



‘Datenschutz mit Augenmaß’ am Beispiel Eintracht Frankfurt Fußball AG



Cebit 2010, 03.03.2010

Dipl.-Betriebswirt (FH) Steffen Weber,
ISO 27001 Lead Auditor
INTARGIA Managementberatung GmbH

ZEIT ONLINE

DEUTSCHLAND INTERNATIONAL WIRTSCHAFT BILDUNG WISS

Campus | Jobs | Immobilien | Geld | Gesundheit | Literatur | Musik | Reisen |

STARTSEITE » WIRTSCHAFT

DRUCKEN PDF-ANSICHT VERSENDEN TEXTGRÖSSE

ÜBERWACHUNG

Bahn bespitzelte Hunderte Mitarbeiter

© ZEIT ONLINE, dpa 21.1.2009 - 17:09 Uhr
SCHLAGWORTE: Datensicherheit Datenschutz

Nach Lidl und Telekom hat nun offenbar auch die Deutsche Bahn ihren Datenskandal. Sie ließ über Jahre ihr oberes Management von einer Detektei ausspionieren



Wie das Magazin Stern berichtet, hat die Deutsche Bahn in den vergangenen Jahren in großem Stil Mitarbeiter ausforschen lassen. Davon seien mehr als 1000 Menschen betroffen gewesen, darunter ein Großteil des oberen



FINANCIAL TIMES DEUTSCHLAND

11 Bewertungen ★★☆☆☆

Kriminalität trifft jede zweite Firma

weitere deutsche Firma ist laut einer Studie Opfer von Kriminalität. Rund die Hälfte der selbst, davon etwa ein Fünftel

Frankfurter Allgemeine FAZ.NET

24. Mai 2008

Home : Politik Wirtschaft Feuilleton : Sport : Gesells
Reise : Wissen : Auto : Computer : Beruf & Chance : Kunstmarkt

Aktuell » Wirtschaft » Unternehmen

Telekom bestätigt Bespitzelungs-Skandal

Telefonverbindungen der Manager ausgespäht

24. Mai 2008 Die Deutsche Telekom soll heimlich Telefonverbindungsdaten ihrer Manager ausspioniert haben, um undichte Stellen in Vorstand und Aufsichtsrat aufzuspüren.

Nach derzeitigen Erkenntnissen sei es 2005 und nach aktuellen Behauptungen auch 2006 zu einer missbräuchlichen Nutzung von Verbindungsdaten gekommen, teilte das Unternehmen am Samstag in Bonn mit und bestätigte einen Bericht des Magazins „Der Spiegel“. Wir haben die Staatsanwaltschaft eingeschaltet und werden sie bei ihren Ermittlungen um eine lückenlose Aufklärung unterstützen“, sagte Telekom-Chef René Kölsch am Freitag.

WELT ONLINE

Schrift: - + Bookmark versenden drucken

DATENKLAU

Hacker stehlen Bewerberdaten bei Beraterfirma

4. September 2008, 14:09 Uhr

Die Unternehmensberatung PwC hat Anzeige gegen Unbekannt erstattet. Hacker verschafften sich Zugriff auf eine Datenbank für Jobsuchende, die sich bei PricewaterhouseCoopers beworben hatten. Jetzt ermittelt die Staatsanwaltschaft.

Nach einem Hacker-Angriff auf eine Datenbank hat die Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PwC) die Frankfurter Staatsanwaltschaft eingeschaltet. Das Unternehmen stellte nach eigenen Angaben Strafanzeige. Zuvor sei aufgefallen, dass Hacker von einer Datenbank für Jobsuchende Informationen gestohlen hatten.

wiwo.de

Unternehmer & Märkte Politik Karriere

wiwo.de » Finanzen » Tausende Kontodaten missbraucht

Datenklau

Tausende Kontodaten missbraucht

12.08.2008 | Jetzt kommentieren! | ☆☆☆☆☆ 0 (0)

Es klingt nach einem riesigen Betrugsskandal. Datenhändler sollen eine CD mit den Kontonummern von tausenden Bankkunden verkauft haben. Anschließend wurden die Konten der ahnungslosen Opfer geplündert. Verbraucherschützer rufen dazu auf, die eigenen Kontoauszüge genau zu prüfen.

