Recklinghäuser Beiträge zu Recht und Wirtschaft

Westfälische Hochschule

ReWir

Nr. 29 / 2015

Fachbereich Wirtschaftsrecht

Hrsg. von Prof. Dr. Bernhard Bergmans und Prof. Dr. Ralf-Michael Marquardt

ISSN 2191-866X

Handlungsempfehlungen für KMU beim Einsatz von Cloud Technologien unter Berücksichtigung der Datensicherheit

Wirtschaftsjurist Patrick Król, LL.M.

Logos Verlag Berlin λογος

A. Einführung

1. Heranführung an die Problematik

In der Industrie und Wirtschaft ist das Thema „Cloud Computing“ nicht mehr als utopische Zukunftsvision anzusehen, sondern längst in der Informationstechnik (IT) angekommen.[1] Die Möglichkeit, im Internet auf IT-Infrastrukturen sowie Applikationen jederzeit zugreifen und je nach Bedarf des Anwenders nutzen zu können, stellt vereinfacht ausgedrückt das Cloud Computing dar.[2] Durch die Digitalisierung haben sich in nahezu allen Wertschöpfungsketten, ob nun im Produktions- oder Dienstleistungsbereich, neue Geschäftsmodelle bzw. -felder entwickelt[3], die dazu beigetragen haben, dass sich das Cloud Computing zu einem wesentlichen Faktor im Hinblick auf die ökonomische Entwicklung zur Industrie 4.0 und auch dem Internet der Dinge herauskristallisiert hat.

Trotz dieses Fortschritts treten einige Problemfelder auf. Zum einen herrscht keine Rechtssicherheit in Europa[4], und dies löst eine starke Verunsicherung bei Cloud-Anwendern aus, da sie die Verantwortung für ihre Daten und deren Verarbeitung tragen müssen[5]. Viele Cloud-Angebote stammen aus dem angelsächsischen Raum, in dem rechtliche Rahmenbedingungen und Vorstellungen im Vergleich zu Kontinentaleuropa in weiten Bereichen auseinander liegen, wodurch die Problematik noch verschärft wird.[6]

Zum anderen ist die Angst groß, die Kontrolle über unternehmensinterne Daten zu verlieren[7]. Hier besteht die Gefahr, enorme wirtschaftliche Schäden durch Cyberangriffe (Industriespionage, Preisgabe von Insiderinformationen, temporär fehlender Zugriff auf Daten bis hin zur permanenten Löschung von wichtigen Informationen)[8] zu erleiden. Auch die IT-Informationssicherheit mit dem Fokus auf Datenverschlüsselung stellt Cloud-Anwender als auch Cloud-Anbieter vor großen Herausforderungen. Eine erst kürzlich vorgestellte Studie des Frauenhofer-Instituts für sichere Informationstechnologie hat einige große Cloud-Anbieter auf ihre angebotenen Dienste hinsichtlich der Sicherheit untersucht und musste mit Bedauern feststellen, dass alle mit technischen Problemen zu kämpfen haben, die Cyberangriffe erst möglich machen.[9] Auch eine Umfrage der BITKOM hat ergeben, dass fast jedes dritte Unternehmen in den vergange-

---

1 *Baun et al.* (2011): Cloud Computing, S. 1; *Bräutigam/Thalhofer* (2013), in: *Bräutigam* (Hrsg) et al., IT-Outsourcing und Cloud Computing, Teil 14, S. 1274 Rdnr. 166.

2 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 2.

3 *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM)* (2014): IT-Strategie – Digitale Agenda für Deutschland, S. 11 und 18.

4 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. ix und 8; *Eriksdotter* (2011), Rechtsleit-faden für Cloud Computing.

5 *Frauenhofer-Institut für sichere Informationstechnologie (SIT)* (2012): Über die Sicherheit von Cloud-Speicherdiensten, Management Summary, S. 4.

6 *Ege* (2012): Von Wolken und Schattenwelten, S. 5.

7 *Frauenhofer SIT* (2012), Über die Sicherheit von Cloud-Speicherdiensten, Management Summary, S. 2; *Metzger et al.* (2011): Cloud Computing, S. 48.

8 *Metzger et al.* (2011): Cloud Computing, S. 57; *Rubin* (2002): Hackerabwehr und Datensicherheit, S. 34; *Müller* (2008): IT-Sicherheit mit System, S. 2 ff.

9 *Frauenhofer SIT* (2012): Über die Sicherheit von Cloud-Speicherdiensten, Management Summary, S. 2 f.

nen zwei Jahren Opfer eines Cyberangriffs geworden ist[10]. Es herrschen somit ausreichende nachvollziehbare Bedenken für den Einsatz von Cloud Computing-Lösungen.[11]

Darüber hinaus stellen sich insbesondere für KMU auch organisatorische Probleme, die es zu bewältigen gilt. Aufgrund ihrer Unternehmensgröße können sie sich keine eigenen Rechenzentren leisten, und da sie sich schließlich auf ihre Kernkompetenzen konzentrieren wollen, müssen sie auf externe Ressourcen zurückgreifen. Deshalb bleibt dem Management nichts anderes übrig, als sich der Datenflut im Netz zu stellen[12] und für ihr eigenes Unternehmen eine individuelle und geeignete Cloud-Strategie zu überlegen, die sie im Unternehmen transferieren und erfolgreich umsetzen, ohne dabei an Wettbewerbsfähigkeit zu verlieren. Dem Trend können sich KMU scheinbar nicht entziehen, besonders weil immer mehr strukturierte und unstrukturierte Daten (Big Data) aus internen und externen Quellen entstehen, die die Unterstützung von Datenmanagement-Lösungen und Serviceangeboten erforderlich machen. Sie müssen sich auf die aufgeworfenen Problemfelder einstellen und versuchen, sie in Zukunft zu vermeiden bzw. zu lösen.[13]

2. Ziel und Aufbau der Arbeit

Das Ziel dieser Arbeit ist, Handlungsempfehlungen, insbesondere für KMU, zu entwickeln, um eine sichere (technische als auch rechtliche) Nutzung von Cloud Computing zu gewährleisten. Es sollen Hilfestellungen in bestimmten Themengebieten wie Cloud-Strategien, Organisation, Vertragsrecht, Datenschutz und Datensicherheit geboten werden, die die Einführung und Nutzung von Cloud Computing vereinfacht bzw. sicherstellt. Auch ein Ausblick auf mögliche gesetzliche Änderungen soll aufgezeigt werden, auf die sich Nutzer als auch Anbieter von Cloud-Technologien einstellen können. Somit soll eine umfassende Sensibilisierung für KMU im Hinblick auf den Einsatz von Cloud-Technologien und dessen Potentiale und Gefahren erfolgen.

Zunächst wird eine kurze Einführung in das Thema Cloud Computing gegeben. In diesem Abschnitt B wird auch eine Risikoanalyse in den jeweiligen Themengebieten durchgeführt, die dazu dient, die grundlegenden Probleme zu identifizieren und zu untersuchen. Hiernach folgt ein Querschnitt des Cloud Computing im Mittelstand, um aufzuzeigen welche Potentiale vorhanden sind, die in Zukunft ausgeschöpft und genutzt werden können. Abschließend werden alle wesentlichen Punkte nochmal zusammengefasst und bewertet. Außerdem wird am Ende der Arbeit ein Ausblick auf die Zukunft gegeben, die die mögliche rechtliche als auch technische Entwicklung von Cloud-Technologien und der IT-Sicherheit skizziert.

---

[10] *BITKOM* Presseinformation (2014): Fast ein Drittel der Unternehmen verzeichnet Cyberangriffe.

[11] *Metzger et al.* (2011): Cloud Computing, S. 37 und 181; *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 175.

[12] *Wachter/Zaelke* (2014): Systemkonsolidierung und Datenmigration als geschäftskritische Erfolgsfaktoren, S. 143.

[13] *Vossen/Haselmann* (2012), Cloud Computing für Unternehmen, S. 7 f.

B. Einführung in das Cloud Computing

1. Kurzdarstellung von Cloud Computing

Für den Begriff „Cloud Computing“ gibt es keine einheitliche Definition[14]. Dies hängt wahrscheinlich stark damit zusammen, dass es sich derzeit noch im Wandel befindet[15]. Sinngemäß steht es jedoch für die „Datenverarbeitung in der Wolke“ und stellt grundsätzlich ein Netzwerk dar, das IT-Infrastrukturen, -Services und -Ressourcen bereitstellt,[16] das Kunden flexibel und skalierbar über das Internet nutzen können,[17] ohne dabei langfristige Kapitalbindungen einzugehen und spezifisches IT-Wissen zu besitzen[18]. Die Bereitstellung und gemeinsame Nutzung von Rechenkapazität, Datenspeicher, fertiger Software und Programmierumgebungen können als klassische Cloud-Dienste wahrgenommen werden[19]. Diese Definition orientiert sich an der allgemein akzeptierten und dynamischen Begriffsbestimmung des amerikanischen National Institute of Standards and Technology (NIST)[20]. Dabei zeichnet sich das Cloud Computing durch fünf wesentliche Eigenschaften aus:[21]

- Diensterbringung auf Anforderung (On-Demand Self-Service),
- Netzwerkbasierter Zugang (Broad Network Access),
- Ressourcen-Pooling (Resource Pooling),
- Schnelle Elastizität (Rapid Elasticity),
- Messbare Dienstqualität (Measured Service).

2. Cloud-Betriebsmodelle

Die Angebote für Cloud-Betriebsmodelle sind in den letzten Jahren enorm angestiegen, sodass sich viele neue Begriffe für Serviceleistungen entwickelt haben.

Alle Arten von Cloud-Services können jedoch unter dem Begriff „Everything-as-a-Service“ (XaaS) zusammengefasst werden. Hierunter kann nämlich jede denkbare IT-Ressource bzw. -Dienstleistung in Form eines Cloud-Dienstes erbracht werden[22]. Die Vielzahl der Begriffe trägt leider nicht dazu bei, dass ein besseres Verständnis für die Komplexität des Cloud Computing entsteht, selbst wenn sie nachvollziehbar erscheinen. Deshalb werden an dieser Stelle drei Hauptbegriffe angeführt, die dazu dienen, die Cloud-Dienste logisch zu trennen.[23] Eine Einteilung erfolgt anhand der Art der angebotenen Dienstleistungen[24], die sich auf Anwendungen, Plattformen für Anwen-

---

14 *Bräutigam/Thalhofer* (2013), in: *Bräutigam et al.*, IT-Outsourcing und Cloud Computing, Teil 14, S. 1194 Rdnr. 1.

15 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 19.

16 *Weichert* (2010), Cloud Computing und Datenschutz, S. 679; *Frauenhofer-Institut für Offene Kommunikationssysteme (FOKUS)* (2011): ISPRAT-Studie, S. 147 ff.

17 *Baun et al.* (2011): Cloud Computing, S. 4.

18 *Pröhl et al*. (2012): Servicemanagement im Cloud Computing, in: *Fröschle*, Cloud-Service-Management, S. 7.

19 *Metzger et al.* (2011): Cloud Computing, S. 2 und 11.

20 *Vossen/Haselmann* (2012), Cloud Computing für Unternehmen, S. 20.

21 *Baun et al.* (2011): Cloud Computing, S. 5 f.

22 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 15.

23 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 27 f.

24 *Frauenhofer FOKUS* (2010): ISPRAT-Studie, S. 16.

dungsentwicklungen und -betrieb sowie auf die Basisinfrastruktur beziehen[25]. Alle as-a-Service-Modelle bauen aufeinander auf bzw. sind aneinander gekoppelt, sodass eine Nutzung für nur ein Modell in der Praxis eher seltener vorkommt[26].

2.1 Software-as-a-Service (SaaS)

Bei diesem Cloud-Dienst besteht das Angebot auf Anwendungen, die ein Cloud-Anwender über die Server des Cloud-Anbieters nutzen kann[27]. Der Zugriff der Software erfolgt über das Internet[28]. Der Cloud-Anbieter ist verantwortlich für die Wartung, Aktualisierung, Fehlerbeseitigung, Weiterentwicklung oder Lizenzierung der benötigten Soft- und Hardware.[29] Der Cloud-Anwender kann lediglich auf die von ihm zu verarbeitenden Daten Einfluss nehmen, die er in die Software einarbeitet[30]. Die angebotenen Leistungen stellen Standardlösungen dar, sodass individuelle Anpassungen auf einen Kunden nur im geringen Umfang möglich sind.[31] Der Betrieb von Software-as-a-Service erfolgt aufbauend auf plattform- oder infrastruktur-orientierten Cloud-Angeboten[32].

2.2 Platform-as-a-Service (PaaS)

Dieser Cloud-Dienst richtet sich an Software-Entwickler[33], die ihre Anwendungen in sog. Entwicklungs- und Laufzeitumgebungen in einer bestimmten Programmiersprache entwickeln und ausführen[34]. Der Cloud-Anbieter stellt die Plattform-Software, die Entwicklungsumgebung sowie auch die Hardware zur Verfügung[35], die von ihm verwaltet wird. Somit legt er fest, welche Programmiersprache, verwendbaren Bibliotheken oder Schnittstellen angeboten werden.[36] An diese Rahmenbedingungen ist der Cloud-Nutzer gebunden[37].

---

[25] Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder; Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises (2014): Orientierungshilfe Cloud Computing, (Im Folgenden zitiert als: Orientierungshilfe Cloud Computing), S. 4.

[26] *Metzger et al.* (2011): Cloud Computing, S. 22.

[27] *Baun et al.* (2011): Cloud Computing, S. 37; *Spies/McCutchen* (2009): USA: Cloud Computing – Schwarze Löcher im Datenschutzrecht, S. XI; *Nägele/Jacobs* (2010): Rechtsfragen des Cloud Computing, S. 281; *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 804; Orientierungshilfe Cloud Computing, S. 8.

[28] *Metzger et al.* (2011): Cloud Computing, S. 36.

[29] *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 28; *ten Hompel/Heidenblut* (2011): Taschenlexikon Logistik, S. 287.

[30] *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 804.

[31] *Frauenhofer FOKUS* (2010), ISPRAT-Studie, S. 17.

[32] Orientierungshilfe - Cloud Computing, S. 8; *Stögmüller* (2013): Münchener Anwaltshandbuch IT-Recht, Teil 5 Rdnr. 330; *Pohle/Ammann* (2009): Über den Wolken… - Chancen und Risiken des Cloud Computing, S. 273; *Niemann/Paul* (2009): Bewölkt oder wolkenlos – rechtliche Herausforderung des Cloud Computings, S. 445; *Schuster/Reichl* (2010): Cloud Computing & SaaS: Was sind die wirklichen neuen Fragen?, S. 38.

[33] *Pröhl* et al. (2012): IT-Servicemanagement im Cloud Computing, S. 7.

[34] *Baun et al.* (2011): Cloud Computing, S. 35; *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 804; Orientierungshilfe Cloud Computing, S. 8.

[35] *Metzger, et al.* (2011): Cloud Computing, S. 21; *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 804; *Spies/McCutchen* (2009): USA: Cloud Computing – Schwarze Löcher im Datenschutzrecht S. XI.

[36] *Haselmann/Vossen* (2012): Database-as-a-Service für kleine und mittlere Unternehmen, S. 15.

[37] *Wind* (2012): Cloud Management mit Open-Source-Plattformen, S. 40.

2.3 Infrastructure-as-a-Service (IaaS)

Bei diesem Cloud-Dienst wird dem Cloud-Nutzer eine IT-Infrastruktur über das Internet zur Verfügung gestellt[38]. Es handelt sich hierbei um virtuelle Speicherkapazitäten, Rechenleistung oder Netzwerkbandbreite[39]. Hierbei wird die Dienstleistung deutlich abgegrenzt (Kapazität der Cloud gestaffelt) und klar geregelt[40]. Demnach ist die Nutzung der Ressourcen mit einer hohen Flexibilität verbunden[41].

3. Cloud-Architekturen

Die Cloud-Architektur wird an dieser Stelle aus organisatorischer Sicht betrachtet. Hierbei werden vier Arten an Modellen der Bereitstellung eines Dienstes beschrieben, wobei sich in Zukunft nur zwei von ihnen (Public Cloud und Community Cloud) als geeignete Modelle für KMU erweisen werden.[42]

3.1 Public Clouds

Eine „Public Cloud“ verfügt über einen öffentlichen Zugang, die in der Praxis am meisten genutzt wird.[43] Hier kann jeder die angebotenen Dienste über ein Web-Portal beziehen und muss nicht zur organisatorischen Einheit gehören.[44] Die genutzten Leistungen werden als Grundlage für die vertragliche Bindung genutzt, wobei ein übergeordneter Rahmenvertrag überflüssig wird. Es gibt außerdem noch zwei Unterformen der Public Cloud, die im Hinblick auf die Datensicherheit unterschieden werden müssen. Zum einen ist es die „Exclusive Cloud“, die deutlich mehr Sicherheit in einer Public Cloud bietet, da sich Cloud-Anbieter und Cloud-Anwender kennen. Hier wird in der Regel ein Vertrag zwischen den Parteien geschlossen, in denen die Dienstleistungen identifiziert und fixiert werden. Die „Open Cloud“ hingegen stellt das Gegenstück der „Exclusive Cloud“ dar. In diesem Fall kennen sich Cloud-Anbieter und Cloud-Anwender gerade nicht persönlich. Das Angebot wird ausschließlich durch den Cloud-Anbieter entwickelt, in denen die Leistung in Form von Service Level Agreements (SLAs) festgeschrieben wird.[45]

---

38 *Pröhl et al.* (2012): IT-Servicemanagement im Cloud Computing, S. 7.

39 *Baun et al.* (2011): Cloud Computing, S. 31; *Stögmüller* (2013): Münchener Anwaltshandbuch IT-Recht, Teil 5 Rdnr. 330; *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 803; Orientierungshilfe Cloud Computing, S. 8.; *Nägele/Jacobs* (2010): Rechtsfragen des Cloud Computing, S. 282.

