GI-Fachgruppe Management von Informationssicherheit (SECMGT)

Threat Model "praktisch": Sicht der DSGVO

Workshop vom 18.11.2013 in Frankfurt/Main

...alles eine Frage der Perspektive !?!

Quelle: celebritycruises.com

Die IT-Perspektive

- Technik
  (Hardware, Software, Netzwerkkomponenten, etc.)
- Überschaubarer Wert
  (absolut bestimmt!)
- Supporting Assets
- Wechsel von IKT-Sicherheit zur Informationssicherheit (?)

Quelle: hostway

Die Datenschutz-Perspektive: Informationen...

- Daten (inkl. personenbezogener Daten)
- Prozessbeschreibungen
  (inkl. notwendiger Compliance-Prozesse)
- Wert abhängig von Geschäftszweck / Aufgabe
  (relativer Wert!)
- Primary Assets

Quelle:
rdv-online.de

Praxissicht-IT: ISO/IEC 27005

- Bestimmung Kontext
  (insb. rechtliche Anforderungen, SLAs,
  interne Festlegungen)
- Festlegung Risikoanalyse Methodologie
  (in Abhängigkeit zum Kontext m. Festlegung der
  Sicherheitsziele)
- Festlegung Risikoappetit des Asset Owners
- Durchführung Risk Assessment zur Steuerung des ISMS
  (unter Betrachtung der Supporting Assets!)

Praxissicht-IT: ISO/IEC 27005

Ergebnis:

Risk Assessment anhand der Interessen der durchführenden Stelle

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten
    (1) Personenbezogene Daten müssen
    a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“);
    b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; (...)
    („**Zweckbindung**“)

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten
    (1) Personenbezogene Daten müssen
    e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; (...)
    („**Speicherbegrenzung**“);

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten
    (1) Personenbezogene Daten müssen
    f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);
    (2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; (...)

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (2) (...)
  - (3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber **innerhalb eines Monats** nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. (...)

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
    (1) Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft,

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
    (1) die dafür ausgelegt sind, die **Datenschutzgrundsätze** wie etwa Datenminimierung **wirksam umzusetzen** und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Dagegen – EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
    (2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten **Verarbeitungszweck** erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
    (3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32:
  - Darüber hinaus werden zahlreiche weitere Nachweispflichten in der EU-DS-GVO eingefordert, die wiederum nach Art. 83 Abs. 4 mit einer Geldbuße von bis zu 10 Mio. € bzw. 2 % des weltweiten Jahresumsatzes geahndet werden können
  - Die Erfüllung dieser Nachweispflichten setzt insoweit faktisch die Einrichtung eines Datenschutzmanagementsystems voraus – dieses kann aber auch aus einer systematischen Zusammen-stellung verteilt vorliegender Quellen über einen spezifischen „View“ erfüllt werden (?)

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32 etc.
  - In der EU-DS-GVO erfolgt nach Art. 32 Abs. 1 lit. b sowie Abs. 2 eine Orientierung auf die Gewährleistung von
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Die Ausrichtung der Schutzvorkehrungen basiert auf einem risikobasierten Ansatz (nach Art. 24 Abs. 1 unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung auf die Rechte & Freiheiten natürlicher Personen)

Dagegen − EU-DSGVO:

- Anforderungen in Art. 5, 12, 25 und 32 etc.
  - Die Maßnahmen (nach Stand der Technik!) sind nach Art. 24 Abs. 1 erforderlichenfalls zu überprüfen und aktualisieren
  - Zudem sind Verfahren zur regelmäßigen Überprüfung, Bewertung & Evaluierung der Wirksamkeit dieser Maßnahmen nötig

  - Diskussion:
    Ausrichtung des Datenschutzmanagementsystems auf ISO/IEC 27001 & 27009 sinnvoll und anwendbar?

