

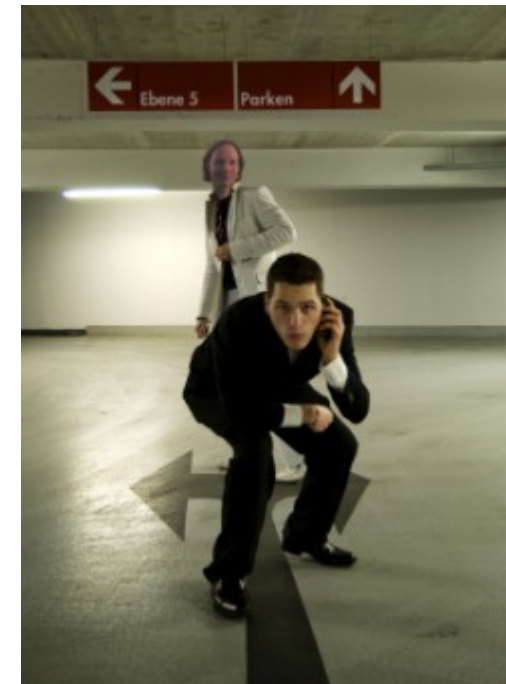
Mit Sicherheit IT-Risiken verringern

Berechtigungsmanagement unterstützt die Informationssicherheit



Referentin

- ▶ Studium der Diplom-Geographie in Frankfurt a.M.
- ▶ Geographische Informationssysteme (GIS),
Softwareentwicklung im Bereich Verkehrsgeographie
- ▶ Softwareentwicklung für Mobilfunk
 - Datensicherheit auf dem Handy (Bluetooth, Viren etc.)
- ▶ Seit 2007 bei Parks Informatik GmbH als Produktmanagerin



Parks Informatik GmbH

- ▶ 1999 begonnen mit Beratung und Erstellung von Berechtigungskonzepten für verschiedene Softwaresysteme (SAP R3, Windows Active Directory, Oracle etc.)
- ▶ Best-Practice-Verfahren und benutzbare Software für verbesserte IT-Sicherheit
- ▶ Entwicklung von Software mit Schwerpunkten
 - Berechtigungsmanagement, Identitymanagement
 - webbasierte Beantragungsverfahren
 - GIS-Systeme mit Berechtigungsmanagement
- ▶ Regelmäßige Beteiligung an interdisziplinären Forschungsprojekten zum kontinuierlichen Abgleich von neuen wissenschaftlichen Trends und Entwicklungen

Einführung

IT-Risiken

Berechtigungsmanagement

Zusammenfassung



Einführung

Fehlende oder falsche Prozesse

▶ Kleine Firmen:

- Berechtigungen auf Zuruf
- Niemand weiß wer worauf zugreifen darf
- Kennworte werden weiter gegeben

▶ Große Firmen:

- Formulare zur Berechtigungsvergabe
- langwierige Prozesse
- Rechte werden nie wieder entzogen
- immer zu viele Rechte
- zwei verschiedene Verschlüsselungsverfahren innerhalb eines Standorts



Einführung

Folgen und Probleme



[Home](#) [Newsticker](#) [7-Tage-News](#) [News-Archiv](#) [Leserforum](#)

[heise online](#) > [News](#) > [2008](#) > [KW 48](#) > [Telekom will nach Datenmissbrauch Strafanzeige](#)

30.11.2008 15:26

Telekom will nach Datenmissbrauch Strafanzeige

vorlesen / [MP3-Download](#)

Nach den jüngsten Datenpannen bei der [Telekom](#) kündigt der Boardvorsitzende die strafrechtliche Konsequenzen an. "Soweit wir einen Hinweis auf einen Täter haben, werden wir Strafanzeige erstatten", [sagte](#) der neue Vorstand des Unternehmens, Manfred Balz, dem Magazin *Focus*. Die fraglich umlaufende Daten [tausender Telekom-Kunden](#). Die fraglich umlaufenden Daten von rund 4000 Kunden seien nicht von der Telekom erstellt worden, sondern von einem Vertriebspartner. Der Verursacher werde noch gesucht. Der [Datenschutz-Vorwurf](#) bei einem Vertriebspartner nicht aus.



