5. Digitalisierungsspezifische Problembereiche und Handlungsempfehlungen

Aus datenschutzrechtlicher Sicht kommt insbesondere den digitalisierungsspezifischen Themengebieten der Webanalyse bzw. des Webtrackings und der Reichweitenmessung, des Cloud-Computing sowie der Vernetzung von Systemen besondere Bedeutung zu. Durch den Transfer personenbezogener Daten zwischen Geschäftspartnern und Dienstleistern bei vernetzten Systemen stellt sich zuallererst oftmals die Frage, welche Partei welche datenschutzrechtlichen Verantwortlichkeiten übernimmt. Nachstehend werden die Besonderheiten der datenschutzrechtlichen Verantwortlichkeit bei digitalisierungsspezifischen Sachverhalten sowie anschliessend jene der Webanalyse, des Cloud-Computing sowie der Vernetzung von Systemen dargestellt.

5.1 Datenschutzrechtliche Verantwortlichkeit bei digitalisierungsspezifischen Sachverhalten

Werden *personenbezogene Daten* zwischen Unternehmen transferiert, so bestimmen sich die datenschutzrechtliche Verantwortlichkeit und der damit einhergehende Handlungsbedarf danach, wer Mittel und Zwecke der Datenverarbeitung festlegt. Geschieht dies gemeinsam durch zwei oder mehrere Verantwortliche (z. B. aufgrund des gemeinsamen Betriebes einer Datenbank), so ist von einer gemeinsamen Verantwortlichkeit („Joint Controllership“) gem. Art. 26 DSGVO auszugehen. Es ist dann ein entsprechender Joint-Controllership-Vertrag abzuschliessen. Darin sind die jeweiligen Verantwortlichkeiten der einzelnen Parteien zu konkretisieren, insbesondere im Hinblick auf die Wahrnehmung der Betroffenenrechte und die Informationspflichten nach den Artikeln 13 und 14 DSGVO (Schneider, 2019). Zusätzlich sind vor allem beim Betrieb gemeinsamer Datenbanken die jeweiligen Datensphären und die TOMs in Abhängigkeit der konkreten Verarbeitungstätigkeiten und der damit einhergehenden individuellen Risiken je Partei zu definieren. Daneben bedarf die Datenübermittlung in diesem, aber auch in jenem Fall, in welchem anstelle der gemeinsamen eine eigene Verantwortlichkeit vorliegt, einer gesonderten Rechtsgrundlage nach Art. 6 DSGVO, da Joint Controller nach Art. 4 Nr. 10 DSGVO sogenannte „Dritte“ sind (Dovas, 2016, S. 512). Eine gemeinsame Verantwortlichkeit kann z. B. bei Big Data-Anwendungen, im Bereich des Affiliate-Marketings oder bei der sukzessiven oder gleichzeitigen Verarbeitung bzw. Übermittlung von Daten zwischen Internetplattformen vorliegen (Dovas, 2016, S. 512).

Wird ein Unternehmen lediglich weisungsgebunden und ohne eigene Entscheidungsbefugnis für und im Auftrag einer verantwortlichen Stelle (den Auftraggeber) tätig (z. B. im Rahmen von IT-Support und Wartungsdienstleistungen), so handelt dieses selbst als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO (Auftragnehmer) und ein Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DSGVO ist abzuschliessen. Beauftragt ein Auftragsverarbeiter z. B. im Rahmen des Softwarehostings seinerseits selbst einen Auftragsverarbeiter (z. B. einen Cloudanbieter), so ist auch zwischen diesen beiden Parteien ein entsprechender Vertrag unter Berücksichtigung der Besonderheiten der Unterbeauftragung abzuschliessen. Der Auftraggeber sollte sich im Rahmen seiner Weisungsbefugnis also stets vertraglich zusichern lassen, dass Unterauftragnehmer / Subdienstleister nur mit seiner vorherigen Genehmigung vom Auftragnehmer eingesetzt werden.