40 *Metzger et al.* (2011): Cloud Computing, S. 21.

41 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 30.

42 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 30 und 31.

43 *Metzger et al.* (2011): Cloud Computing, S. 34; *Nägele/Jacobs* (2010): Rechtsfragen des Cloud Computing, S. 282; *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 803 f.; *Pohle/Ammann* (2009): Über den Wolken… - Chancen und Risiken des Cloud Computing, S. 274; Orientierungshilfe Cloud Computing, S. 7.

44 *Baun et al.* (2011): Cloud Computing, S. 27 f.

45 *Metzger et al.* (2011): Cloud Computing, S. 19; *Bräutigam/Thalhofer* (2013), in: *Bräutigam et al.*, IT-Outsourcing und Cloud Computing, Teil 14, S. 1202 Rdnr. 16.

3.2 Private Clouds

Eine „Private Cloud“ verfügt über einen nicht öffentlichen Zugang, die lediglich von großen Unternehmen genutzt wird.[46] Hierbei übernimmt die Verwaltung der Cloud entweder das Unternehmen selbst[47] oder ein externer Dienstleister. Das Rechenzentrum kann sich auf dem Gelände des Unternehmens befinden oder auch ausgelagert werden. Der Zugang zu der Cloud ist beschränkt auf die Mitglieder des Unternehmens.[48] Für die Wahl einer „Private Cloud“ werden meist Sicherheitsgründe erwähnt[49], da große Unternehmen über-wiegend eigene Ressourcen nutzen.[50] Die Kontrolle über die Daten hat die Organisation selbst und kann somit besser datenschutzrechtliche Rahmen-bedingungen für personenbezogene Daten einhalten oder unternehmensinterne Daten schützen.[51]

Es gibt aber auch die Möglichkeit eine sog. „Virtual Private Cloud“ zu schaffen. Hierbei wird ein Bereich in einer öffentlichen Cloud sinnvoll abgetrennt, sodass der Zugriff nur durch eine Organisation erfolgen kann. Die Trennung der Daten erfolgt ausschließlich auf Software-Ebene, sodass eine physische Trennung nicht gewährleistet werden kann. Dies macht deutlich, dass es sich gerade nicht um eine Private Cloud handelt, die den Schutz der Isolation bietet.[52]

3.3 Hybrid Clouds

Eine „Hybrid Cloud“ ist ein Zusammenschluss von einer Public Cloud und einer Private Cloud.[53] Hierbei werden bestimmte Dienste in die Public Cloud ausgelagert, da Ressourcenengpässe erreicht oder eine Verknüpfung erstellt werden soll, um den Austausch von Daten und Programmen zu ermöglichen.[54] Der Regelbetrieb erfolgt weiterhin über die Private Cloud.[55] Bei der Hybrid-lösung muss jedoch darauf geachtet werden, dass nur unkritische Funktionalitäten bzw. Daten ausgelagert werden dürfen.[56] Hybrid Clouds werden über-wiegend von großen Unternehmen genutzt.[57]

---

46 *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 804; *Pohle/Ammann* (2009): Über den Wolken… - Chancen und Risiken des Cloud Computing, S. 274; Orientierungshilfe Cloud Computing, S. 7.

47 *Stögmüller* (2013): Münchener Anwaltshandbuch IT-Recht, Teil 5 Rdnr. 333; *Nägele/Jacobs* (2010): Rechtsfragen des Cloud Computing, S. 282; *Niemann/Paul* (2009): Bewölkt oder wolkenlos – rechtliche Herausforderung des Cloud Computings, S. 445.

48 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 30.

49 *Schödwell et al.* (2014): Herausforderungen und Erfolgsfaktoren der Migration in eine Community Cloud für die öffentliche Verwaltung, S. 133.

50 *Baun et al.* (2011): Cloud Computing, S. 28.

51 *Metzger et al.* (2011): Cloud Computing, S. 33; *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 803 f.

52 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 31 f.; *Dettling/Eberhardt* (2011): Cloud Computing – IT-Dienste der nächsten Generation, S. 174.

53 Orientierungshilfe Cloud Computing (o. Fn. 36), S. 7; *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 804.

54 *Dettling/Eberhardt* (2011): Cloud Computing – IT-Dienste der nächsten Generation, S. 174; Orientierungshilfe Cloud Computing (o. Fn. 36), S. 7.

55 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 31 f.

56 *Baun et al.* (2011): Cloud Computing, S. 29.

57 *Metzger et al.* (2011): Cloud Computing, S. 34 f.

3.4 Community Clouds

Eine „Community Cloud“ stellt eine nicht öffentliche Cloud dar, wobei sich aber mehrere Organisationen mit ähnlichen Strukturen die Dienste teilen.[58] Die Verwaltung der Cloud übernehmen entweder die Organisationen selbst oder ein externer Dienstleister. Das Rechenzentrum befindet sich entweder bei einer der Organisationen oder bei einem externen Dienstleister. Die typischen Nutzer solcher Clouds sind KMU, die sich zwar eine Private Cloud wünschen, jedoch die Anforderungen aufgrund ihrer Größe nicht erfüllen können[59] und somit gezwungen sind auf die Dienste einer Community Cloud zurückzugreifen.[60] Besonders bei branchenspezifischen Anforderungen und der Einhaltung von gesetzlichen Bestimmungen sind solche Clouds sehr geeignet.[61]

C. Wirtschaftliche Bedeutung von Cloud Computing

1. Statistische Daten

Grundsätzlich gibt es ein ambivalentes Bild zum Thema Cloud Computing aufgrund von unterschiedlichen Prognosen und Einschätzungen. Auf der einen Seite stehen die positiven Marktwachstumschancen, die ein sehr hohes und stabiles Niveau prognostizieren[62] und auf der Gegenseite die große Skepsis im Hinblick auf die Gefahren und Risiken, die auf den Markt eher hemmend bzw. schädigend wirken. Es gibt somit zwei etwa gleichstarke Parteien, die Pro und Contra dem Cloud Computing gegenüberstehen.[63] Festzuhalten ist jedoch, dass trotz dieser gespaltenen Ansicht für die Zukunft des Cloud Computing gute Chancen auf dem Markt prognostiziert werden können. Dabei gehen die meisten Prognosen von einem weltweiten Durchschnittswachstum zwischen 30 % und 50 % pro Jahr aus.[64] In Deutschland sind ähnliche Wachstumsraten gegeben.

Der Cloud Vendor Benchmark 2014 der Experton Group liefert detaillierte Daten über die Investitionen und Ausgaben im Bereich Cloud Computing in Deutschland. Dieser Markt umfasst Cloud-Services, Cloud-Technologien sowie Dienstleistungen für Beratung und Integration. Hierbei wird für das Jahr 2015 ein Ausgaben- und Investitionsvolumen von 9,23 Mrd. Euro prognostiziert. Im Jahr 2013 waren es hingegen 4,52 Mrd. Euro. Dies stellt somit eine deutliche Verdoppelung dar. Außerdem werden deutsche Unternehmen laut der Prognose etwa neun Prozent ihrer IT-Ausgaben im Jahr 2015 in Cloud Computing investieren.[65] Ein ähnliches Bild liefert die Marktanalyse der International Data Corporation (IDC), die einen weltweiten Cloud-Markt von etwa 72,7 Mrd. US-Dollar für das Jahr 2015 prognostiziert. Im Jahr 2013 betrug das Volumen noch knapp 43 Mrd. US-Dollar und soll bis zum Jahr 2017 auf 106,7 Mrd. US-Dollar wach-

---

58 Orientierungshilfe Cloud Computing, S. 7.

59 *Schödwell et al.* (2014): Herausforderungen und Erfolgsfaktoren der Migration in eine Community Cloud für die öffentliche Verwaltung, S. 140.

60 *Vossen/Haselmann* (2012): Cloud Computing für Unternehmen, S. 31.

61 *Schödwell et al.* (2014): Herausforderungen und Erfolgsfaktoren der Migration in eine Community Cloud für die öffentliche Verwaltung, S. 133; *Heidrich/Wegener* (2010): Sichere Datenwolken, S. 804.

62 BITKOM Presseinformation (2014): Markt für Cloud Computing wächst ungebrochen.

63 BITKOM Research/KMPG (2015): Cloud-Monitor 2015, S. 6 f.

64 *ten Hompel et al.* (2013): Cloud Computing für Logistik 2, S. 29.

65 Presseportal (2014): 9,23 Mrd. Euro wird das Cloud Computing-Marktvolumen 2015 betragen.

sen. Hierbei umfasst der Markt bei dieser Studie lediglich die Cloud-Services.[66] Dabei wird auch für die nächsten Jahre ein anhaltendes Wachstum von durchschnittlich 35 % erwartet und somit in Deutschland ein Marktvolumen von etwa 19,8 Mrd. Euro schaffen.[67]

Deutsche Unternehmen sind unterschiedlich stark an Cloud-Services für Infrastruktur (IaaS), Plattformen (PaaS) und Software (SaaS) interessiert. In diesem Bereich werden die Investitionen am stärksten zunehmen. Zwar werden die Bereiche Integration und Beratung von Cloud Computing ebenfalls wachsen, aber im Vergleich zu den Cloud-Services deutlich geringer ausfallen. Besonders der Cloud-Service SaaS wird von den Unternehmen stark nachgefragt[68]. Bis Ende 2014 sollen in Deutschland etwa 2,5 Mrd. Euro in solche Cloud-Dienste in-vestiert werden, die Dreiviertel des Gesamtvolumens der Ausgaben für Cloud-Services im B2B-Bereich ausmachen. Die Ausgaben für SaaS sind derzeit noch sieben Mal größer als für IaaS[69]. Laut dem Marktforschungsunternehmen Gartner liegen weltweit die Investitionen im SaaS-Bereich bei etwa 23,72 Mrd. US-Dollar. Somit liegt der Fokus deutlich beim Service-Angebot im Softwarebereich.[70] Zu diesem Ergebnis kommt auch die Studie „IT-Cloud-Index“ der techconsult GmbH, die im Auftrag von HP Deutschland durchgeführt wurde. Hierbei stehen insb. Leistungen aus dem SaaS-Segment wie Office- und CRM-Lösungen als auch Email- und Collaboration-Dienste bei Unternehmen hoch im Kurs. Aber auch Security-Lösungen werden stetig interessanter, besonders aufgrund der Gefahr der Datensicherheit.[71]

Der ITK-Markt in Deutschland kann aufgrund der rasant entwickelnden Informationstechnologie weiterwachsen. Im Jahr 2015 wird der Umsatz mit Software, IT-Dienstleistungen und IT-Hardware um etwa 2,4 % auf 79,7 Mrd. Euro steigen. Dies geht aus einer aktuellen Prognose des European Information Technology Observatory (EITO) hervor. Dieses positive Wachstum ist verantwortlich für die Schaffung von 120.000 neuen Arbeitsplatzen in der IT und ein Abschwung ist nicht in Sicht. Am stärksten wächst hier der Bereich Software, das um etwa 5,5 % auf 20,2 Mrd. Euro zulegt. Auch der Umsatz mit IT-Dienstleistungen soll laut der Prognose um etwa drei Prozent auf 37,4 Mrd. Euro ansteigen. Nur der Bereich IT-Hardware wird im diesem Jahr abnehmen, obwohl das Jahr 2014 einen Anstieg von 5,8 % aufgrund von Ersatzinvesti-tionen (Supportende für Windows XP) verzeichnete.[72]

Das Statistische Bundesamt (Destatis) hat 2014 eine Erhebung durchgeführt und festgestellt, dass mittlerweile zwölf Prozent der Unternehmen in Deutschland Cloud Computing einsetzen. Die Nutzung hängt aber stark von der Unter-nehmensgröße ab. Hierbei greifen 27 % der großen Unternehmen mit 250 und mehr Beschäftigten auf solche Dienste zurück. Bei mittleren Unternehmen mit 50 bis 249 Beschäftigten sind es 16 % und bei kleinen Unternehmen mit zehn bis 49 Beschäftigten zehn Prozent. Am häufigs-

66 Matzer (2014): Der deutsche Cloud-Markt wächst, doch die Fertigungsindustrie hinkt hinterher.

67 BITKOM Presseinformation (2014): Markt für Cloud Computing wächst ungebrochen.

68 *BITKOM Research; KMPG* (2014): Cloud-Monitor 2015, S. 15.

69 Presseportal (2014): 9,23 Mrd. Euro wird das Cloud Computing-Marktvolumen 2015 betragen.

70 *Matzer* (2014): Der deutsche Cloud-Markt wächst, doch die Fertigungsindustrie hinkt hinterher.

71 *Techconsult GmbH/Hewlett-Packard GmbH* (2013): IT-Cloud-Index, Q4/2012; *BITKOM Research/KMPG* (2014): Cloud-Monitor 2015, S. 16.

72 BITKOM Presseinformation (2014): Deutscher IT-Markt wächst 2015 um 2,4 %.

ten wurde das Cloud Computing zur Speicherung von Daten (56 %), für E-Mails (46 %) und zum Betrieb von Unternehmensdatenbanken (34 %) genutzt.[73]

In Europa setzt sich das Cloud Computing eher langsam durch. Der EU28-Durchschnitt liegt bei etwa 19 %, sodass fast jedes fünfte Unternehmen in Europa auf Cloud-Dienste zurückgreift. Hierbei werden nur Unternehmen mit zehn oder mehr Beschäftigten gezählt. In Deutschland sind es hingegen nur elf Prozent, das damit zu begründen ist, dass unzureichende Kenntnisse vorhanden sind, die den Einsatz von Cloud-Diensten erheblich behindern. Hierbei sind insb. Sicherheits- und Rechtsfragen zu nennen, die den Unternehmen Un-sicherheiten bereiten. Im Gegensatz zu Deutschland ist bspw. Finnland mit 51 % deutlich aufgeschlossener beim Einsatz von Cloud Computing-Diensten. Dort nutzen nämlich die Hälfte aller Unternehmen solche Dienste.[74]

Die Europäische Kommission ließ schon 2012 verlauten, dass sich das EU-Bruttoinlandsprodukt (BIP) mithilfe von Cloud Computing bis 2020 jährlich um 160 Mrd. Euro steigern lässt und auch neue Arbeitsplätze schaffen kann.[75] Mit der Unterstützung der Politik könnte der BIP-Beitrag sogar deutlich höher ausfallen. Hierfür müssten alle Rechtsunsicherheiten beseitigt werden, indem eine einheitliche Modernisierung der rechtlichen Rahmenbedingungen für das Cloud Computing umgesetzt wird. Außerdem wäre der Ausbau der Breitbandinfrastruktur eine weitere sinnvolle Maßnahme, denn ohne diese stößt Cloud Computing schnell an seine Grenzen und kann sein umfassendes Potenzial gar nicht erst entfalten.

2. Grundhaltung zum Cloud Computing

Die Grundhaltung von Unternehmen zum Cloud Computing hat sich in den letzten Jahren enorm verändert. Als noch im Jahr 2011 lediglich 28 % der befragten Unternehmen dem Thema aufgeschlossen gegenüberstanden, waren es im Jahr 2012 bereits 35 %. Im Jahr 2013 stieg sie weiter um vier Prozent an. Im darauffolgenden Jahr erreichte sie den Wert von 40 %[76]. Die Tendenz ist steigend und ist sicherlich damit zu begründen, dass eine bessere Informationspolitik herrscht, die die Unsicherheiten der Unternehmen deutlich verringert. Die Zahl der Skeptiker hingegen lag im Jahr 2011 bei 38 % und stieg im darauffolgenden Jahr auf 44 %. Im Jahr 2013 erreichte sie den Wert von 39 % und sank weiter, sodass sie im Jahr 2014 auf 35 % fiel. Im Hinblick auf die NSA-Affäre kann sicherlich eine Erklärung für die bleibende Skepsis bzgl. des Cloud Computing gegeben werden[77]. Trotzdem bleibt bei steigender Tendenz der aufgeschlossenen Unternehmen die Mehrheit unentschlossen bis gar kritisch gegenüber einem Einsatz von Cloud Computing. Positiv ist jedoch, dass die Zahl der unentschlossenen Unternehmen von 33 % auf 22 % gesunken ist.[78] Gerade weil das Thema nicht nur bei großen Unternehmen, sondern auch bei KMU auf enormes Interesse stößt, ist es nicht verwunderlich, dass auch diese Stellung beziehen müssen und somit nicht mehr zum Kreis der Unentschlossenen gehören. Hierbei spielt aber insb. die Größe des Unternehmens eine zentrale Rolle für den Einsatz von Cloud Computing. Besonders der

---

[73] Statistisches Bundesamt Pressemitteilung (2014): 12 % der Unternehmen setzen auf Cloud Computing; Statistisches Bundesamt (2014): Nutzung von Informations- und Kommunikationstechnologien in Unternehmen, S. 7 und S. 11-13.

[74] Eurostat Pressemitteilung (2014): Nutzung von IKT in Unternehmen im Jahr 2014.

[75] *Europäische Kommission* (2012): Mehr Schwung für das Cloud Computing.

[76] *BITKOM Research; KMPG* (2015): Cloud-Monitor 2015, S. 7.

[77] *BITKOM Research; KMPG* (2015): Cloud-Monitor 2015, S. 29.

[78] *BITKOM Research; KMPG* (2015): Cloud-Monitor 2015, S. 7.