Dagegen − EU-DSGVO:

- Zertifizierbar sind...
  - Die EU-DS-GVO sieht ausdrücklich vor, dass entsprechende Nachweise auch durch Vorlage eines geeigneten Zertifikats nach einem von den zuständigen Aufsichtsbehörden genehmigten Zertifizierungs-verfahren erbracht werden können hinsichtlich:
  - Erfüllung der Pflichten des Verantwortlichen zu Sicherstellung & Nachweis, dass die Verarbeitung unter Einhaltung der EU-DS-GVO erfolgt (Art. 24 Abs. 3)
  - Nachweis von Data Protection by Design / Default (Art. 25 Abs. 3)
  - Hinreichende Garantien für geeignete technische & organisatorische Maßnahmen des Auftragsverarbeiters (Art. 28 Abs. 5)

Dagegen − EU-DSGVO:

- Zertifizierbar sind...
  - Angemessenheit getroffener Schutzvorkehrungen (Art. 32 Abs. 3)
  - Geeignete Garantien in einem Drittland zusammen mit rechtsverbindlichen & durchsetzbaren Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters (Art. 46 Abs. 2 lit. f)

Dagegen − EU-DSGVO:

- Im Rahmen der EU-DS-GVO nutzbare Zertifikate müssen nach Art. 43 Abs. 1 von einer Zertifizierungsstelle stammen, die akkreditiert wurde durch:
- eine zuständige Aufsichtsbehörde gemäß Art. 55 & 56 oder
- die nationale Akkreditierungsstelle nach EU-Verordnung 765 / 2008 (in Deutschland: DAkkS) im Einklang mit EN ISO/IEC 17065:2012 (...)

Dagegen − EU-DSGVO:

- Derartige Zertifizierungsstellen müssen nach Art. 43 Abs. 2
  - unabhängig sein & einschlägiges Fachwissen zur Zufrie-denheit der zuständigen Aufsichtsbehörde nachweisen
  - Verfahren zu Erteilung, regelmäßige Überprüfung und Widerruf der Zertifizierungen festlegen
  - transparente Beschwerdeverfahren aufweisen
  - frei von Interessenkonflikten zur Zufriedenheit der zustän-digen Aufsichtsbehörde sein

Dagegen − EU-DSGVO:

- Derartige Zertifizierungsstellen müssen nach Art. 43 Abs. 2
  - Der Aufwand zum Aufbau eines geeigneten (zustimmungs-fähigen) Zertifizierungsstandards ist ausgesprochen hoch
    - nur im Rahmen des ISO-Normenwerks sinnvoll
    - allerdings ist auch Erweiterung bei ISO/IEC 27006 nötig
- Bisher nur ein Standard bekannt, der EU-DS-GVO bereits berücksichtigt: ADCERT (angelehnt an ISO/IEC 27001); ansonsten viele noch in Anpassung (7 derzeit auf EU-DSRL ausgerichtet)

Dagegen − EU-DSGVO:

- Ergebnis:

- Datenschutz dagegen geht von Interessen der Betroffenen aus
- weitere Sicherheitsziele:
  - Transparenz
  - Intervenierbarkeit
  - Datensparsamkeit
  - Einhaltung der Zweckbindung

Praxisproblem

- Daten über Kunden / Patienten / Mandanten / Versicherte / kritische Infrastrukturen etc.
  - wesentliches Schutzgut
  - i.d.R. große Anzahl Betroffener
  - dann Datenschutz maßgeblich für ISMS!
- Daten über Mitarbeiter dagegen häufig (international) kein ausdrückliches Schutzgut
  - i.d.R. (vergleichsweise) kleine Anzahl Betroffener
  - hier Datenschutz faktisch nur unter Compliance betrachtet

Praxisproblem

- Ergebnis:

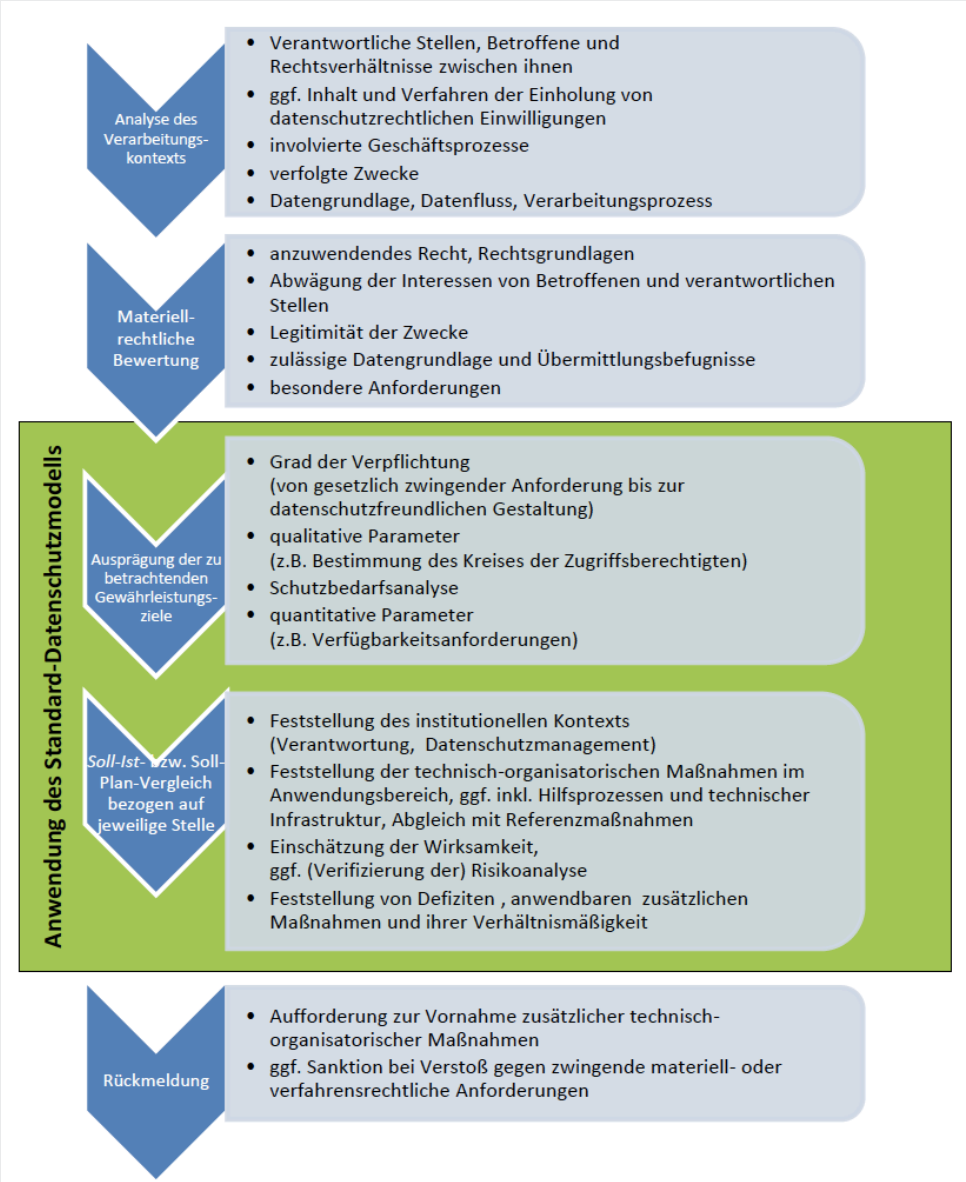
- Unterschiedliche Wertschätzung innerhalb der Einrichtung für jeweilige Teil-Informationen
- Unterschiedliche Wichtigkeit für ISMS-Steuerung!

Perspektive Datenschutz-Aufsicht:

Standard-Datenschutzmodell

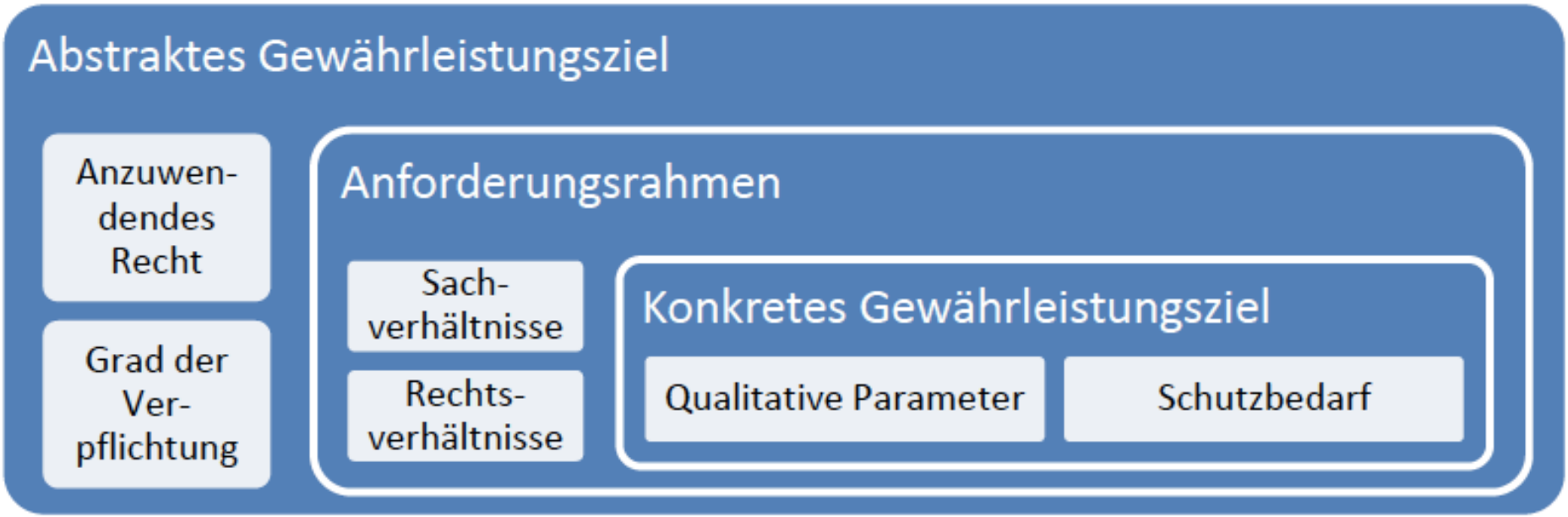
- Das SDM wurde im Auftrag der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder von einer Arbeitsgruppe der Aufsichtsbehörden entwickelt. In Abstimmung befindet sich derzeit ein Maßnahmenkatalog, welcher künftig Bestandteil des SDM sein wird und in Abhängigkeit der technischen Entwicklung in kürzeren Zyklen überarbeitet als das SDM selbst.

SDM - Aufbau



Quelle: ULD

SDM - Gewährleistungsziele



Quelle: ULD

Wer ist der Angreifer?

- Datenschutz:
- Die Organisation ist der Angreifer!
- Folge? Die Organisation muss (jederzeit) prüffähig nachweisen (können), dass sie kein Angreifer ist, sich an die Regeln hält und bei all dem ihre Verfahren und Prozesse beherrscht.

Quelle: ULD

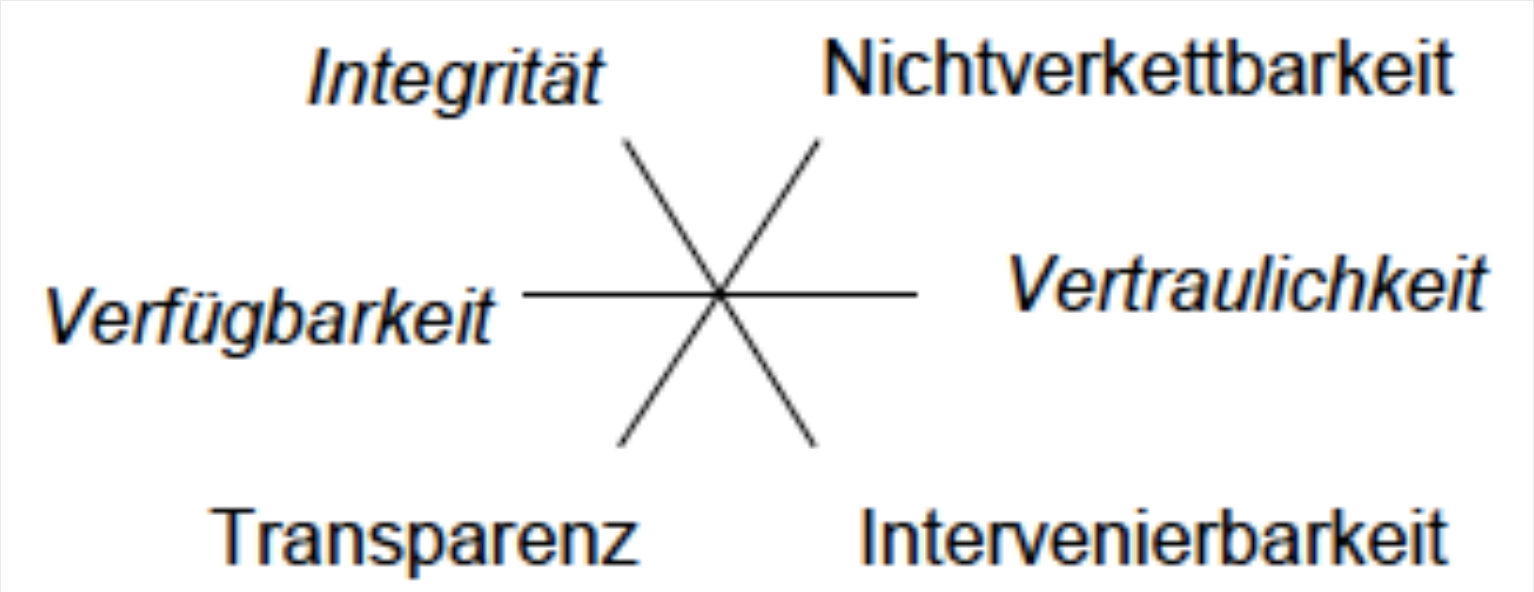
Wer ist der Angreifer?

- Datensicherheit:
- Die Person ist der Angreifer!

- Folge? Die Person muss nachweisen, dass sie kein Angreifer ist und dass sie ggfs. mit einem Zugriff auf ihre Person rechnen muss.
  Klassischer Schutz: Login/Authentisierung, Autorisierung der Person gegenüber Organisation, Rollenkonzepte, Kontrolle der MA.

Quelle: ULD

...die Schutzziele (SDM/ULD)



Quelle: ULD

Maßnahmen vs. Schutzziel

- Verfügbarkeit, Vertraulichkeit, Integrität
- (Verfügbarkeit) -> Redundanz
- (Vertraulichkeit) ->
  Abschottung von Systemen, Verschlüsselung von Daten und Kommunikationen sowie Rollentrennungen.
- (Integrität) -> Hash-Wert-Vergleiche vorher/nachher

Quelle: ULD

Maßnahmen vs. Schutzziel

- Transparenz
- Maßnahmenbündel:
- „Projektmanagement, Berichtswesen, Verfahrens- bzw. Technikdokumentation, Information und Kommunikation mit den Betroffenen“, z.B.
  - Dokumentation der IT des Verfahrens, der Daten und der Datenflüsse, der Sicherheitsmaßnahmen, der Systeme und Prozesse, der Tests und Freigaben.
  - Setzen von Prüfankern in Systemen und Prozessen.
  - Unterrichtung von Betroffenen (Publikation eines „Datenbriefs“?)
  - ...

Quelle: ULD

Maßnahmen vs. Schutzziel

- Nichtverkettbarkeit
- Maßnahmenbündel: „Rollen- und Strukturkonzept“
  - Angemessene Funktionstrennungen zwischen oder auch innerhalb von Organisationen mit Verantwortungszuweisungen an kompetente MitarbeiterInnen.
  - Kontrollierte Konzeption, Implementierung, Konfiguration, Inbetriebnahme und Außerbetriebnahme, mit Tests und Simulationen in den jeweiligen Phasen nach best-practice Gesichtspunkten.
  - ...

Quelle: ULD

Maßnahmen vs. Schutzziel

- Intervenierbarkeit
- Maßnahmenbündel: „Operativ gegebener Zugriff auf Daten und deren Verarbeitung“
  - Einrichtung eines SPOC (Single-Point-Of-Contact) für Betroffene zur Adressierung einer Intervention mit Verfolgbarkeitsoption.
  - Gestalten und Steuern von Prozessen, Stoppen und Wiederanfahren von Systemen, geregeltes Changemanagement
  - ...

Quelle: ULD

Komponenten im SDM

- Daten (und Datenformaten)
- IT-Systemen (und Schnittstellen)
- Prozesse (und adressierbare Rollen)

Quelle: ULD

Schutzbedarfe im SDM (à la BSI)

- **Normal:** Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für Betroffene relativ leicht zu heilen.
- **Hoch:** die Schadensauswirkungen werden von Betroffenen als beträchtlich eingeschätzt, z.B. weil der Wegfall einer von einer Organisation zugesagten Leistung die Gestaltung des Alltags nachhaltig veränderte und der Betroffene nicht aus eigener Kraft handeln kann sondern auf Hilfe angewiesen wäre.

Quelle: ULD

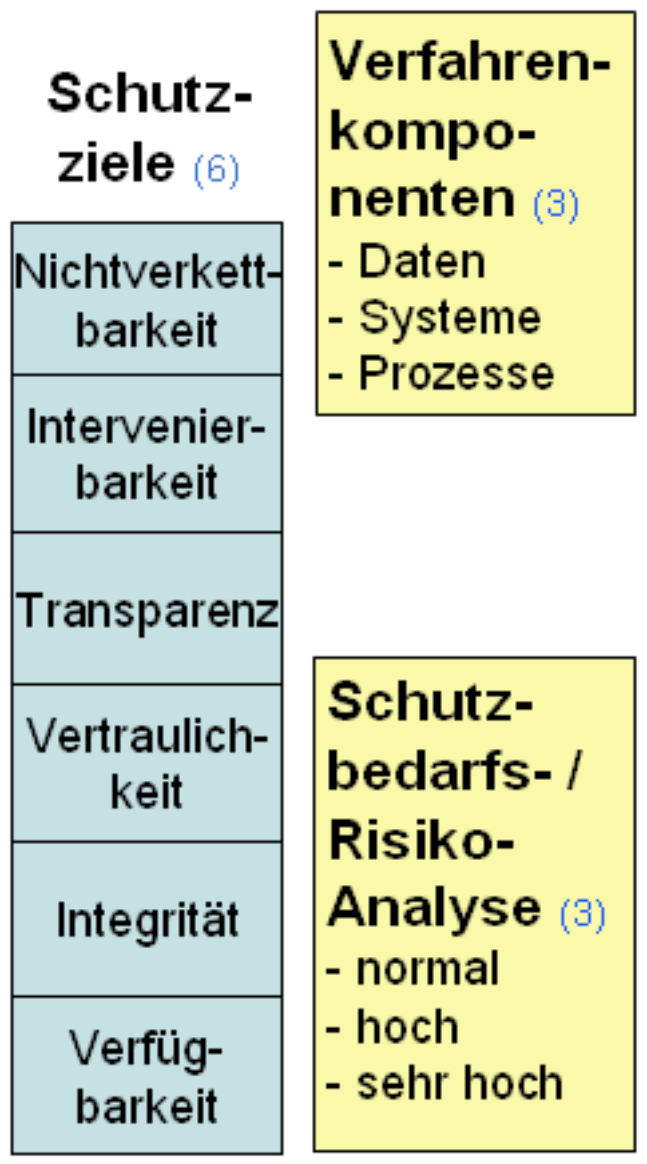
Schutzbedarfe im SDM (à la BSI)

- **sehr hoch:** Die Schadensauswirkungen nehmen ein unmittelbar existentiell bedrohliches, also: katastrophales Ausmaß für Betroffene an.

Quelle: ULD

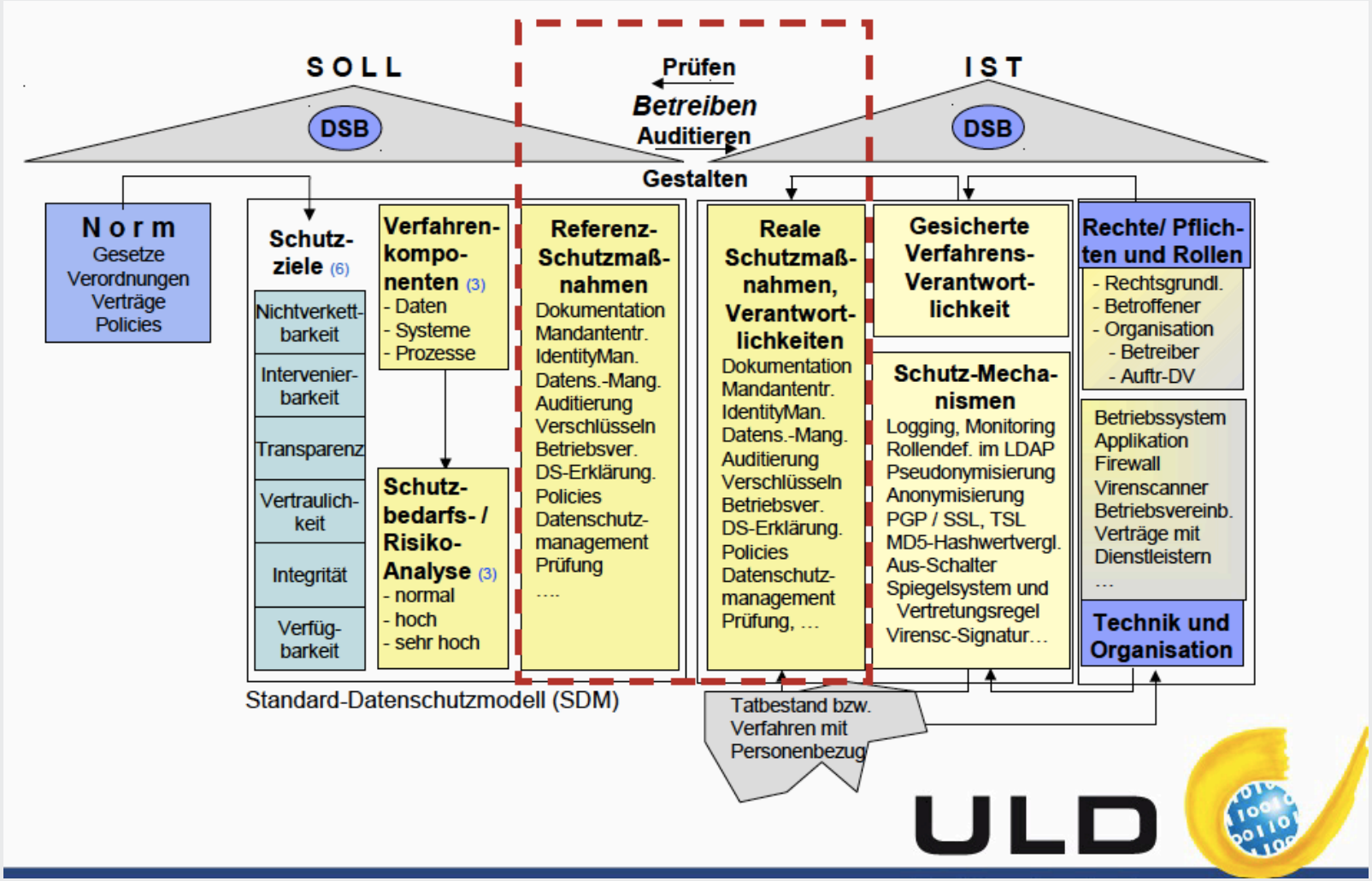
Schutzbedarfe im SDM (à la BSI)

- **Ergebnis:**
  54 Datenschutzmaßnahmen



Quelle: ULD

Quelle: ULD



Quelle: ULD

Quelle: ULD

	Daten	Systeme	Prozesse
Verfügbarkeit	D1.1 Einschränkung von Lösch-/Veränderungsrechten D 1.2 Schutz vor Schadsoftware D 1.3 Backup der Daten	S 1.1: Schutz vor Schadsoftware S 1.2: Backup von Konfigurationen und Software S 1.3: Hardwareredundanz S 1.4: Ausweichräume, und -Netze	P 1.1: Vertretungspersonal P 1.2: Fähigkeit zur Aufgabenerledigung durch Dritt (Vorbereitung Outsourcing) P 1.3: Ausweichprozesse, Amtshilfe
Vertraulichkeit	D 2.1: Einschränkung von Leserechten (für Datenverarbeiter, ggf. durch den Nutzer selbst) D 2.2: Protokollierung lesender Zugriffe D 2.3: Verschlüsselung der Daten D 2.4: Ende-zu-Ende-Verschlüsselung	S 2.1: Einschränkung von lesenden Zugriffsrechten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 2.2: Verschlüsselung auf Systemebene (Festplatten, Datenbank)	P 2.1: Verpflichtung auf das Datengeheimnis (BDSG P 2.2: Verschwiegenheitsvereinbarungen P 2.3: Geeignete Organisation bei der Vergabe von Zugriffsrechten („need-to-know")
Integrität	D 3.1: Einschränkung von Schreib- und Änderungsrechten D 3.2: Protokollierung von schreibenden/ändernden Zugriffen D 3.3: Protokollierung geänderter Daten D 3.4: Nachberichtigung D 3.5: technische Integritätskontrollen (Signaturen/Hashes)	S 3.1: Einschränkung von schreibenden Zugriffen/Konfigurationmöglichkeiten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 3.2: Regelmäßige Integritätsprüfungen/Audits	P 3.1: Detaillierte Planung von Verfahren und Verfahrensschritten P 3.2: Geordnete Zuweisung von Rechten und Rolle P 3.3: Geordnete Änderung von Verfahren und Verfahrensschritten P 3.4: Regelmäßige Überprüfung
Nicht-Verkettbarkeit	D 4.1: Einschränkung von Verarbeitung-s-/Nutzungs- /Übermittlungsrechten für einzelne Daten D 4.2: Kennzeichnung der Zwecke auf Ebene der Daten D 4.3: Einschränkung von identifizierenden Daten; Pseudonymisierung D 4.4: Anonymisierung von Daten	S 4.1: Kennzeichnung der Zwecke auf Ebene des Systeme S 4.2: Trennung von Datenbeständen S 4.3: Einschränkungen von Verarbeitungs-, Nutzungs- und Übermittlungsmöglichkeiten (Funktionalitätseinschränkung) S 4.4: Trennung auf Systemebene (Software, Hardware; Mandantenfähigkeit)	P 4.1: Trennung auf Verfahrensebene P 4.2: Rechte + Rollenvergabe, ggf. an eine andere rechtliche Entität (z. B. Personalvertretung) P 4.3: Gewaltenteilung

Quelle: ULD