it.sec
security for your information

Datenschutzbezogenes Risikomanagement

Workshop von CAST & GI-FG SECMGT am 28.02.2013

Bernhard C. Witt (it.sec GmbH & Co. KG)

Bernhard C. Witt

- Berater für Datenschutz und Informationssicherheit bei der it.sec GmbH & Co. KG
  verantwortlich für die Geschäftsfelder
  ° Datenschutz (→ externer Datenschutzbeauftragter)
  ° IT Governance, Risk & Compliance Management
- Industriekaufmann, Diplom-Informatiker
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (BSi)
- CRISC (ISACA)
- Lehrbeauftragter an der Universität Ulm (seit 2005)
- Autor der Bücher „IT-Sicherheit kompakt und verständlich“ (2006) und „Datenschutz kompakt und verständlich“ (2008 & 2010)
- Sprecher der GI-Fachgruppe Management von Informationssicherheit (seit 2009)
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit (seit 2009)
- Mitglied im Leitungsgremium der GI-Fachgruppe Datenschutzfördernde Technik (seit 2012)
- Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfahren“ AK 1 & 4 (seit 2011)

it.sec
security for your information

Zur it.sec GmbH & Co. KG

IT Governance, Risk & Compliance Management

- Management von Informations-sicherheit & Business Continuity
- Toolgestütztes IT Governance, Risk & Compliance Management
- Compliance zu multiregulatorischen Anforderungen (inkl. internationaler Standards)
- Sicherheitskonzepte, Policies, Prozesse & Prozeduren

Penetrationstests, IT-Forensik Assessments & Audits

- Penetrationstests IT-Infrastruktur & Web-Applikations-Sicherheit
- IT Security & Compliance Checks
- Abwehr von Targetted / Client-side Attacks
- Beweissicherung & IT-Forensik

Infrastruktursicherheit & Data Protection

- Härtung Server-, Client- & Netzwerk-systeme
- Intrusion Detection & Prevention
- Data Leakage Detection & Prevention
- SCADA Security

Datenschutz

- Externer Datenschutzbeauftragter
- Datenschutzaudits & Auftrags-kontrollen
- Datenschutzkonzepte
- Schulungen

Zur GI-FG SECMGT

Die GI-Fachgruppe **Management von Informationssicherheit**

bietet den im Bereich des Managements von Informationssicherheit tätigen Personen eine neutrale Plattform, um sich miteinander zu vernetzen sowie Wissen und Erfahrungen auszutauschen.

- ist Teil der **Gesellschaft für Informatik** e.V. (gemeinnützige Fachgesellschaft zur Förderung der Informatik)
- beschäftigt sich mit der Verzahnung von informationstechnischen sowie organisatorischen Schutzmaßnahmen und dem Risikomanagement in Behörden oder Unternehmen
- vertritt praxisorientierte Themen zu Management, Konzeption, Betrieb und Fortentwicklung von Informationssicherheit
- veranstaltet mehrere Workshops pro Jahr (auch Nichtmitglieder sind stets willkommen); durch Teilnahme können CPEs erworben werden
- hat AK zu kritischen Informations- & Kommunikationsinfrastrukturen

→ **Nähere Informationen unter www.fg-secmgt.gi.de**

Inhalt

- Risikobasierter Ansatz im Datenschutzrecht
- Bewertung von Datenschutz-Risiken im Rahmen der Vorabkontrolle
- Bewertung von Datenschutz-Risiken im Rahmen der Auftragskontrolle
- Vorgehen zur Datenschutz-Folgenabschätzung nach geplanter EU-Datenschutz-Grundverordnung
- Compliance Management von Datenschutzrisiken

Risikobasierter Ansatz im Datenschutzrecht (1)