Druckversion Artikel senden Bookmarks

Kurzportrait INTARGIA Managementberatung GmbH

- Seit 1989 **zielorientierte Beratung und Umsetzungsunterstützung** an den Nahtstellen zwischen Strategien, Prozessen und IT-Management
- Unternehmenssitz in Dreieich bei Frankfurt am Main, 20 Mitarbeiter
- **Ganzheitliche Sicht:**
Strategien \leftrightarrow Prozesse \leftrightarrow Technologien \leftrightarrow Wirtschaftlichkeit
- Erarbeitung und Umsetzung **pragmatischer Lösungen**
- **Herstellerneutrale Beratung**, frei von subjektiven Produkt- und Lieferinteressen
- Beratungsschwerpunkte **IT-Management-** und **IT-Projektberatung**

IT-Managementberatung



„Wir unterstützen unsere Kunden dabei, aus dem operativen Instrument IT ein unternehmerisches, strategisches Planungs- und Führungsinstrument zu machen.“



Strategie & Masterplan

IT-Strategie als Enabler und Basis für effizientes IT-Business-Alignment.



Service Management & IT-Organisation

Die Service Orientierte Organisation (SOO) als Dirigent von Menschen, Prozessen und internen sowie externen IT-Dienstleistern.



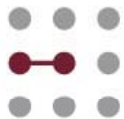
Prozess & Konzept

IT als Plattform für erfolgreiche Geschäftskonzepte sowie effiziente und ressourcenschonende Abläufe.



Auditierung und Due Diligence

Existenzieller Veränderungsprozesse (wie M&A) und kritische Situationen des IT-Managements benötigen eine unabhängige, neutrale Situationsdiagnose und Begleitung.



Softwareauswahl & Vertrag

Das Treffen der "richtigen" Auswahlentscheidung und die Compliance-konforme Gestaltung von Verträgen.



IT-Risikomanagement

Die effektive Minimierung der Geschäftsrisiken durch integriertes IT-Sicherheits-, Datenschutz-, Kontinuitätsmanagement-, Compliance- und Projektrisiko-Management.



(Out-)Sourcing

Fremdbezug von IT-Services als Gestaltungsoptionen im Spannungsfeld der erforderlichen Qualität sowie von Kosteneffizienz und Flexibilität.

IT-Managementberatung



„Wir unterstützen unsere Kunden dabei, aus dem operativen Instrument IT ein unternehmerisches, strategisches Planungs- und Führungsinstrument zu machen.“



Strategie & Masterplan

IT-Strategie als Enabler und Basis für effizientes IT-Business-Alignment.



Service Management & IT-Organisation

Die Service Orientierte Organisation (SOO) als Dirigent von Menschen, Prozessen und internen sowie externen IT-Dienstleistern.



Prozess & Konzept

IT als Plattform für erfolgreiche Geschäftskonzepte sowie effiziente und ressourcenschonende Abläufe.



Auditierung und Due Diligence

Existenzieller Veränderungsprozesse (wie M&A) und kritische Situationen des IT-Managements benötigen eine unabhängige, neutrale Situationsdiagnose und Begleitung.



Softwareauswahl & Vertrag

Das Treffen der "richtigen" Auswahlentscheidung und die Compliance-konforme Gestaltung von Verträgen.



(Out-)Sourcing

Fremdbezug von IT-Services als Gestaltungsoptionen im Spannungsfeld der erforderlichen Qualität sowie von Kosteneffizienz und Flexibilität.



IT-Risikomanagement

Die effektive Minimierung der Geschäftsrisiken durch integriertes IT-Sicherheits-, Datenschutz-, Kontinuitätsmanagement-, Compliance- und Projektrisiko-Management.