Mittelstand hat eine Kehrtwende gemacht und ist beim Einsatz von Cloud-Technologien ebenso aufgeschlossen wie große Unternehmen (alle jeweils mit 51 % im Jahr 2013). Nur kleine Unternehmen stehen dem Cloud Computing noch skeptisch gegenüber (36 % im Jahr 2013).[79]

Grundsätzlich hat sich das Bild zum Cloud Computing zum Jahr 2010 bis heute deutlich verbessert. Die Nutzer solcher Dienste sind nämlich mit dem Umgang viel sicherer geworden. Dies bestätigt auch eine Studie des Wirtschaftsprüfungs- und Beratungsunternehmens PricewaterhouseCoopers (PwC). Dort wurden 60 Anbieter auf dem deutschen Cloud Computing-Markt befragt. Der Grund für diese Entwicklung ist, dass der Markt deutlich reifer und differenzierter geworden sei und Nutzer somit bessere Chancen haben eine geeignete Lösung für ihr Unternehmen zu finden.[80]

Die Planung für die Implementierung von Cloud-Technologien in Unternehmen ist gespalten. Für etwa ein Drittel ist Cloud Computing kein Thema. Dagegen planen bzw. diskutieren 24 % den Einsatz.[81] Die Studie „Cloud Computing im Mittelstand“ der TecChannel-Redaktion hat ebenfalls eine Befragung durchgeführt und kommt auf ähnliche Ergebnisse. Hierbei plant jedes fünfte Unternehmen den Einsatz von Cloud-Technologien im Unternehmen und etwa 42 % sehen keinen Bedarf.[82]

Als noch zu Beginn des Cloud Computing die Kostenreduzierung und Flexibilität von Abrechnungsmodellen im Vordergrund stand, hat sich die Tendenz aktuell in eine andere Richtung entwickelt. Jetzt sind Datensicherheit (96 %), Verfügbarkeit (97 %) und Performance (93 %) umso wichtiger für die Kundenzufriedenheit geworden.[83] Diese sind einer der wichtigsten Kriterien für die Wahl eines Cloud-Anbieters.

Laut der Studie „Global Technology Adoption Index (GTAI)“ in der weltweit mehr als 2.000 Unternehmen befragt wurden, gibt es eine starke Korrelation zwischen Cloud-Nutzung und dem Unternehmenswachstum. 72 % der Unternehmen, die auf Cloud-Dienste zurückgreifen, erreichen sechs Prozent oder mehr Wachstum in den letzten drei Jahren. Dabei hatten nur vier Prozent der Unternehmen kein oder ein negatives Wachstum. Dagegen haben 24 % der Unternehmen, die nicht auf Cloud-Dienste zurückgreifen, ein Wachstum von sechs Prozent oder mehr, während 37 % kein oder ein negatives Wachstum in den letzten drei Jahren verzeichneten. Die Vorteile von Cloud Computing kommen stärker zum Tragen, wenn sich Unternehmen für mehr als eine Art von Cloud-Lösung entscheiden. Die drei am häufigsten realisierten Vorteile des Cloud Computing sind eine bessere IT-Ressourcen Verteilung (44 %), Kosteneinsparungen (42 %) und höhere Effizienz (40 %).[84]

3. Der Einsatz von Cloud Computing in Unternehmen

Anhand der Umfrage „Cloud-Monitor 2015“ der BITKOM, die im Auftrag der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG durchgeführt wurde, sind vor allem Unternehmen aus den Branchen Informations- und Telekommunikation, Automobilbau, Verkehr und Logistik sowie Finanzen (Banken und Versicherungen) dem Thema Cloud Computing sehr aufgeschlossen. Deutlich dahinter liegen die Unternehmen aus den

---

79 *BITKOM Research; KMPG* (2014): Cloud-Monitor 2014, S. 7 f.

80 *PricewaterhouseCoopers (PwC)* (2013): Cloud Computing – Evolution in der Wolke, S. 29.

81 *BITKOM Research, KMPG* (2015): Cloud-Monitor 2015, S. 8.

82 *Herrmann* (2014): Cloud Computing – der deutsche Mittelstand hinkt hinterher.

83 *PwC* (2013): Cloud Computing – Evolution in der Wolke, S. 26.

84 Dell Pressemitteilung (2014): Dell-Studie: Die Wahrheit über Sicherheit, Cloud, Mobility und Big Data.

Branchen Chemie- und Pharma-industrie, Handel, Maschinen- und Anlagenbau sowie sonstige Branchen (ohne öffentliche Verwaltung).[85] Es fällt auf, dass der Unterschied zwischen den einzelnen Branchen bzgl. des Einsatzes von Cloud-Technologien immer geringer wird. Gerade die IT- und Telekommunikationsbranche sticht mit 71 % hervor. Besonders in den Bereichen Chemie- und Pharmaindustrie, Maschinen- und Anlagenbau, Handel sowie den sonstigen Branchen (ohne öffentliche Verwaltung) besteht noch Nachholbedarf. Hier sind die Werte unter 50 %. Trotzdem ist das Nutzungsbild von Cloud-Technologien in den jeweiligen Branchen weitestgehend gut.[86]

Die Cloud-Nutzung der Unternehmen hat sich im Vergleich zu den Vorjahren moderat entwickelt. Die meisten Unternehmen entscheiden sich für eine „Private Cloud" (39 %).[87]

Obwohl alle Branchen aufgrund von diversen Skandalen (NSA-Affäre) mit schmälernden Wachstumszahlen zu kämpfen haben, bleibt das Interesse für Cloud-Technologien weiterhin hoch. Besonders der Mittelstand hat in Sachen Cloud Computing aufgeholt. Trotzdem bevorzugt dieser eher Private Cloud-Lösungen. Großunternehmen mit mehr als 2.000 Beschäftigten haben weiterhin in beiden Bereichen die höchsten Werte zu verzeichnen. Nur kleine Unternehmen mit weniger als 100 Beschäftigten sind dem Thema Cloud Computing immer noch nicht wirklich näher gekommen. Hier bleibt die Meinung weiterhin unverändert.

KMU sind weltweit entscheidende Wachstumstreiber für die Wirtschaft und Schaffung von Arbeitsplätzen. Die Boston Consulting Group (BCG) hat in der Studie „Der Zeit voraus" KMU hinsichtlich des Einflusses neuer Technologien auf den Erfolg untersucht. Hierbei konnte festgestellt werden, dass der effektive Einsatz neuer Informationstechnologien durch KMU ein wichtiger Bestandteil des Gesamterfolgs sei.[88] Für Deutschland wurde die Prognose aufgestellt, dass durch die Förderung des Einsatzes von Cloud-Technologien in KMU ein zusätzliches Umsatzpotenzial von etwa 150 Mrd. US-Dollar erreicht werden könnte. Darüber hinaus könnten 670.000 neue Arbeitsplätze geschaffen werden. Dies stellt ein enormes Wachstum dar, das nicht unberücksichtigt bleiben darf.[89] Hierbei erschweren jedoch zahlreiche Barrieren den Einsatz solcher Technologien[90].

4. Öffentliche Wahrnehmung in Europa

In Europa ist die Wahrnehmung von Cloud Computing noch sehr gespalten. Größte Bedenken scheinen immer noch die Auslagerung von Daten und der damit verbundene Kontrollverlust auszulösen. Es bestehen somit weiterhin große Sicherheitsbedenken beim Speichern von Daten in der Cloud.[91] In der EU28 liegt der Durchschnitt für die Nutzung von Online-Speicherdiensten im privaten Bereich im Alter von 16 und 74 Jahren bei 21 %. In Deutschland sind es ebenfalls 21 %, wobei in Dänemark mit 42 %, dem Vereinigten Königreich mit 38 %, Luxemburg und Schweden mit jeweils 35 % und den Niederlanden mit 34 % solche Dienste am häufigsten genutzt werden. In Litauen, Polen und Rumänien liegt der Schnitt jeweils bei acht Prozent, sodass diese das

[85] *BITKOM Research; KMPG* (2015): Cloud-Monitor 2015, S. 10.

[86] *BITKOM Research; KMPG* (2015): Cloud-Monitor 2015, S. 10.

[87] *BITKOM Research; KMPG* (2015): Cloud-Monitor 2015, S. 8.

[88] *Boston Consulting Group (BCG*) (2013): Der Zeit voraus, S. 16.

[89] *BCG* (2013): Der Zeit voraus, S. 17 und S. 33.

[90] *BCG* (2013): Der Zeit voraus, S. 18.

[91] *ten Hompel et al.* (2013): Cloud Computing für die Logistik 2, S. 36.

Schlusslicht in Europa darstellen.[92] Einen richtigen Durchbruch konnte das Cloud Computing leider noch nicht erfahren. Dennoch ist festzuhalten, dass es ein wichtiger Bestandteil der heutigen Gesellschaft und Wirtschaft geworden ist und in Zukunft sicherlich noch für viele neue Entwicklungen und Innovationen sorgen wird. Dafür müssen aber die Problemfelder, die schon bekannt sind, beseitigt werden. Die Europäische Union arbeitet bereits seit mehreren Jahren an einer EU-Datenschutzreform, um die unbedenkliche Nutzung in Europa zu gewährleisten.[93]

5. Problemfelder des Cloud Computing

Gegenwärtig gibt es immer noch genügend Problemfelder, die den Einsatz von Cloud-Technologien verhindern bzw. erschweren. Das Statistische Bundesamt liefert aufgrund einer Erhebung zahlreiche Gründe für die Nichtnutzung von Cloud Computing. Die meisten Unternehmen sehen die Sicherheitsbedenken mit 37 % als Kernproblem. Des Weiteren sind Unsicherheiten bzgl. geltendem Recht und rechtlicher Zuständigkeit (32 %) und die Unsicherheit bzgl. des Standorts der Daten (31 %) ebenfalls Gründe für die Nichtnutzung. Auch unzureichende Kenntnisse von Cloud Computing (27 %) und hohe Kosten für Cloud-Services (22 %) werden ebenfalls als Begründung genannt.[94]

5.1 Unzureichende Ressourcenausschöpfung

Da das Cloud Computing bislang noch nicht seine versprochenen Vorteile in vollem Umfang ausschöpfen konnte und der Markt sicherlich noch am Anfang steht, ist dies ein gegenwärtiges Problem, das in Zukunft gelöst werden sollte, um potentielle Nutzer von der Cloud-Lösung zu überzeugen. Die Studie „Avoiding the hidden costs of cloud 2013“ vom Softwareanbieter Symantec GmbH kommt zu diesem Schluss. Besonders problematisch ist hierbei die Nutzung von Cloud-Diensten durch Fachabteilungen ohne Absprache mit der eigenen IT-Abteilung. Dies führt logischerweise zu einem Durcheinander, das vielmehr höhere statt einsparende Kosten verursacht. Außerdem werden Unternehmensdaten unnötig einem Risiko ausgesetzt.[95] Auch die kuriosen Backup- und Recovery-Strategien lassen die gewünschten Kostensenkungs-potenziale verpuffen. Hier werden teilweise mehrere und parallele Lösungen genutzt, die sicherlich nicht zielführend sind.[96] Ebenso kommen die ineffizienten Nutzungsraten von Cloud-Speichersystemen hinzu. Während bei stationären Lösungen eine ideale Auslastung bei etwa 50 % liegt, werden Cloud-Speicher weltweit nur zu 17 % genutzt. In Deutschland liegt der Wert bei 26 % und somit im weltweiten Vergleich etwas höher. Werden hierbei jedoch ausschließlich KMU betrachtet, so lässt sich eine geringe Quote von sieben Prozent feststellen. Somit zahlen KMU für über 90 % ungenutzte Dienste.[97]

Auch das Thema Green-IT, also Energieeinsparungsmöglichkeiten bei der Auslastung der Server, verwirklicht noch nicht die angestrebten Ziele. Weit unter 20 % beträgt die tatsächliche Auslastung der Server. Der restliche Anteil befindet sich im Leerlaufbe-

---

92 Eurostat Pressemitteilung (2014): Internetnutzung von Personen im Jahr 2014.

93 Europäische Kommission Pressemitteilung (2012): Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern.

94 *Statistisches Bundesamt* (2014): Nutzung von Informations- und Kommunikationstechnologien in Unternehmen, S. 7 und S. 13.

95 *Symantec* (2013): Avoiding the hidden costs of cloud 2013, S. 5.

96 *Symantec* (2013): Avoiding the hidden costs of cloud 2013, S. 6.

97 *Symantec* (2013): Avoiding the hidden costs of cloud 2013, S. 7.

trieb. Dies besagt eine Studie von McKinsey & Company.[98] Den Unternehmen fehlen die jeweiligen Anreize, um in energie-effiziente IT-Infrastrukturen zu investieren. Auch der relativ preiswerte Strompreis bewegt Unternehmen noch nicht dazu, ihre Strategie der Green-IT anzupassen. Zwar gibt es einige große Unternehmen wie Apple, Google und Facebook, die sich bemühen energieeffiziente Rechenzentren zu betreiben,[99] aber dies reicht natürlich noch nicht aus, gerade weil durch das Cloud Computing die Anzahl der Rechenzentren und somit auch der Energiebedarf in Zukunft steigen werden.

Die von Rittal, ein deutscher Systemanbieter für Gehäuse- und Schaltschranktechnik, in Auftrag gegebene IDC-Studie „Wachstumsmotor IT: So fördern effiziente Rechenzentren das Unternehmenswachstum“ verdeutlicht die aktuell schlechte Lage der Energieeffizienz in mittelständischen Data Centern. Grund dafür sind die veralteten Serveranlagen. Die Komponenten eines Rechenzentrums sollten grundsätzlich alle zwei bis vier Jahre erneuert werden, um von den technischen Weiterentwicklungen und Energieeinsparungsmöglichkeiten profitieren zu können. Der Studie zufolge liegt das durchschnittliche Alter von mittelständischen Data Centern bei etwa sieben Jahren und somit weit über den Empfehlungen. Auch bei der Kühlung werden enorme Mengen an Energien verschwendet (Raum- anstatt Serverkühlung). KMU werden sicherlich in Zukunft beim Thema Green IT keinen Bogen mehr machen können. Trotzdem bleiben Faktoren wie hohe Verfügbarkeit, Systemmanagement und Mitarbeiterqualifikation weiter vorne.[100]

5.2 Fehlende bzw. unzureichende Informationstransparenz

Die Anzahl an Cloud-Anbietern sowohl national als auch international ist recht überschaubar, die Auswahl hingegen relativ schwierig. Dies ist damit zu begründen, dass die jeweiligen Angebote sehr intransparent sind. Auch die unzureichenden eigenen Kenntnisse im Bereich des Cloud Computing erschweren die Auswahl für einen Dienst umso mehr[101]. Bei einer Umfrage der SAGE Gruppe, der führender Anbieter von betriebswirtschaftlicher Software für KMU weltweit ist, wurde festgestellt, dass 23 % der Unternehmen, die sich gegen den Einsatz von Cloud Computing aussprachen, ein intern fehlendes Verständnis für die Vorteile besitzen[102].

5.3 Service Level Agreements (SLAs)

Service Level Agreements (SLAs) sind Leistungsscheine, die auch konkrete Qualitätsanforderungen an den jeweiligen Cloud-Service enthalten. In diesen sollten der Inhalt und die Besonderheiten des Cloud-Services beschrieben werden.[103] Hierbei dienen als Parameter für die Messung der Qualität der Cloud-Leistungen die Verfügbarkeit,

---

98 *Glanz* (2012): The Cloud Factories, Power, Pollution and the Internet.

99 *Greenpeace* (2014): Clicking Green: How Companies are creating the Green Internet.

100 *Ritall* (2014): Whitepaper von IDC und Rittal: Rechenzentren werden immer mehr zum Wettbewerbsfaktor.

101 *Statistisches Bundesamt* (2014): Nutzung von Informations- und Kommunikationstechnologien in Unternehmen, S. 7 und S. 13.

102 Sage Pressemitteilung (2014): Sage-Studie: Deutsche Unternehmer schöpfen Potenzial der Cloud noch nicht aus.

103 *Intveen/Hilber/Rabus* (2014), in: *Hilber*, Handbuch Cloud Computing, Teil 2 S. 190 Rz. 201.

Reaktions- und Entstörzeiten im Falle von Störungen oder Performance- und Antwortzeiten einer bestimmten Software[104].

Laut der Studie „Die Kontrolle über Ihre Cloud Apps zurückgewinnen: Welche SLAs bieten Ihnen wirklich Schutz“, die im Auftrag von Compuware von den Marktforschern Research in Motion (RIM) erstellt wurde, glauben 79 % der befragten Unternehmen, dass die angebotenen SLAs von Cloud-Service-Anbietern zu einfach gehalten sind. Aufgrund dessen befürchten 75 % der Unternehmen, dass Cloud-Service-Anbieter Probleme auf Infrastruktur- oder Plattformebene verheimlichen, von denen die Leistung ihrer Anwendung beeinträchtigt werden könnte. Die Unternehmen wünschen sich daher deutlich mehr Transparenz und Kontrolle, um den Einsatz von Cloud-Technologien zu gewährleisten.[105] Gerade bei unzureichenden Leistungsbeschreibungen erweisen sich die Ableitung und Durchsetzung eines vertraglichen Anspruchs auf Schlechtleistung als schwierig[106].