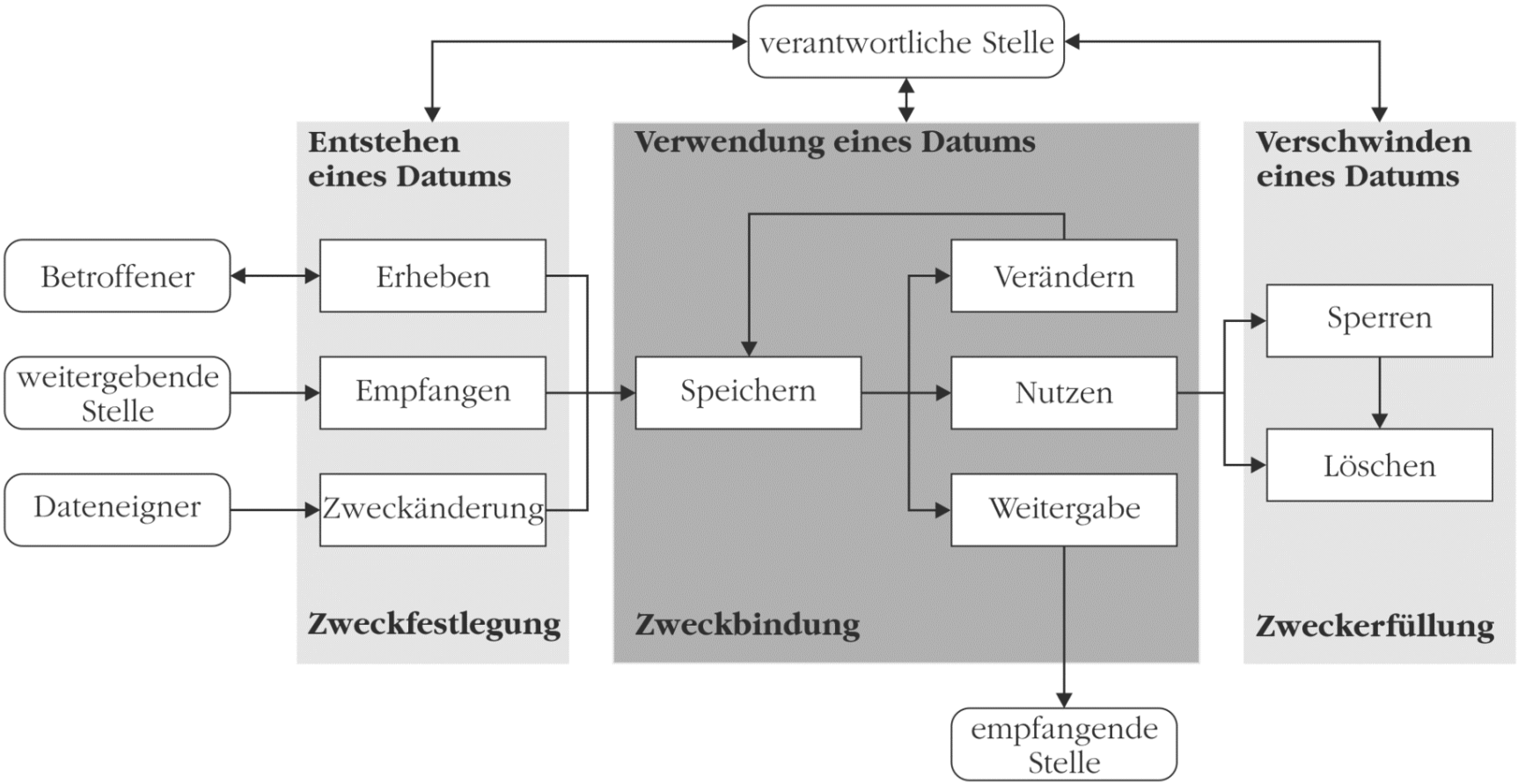
- Datenschutz betrifft nur Umgang mit **personenbezogenen Daten**
- Unzulässiger Umgang mit eigenem Bußgeldkatalog bestraft bzw. bei Vorsatz strafbar
- **Bußgeldkatalog** in zwei Kategorien unterteilt:
  ° Verstoß gegen Formvorschriften → max. 50.000 € Strafe
  ° Schwerwiegender Verstoß → max. 300.000 € Strafe
  + ggf. Gewinnabschöpfung
- Bußgeld wird nur dann fällig, wenn Aufsichtsbehörde dieses verhängt (geschieht selten und i.d.R. nicht unter Ausschöpfung des Maximalbetrags) → direkter finanzieller Schaden
- Zudem besteht **Meldepflicht bei Datenpannen**, sofern
  ° Unbefugter Kenntnis über sensible Daten erhalten hat
  ° Schwerwiegende Beeinträchtigungen für die Betroffenen drohen
  → Reputationsverlust! (+ indirekter finanzieller Schaden)
- Meldepflicht gegenüber Aufsichtsbehörde und den Betroffenen

→ **Datenschutzrisiken = Risiken des Datenschutzrechtsverstoßes**

Risikobasierter Ansatz im Datenschutzrecht (2)

