

- Datenschutz
- Risiko- und Qualitätsmanagement
- Geheimhaltungsmanagement

Technisch-organisatorischer Datenschutz in der Praxis



Zur Person

- Seit 1984 im Projektmanagement im Großhandel, Bauindustrie und Maschinenbau
- Leitung von EDV und Rechenzentrum im Großhandel
- 10 Jahre Vertriebsleiter IT- Sicherheit
- DGQ-ID: P/QB/3/9602/005
- TÜV NORD: Datenschutzbeauftragter (TÜV)
- TÜV Rheinland: Datenschutzauditor (TÜV)
- Auditor für IT-Sicherheit / Datenschutz



Agenda

- Warum Datenschutz
- Das Bundesdatenschutzgesetz
- Gefahren im Netz
- KonTraG
- GDPdU
- Nutzungsrichtlinien in der Praxis
- Handlungsleitfaden BDSG & ISO 27001
- Mein TIPP



Warum Datenschutz



Neuer Datenskandal bei der Telekom

(<http://www.silicon.de/mobile/wireless/0,39039018,39199531,00/neuer+datenskandal+bei+der+telekom.htm>)

Von: Lutz Poessneck

Mittwoch, 26. November 2008

Die Deutsche Telekom hat erneut mit einem Datenskandal in erheblichem Ausmaß zu kämpfen. Das berichtet das Magazin stern.

Demnach verschafften sich dubiose Adresshändler und Callcenter offensichtlich Zugriff auf Namen, Adressen, Vertragsdaten und Bankverbindungen von mehreren tausend Festnetzkunden. Insider berichten, es würden derzeit viele zehntausend streng vertrauliche Kundenprofile auf dem Schwarzmarkt angeboten – anders als bei früheren Datenmissbrauchsfällen bei der **Telekom** beinhalten die Datensätze diesmal alle Bank- und Geburtsdaten. Einige Kunden beschwerten sich bereits über illegale Abbuchungen von ihren Konten.

Der stern hat nach eigenen Angaben mehrere tausende Datensätze eingesehen, die in der Branche kursieren. Betroffen sind ausschließlich Kunden, die ihren Festnetz- und Internetanschluss bei der Telekom haben. Im Zuge der Recherche wurden der Telekom Datensätze übergeben. Der Konzern kann sich die Herkunft nicht erklären und will Anzeige erstatten. Sicherheitschef Volker Wagner meint aber, es handle sich nicht um Original-Listen aus einem Telekom-System: "Zum einen stimmt die Form nicht; zum anderen sind Angaben zu Bankverbindungen und Geburtsdaten teilweise unterschiedlich zu unseren Kundendaten." Die Vermutung ist, dass Adresshändler oder Callcenter Telekom-Listen mit Informationen aus anderen Quellen angereichert haben.



Warum Datenschutz



Datenskandal: 21 Millionen Kontonummern geklaut

(<http://www.silicon.de/cio/wirtschaft-politik/0,39038992,39199988,00/datenskandal+21+millionen+kontonummern+geklaut.htm>)

Von: Anja Schütz

Montag, 8. Dezember 2008

Bankverbindungen von 21 Millionen Bundesbürgern befinden sich auf dem Schwarzmarkt für persönliche Daten im Umlauf. Nach einem Bericht der Wirtschaftswoche müsse damit gerechnet werden, dass bei drei von vier deutschen Haushalten unberechtigt Geld von ihrem Konto abgebucht wird.

Dem Düsseldorfer Magazin **Wirtschaftswoche**^[1] wurde von Händlern die gigantische Datenmenge für zwölf Millionen Euro angeboten. Als 'Appetizer' erhielt das Wirtschaftsmagazin eine Muster-CD mit 1,2 gestohlenen Kundendaten. Die CD wurde mittlerweile an die Düsseldorfer Staatsanwaltschaft übergeben. Ein Sprecher erklärte, dass nun untersucht werden müsse, wie so viele Kontonummern illegal in Umlauf gelangen konnten.

Dem Bericht zufolge enthalten die Datensätze neben den Angaben zur Person wie Geburtsdaten, die Bankverbindung einschließlich Kontonummer und Bankleitzahl und in einigen Fällen sogar Details zur Vermögenslage. "Jeder muss befürchten, dass er betroffen ist", sagte der Bundesdatenschutzbeauftragte Peter Schaar gegenüber dem NDR. Er empfiehlt allen Bundesbürgern ihre Kontoauszüge sorgfältig zu prüfen.