Sparkasse Köln/Bonn: Ärger mit einem Ex-Berater

Mitarbeiterdaten der Sparkasse an 25 Festplatten lagern. Der Mann hatte im WDR angegeben, die Daten ohne Abgabe einer sonst üblichen Vertraulichkeitserklärung und ohne Anonymisierung erhalten zu haben. Die Staatsanwaltschaft Köln schaltete sich daraufhin ein, um die Vorwürfe zu prüfen.

Nun scheint der Berater allerdings zurückzurudern: Er habe im Laufe

sueddeutsche.de

[Home](#) [E-Paper](#) [Immobilienmarkt](#) [Stellenmarkt](#) [Motormarkt](#) [Anzeigen](#) [SZ-Shopping](#)

[Politik](#) | [Wirtschaft](#) | **[Geld](#)** | [Kultur](#) | [Sport](#) | [Leben](#) | [Karriere](#) | [München](#) | [Bayern](#) | [Paris](#)

[Vermögen & Vorsorge](#)

GELD

[Ärger bei Goldman Sachs](#)

Geheimcode - einfach geklaut

07.07.2009, 17:09

Von [Nikolaus Piper](#), New York

Panik bei Goldman Sachs: Ein ranghoher Spezialist der Investmentbank hat offenbar einen wichtigen Code gestohlen - und eine Kopie in Deutschland deponiert. Noch fehlt jede Spur.

HAFT

[RUM](#) | [SPIEGEL WISSEN](#)

[Netzwelt](#) | [Wissens](#)

[Feedback](#) | [Merken](#)

Schrift:

Bahn wehrt sich gegen Spitzelvorwurf

Die Bahn gerät unter Druck: Der Staatskonzern soll bis zu tausend Mitarbeiter ausgespäht haben. Der Konzern hat Ermittlungen eingeräumt - aber nur im kleinen Stil. Es habe sich um Aktionen zur Bekämpfung von Korruption gehandelt.

Einführung

IT-Risiken

Berechtigungsmanagement

Zusammenfassung



IT-Risiken

Ursachen und Probleme

- ▶ Unwissenheit über Möglichkeiten, Spionage oder Datenmissbrauch abzuwenden
- ▶ Keinen Einsatz definierter Regelungen (Compliance)
- ▶ Fehlende Gesamtübersicht zu den einzelnen IT-Systemen im Unternehmen
- ▶ Unzureichende Kommunikation
- ▶ Fehlende Sensibilität für die Notwendigkeit, sich zu schützen



IT-Risiken einschränken durch gesetzliche Anforderungen

Gesetze und Standards in Unternehmen

- ▶ Basel II
- ▶ Deutsches Handelsrecht (HGB)
- ▶ Bundesdatenschutzgesetz (BDSG)
- ▶ Branchenspezifische Regelungen (z.B. MaRisk für Kreditinstitute)
- ▶ KonTraG

- ▶ COBIT
- ▶ ISO/IEC 27001 bzw. ISO/IEC 17799
- ▶ IDW PS 330



IT-Risiken Folgen

- ▶ Spionage
- ▶ Datenmissbrauch
- ▶ Haftung
- ▶ Vertrauensverlust
- ▶ Imageverlust
- ▶ Finanzielle Schäden



Einführung

IT-Risiken

Berechtigungsmanagement

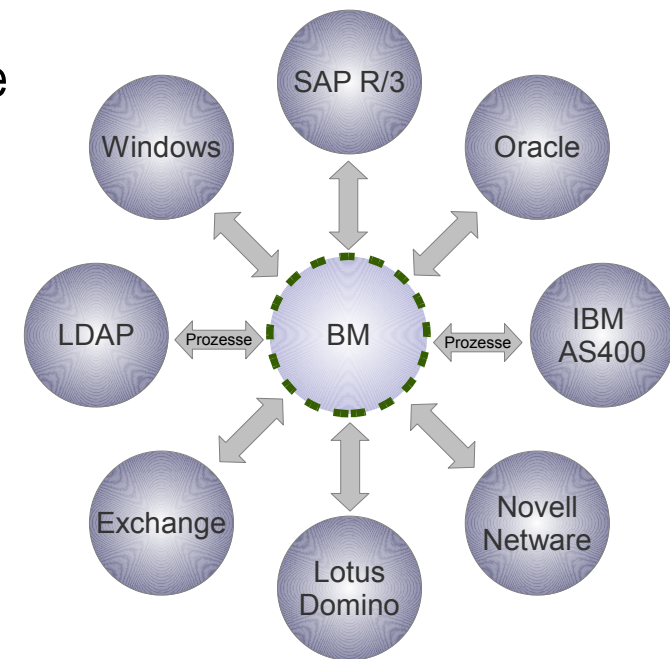
Zusammenfassung



Berechtigungsmanagement

Überblick

- ▶ Berechtigungsmanagement beinhaltet alle Prozesse zur Verwaltung von Benutzern und Berechtigungen in verschiedenen IT-Systemen
- ▶ Berechtigungsmanagement definiert und kontrolliert die System- und Datenzugriffe aller Mitarbeiter
- ▶ Berechtigungsmanagement ist eine wichtige technische Säule, um IT-Risiken zu verringern
- ▶ Einhaltung von Gesetzen und Richtlinien wird durch Berechtigungsmanagement unterstützt (Basel II, BDSG etc.)



Berechtigungsmanagement

Forderungen des BDSG



- ▶ Anlage zu § 9 Satz 1 des BDSG fordert u.a.:
 - **Zugangskontrolle**
Benutzername und Kennwort
 - **Zugriffskontrolle**
Verwaltung von Benutzern und Berechtigungen
 - **Weitergabekontrolle**
Protokollierung von Datenzugriffen
 - **Eingabekontrolle**
Nachträgliche Prüfung der Datenzugriffe



Berechtigungsmanagement

Zusätzliche Effekte



- ▶ Niemand bekommt überflüssige Berechtigungen
 - jeder Benutzer erhält nur die unbedingt benötigten Berechtigungen
- ▶ Kritische Berechtigungen werden nicht an einen einzigen Benutzer vergeben
 - automatische Prüfung bei der Berechtigungsvergabe durch die Einrichtung von Funktionstrennung
- ▶ Besondere Protokollierung bei heiklen Systemzugriffen
 - kritische Systemzugriffe werden protokolliert und gesondert ausgewertet



Berechtigungsmanagement

Praktische Umsetzung – Beispiel „Neuer Mitarbeiter“

- ▶ Sie stellen einen neuen Mitarbeiter ein:
 1. Daten des neuen Mitarbeiters eingeben
 2. In zentraler Verwaltungsanwendung Konto anlegen und Berechtigungen vergeben
 3. Mitarbeiter kann loslegen
 4. Bei Bedarf jederzeit weitere Berechtigungen zuweisen



Berechtigungsmanagement

Praktische Umsetzung – Weitere Beispiele

- ▶ **Abteilungswechsel eines Mitarbeiters**
 - bisherige Berechtigungen entziehen, neue notwendige einrichten
- ▶ **Ausscheiden eines Mitarbeiters**
 - alle Konten und Berechtigungen müssen deaktiviert bzw. gelöscht werden
- ▶ **Externe Mitarbeiter**
 - Einrichten von temporären und eingeschränkten Berechtigungen
- ▶ **Revision / Betriebsprüfung / Wirtschaftsprüfer**
 - es kann jederzeit festgestellt werden, welcher Mitarbeiter Zugriff auf welche Daten hat



Einführung

IT-Risiken

Berechtigungsmanagement

Zusammenfassung



Zusammenfassung

Berechtigungsmanagement – Vorteile

- ▶ Transparenter Überblick über Konten und Datenzugriffe
 - für Geschäftsführung, Revisoren, Systemverantwortliche etc.
- ▶ Risikominimierung
- ▶ Einsparungen
 - Systemverantwortliche können sich produktiv betätigen
- ▶ Vertrauensschaffung für Mitarbeiter und Kunden
- ▶ Rechtssicherheit
 - Verbesserung der Unternehmenssicherheit



Herzlichen Dank für Ihre Aufmerksamkeit!



„Die Summe unserer Erkenntnisse besteht aus dem
was wir gelernt, und aus dem, was wir vergessen haben.“

(Marie von Ebner-Eschenbach)



Für weitere Fragen stehen wir Ihnen gerne zur Verfügung:

Parks Informatik GmbH

Girardetstraße 2-38

D-45131 Essen

Tel. 0201 / 5 45 28 – 0

<http://www.parks-informatik.de>

parks@parks-informatik.de

