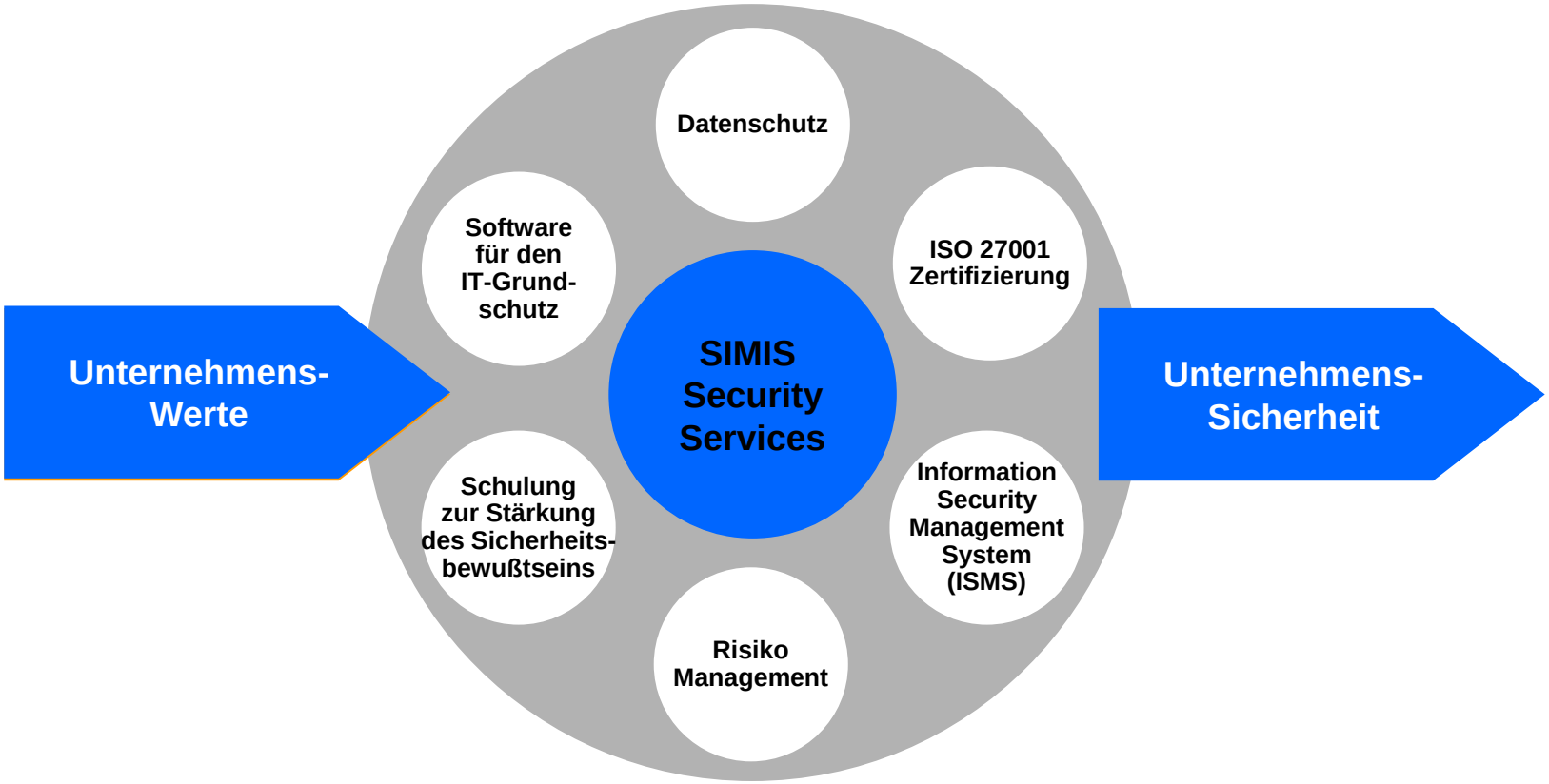
Informationssicherheit und Datenschutz im Unternehmen

Erich Zimmermann
Externer Datenschutzbeauftragter (IHK)
Sprecher der Initiative „Sicherheit mit System“

e.zimmermann@simis.org

www.simis.org

SiMiS - Sicherheit mit System –
Security Services - Übersicht



Wir schützen Unternehmenswerte durch Datenschutz-Services und zertifizierbare Informationssicherheit (ISO 27001)

ökonomisch, methodisch, skalierbar und zu Festpreisen.