Einige Referenzen aus dem Bereich IT-Risikomanagement



Eintracht Frankfurt Fußball AG

Datenschutzmanagement, externer betrieblicher Datenschutzbeauftragter



expert AG

Datenschutzmanagement, externer betrieblicher Datenschutzbeauftragter



Lufthansa AG

Compliance Management



Deutscher Akademischer Austauschdienst

IT-Sicherheitskonzept



DAP GmbH

Datenschutzmanagement, externer betrieblicher Datenschutzbeauftragter



Hochschule Aschaffenburg

IT-Sicherheitsaudit

Agenda

Datenschutz

Datenschutz – Anforderungen an Organisationen

Beitrag

Der Beitrag zur Werthaltigkeit von Organisationen

DSMS

Datenschutz mit Augenmaß

Maßnahmen

Beispielhafte Maßnahmen bei EFFAG

Fragen

Ihre Fragen

Agenda

Datenschutz

Datenschutz – Anforderungen an Organisationen

Beitrag

Der Beitrag zur Werthaltigkeit von Organisationen

DSMS

Datenschutz mit Augenmaß

Maßnahmen

Beispielhafte Maßnahmen bei EFFAG

Fragen

Ihre Fragen

Datenschutz – Anforderungen an Organisationen

Wichtigste Norm: Bundesdatenschutzgesetz

- Schutz personenbezogener Daten natürlicher Personen (§ 3 Abs. 1 BDSG)
- Öffentliche und nicht-öffentliche Stellen (§ 1 Abs. 2 BDSG)
- Automatisierte Verarbeitung von Daten (§ 3 Abs. 2 BDSG)
- Zulässig falls kodifiziert oder Betroffener eingewilligt hat (§ 4 BDSG)
- Wesentliche Pflichten von Organisationen
 - Datenschutzbeauftragter (§ 4f)
 - Technische und organisatorische Maßnahmen (§ 9)
 - Informationspflicht bei Erhebung (§ 4 Abs. 3), Auskunftspflicht ggü. Betroffenen (§ 34), Auskunftspflicht ggü. Aufsichtsbehörde (§ 38 Abs. 3), Verpflichtungspflicht der Mitarbeiter auf Datengeheimnis (§ 5), Verpflichtungspflicht von Dritten bei Auftragsdatenverarbeitung (§ 11)
- Konsequenzen bei Nichtbeachtung
 - Bußgelder bis 300.000 Euro (§ 43), Strafrechtliche Konsequenzen – Bis zu zwei Jahren Freiheitsstrafe (§ 44), Schadensersatzansprüche, Reputationsschaden

Agenda

Datenschutz

Datenschutz – Anforderungen an Organisationen

Beitrag

Der Beitrag zur Werthaltigkeit von Organisationen

DSMS

Datenschutz mit Augenmaß

Maßnahmen

Beispielhafte Maßnahmen bei EFFAG

Fragen

Ihre Fragen

Der Beitrag von Datenschutz zur Werthaltigkeit von Organisationen

1. Compliance

- Vermeidung von Geldbußen, Schadensersatzforderungen und strafrechtlicher Konsequenzen
- Schutz vor Reputationsschäden (Umsatzeinbußen und Wiederherstellung Marktvertrauen)

2. Risikominimierung

- Interne Bedrohungen (Menschliche oder technische Fehler, Unachtsamkeit)
- Externe Bedrohungen (Wirtschaftsspionage/Social Engineering, Hacking, Malware etc.)

3. Prozess- und Organisationsverbesserung

- Transparenz durch Beschäftigung mit Prozessen
- Datenschutzkonform geplante Verfahren, Anwendungen und Systeme
- Verbesserung des Verständnisses, was ein angemessenes Verhalten im Umgang mit Daten von Kollegen und Kunden ist