- **Risikomanagement im Datenschutz**:
  → **Ziel**: Vermeidung ungewollter (!) Datenschutzrisiken
  → **Vorgaben des Gesetzgebers**:
  1. Durchführung Zulässigkeitsprüfung wg. „Verbot mit Erlaubnis-vorbehalt“ für jedes Verfahren
  2. Durchführung Erforderlichkeitsprüfung zu Daten
  3. Ergreifung erforderlicher Schutzvorkehrungen
  4. Durchführung Vorabkontrolle bei riskanten Verfahren
  5. Durchführung Auftragskontrolle bei Outsourcing
- **Verfahren** ist datenschutzrechtlich **zulässig**, wenn es hierzu eine gesetzliche Vorschrift gibt
  ° ausdrücklicher Erlaubnistatbestand (gilt für sehr viele Fälle!)
  ° Abwägung betriebliches Interesse vs. Betroffeneninteresse (für öffentlichen Bereich stark eingeschränkt!)
  ° informierte & freiwillige Einwilligung des Betroffenen
  ° Verwendung öffentlicher Daten (ohne Zugriffsschutz und zulässigerweise veröffentlicht → keine illegal veröffentlichten Daten)

Exkurs: Verfahren im Datenschutz

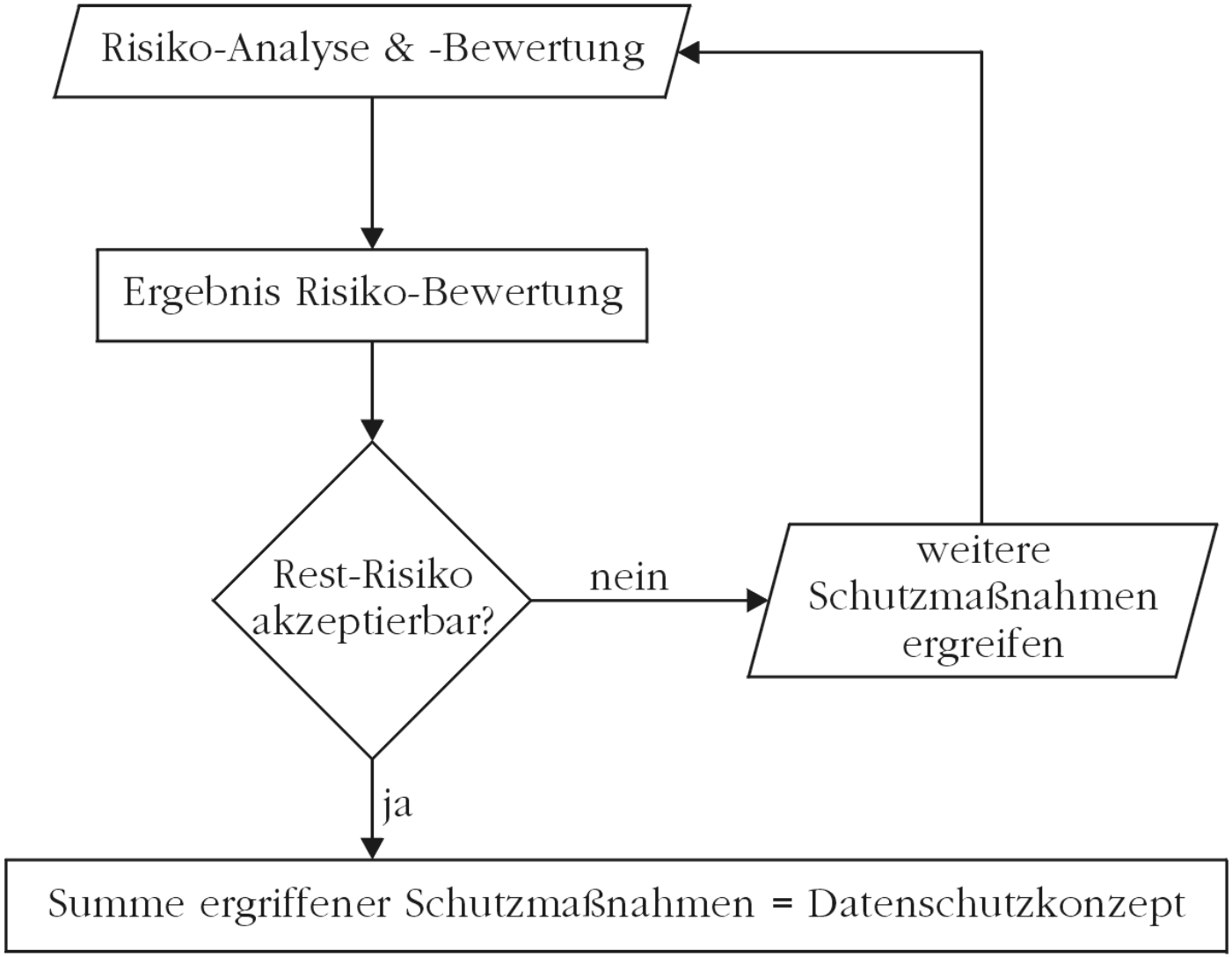


Verfahren = Festgelegte Art und Weise, wie eine Tätigkeit mittels automatisierter Verarbeitung bei jedem Einzelschritt im Life Cycle eines personenbezogenen Datums durchzuführen ist

Risikobasierter Ansatz im Datenschutzrecht (3)

- Bei jeweiligem Verarbeitungsschritt dürfen **nur erforderliche Daten** erhoben, verarbeitet oder genutzt werden
  → Begründungspflicht für jedes einzelne Datenfeld
  → Datenfeld muss für Zweckerfüllung benötigt werden
  → Wenn Zweck auch ohne Datenfeld erfüllbar ist, ist auf dieses Datenfeld im entsprechenden Verarbeitungsschritt zu verzichten (Datensparsamkeit)
- **Technische & organisatorische Maßnahmen** müssen Schutzgrad der Daten entsprechen und angemessen sein
  (→ Wirtschaftlichkeitsprüfung)
  ° Gliederung anhand Kontrollbereiche (z.B. gem. BDSG) oder Sicherheitsziele (gem. diverser LDSG); Gliederung jedoch im Bundesgebiet uneinheitlich!
  ° Zusammenfassung der Maßnahmen = **Datenschutzkonzept**