5.2 Datenschutzrechtliche Besonderheiten der Webanalyse, des Cloud-Computing sowie der Vernetzung von Systemen

Der Einsatz von Webtracking-Tools (z. B. Google Analytics, Matomo), die Nutzung von Cloudangeboten (z. B. durch Speicherplatz) sowie die Vernetzung von Systemen ziehen jeweils datenschutzrechtliche Besonderheiten nach sich. Dazu sind in Abbildung 14 die jeweiligen grundlegenden Handlungsempfehlungen beispielhaft zusammengefasst. Dabei wird davon ausgegangen, dass *personenbezogene Daten* verarbeitet werden.

Daten als Asset

1. Paradigmenwechsel im Umgang mit Daten ohne Personenbezug

Daten und ihre Verwertung durch Analysemethoden tragen nicht nur zur Realisierung von Effizienzpotenzialen beim Einsatz von Ressourcen bei. Sie eröffnen auch die Weiterentwicklung bestehender und die Einführung neuer Geschäftsmodelle (Geissbauer, Schrauf, Berttram, & Cheraghi, 2017, S. 26). Damit stossen Daten bzw. die hieraus gewonnene Information sukzessive in das Zentrum erfolgsrelevanter Wertschöpfungsfaktoren vor. Das könnte sie zukünftig auf eine Ebene mit Arbeitskraft, Technologie und Kapital als Kernfaktoren der Wertschöpfung heben (Porter & Happelmann, 2015, S. 3; Otto, et al., 2016, S. 10). In Unterscheidung zu den vorgenannten Produktionsfaktoren ist ausserdem zu

Webtracking-Tools (z. B. Google Analytics, Matomo)	Cloud Computing, z. B. in Form von Speicherplatz	Vernetzung von Systemen
· Sicherstes Vorgehen auf Basis einer expliziten Einwilligung · Information der Website-Besucher über Tracking-Methoden in Datenschutzhinweisen · Wahl der jeweils möglichen datenschutzfreundlichen Voreinstellungen	· in der Regel Abschluss einer Vereinbarung zur Auftragsverarbeitung erforderlich · Zusicherung von Serverstandorten in der EU / des EWR empfehlenswert · Anonymisierung der Daten, Einsatz von adäquaten Verschlüsselungstechnologien	· Klärung der datenschutzrechtlichen Verantwortlichkeiten für die Systeme / Systemkomponenten · Wahrung des Grundsatzes der Zweckbindung, Vorsicht bei der Verknüpfung von Datensätzen · Wahrung der Transparenzpflichten gegenüber Betroffenen

Abbildung 14: Handlungsempfehlungen für Webtracking-Tools, Cloud-Computing und der Vernetzung von Systemen

berücksichtigen, dass Daten nicht rivalisierende und nicht abnutzbare (virtuelle) Güter sind (Schmidt, Schmidt & Zech, 2018, S. 627).

Unternehmen stehen in Anbetracht dieses Potenzials nicht mehr nur vor der Frage, wie sie Eigentums- und Nutzungsrechte an herkömmlichen materiellen und immateriellen Wertschöpfungsfaktoren sichern und disponieren, sondern ob und wie entsprechende Rechte auch an Daten als solchen entstehen können.

Im Folgenden wird zunächst auf die Eingrenzung des Datenbegriffs eingegangen. Anschliessend wird aufgezeigt, ob und wie Daten ohne Personenbezug nach geltendem Recht Schutz geniessen.