4. Wettbewerbsvorteile

- Kommunizierbarer Wettbewerbsfaktor für Kunden, Partner und Mitarbeiter

Agenda

Datenschutz

Datenschutz – Anforderungen an Organisationen

Beitrag

Der Beitrag zur Werthaltigkeit von Organisationen

DSMS

Datenschutz mit Augenmaß

Maßnahmen

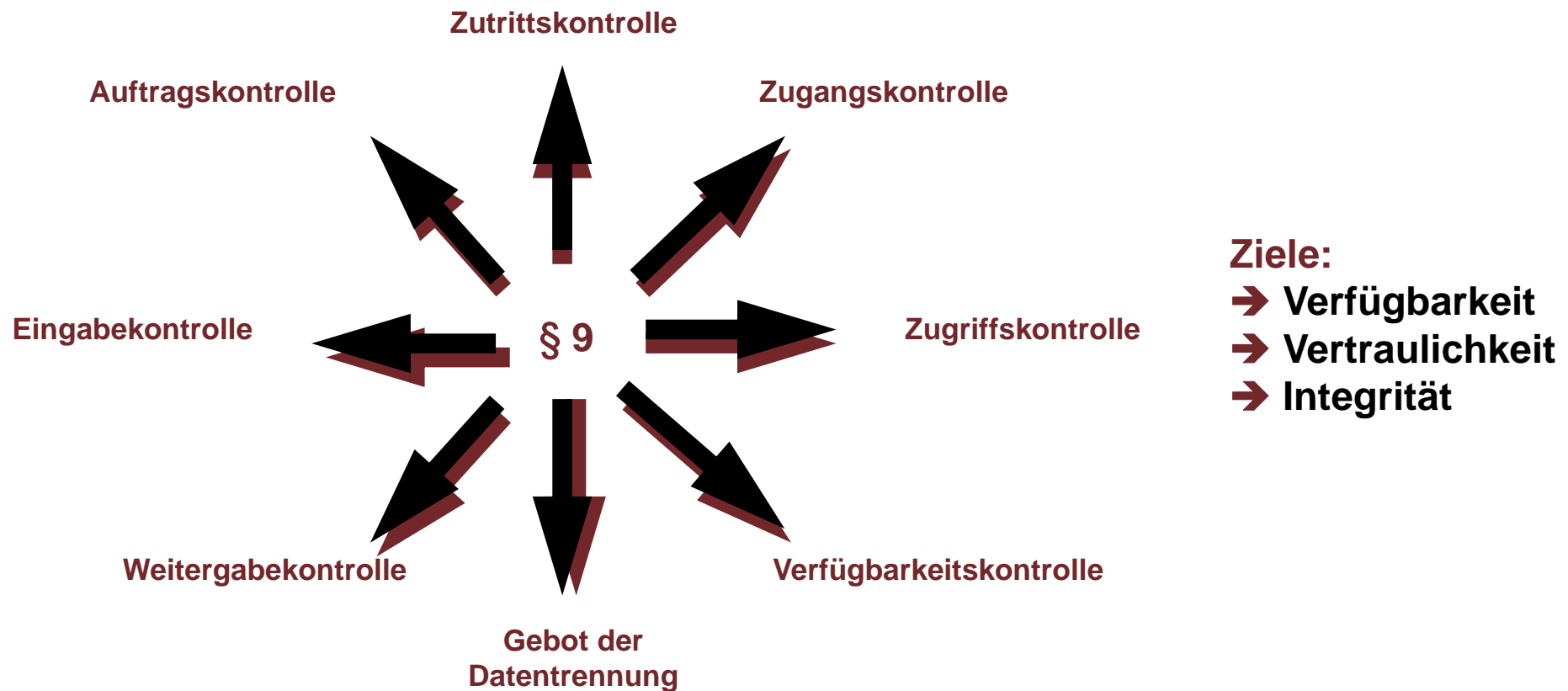
Beispielhafte Maßnahmen bei EFFAG

Fragen

Ihre Fragen

Das INTARGIA Datenschutzmanagement-System

§ 9 BDSG – Notwendige technische & organisatorische Maßnahmen



Das INTARGIA Datenschutzmanagement-System

Quellen für technische und organisatorische Maßnahmen

- Normen
- Standards
 - BSI 100-1 bis 100-4, IT-Grundschutz-Kataloge
 - ISO 27000ff.
- Praxisleitfäden
 - GDD (Mitarbeiterdatenschutz, Kundendatenschutz)
 - BSI, „Baustein B 1.5 Datenschutz / Quelle: BfDI“
- Arbeitshilfen
 - GDD
 - ULD
- Praxiserfahrungen



Rahmenbedingungen des Umfeldes der Eintracht Frankfurt Fußball AG



- Aktiengesellschaft, ausgegründet aus dem e. V.
- Ca. 50 Mitarbeiter (exkl. Spieler)
- Beinhaltet Mitarbeiter der AG und Spieler der Profimannschaften
- Sitz des Unternehmens in der Commerzbank-Arena, Frankfurt
- Eigene IT-Abteilung

→ Mittelständisches Unternehmen

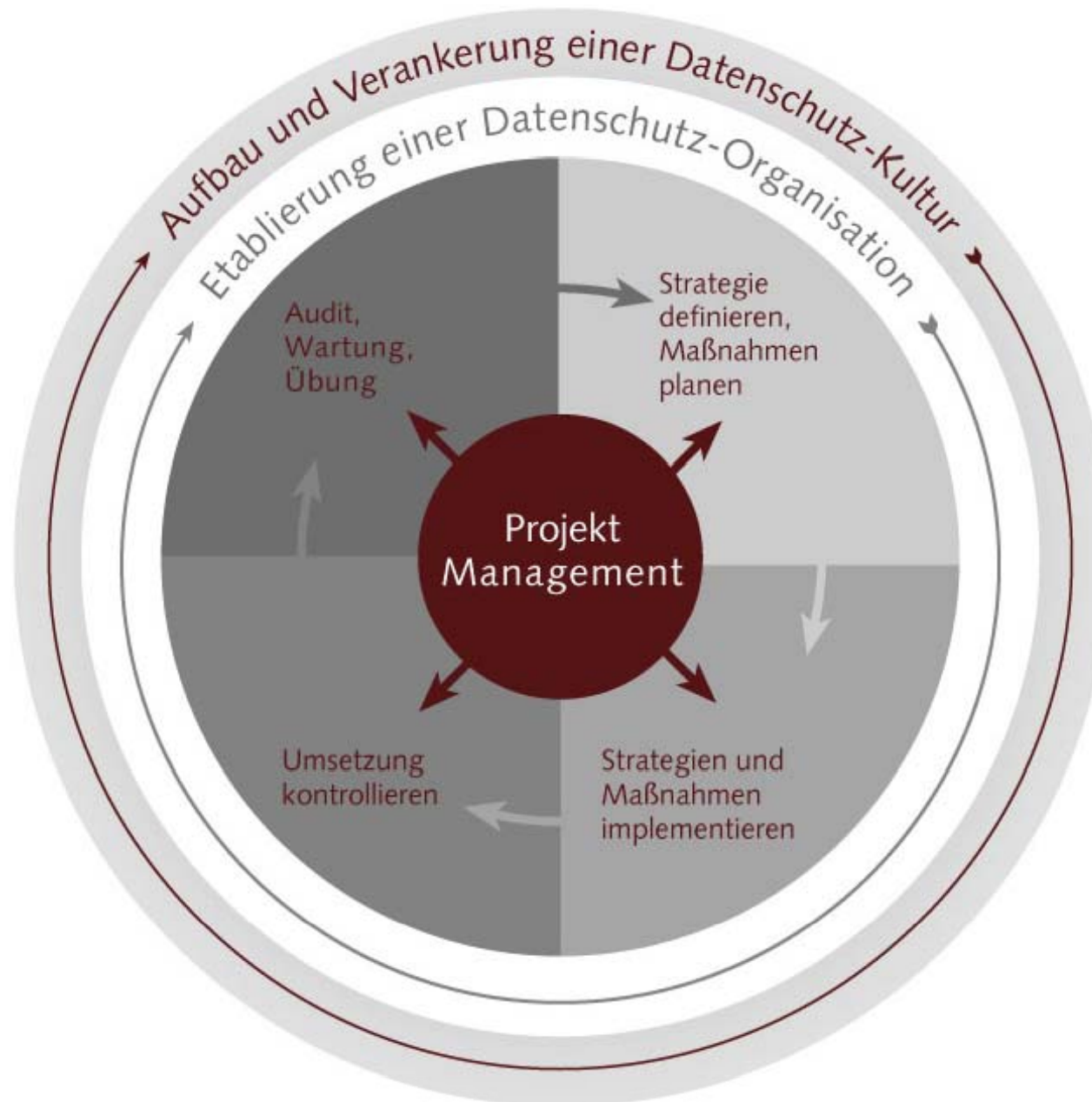
- Organisation steht im Blickfeld der Öffentlichkeit
- (Hoch-)kritische Aspekte wie z. B. Spielerverträge, Medizinische Informationen, Sponsorenverträge, Fans (z. B. Jahreskarteninhaber, Business-Kunden etc.)

Rahmenbedingungen des Umfeldes der Eintracht Frankfurt Fußball AG



- 2007: Datenschutz als Wettbewerbsfaktor im Unternehmen erkannt
- Durchführung eines Datenschutzaudits
- Bestellung von INTARGIA Geschäftsführer Dr. Thomas Jurisch zum externen Datenschutzbeauftragten
- Seitdem jährliche Re-Audits zur kontinuierlichen Verbesserung des Datenschutzniveaus

→ Einführung des INTARGIA Datenschutzmanagement-Systems



Das INTARGIA Datenschutzmanagement-System

Schritt 1: Durchführen eines Initial-Audits

- Selbstanalyse
- Vor-Ort-Audit mit Stichprobenprüfung
- Aufdecken von notwendigem Handlungsbedarf
- Erstellung eines umfassenden Auditberichts mit Informationen über Ist-Situation, Untersuchungsergebnissen und Handlungsempfehlungen
- Ergebnispräsentation und Maßnahmenplanung



Das INTARGIA Datenschutzmanagement-System

Initialaudit – Beispiele für Auditfragen

Audit,
Wartung,
Übung

Teil B: Prüfkatalog allgemeiner Teil

1) Zutrittskontrolle

Beschreibung: Mit den einzelnen Zutrittskontrollen ist zu unterbinden, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erlangen können. Es stellt sich stets die Frage, welche technischen und organisatorischen Maßnahmen zur räumlichen Zutrittskontrolle eingesetzt werden.

Fragen	Antworten
Existiert ein zentraler Werkschutz/Pförtner/Empfang?	
Existieren Türsicherungen an allen relevanten Zugangstüren zum Gebäude/Stockwerk/Abteilung? (Realisiert z. B. per Schliesssystem, Magnetkarten, Chipkarten, Ausweislesegeräte, Zugangscodes/Numpads)?	
Wird die Vergabe dieser Zutrittsmedien systematisch vorgenommen, überwacht und ist dies revisionssicher dokumentiert (z. B. per Schlüsselbuch)?	

Das INTARGIA Datenschutzmanagement-System

Initialaudit – Beispiel für Auditbericht

5.2.3 Zugangskontrolle

Zugangskontrollen sollen verhindern, dass Unbefugte Datenverarbeitungsanlagen nutzen können. Es geht dabei um eine sichere Identifikation mit anschließender Authentifikation des Nutzers. Der durch Zugangskontrollen umfasste Bereich erstreckt sich vom Einschalten des informationstechnischen Gerätes bis zum „Hochfahren“ des Betriebssystems. Der Bereich der Zugangskontrollen umfasst nicht den Zugriff auf Applikationen, Daten oder periphere Geräte.

Fragen	
Existiert ein zentraler Zugang zu den Systemen (z. B. per Identity and Access Management, Single-Sign-on etc.)?	<input checked="" type="radio"/>
Welche IT-Systeme sind mit einer dezentralen Zugangskontrolle ausgestattet? Wie ist diese ausgestaltet?	<input type="radio"/>
Gibt es eine organisatorische Rolle, welche dieses Vergabeverfahren dokumentiert, kontrolliert und aktualisiert?	<input type="radio"/>
Wie wird mit den Zugängen von ausscheidenden Mitarbeitern umgegangen? Ist dieses Verfahren revisionssicher dokumentiert?	<input type="radio"/>

Status

Es existiert kein Single-Sign-On. Es sind verschiedene Zugänge für die zwei Hauptprogramme Navision und Windows vorhanden. Die Zuständigkeit über die Zugänge hat die IT-Abteilung. Eine Dokumentation über die Vergabe von Zugängen existiert. Innerhalb des Vergabeprozesses muss die Fachabteilung den Zugang beantragen. Die IT-Abteilung sendet daraufhin ein auszufüllendes Dokument.

Der Entzug der Zugänge ist auskunftsgemäß aktuell noch nicht optimal geregelt.

Untersuchungsergebnisse

Der Prozess des zentralen Entzugs ist noch nicht vollständig automatisiert umgesetzt.

Handlungsempfehlungen

- Der Prozess für die Vergabe und den Entzug der Zugangsrechte sollte im Rahmen der unternehmensweiten Einführung des Laufzettels (Verantwortlich: Personalabteilung) vollständig in die Organisation integriert werden.

Audit,
Wartung,
Übung

Das INTARGIA Datenschutzmanagement-System

Schritt 2: Strategie definieren, Maßnahmen planen

- Festlegung der Datenschutzstrategie für das Unternehmen:
 - Auswahl von Maßnahmen
 - Priorisierung der Maßnahmen
 - Vergabe von Verantwortlichkeiten
 - Festlegung von Umsetzungsfristen

A grey quarter-circle graphic located on the right side of the slide, containing the text "Strategie definieren, Maßnahmen planen".

Strategie
definieren,
Maßnahmen
planen

Das INTARGIA Datenschutzmanagement-System

Schritt 3: Strategie und Maßnahmen implementieren

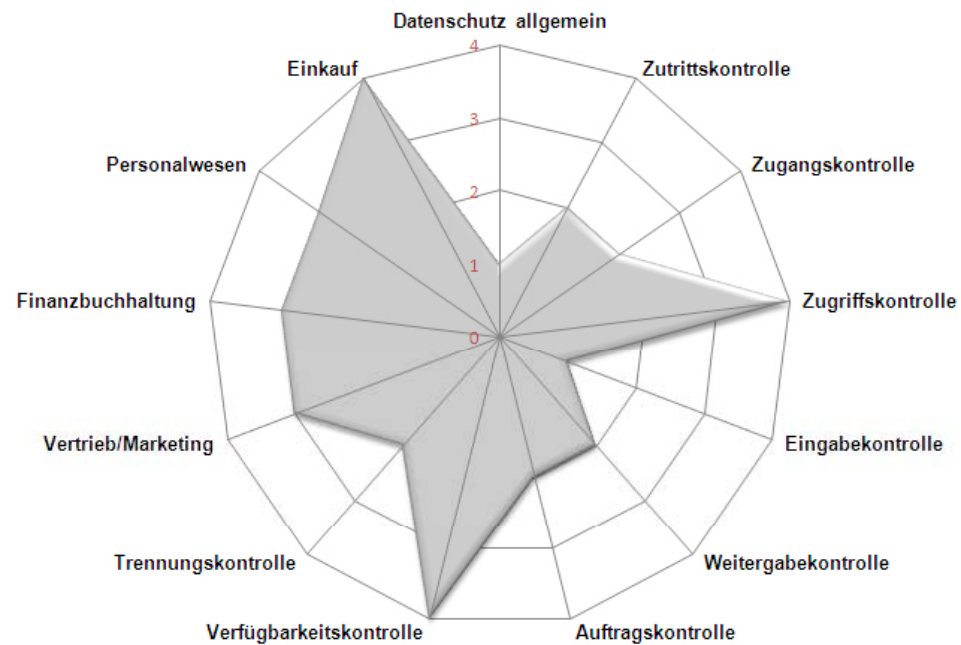
- Aufbau einer Datenschutz-Organisation
- Umsetzung der technischen und organisatorischen Maßnahmen
- Datenschutzhandbuch
- Verzeichnis der Verfahrensverzeichnisse
- Datenschutz-Kultur
- Datenschutzbeauftragter als ständiger, zentraler Ansprechpartner

Strategien und
Maßnahmen
implementieren

Das INTARGIA Datenschutzmanagement-System

Schritt 4: Umsetzung kontrollieren

- Zyklische Audits
- Fortschrittsmessung mit Hilfe eines Reifegradmodells



- Regelmäßiges Reporting, Dokumentation von Status und Fortschritt



Agenda

Datenschutz

Datenschutz – Anforderungen an Organisationen

Beitrag

Der Beitrag zur Werthaltigkeit von Organisationen

DSMS

Das INTARGIA Datenschutzmanagement-System

Maßnahmen

Beispielhafte Maßnahmen bei EFFAG

Fragen

Ihre Fragen

Beispielhafte Maßnahmen bei Eintracht Frankfurt Fußball AG

- Bestellung eines externen Datenschutzbeauftragten
- Ergänzungen in den Dienstleisterverträgen
- Einführung eines Laufzettelprozesses zur digitalen Abbildung der Prozesse von der Bewerbung eines Mitarbeiters bis zur Vertragsbeendigung
- Optimierung der Zutrittsmedien
- Erstellung eines Verschlüsselungskonzeptes für mobile Medien (Notebooks, PDA, USB-Sticks etc.)
- Optimierung des Datensicherungskonzeptes
- Durchführung von Datenschulungen mit allen Mitarbeitern
- Etc...

Agenda

Datenschutz

Datenschutz – Anforderungen an Organisationen

Beitrag

Der Beitrag zur Werthaltigkeit von Organisationen

DSMS

Das INTARGIA Datenschutzmanagement-System

Maßnahmen

Beispielhafte Maßnahmen bei EFFAG

Fragen

Ihre Fragen



INTARGIA

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:

INTARGIA Managementberatung GmbH

Steffen Weber

Tel: +49 (0) 6103 – 50860

it-risikomanagement@intargia.com