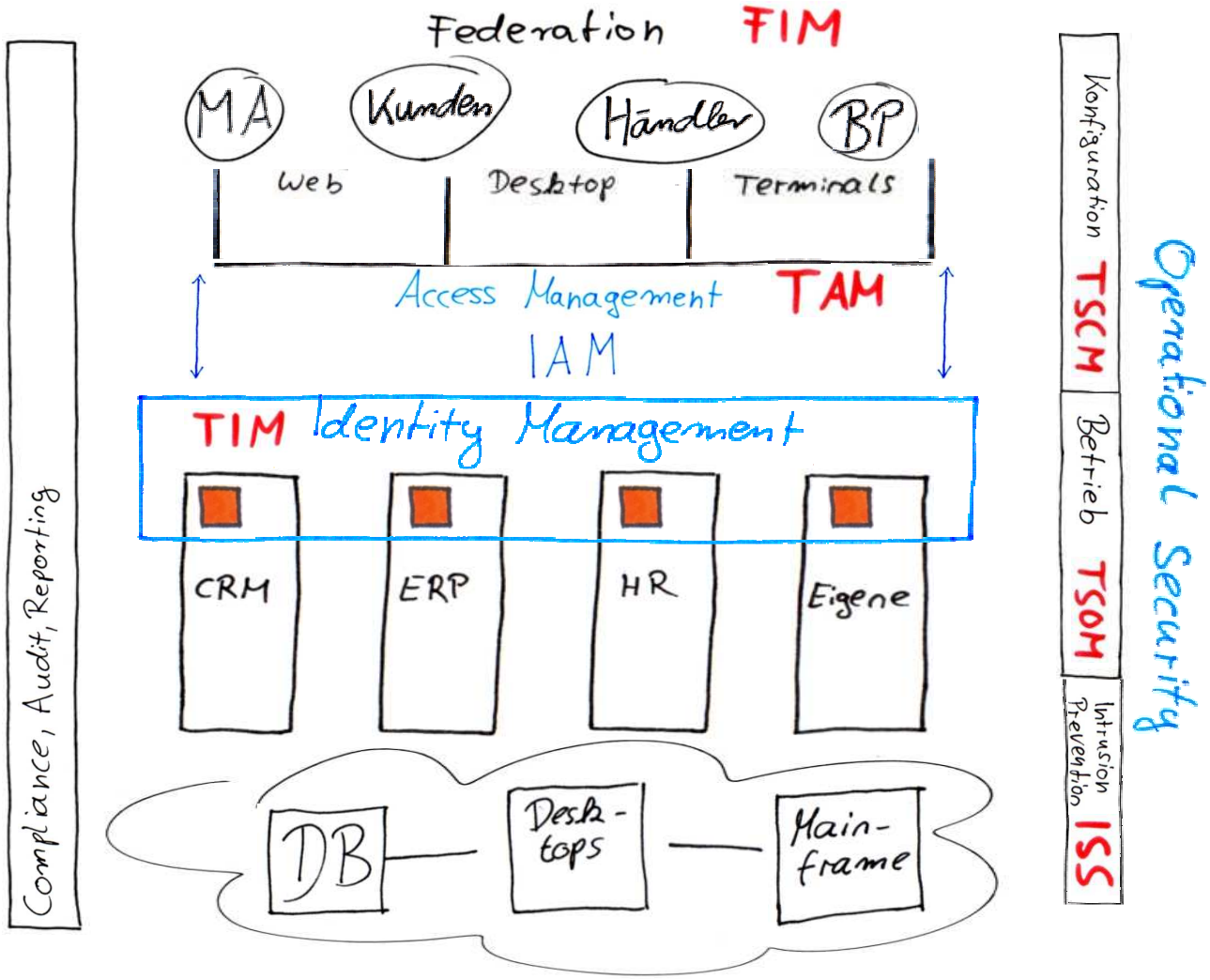
Wer führte **welche** Art von Aktion auf **welchem** System aus?



Compliance, Audit und Reporting stellt den 3. Themenkomplex dar.

Das IBM Tivoli Security Portfolio stellt für jede Anforderung die passende Lösung zur Verfügung!

- **Tivoli Identity Manager**
- **Tivoli Access Manager**
- **Tivoli Federated Identity Manager**
- **Tivoli Security Compliance Manager**
- **Tivoli Security Operations Manager**
- **Tivoli zSecure Suite**
- **Tivoli Compliance Insight Manager**
- **Tivoli Security Policy Manager**
- **Tivoli Key Lifecycle Manger**



Fragen ?

"Information security is a major priority at this company.
We've done a lot of stupid things we'd like to keep secret."

Obrigado
Portugal

Dziekuje
Poland

Dankschen
Austria

Thanks
United States

Takk
Norway

Toda
Israel

Gracias
Spain

Danke
Germany

Bedankt
Netherlands

Tak
Denmark

Dekuju
Czech Republic

Merci
France

Engraziel
Switzerland

Tesekkür ederim
Turkey

Tack
Sweden

Jag tackar
Finland

Thank You
United Kingdom

Grazie
Italy

Dakujem
Slovakia

Спасибо
Russia