2. Datenbegriff

Obwohl Daten eine zunehmende wirtschafliche Bedeutung beizumessen ist, sind sie als Rechtsobjekt in den Rechtsordnungen der DACH-Region nur schwer greifbar (Schmidt, Schmidt & Zech, 2018, S. 627; Markendorf, 2018, S. 409). Dort findet sich weder eine Legaldefinition des Datenbegriffs, noch ein allgemeines „Datengesetz“ (Schmidt, Schmidt & Zech, 2018, S. 627; Markendorf, 2018, S. 409). Zwar wird im Rechtsgebiet des Datenschutzes der Begriff des personenbezogenen Datums als Information, die sich auf eine identifizierte oder identifizierbare natürliche Person bezieht (Art. 4 Nr. 1 EU-DSGVO) bzw. als Angabe, die sich auf eine bestimmte oder bestimmbare Person bezieht (Art. 3 lit. b DSGVO), definiert. Doch handelt es sich hier lediglich um eine Teilmenge des umfassenderen Datenbegriffs. Vereinzelt ist der Datenbegriff darüber hinaus in straf-[2] und urheberrechtlichen[3] Bestimmungen anzutreffen, jedoch ohne hierin näher definiert zu werden.

Der Versuch einer Schärfung des Datenbegriffs wird von der Literatur zumeist unter Heranziehung der Zeichenlehre (Semiotik) vorgenommen. So lassen sich Daten als maschinenlesbar codierte Information auf der syntaktischen Ebene definieren. Dabei liegen Daten regelmässig auf physikalischer bzw. strukturierter Form auf einem Datenträger vor, der die darstellende Syntaktik ermöglicht (Schmidt, Schmidt & Zech, 2018, S. 627). Auf dieser Ebene sieht die Informatik bei der Zusammenfassung konkreter Wertebereiche und hierauf definierter Operationen zu einer Einheit, bestimmte Datentypen vor. Unter elementaren Datentypen werden ganze, natürliche, Festkomma- und Gleitkommazahlen sowie Aufzählungstypen, logische Werte (sogenannte „Booleans“) und Zeichen verstanden (Müller, Käser, Gübell & Klaus, 2009, S. 240). Hiervon werden dynamische und zusammengesetzte Datentypen (Zeichenketten fester, variabler und dynamischer Länge und Zeichenverbund) unterschieden (Müller, Käser, Gübell & Klaus, 2009, S. 240). Oberhalb der syntaktischen Ebene können Daten eine Bedeutung (Semantik) in Form von Information und Wissen aufweisen. Daten lassen sich mithin auf der Bedeutungsebene (semantische Information) und auf der Zeichenebene (syntaktische Information) abgrenzen (Schmidt, Schmidt & Zech, 2018, S. 627).

[2] für Deutschland: §§ 202a ff. StGB, § 303a StGB; für Österreich: §§ 119a, 126a, 225a StGB; für die Schweiz: Art. 143 StGB
[3] für Deutschland: § 4, §§ 87a ff. UrhG; für Österreich: § 40f UrhG, §§ 76a ff. UrhG; Die Schweiz kennt – anders als die EU – kein „Datenbankgesetz“ (sui-generis-Schutz) und deshalb auch keine gesetzliche Definition des Begriffs „Datenbank“.

Neben dieser semiotischen Eingrenzung des Datenbegriffs können Daten auch nach Ebenen ihrer Entstehung bzw. Verarbeitung kategorisiert werden. Die Abbildung 15 und die Abbildung 16 (s. S. 44) zeigen die Ebenen von Datenerzeugung, Konnektivität, Datenkuratierung sowie -analyse und zuordenbare Datentypen und Verarbeitungszustände exemplarisch anhand des Maschinenparks eines fertigenden Unternehmens.

Ob und wie solche Daten ohne Personenbezug rechtlichen Schutz geniessen können, soll im Weiteren dargestellt werden.