  ° Stand der Technik datenschutzrechtlich nur ausdrücklich für Verschlüsselung vorgeschrieben

Risikobasierter Ansatz im Datenschutzrecht (4)



Risikobewertung: Vorabkontrolle (1)

- Weisen Verfahren bzw. eingesetzte IT-Systeme besondere (!) Risiken für Rechte und Freiheiten der Betroffenen auf, ist eine Vorabkontrolle durchzuführen
- Vorabkontrolle ausdrücklich vorgeschrieben bei
  ° Umgang mit „**besonderen Arten personenbezogener Daten**“
  ° Zweck der **Persönlichkeitsbewertung** (zu Fähigkeiten, Leistung oder Verhalten)
  sofern nicht ausdrücklich gesetzlich vorgeschrieben, basierend auf Einwilligung des Betroffenen oder erforderlich zur Begründung bzw. Durchführung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses (= Vertrag + Vertragsanbahnung)
  → **Ausnahmeregel führt in der Praxis dazu, dass Vorabkontrolle zu selten durchgeführt wird** (Folge: trügerische Sicherheit)
- Vorabkontrolle ist durch den Datenschutzbeauftragten durchzuführen
- Nichtdurchführung selbst ist nicht strafbewährt, sondern nur die potenziellen Folgen (i.d.R. schwerwiegender Verstoß)

Risikobewertung: Vorabkontrolle (2)

- **Gegenstand der Vorabkontrolle**:
  ° Zulässigkeitsprüfung (→ „Materielle“ Zulässigkeit)
  ° Angemessenheit der Schutzvorkehrungen (→ Gewährleistung, dass von Verfahren / IT-System keine besonderen Risiken ausgehen)
  → Instrument präventiver Compliance

Checkliste für Vorabkontrolle

- ☐ besondere Arten personenbezogener Daten?
- ☐ Leistungs- / Verhaltens- / Fähigkeitsbewertung?
- ☐ Erstellung Persönlichkeitsprofil?
- ☐ neu entwickelte bzw. hochkomplexe IuK-Technik?
- ☐ Medienwechsel bei vertraulichem Verfahren?
- ☐ gravierende Wirkung auf Betroffenen?
- ☐ verschiedene Zwecke mit einem IT-System?
- ☐ Daten verschiedener Auftraggeber auf einem IT-System?
- ☐ Daten mit Amtsgeheimnis?
- ☐ Personalplanungs-/-informationssystem?
- ☐ CRM-System mit ERP-System vernetzt?