Aktuell gibt es keine allgemeingültigen Standards von SLAs. Besonders schwierig ist es solche zu entwickeln, die im gesamten EU-Wirtschaftsraum rechtskonform sind. Da Cloud Computing einen globalen Charakter aufweist, unterliegen die Verträge unterschiedlichen Rechtsordnungen. Somit sind auch die rechtlichen Anforderungen, insb. im Hinblick auf den Schutz personenbezogener Daten, die in der Cloud gespeichert werden, unterschiedlich. Die Komplexität der Verträge steigt, sodass potentielle Cloud-Nutzer, insb. KMU, eher abgeneigt sind Cloud-Technologien im Unternehmen einzusetzen. Auch ist die Verwendung von unbestimmten Rechtsbegriffen problematisch, da hier hoher Interpretationsgehalt besteht, der zu Konflikten führen kann[107]. Trotzdem gibt es bereits Bemühungen auf europäischer Ebene Leitlinien für Unternehmen anzubieten, die als Orientierung dienen und Sicherheit im Rechtsverkehr schaffen sollen. Die Europäische Kommission hat im Zuge der Europäischen Cloud-Strategie den Auftrag der Cloud Select Industry Group erteilt, Leitlinien zu entwickeln, die das Vertrauen in Cloud-Dienste erhöhen soll. Insbesondere sollen kleine Unternehmen davon profitieren. In diesen Leitlinien sollen alle wesentlichen Punkte einfach formuliert sein. Die EU-Kommission sieht die Verfügbarkeit und Zuverlässigkeit des Cloud-Dienstes, die Qualität von Unterstützungsdiensten, die der Cloud-Anbieter bereitstellt, die Sicherheitsniveaus und wie die in der Cloud gespeicherten Daten besser verwaltet werden können, als die wichtigsten Punkte an, die klar geregelt werden sollten. Diese Entwicklung ist ein guter Weg in Richtung standardisierte SLAs.[108]

Weitere Maßnahmen zur Standardisierung von SLAs z. B. durch internationale Normen wie ISO/IEC 19086, könnten erheblich dazu beitragen, dass weltweit eine konforme Regelung bestehe. Daher wird die Cloud Select Industry Group zusammen mit der ISO-Arbeitsgruppe für Cloud Computing arbeiten, um einen gemeinsamen europäischen Lösungsansatz zu entwickeln. Diese könnten somit bei Überlegungen zu internationalen SLA-Standards herangezogen werden.[109] Das Europäische Institut für Tele-

---

[104] *Intveen/Hilber/Rabus* (2014), in: Hilber, Handbuch Cloud Computing, Teil 2 S. 191 f. Rz. 202.

[105] *Research in Motion (RIM)* (2013): Die Kontrolle über ihre Cloud Apps zurückgewinnen: Welche SLAs bieten ihnen wirklich Schutz, S. 3 und S. 6.

[106] *Bräutigam/Thalhofer* (2013), in: *Bräutigam et al.*, IT-Outsourcing und Cloud Computing, Teil 14, S. 1269 Rdnr. 145.

[107] *Intveen/Hilber/Rabus* (2014), in: Hilber, Handbuch Cloud Computing, Teil 2 S. 194 Rz. 212.

[108] Europäische Kommission Pressemitteilung (2014): Neue Leitlinien für EU-Unternehmen bei der Nutzung der Cloud.

[109] Europäische Kommission Pressemitteilung (2014): Neue Leitlinien für EU-Unternehmen bei der Nutzung der Cloud.

kommunikationsnormen (ETSI) und EuroCloud Europe arbeiten schon seit Jahren daran, auf internationaler Ebene einen gemeinsamen Rechtsrahmen zu schaffen, bislang jedoch leider mit geringem Erfolg. Dies liegt unter anderem daran, dass die beteiligten Parteien unterschiedlichen Lagern angehören (Cloud-Anbieter, Verbraucher, Kleinunter-nehmen, Akademiker und Rechtsanwälte) und somit jeweils unterschiedliche Ansichten in die Diskussionen einbringen.[110]

Auf nationaler Ebene sollten sich deutsche Cloud Provider daher an die Richtlinie des Deutschen Instituts für Normung e. V. (DIN) orientieren[111]. Außerdem bietet der TÜV Rheinland eine Zertifizierung für Cloud-Service-Anbieter an, wobei die Prüfung auf eigene Anforderungen basiert, die sich dennoch nach dem Bundesdatenschutzgesetz (BDSG) sowie internationalen Normen richtet.[112] Des Weiteren können Unternehmen ihre IT-Produkte und -Services seit Anfang 2009 vom unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein mit dem European Privacy Seal (EuroPriSe) zertifizieren lassen. Dieses Siegel wurde aus einem eTEN-Forschungsprojekt der Europäischen Union zur Verbreitung transeuropäischer elektronischer Dienste entwickelt und orientiert sich direkt an den EU-Datenschutzrichtlinien.[113] Gerade die Zertifizierung dient als Sicherheit für Cloud-Nutzer. Wenn über die Cloud persönliche Daten verarbeitet werden, verpflichtet sich der Auftraggeber aufgrund § 11 BDSG vor Beginn der Datenverarbeitung und auch regelmäßig während der Auftragszeit den Auftragnehmer zu überprüfen, ob er die technischen und organisatorischen Maßnahmen einhält. Das Ergebnis dazu muss er außerdem dokumentieren. Dies ist in der Praxis sicherlich eine unmögliche Aufgabe, insb. für KMU, da die Auftragnehmer große Unternehmen wie z. B. Microsoft sind, dessen Rechenzentren sich überall auf der Welt befinden und eine Überprüfung zur Einhaltung des Datenschutzes unzumutbar erscheint.

Es bleibt jedoch abzuwarten, welche Standards tatsächlich international Einklang finden werden. Daher bleibt erstmal mittelfristig die Lösung, genaue SLAs zu vereinbaren, um Missverständnissen vorzubeugen und Interpretationsmöglichkeiten auszuschließen[114].

5.4 Sitz des Cloud-Anbieters bzw. dessen Serverstandorte

Laut dem Cloud-Monitor 2015 finden 74 % der befragten Unternehmen als Kriterium für die Auswahl eines Cloud-Providers sehr wichtig, dass sich das Rechenzentrum im Rechtsgebiet der EU befindet. 67 % erwarten zudem, dass auch der Hauptsitz ebenfalls dort liegt.[115] Diesem Meinungsbild versuchen internationale Anbieter teilweise gerecht zu werden, in dem sie spezielle EWR-/EU-Clouds in ihr Portfolio aufnehmen. Dies ändert jedoch nichts daran, dass ihr Hauptsitz weiterhin außerhalb des Rechtsgebiets der EU liegt und die Unternehmen somit möglicherweise anderen gesetzlichen Bestimmungen, wie z. B. dem „Foreign Intelligence Surveillance Act“ (FISA) oder dem „Patriot Act“ (zur Spionage- und Terrorabwehr) in den USA unterliegen. Dabei können

[110] *Moutafis* (2014): Der lange Weg zum EU-weiten Cloud-Recht.

[111] *ten Hompel et al.* (2013): Cloud Computing für Logistik 2, S. 42.

[112] *Rieth* (2013): Europäischer Datenschutztag 2013 – Risiken bei Cloud Service-Angeboten genau prüfen.

[113] *ten Hompel et al.* (2013): Cloud Computing für Logistik 2, S. 42.

[114] *ten Hompel et al.* (2013): Cloud Computing für Logistik 2, S. 42.

[115] *BITKOM Reseach/KMPG* (2015): Cloud-Monitor 2015, S. 32.

US-Behörden aufgrund der persönlichen Datenhoheit auf die Daten der Cloud global zugreifen. Es spielt dann keine Rolle mehr, wo sich das Rechenzentrum befindet.[116]

Cloud-Anbieter aus dem angloamerikanischen Raum können sich auch dem europäischen Datenschutzniveau verpflichten. Dies wird durch das Safe-Habor-Abkommen, das eine Vereinbarung zwischen der EU und dem Department of Commerce (Handelsministerium der USA) darstellt, ermöglicht[117]. Diese Zertifizierung soll solche Unternehmen auszeichnen, die ein angemessenes Datenschutzniveau vorweisen[118]. Hierbei melden die Unternehmen der Federal Trade Commission (FTC), dass sie sich den Grundsätzen des Safe-Harbor-Abkommens verpflichten und zertifizieren sich dadurch selbst[119]. Dies wird in der Praxis oftmals als großer Kritikpunkt angesehen. Eine Liste der zertifizierten Unternehmen wird vom Department of Commerce veröffentlicht.[120]

Das Bundesgericht in New York hat in einem Urteil Microsoft dazu verpflichtet Daten, die sich nicht in den USA befinden, an US-Behörden auszuhändigen. Der Konzern hatte sich erfolglos gegen einen Durchsuchungsbefehl gewehrt. Das Urteil ist jedoch noch nicht rechtskräftig, da die grundsätzliche Entscheidung über dieses Thema ausgesetzt und Berufung eingelegt wurde.[121] Dieses Urteil könnte nicht nur für Microsoft, sondern auch für alle anderen US-Unternehmen ein ernstzunehmendes Problem werden, die dem Cloud Computing-Geschäft erheblich schaden könnte. Das Vertrauen in solche Dienste hat ohnehin schon aufgrund der NSA-Affäre stark gelitten, sodass dieses Urteil die Skepsis nur noch verstärken wird.

5.5 Datensicherheit

Die Datensicherheit ist ein Thema, das von vielen Unternehmen immer noch sehr kritisch betrachtet wird. In der Praxis sind diese Befürchtungen auch nicht unbegründet wie die Studie „Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co.?“ der Corporate Trust aufzeigt. Hierbei hatte laut der Studie jedes zweite Unternehmen in den vergangenen zwei Jahren bereits Spionageangriffe oder Verdachtsfälle zu verzeichnen. Dieser jährliche finanzielle Schaden durch Industriespionage beläuft sich in Deutschland auf etwa zwölf Milliarden Euro. Dabei haben etwa 78 % der betroffenen Unternehmen einen finanziellen Schaden erlitten. Bei dem Großteil der geschädigten Unternehmen lag der Schaden zwischen 10.000 und 100.000 Euro. Auch ein immaterieller Schaden ist bei den Unternehmen zu verzeichnen. Hierbei waren etwa 37 % der Unternehmen betroffen. Insbesondere waren Patentrechtsverletzungen und Imageschäden bei Kunden oder Lieferanten die häufigsten Schädigungen. Im Mittelpunkt der Angriffe steht weiterhin der Mittelstand. Dies liegt womöglich daran, dass große Unternehmen deutlich mehr in ihre IT-Sicherheit investieren und daher auch als mögliche Angriffsziele eher seltener in Betracht kommen.[122]

---

[116] *ten Hompel et al.* (2013): Cloud Computing für Logistik 2, S. 43.

[117] *Europäische Kommission* (2000): Az. K(2000) 2441, S. 7.

[118] *Europäische Kommission* (2000): Az. K(2000) 2441, S. 4 ff.

[119] *Bräutigam/Thalhofer* (2013), in: *Bräutigam et al.*, IT-Outsourcing und Cloud Computing, S. 1229 Rdnr. 72.

[120] *Bräutigam/Thalhofer* (2013), in: *Bräutigam et al.*, IT-Outsourcing und Cloud Computing, S. 1228 Rdnr. 70.

[121] *Spiegel Online* (2014): Erstes Urteil: Microsoft muss US-Ermittlern Daten aus Europa herausgeben.

[122] *Corporate Trust* (2014): Studie: Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co?, S. 8-9.

Die Studie „Net Losses: Estimating the Global Cost of Cybercrime" von dem unabhängigen Center for Strategic and International Studies (CSIS) in Washington, das in Zusammenarbeit mit dem IT-Sicherheitsunternehmen McAfee erstellt wurde, hat eine weltweite Schadenshöhe von etwa 300 Mrd. Euro durch Internetkriminalität festgestellt.[123] Dabei belegt Deutschland den ersten Platz der 32 untersuchten Länder. Der Schaden wird gemessen am Bruttoinlandsprodukt (BIP). Hierbei liegt der in Deutschland festgestellte Prozentsatz bei 1,6. Im Vergleich zu den USA liegt der Satz bei 0,64 und zu China bei 0,64.[124] Das größte Problem ist bislang der Datendiebstahl. Obwohl der persönliche Datendiebstahl weltweit mindestens 800 Mio. Menschen betrifft, entsteht der größte Schaden bei den Unternehmen. Hierbei werden digitale Identitäten oder auch intellektuelles Eigentum gestohlen, das einen hohen unternehmerischen Wert aufweist. Es gibt keine Branche die nicht betroffen ist, jedoch liegt der Schwerpunkt der Angriffe in den Bereichen Finanzen, Chemie, Luftfahrt, Energie, Rüstung und IT. Auch die deutsche Automobilindustrie ist ein beliebtes Ziel von Angriffen.[125] Obwohl sich die Unternehmen im Vergleich zu den letzten Jahren stärker für das Thema Datensicherheit interessieren und auch deutlich mehr in diesen Bereich investieren, wird sich alles aufgrund der Vernetzung von Industrieanlagen (Stichwort: Industrie 4.0) sowie die weiteren Entwicklungen im Bereich „Internet der Dinge" (bspw. Vernetzung von Haushaltsgeräten) noch viel komplexer gestalten[126]. Immerhin sollen laut der Studie „IT-Sicherheit und Datenschutz 2015" von der Nationalen Initiative für Informations- und Internet-Sicherheit (NIFIS e. V.) für das Jahr 2015 die Ausgaben für IT-Sicherheit um 50 % steigen. Das glaubt immerhin fast die Hälfte der befragten deutschen Unternehmen. Die Studie hält außerdem fest, dass ein erhöhtes Sicherheitsbedürfnis zu den Mehrausgaben führt. Die Sensibilisierung für die Thematik ist bei fast allen deutschen Unternehmen angekommen. Zukünftig wird sich auch das Investitionsbild nicht ändern. Laut der Studie geht bis 2020 fast die Hälfte der befragten deutschen Unternehmen davon aus, dass eine Verdoppelung der Ausgaben für IT-Sicherheit und Datenschutz erfolgt.[127]

Beim Einsatz von Cloud-Technologien tun sich Unternehmen bei der Daten-sicherheit, insb. bei Sicherheitstechnologien wie Verschlüsselung, Authentifizierung und Schlüsselmanagement noch deutlich schwer. Dies ergab die Studie „The Challenges of Cloud Information Governance: A Global Data Security Study" vom Ponemon Institute, die im Auftrag von SafeNet erstellt wurde. Hierbei haben viele IT-Abteilungen in Unternehmen Schwierigkeiten die Kontrolle über die Unternehmensdaten auszuüben und zu gewährleisten. Lediglich 38 % der befragten Unternehmen haben eine eigene Strategie, die klare Regeln für den Schutz vertraulicher Informationen in der Cloud definiert. Außerdem hat die Studie festgestellt, dass etwa 50 % der im Unternehmen eingesetzten Cloud-Technologien ohne Absprache der IT-Abteilungen genutzt werden. Ebenso hält die große Mehrheit der Befragten (71 %) die Verschlüsselung in der Cloud für wichtig, jedoch nutzen nur 39 % diese auch wirklich. Die Lage wird sich in den nächsten Jahren noch verschärfen. Aufgrund der steigenden Nutzung der Cloud finden die Befragten es immer schwieriger, ihre sensiblen Daten mit konventionellen Sicherheitsmethoden ab-

[123] *CSIS/McAfee* (2014): Net Losses: Estimating the Global Cost of Cybercrime, S. 2.

[124] *CSIS/McAfee* (2014): Net Losses: Estimating the Global Cost of Cybercrime, S. 8.

[125] Clauß (2014): Cybercrime schadet Deutschland am stärksten.

[126] *CSIS/McAfee* (2014): Net Losses: Estimating the Global Cost of Cybercrime, S. 18; *Bundesamt für Sicherheit in der Informationstechnik (BSI)* (2014): Die Lage der IT-Sicherheit in Deutschland 2014, S. 7-8.

[127] *NIFIS* (2014): Studie: IT-Sicherheit und Datenschutz 2015, S. 6-7.

zusichern.[128] Auch die Vernetzung im B2B- und B2C-Bereich im Zuge der technischen Entwicklungen wird die Herausforderung an die Unternehmen sichtlich erschweren.

Auch das Frauenhofer-Institut für sichere Informationstechnologie (SIT) hat sich mit der Datensicherheit in der Cloud auseinandergesetzt. In der Studie „Über die Sicherheit von Cloud-Speicherdiensten" hat das Institut festgestellt, dass zwar alle analysierten Cloud-Anbieter der Studie für die Themen Daten-sicherheit und Datenschutz sensibilisiert und auch bemüht sind den Anforderungen gerecht zu werden, aber dennoch keine einheitliche Lösung gefunden haben, die alle Sicherheitsanforderungen erfüllt.[129] Daher wird die IT-Sicherheit in den kommenden Jahren für Unternehmen besonders beim Einsatz von Cloud-Technologien eine zentrale Rolle einnehmen. Auch auf der Software-Entwicklungsebene muss sich die Priorität von Sicherheit ändern. Präventive Maßnahmen können mögliche Schäden von Cyberkriminalität und Industriespionage deutlich reduzieren.

Außerdem ist problematisch, dass es bislang noch keine einheitlichen Zertifizierungen für das Cloud Computing gibt. Aktuell existieren zwar Unmengen an Pilotprojekt auf nationaler, europäischer und auch internationaler Ebene (etwa 150 Organisationen befassten sich mit der Thematik). Trotzdem sind es einfach zu viele Projekte, die eher viele Unsicherheiten schüren. Auch die Aussagekraft hält sich in Grenzen, da es keine einheitlichen Standards und unterschiedliche Rechtsauffassungen gibt. Einziger Lichtblick ist der neue ISO-Datenschutz-Standard ISO/IEC 27018 der seit August 2014 existiert und sich in die ISO 27000-Reihe eingliedert. Hierbei befasst sich diese Zertifizierung speziell mit der Regulierung der Verarbeitung von personenbezogenen Daten in der Cloud und orientiert sich im Wesentlichen an den Schutz- und Überwachungspflichten des europäischen Datenschutzrechts. Für die Zukunft wird sich allerdings weiterhin beim Thema Zertifizierung von Cloud Computing-Diensten erstmal nichts ändern. Der BSI und auch der BITKOM-Verband empfehlen daher sich an bestehende Zertifizierungen aus dem IT-Bereich wie z. B. dem IT-Grundschutz, ISO 27001 und ISO 27002 zu orientieren. Trotzdem kann eine Zertifizierung, egal wie valide sie ist, nicht die eigene Pflicht zur Überprüfung der Datensicherheit und dem Datenschutz ersetzen. Sie soll lediglich eine Vergleichbarkeit zwischen einzelnen Cloud-Anbietern ermöglichen und auch eine gewisse Vertrauensbasis schaffen. Besonders KMU können von solchen Zertifizierungen profitieren, da gerade diese Zielgruppe die größten Bedenken in Sachen Cloud Computing hat, die mit der Schaffung von Vertrauen in Form von einheitlichen Zertifizierungen und Standards beseitigt werden könnten.[130]

D. Aktuelle Rechtslage und Entwicklungen im Cloud Computing

1. Auf nationaler Ebene

In Deutschland hat der Datenschutz eine hohe Priorität aufgrund seines Grundrechtscharakters. Daher sind auch die Gesetze im internationalen Vergleich deutlich strenger geregelt. Diese spiegeln sich insb. im Bundesdatenschutzgesetz (BDSG) wieder. Auch das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) spielen eine

[128] *Ponemon Institute/SafeNet* (2014): The Challenges of Cloud Information Governance: A Global Data Security Study, S. 1 ff.