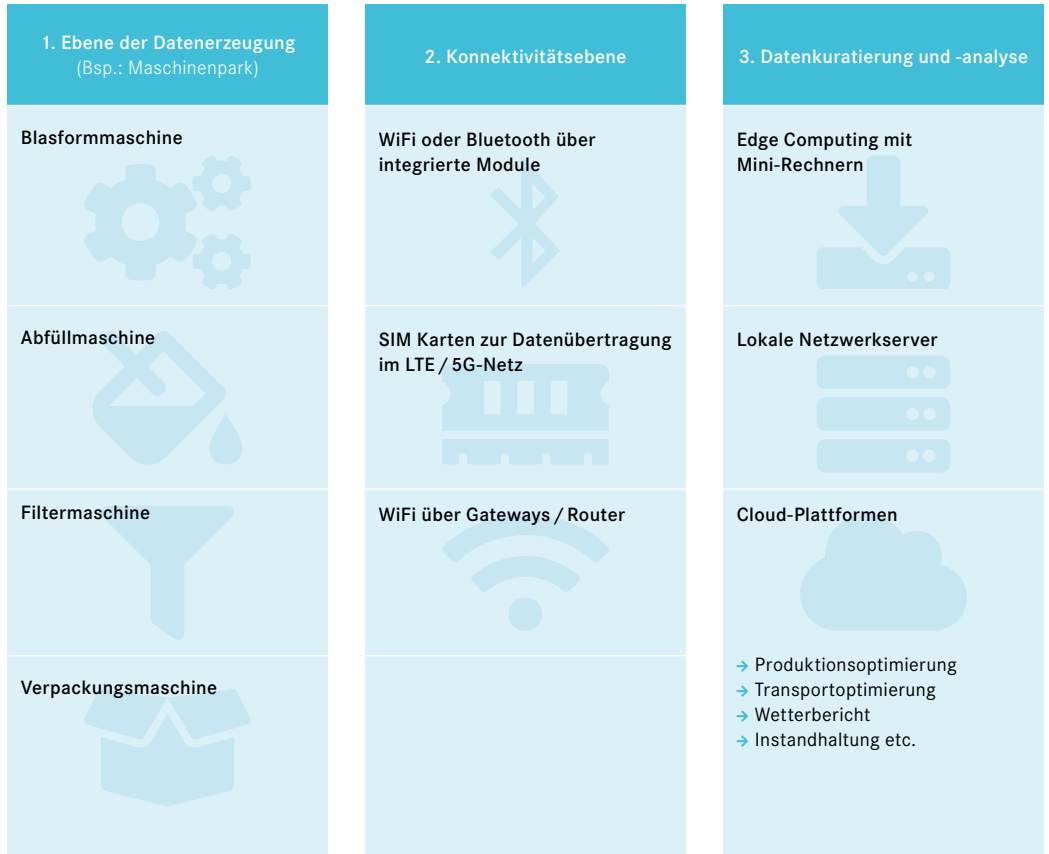

Abbildung 15: Ebenen der Datenverarbeitung am Beispiel eines Maschinenparks (1)

1. Ebene der Datenerzeugung (Bsp.: Maschinenpark)	2. Konnektivitätsebene	3. Datenkuratierung und -analyse
Erzeugungsort Maschine	**Bestimmungsort** Mini-Rechner / Lokaler Netzwerkserver / Cloud-Server	**Weiterer Speicher- / Verarbeitungsort** Mini-Rechner / Lokaler Netzwerkserver / Cloud Server
Inhalt Temperatur	**Inhalt** Temperatur	**Inhalt** Temperatur, Temperaturprofil, Auslastungs- und Abnutzungs-status
Aggregationsstufe Rohdatum	**Aggregationsstufe** Datenpaket	**Aggregationsstufe** Rohdatum, Analyseergebnis, Datenbankelement
Datentyp Primitiv (Zahlen, Zeichen, Wahr-heitswerte) oder Komplex (Arrays, List, Set, Multiset, Zeilen)	**Übertragungsprotokoll** LoRa-WAN-Protokoll	**Datentyp** Primitiv (Zahlen, Zeichen, Wahr-heitswerte) oder Komplex (Arrays, List, Set, Multiset, Zeilen)
Erster Speicherort Lokaler SPS Speicher		
Sphäre intern		**Sphäre** Intern (Edge Computing, lokale Server) und extern (Cloud-Anbie-ter, Applikationsanbieter, etc.)