Klassifizierung Datenschutzrisiko: Beispiel 1

Schutzgrad

Schutzgrad 1 (kein Schutzbedarf):
Daten weisen keinen Personenbezug auf

Schutzgrad 2 (niedriger Schutzbedarf):
ein Personenbezug kann nur mit erheblichem Aufwand hergestellt werden

Schutzgrad 3 (mittlerer Schutzbedarf):
Daten sind mit vertretbarem Aufwand repersonalisierbar oder stammen aus allgemein zugänglichen Quellen

Schutzgrad 4 (hoher Schutzbedarf):
ein Vertraulichkeitsverlust der Daten erzeugt bereits einen Schaden für den Betroffenen, z.B. aufgrund von Zusatzwissen

Schutzgrad 5 (sehr hoher Schutzbedarf):
besonders sensible bzw. aufgrund einer besonderen Schutzverpflichtung geschützte Daten

Eintrittsstufe

Eintrittsstufe 1 (keine Kompromittierung):
mit einer an Sicherheit grenzenden Wahrscheinlichkeit erfolgt keine Kompromittierung

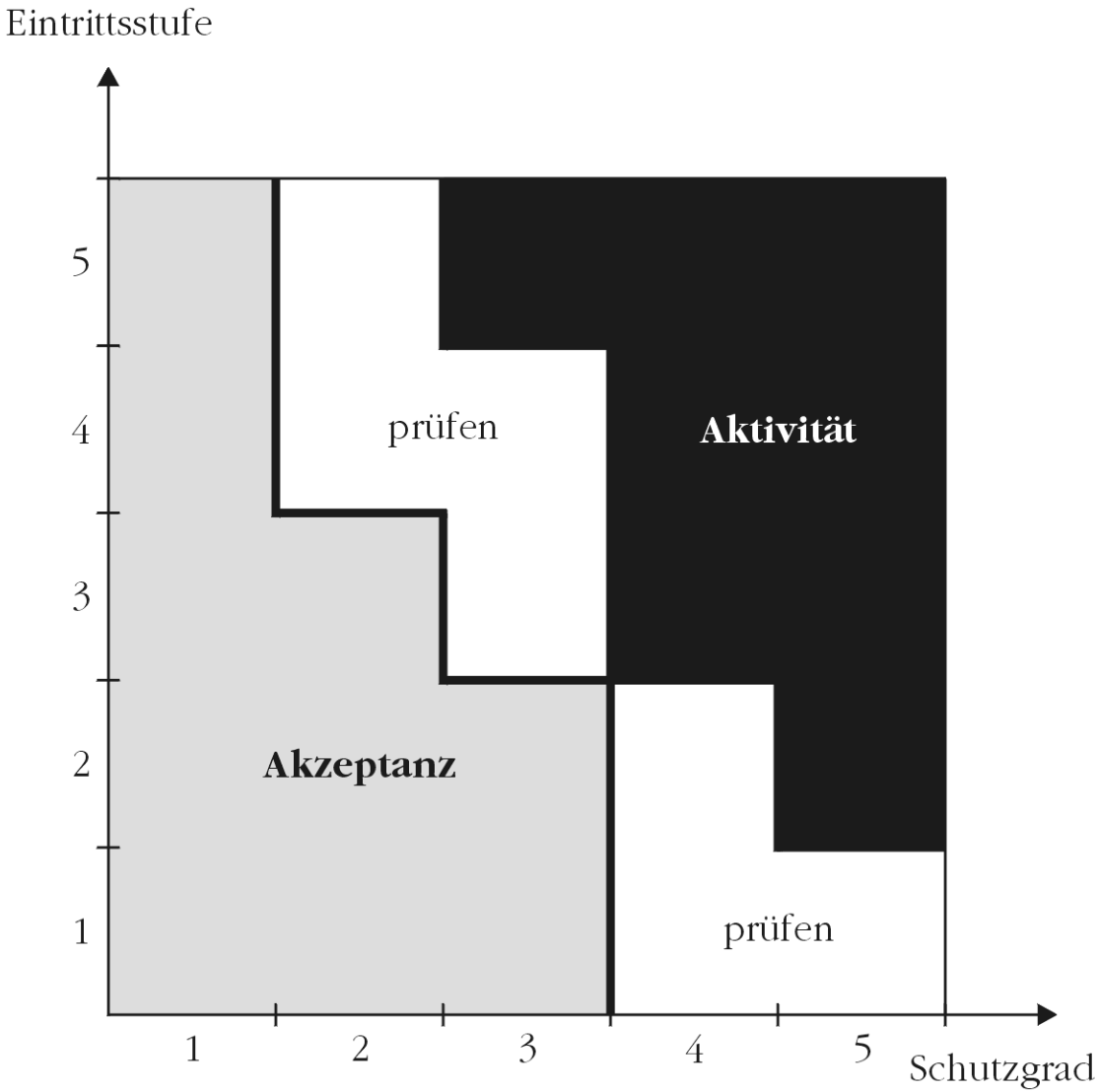
Eintrittsstufe 2 (unwahrscheinliche Komprom.):
ein Störer oder Angreifer muss über erhebliche Ressourcen oder Kenntnisse verfügen, um eine Kompromittierung erreichen zu können

Eintrittsstufe 3 (mögliche Kompromittierung):
ein Störer oder Angreifer muss über begrenzte Ressourcen oder Kenntnisse verfügen, um eine Kompromittierung erreichen zu können

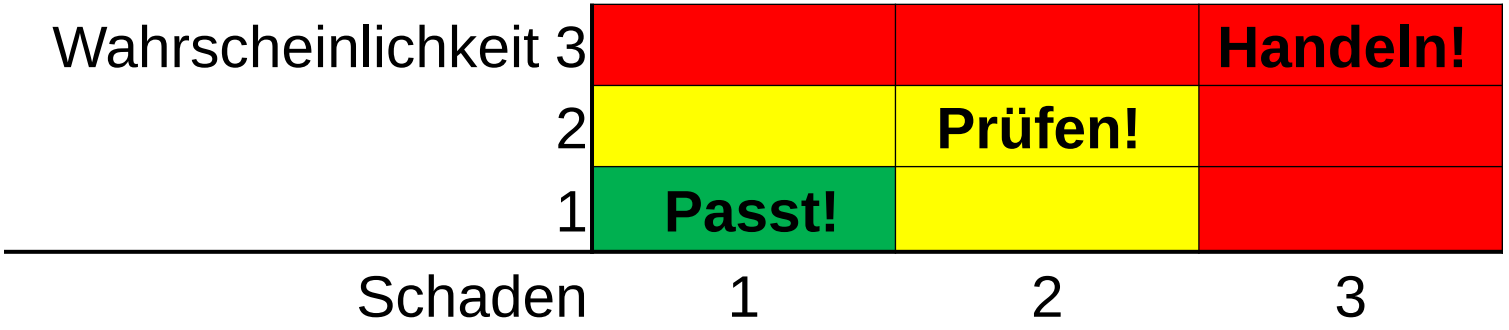
Eintrittsstufe 4 (wahrscheinliche Komprom.):
für eine Kompromittierung sind keine Ressourcen oder Kenntnisse erforderlich, die nicht leicht zu beschaffen sind

Eintrittsstufe 5 (sichere Kompromittierung):
eine Kompromittierung kann bereits aufgrund üblicher Basisausstattungen stattfinden

Klassifizierung Datenschutzrisiko: Beispiel 1



Klassifizierung Datenschutzrisiko: Beispiel 2



Wahrscheinlichkeit:
Eintritt einer Verletzung des informationellen Selbstbestimmungsrechts
1 = möglich
2 = wahrscheinlich
3 = sicher

Schaden:
Grad der Verletzung des informationellen Selbstbestimmungsrechts
1 = niedrig (ohne Wirkung)
2 = mittel (formaler Verstoß)
3 = hoch (Bußgeld/Datenpanne)

→ **Vermeidung akuter Datenschutzrisiken**
→ **Vermeidung strafbewährter Datenschutzrisiken**

Risikobewertung: Auftragskontrolle (1)

- Sofern Outsourcingpartner **Auftragsdatenverarbeitung** durchführen soll, bestehen detaillierte Vorgaben (Schriftformerfordernis, Weisungsgebundenheit, vordefinierter Regelungsumfang, Prüfpflicht), damit der Auftrag datenschutzrechtlich privilegiert ist
  → Auftragnehmer wird dann **Teil der verantwortlichen Stelle**!
  → Werden nicht alle Vorgaben vollständig eingehalten, liegt datenschutzrechtlich dagegen eine sog. „Funktionsübertragung“ vor (diese erfordert zulässigen Übermittlungstatbestand für Auftraggeber und zulässigen Empfangstatbestand für Auftragnehmer; aufgrund der Zweckänderung zudem Abwägung durchzuführen)
- Auftragnehmer ist **anhand** seiner **Schutzvorkehrungen sorgfältig (!) auszuwählen**
  → **Prüfpflicht** vor Aufnahme der Auftragsdatenverarbeitung
  → Pflicht zur regelmäßig durchzuführenden Auditierung
- Auftragskontrolle kann von beliebiger Stelle durchgeführt werden
- Nichtdurchführung selbst ist strafbewährt (Verstoß gegen Formvorschriften), Folgen waren Auslöser für BDSG-Verschärfung

Risikobewertung: Auftragskontrolle (2)

- Das eigentliche Problem bei der Auftragskontrolle liegt in den **unterschiedlichen Sichtweisen** von Auftraggeber & Auftragnehmer:
  - ° Rechtsfolgen eines Datenschutzverstoßes gelten voll gegenüber der verantwortlichen Stelle (Auftraggeber), Auftragnehmer kann allenfalls in Regress genommen werden (fehlende Regelungen / Weisungen gehen voll zu Lasten des Auftraggebers)
  - ° Auftragnehmer nimmt möglicherweise andere Risikobetrachtung vor als der Auftraggeber (hat u.U. höheren „Risikoappetit“)
  - ° Haftung von Verträgen faktisch in Bezug auf Vertragssumme beschränkt, deckt nicht zwingend das Schadensrisiko für Auftraggeber
  - ° Auftragnehmer möchte nicht auf Schwachstellen oder Incompliance den Auftraggeber hinweisen, um evtl. Sanktion auszulösen
  - → In der Praxis **leider oft vernachlässigte Datenschutzrisiken**!
  - → Auftraggeber sollte Datenschutzrisiko des Auftragnehmers bestimmen und **in eigenes Risikomanagement einbeziehen**!

Risikobewertung: Auftragskontrolle (3)

Einsparungseffekte

- Bereithalten für Auftragsabwicklung benötigter Ressourcen:
  - ° Räume
  - ° Technik
  - ° Ausführendes Personal
- Aufrechterhaltung des nötigen Know-hows bei ausführendem Personal (gerade bei hochspezialisierter Technik)
- Wartung von Technik und Räumen
- Schutzmaßnahmen

Kosten

- Entgelt für vereinbarte Tätigkeit des Auftragnehmers
- Personalkosten für Service Manager (zur Lenkung des Auftragnehmers)
- Aufrechterhaltung des nötigen Know-hows für Service Manager
- Overhead für Kommunikation mit Auftragnehmer
- Kosten für Auftragskontrollen
- Kostendifferenz bei Vorfällen

Risikobewertung: Auftragskontrolle (4)

- Nötig ist also eine **Aushandlung** zwischen Auftraggeber und Auftragnehmer zu:
  1. Welche Informationen über das **Sicherheitsniveau** beim Auftragnehmer sind für realistische Bewertung der Datenschutzrisiken nötig?
  2. Welche **Kontrollrechte** sind für Auftraggeber erforderlich, um sich ein zutreffendes Bild über Datenschutzlage beim Auftragnehmer vor allem hinsichtlich dessen Risikoappetit verschaffen zu können?
  3. Ab wann besteht ein ausreichendes **Vertrauen**, so dass der Auftragnehmer tatsächlich auch aufgetretene Schwachstellen dem Auftraggeber mitteilt, ohne „das Schlimmste“ befürchten zu müssen?

Neu: Datenschutz-Folgenabschätzung (1)

- Gemäß dem Entwurf für eine EU-Datenschutzgrundverordnung (EU-DSGVO) vom 25.01.2012 ist Folgendes geplant:
  - ° Jede verantwortliche Stelle hat sicherzustellen, dass die konkrete Datenverarbeitung **in Einklang mit der EU-DSGVO** durchgeführt wird, dabei die **Betroffenenrechte gewährleistet** werden, und muss dies **nachweisen** können (Art. 22 Abs. 1 + Art. 23 Abs. 1).
  - ° Die **Wirksamkeit** der dazu eingesetzten Maßnahmen muss (von unabhängiger Seite) **überprüft** werden (Art. 22 Abs. 3).
  - ° **Nur benötigte Daten** dürfen verarbeitet werden (Art. 23 Abs. 2).
  - ° Gleiches gilt für **Auftragsdatenverarbeitungen** (Art. 26 Abs. 1).
  - ° Schutzvorkehrungen müssen Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist (Art. 30 Abs. 1).
  - ° Maßnahmen nach der Risikobewertung zu treffen zum Schutz vor unbeabsichtigter / widerrechtlicher Zerstörung, unbeabsichtigtem Verlust, zur Vermeidung unrechtmäßiger Verarbeitung wie z.B. unbefugte Offenlegung / Verbreitung / Einsichtnahme (Art. 30 Abs. 2)