Datenschutz im Unternehmen

Datenschutz in der Presse …Deutsche Bahn, Kreditkarten, Sony usw.

20. Mai 2008 Drucken | Senden | Leserbrief | Bookmark

DETEKTIV-OFFENSIVE Schrift: – +

Lidl ließ mehr als 500 Filialen überwachen

Im Spitzelskandal bei Lidl werden erste Details bekannt. Laut baden-württembergischem Innenministerium ließ der Discounter mehr als 500 Filialen von Detektiven überwachen. Datenschützer drohen mit einem Bußgeld von bis zu 250.000 Euro.

Stuttgart - Erste Fortschritte bei der Aufklärung der Lidl-Spitzelaffäre: Nach Angaben von Baden-Württembergs Innenminister Heribert Rech (CDU) hat der Discounter Lidl mehr als 500 Filialen in mehreren Bundesländern von Detekteien überwachen lassen.

DPA

Lidl (in Stuttgart): Intimste Details protokolliert

Die Aufträge hätten mehr als 30 rechtlich selbstständige Regionalgesellschaften des Unternehmens erteilt. Das erklärte Rech auf Anfrage eines Grünen-Landtagsabgeordneten in Stuttgart.

Rech berief sich bei seinen Angaben auf Daten, die Lidl den Datenschützern des Landes mitgeteilt habe. Es ist das erste Mal, dass eine konkrete Zahl von Spitzelfällen genannt wird. Die Überwachungsmaßnahmen hätten sich dem Discounter zufolge "nicht vorrangig gegen Mitarbeiter gerichtet", sagte Rech. Genau das legen jedoch die Dokumente nahe, die der "Stern" im April veröffentlicht hatte. Demnach haben die von Lidl beauftragten Detekteien intimste Details aus dem Privatleben der Supermarkt-Mitarbeiter protokolliert (mehr...).

Alle Artikel

01.06.2008 Drucken | Senden | Bookmark | Leserbrief | Merken

AUSSPÄH-AFFÄRE Schrift: – +

Obermann schwört Telekom-Kunden Datensicherheit

In der Spitzel-Affäre um die Deutsche Telekom ist Vorstands-Chef René Obermann in die Offensive gegangen: Er habe nichts vertuscht und werde die Verantwortlichen zur Rechenschaft ziehen, sagt er in einem Interview - und verspricht: "Die Kundendaten sind bei der Telekom sicher."

Berlin - Im Zusammenhang mit der Bespitzelung von Aufsichtsräten und Journalisten durch die Deutsche Telekom hat Vorstand-Chef René Obermann den Vorwurf der Vertuschung vehement von sich gewiesen. "Ich habe von einem ersten Fall von Datenmissbrauch bei der Telekom im Sommer des vergangenen Jahres erfahren und danach nichts vertuscht, sondern die nötigen personellen und organisatorischen Konsequenzen gezogen", sagte er der "Bild am Sonntag".

AP

Telekom-Vorstandsvorsitzender Rene Obermann: Verantwortliche "ohne Ansehen von Rang und Person zur Rechenschaft" ziehen

Datenschutz im Unternehmen

31.05.2011 um 19:22 Uhr

Hacker klauen Kundendaten bei Neckermann.de

Frankfurt/Main (dpa) - Hacker haben beim Versandhändler Neckermann.de Daten von 1,2 Millionen Gewinnspielteilnehmern abgegriffen. Davon sind vorwiegend Nutzer aus Deutschland betroffen, teilte das Unternehmen mit. **(Bild dpa)**

Den Kriminellen fielen nach Unternehmensangaben vom Dienstag (31. Mai) Namen und E-Mail-Adressen von Nutzern vorwiegend aus Deutschland in die Hände. "Unser Hauptserver und damit unser Online-Shop war nicht betroffen", betonte eine Neckermann-Sprecherin. Der Angriff sei am vergangenen Donnerstag aufgefallen. Neckermann.de habe umgehend die Sicherheit des Servers verstärkt und die betroffenen Gewinnspielteilnehmer informiert. Bei der Staatsanwaltschaft Frankfurt wurde Anzeige gegen Unbekannt gestellt.