Abbildung 16: Ebenen der Datenverarbeitung am Beispiel eines Maschinenparks (2)

3. Rechte an nicht personenbezogenen Daten

Wo das Recht einer natürlichen oder juristischen Person Nutzungs- und Verwertungsrechte an materiellen und immateriellen Gütern zuweist, dient dies regelmässig der Schaffung von Rechtssicherheit und Transparenz. Somit können entsprechende Positionen leichter zum Gegenstand vertraglicher Transaktionen gemacht werden (Sattler, 2017, S. 30). Neben der Frage, ob Daten dem sachenrechtlichen oder geistigen Eigentum zugänglich sind, wird in der juristischen Literatur auch ein wettbewerbsrechtlicher und deliktischer Schutz (Recht der unerlaubten Handlung im Zivilrecht) selbiger diskutiert. In Einzelfällen kann ein Zugriff auf Daten auch strafrechtliche Tatbestände erfüllen.

Daten im vorstehend zugrunde gelegten Sinne sind virtuelle Rohmaterialien, die de lege lata keinem normativen Schutzbereich unterfallen (Ensthaler, 2016, S. 3474). Zwar dürfte in Deutschland und Österreich dem Datenbankherstellerrecht bei der methodischen Sammlung, Verarbeitung und Analyse nicht personenbezogener Daten in der Praxis noch die vergleichsweise grösste Bedeutung zukommen (Ehlen, 2016, S. 571; Hürlimann & Zech, 2016, S. 92). Jedoch zielt dieses Recht lediglich auf den Schutz getätigter Investitionen zur Erstellung betreffender Datenbanken ab. Es schützt aber nicht die zugrundeliegenden Einzelelemente, d. h. die Investition in die Erzeugung der Daten als solche. Über den bestehenden normativen Rahmen können höchstens Abwehrrechte aus dem Straf-, Wettbewerbs- oder Deliktsrecht entstehen, die jedoch im Falle der aktiven Zusammenarbeit zwischen vernetzten Wertschöpfungsakteuren (bspw. Lieferanten, Hersteller, Cloud-Anbieter, Softwarehäusern und Kunden) zumeist ins Leere laufen dürften (Żdanowiecki, 2015, S. 23).

Der Vergleich mit Kapitel „Daten mit Personenbezug“, führt nun einen wesentlichen Unterschied zum rechtlichen Umgang mit nicht personenbezogenen Daten vor Augen: Das Datenschutzrecht verbietet die Verarbeitung personenbezogener Daten, es sei denn, ein gesetzlicher Erlaubnistatbestand lässt dies zu (Verbot mit Erlaubnisvorbehalt); Daten ohne Personenbezug sind hingegen „vogelfrei“, sofern nicht ein gesetzliches oder vertragliches Verbot greift (Erlaubnis mit Verbotsvorbehalt) (Sattler, 2017, S. 46). Nicht *personenbezogene Daten* unterliegen damit dem Grundsatz der Privatautonomie (Sattler, 2017, S. 46).

Hieraus lässt sich also ableiten, dass es aus Unternehmenssicht dringenden Handlungsbedarf für Massnahmen der KMU zur Sicherung des ggf. geschäftskritischen Assets „Daten“ gibt.

4. Vertragliche Zuordnung von Daten

Ein Rechtsinstitut zur abschliessenden und eindeutigen Rechtezuweisung an einzelnen Daten, unstrukturierten Datenanhäufungen, aber auch an einzelnen Analyseergebnissen, ist aktuell nicht existent – Daten folgen keiner proprietären Zuweisungslogik (Heymann, 2016, S. 652), ihre Exklusivität kann nur durch faktische Gegebenheiten erreicht werden (Stender-Vorwachs, 2018, S. 1362). Ausserhalb oben beschriebener Rechtskonstrukte kommt deshalb zur Schaffung einer zumindest zwischen Vertragsparteien wirkenden Rechtsklarheit, nur die Ausgestaltung relativ wir-

kender Regelungen im Wege der Vertragsgestaltung in Betracht (Ensthaler, 2016, S. 3474; Chirco, 2016, S. 14; Schlinkert, 2017, S. 224). Streng genommen werden hierbei auch keine Rechte an Daten übertragen, „vielmehr handelt es sich um eine schuldrechtliche Gestattung zur Nutzung der Daten“ (Roßnagel, 2017, S. 12).

Bei einer vertraglichen Zuweisung von Daten und hieran anknüpfender Nutzungsrechte, liegt das rechtliche Risiko zuvorderst bei dem Unternehmen, in dessen Vermögenssphäre die Daten erstmalig generiert werden (Sattler, 2017, S. 46). Um sich im interparteilichen Verhältnis klaren und rechtssicheren Regelungen zu nähern, sollte sich der betreffende faktische „Datenherrscher“ in einem ersten Schritt vergegenwärtigen, wo im Unternehmen welche Daten erfasst werden (siehe erste Ebene „Datenerzeugung“ in Abbildung 16). Anschliessend sollte die Kritikalität anfallender Daten hinsichtlich ihrer strategischen Nutzen- und Risikopotenziale bewertet werden, um letztendlich ableiten zu können, an welchen Schnittstellen welche Daten in welchem Zustand (roh, aggregiert, Datenbank) das Unternehmen verlassen dürfen und sollen (Sattler, 2017, S. 46). Eine nach diesen Fragen ausgerichtete Datenkartierung gibt Aufschluss über die erforderliche Intensität der vertraglichen Bindung etwaiger Partner.

Je nach Bedeutung identifizierter und bewerteter Daten(ströme) sollte dem betroffenen Unternehmen daran gelegen sein, den Umgang mit nicht personenbezogenen Daten entsprechend der festgestellten Kritikalität zu regeln. Einerseits können Regelungen über Daten in den betreffenden Leistungsverträgen der Partner (bspw. Softwarelizenz-, Projekt-, Wartungs- oder Pflegeverträge) aufgenommen bzw. herkömmliche Regelungen solcher Verträge um datenbezogene Aspekte ergänzt werden (Sattler, 2017, S. 48). Alternativ bietet sich die Vereinbarung eines gesonderten Datenlizenzvertrags an.

IT-Sicherheit

Unabhängig davon, in welcher Branche ein KMU angesiedelt ist, wird es sich mittlerweile sehr wahrscheinlich bedeutenden, punktuell sogar existenzgefährdenden Risiken ausgesetzt sehen, die sich in der einen oder anderen Weise auf den Einsatz von Informationstechnologie (IT) zurückführen lassen. Obwohl IT einerseits enorme Nutzenpotenziale für Unternehmen birgt, haben deutsche Unternehmen die Wichtigkeit hiermit verbundener Sicherheitsvorkehrungen erkannt, sei es antizipativ, reaktiv oder – leider – aufgrund der Realisierung entsprechender Risiken im eigenen Unternehmen. Erhebungen, wie die Erfassung der „Hightech-Themen 2018“ oder der „Markt für IT-Sicherheit“ des Bitkom, legen die Richtigkeit dieser These nahe. So wurde IT-Sicherheit in der Umfrage des Bitkom zu den wichtigssten Technologie- und Markttrends zum Topthema 2018 gewählt (Abbildung 17). Der deutsche Markt für IT-Sicherheit scheint diesen Trend mit einem Gesamtumsatzanstieg zwischen 2017 und 2019 (Prognose) in Höhe von 18,9 % (Abbildung 18) widerzuspiegeln.