Erste Spuren führen zu kleineren Callcenter-Betreibern. Auf den umkämpften Massenmärkten wie Telekommunikation, Energieversorgung oder Kabelfernsehen bedienen sich immer mehr Anbieter fast nur noch externer Dienstleister und Callcenter. Diese externen Dienstleister erhalten die relevanten Kundendaten teilweise vom Auftraggeber. Wenn die Dienstleister jedoch ihrerseits Subunternehmer einschalten, geht die Kontrolle über die Daten irgendwann verloren.



Warum Datenschutz



NEU:
silicon.de bei twitter
Immer und überall up to date!



Neues von der "Spitzel"-Bahn

(http://www.silicon.de/cio/wirtschaft-politik/0,39038992,41003073,00/neues+von+der+_spitzel_bahn.htm)

Von: Martin Schindler

Montag, 20. April 2009

Die Deutsche Bahn soll nicht nur Festplatten von Mitarbeitern durchforstet, sondern auch den E-Mail-Verkehr eines SPD-Politikers überwacht haben. Die Bahn gerät mit dem Vorgehen gegen undichte Stellen im Unternehmen immer weiter ins Kreuzfeuer der Kritik.

Die Aktion 'Leakage', mit der das Unternehmen seit 2005 nach undichten Stellen bei der Bahn intern und, wie sich jetzt herausstellt, auch extern fahndet, beherbergt laut Berichten eine schwarze Liste mit unliebsamen Kritikern der Bahn.

Wie das Berliner Blatt 'Tagesspiegel am Sonntag' berichtet, soll dabei auch die E-Mail-Kommunikation eines Referenten des verkehrspolitischen Sprechers der SPD, Uwe Beckmeyer, über mehrere Jahre hinweg überwacht worden sein.

Die Liste soll neben dem Mitarbeiter der Bundestagsfraktion auch rund 30 weitere Namen mit Personen umfassen, die unter der besonderen Beobachtung der Bahn standen.

Wie das Nachrichten-Magazin Der Spiegel berichtete, sollen bei der Bahn auch Festplatten von Mitarbeitern nach bestimmten Schlagworten überprüft worden sein. Die Bahn hat dieses Vorgehen inzwischen eingeräumt. Dabei seien jedoch nur Fälle überprüft worden, bei denen ein konkreter Verdacht auf illegale Weitergabe von internen Informationen vorlag. Dadurch habe sich die Bahn gegen weiteren Schaden schützen wollen. Laut Spiegel handle es sich bei den durchsuchten Festplatten um Gruppenlaufwerke, auf denen Mitarbeiter Dateien speichern konnten.



Das Bundesdatenschutzgesetz

- Das Bundesdatenschutzgesetz regelt die Zulässigkeit der Verarbeitung von Bürgerdaten:
 - durch Behörden des Bundes
 - durch private Unternehmen.



BDSG und das Datensparsamkeitsgebot

- Was ist beim Datensparsamkeitsgebot zu beachten?
- Daten werden redundant gespeichert
 - CRM-Systeme
 - Outlook / E-Mailsysteme
 - FileServer z. B. Excel-Tabellen



Das E-Mail-Volumen wächst und wächst !



