Lufthansa Group

22.09.2015

Personaldaten sicher geschützt

Angela Espinosa, Deutsche Lufthansa AG

Agenda

- Vorstellung
- Datenschutz
- Säulen des Datenschutzes
- Technische und organisatorische Maßnahmen
- Anforderungen auf Datenbankebene
- Sanktionen

Lufthansa Group

Vorstellung

- Lufthansa Group weltweit operierender Luftverkehrskonzern (540 Tochterunternehmen)

- In 4 Geschäftsfelder organisiert:
  - Passage Airline Gruppe
  - Logistik
  - Technik
  - Catering

- 118.973 Mitarbeiter, 30 Mrd. Euro Jahresumsatz

- großer Bedarf an IT Services durch die Digitalisierung und Modernisierung
- Auftrag verschiedener IT-Provider

- Nicht nur Flugdaten, auch Personal- und Kreditkartendaten verarbeitet und gespeichert
  → Unterliegen Regularien durch Datenschutzgesetz oder PCI etc.
  → Kontrolle und vertragliche Regelungen mit Providern

Datenschutz

- **Der Mensch steht im Vordergrund**
  → Schutz der persönlichen Daten

- Datenschutz mittelbar im Grundgesetz verankert
  „Recht auf informationelle Selbstbestimmung“
  durch Verfassungsgerichtsurteil (Volkszählungsurteil 1983)

Datenschutz – persönliche Daten

Personenbezogene Daten sind Einzelangaben über	
persönliche Verhältnisse	**sachliche Verhältnisse**
Name, Anschrift, Größe, Alter, Konfession, Beruf, Krankheiten	Kfz-Typ, Einkommen, Steuern, Versicherungen
einer	
bestimmten Person	**bestimmbaren Person**
Adresse, Telefonnummer, Vorlieben, Gesundheit, Foto	IP-Adresse, Rentenversicherungsnummer, User-ID
Personenbezogene Daten der besonderen Art (§ 6 BDSG)	
rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben	

Datenschutz

- **Jeden Tag hinterlassen wir Datenspuren…**

- Mobile Geräte machen uns sichtbarer als wir wollen…

Soziale Netzwerke, Krankenversicherung, Versandhandel, Finanzamt, Bank, Schufa, Medizinisches Labor, Versicherungen, Krankenhaus, Arzt, Arbeitgeber, Energieversorger, Onlineshops, Urlaubsportale, Bücherei, Schule, Kundenkartenanbieter, etc…..

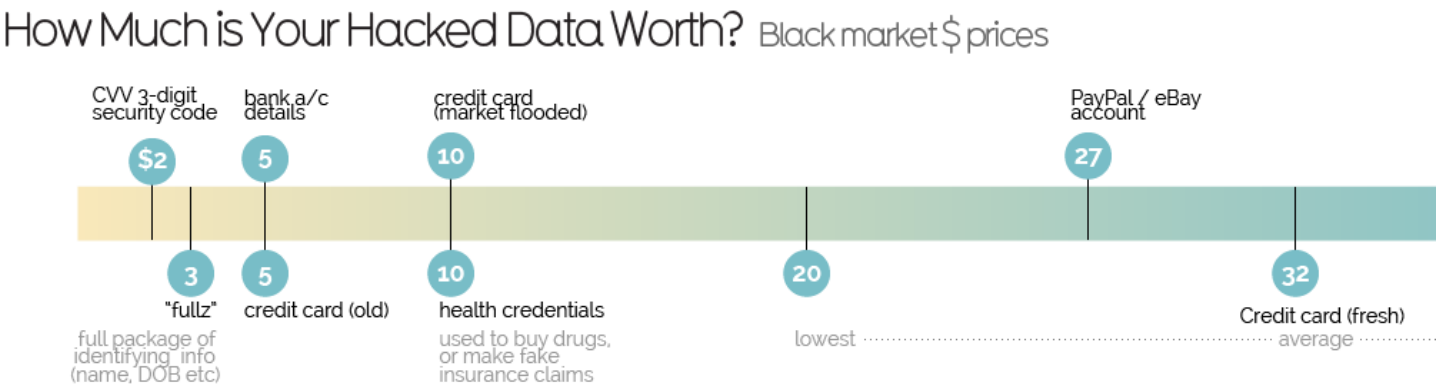
Datenschutz

- **….daraus werden höchst interessante und wertvolle Informationen**

- Sicherheitsbehörden → Verbesserung der Verbrechensbekämpfung
- Finanzbehörden → Aufdecken von Steuerdelikten
- Unternehmen → Überwachung der Mitarbeiter
- Kundenprofile → Besseres Marketing und Preisdifferenzierung
- Identitätsklau → Missbrauch der eigenen Daten

Quelle: http://www.trendmicro.de/infografiken/wie-viel-sind-ihre-daten-wert/

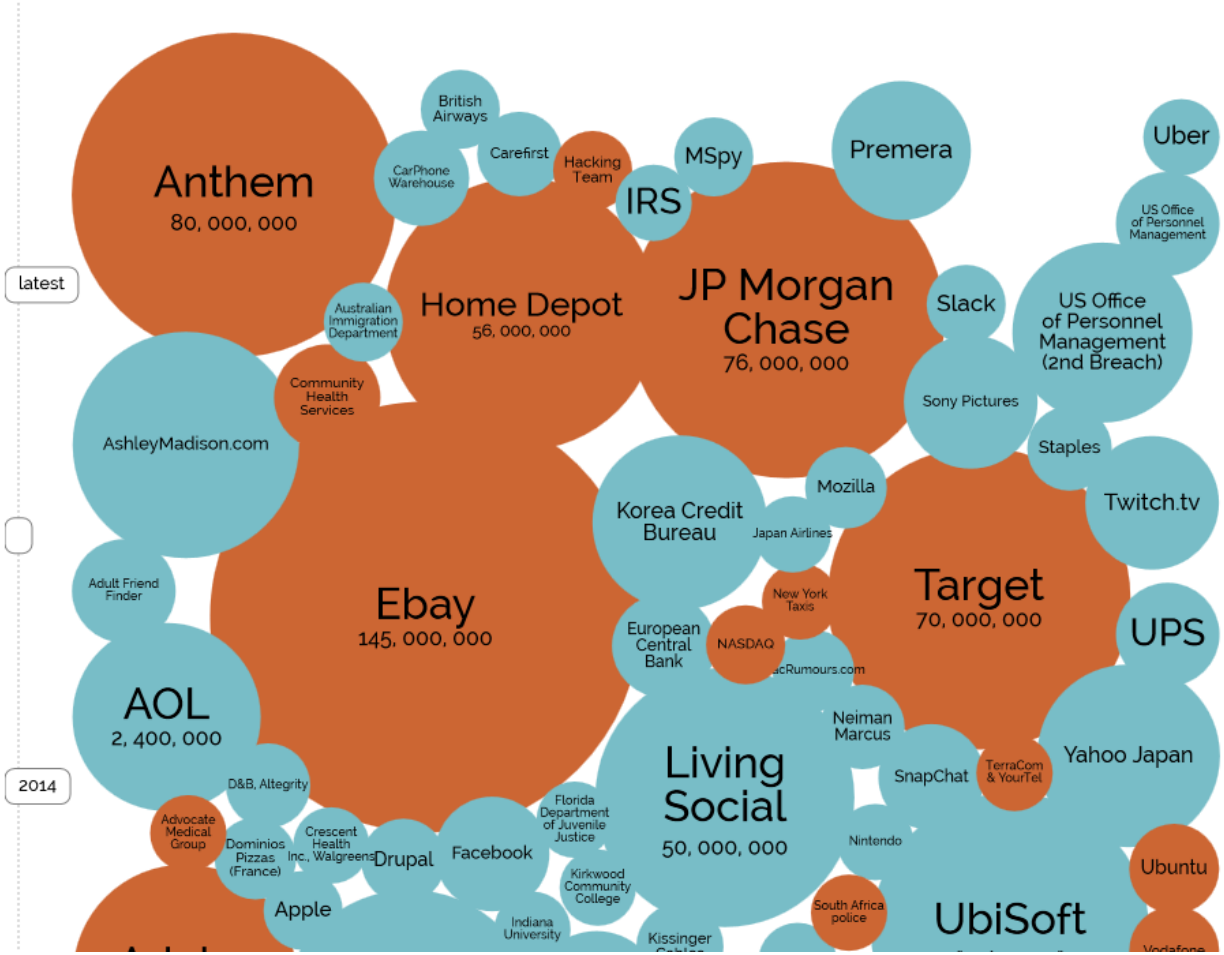
Man kann richtig Geld damit verdienen!



Quelle: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Datenschutz

- Wie viele Datenpannen gibt es denn?



70
CONTRIBUTING ORGANIZATIONS

79,790
SECURITY INCIDENTS

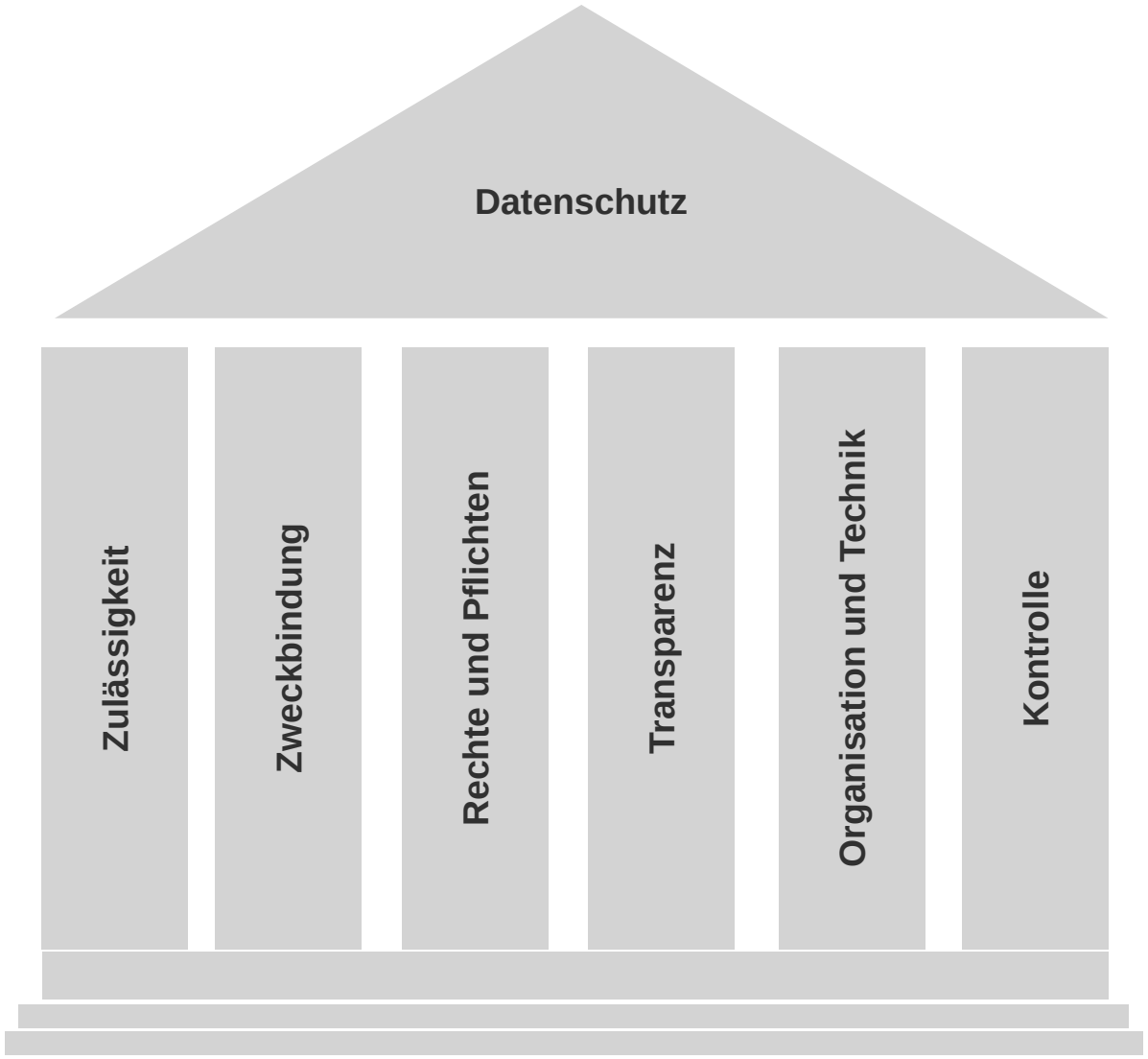
2,122
CONFIRMED DATA BREACHES

61
COUNTRIES REPRESENTED[1]

Quelle: http://www.verizonenterprise.com/de/DBIR/2015

Quelle: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Säulen des Datenschutzes



Generelle Anforderungen im Vorfeld

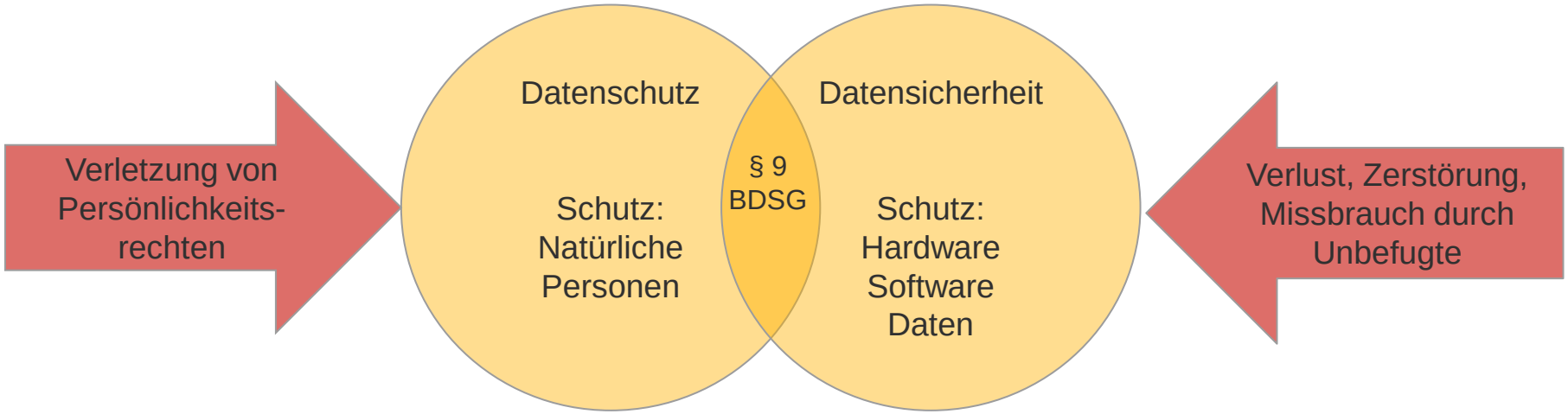
- Datenschutzrechtliche Vorabkontrolle bei Daten der besonderen Art (§ 6, durch DSB)
- Zulässigkeit, Zweckbindung (Verarbeitung und Nutzung)
- Rechtsgrundlage sollte im Verfahrensverzeichnis dokumentiert sein
- Einwilligungen schaffen mehr Transparenz
- Prüfung der Erforderlichkeit (Datensparsamkeit)

- Angemessene technische & organisatorische Maßnahmen:
  - Schutzbedarfsfeststellungen & Risikoanalysen
  - Schutzstufenkonzepte (je nach Schutzbedarf der Daten)
  - Berechtigungskonzepte
  - Verschlüsselung
  - Prozessmanagement
  - Datenschutzmanagement
  - Dokumentation

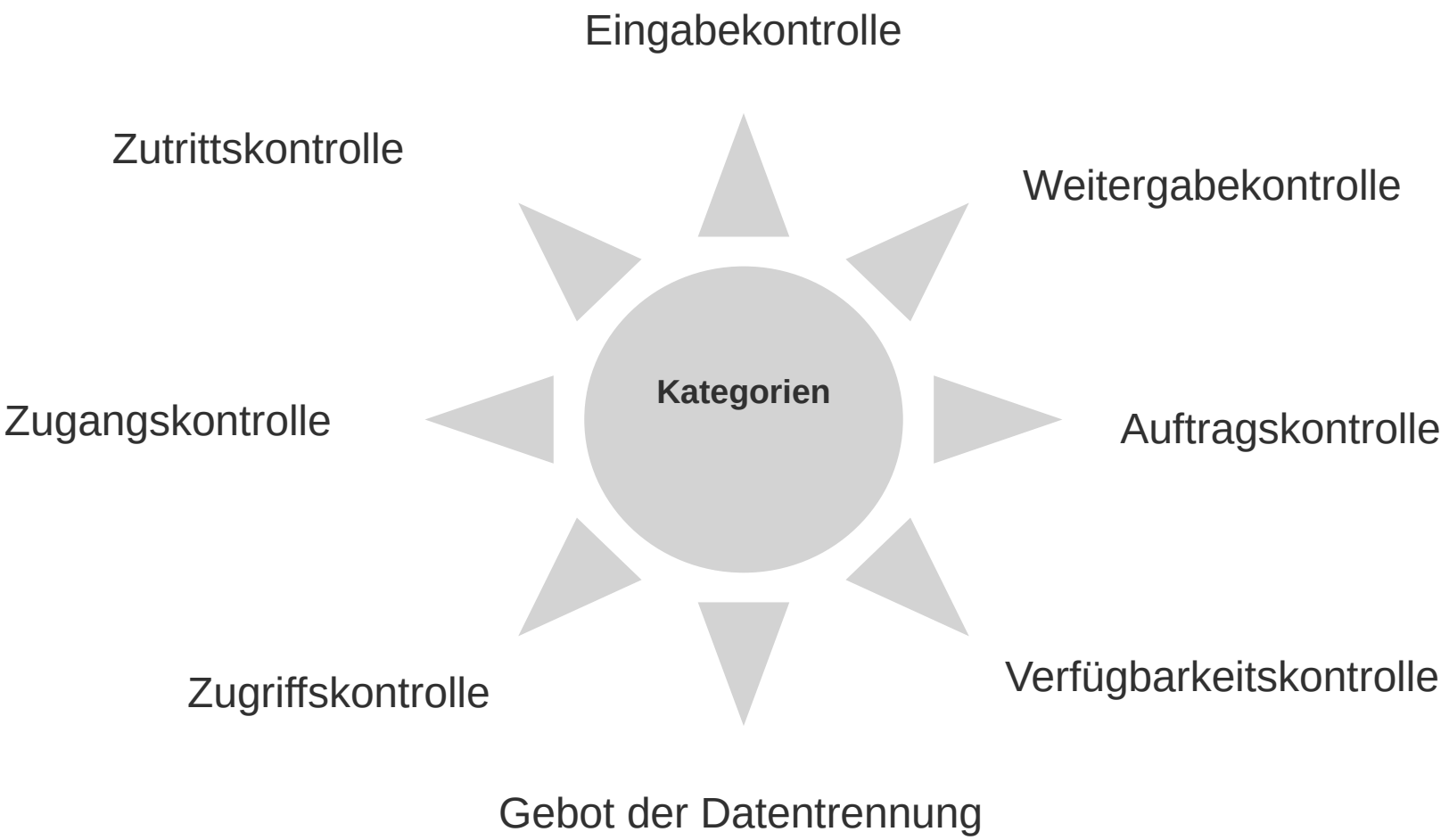
Technische und organisatorische Maßnahmen § 9 BDSG

- „Öffentliche und nicht-öffentliche Stellen, …, haben die **technischen und organisatorischen** Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.“

- **Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht**. (§ 9 BDSG)



Technische und organisatorische Maßnahmen § 9 BDSG



Anforderungen aus dem BDSG auf Datenbankebene

Zutrittskontrolle

- Gebäudesicherung
  - Zäune
  - Pforte
  - Videoüberwachung
- Sicherung der Räume
  - Sicherheitsschlösser
  - Chipkartenleser
  - Codeschlösser
  - Sicherheitsverglasung
  - Alarmanlagen
- Datenbanktechnisch weniger wichtig, aber trotzdem Augen offen halten

Anforderungen aus dem BDSG auf Datenbankebene

Zugangskontrolle (Authentifizierung)

- Personalisierung in der Datenbank oder auf andere Art (OS-Ebene)
  → Oracle bietet Enterprise User Security an (Nutzung von AD, LDAP)
  → Starke Authentisierung via Kerberos, Radius, Zertifikate und Token

- sichere Passwörter erzwingen → Passwort Verify Funktion
- eigene definieren oder mitgelieferte ora12c_strong_verify_function
- (ab 9 Zeichen, 2 x Groß- und Kleinbuchstaben & Zahlen & Sonderzeichen)

- Profile einrichten (Reuse Max, Idle Time, Expire Time, Password_Verify_Function, Password Lock Time, Failed Login Attempts)
  → Benutzern zuweisen und dann Passwörter setzen

- Zugriff auf Passwortspeicher einschränken (sys.user$)
  REVOKE ALL on SYS.USER$/SYS.LINK$ from <username>;
  SELECT ANY DICTIONARY hat SELECT on sys.user$
  DROP TABLE SYS.USER$MIG;

[none]
[name of product / vendor]
1234 or 4321
access
admin
anonymous
database
guest
manager
pass
password
root
sa
secret
sysadmin
user

Anforderungen aus dem BDSG auf Datenbankebene

Zugangskontrolle (Authentifizierung)

- Passworthasheinträge beschränken/löschen (sqlnet.ora)
  SQLNET.ALLOWED_LOGON_VERSION_SERVER = 12/12a

- Änderung v. Standardpasswörtern Oracle interner Benutzer
  SELECT USERNAME FROM DBA_USERS_WITH_DEFPWD WHERE USERNAME NOT LIKE '%XS$NULL%';

- Änderung v. Standardeinstellungen (Listenerport 1521, DBname ORCL, etc.)
- Ungenutzte Optionen und Features abschalten/deaktivieren/löschen (XML, JAVA, etc. MOS 2001512.1), Demo- und Testschemas erst gar nicht installieren (SCOTT, HR)

- Regelmäßiges Aktualisieren der Oracle Software (Security Alerts/Patches prüfen)
  SELECT * FROM DBA_REGISTRY_HISTORY;

- Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugangsberechtigungen (Zeitnahe Sperrung ausgeschiedener Mitarbeiter)

Anforderungen aus dem BDSG auf Datenbankebene

Zugangskontrolle (Authentifizierung)

- Änderung des aktiven Listeners nur in listener.ora mit Restart
  ADMIN_RESTRICTIONS_<listener_name>=ON

- Einschränkung der Protokolle, die sich auf Listener verbinden dürfen
  SECURE_REGISTER_<listener_name>=IPC/TCPS

- TNS Poison Attack vorbeugen (nur lokale Verbindungen zulassen)
  ALTER SYSTEM SET LOCAL_LISTENER=
  '(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=REGISTER)))‘ SCOPE=BOTH;
  Ab 11.2.0.4 VALID_NODE_CHECKING_REGISTRATION_<listener_name>=*ON*

- Zugangswege einschränken über die Verbindungen über Listener (sqlnet.ora)
  TCP.VALIDNODE_CHECKING = YES
  TCP.INVITED_NODES = (hostname1, name2)
- Logon Trigger für Beschränkung des Zugriffs durch Applikationsbenutzer

Anforderungen aus dem BDSG auf Datenbankebene

Zugriffskontrolle (Autorisierung)

- Berechtigungskonzept, welcher Benutzer hat welche Rechte auf welche Daten
  → Virtual Private Database (neues Konzept RAS; XS$NULL Auditing)
  → Label Security (bis auf Zeilenebene einschränken)

- Applikationsuser trennen von Applikationsdatenschema

- PUBLIC hat mehr als 10.000 Rechte → jeder Benutzer erbt diese Privilegien

- Wichtig: Entfernen von Ausführungsrechten von PUBLIC auf Objekte und Pakete
  REVOKE EXECUTE on DBMS_ADVISOR from PUBLIC;

  → Quelle: https://www.cisecurity.org/

Anforderungen aus dem BDSG auf Datenbankebene

Zugriffskontrolle (Autorisierung)

- Benutzerberechtigungen einschränken (auch Oracle interne Benutzer)
  REVOKE EXECUTE ANY PROCEDURE from OUTLN/DBSNMP;
- Motto: "So wenig wie möglich und so viele wie nötig" (ANY, DBA-Rechte)
- Oracle 12c bietet Privilege Analysis (Database Vault)
- Konzentration von Funktionen vermeiden (root+DBA) → Separation of duties
- 07_DICTIONARY_ACCESSIBILITY=FALSE
  Erlaubt sonst Zugriff auf Objekte im SYS Schema durch die
  EXECUTE ANY PROCEDURE und SELECT ANY DICTIONARY Berechtigung
- Zugriff auf OS-Dateien beschränken $ORACLE_HOME/…

Anforderungen aus dem BDSG auf Datenbankebene

Weitergabekontrolle

- Schutz der Daten bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger sowie bei nachträglicher Überprüfung (oft Aufgabe der Applikation)
  → Daten nur verschlüsselt, pseudonymisiert oder anonymisiert „weitergeben“
  → De facto Standards benutzen
    TLS 1.1/1.2 (Transport über öffentliche Netze)
    Tunnelverbindungen (Virtual Private Network)
    S/MIME bei Email (elektronische Signatur)
    X.509 V3 für Kodierung von asymmetrischen Schlüsseln

- verschlüsseltes Backup (Schlüsselmanagement)

- Sofortiges Löschen des Übergangs-Datenträgers
- Löschen der Verschlüsselung und Schlüssel

- Weitergabe dokumentieren und kontrollieren (Protokolle oder bei Medienbruch)

Anforderungen aus dem BDSG auf Datenbankebene

Verschlüsselung (explizit in Zugangs-, Zugriffs-, Weitergabekontrolle)

- Zugang zur Datenbank
  - Übertragung der Passwörter verschlüsselt (nicht bei UPDATE oder ALTER USER)
  - Netzwerkverschlüsselung (Teil der Enterprise Edition)

- Zugriff auf die Daten
  - Verschlüsselung durch die Applikation (Schlüsselmanagement)
  - Verschlüsselung mittels DBMS_CRYPTO
  - Verschlüsselung von Tablespaces oder Spalten (Tablespace Data Encryption)
  - Oracle Database Vault als zusätzliche Sicherheitsmaßnahme (Zugriff einschränken)

- Transport der Daten
  - Applikation stellt Verschlüsselung und Protokollierung sicher
  - Data Pump nur verschlüsselt durchführen (ENCRYPTION Zusatz)
  - Daten anonymisieren/pseudonymisieren (kein Bezug zu Daten)
  - Backupverschlüsselung

Anforderungen aus dem BDSG auf Datenbankebene

Gebot der Datentrennung

- Daten zu unterschiedlichen Zwecken getrennt speichern
- Mitarbeiter- und Kundendaten trennen
- Logische Trennung (eigene Tablespaces)
  → untersch. Schemata und Trennung des Zugangs über untersch. Benutzer

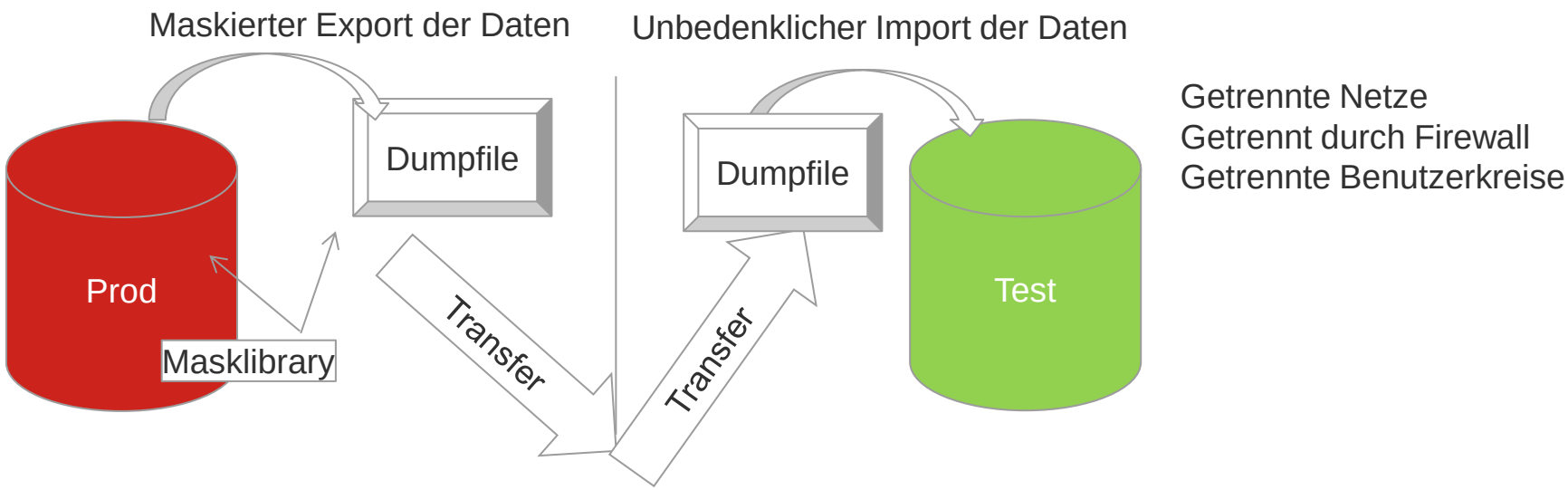
- Andere Möglichkeiten der Datentrennung wären:
  - Einsatz verschiedener Datenbanken
  - Einsatz von Zugriffskontrollsoftware und Einrichtung von Zugriffsrechten
  - Verschiedene Verschlüsselung für einzelne Datensätze
  - Verschiedene Schlüssel pro Mandant

- Testumgebungen getrennt von Produktivumgebung nur mit anonymisierten Daten

Anforderungen aus dem BDSG auf Datenbankebene

Gebot der Datentrennung - Regelmäßige Übertragung der Proddaten in Testumgebung

- Nur durch Anonymisierung/Pseudonymisierung
- Oracle bietet Data Masking in Verbindung mit Oracle Enterprise Manager
- Data Masking light mittels remap Data API (selbstgemacht)
- Finden, Bewerten (Application Data Model), Maskieren (Formatlibs), Testen
- Data Masking Policies und At-Source Data Masking



Anforderungen aus dem BDSG auf Datenbankebene

Verfügbarkeitskontrolle (Schutz vor Zerstörung und Verlust der Daten)

- Detaillierter Notfallplan (Desaster Recovery Plan)
- USV unterbrechungsfreie Stromversorgung, Firewall
- Spiegelung von Festplatten, RAID-Verfahren, Virenschutz (auf OS-Ebene)
- Monitoring der Datenbank mit zugehörigem Alerting (z.B. Oracle Enterprise Manager)
- Backup-Konzept (Fullbackup, inkrementelle Backups)
- Regelmäßiges und sicheres Backup der Archivelogs und Datafiles mit RMAN
  → Regelmäßige Restore- und Recoverytests durchführen
- Multiplexed Controlfiles/Redologs auf verschiedene Festplatten

Anforderungen aus dem BDSG auf Datenbankebene

Protokollierung (zweckgebunden, datensparsam, vollständig) - Eingabekontrolle

- Praktisch in jeder Kontrolle Forderung nach Nachweisfähigkeit

- Protokollierungsdaten nicht zur Verhaltens- oder Leistungskontrolle

- Strikte Zweckbindung, umfassenden Einblick in Tätigkeiten der Administratoren, Nutzer
- Wichtig: Art, Dauer und Umfang beschränken

- Wer, wann, welche personenbezogenen Daten wie verarbeitet hat
- Tatsächlich erfolgte Operationen, Anwendungen, Maschinen, Personen mit Zeitbezug

- Kein nachträgliches Ändern, nur Berechtigten zugänglich

- Test der ordnungsgemäßen Funktion - Stichproben
- Aufbewahrungsdauer hängt ab von Auswertungszyklus

Anforderungen aus dem BDSG auf Datenbankebene

Audit aktivieren - Oracle 11g Datenbanken haben es schwerer

- "Die Kombination macht es"
- Angefangen mit privilegierten Benutzern:
- SYSDBA und SYSOPER Auditing
  AUDIT_SYS_OPERATIONS=TRUE
- Loggen in das Syslog Log
  AUDIT_TRAIL=OS
- Empfangskanal für Syslog Deamon
  AUDIT_SYSLOG_LEVEL=LOCAL2.WARNING.

Anforderungen aus dem BDSG auf Datenbankebene

- Auditieren von normalen Benutzern:

- "Normales" Auditing loggt nicht alle Informationen mit (SQL Statement fehlt)
- Trick:
  AUDIT_TRAIL=XML, EXTENDED

- alle wichtigen Informationen zu Benutzern und deren Statements
  → nicht an den SYSLOGD
  → Erzeugung von XML Dateien

- AUDIT_DUMP_DEST geeignet definieren → eigenes gesichertes Filesystem

- Beachtung der Berechtigung der Dateien (nur von Oracle Software Owner beschreibbar) _TRACE_FILES_PUBLIC=FALSE (default)

Anforderungen aus dem BDSG auf Datenbankebene

Was heißt das im Umkehrschluss?

1. Einschränken des Oracle Software Owner in seiner Benutzung

2. „/ as sysdba“ (Sammelaccount) darf nicht benutzt werden
   → Nachvollziehbarkeit „gestört“

3. zusätzlichen eingeschränkten Benutzer für den normalen Betrieb einsetzen
   kann nicht die XML Dateien manipulieren
   Prozessbeschreibung/Konzept

4. Schnellstmöglicher Transfer der XML Dateien auf zentralen Protokollserver
   Eingeschränkten Share an Betriebssystem mounten (nur von root zugreifbar)
   Dateien dorthin zeitnah verschieben

5. Zentraler Protokollserver muss XML Dateien auswerten können z.B. von ArcSight
   (SmartConnector for Oracle Audit XML Connector)

Anforderungen aus dem BDSG auf Datenbankebene

Oder einfach auf Oracle 12c umsteigen und Unified Auditing einsetzen (autom. aktiviert)

- Umfangreicher in seiner Protokollierung (Backup, Restore, Dumps, oradebug etc.)
- Protokolliert auch, wenn die Datenbank readonly gemounted ist (in OS-Dateien)
- Protokoll-Tabelle ist nur read-only zugreifbar (unified_audit_trail im Audsys Schema)
- Protokolleinträge abholen lassen durch Datensammler vom Protokollserver
- Lösch-Job nicht vergessen, da sonst die Datenbank platzt:

```
exec DBMS_AUDIT_MGMT.CREATE_PURGE_JOB
(AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
AUDIT_TRAIL_PURGE_INTERVAL => Zeitintervall,
AUDIT_TRAIL_PURGE_NAME => ‚Purge_audit_tabelle',
USE_LAST_ARCH_TIMESTAMP => TRUE);
```

Anforderungen aus dem BDSG auf Datenbankebene

- Audit-policy einstellen
- Oracle 12c standardmäßig ORA-SECURECONFIG

```
CREATE AUDIT POLICY ORA_SECURECONFIG
 PRIVILEGES ALTER ANY TABLE, CREATE ANY TABLE, DROP ANY TABLE,
            CREATE ANY PROCEDURE, DROP ANY PROCEDURE, ALTER ANY PROCEDURE,
            GRANT ANY PRIVILEGE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE,
            AUDIT SYSTEM, CREATE EXTERNAL JOB, CREATE ANY JOB,
            CREATE ANY LIBRARY,
            EXEMPT ACCESS POLICY,
            CREATE USER, DROP USER,
            ALTER DATABASE, ALTER SYSTEM,
            CREATE PUBLIC SYNONYM, DROP PUBLIC SYNONYM,
            CREATE SQL TRANSLATION PROFILE, CREATE ANY SQL TRANSLATION PROFILE,
            DROP ANY SQL TRANSLATION PROFILE, ALTER ANY SQL TRANSLATION PROFILE,
            CREATE ANY SQL TRANSLATION PROFILE, DROP ANY SQL TRANSLATION PROFILE,
            ALTER ANY SQL TRANSLATION PROFILE, TRANSLATE ANY SQL,
            EXEMPT REDACTION POLICY,
            PURGE DBA_RECYCLEBIN, LOGMINING,
            ADMINISTER KEY MANAGEMENT
ACTIONS     ALTER USER, CREATE ROLE, ALTER ROLE, DROP ROLE, SET ROLE,
            CREATE PROFILE, ALTER PROFILE, DROP PROFILE,
            CREATE DATABASE LINK, ALTER DATABASE LINK, DROP DATABASE LINK,
            LOGON, LOGOFF, CREATE DIRECTORY, DROP DIRECTORY;
```

- Erweiterung durch Zugriffe auf bestimmte Pakete (DBMS_FGA und Tabellen (sys.user$)

- Zugriffe auf die sensitiven Daten protokollieren mit Fine Grained Auditing

Anforderungen aus dem BDSG auf Datenbankebene

SIEM USE CASES - Definition von verdächtigen und auffälligen Events

- Alarm auslösen
- Beispielsweise:
  - Benutzer ändert einen Datenbankparameter
  - Benutzer legt einen anderen Benutzer an
  - Verschiedene Möglichkeiten: create user, grant user identified by

- Konfiguration beliebig erweitern

- Beispiele des Identitätswechsels ohne Passwort:
  - DBMS_SYS_SQL (undokumentiert), DBMS_IJOB (undokumentiert)
  - sys.kupp$proc (undokumentiert), Alter User su (feature)
  - Proxy User (feature), Any Procedure (feature)
  - Become User (feature), KUPP_PROC_LIB (undokumentiert)

- in Oracle 12c Auditieren von oradebug möglich (wichtig)

Anforderungen aus dem BDSG auf Datenbankebene

Auftragskontrolle (§ 5 und § 11 BDSG)

- Datengeheimnispflicht innerhalb der Firma (§ 5 BDSG)
- Verarbeitung der Daten im Auftrag → entsprechend Weisungen des Auftraggebers
- Gewährleistung des Datenschutz beim Outsourcing der Datenverarbeitung
- Auftraggeber verpflichtet:
- Vertragsschluss nach § 11 BDSG mit dem Auftragnehmer (ADV)
  → Durchführung regelmäßiger Kontrollen
- datenbanktechnisch eher uninteressant, aber Augen offen halten

Anforderungen aus dem BDSG auf Datenbankebene

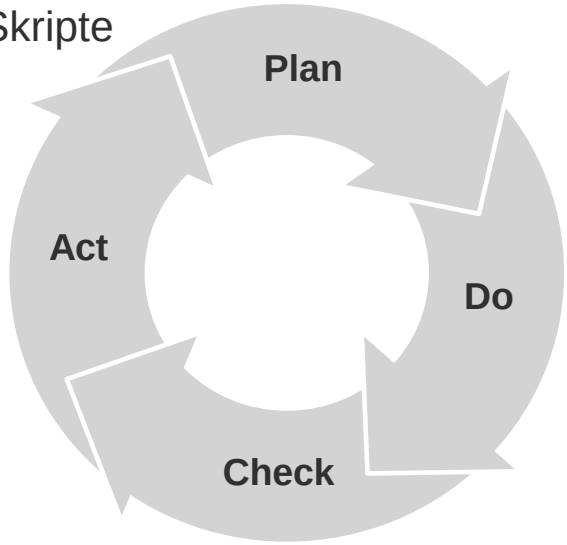
Regelmäßiges Überprüfen

- leider wird kein explizites Datenschutzmanagementsystem gefordert
- Aber allein durch andere gesetzliche Anforderungen sinnvoll

- Kontrolle ist das A und O

- Regelmäßige Checks der Härtung und Sicherheitsmaßnahmen
  → durch Oracle Enterprise Manager oder automatisierte Skripte

- Weiterentwicklung bei neuen Versionen/Features/Sicherheitsanforderungen



Aufgepasst

- Interessante Abfragen:
  - Fehlzeiten Mitarbeiter → Besuche bei Suchtberatung des Unternehmens
  - Betriebsrat → Dauer und Häufigkeit von Schulungen
  - Was verdient mein Kollege

- Unrechtmäßige Einsichtnahme in personenbezogenen Daten
  → Überschreitung der Zweckbindung (z.B. JOIN über bestimmte Tabellen)

- Benachrichtigung der Betroffenen
  → § 42a BDSG
  → Meldepflicht bei unrechtmäßigen Erlangen von Daten

- „Melden macht frei“ an den Datenschutzbeauftragter oder Aufsichtsbehörde

Sanktionen

- Datenschutzverstöße gesetzlich mit Bußgeldvorschriften des § 43 BDSG sanktioniert
- Bußgelder von 50.000 – 300.000 Euro können drohen
- Bußgeldtatbestand mit jedem einzelnen Vergehen
  „Kleinvieh macht auch Mist“
- Beispiele aus der Realität (Höhe des Bußgeldes):
  - Einzelhandelskette 1.462.000 €
  - Bank 120.000 €
  - Drogeriemarktkette 137.500 €
  - Transportunternehmen 1.123.503,50 €

Danke für die Aufmerksamkeit!