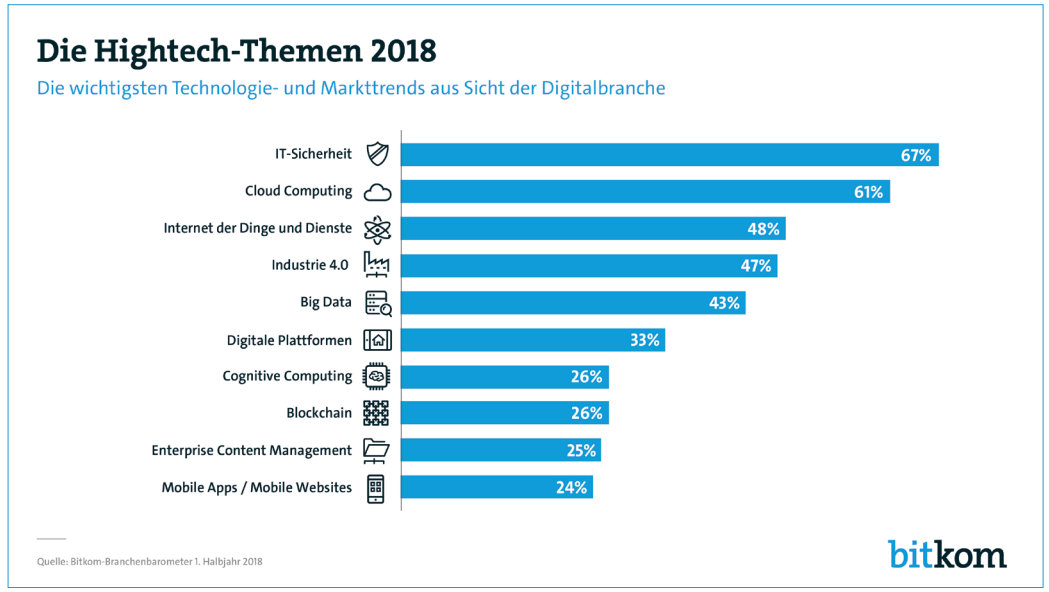

Abbildung 17: Die Hightech-Themen 2018 (Bitkom, 2018a)

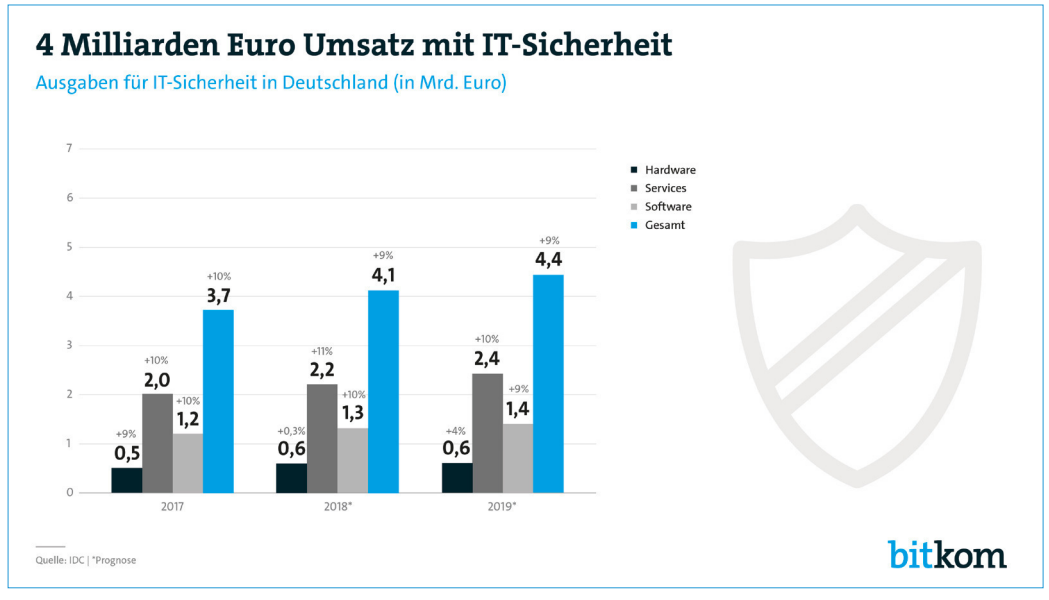

Abbildung 18: 4 Milliarden Euro Umsatz mit IT-Sicherheit (Bitkom, 2018b)