Ich hab' nichts zu verbergen!

Blutgruppe B, Herzinfarktrisiko 14%, KV-Datensatz
(Genanalyse) liegt vor, Krankenversicherung: Standard,
Zusatzversicherung angeboten (File 23A18)
Risikoklasse 4 - (Nachuntersuchung erforderlich
in Q8, Verdacht auf KV-Risiko Stufe 3)
Drogenkonsum: Nicht aktuell.
Alkoholkonsum mittel bis niedrig,
Einkommen €1434;-, RV, PV, KS, VWL
Kredit: DB, €40.000, Konto: €-729
Zahlungsmoral: nachlässig, Versand auf Rechnung
einstellen, Kundennr: 393848, Punkte: 2930,
Umsatzpotential nicht ausgeschöpft.
Interessensprofil Musik/Buch: liegt vor
Interessensprofil Reisen: liegt vor,
Bürgerklasse 3 (Normal, Wiedervorlage, geplant 2009,
ID-Code C89A839A) Soziales Umfeld: Thomas B.,
Kerstin A., Verena L. (siehe Datensatz B33421)
Arbeitgeber K8273-23, Datenbankabgleich: OK
Verspätungen: 4, Abmahnung: Nein, Auto: Ford Fiesta,
TÜV, Teilkasko, Verkehrsdelikte: 2 (leicht) 0 (schwer)
Risikostufe: 3, Tendenz fallend, Maut-ID A38-92384
Fahrzeugbewegungsdaten: liegen vor ab 04/2006
Politische Ausrichtung: SPD (bis 2005), Seit 2005
Nichtwähler, Teilnahme an AK-Demo 2005 (Video #0232-4)

...bis auf meine Privatsphäre.

www.datenschutzzentrum.de ULD

Datenschutz im Unternehmen

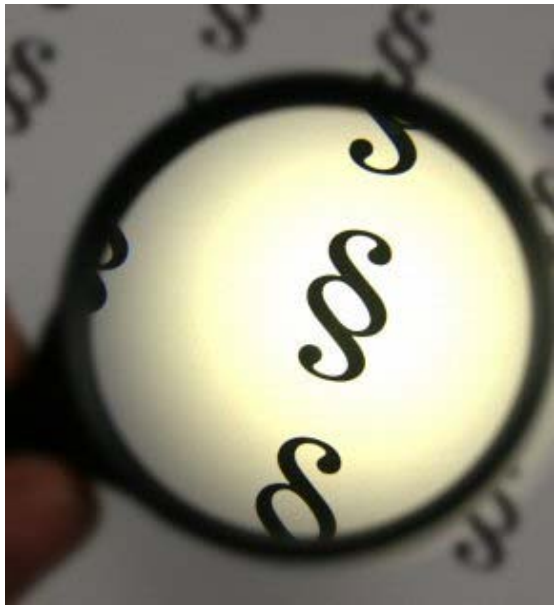
Was sind personenbezogene Daten?

Informationen über persönliche oder sachliche Verhältnisse

- Persönliche Grunddaten (z.B. Name, Anschrift, Geburtsdatum, Alter, Nationalität, Bankverbindung)
- Familiendaten (z.B. Daten über Angehörige)
- Daten über Wohnverhältnisse (z.B. Inhaber einer Sozial- oder Werkswohnung)
- Daten über Einkommen, Vermögen oder Besteuerung
- Daten natürlicher Personen in Verträgen

- Werturteile wie z.B. „guter Kunde“, „schlechter Schüler“
- Scorewert der SCHUFA
- Gesundheitsdaten
- Genetische und biometrische Daten
- Statische IP-Adresse
- und einige mehr …

Szenario : Welche Rechte hat der Betroffene?