[129] *Frauenhofer SIT* (2012): Über die Sicherheit von Cloud-Speicherdiensten, Management Summary, S. 4.

[130] *Manhart* (2015): Was ist was bei der Cloud-Zertifizierung; *Schonschek* (2014): Cloud-Zertifizierung: Noch keine Einheitlichkeit in Sicht.

übergeordnete Rolle. Die noch gültige europäische Richtlinie 95/46/EG[131] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist in Deutschland durch das BDSG umgesetzt. Da es sich hierbei um eine Richtlinie handelt, muss diese in nationales Recht umgesetzt werden, um ihren Gehalt zu verwirklichen. Die Bestimmungen der Richtlinie werden auf das Cloud Computing angewendet[132].[133] Das Wachstum bzw. die weitere Entwicklung des Cloud Computing hängt natürlich auch von solchen Gesetzen ab, weil diese den Rahmen vorgeben. Einer Studie der Business Software Alliance (BSA) zufolge, die ein internationaler Interessenverband von Software-Anbietern ist, stellt die strenge Haltung in Deutschland in Bezug auf den Datenschutz eine Gefahr für die Entwicklung des Cloud Computing dar. Sie sehen die gesetzlichen Regelungen eher als unzumutbare Hürden an, die es der Cloud erschweren sich durchzusetzen. Auch die große Anzahl der deutschen Datenschutzbehörden ist laut der Studie der BSA eher negativ aufzufassen und stellt das typische Bild deutscher Bürokratisierung dar.[134] Der Bundestagsausschuss „Digitale Agenda“ ist anderer Meinung. Ein hohes Datenschutzniveau schließt Wettbewerb nicht aus. Gerade dies sollte als Wettbewerbsfaktor genutzt werden. Besonders hier können KMU punkten und sich im internationalen Wettbewerb beweisen.[135]

2. Auf internationaler Ebene

Die datenschutzrechtliche Beziehung zwischen den USA und der EU hat durch die Snowden-Enthüllungen enormen Schaden erlitten. Daher verhandelt auch die Europäische Kommission bereits seit Herbst 2013 mit der US-amerikanischen Regierung an neuen Regularien bzgl. des Safe-Harbor-Abkommens. Diese sind Grundlage für den Datenverkehr zwischen der EU und USA. Hierbei sind mehr als 5.000 Unternehmen eingetragen, die sich den Safe-Harbor-Regelungen verpflichten[136]. Im Fokus der Verhandlungen soll eine angemessene Berücksichtigung der Grundrechte von europäischen Bürgern stehen. Im Sommer 2014 sollten diese eigentlich zu einem positiven Abschluss kommen, aber diese ziehen sich immer noch hin. Andrea Voß, Bundesbeauftragte für Datenschutz und Informationsfreiheit, empfiehlt sogar der Europäischen Kommission bei bleibenden Verhandlungsproblemen bzw. bei Verhandlungsabbruch, das Safe-Harbor-Abkommen auszusetzen oder ein neues Abkommen zu vereinbaren.[137] Die Europäische Kommission erkennt die Schwächen des Abkommens an, spricht sich aber trotzdem für die Beibehaltung aus. Sie will das Abkommen stärken, indem sie die Schwächen durch geeignete Maßnahmen beseitigt. Die US-Behörden müssen hier gründlicher überwachen und prüfen, ob die beitretenden Unternehmen wirklich den Safe-Harbor-Grundsätzen zum Datenschutz gerecht werden. Auch muss ein deutlicher Hinweis gegeben werden, wer aktuell noch zertifiziert ist und wer nicht. Auch die Transparenz im Hinblick auf die Datenverarbeitung und -weitergabe muss verbessert werden.[138] Es bleibt abzuwarten, inwieweit sich die Verhandlungen entwi-

---

131 Amtsblatt der Europäischen Gemeinschaft (1995): ABl. L 281.

132 Art. 29-Datenschutzgruppe (2012): Stellungnahme 5/2012 zum Cloud Computing, S. 8 Ziff. 3.2.

133 *Hartung/Storm* (2014), in: *Hilber*, Handbuch Cloud Computing, Teil 4 S. 323 Rz. 2.

134 *Business Software Alliance (BSA)* (2013): Global Cloud Computing Scorecard.

135 Deutscher Bundestag Pressemitteilung (2015): Datenschutz als Wettbewerbsvorteil.

136 https://safeharbor.export.gov/list.aspx.

137 Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI) Pressemitteilungen (2015): Andrea Voßhoff: Die EU Kommission muss jetzt Klartext reden!

138 Europäische Kommission (2013): COM(2013) 846 final, S. 7-9; Europäische Kommission (2013): COM(2013) 847 final, S. 20-22.

ckeln werden. Eine zügige und gemeinsame Entscheidung wäre aber eine wünschenswerte Lösung.

Aktuell verhandelt die EU mit den USA über eine „Transatlantische Handels- und Investitionspartnerschaft“ (TTIP). Hierbei soll das zu verhandelnde Abkommen beiderseits anerkennende Standards etablieren, die sowohl Verbrauchern als auch Unternehmen zu Gute kommen. Auch Zölle und Handelsbarrieren im transatlantischen Handel sollen abgebaut werden, die zu einer Verbesserung der Wirtschaftsleistung und Wettbewerbsfähigkeit beitragen sollen. Grundsätzlich sollen die unterschiedlichen Vorschriften und Regeln der beiden verhandelnden Parteien langfristig so gestaltet werden, dass sie besser zusammenpassen.[139] In der öffentlichen Diskussion unterzieht sich das Abkommen einer kritischen Betrachtung, die sicherlich nachvollziehbar ist. Hierbei hat sich der Bundesverband IT-Sicherheit e. V. (TeleTrusT) insb. mit dem Schwerpunkt Datenschutz und IT-Sicherheit beschäftigt und warnt, dass sowohl die deutschen als auch die europäischen Qualitätsstandards sinken könnten. Bei den Verhandlungen werden nationale Institutionen wie z. B. in Deutschland der BSI nicht direkt in die Verhandlungen mit einbezogen und müssen ihre Vorstellungen den Verhandlungsführern der EU-Kommission erst beibringen. Wenn amerikanische NIST Standards für die IT-Standardisierung beim TTIP gewählt werden, die im Vergleich zu deutschen Standards geringer sind, wird dies womöglich der gesamten deutschen IT-Sicherheitsindustrie schaden. Grundsätzlich sind Bemühungen um globale Standards zu begrüßen, wenn sie nicht die eigenen, nationalen und etablierten Standards senken. Das hohe Niveau sollte beibehalten werden und gerade die USA könnte sich aufgrund ihrer Verfehlungen der letzten Vergangenheit hieran orientieren.[140]

Auch das plurilaterale Abkommen zum Handel mit Dienstleistungen „Agreement on Trade in Services“ (TiSA), dass seit April 2013 im geheimen zwischen 24 WTO-Mitgliedstaaten, darunter auch die EU, verhandelt wird, ist in der öffentlichen Kritik[141]. Grundsätzlich soll das Ziel des Abkommens sein eine Erleichterung des Marktzugangs im Dienstleistungshandel zu ermöglichen. Unter den Geltungsbereich des Abkommens fallen insb. technische Dienste wie Internetversorgung, elektronische Transaktionen und digitale Signaturen, die in der Öffentlichkeit mit großer Skepsis begegnet werden. Hier ist der mögliche Einfluss auf die zukünftigen Technologien und transatlantischen Datenströme deutlich erkennbar.[142]

Bei beiden Abkommen versucht die USA starken Einfluss auf die europäische Politik, insb. den europäischen Datenschutz, zu nehmen und diese im besten Fall auszuhebeln. Privacy International, das Center for Digital Democracy, der Europäische Verbraucherverband BEUC und der US-Verbraucherverband sind der Auffassung, dass die Kapitel E-Commerce und elektronische Datenflüsse in den Abkommen die europäische Datenschutz-Grundverordnung bedrohen. Die Verhandlungsführer der EU-Kommission verfügen auch nicht über ein Mandat für die Verhandlung von Regeln für den Datenschutz. Die USA sieht den Datenschutz in der EU als ein Handelshemmnis, das gerade von der EU als Grundrecht angesehen wird und somit auch logischerweise

---

[139] Bundesministerium für Wirtschaft und Energie (BMWi) (2015): Häufig gestellte Fragen zur Transatlantischen Handels- und Investitionspartnerschaft (TTIP).

[140] TeleTrusT Pressemitteilung (2015): Bundesverband IT-Sicherheit warnt vor Absenkung des IT-Sicherheitsniveaus durch TTIP.

[141] *BMWi* (2015): TiSA: Verhandlungen und Akteure.

[142] *Biselli* (2015): Leak zeigt: Handelsabkommen TiSA könnte nationale Datenschutzbestimmungen aushebeln.

von den Verhandlungen ausgeschlossen werden muss. Es bleibt abzuwarten wie sich Europa zu diesen Abkommen entscheiden wird.[143]

3. Auf europäischer Ebene

Ende dieses Jahres wird die Datenschutz-Grundverordnung erwartet, die die zurzeit geltende europäische Datenschutzrichtlinie aus dem Jahr 1995 ersetzen soll. Diese soll an die technischen Entwicklungen der letzten Jahre angepasst werden und den Datenschutz in Europa harmonisieren, dabei aber das Datenschutzniveau möglichst hochhalten. Auch eine Entbürokratisierung soll die unnötigen bürokratischen Hürden beseitigen.[144] Da die Mitgliedsstaaten unterschiedliche Gesetze und Anwendungen haben, die zu einem ungleichen Datenschutzniveau führen, muss hier eine klare und einheitliche Linie geschaffen werden, die im ganzen EU-Rechtsraum gilt. Seit 2012 arbeiten die Europäische Kommission, das Europäische Parlament und der Rat der Europäischen Union an der Verordnung. Dabei werden die Entwürfe zusammen mit Vertretern aus der Wissenschaft, Wirtschaft, Verwaltung und Bürgerrechtsorganisationen in Deutschland, Europa und weltweit diskutiert.[145] Für die Nutzer sowie Daten-Verarbeiter sollen europaweit dieselben Rechte und Pflichten gelten. Außerdem können Unternehmen nicht mehr den EU-Mitgliedstaat mit dem niedrigsten Datenschutzniveau (bspw. Irland) wählen, da ein europaweites einheitliches Datenschutzniveau gelten würde. Europäisches Datenschutzrecht wird für alle Akteure, die auf dem europäischen Markt tätig sind, gelten. Das heißt konkret, dass es keine Rolle mehr spielt, wo der Sitz des Unternehmens ist, sondern nur, ob sie auf dem Markt tätig sind (Marktortprinzip). Darüber hinaus soll datenschutzkonforme Technikgestaltung in Form von „Privacy by design“ das Vertrauen in den europäischen Datenschutz in der EU stärken. Die Verordnung wird bei Verabschiedung nach einer Übergangszeit von zwei Jahren unmittelbar in allen EU-Mitgliedsstaaten gelten.[146]

Tatsächlich sehen die Verhandlungen aber eher eine Verschlechterung des Datenschutzniveaus vor, die sicherlich der Lobbyarbeit von zahlreichen Unternehmen der Wirtschaft geschuldet ist. Dies belegt die Initiative LobbyPlag, die 11.000 Dokumentseiten aus den Verhandlungen des EU-Ministerrats zur geplanten Datenschutz-Grundverordnung veröffentlicht hat. Besonders die Bundesregierung fällt negativ auf. Sie setzt sich dafür ein, dass der Datenschutz abgeschwächt wird, obwohl sie einst noch am ambitioniertesten war. Hier wird der Einfluss der Wirtschaftslobby deutlich. Auch die britische Bürgerrechtsorganisation Statewatch hat ein vertrauliches Dokument der Arbeitsgruppe Dapix des Rats veröffentlicht, dass zu einem ähnlichen Ergebnis kommt.[147]

Auf die kommenden europapolitischen Entwicklungen sind die meisten Unternehmen jedoch nicht wirklich vorbereitet, obwohl vieles bekannt ist. Dies geht aus dem Report „Mixed state of readiness for new Cybersecurity Regulations in Europe“, der von IDG Connect in Auftrag von FireEye auf Basis einer Umfrage in Unternehmen in Deutschland, Frankreich und Großbritannien erstellt wurde, hervor. Nur etwa 66 % der Befrag-

---

[143] *Bendrath* (2015): TTIP und TISA: Die USA wollen Datenschutz wegverhandeln.

[144] *Hartung/Storm* (2014), in: Hilber, Handbuch Cloud Computing, Teil 4 S. 324 f. Rz. 6-7.

[145] *Bundesministerium für den Datenschutz und die Informationsfreiheit (BfDI)* (2015): Die Reform des Europäischen Datenschutzrechts.

[146] *Europäische freie Allianz (EFA)* (2015): EU-Datenschutzgrundverordnung: Stand der Dinge 10 wichtigsten Punkte.

[147] *Beuth* (2015): Bundesregierung hofiert Lobbyisten.

ten sind überzeugt, die Auswirkungen der europapolitischen Veränderungen in Form der europäischen Datenschutz Grundverordnung (DS-GVO) und der Richtlinie zur Netz- und Informations-sicherheit (NIS-Richtlinie) vollständig zu kennen. Die Ursache für eine starke Verunsicherung der Unternehmen liegt darin, dass fehlende Informationen vorliegen. Mehr als 60 % der Befragten verfügen über keine oder nur geringe Möglichkeiten einer Beratung zur neuen Gesetzgebung. Bei 39 % der befragten Unternehmen sind alle Maßnahmen, die von der NIS-Richtlinie gefordert sind, umgesetzt worden. Hingegen sind es lediglich 20 % bei der DS-GVO. Deutschland ist im Vergleich zu Frankreich und Großbritannien deutlich sensibilisierter für die kommenden europapolitischen Veränderungen. Die Zuständigkeiten sind in den meisten Fällen schon festgelegt. Hierbei planen in Deutschland mehr als Dreiviertel (76 %) der befragten Unternehmen ihrer internen IT-Abteilung die Verantwortung zu übertragen. Im Vergleich sind es in Frankreich lediglich knapp die Hälfte (46 %). Als große Herausforderungen sehen 64 % der Befragten die zusätzlichen Kosten für Hard- und Software, die Implementierungskosten (58 %) und die Komplexität der Richtlinien (56 %) an. Im Kontext zu Datenlecks sind mögliche Geldstrafen (58 %), Auswirkungen auf Geschäft und/oder Gewinn (58 %) und Reputationsschäden (57 %) als einer der größten Sorgen der befragten Unternehmen anzusehen.[148]

Insbesondere die KMU treffen die kommenden europapolitischen Veränderungen stark. Die enthaltende Dokumentationspflicht in der DS-GVO hat für KMU gravierende Auswirkungen. Sie müssen einen erheblichen bürokratischen und somit finanziellen Mehraufwand leisten, der nicht im Verhältnis zur Reduzierung der Risiken bei der Datenverarbeitung steht. Daher empfiehlt der Bundesverband mittelständische Wirtschaft (BVMW), dass diese Dokumentationspflicht auf ein vertretbares Maß eingeschränkt werden soll. Darüber hinaus müssen KMU laut der DS-GVO Auskunft zu sämtlichen erhobenen Daten an jeden Betroffenen erteilen. Hierbei ist dies in den meisten Fällen nicht darstellbar und mit einem hohen Aufwand verbunden. Daher wird die Empfehlung ausgesprochen, dass nur auf Anfrage der betroffenen Person eine Auskunft erteilt werden soll, um den Aufwand so niedrig wie möglich zu halten, aber dennoch dem Inhalt der Regelung zu folgen. Auch ein Datenschutzbeauftragter wird in der kommenden DS-GVO gefordert, jedoch erst ab einen zu verarbeiteten Datensatz von 5.000 pro Jahr. Hier empfiehlt der Bundesverband mittelständische Wirtschaft darüber hinaus ein weiteres Kriterium hinzuzufügen. Und zwar sollte ein Datenschutzbeauftragter ernannt werden, wenn mehr als zehn Mitarbeiter mit der Bearbeitung der relevanten Daten beschäftigt sind. Mittlerweile wird sogar diskutiert, ob die Regelung mit der Ernennung eines Datenschutzbeauftragten eine obligatorische werden soll und somit keine Pflicht mehr darstelle. Die Pflicht zur Datenschutz-Folgenabschätzung ist zwar sinnvoll, aber für KMU mit einem erheblichen Mehraufwand verbunden. Der Mehrwert ist deutlich geringer als der Mehraufwand. Daher wird die Empfehlung ausgesprochen, diesen auf ein Minimum für KMU zu begrenzen. Bei Sanktionen müssen die Verhältnisse von KMU berücksichtigt werden. Hier sollten eine Differenzierung nach der Art, der Schwere und der Anzahl der Verstöße und eine Abstufung bzgl. der Größe und des Umsatzes eines Unternehmens erfolgen. Da die Verordnung sehr komplex und nicht für jedermann verständlich ist, sollte eine genaue Formulierung gewählt werden, um zusätzliche Kosten aufgrund fehlender Verständlichkeit zu vermeiden. Es wird deutlich, dass eine Berücksichtigung für KMU gänzlich fehlt und die DS-GVO sich eher an internationale Konzerne richtet. Hier empfiehlt der Bundesverband mittelständische Wirtschaft eine Mittelstandsklausel in die Verordnung aufzunehmen, die Ausnahmeregelungen

[148] *Datenschutz Praxis* (2015): Datenschutz-Grundverordnung: Viele Unternehmen sind nicht vorbereitet.

und Änderungen enthält, die den An-forderungen des Mittelstandes nicht nur in Deutschland gerecht wird.[149]

E. Allgemeine Handlungsempfehlungen für den Einsatz von Cloud-Technologien im Hinblick auf die Datensicherheit in Unternehmen

1. Privacy by design & Privacy by default

Der Begriff „Privacy by design“ wurde von Ann Cavoukian, der kanadischen Information & Privacy Beauftragten von Ontario definiert. Es beschreibt die frühe Einbettung der Datenschutzaspekte in der Gesamtentwicklung von Prozessen, Systemen und Produkten in technischer Hinsicht. Da das Beheben von Datenschutzbedenken nach Feststehen des Gesamtkonzepts sich als mühsam und sehr zeitaufwändig erweist, gilt es daher von vorneherein diese Bedenken zu beseitigen. Ziel des Privacy by design-Konzepts ist die Gewährleistung des Datenschutzes und die persönliche Kontrolle über die eigenen Daten sowie die Gewinnung eines nachhaltigen Wettbewerbsvorteils für Organisationen. Somit erstreckt sich dieses Konzept auf drei Anwendungsbereiche:[150]

- IT-Systeme,
- verantwortungsvolle Geschäftspraktiken,
- physikalisches Design und vernetzte Infrastruktur.

Der Begriff „Privacy by default“ fällt unter das Privacy by design-Konzept und beschreibt hierbei den Datenschutz als Standardfunktion. Bei diesem wird der Datenschutz durch automatische Vor- bzw. Grundeinstellung gewährleistet. Hierbei ist der Schutz systemimmanent, sodass ein aktives Eingreifen gar nicht notwendig ist.[151] Diese beiden Ansätze sollen in der kommenden EU-DSGVO in Art. 23 rechtlich verankert werden. Dabei soll bei der Entwicklung von Technologien stets der Stand der Technik als Orientierung dienen. Hierbei hat die Kommission sogar das Recht Standards und Techniken festzulegen.[152]

Die Europäische Agentur für Netz- Informationssicherheit (ENISA) hat in einem Bericht[153] Empfehlungen ausgearbeitet, wie Datenschutz in die Prozesse und Anwendungen konkret verankert werden kann. Hierbei hat die ENISA acht Empfehlungen erarbeitet, die die größten Probleme bei der Umsetzung von Privacy by design beseitigen sollen. Die Politik soll sich aktiv einsetzen und von öffentlichen Förderungsprojekten sollten Leitfäden veröffentlicht werden. Aufsichtsbehörden sollten die Möglichkeit bekommen bereits bestehende Privacy by design-Konzepte anzuerkennen und auszuzeichnen. Forschungsergebnisse sollten so transparent wie möglich gestaltet sein, sodass jeder schnell und einfach informiert werden kann. Ebenso sollten Entwicklungswerkzeuge möglichst frei und für jedermann zugänglich gemacht werden. Die Interoperabilitätsstandards sollten für die Datenschutzfunktion bereitstehen, sodass die Privacy-Techniken leichter implementiert werden können. Auch Authentifikationsverfahren sollten angeboten werden, die eine sichere Kommunikation gewährleisten. Außerdem werden von der ENISA verschiedene Ende-zu-Ende-Verschlüsselungen sowie Ver-

[149] *BMWV* (2014): Positionspapier EU-Datenschutz-Grundverordnung, S. 1 f.

[150] *Cavoukian* (2011): Privacy by Design, die 7 Grundprinzipien, S. 1.

[151] *Cavoukian* (2011): Privacy by Design, die 7 Grundprinzipien, S. 2.

[152] *Europäische Kommission* (2012): KOM(2012) 11 endgültig, S. 64.

[153] *ENISA* (2015): Privacy and Data Protection by Design – from policy to engineering.

schleierungsmöglichkeiten für Metadaten mit Hilfe von „Virtual Private Networks“ (VPNs) und Onion-Routing angeboten.[154]

KMU können künftig auf diese Ansätze vertrauen, da die Anbieter von Cloud-Technologien rechtlich gezwungen werden sich an diese zu halten. Damit entlastet es sie weitestgehend von der Umsetzung von datenschutzfreundlichen Maßnahmen, da die Anbieter und Entwickler in der Pflicht stehen. Entwickeln KMU hingegen eigene individuelle Anwendungen, so stehen sie ebenfalls in der Pflicht sich an das Privacy by design-Konzept zu halten. Dabei können sie sich an Leitfäden, Forschungsergebnisse und Empfehlungen zu Verschlüsselungen und Verschleierungsmöglichkeiten der ENISA oder anderen Institutionen (z. B. BSI und BITKOM) orientieren.

2. Security by design

„Security by design“ kann unterschiedlich verstanden werden. Im engeren Sinn ist unter diesem Begriff die Berücksichtigung von Sicherheit in den Entwurf-Phasen von Software-Entwicklungsprozessen zu verstehen und im weiteren Sinn die Sicherheit im kompletten Lebenszyklus eines Software-Produkts. Hierzu zählt auch die sichere Verankerung von zu integrierenden Softwarekomponenten anderer Hersteller. Security by design ist daher nicht als Technik zu verstehen, sondern als eine Sicherheitsmaßnahme, die den Entwicklungsprozess kontinuierlich begleitet. Dabei sollen die Maßnahmen eine nachhaltige und integrierte Sicherheit der Software-Produkte gewährleisten.[155]

KMU sind in Deutschland auf die Hilfe von großen Software-Anbietern und auch auf die Forschung und Politik angewiesen, da sie selbst nicht die nötigen Mittel und Erfahrungen auf dem Gebiet der Sicherheit vorweisen können[156]. Somit müssen die Software-Anbieter bei der Entwicklung ihrer Produkte die Sicherheit schon von Beginn an miteinbeziehen. Denn die nachträgliche Hinzufügung von Sicherheitsmaßnahmen hat in der Vergangenheit bekanntlich nicht wirklich dazu beigetragen die Sicherheit zu erhöhen. Nicht ohne Grund sind die Angriffe auf Unternehmen in den letzten Jahren deutlich angestiegen, da immer mehr Sicherheitslücken bekannt geworden sind, die die Angreifer im Netz nutzen. Selbst große Unternehmen wie Sony oder Amazon sind Opfer von solchen Angriffen geworden.[157] Eine gesetzliche Verankerung in Form der EU-DSGVO sollte Software-Anbieter dazu verpflichten ausreichende Maßnahmen zu ergreifen, um ein hohes Maß an Sicherheit bei Software-Produkten zu gewährleisten. Noch gibt es leider keine wirklich greifenden gesetzlichen Regelungen, die näheres bestimmen. Daher muss sich an dieser Stelle die Politik sowohl auf nationaler als auch auf europäischer Ebene stark machen, um das Ziel der Sicherheit in Zukunft erfüllen zu können. Hierbei gibt es bereits erste positive Anzeichen der Bundesregierung in Form eines Gesetzesentwurfs zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Hierbei soll dem BSI die Möglichkeit gegeben werden bestimmte IT-Produkte auf ihre IT-Sicherheit zu überprüfen und diese Ergebnisse zu veröffentlichen. Damit soll die Transparenz bei der Sicherheit von IT-Produkten erhöht werden

---

154 *Schneider et al.* (2015): ENISA: Empfehlungen für Privacy by Design.

155 *Frauenhofer SIT* (2013): Trend- und Strategiebericht: Entwicklung sicherer Software durch Security by design, S. 4.

156 *Frauenhofer SIT* (2013): Trend- und Strategiebericht: Entwicklung sicherer Software durch Security by design, S. 5 und S. 10 f.

157 *Frauenhofer SIT* (2013): Trend- und Strategiebericht: Entwicklung sicherer Software durch Security by design, S. 4 f.

und zugleich eine höhere Akzeptanz schaffen.[158] Zwar steht noch nicht fest, wann das Gesetz in Kraft treten wird, aber es wird kommen, da es auch dringend benötigt wird. Auf europäischer Ebene wird wohl die kommende EU-DSGVO das gewünschte, an den technologischen Entwicklungen angepasste, Regelwerk darstellen. Auch die Forschung ist als unterstützendes Instrument bei der Erfüllung der Ziele der Sicherheit gefordert. Hierbei sollen auf nationaler und europäischer Ebene Forschungsprojekte initiiert und gefördert werden, die anschließend öffentlich präsentiert und geteilt werden. Das Bundesministerium für Bildung und Forschung (BMBF) fördert bereits bestimmte Forschungsprojekte (IT-Sicherheit, Big Data, Industrie 4.0). Auf die Ergebnisse der Forschungsberichte können sowohl die Software-Anbieter als auch die Unternehmen zugreifen.

3. Faktor Mensch als Fehlerquelle

Die IT-Sicherheit in Unternehmen hängt längst nicht mehr nur von der Technik ab. Auch der Faktor Mensch ist mindestens genauso wichtig geworden. Leider hat dieser in der Vergangenheit zu wenig Beachtung bekommen. Gerade Mitarbeiter in Unternehmen stellen ein hohes Sicherheitsrisiko für Cyberattacken dar. Aufgrund von Unsicherheiten und fehlendes Know-how fallen immer wieder Mitarbeiter auf sogenannte „Phishing-Mails“ herein. Hierunter werden E-Mails verstanden, die versuchen das Vertrauen von Mitarbeitern zu gewinnen, um an vertrauliche Informationen zu gelangen (bspw. Zugangsdaten zu Firmenrechnern oder Bankdaten). Dabei fällt jeder siebte Mitarbeiter auf solche E-Mails herein. „Gute“ Phishing-Mails haben sogar eine Erfolgsquote von 45 %. Dies ergab die Studie „Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild”[159] von Google. Wie Mitarbeiter auf das Thema IT-Sicherheit sensibilisiert werden können, wird in den nächsten drei Jahren von der Universität Bonn interdisziplinär erforscht. Finanziert wird das ganze Projekt vom Bundesministerium für Forschung und Bildung. Leider gibt es bis dato noch keine wirklichen Forschungsergebnisse auf diesem Gebiet. Ab 2018 wird das Projekt die gewünschten Erkenntnisse liefern, die in Zukunft die IT-Sicherheit in Unternehmen bzgl. des Faktors Mensch verbessern kann.[160]

Um mögliche menschliche Fehler auf ein Minimum zu reduzieren, können folgende Möglichkeiten zum Einsatz kommen:

- Beratung bei Cloud-Technologien und Cloud-Verträgen: Da sowohl Mitarbeiter als auch die Geschäftsleitung in KMU überwiegend fehlendes Wissen in den Bereichen IT-Sicherheit, Cloud-Technologien und Vertragsrecht haben, so müssen die Cloud-Anbieter ihre Angebote transparenter machen und auch die Cloud-Verträge dem Kunden näherbringen. Darüber hinaus können KMU auf sog. Cloud-Marktplätzen (bspw. die „german:businesscloud“ des Cloud-ECOSystems)[161] Angebote vergleichen oder Zertifikate als Sicherheitsnachweise heranziehen, um eine richtige Auswahl treffen zu können. Vielen KMU ist nicht bewusst, dass sie ihre IT-Anwendungen auch Cloud-tauglich machen müssen, um überhaupt die Dienste richtig nutzen zu können. Daher müssen Cloud-Anbieter hier besonders intensive Beratungsgespräche führen.

---

[158] Bundesministerium des Innern (BMI) (Nachrichten) (2015): „Wir wollen die deutschen IT-Systeme zu den sichersten in der Welt machen”.

[159] *Google, Inc.* (2014): Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild.

[160] *Krüger* (2015): Schutz vor Datenklau: Forscher simulieren Phishing-Angriffe auf Firmen.

[161] *Kunisch* (2015): Drei Modelle für Cloud-Marktplätze.

- Unterweisungen bzw. Belehrungen: Da in vielen Unternehmen zwar viel gesprochen, aber nicht wirklich gehandelt wird, sollte bereits in der Führungsebene ein IT-Sicherheitsbewusstsein geführt und vorgelebt werden, an denen sich die Mitarbeiter orientieren können. Hierbei können Unterweisungen oder Belehrungen von Führungskräften oder Externen in Einzel- oder Gruppengesprächen geführt werden. Auch die Dokumentation ist hier wichtig, um sicherzustellen, dass die durchgeführten Maßnahmen ziel-führend und somit erfolgreich waren. Welche Mitarbeiter inwieweit unterwiesen oder belehrt werden sollten, muss vorher abgeklärt werden, da jeder Mitarbeiter unterschiedlich stark in die Prozesse der IT eingebunden ist. Dabei können auch Aushänge am schwarzen Brett, Publikationen im Intranet oder E-Mails dazu beitragen, Mitarbeiter zu informieren und auf zu klären.[162]
- Seminare und Workshops: Um die Mitarbeiter auf mögliche IT-Gefahren hinzuweisen und auf das Thema IT-Sicherheit zu sensibilisieren, können sowohl intern als auch extern Seminare und Vorträge veranstaltet und durchgeführt werden. Es gibt zahlreiche Angebote, dabei sind für KMU wahrscheinlich die kostengünstigen bzw. kostenlosen Angebote am interessantesten. Hierbei bietet bspw. die BITKOM Akademie zahlreiche Seminare an, die nicht nur das Thema IT-Sicherheit, sondern auch Themen wie Datenschutz, Cloud, etc. behandeln[163]. Die BITKOM Akademie wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) gefördert, sodass kostenlose Angebote überhaupt möglich sind. Dabei werden die meisten Angebote über Online-Kurse durchgeführt, sodass die Mitarbeiter flexibel daran arbeiten können.
- Verantwortlichen für IT-Sicherheit benennen: Die Benennung eines Verantwortlichen und die klare Definition seines Aufgabenbereiches kann dazu beitragen, die IT-Sicherheit im Unternehmen zu verbessern. Dieser nimmt Verstöße, Meldungen und Verbesserungsvorschläge von Mitarbeitern auf, um somit gezielte Maßnahmen einleiten zu können bzw. die sowohl präventiv als auch repressiv wirken.
- Unternehmenskultur: Auch die sog. „Angstkultur“ die von Mitarbeitern gelebt wird, die dazu führt, dass Fehler oder Verstöße gar nicht erst gemeldet werden, muss sich ändern. Hierbei hat die Führungsebene die Aufgabe sicherzustellen, dass es keine negativen Konsequenzen für Mitarbeiter gibt. Wenn diese Angstkultur kontrolliert und beseitigt werden kann, so werden die Mitarbeiter auch eher dazu bereit sein, Fehler oder Verstöße zuzugeben. Hier empfiehlt es sich eine Unternehmenskultur einzuführen, die von der Führungsebene vorgelebt wird, die insb. die IT-Sicherheit in den Vordergrund stellt. Wenn dies von allen Mitarbeitern verinnerlicht werden kann, so steht der IT-Sicherheit im Unternehmen bezogen auf den menschlichen Faktor nichts mehr entgegen.

4. Maßnahmen zum Schutz vor behördlichen Zugriffen

Grundsätzlich ist die Empfehlung auszusprechen, Cloud-Angebote aus Drittstaaten zu meiden, da ein Zugriff durch ausländische Behörden (insb. durch den Patriot Act) jederzeit möglich ist. Wenn also Daten ins Ausland transferiert werden, so unterliegen sie nicht mehr deutschen Datenschutzrecht, sondern dem Recht des jeweiligen Ziellandes. Es können aber auch weitergehend Zugriffsmöglichkeiten durch Sicherheits-, Strafverfolgungs- oder Finanzbehörden bestehen. Auch solche Daten, die sich zwar nicht in einem Drittstaat befinden, aber dennoch von Drittstaaten kontrolliert werden,

[162] *Deutschland sicher im Netz* (DsiN) (2014): DsiN Sicherheitsmonitor – Mittelstand, S. 28.

[163] https://www.bitkom-akademie.de/seminare.

können von solchen Zu-griffen betroffen sein.[164] Da spielt es keine Rolle, ob das Unternehmen ein Zertifikat des Safe-Harbor-Abkommens trägt oder eine EU-Standardvertrags-klausel-Vereinbarung geschlossen wurde. Ab dem Datentransfer gilt nunmehr US-Datenschutzrecht und das Verständnis der Amerikaner zum Datenschutz ist anders als das der Europäer.[165] Eine Verschwiegenheitsverpflichtung des Cloud-Anbieters ist ebenfalls möglich, aber der Zugriff ist den in- und ausländischen Behörden gesetzlich gestattet, sodass solch eine Vertragsklausel keine wirkliche Wirkung erzielen kann. Informations- und Verteidigungspflichten an den Cloud-Anbieter, die im Vertrag geregelt werden können, sind denkbar, um einen wirksamen Schutz gegen Zugriffe zu erreichen. Darüber hinaus kann der Cloud-Anbieter vertraglich dazu verpflichtet werden, technische Vorkehrungen zu treffen, die einen Zugriff durch Behörden verhindern oder zumindest erschweren. Hierbei wären die Pseudonymisierung und Verschlüsselung der Daten eine mögliche Idee zur Umsetzung. Letzteres ist logischerweise nur sinnvoll, wenn der Cloud-Anbieter die Schlüssel nicht hat bzw. kennt. Ansonsten wäre er gesetzlich verpflichtet auch die Schlüssel preiszugeben.[166]

5. E-Mail-Sicherheit

Die E-Mail stellt weiterhin das meistgenutzte Kommunikationsmedium im Unternehmen dar. Obwohl die Zahlen des E-Mail-Verkehrs deutlich angestiegen sind und im Laufe der Zeit weiterhin zunehmen werden, sind die Sicherheitsvorkehrungen, um diese geschäftskritischen Daten zu schützen, rückläufig gesunken. Mehr als die Hälfte (57 %) verschickt ihre E-Mails ungeschützt, obwohl sie das Risiko kennen. Hierbei gaben zwölf Prozent an sich überhaupt keine Gedanken über Sicherheitsvorkehrungen zu machen. Die Hälfte der Unternehmen kommuniziert ohne jegliche Absicherung. Das Sicherheitsbewusstsein ist zwar vorhanden, die praktischen Maßnahmen bleiben jedoch aus. Vermutlich liegt es daran, dass viele Unternehmen überfordert sind. Teilweise sind viele der Meinung, dass der Schutz des Internet-Zugangs ausreiche. Dies ist gerade ein fataler Irrtum. Zwar gibt es einige wenige die Dokumente mit Passwörtern (acht Prozent) versehen, elektronische Signaturen und Verschlüsselungen (15 %) und Verschlüsselungen der Anhänge mit Passwörtern (15 %) nutzen. Trotzdem entwickeln sich die Zahlen rückläufig, sodass dringender Handlungsbedarf besteht. Diese Erkenntnisse liefert der „DsiN Sicherheitsmonitor - Mittelstand“ vom Verein Deutschland sicher im Netz, der zugleich auch Empfehlungen ausspricht, wie eine sichere E-Mail-Kommunikation gewährleistet werden kann.[167]

KMU sollten E-Mails grundsätzlich immer mit Hilfe von Verschlüsselungsverfahren und elektronischen Signaturen absichern. Um die Integrität und Authentizität der E-Mails zu gewährleisten, sollten elektronische Signaturen eingesetzt werden. Für die meisten Fälle ist die fortgeschrittene elektronische Signatur völlig ausreichend. Die qualifizierte elektronische Signatur wird wohl bei Rechtsgeschäften, da sie der gesetzlichen Schriftform unterliegen und diese durch die elektronische Form nach § 126a BGB ersetzt werden kann, zum Einsatz kommen. Hierbei gibt die BNetzA auf Basis einer Empfeh-

[164] *Bräutigam/Thalhofer* (2013), in: *Bräutigam et al.*, IT-Outsourcing und Cloud Computing, Teil 14, S. 1242 f. Rdnr. 97 ff.

[165] *Hoeren* (2015): Datenschutz in der Cloud: Probleme der Werbewirtschaft bei der Auslagerung von Daten auf amerikanische Cloud-Anbieter, S. 3.

[166] *Bräutigam/Thalhofer* (2013), in: *Bräutigam et al.*, IT-Outsourcing und Cloud Computing, Teil 14, S. 1247 Rdnr. 104.

[167] *DsiN* (2014): DsiN Sicherheitsmonitor - Mittelstand, S. 14 f. und S. 23.

lung des BSI jährlich eine Übersicht[168] aller für elektronische Signaturen geeigneten mathematischen Verfahren inkl. der notwendigen Schlüssellängen. Auch ungültige Signaturen werden hier aufgelistet. Als Alternative zu den Verschlüsselungsverfahren können verschlüsselte Anhänge (passwortgeschützt) als E-Mail versendet werden. Das Passwort sollte den Mindeststandard von acht bis zwölf Zeichen erfüllen, alphanummerisch sein und Groß- und Kleinschreibung enthalten. Dies ist zwar einfach umzusetzen, aber im Vergleich zu den Verschlüsselungsverfahren deutlich unsicherer.[169] Um die Vertraulichkeit sowie den Datenschutz zu gewährleisten und einzuhalten, sind Verschlüsselungsverfahren einzusetzen. Hierbei haben KMU keine festen Vorgaben, können sich aber an den Empfehlungen vom BSI orientieren. Auch der Einsatz von Cloud-Diensten ist zu empfehlen, wenn kein eigenes Know-how bezogen auf die Verschlüsselungstechniken vorhanden ist. Hierbei übernimmt der Cloud-Anbieter die Verantwortung für die Verschlüsselung, sodass E-Mails manuell oder auch automatisch verschlüsselt werden können. Dabei sollten KMU jedoch darauf achten, diese Daten separat zu verschlüsseln (bspw. mit einem Passwort zu schützen), da der Cloud-Anbieter aufgrund der Kenntnis des Verschlüsselungsverfahrens theoretisch Einblick in die Daten bekommen könnte.[170] Bei der clientbasierten Verschlüsselungslösung, auch bekannt unter der „Ende-zu-Ende-Verschlüsselung“, übernehmen die Endgeräte das Verschlüsseln, Entschlüsseln, Signieren und die Verifikation von Nachrichten. Durch diesen Ansatz wird eine durchgängige Verschlüsselung einer E-Mail über ihren gesamten Übertragungsweg gewährleistet. Für die Anwendung wird die nötige Software, aber auch das Fachwissen benötigt. Ebenso ist es mit einem hohen Administrationsaufwand verbunden. Problematisch bei diesem Konzept ist eine Virenprüfung, da die E-Mails aufgrund ihrer Verschlüsselung nicht auf ihren Inhalt geprüft werden können.[171] Für KMU ist dieses Konzept zwar nicht sehr interessant, da es mit einem hohen Aufwand verbunden ist und Fachwissen benötigt. Jedoch gibt es die Möglichkeit auf Cloud-Dienste mit denselben Funktionen zuzugreifen. Hier können KMU auf das Fachwissen zurückgreifen, den Administrationsaufwand sowie die Verantwortung für die Ver- und Entschlüsselung von E-Mails dem Cloud-Anbieter überlassen. Bei der Wahl des richtigen Cloud-Anbieters sollten Zertifikate herangezogen werden, die belegen, dass Sicherheitsstandards eingehalten werden. Außerdem sollten sich die Rechenzentren aus Sicherheitsgründen in Deutschland befinden.[172] Neben den Cloud-Diensten können auch andere Service-Provider als Lösung genutzt werden, falls die Nutzung einer eigenen Verschlüsselungsinfrastruktur nicht in Frage kommt. Hier sind der E-Postbrief und die De-Mail zu nennen. Bei diesen Lösungen geht es vielmehr um eine rechtssichere, datenschutzkonforme und nachweisbare digitale Kommunikation. Hierbei ist die Verschlüsselung der E-Mails ein Nebenprodukt und steht somit nicht im Vordergrund. Diese Dienste sollen das Einschreiben im Briefverkehr zu Behörden oder Vertragspartnern ersetzen. Für die Nutzung wird ein Konto benötigt, das gleichzeitig die Echtheit des Kontoinhabers verifiziert. Das De-Mail-Konzept, ist ein staatlich gefördertes Vorhaben des BMI, das sogar Einklang in einem speziellen Gesetz (De-Mail-Gesetz) gefunden hat. Das De-Mail-Gesetz trat am 03.05.2011 in Kraft. Hierbei sollen die entsprechenden Dienstleistungen von akkreditierten privaten Unternehmen angeboten werden. Die

---

[168] http://www.bundesnetzagentur.de/cln_1911/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/AufsichtundAkkreditierungvonAnbietern/ ZertifizierungsDiensteAnbietr_node.html.

[169] *DATEV* (2013): Verschlüsselung von E-Mails, S. 15.

[170] *DATEV* (2013): Verschlüsselung von E-Mails, S. 14.

[171] *DATEV* (2013): Verschlüsselung von E-Mails, S. 16.

[172] *DATEV* (2013): Verschlüsselung von E-Mails, S. 17.

Anbieter orientieren sich an den gesetzlichen Rahmen, sodass die Ausgestaltung der De-Dienste und Funktionen sich von Anbieter zu Anbieter unterscheiden können.

Obwohl genügend Möglichkeiten zur Erhöhung der E-Mail-Sicherheit vorhanden sind, stellt sich die Frage, wieso dies in der Praxis nicht umgesetzt werden kann. Zum einen müssen Cloud-Anbieter oder Service-Provider ihre Angebote so gestalten, dass sie für jeden transparent, einfach zu handhaben, aber zugleich umfangreich und komplex genug sind, um den Anforderungen einer hohen E-Mail-Sicherheit gerecht zu werden. Zum anderen ist auch die Politik gefragt. Hierbei hat sie bereits erste Erfolge (De-Mail-Gesetz) verzeichnen können. Auch das kommende nationale IT-Gesetz wird wohl einige rechtliche Änderungen mit sich bringen. Auf europäischer Ebene bleibt weiterhin abzuwarten, welche Auswirkungen die kommende EU-DSGVO auf die Anbieter und auch Nutzer haben wird. Dennoch wird die rechtliche Verankerung von „Privacy by design“ und „Privacy by default“ die Software-Branche dazu verpflichten, bereits bei der Entwicklung von Software-Produkten ausreichende Sicherheitsvorkehrungen zu treffen und in die Systeme einzubetten.

F. Ausblick auf die Zukunft der IT-Sicherheit

Die IT-Sicherheit wird der Schlüssel für den Erfolg von Big Data, Cloud Computing, Industrie 4.0 und dem Internet der Dinge sein. Der Bedarf und die Anforderungen werden stetig ansteigen und im weiteren Zeitverlauf den Trend nach oben beibehalten. Somit wird sich der Markt für IT-Sicherheit in den nächsten Jahren aufgrund der Markttreiber Politik, technologische Trends und Wirtschaft positiv entwickeln. Deutschland ist als Standort sehr gut und hat auch weiterhin gute Chancen im internationalen Wettbewerb Schritt zu halten. Nur müssen hierfür die richtigen Maßnahmen eingeleitet werden, damit auch das Vertrauen in die Möglichkeiten der IT weiterhin bestehen bleibt. Besonders der Mittelstand muss gefördert werden, da hier die Ausgaben für IT-Sicherheit in den letzten Jahren gesunken sind, obwohl die Gefahren und Risiken bekannt sind[173]. Auch die Politik setzt sich viel zu wenig in Bezug auf die Belange von KMU ein. Besonders bei der Entwicklung eines IT-Sicherheitsgesetzes wird nicht explizit auf die KMU eingegangen, obwohl dies notwendig erscheint. Hier wäre eine klare Differenzierung zwischen KMU und Großunternehmen wünschenswert, um den unterschiedlichen Anforderungen gerecht zu werden.[174] Auch auf europäischer Ebene wird die kommende EU-DSGVO einiges an Veränderungen bringen, auf die sich die Unternehmen einstellen können. Ebenso wird die Grundidee des Security by design-Ansatzes sicherlich dazu beitragen, die IT-Sicherheit bei Anwendungen und virtuellen Infrastrukturen zu verbessern. Hierbei wird jedoch der Fokus eher bei den Anbietern liegen. Erwähnenswert sind auch die politischen Anstrengungen bzgl. nationalen und europäischen Forschungsprojekten im Hinblick auf die IT-Sicherheit, insb. von KMU. Aufgrund der staatlichen Unterstützung sind diese erst möglich geworden und werden im Laufe der nächsten Jahre die wesentlichen Erkenntnisse liefern, um die IT-Sicherheit in Unternehmen zu erhöhen bzw. zu verbessern. Trotzdem darf nicht vergessen werden, dass es nie eine 100%ige Garantie geben wird, dass Systeme, Anwendungen oder virtuelle Infrastrukturen sicher sind. Der Grund hierfür ist, dass sich die technologischen Entwicklungen ständig im Wandel befinden und auch die Gefahren und Risiken sich stetig weiterentwickeln bzw. verändern.

---

[173] *PwC* (2014): Managing cyber risks in an interconnected world, S. 9 f.

[174] *BITKOM* (2014): Der IT-Mittelstand in Deutschland, S. 27 f.

Literaturverzeichnis

Adobe (2015), Adobe Creative Cloud / Häufig gestellte Fragen, online unter: https://www.adobe.com/content/dotcom/de/products/creativecloud/faq.html#what-cc [Abruf: 04.04.2015].

Adobe (2015), Adobe Creative Cloud-Hilfe / Häufig gestellte Fragen zu Creative Cloud und Behance, online unter: https://helpx.adobe.com/de/creative-cloud/kb/behance-integration-faq.html [Abruf: 04.04.2015].

Adobe (2015), Corporate Fact Sheet, Adobe im Überblick, online unter: http://www.adobe.com/de/company/fast-facts.html [Abruf: 05.04.2015].

Adobe (2014), Datenschutzzentrum von Adobe / Datenschutzrichtlinie von Adobe, online vom 08.12.2014 unter: http://www.adobe.com/de/privacy/policy.html#cover [Abruf: 06.04.2015].

Adobe (2015), Legal information / Allgemeine Nutzungsbedingungen von Adobe, online unter: http://www.adobe.com/de/legal/general-terms.html [Abruf: 07.04.2015].

Arbeitskreis Industrie 4.0 (2013), Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Deutschlands Zukunft als Produktionsstandort sichern, Abschlussbericht des Arbeitskreises Industrie 4.0, online vom April 2013 unter: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Abschlussbericht_Industrie4.0_barrierefrei.pdf [Abruf: 09.03.2015].

Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder; Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises (2014), Orientierungshilfe Cloud Computing, online vom 09.10.2014 unter: https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf [Abruf: 17.01.2015].

Art. 29-Datenschutzgruppe (2012), Stellungnahme 5/2012 zum Cloud Computing, online vom 01.07.2012 unter: https://www.lda.bayern.de/lda/datenschutzaufsicht/ lda_daten/WP169_CloudComputing.pdf [Abruf: 17.02.2015].

Bachmann, Ronald; Kemper, Guido; Gerzer, Thomas (2014), Big Data – Fluch oder Segen?, Unternehmen im Spiegel gesellschaftlichen Wandels, 1. Auflage, Heidelberg: mitp Verlag.

Baron, Pavlo (2013), Big Data für IT-Entscheider, Riesige Datenmengen und moderne Technologien gewinnbringend nutzen, München: Carl Hanser Verlag.

Baun, Christian; Kunze, Marcel; Nimis, Jens; Tai, Stefan (2011), Cloud Computing: Web-basierte dynamische IT-Services (Informatik im Fokus), 2. Auflage, Berlin: Springer-Verlag.

Bendrath, Ralf (2015), TTIP und TISA: Die USA wollen Datenschutz wegverhandeln, online vom 11.02.2015 unter: https://netzpolitik.org/2015/ttip-und-tisa-die-usa-wollen-datenschutz-wegverhandeln/ [Abruf 23.02.2015].

Beuth, Patrick (2015), Bundesregierung hofiert Lobbyisten, online vom 10.03.2015 unter: http://www.zeit.de/digital/datenschutz/2015-03/eu-datenschutzgrundverordnung-ministerrat-bundesregierung-lobbyplag [25.02.2015].

Biselli, Anna (2015), Leak zeigt: Handelsabkommen TiSA könnte nationale Datenschutzbestimmungen aushebeln, online vom 17.12.2014 unter: https://netzpolitik.org/2014/leak-zeigt-handelsabkommen-tisa-koennte-nationale-datenschutzbestimmungen-aushebeln/ [Abruf: 27.02.2015].

BITKOM (2013), Bring Your Own Device, online vom 11.04.2013 unter: http://www.bitkom.org/files/documents/20130404_LF_BYOD_2013_v2.pdf [Abruf: 14.03.2015].

BITKOM (2014), Der IT-Mittelstand in Deutschland, Mittelstandsbericht 2014, online vom 14.10.2014 unter: http://www.bitkom.org/files/documents/ 20141017_ mittelstandsbericht.pdf [Abruf: 18.05.2015].

BITKOM (2014), IT-Strategie – Digitale Agenda für Deutschland, Deutschland zum Digitalen Wachstumsland entwickeln., online vom 27.03.2014 unter: http://www. bitkom.org/files/documents/BITKOM_IT-Strategie.pdf [Abruf: 07.01.2015].

BITKOM (2014), Potenziale und Einsatz von Big Data, Ergebnisse einer repräsentativen Befragung von Unternehmen in Deutschland, online vom 05.05.2014 unter: https://www.bitkom.org/files/documents/Studienbericht_Big_Data_in_deutschen_Unternehmen.pdf [Abruf: 07.03.2015].

BITKOM Presseinformation (2014), Deutscher IT-Markt wächst 2015 um 2,4 %, online vom 10.12.2014 unter: http://www.bitkom.org/de/presse/81149_81011.aspx [Abruf: 19.01.2015].

BITKOM Presseinformation (2014), Fast ein Drittel der Unternehmen verzeichnet Cyberangriffe, online vom 11.03.2014 unter: http://www.bitkom.org/de/presse/ 81149_78903.aspx [Abruf: 07.01.2015].

BITKOM Presseinformation (2014), Markt für Cloud Computing wächst ungebrochen, online vom 06.11.2014 unter: http://www.bitkom.org/de/presse/81149_80724.aspx [Abruf: 19.01.2015].

BITKOM; Frauenhofer-Institut für Arbeitswirtschaft und Organisation (IAO) (2014), Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland, online unter: http:// www.bitkom.org/files/documents/Studie_Industrie_4.0.pdf [Abruf: 11.03.2015].

BITKOM Research; KMPG (2014), Cloud-Monitor 2014, online vom 11.03.2014 unter: http://www.bitkom.org/files/documents/Cloud_Monitor_2014_KPMG_Bitkom_Research.pdf [Abruf: 19.01.2015].

BITKOM Reseach; KMPG (2015), Cloud-Monitor 2015, online vom 21.04.2015 unter: http://www.bitkom.org/files/documents/Cloud_Monitor_2015_KPMG_Bitkom_Research.pdf [Abruf: 22.05.2015].

Boston Consulting Group (BCG) (2013), Der Zeit voraus, Der Einfluss neuer Technologien auf den Erfolg führender KMU, online vom Oktober 2013 unter: http://www.bcg.de/documents/file151680.pdf [Abruf: 02.02.2015].

BCG (2015), Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries, online vom April 2015 unter: https://www.bcgperspectives.com/ Images/Industry_40_Future_of_Productivity_April_2015_tcm80-185183.pdf [Abruf: 16.05. 2015].

BCG Pressemitteilung (2015), Deutscher Arbeitsmarkt profitiert von positiven Effekten durch Industrie 4.0, online vom 09.04.2015 unter: http://www.bcg.de/ media/PressReleaseDetails.aspx?id=tcm:89-185709 [Abruf: 17.04.2015].

BCG Pressemitteilung (2014), Industrie 4.0 sichert deutschen Unternehmen langfristigen Spitzenplatz, online vom 21.11.2014 unter: http://www.bcg.de/media/ PressReleaseDetails.aspx?id=tcm:89-177192 [Abruf: 16.04.2015].

Bräutigam, Peter (Hrsg.) et al. (2013), IT-Outsourcing und Cloud-Computing, Eine Darstellung aus rechtlicher, technischer, wirtschaftlicher und vertraglicher Sicht, 3. völlig neu bearbeitete und erweiterte Auflage, Berlin: Erich Schmidt Verlag GmbH & Co KG.

Bundeskartellamt (2005), B 7 – 162/05, Fusionsverfahren gemäß § 40 Abs. 2 GWB, Beschluss in dem Verwaltungsverfahren zwischen Adobe und Macromedia wegen Prüfung eines Zusammenschlussvorhabens nach § 36 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB), online vom 23.12.2005 unter: http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Fusionskontrolle/ 2005/B7-162-05.pdf?__blob=publicationFile&v=3 [Abruf: 23.03.2015].

Bundesministerium des Innern (BMI) (Nachrichten) (2015), „Wir wollen die deutschen IT-Systeme zu den sichersten in der Welt machen", online vom 20.03.2015 unter: http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2015/03/erste-lesung-it-sicherheitsgesetz-im-bundestag.html?nn=3446780 [Abruf: 13.05.2015].

Bundesministerium für Bildung und Forschung (BMBF) (2015), Big Data – Management und Analyse großer Datenmengen, online vom 16.03.2015 unter: http://www.bmbf.de/de/23429.php [Abruf: 26.03.2015].

BMBF (2015), Selbstbestimmt und sicher in der digitalen Welt 2015-2020, online vom 11.03.2015 unter: http://www.bmbf.de/pub/Forschungsrahmenprogramm_ IT_ Sicherheit.pdf [Abruf: 27.03.2015].

BMBF Pressemitteilung (2015), Forschung für Big Data und IT-Sicherheit neu aufgestellt, online vom 10.03.2015 unter: http://www.bmbf.de/_media/press/Pm0310-018%281%29.pdf [Abruf: 28.03.2015].

Bundesministerium für den Datenschutz und die Informationsfreiheit (BfDI) (2015), Die Reform des Europäischen Datenschutzrechts, online unter: http://www.bfdi.bund.de/DE/Europa_International/Europa/Reform_Datenschutzrecht/ReformEUDatenschutzrechtArtikel/ReformEUDatenschutzRecht.html;jsessionid=AFDFAA7E8451773EB8FF46BD78AF14DF.1_cid344?cms_sortOrder=score+desc&cms_templateQueryString=eu+datenschutz+grundverordnung [Abruf: 24.02.2015].

Bundesministerium für den Datenschutz und die Informationsfreiheit (BfDI) Pressemitteilungen (2015), Andrea Voßhoff: Die EU Kommission muss jetzt Klartext reden!, online vom 27.01.2015 unter: http://www.bfdi.bund.de/DE/Infothek/ Pressemitteilungen/2015/01_AndreaVosshoffDieEUKommissionMussJetztKlartextReden.html [Abruf: 23.02.2015].

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2015), Cloud Zertifizierung, online unter: https://www.bsi.bund.de/DE/Themen/CloudComputing/ CloudZertifizierung/CloudZertifizierung_node.html [Abruf: 11.05.2015].

BSI (2014), Die Lage der IT-Sicherheit in Deutschland 2014, online vom 15.12.2014 unter: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html [Abruf: 07.02.2015].

BSI (2013), Mobile Device Management, online vom 13.03.2013 unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/anwender/ mobilesec/BSI-CS_052.pdf;jsessionid=82C1A8362A315B162469F33FF1A644D6.2_cid369?__blob=publicationFile [Abruf: 16.05.2015].

BSI (2006), Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen, online vom 21.11.2006 unter: https://www.bsi.bund.de/DE/Publikationen/Broschuren/Mobile/ mobileendgeraete.html [Abruf: 17.05.2015].

BSI (2011), Sicherheitsempfehlungen für Anbieter, Mindestanforderungen in der Informationssicherheit, online vom 10.05.2011 unter: https://www.bsi.bund.de/DE/ Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html [Abruf: 13.04.2015].

Bundesministerium für Wirtschaft und Energie (BMWi) (2014), Firmendaten: Wie sicher ist ihr Unternehmen?, Praktische Informationen für einen besseren Schutz ihrer IT-Systeme, online vom Februar 2014 unter: http://www.bmwi.de/DE/Mediathek/publikationen,did=624912.html [Abruf: 25.04.2015].

BMWi (2015), Häufig gestellte Fragen zur Transatlantischen Handels- und Investitionspartnerschaft (TTIP), online vom Januar 2015 unter: http://www.bmwi.de/DE/ Themen/ Aussenwirtschaft/Freihandelsabkommen/TTIP/faqs.html [Abruf: 18.02.2015].

BMWi (2015), TiSA: Verhandlungen und Akteure, online unter: http://www.bmwi.de/DE/Themen/Aussenwirtschaft/Freihandelsabkommen/TiSA/tisa-verhandlungen-und-akteure.html [Abruf: 19.02.2015].

Bundesverband mittelständische Wirtschaft e. V. (BVMW) (2014), Positionspapier EU-Datenschutz-Grundverordnung, online vom November 2014 unter: http://www.bvmw.de/fileadmin/download/Downloads_allg._Dokumente/politik/positionspapiere/positionspapier_eu-datenschutz-grundverordnung.pdf [Abruf: 19.02.2015].

Business Software Alliance (BSA) (2013), Global Cloud Computing Scorecard, A Clear Path to Progress, online vom März 2013 unter: http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf [Abruf: 09.02.2015].

Cavoukian, Ann (2011), Privacy by Design, die 7 Grundprinzipien, online vom Februar 2011 unter: https://www.privacybydesign.ca/content/uploads/2009/08/ 7foundational principles-german.pdf [Abruf: 13.05.2015].

Center for Strategic and International Studies (CSIS); McAfee (2014), Net Losses: Estimating the Global Cost of Cybercrime, online vom Juni 2014 unter: http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf [Abruf: 13.02.2015].

CIO (2015), Wolkige Aussichten: Softwarefirmen suchen Heil in Mietsoftware, online vom 20.01.2015 unter: http://www.cio.de/a/softwarefirmen-suchen-heil-in-miet software, 3092363 [Abruf: 11.05.2015].

Clauß, Ulrich (2014), Cybercrime schadet Deutschland am stärksten, online vom 09.06.2014 unter: http://www.welt.de/politik/deutschland/article128845865/ Cybercrime-schadet-Deutschland-am-staerksten.html [Abruf: 17.02.2015].

Corporate Trust (2014), Studie: Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co?, online vom 23.10.2014 unter: http://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf [Abruf: 26.01.2015].

CSC Pressemitteilung (2015), Industrie-4.0–Studie: Deutsche Firmen setzen Vorsprung aufs Spiel, online vom 15.01.2015 unter: http://www.csc.com/de/press_releases/117841-industrie_4_0_studie_deutsche_firmen_setzen_vorsprung _aufs_spiel [Abruf: 30.03.2015].

Datenschutz Praxis (2015), Datenschutz-Grundverordnung: Viele Unternehmen sind nicht vorbereitet, online vom 29.01.2015 unter: https://www.datenschutz-praxis.de/fachnews/datenschutz-grundverordnung-viele-unternehmen-sind-nicht-vorbereitet/ [Abruf: 26.02.2015].

DATEV (2013), Verschlüsselung von E-Mails, Leitfaden zur E-Mail-Sicherheit für Unternehmen, online vom 05.07.2013 unter: http://www.datev.de/portal/ ShowContent.do?pid=dpi&cid=218150 [Abruf: 18.05.2015].

Dell Pressemitteilung (2014), Dell-Studie: Die Wahrheit über Sicherheit, Cloud, Mobility und Big Data, online vom 05.11.2014 unter: http://www.dell.com/learn/de/de/decorp1/press-releases/2014-11-05-dell-global-technology-adoption-index [Abruf: 20.01.2015].

Dettling, Jürgen; Eberhardt, Michael (2011), Cloud Computing – IT-Dienste der nächsten Generation, in: Gründer, Torsten (Hrsg.): IT-Outsourcing in der Praxis, Strategien, Projektmanagement, Wirtschaftlichkeit, 2. völlig neu bearbeitete und erweiterte Auflage, Berlin: Erich Schmidt Verlag.

Deutsche Bank Research (2014), Big Data – Die ungezähmte Macht, online vom 04.03.2014 unter: https://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000328652/Big+Data+-+die+ungez%C3%A4hmte+Macht.pdf [Abruf: 08.04.2015].

Deutscher Bundestag Pressemitteilung (2015), Datenschutz als Wettbewerbsvorteil, Ausschuss Digitale Agenda, online vom 05.03.2015 unter: https://www.bundestag.de/presse/hib/2015_03/-/363820 [Abruf: 16.03.2015].

Deutschland sicher im Netz (DsiN) (2014), DsiN Sicherheitsmonitor – Mittelstand, online unter: https://www.sicher-im-netz.de/sites/default/files/media/dsin_ sicherheitsmonitor_2014_web.pdf [Abruf: 11.05.2015].

Däubler, Wolfgang; Klebe, Thomas; Wedde, Peter; Weichert, Thilo (2014), Bundesdatenschutzgesetz. Kompaktkommentar zum BDSG, 4. Auflage, Frankfurt a. M.: Bund-Verlag.

eBusiness-Lotse Oberschwaben-Ulm (2014), Leitfaden: Private Endgeräte geschäftlich nutzen, online vom Mai 2014 unter: http://www.mittelstand-digital.de/DE/ Wissenspool/unternehmensprozesse,did=640766.html [Abruf: 12.05.2015].

Eckert, Claudia (2014), IT-Sicherheit, Konzepte-Verfahren-Protokolle, 9. Auflage, München: Oldenbourg Wissenschaftsverlag GmbH.

Edlund, Patrik (2015), HP-Studie belegt: 70 Prozent der Unternehmen haben keine BYOD-Regeln, online vom 26.02.2015 unter: http://h30507.www3.hp.com/t5/HP-IT-Blog-f%C3%BCr-Deutschland/HP-Studie-belegt-70-Prozent-der-Unternehmen-haben-keine-BYOD/ba-p/180626#.VU3h3fBvWvB [Abruf: 13.05.2015].

Ege, Konrad (2012), Von Wolken und Schattenwelten, in: Fröschle, Hans-Peter (Hrsg.): Cloud-Service-Management – HMD – Praxis der Wirtschaftsinformatik, Heft 288, Heidelberg: dpunkt.verlag.

ENISA (2015), Privacy and Data Protection by Design – from policy to engineering, online vom 12.01.2015 unter: www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/at_download/fullReport [Abruf: 15.05.2015].

Eriksdotter, Holger (2011), Rechtsleitfaden für Cloud Computing, online vom 03.01.2011 unter: http://www.cio.de/a/rechtsleitfaden-fuer-cloud-computing, 2258171,2 [Abruf: 07.01.2015].

Europäische freie Allianz (EFA) (2015), EU-Datenschutzgrundverordnung: Stand der Dinge 10 wichtige Punkte, online vom 07.01.2015 unter: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Datenschutzreform_Stand_der_Dinge_10_Punkte_070115.pdf [Abruf: 18.02.2015].

Eurostat Pressemitteilung (2014), Internetnutzung von Personen im Jahr 2014, Jede fünfte Person nutzte Cloud Dienste zur Speicherung von Dateien, Kostenlose Dienste am häufigsten genutzt, online vom 16.12.2014 unter: http://ec.europa.eu/eurostat/documents/2995521/6343585/4-16122014-BP-DE.pdf/25edf9e7-ac25-46e4-bbf4-ff7bb29be250 [Abruf: 21.01.2015].

Eurostat Pressemitteilung (2014), Nutzung von IKT in Unternehmen im Jahr 2014, Jedes fünfte Unternehmen in der EU28 nutzt Cloud Computing Dienste, Unzureichende Kenntnisse waren der Hauptgrund für die Nichtnutzung von Cloud Diensten, online vom 09.12.2014 unter: http://ec.europa.eu/eurostat/documents/2995521/6208102/4-09122014-AP-DE.pdf/ 4a3fdeb8-d389-41a2-92cc-db541a45646e [Abruf: 17.02.2015].

Frauenhofer Institut für Sichere Informationstechnologie (SIT) (2012), Doppelsieg für IT Security made in Darmstadt, online vom 29.11.2012 unter: https://www.sit. fraunhofer.de/de/news/aktuelles/presse/details/news-article/doppelsieg-fuer-it-security-made-in-darmstadt/ [Abruf: 20.05.2015].

Frauenhofer SIT (2013), Trend- und Strategiebericht: Entwicklung sicherer Software durch Security by design, Stuttgart: Frauenhofer Verlag.

Frauenhofer SIT (2014), Whitepaper: OmniCloud – Sichere und flexible Nutzung von Cloud-Speicherdiensten, online unter: http://www.omnicloud.sit.fraunhofer.de/ download/omnicloud-whitepaper-de.pdf [Abruf: 21.05.2015].

Frauenhofer SIT (2012), Über die Sicherheit von Cloud-Speicherdiensten, Management Summary, online vom März 2012 unter: https://www.sit.fraunhofer.

de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_ManagementSummary.pdf [Abruf: 15.01.2015].

Frauenhofer Institut für Offene Kommunikationssysteme (FOKUS) (2011), ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, online vom 29.01.2010: http://www.cloud.fraunhofer.de/content/dam/allianzcloud/de/documents/ISPRAT_cloud_studievorabversion20101129tcm421-76759.pdf [Abruf: 14.01.2015].

Frauenhofer Institut für Intelligente Analyse- und Informationssysteme (IAIS) (2012), Big Data – Vorsprung durch Wissen, Innovationspotenzialanalyse, online vom Dezember 2012 unter: http://www.iais.fraunhofer.de/fileadmin/user_upload/ Abteilungen/KD/uploads_BDA/Innovationspotenzialanalyse_Big-Data_FraunhoferIAIS_2012.pdf [Abruf: 16.03.2015].

Frauenhofer Institut für angewandte und integrierte Sicherheitssysteme (AISEC); Arbeitsgruppe Cybersicherheit IMK (2013), Sicherheit mobile Endgeräte im Cyberraum, Leitfaden zur Sicherheit mobiler Endgeräte für Behörden und KMU, online vom 17.07.2013 unter: https://www.dvz-mv.de/cms2/DVZ_prod/DVZ/_Dateien/_Aktuell_Download/Vortraege_IT-Sicherheitstag_2013/00_leitfaden_sicherheit-mobiler-endgeraete-fuer-behoerden_fraunhofer_2013-07-17.pdf [Abruf: 17.05.2015].

Fröschle, Hans-Peter; Reinheimer, Stefan (Hrsg.) (2010), Cloud Computing & SaaS – HMD – Praxis der Wirtschaftsinformatik, Heft 275, Heidelberg: dpunkt.verlag.

Fröschle, Hans-Peter (Hrsg.) (2012), Cloud-Service-Management – HMD – Praxis der Wirtschaftsinformatik, Heft 288, 1. Auflage, Heidelberg: dpunkt.verlag.

Gartner, Inc. (2013), Gartner IT Glossary – Big Data, online unter: http://www.gartner.com/it-glossary/big-data [Abruf: 20.03.2015].

Glanz, James (2012), The Cloud Factories, Power, Pollution and the Internet, online vom 22.06.2012 unter: http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html?_r=1 [Abruf: 10.02.2015].

Google, Inc. (2014), Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild, online vom 07.11.2014 unter: http://conferences2.sigcomm.org/imc/2014/ papers/p347.pdf [Abruf: 30.04.2015].

Greenpeace (2014), Clicking Green: How Companies are creating the Green Internet, online vom April 2014 unter: http://www.greenpeace.org/usa/en/campaigns/global-warming-and-energy/A-Green-Internet/clickingclean/ [Abruf: 14.02.2015].

Haselmann, Till; Vossen, Gottfried (2010), Database-as-a-Service für kleine und mittlere Unternehmen, Ein praxistauglicher Leitfaden für KMU, die „in die Cloud gehen" möchten, online vom 25.11.2010 unter: http://www.wi1.uni-muenster.de/pi/iai/publikationen/DaaS-fuer-KMU.pdf [Abruf: 15.01.2015].

Heidrich, Joerg; Wegener, Christoph (2010), Sichere Datenwolken, in: MultiMedia und Recht (MMR), Zeitschrift für Informations-, Telekommunikations- und Medienrecht, Heft 12, München: Verlag C. H. Beck.

Herrmann, Wolfgang (2014), Cloud Computing – der deutsche Mittelstand hinkt hinterher, online vom 10.03.2014 unter: http://www.tecchannel.de/ wege_in_die_cloud/2053924/cloud_studie_tc_2014_tx/ [Abruf: 31.01.2015].

Hilber, Marc (Hrsg.) et al. (2014), Handbuch Cloud Computing, Köln: Verlag Dr. Otto Schmidt KG.

Hilber, Marc; Knorr, