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.

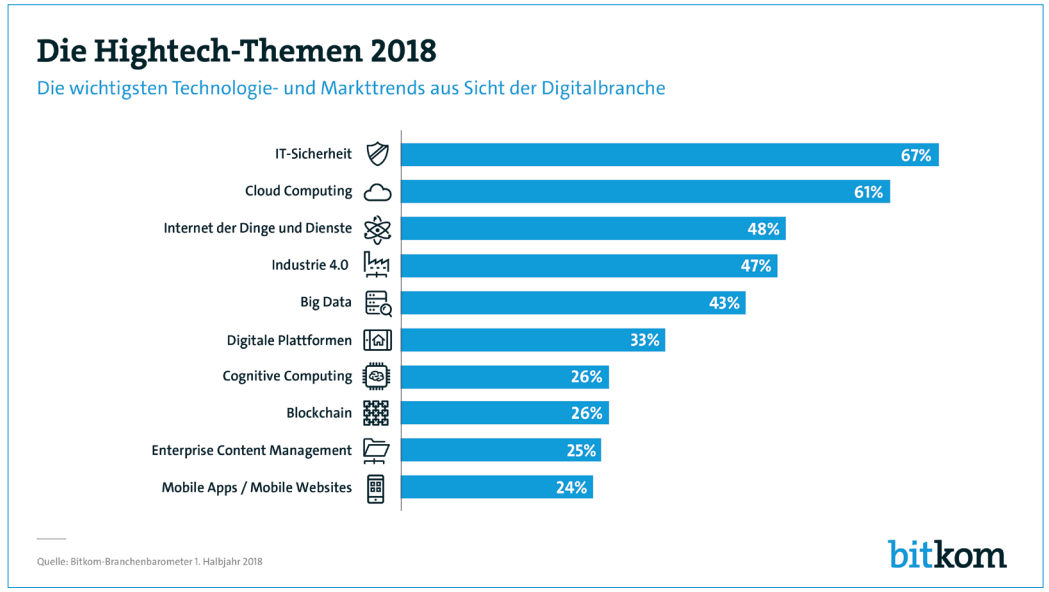

Abbildung 17: Die Hightech-Themen 2018 (Bitkom, 2018a)

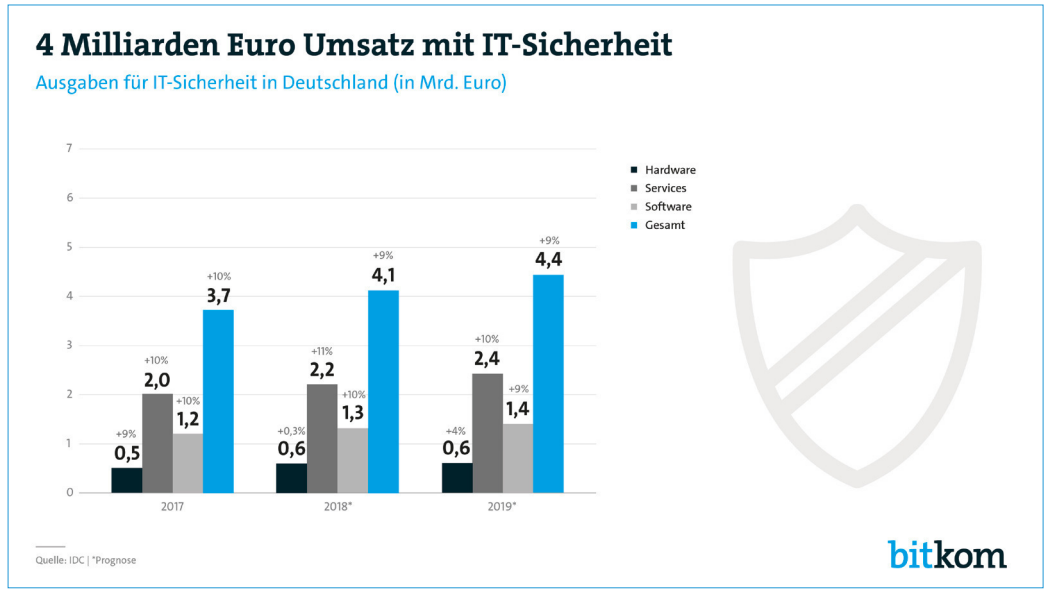

Abbildung 18: 4 Milliarden Euro Umsatz mit IT-Sicherheit (Bitkom, 2018b)

Die Frage, wer für die Implementierung von IT-Sicherheitsmassnahmen im Unternehmen verantwortlich ist, wird von Unternehmen unterschiedlich beantwortet. Während in Schweizer KMU anscheinend grösstenteils die Geschäftsführung das Thema IT-Sicherheit verantwortet (gfs. zürich Markt- und Sozialforschung, 2017, S. 8), trägt hierfür in deutschen Unternehmen überwiegend die hauseigene EDV-Abteilung oder aber ein externer Dienstleister Sorge (Deutsche Telekom / T-Systems, 2014, S. 17).