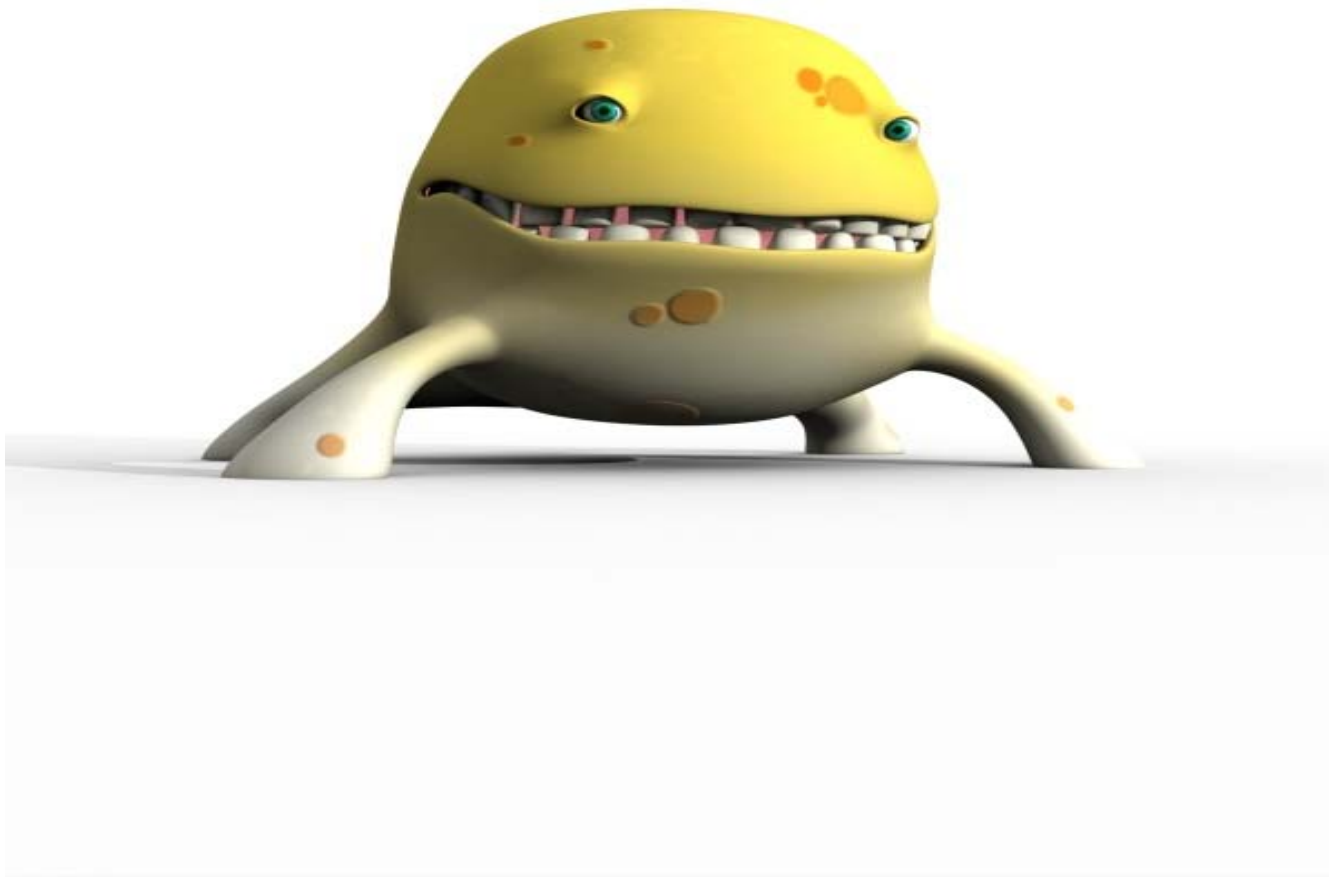
E-Mails lösen in den nächsten Jahren die traditionellen Mittel **vertraulicher** Kommunikation wie Einschreiben und Kurierdienste ab.

Wachsende Bedeutung durch:

- Elektronische Rechnung
- Handels- und Geschäftsbrief



Viren, Würmer & Co.





Surfen im Internet

Wer im Internet surft hinterlässt Spuren:

- IP-Adresse - Adresse des Providers ist darüber zu ermitteln
- Betriebssystem
- Browser - installierte Erweiterungen
- Bildschirmauflösung
- Die Adresse der überweisenden Seite
- Bei Suchmaschine das übergebene Suchwort



Uns kann das nicht passieren:



Sind Sie sich wirklich sicher?

Mit einer guten Idee wird man schneller zur Zielscheibe als man denkt!

Nein kein großer Denker – aus meiner Praxis!



Der Fall 'Natalie'

Sophos - Online Communities zunehmend IT-Sicherheits-Risiko: Experten warnen vor massivem Anstieg von Datendiebstahl und -missbrauch auf Social Network Websites

Fünf Minuten reichten aus:
über **50 Ahnungslose User**
gingen 'Natalie' ins Netz



Quelle: <http://www.sophos.de/pressoffice/news/articles/2008/01/online-communities.html> - 21. Januar 2008



Der Fall 'Natalie'

Das Ergebnis: - **nur 5 Minuten!**

- 19 sofort bestätigte Kontakte
- 27 E-Mails mit Kontaktanfragen
- 48 Nachrichten
- damit freien Zugang zu den persönlichen Daten, wie Adresse, Alter, Instant-Messenger-Namen und persönliche Interessen.



KonTraG

- Das **K**ontrolle und **T**ransparenz **G**esetz verpflichtet zur Früherkennung von Risiken auch in der IT, zu einem IT- Risiko- Management und zur Schaffung sicherer Netzwerkinfrastrukturen.





GDPdU

Grundsätze für die Anwendung der Regelungen zum **D**atenzugriff und zur **P**rüfbarkeit **d**igitaler **U**nterlagen:

- Digital gespeicherte Daten maximal **10 Jahre** aufzubewahren!
- In dieser Zeit die Daten **Z3-fähig** zu halten!
- Ab **2002** die Daten für den Einsatz von IDEA sicherzustellen!

- Bestätigungsvermerk in der Jahresendprüfung wird nicht erteilt!
- Bei nicht ordnungsgemäßer Buchführung Schätzung der Besteuerungsgrundlagen!
- Finanzierungs- und Kreditbeeinträchtigungen!



EDV-Nutzungsrichtlinien

- Aufgrund der steigenden Gefahren durch Malware, sowie Bedrohungen durch Konkurrenzausspähung, etc. ... sind EDV-Nutzungsrichtlinien erforderlich.
- Auch der Gesetzgeber fordert die Umsetzung organisatorischer / technischer Maßnahmen und deren Kontrolle durch Sachkundige.



EDV-Nutzungsrichtlinien

- Durch das BDSG sind Verzeichnisse vorgeschrieben, in denen EDV-Sicherheitsmaßnahmen dokumentiert werden.
- Um diese EDV-Sicherheitsmaßnahmen durchzusetzen, sind Verhaltensregeln in Form von **EDV-Nutzungsrichtlinien** erforderlich.



Das BDSG - Anlage (zu § 9 Satz 1)

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren **(Zutrittskontrolle)**,
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können **(Zugangskontrolle)**,
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle)**,
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist **(Weitergabekontrolle)**,
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle)**,
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle)**,
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind **(Verfügbarkeitskontrolle)**,
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

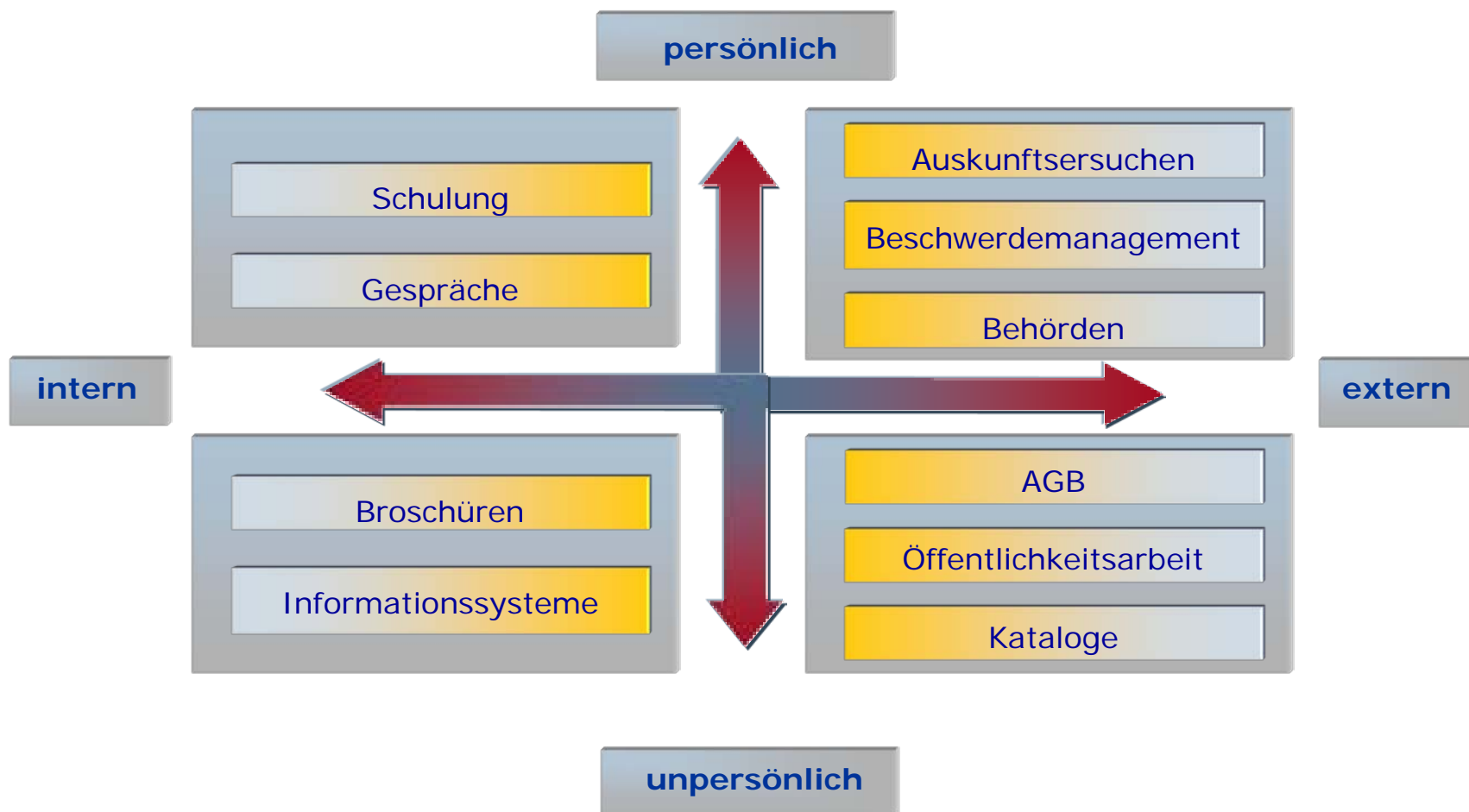


EDV-Nutzungsrichtlinien

- **E-Mail-Sicherheitsrichtlinie**
- **Passwortpolicy**
- **Richtlinie Internetnutzung**
- **Richtlinie Wechseldatenträger**
- Nutzung des Notebooks/PDAs
- Nutzung WLAN
- Sicheres Löschen von Daten
- Verschlüsselung von Daten
- Computerviren



Die Aufgaben des DSB



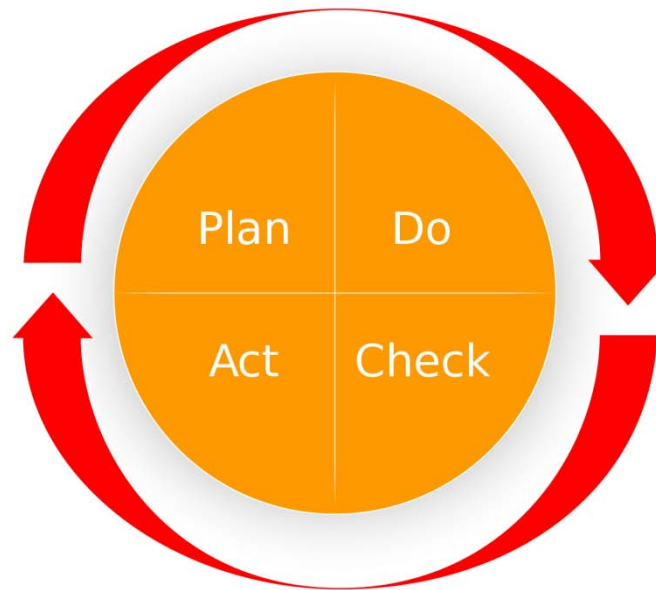


DIN ISO/IEC 27001:2008-09

- Informationstechnik
- IT-Sicherheitsverfahren
- **Informationssicherheits-Managementsysteme**
- Anforderungen



ISMS - Plan-Do-Check-Act (PDCA)



Plan (Plan), Do (Tun), Check (Prüfung), Act (Aktion)



ISMS - Auszug

- A.11 Zugangskontrolle
- A.11.3.1 Passwortverwendung
- A.11.5 Zugriffskontrolle auf Betriebssysteme
- A.11.7 Mobile Computing und Telearbeit
- A.12.2 Korrekte Verarbeitung in Anwendungen
- A.15 Einhaltung von Vorgaben (**Compliance**)
- ...



Mein TIPP!

- Die Lebenszeit reicht nicht aus um alle Fehler selbst zu machen, deshalb nutzen sie die Unterstützung einer sachkundigen Stelle...

... die Sie und Ihr Business versteht.



[eckert security] Management

- Datenschutz
- Risiko- und Qualitätsmanagement
- Geheimhaltungsmanagement

