it.sec
security for your information

Risikomanagement im Rahmen von Outsourcing

Bernhard C. Witt
Senior Consultant für Datenschutz und Informationssicherheit

Workshop der GI-Fachgruppe Management von Informationssicherheit
10. Juni 2016, Frankfurt/Main

© 2016 it.sec GmbH & Co. KG www.it-sec.de

Bernhard C. Witt

- **Senior Consultant** für Datenschutz und Informationssicherheit bei der it.sec GmbH & Co. KG, verantwortlich für Datenschutz & 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)
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit (seit 2009), deren stellvertretender Sprecher seit 11/2013
- Mitglied im Leitungsgremium der GI-Fachgruppe Management von Informationssicherheit (seit 2007), deren Sprecher von 02/2009 – 11/2013
- Mitglied im Leitungsgremium der GI-Fachgruppe Datenschutz-fördernde Technik (seit 2012)
- Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfahren“ AK 1 & 4 (seit 2011)

Zur it.sec:

- Seit 1996 Dienstleister zur Informationssicherheit
- Penetrationstests
- IT-Forensik
- IT GRC Management

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Motivation für Outsourcing

Einsparungseffekte

- Bereithalten der zur Auftragsabwicklung benötigten Ressourcen:
  - ° Räume
  - ° Technik
  - ° Ausführendes Personal
- Aufrechterhaltung des nötigen Know-hows bei ausführendem Personal (gerade bei hochspezialisierter Technik)
- Wartung von Technik und Räumen
- Ergreifung und Aufrechterhaltung nötiger 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 durchzuführende Auftragskontrollen
- Kostendifferenz bei Eintritt von Vorfällen

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Bernhard C. Witt
bcwitt@it-sec.de

© 2016 it.sec GmbH & Co. KG www.it-sec.de

Auftragsdatenverarbeitung (1)

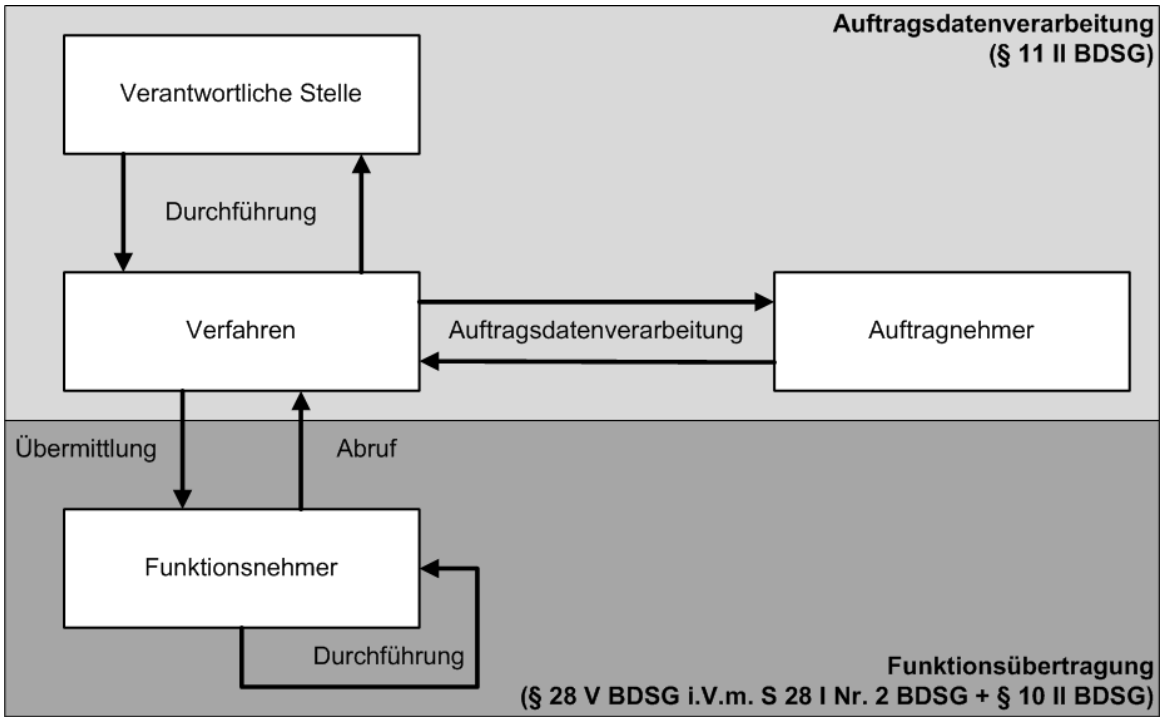
Datenschutzrechtliche Anforderungen zur Auftragsdatenverarbeitung:

- Zur sog. **Auftragsdatenverarbeitung** bestehen nach § 11 BDSG bzw. Art. 28 EU-DS-GVO detaillierte Vorgaben wie
  - Schriftformerfordernis (mit ausgelisteten Vertragsbestandteilen)
  - Weisungsgebundenheit
  - Prüfpflichten
  - Genehmigungserfordernis für Einsatz von Unterauftragnehmern
  - Löschung / Herausgabe der Daten zu Vertragsende
- Auftragnehmer ist anhand seiner Schutzvorkehrungen (= technische & organisatorische Maßnahmen) sorgfältig (!) auszuwählen
  → Prüfpflicht vor Aufnahme der Auftragsdatenverarbeitung
  → Maßnahmen nach Stand der Technik (Art. 32 Abs. 1 EU-DS-GVO)
  → Pflicht zur regelmäßig (!) durchzuführenden Wirksamkeitskontrolle
- Gemäß Art. 28 Abs. 1 EU-DS-GVO muss der Auftragnehmer zudem hinreichende Garantien zur Einhaltung der EU-DS-GVO und zum Schutz der Betroffenenrechte nachweisen (z.B. durch Zertifikat)!

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Auftragsdatenverarbeitung (2)

- Auftragsdatenverarbeitung ist datenschutzrechtlich privilegiert
  → Auftragnehmer wird Teil der verantwortlichen Stelle!
  → Werden jedoch nicht alle Vorgaben vollständig eingehalten, liegt alternativ eine sog. „Funktionsübertragung“ vor



Funktionsübertragung erfordert zulässigen Übermittlungstatbestand f. Auftraggeber und zulässigen Empfangstatbestand f. Auftragnehmer; aufgrund der Zweckänderung (wg. Eigeninteresse) ist zudem eine verschärfte Abwägung durchzuführen

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Auftragsdatenverarbeitung (3)

- Nach § 43 Abs. 1 Nr. 2b BDSG ist einerseits ein
  - nicht richtiger
  - nicht vollständiger
  - nicht in der vorgeschriebenen Weise erteilter

  Auftrag bußgeldbewährt
  → Formfehler führen dazu, dass entweder ein Bußgeldtatbestand erfüllt ist oder eine Funktionsübertragung vorliegt, die ggf. generell unzulässig ist und teuereren Bußgeldtatbestand erfüllt…
- Nach § 43 Abs. 1 Nr. 2b BDSG ist andererseits bußgeldbewährt, wenn sich der Auftraggeber nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt
  → Dokumentationspflicht!
  → Nachweis erfolgt oft anhand „Papierprüfung“
- Ordnungswidrigkeiten nach § 43 Abs. 1 BDSG können mit einer **Geldbuße von bis zu 50.000 €** bestraft werden

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Auftragsdatenverarbeitung (4)

- Ab 25. Mai 2018 (Inkrafttreten der EU-DS-GVO) steigt das Bestrafungsrisiko deutlich:
  - Die Nichteinhaltung von Auflagen zur Auftragsdatenverarbeitung
  - Unzureichende Maßnahmen zur Sicherheit der Verarbeitung
  - Unzureichende Meldungen von Verletzungen des Schutzes personenbezogener Daten
  - Missachtung von Privacy by Design / Default

  kann mit **Geldbußen von bis zu 10 Mio. € bzw. von bis zu 2 % des weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres geahndet werden!
- Verstöße gegen die Betroffenenrechte und eine unzulässige Übermittlung von Daten in Drittstaaten können sogar mit **Geldbußen von bis zu 20 Mio. € bzw. von bis zu 4 % des weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres geahndet werden!
- Diese **Bußgeldtatbestände gelten** für Auftraggeber wie Auftragnehmer gleichermaßen und dürfen **schon ab 25.05.2018** verhängt werden!

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Auftragsdatenverarbeitung (5)

- Problem: die Vertragspartner haben **unterschiedliche Sichtweisen**:
  - **Rechtsfolgen eines Datenschutzverstoßes** gehen **voll zu Lasten der verantwortlichen Stelle** (Auftraggeber)
  - Auftragnehmer kann allenfalls in Regress genommen werden
  - Fehlende Regelungen / Weisungen treffen nur Auftraggeber
  - Auftragnehmer nimmt möglicherweise **andere Risikobetrachtung** vor als der Auftraggeber (hat u.U. höheren „Risikoappetit“)
  - Zudem bestehen Unterschiede in Betrachtung von IT-Risiken, Informationssicherheits-Risiken und Datenschutz-Risiken
    → IT- & IS-Risiken aus Sicht des Verarbeiters
    → DS-Risiken dagegen aus Sicht des Betroffenen
  - Auftragnehmer möchte nicht auf Schwachstellen oder Incompliance hinweisen, da dies ggf. Sanktionen auslösen kann
  - Haftung von Verträgen faktisch in Bezug auf Vertragssumme beschränkt, deckt meist nicht das Schadensrisiko für Auftraggeber

→ **In der Praxis leider oft unterschätzte Datenschutzrisiken!**

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Sichere Supply Chain (1)

Nach Kapitel 15 der **ISO/IEC 27002:2013** sollte sich ein Auftraggeber um **Informationssicherheit in Lieferantenbeziehungen** kümmern:

- Sobald ein Auftragnehmer bzw. Lieferant Zugriff auf (Primary oder Supporting) Assets des Auftraggebers erhält, sollten mit diesem **einzuhaltende Anforderungen zur Informationssicherheit** vereinbart und dokumentiert werden.
- In einer Informationssicherheitsrichtlinie für Lieferantenbeziehungen sollte insbesondere festgelegt werden:
  - **Mindestanforderungen an die Informationssicherheit** für jede Informations- und Zugriffsart entsprechend den geschäftlichen Bedürfnissen und den Anforderungen des Auftraggebers sowie entsprechend des Risikoprofils des Auftraggebers
  - **Prozesse und Verfahren zur Überwachung** der Einhaltung der festgelegten Anforderungen an die Informationssicherheit für jede Lieferanten- und Zugriffsart
  - **Umgang mit Vorfällen und Gefahren** im Zusammenhang mit dem Lieferantenzugriff

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Sichere Supply Chain (2)

In **Lieferantenvereinbarungen** sollte hierzu insbesondere festgelegt und dokumentiert werden:

- Wie vom Auftragnehmer / Lieferant die Einhaltung gesetzlicher und behördlicher **Anforderungen zu Datenschutz, geistigen Eigentumsrechten und Urheberrecht** sichergestellt wird
- Verpflichtungen zur Umsetzung vereinbarter Maßnahmen hinsichtlich
  - Zugangs- bzw. Zugriffssteuerung,
  - Leistungsüberprüfung,
  - Überwachung,
  - Berichterstattung und
  - Auditierung
- Vertragsrelevante Richtlinien zur Informationssicherheit
- Anforderungen und Verfahren für die Handhabung von Vorfällen
- Relevante Vorschriften für Unteraufträge
- Recht zur Überprüfung der Lieferantenprozesse und vertragsbezogener Maßnahmen sowie Vorlage unabhängiger Wirksamkeitskontrollberichte

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Sichere Supply Chain (3)

In **Lieferantenvereinbarungen** sollten ferner insbesondere die Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, aufgenommen werden:

- Verpflichtung zur Weitergabe der Sicherheitsanforderungen innerhalb der gesamten Lieferkette (inkl. Unterauftragnehmer, Lieferanten des Auftragnehmers / Lieferanten)
- Zusicherung, dass bereitgestellte Informations- und Kommunikationstechnik wie erwartet funktioniert und keine unerwarteten oder unerwünschten Eigenschaften aufweist
- Festlegung von Regeln für die Mitteilung von Informationen über mögliche Probleme und Kompromisse zwischen Auftraggeber und Auftragnehmer / Lieferant

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Sichere Supply Chain (4)

Das **vereinbarte Niveau der Informationssicherheit** sollte im Einklang mit den Vereinbarungen **aufrecht erhalten** werden insbesondere durch:

- Durchführung von Lieferanten-Audits, inkl. Problem-Nachverfolgung
- Bereitstellung von Informationen zu Informationssicherheitsvorfällen und Überprüfung dieser Informationen
- Überprüfung der Aufzeichnungen zu Informationssicherheitsereignissen, Problemen im Zuge der Auftragsausführung, Ausfällen, Fehler-Nachverfolgungen und Unterbrechungen
- Überprüfung von Aspekten der Informationssicherheit bei den Beziehungen des Auftragnehmers / Lieferanten zu seinen eigenen Lieferanten
- **Erneute Risikobeurteilung**, insbesondere bei
  - Änderungen an den vertraglichen Vereinbarungen mit dem Auftragnehmer / Lieferant
  - Neue oder geänderte Maßnahmen zur Lösung von Informationssicherheitsvorfällen und zur Verbesserung der Sicherheit
  - Nutzung neuer Technologien oder neuer Entwicklungswerkzeuge

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Sichere Supply Chain (5)

Auch hier bestehen deutliche Unterschiede zwischen Auftraggeber und Auftragnehmer / Lieferant im Kontext der Supply Chain:

- Auftragnehmer hat oft **anderen Risikoappetit** als ihre Auftraggeber
  → Pönale i.d.R. weit geringer als potenzieller Schaden bei Risikoeintritt!
  → Wirtschaftliches Handeln legt teils Akzeptanz Pönale nahe
- Auftragnehmer verwendet oft **andere Methodologie zur Risikoanalyse** (oder anders ausgeprägter Methodologie) als ihre Auftraggeber
  → das steht in Beziehung zum jeweiligen Geschäftsmodell…
- Auftragnehmer hat **andere Vorstellung hinsichtlich meldepflichtiger Security Incidents** als Auftraggeber, wenn dies nicht ausdrücklich festgelegt wurde (was jedoch in der Praxis nur bedingt möglich ist…)
- Für Auftragnehmer ist es i.d.R. von **nachrangigem Interesse**, **welche Datenkategorien** im Auftrag verarbeitet werden, für Auftraggeber sind dagegen die überlassenen Daten u.U. grundlegend

→ **Das jeweils implementierte ISMS weicht stark voneinander ab!**

→ **Vorgelegtes Zertifikat genau prüfen (Scope, SoA, Aussteller)!**

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Ergebnis

- Nötig ist **Aushandlung** zwischen Auftraggeber & Auftragnehmer zu:
  1. Welche Informationen über das **Sicherheitsniveau** beim Auftragnehmer sind für realistische Bewertung der mit der Auslagerung verbundenen Risiken nötig?
  2. Welche **Kontrollrechte** sind für Auftraggeber erforderlich, um sich ein zutreffendes Bild über das Sicherheitsniveau 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?
- Die Auslagerung selbst stellt ein **spezifisches Risiko** dar, das im Hinblick auf die Konsequenzen für den Auftraggeber (ohne unterstellte kompensatorische Maßnahmen) zu bewerten ist
- Im Rahmen des Risikomanagements sollte auch bei entsprechender Auslagerung die **zugehörigen Gefährdungen** (Bedrohungen und Verwundbarkeiten) **miteinbezogen** werden (zugesicherte Maßnahmen des Auftragnehmers dienen dann der Mitigation der ermittelten Risiken)

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung

Vielen Dank!

- **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

  tel: +49 (0) 731 20589-0
  mailto:info@it-sec.de
  http://www.it-sec.de

© it.sec GmbH & Co. KG - Keine Vervielfältigung oder Weitergabe ohne Genehmigung