Ob und wieweit gesetzliche Verpflichtungen über die Implementierung von IT-Sicherheitsmassnahmen bestehen und durch wen diese ggf. wahrzunehmen sind, soll im Folgenden dargestellt werden.

1. Gesetzliche Grundlagen über IT-Sicherheit in den DACH-Staaten

Ein branchenübergreifendes „Gesetz zur IT-Sicherheit“ existiert als solches nicht (Voigt, 2018, S. 10). Der rechtliche Rahmen der IT-Sicherheit ergibt sich vielmehr aus der Summe unterschiedlicher Normen. Auf sektoraler Ebene sind dabei insbesondere die NIS-Richtlinie (RICHTLINIE (EU) 2016 / 1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union) und die entsprechenden Umsetzungsgesetze in Deutschland und Österreich zu berücksichtigen. Zudem gibt es speziell für Deutschland das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Unternehmen, die wichtige Infrastruktur- und Versorgungsleistungen erbringen, zur Einhaltung von Mindest-Sicherheitsstandards verpflichtet (Voigt, 2018, S. 10). Diese rechtlichen Mindestvorgaben beziehen sich zwar nur auf bestimmte Branchen, schaffen aber zumindest in ihrem Anwendungsbereich einen einheitlichen normativen Rahmen. Ausserhalb dieses Anwendungsbereichs ist das Pflichtenprogramm für Unternehmen aufgrund der bestehenden Rechtszersplitterung jedoch nur schwer zu erfassen (Voigt, 2018, S. 10). Auf Grundlage des vorhandenen Rechtsrahmens lassen sich die rechtlichen Anforderungen an die IT-Sicherheit grob wie folgt unterteilen:

(1) ordnungsrechtliche Anforderungen
(2) gesellschaftsrechtliche Anforderungen
(3) vertragsrechtliche Nebenpflichten
(4) IT-Sicherheit „by design“

1.1 Ordnungsrechtliche Anforderungen

Auf europäischer und nationaler Ebene haben die Gesetzgeber die Wichtigkeit hinreichender IT-Sicherheitsmassnahmen erkannt, weshalb auch eine erhöhte legislative Aktivität in diesem Bereich festzustellen ist. Besonders der europäische Gesetzgeber wird zunehmend aktiv, wie die im August 2016 in Kraft getretene NIS-Richtlinie sowie weitere legislative Bestrebungen zeigen (Europäische Kommission, 2018). Auch auf nationaler Ebene werden Unternehmen teils durch neue Gesetze immer stärker in die Pflicht genommen, IT-Massnahmen zu implementieren.

In Österreich wurde die NIS-Richtlinie mit Inkrafttreten des Netz- und Informationssystemsicherheitsgesetzes (NISG) am 29.12.2018 umgesetzt. In Deutschland wurde die NIS-Richtlinie bereits mit dem NIS-Umsetzungsgesetz vom 29.06.2017 umgesetzt, wobei man sich in einer günstigen Ausgangsposition sah, denn in Deutschland besteht mit dem IT-Sicherheitsgesetz seit Juli 2015 bereits ein einheitlicher Rechtsrahmen für mehr IT-Sicherheit bei Kritischen Infrastrukturen (KRITIS), der nur noch angepasst werden musste.

Auch wenn in der Schweiz Forderungen nach einem engmaschigeren normativen Rahmen zur IT-Sicherheit immer lauter werden (Mäder, 2018), findet sich hier bisher nur das „Bundesgesetz über die Informationssicherheit beim Bund“. Der Anwendungsbereich dieses Gesetzes ist indes nur auf Behörden und bestimmte Organisationen (die Parlamentsdienste, die Bundesverwaltung, die Verwaltungen der eidgenössischen Gerichte, die Armee, Organisationen nach Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes für ihre Verwaltungsaufgaben) begrenzt, private Unternehmen werden gerade nicht erfasst.

Im Ergebnis dürften ordnungsrechtliche Anforderungen, mit Ausnahme des Datenschutzrechts (siehe hierzu das Kapitel „Daten mit Personenbezug“), für KMU meist unerheblich sein, da in Deutschland und Österreich überwiegend kritische Infrastrukturen in den sachlichen Anwendungsbereich entsprechender Vorschriften fallen. Für kritische Infrastrukturen relevante Rechtsvorschriften können für KMU höchstens im Falle der Wahrnehmung einer Zuliefererfunktion für selbige relevant werden. Telemedien- und telekommunikationsrechtliche Vorschriften zur IT-Sicherheit dürften zwar nur ausnahmsweise einschlägig sein. KMU mit neuartigen Services und vernetzungsfähigen Produkten sollten in diesem Zusammenhang trotzdem prüfen, ob sie als Telemediendienste- oder Telekommunikationsanbieter gelten.

1.2 Pflicht zur IT-Sicherheit aus dem Gesellschaftsrecht

Neben Vorschriften, deren Inhalt sich spezifisch auf den Einsatz von Informationstechnologie stützt, können sich für die Geschäftsleitung eines Unternehmens Pflichten zur Implementierung von IT-Sicherheitsmassnahmen aus Leitungspflichten ergeben. In den Rechtsordnungen der DACH-Region finden sich ähnlich lautende Vorschriften, die der Geschäftsleitung – sei es dem Geschäftsführer einer GmbH oder dem Vorstand bzw. dem Verwaltungsrat einer AG – die Pflicht auferlegen, bei der Geschäftsführung die Sorgfalt eines ordentlichen Geschäftsmannes (GmbH) bzw. eines ordentlichen und gewissenhaften Geschäftsleiters (AG) anzuwenden und die Interessen der Gesellschaft zu wahren.[4] Die Pflichten der Geschäftsleitung ergeben sich dabei einerseits explizit aus gesellschaftsrechtlichen Vorschriften sowie den Statuten der Gesellschaft oder sind andererseits der originären Leitungsaufgabe immanent.

Unter die Pflicht zur sorgfältigen Unternehmensführung fällt nach wohl herrschender Meinung auch die Implementierung von IT-Sicherheitsmassnahmen, als Bestandteil der Organisationspflicht sowie der Pflicht, Schäden vom Unternehmen abzuwenden. Ähnlich der Pflicht zur Compliance, als Ausprägung der sog. Legalitätspflicht, steht der Geschäftsleitung lediglich ein Ermes-

[4] siehe für Deutschland: § 43 Abs. 1 GmbHG, § 93 Abs. 1 S. 1 AktG; Österreich: § 25 Abs. 1 GmbHG, § 84 Abs. 1 S.1 AktG; Schweiz: Artt. 717 Abs. 1, 812 Abs. 1 OR.

sensspielraum hinsichtlich des Umfangs zu implementierender IT-Sicherheitsmassnahmen zu, während das „Ob“ zumeist nicht dem „Business Judgment“ unterliegen dürfte.

1.3 Vertragsrechtliche Nebenpflichten

Selbst wenn Unternehmen Vertragsbeziehungen eingehen, deren jeweiliger Gegenstand keinen direkten Bezug zu IT-Sicherheit aufweist, können die Parteien im Rahmen der Erfüllung ihrer vertraglichen Nebenpflichten dazu gezwungen sein, IT-Sicherheitsmassnahmen vorzuhalten. Die Verpflichtung zur Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen der anderen Vertragspartei kann die Einhaltung einschlägiger gesetzlicher IT-Sicherheitspflichten auch zu einer vertraglichen Pflicht machen, „da den Vertragspartnern durch Zwischenfälle materielle oder immaterielle Schäden entstehen können“ (Voigt, 2018, S. 42). Vertragliche Nebenpflichten zur IT-Sicherheit sind umso bedeutsamer, je abhängiger eine Vertragspartei von den Leistungen und der Wirksamkeit dieser IT-Sicherheit des anderen Vertragspartners ist. Die entsprechenden risikobasierten Massnahmen sind jeweils für den konkreten Einzelfall zu bestimmen (Voigt, 2018, S. 42).

1.4 IT-Sicherheit „by design“

Aufgrund der Vernetzung von Zuliefererkomponenten, Herstellerprodukten sowie unternehmensinternen IT-Systemen werden die vernetzten Objekte selbst zu Quellen für IT-Sicherheitsrisiken (Rockstroh & Kunkel, 2017, S. 77). Von vernetzten Produkten ausgehende Sicherheitsrisiken bedrohen nicht nur Vermögenssphären, in welchen sich betreffenden Produkte letztendlich befinden, sondern alle hiermit sphärenübergreifenden vernetzten Systeme gleichermassen (Bundesamt für Sicherheit in der Informationstechnik, 2013, S. 10; Schlinkert, 2017, S. 222). Daher liegt auch die Vorhaltung produktbezogener IT-Sicherheitsmassnahmen im Interesse aller Wertschöpfungsakteure und Verbraucher.

Hersteller bzw. Verkäufer von IT-Produkten haften für IT-Schwachstellen zunächst regelmässig nach dem allgemeinen kaufrechtlichen Gewährleistungsrecht (Rockstroh & Kunkel, 2017, S. 77). Ein Produkt ist aus kaufrechtlicher Sicht frei von Sachmängeln, wenn es die zwischen den Vertragsparteien vereinbarte Beschaffenheit aufweist oder sich nicht für die gewöhnliche Verwendung eignet.[5] Aus diesem Grund sollten Hersteller und Verkäufer vernetzter Produkte die IT-sicherheitsrelevanten Eigenschaften möglichst umfassend und präzise beschreiben (Rockstroh & Kunkel, 2017, S. 77). Aus delikts-[6] und produkthaftungsrechtlicher Sicht können sich Herstellerpflichten u. a. aus technischen Standards wie IEC 62443 sowie aus den berechtigten Erwartungen der Kunden an die IT-Sicherheit des jeweiligen Produkts ergeben. Es ist dabei stets zu berücksichtigen, dass Software nicht fehlerfrei programmiert werden kann, sich die Bedrohungslagen immer schneller verändern und dass das erforderliche Mass an IT-Sicherheit nur durch Zusammenwirken aller Beteiligten erreicht werden kann (Rockstroh & Kunkel, 2017, S. 77).

[5] für Deutschland: § 434 BGB; für Österreich: § 922 ABGB; für die Schweiz: Art. 197 OR
[6] insbesondere Produzentenhaftung in Deutschland

Cyber-Physische Systeme

Der Begriff des Cyber-Physischen Systems (CPS) beschreibt ein Phänomen der digitalen Vernetzung und Automatisierung. Ein CPS besteht aus einer Vielzahl von Endgeräten, die in ein einheitliches, oft unternehmensübergreifendes Netzwerk integriert sind, in welchem sie miteinander kommunizieren und angesteuert werden können (Bundesministerium für Bildung und Forschung, 2015, S. 6). Ein typisches CPS ist beispielsweise eine digital integrierte, industrielle Wertschöpfungskette, deren Bestelloberflächen, Industrieroboter, Smart-Lager, Logistikroboter und sogar Endprodukte allesamt miteinander Daten austauschen und zentral angesteuert werden können. Wichtiges Merkmal eines CPS ist seine Fähigkeit, koordiniert und ohne menschliches Zutun auf Veränderungen in seiner Umwelt zu reagieren (Bruch, 2015, S. 87). So kann das beschriebene System bei einem Auftragseingang selbstständig Produktionsprozesse anstossen, die notwendigen Bauteile bestellen und Lagerraum freiräumen.

In der Praxis bieten diese Systeme potenziell beachtliche Effizienzvorteile. Sie verursachen aber technische Herausforderungen bei ihrer Implementierung und werfen eine Reihe von Rechtsfragen auf. Da sich diese Fragen vor allem mit der Haftung für eventuelle Fehler des Systems befassen, sind sie nicht nur für Nutzer von CPS relevant, sondern auch für deren Kunden und Geschäftspartner.

1. Vertragsrechtliche Implementierung eines CPS

Die Komplexität eines CPS spiegelt sich in den für eine Implementierung notwendigen vertraglichen Strukturen wider. Im Mittelpunkt steht das Verhältnis zwischen dem Betreiber und dem Hersteller bzw. Provider der CPS-Endgeräte. Da der Provider, neben der reinen Überlassung der Endgeräte, regelmässig auch eine Reihe von internetbasierten Diensten rund um deren Steuerung und Vernetzung erbringt, lässt sich das Betreiber-Provider-Verhältnis meist nur als typengemischter Vertrag zusammenfassen. Dieser kann wiederum, nach den Umständen des Einzelfalls, kauf-, miet-, dienst-, oder werkvertragliche Elemente enthalten (Heuer-James, Chibanguza & Stücker, 2018, S. 2823; Horner & Kaulartz, 2016, S. 24). Wird die Konnektivität der Endgeräte nicht durch die IT-Infrastruktur des Betreibers gewährleistet, so ist es regelmässig notwendig, hierzu zusätzlich einen Mobilfunkanbieter einzuschalten, welcher im Rahmen eines Dienstvertrages Datenvolumen zur Verfügung stellt (Langer, 2016, S. 29).

2. Zurechnung von Systemverhalten

Die Frage der Zurechnung des Verhaltens eines CPS zu einer Vertragspartei ist von grosser Bedeutung für die Praxis, jedoch rechtlich noch in weiten Teilen unklar. Grund hierfür ist die vermeintliche Autonomie eines CPS. Dieses besitzt freilich keinen eigenen Handlungswillen, vielmehr reagiert es auf Basis von Verknüpfungen und Algorithmen auf seine Umwelt. Dieser Entscheidungsfindungsprozess wird durch eine Vielzahl von Faktoren beeinflusst – hierzu zählen insbesondere die zur Steuerung verwendete Software,