

Berechtigungsmanagement zur Unterstützung der Compliance



Compliance

Berechtigungsmanagement

Praktische Umsetzung

Zusammenfassung



Themenfeld Compliance

Überblick



- ▶ Absprachen oder auch freiwillige Kodizes zum Umgang miteinander gibt es in allen Lebensbereichen (Straßenverkehr, Haushalt, Schule, Sport etc.)
- ▶ Existierende Moral, gesellschaftliche Umgangsformen, Rechte und Pflichten haben sich teilweise zu Gesetzen und Verordnungen (Compliances) entwickelt
- ▶ Es wird gesellschaftlich erwartet, dass sich jeder Mensch „compliant“ verhält
- ▶ In Unternehmen bezeichnet der Begriff Compliance die Einhaltung von Gesetzen und Richtlinien sowie von Verträgen und spezifischen Regelungen



Themenfeld Compliance

Gesetze und Standards in Unternehmen

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

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



Themenfeld Compliance

In der Praxis ;-)



[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.

Compliance: Probleme Geschäftsprozesse



- ▶ Regelungen unvollständig oder gar nicht definiert
- ▶ Keine oder unzureichenden Kontrollen der Regelungen vorhanden
- ▶ Keine aktiven Maßnahmen (nur reagierend) vorhanden
- ▶ Unzureichende Kommunikation führt zu mangelnder Akzeptanz durch Benutzer: kein offensichtlicher Nutzen, eher bürokratischer Aufwand



Compliance: Probleme Technik



- ▶ Compliance-Regeln sind nicht technisch abgebildet
- ▶ Berechtigungen und Regeln sind nicht zentral definiert
- ▶ Fehlende Gesamtübersicht wegen getrennter Verwaltung der einzelnen IT-Systeme
- ▶ Fehlendes Wissen über Möglichkeiten zur technischen Umsetzung



Compliance: Ziele

Geschäftsprozesse



- ▶ Einsatz von effektiven Compliance-Mechanismen (Definition, Durchsetzung und Einhaltung von Richtlinien)
- ▶ Optimierung der Kontrollmechanismen
- ▶ Schnelle Reaktion bei Ereignissen mit sicherheitskritischem Hintergrund
- ▶ Erfüllung der Anforderungen von Mitarbeitern, Controllern, Revisoren (intern / extern)



Compliance: Ziele

Wirtschaftliche Aspekte

- ▶ Risiken minimieren
 - > Datenverlust, Imageverlust, Vermeidung von Strafzahlungen wegen Unterlassung
- ▶ Kosten senken
 - > keine materiellen Schäden, Mitarbeiter sind nicht mit unproduktiven Tätigkeiten belastet
- ▶ Gewinne steigern
 - > Stärkung des Vertrauens seitens Kunden und Mitarbeitern



Compliance

Berechtigungsmanagement

Praktische Umsetzung

Zusammenfassung



Themenfeld Berechtigungsmanagement

Überblick



- ▶ Compliance beschäftigt sich zu einem wichtigen Teil mit Berechtigungsmanagement
- ▶ 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 der Compliance
- ▶ Einhaltung von Gesetzen und Richtlinien wird durch Berechtigungsmanagement unterstützt (Basel II etc.)



Themenfeld Berechtigungsmanagement

Anforderungen



- ▶ Unkomplizierte technische Umsetzung von Richtlinien
- ▶ Einfache Zuordnung von Benutzern zu Rollen oder Stellen
- ▶ Abbildung eines organisatorischen Ist-Zustands des Unternehmens (Organigramm)
- ▶ Abbildung definierter Regelungen (4-Augen-Prinzip, Trennung von Verantwortung etc.) in allen Systemen
- ▶ Systemübergreifendes Berechtigungsmanagement
- ▶ Berücksichtigung wissenschaftlicher Grundlagen (z.B. Methode RBAC 'role based access control')



Themenfeld Berechtigungsmanagement

Grundlegende Regelungen



- ▶ Eindeutige Datenzugriffe durch Benutzeranmeldung
- ▶ Einrichtung von Benutzerkonten durch Genehmigungsverfahren (z.B. mit Vier-Augen-Prinzip-Policy)
- ▶ Konten ausgeschiedener Mitarbeiter zeitnah deaktivieren oder löschen
- ▶ Jeder Benutzer erhält nur die unbedingt benötigten Berechtigungen (principle of the least privilege)
- ▶ Kritische Berechtigungen – auf Funktionstrennung basierend – nicht an einen einzigen Benutzer vergeben
- ▶ Kritischen Systemzugriffe und Administrationstätigkeiten protokollieren



Compliance

Berechtigungsmanagement

Praktische Umsetzung

Zusammenfassung



Praktische Umsetzung

Berechtigungsmanagement – Aktives Handeln

- ▶ Maßnahmen zur Identifikation treffen (Gewährleistung einer Kontenanmeldung)
- ▶ Maßnahmen zur Benutzerverwaltung treffen (Genehmigungsverfahren, Kontenverwaltung)
- ▶ Maßnahmen zur Berechtigungsvergabe treffen (zeitnahe transparente Einrichtung, Entzug bei Unternehmensaustritt, Änderung bei Wechsel der Tätigkeit)
- ▶ Maßnahmen zur Protokollierung treffen (Berichte und Protokolle zu kritischen Datenzugriffen verfügbar und archivierbar machen)
- ▶ Maßnahmen zur Überprüfbarkeit treffen (Sicherheitsrichtlinien regelmäßig überprüfen, Verstöße auffinden und ahnden)



Praktische Umsetzung

Berechtigungsmanagement – Durchführung

- ▶ Unterstützung durch Experten einholen (intern, extern)
- ▶ Prozesse / Richtlinien definieren
- ▶ Notwendigkeit und Nutzen für alle Mitarbeiter verdeutlichen
- ▶ Verfahren / Werkzeuge für einen Beantragungs- und Genehmigungsprozess einsetzen
- ▶ Verfahren / Werkzeuge zur zentralisierten Verwaltung von Benutzern und Berechtigungen installieren
- ▶ Kontrolle / Revision / Überprüfung regelmäßig durchführen
- ▶ Verbesserung / Optimierung prüfen und ggf. umsetzen
- ▶ Ahndung von Verstößen, Belohnung bei Einhaltung einführen



Praktische Umsetzung

Berechtigungsmanagement – Vorteile

- ▶ Risikominimierung aktiv eingeleitet
- ▶ Einsparungen (Mitarbeiter können sich produktiv betätigen)
- ▶ Transparenter Überblick über Konten und Datenzugriffe (für Mitarbeiter, Geschäftsführung, Revisoren etc.)
- ▶ Vertrauensschaffung für Mitarbeiter und Kunden
- ▶ Abbau von Vorurteilen gegenüber Compliance-Maßnahmen (spießig, untauglich, unnütz, zu starke Kontrolle etc.)



Compliance

Berechtigungsmanagement

Praktische Umsetzung

Zusammenfassung



Zusammenfassung

Berechtigungsmanagement zur Unterstützung der Compliance

- ▶ Einsatz von Compliance notwendig zur Existenzsicherung
- ▶ Berechtigungsmanagement als ein Mittel zur Compliance-Durchführung
- ▶ Unkomplizierte Umsetzung von Unternehmensregelungen in digitale Technik
 - > Zentrales Berechtigungsmanagement für Zugriffskontrolle
 - > Computergestütztes Beantragungs- und Genehmigungsverfahren
- ▶ Schafft Transparenz und Vertrauen für alle Beteiligten



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

Girardetstr. 2-38

D-45131 Essen

Tel. 0201 / 5 45 28 – 0

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

parks@parks-informatik.de