Unabdingbare Rechte des Betroffenen (§6 Abs.1 BDSG)

- Benachrichtigung
- Auskunft
- Berichtigung, Löschung, Sperrung
- Widerspruchsrechte

Recht auf Benachrichtigung

- §19, 19a BDSG (öffentlich), §33 BDSG (privat).

Recht auf Auskunft

- §19 BDSG (öffentliche), §34 BDSG (privat).

Recht auf Berichtigung, Löschung, Sperrung

- §20 BDSG (öffentliche), §35 BDSG (privat).

Recht auf Widerspruch

- §20 BDSG (öffentliche), §35 BDSG (privat).

Datenschutz im Unternehmen

Musterschreiben (Betroffenen-Anfrage) nach BDSG, das jederzeit bei Ihnen eintreffen kann (per Einschreiben, per eMail, per Fax ..)

Sehr geehrte Damen und Herren,

unter Bezug auf §34 BDSG ersuche ich Sie, mir schriftlich, unverzüglich und kostenlos Auskunft über die zu meiner Person bei Ihnen gespeicherten Informationen zu erteilen :

- ***Werden in Ihrem Unternehmen Daten über mich gespeichert ?***
- ***Welche Daten zu meiner Person werden gespeichert ?***
- ***Wer verarbeitet die Daten ?***
- ***Von wem haben Sie Ihre Daten über meine Person erhalten (Quelle) ?***
- ***Zu welchem Zweck werden die Daten verarbeitet ?***
- ***An welche weiteren Empfänger wurden in der Vergangenheit meine persönlichen Daten weitergegeben ?***
- ***Nennen Sie mir Ihren Datenschutzbeauftragten und dessen Kontaktdaten.***

Bitte erteilen Sie mir Auskunft bis zum TT.MM.JJJJ. Mit freundlichen Grüßen

Datenschutz im Unternehmen

Datenschutz warum ?

- Kunden, Lieferanten und Arbeitnehmer erwarten, dass der Datenschutz ernst genommen und mit ihren Daten sehr sorgfältig umgegangen wird (Vertraulichkeit – Verfügbarkeit – Integrität). Die Sensibilität erhöht sich stetig (siehe Vorkommnisse bei Telekom, Bahn, Lidl, easy-cash..)
- Immer häufiger bedingen Kunden-Aufträge einen nachgewiesenen Datenschutz und eine zuverlässige Informationssicherheit (ISO 27001).
- Datenschutz und Informations-Sicherheit sind integraler Bestandteil des Qualitätsmanagements.
- Neben den klassischen Bereichen „ISO Auditierung“ und „Wirtschaftsprüfung“ führen gelebter Datenschutz und Informationssicherheit aufgrund transparenter Risiken und Prävention zu Nachlässen bei den Versicherungsprämien und zu günstigerem Rating der Banken (operationelle Risiken / Compliance).

Datenschutz warum ?

- Bei Kapitalgesellschaften haften die Geschäftsführer bzw. Vorstände für die Aufrechterhaltung des Betriebsablaufes (Risiken managen) und die Einhaltung gesetzlicher Vorschriften (Compliance) mit ihrem Privatvermögen, insbesondere bei Informationssicherheit und Datenschutz.
- Datenschutz und Informationssicherheit sind Alleinstellungsmerkmale und tragen werbewirksam zur Imageförderung bei.
- Datenschutz ist gesetzlich vorgeschrieben !

Rechtliche Rahmenbedingungen und unternehmerische Pflichten

Unternehmer hat gesetzliche Vorgaben im Risikomanagement
– insbesondere im IT- Bereich und Datenschutz zu beachten !

- GmbH Gesetz (§ 43 1 und 2) – Obliegenheiten eines ordentlichen Geschäftsmannes,
- § 91 bzw. 93 Abs 2 Aktiengesetz (KonTraG) – Pflicht zur Abwehr von Risiken, Sorgfaltspflicht von Vorständen,
- Bundesdatenschutzgesetz (BDSG),
- § 203 StGB – Strafe für bestimmte Berufsgruppen (z.B. Steuerberater, Ärzte, Anwälte..),
- 8. EU Richtlinie (EURO-SOX) – Anforderung an IT- Controls durch Wirtschaftsprüfer, (Erfordernis von IT- Sicherheitskonzepten), Wirtschaftsprüfer schaut auf Einhaltung der Vorgaben
- Telekommunikationsdienstleistungsgesetz
- Verschärfung diverser Gesetzgebung in 2009, 2010, 2011 ff. in der Datensicherheit (Vorfälle bei Deutsche Bahn, Telekom, LIDL .). usw...

Datenschutz im Unternehmen

Wer muss gemäß BDSG den Datenschutz wie umsetzen?

Erfordernisse des Datenschutzes

- **Jedes Unternehmen muss Datenschutz umsetzen, unabhängig von der Anzahl der Mitarbeiter.**
- **Ab *zehn* Personen, die auf personenbezogene Daten zugreifen können bzw. bei hochsensiblen personenbezogenen Daten (Finanzen, Gesundheit..) - die eine Vorabkontrolle nach BDSG erfordern - alle Unternehmen, muss ein interner oder externer Datenschutzbeauftragter (DSB) bestellt sein.**
- **Bei Verstößen: Bußgeld bis zu 300.000 €, bei Vorsatz und Wille zur Bereicherung auch Freiheitsstrafe bis zu 2 Jahren.**
- **Falls kein DSB bestellt ist, haftet der Geschäftsführer persönlich. Ist ein DSB bestellt, haftet dieser für die Umsetzung der gesetzlichen Anforderungen. Die Einhaltung der durch den DSB festgelegten Verfahren obliegt weiterhin dem Unternehmen.**

Datenschutz im Unternehmen

Der Datenschutzbeauftragte (DSB)

Nachweis der *Fachkunde*

- **Juristische Kenntnisse**
- **EDV-Kenntnisse (Hardware, Software, IT-Sicherheit, Datenbanken)**
- **Betriebswirtschaftliche Kenntnisse**
- **Erstellung von Datenschutzkonzepten, Durchführung von Datenschutzaudits**
- **Kenntnisse der Unternehmensabläufe**
- **Verschwiegenheit**
- **Didaktische Fähigkeiten, Durchsetzungsvermögen, Konfliktlösungsbereitschaft**
- **Genaue Arbeitsweise**

Fazit

Der Datenschutzbeauftragte benötigt umfangreiche und aktuelle Fach- und Spezialkenntnisse

Datenschutz im Unternehmen

Der Datenschutzbeauftragte (DSB)

Nachweis der *Zuverlässigkeit*

- **Es darf kein Konflikt mit anderen Aufgaben bestehen, bei Zeitkonflikten muss der Datenschutz immer vorrangig bearbeitet werden.**
- **Darf sich nicht selbst kontrollieren (typischerweise daher ausgeschlossen: Geschäftsführer, IT-Leiter, Personalleiter, evtl. auch Einkaufs- / Verkaufsleiter).**
- **Darf sich nicht in einem Interessenskonflikt mit den Aufgaben als DSB befinden (Beispiel: Ein Ehepartner partizipiert direkt am wirtschaftlichen Erfolg des Unternehmens).**
- **Verschwiegenheit und Diskretion zu Belangen des Betroffenen muss gewahrt bleiben.**

Datenschutz im Unternehmen

Der Datenschutzbeauftragte (DSB)

Sonderstellung des internen Datenschutzbeauftragten

- **Betrieblicher DSB ist kein Weisungsempfänger.**
- ***Nicht kündbar*** **in Sachen Datenschutz, nur abberufbar durch Aufsichtsbehörde.**
- **Betrieblicher DSB kann eigenes Budget fordern.**

Datenschutz im Unternehmen

Der Datenschutzbeauftragte (DSB)

Vorteile **externer** Datenschutzbeauftragter

- **Dienstvertragsverhältnis (Haftung (versichert) / Vertretung) – kein Arbeitnehmer mit hohem Kündigungsschutz**
- **ist aktuell ausgebildet, erfahren und bildet sich zeitnah weiter**
- **verfügt über Vorlagen, Muster etc. aus anderen Projekten**
- **ist unabhängig (neutral) und objektiv (vermischt nicht seine Aufgaben im Unternehmen mit den Datenschutzthemen)**
- **pflegt den Erfahrungsaustausch in Netzwerken**
- **haftet (Beraterhaftpflicht) und ist entspr. versichert**

Datenschutz was ist zu tun ?

SiMiS-Service (externer Datenschutzbeauftragter) (1):

- **Gestellung des externen Datenschutzbeauftragten bzw. Coaching der Unternehmensleitung bei kleineren Unternehmen**
- **Erstellung und lfd. Pflege der gesetzl. Datenschutzdokumentation (Verfahrensübersicht, Verfahrensbeschreibung, techn.-organisatorische Maßnahmen usw.) nach BDSG (Bundesdatenschutzgesetz)**
- **Erstellung und Pflege der**
  - internen Richtlinien nach BDSG (z.B. Passwort, Internet-eMail..)
  - Personal-Datenschutz-Verpflichtung und - Schulung
  - externen Verpflichtungen (der Lieferanten) nach § 11 BDSG

Datenschutz was ist zu tun ?

SiMiS-Service (externer Datenschutzbeauftragter) (2):

- **Organisation und Überwachung der Einholung von umfassenden Einwilligungen zur erstmaligen bzw. weiteren Nutzung von personenbezogenen Daten der Betroffenen (Kunden, Arbeitnehmer, Geschäftspartner..) gem. verschärfter Datenschutz-Bestimmungen (Direktmarketing !)**
- **Direktmarketing - Datenschutz-Belange (was ist zu beachten – zu tun ?)**
- **Online-Shop - Datenschutz-Belange / Internet-Präsenz**
- **IT- Security - Datenschutz-Belange (ISO 27001- basiert)**

Datenschutz was ist zu tun ?

SiMiS-Service (externer Datenschutzbeauftragter) (3):

- **Sichern der Betroffenenrechte (§§34, 35 BDSG)**
- **Beantwortung von Betroffenen-Anfragen nach §34 BDSG**
- **Erstellen von Richtlinien und Einleitung der nach §9 BDSG erforderlichen technisch-organisatorischen Maßnahmen.**
- **Sicherung des verschärften Arbeitnehmerdatenschutzes**
- **Regelmäßige Überprüfung der Umsetzung des Datenschutzes im Unternehmen (§4g Abs. 1) und**
- **Siegelvergabe geprüfter Datenschutz Initiative „Sicherheit mit System“**

Datenschutz als Wettbewerbsvorteil !

Inhalte Datenschutz-Handbuch

Bestellung des Datenschutzbeauftragten (interner oder externer)
Verfahrensverzeichnis / Verfahrensbeschreibungen
Öffentliches Verfahrensverzeichnis
Datenschutzrichtlinien (eMail, Passwort..)
Verpflichtungserklärungen (intern, extern)
Technisch-organisatorische Maßnahmen
Arbeitnehmerschulungen (Awareness)
Sonstige Dokumente (Auditprotokolle, Checklisten..)

Anhang
Gesetze: BDSG,Telemediengesetz (TMG),Landesdatenschutzgesetz

„Prüfsiegel“


SIMIS Sicherheit mit System
Geprüfter
Datenschutz
SIMIS
DATA
WWW.SIMIS.ORG
PRÜFSIEGEL

Erich Zimmermann

Sprecher der Initiative „Sicherheit mit System“

externer Datenschutzbeauftragter (IHK)

- SiMiS-Datenschutz GmbH
- Datenschutz-Dienstleistungen
- Schwarzwaldstr. 17
- D-68163 Mannheim
- Tel. 0621 - 30696731
- Fax. 03212 - 3912345
- mob. 0160-90248450 www.simis.org
- eMail:e.zimmermann@simis.org
- www.simis.org