Neu: Datenschutz-Folgenabschätzung (2)

- Gemäß dem Entwurf für eine EU-Datenschutzgrundverordnung (EU-DSGVO) vom 25.01.2012 ist Folgendes geplant (Fortsetzung):
  - ° Bergen Verarbeitungsvorgänge aufgrund ihres **Wesens**, **Umfangs** oder ihrer **Zwecke** konkrete Risiken für die Rechte & Freiheiten der Betroffenen ist **Datenschutz-Folgenabschätzung** durchzuführen (Art. 33 Abs. 1), vor allem in den Fällen (Art. 33 Abs. 2)
    - * systematischer & umfassender Auswertung der Persönlichkeit
    - * der Verarbeitung besonders sensibler Daten, der Daten über Kinder, genetischer bzw. biometrischer Daten
    - * weiträumiger Videoüberwachung
    - * sonstiger Verarbeitungen gemäß einer vorgegebenen Liste der Aufsichtsbehörden (bisher leer)
  - ° Bei der Folgenabschätzung ist den **Betroffenenrechten & -interessen** Rechnung zu tragen und die Risiken in Bezug auf die Rechte & Freiheiten der Betroffenen zu bewerten (Art. 33 Abs. 3).
  - ° Die Meinung der Betroffenen oder ihrer Vertreter ist einzuholen (Art. 33 Abs. 4).

Neu: Datenschutz-Folgenabschätzung (3)

- Gemäß dem Entwurf für eine EU-Datenschutzgrundverordnung (EU-DSGVO) vom 25.01.2012 ist Folgendes geplant (2. Fortsetzung):
  - ° Die Folgenabschätzung wird von beliebiger Stelle durchgeführt; die Durchführung der Folgenabschätzung aber vom Datenschutzbeauftragten überwacht (Art. 37 Abs. 1), sofern einer bestellt werden musste.
  - ° Die **Nicht-Durchführung** der Folgenabschätzung kann mit einer **Geldbuße bis zu 1 Mio EUR bzw. bis zu 2 % des Jahresumsatzes** geahndet werden (Art. 79 Abs. 6 lit. i)!

→ Datenschutz-Folgenabschätzung muss **Betroffenensicht** abbilden

→ **Nur zulässige Verarbeitung** darf durchgeführt werden

→ **Nur erforderliche Daten** dürfen verarbeitet werden

→ **Schutzvorkehrungen** müssen **wirksam** sein

→ Datenschutz-Folgenabschätzung auch im Falle einer **Auftragsdatenverarbeitung** durchzuführen

→ Datenschutz-Folgenabschätzung = **präventives** Instrument

Compliance Management Datenschutzrisiken

- Beim „klassischen“ Informationssicherheitsmanagementsystem (ISMS) werden datenschutzrechtliche Risiken durch den **Kontext** des ISMS & Risk Assessments (RA) berücksichtigt (= **rechtliche Anforderungen**)
- RA **Methodologie** hat u.a. rechtliche Anforderungen einzubeziehen
- **„Klassisches“ RA** geht jedoch von Interessen der das RA durchführenden Stelle aus
- **Datenschutzbezogenes RA** geht dagegen von Interessen der Betroffenen aus (→ Transparenz, Intervenierbarkeit, Datensparsamkeit & Einhaltung der Zweckbindung weitere Ziele!)
- **Compliance Management** richtet sich danach aus, bußgeldbewährte sowie akute Datenschutzverstöße zu vermeiden
- **Nötig**: Zulässigkeitsprüfung, Datensparsamkeit & Nachweis ausreichender Schutzvorkehrungen (bei gesamtem Verfahren)
- Schutzvorkehrungen abhängig von Schutzgrad der Daten
- Abweichende Sichtweise von Auftragnehmern ist einzubeziehen

Vielen Dank für Ihre Aufmerksamkeit!

it.sec GmbH & Co. KG
Einsteinstr. 55
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Einsteinstr. 55
D-89077 Ulm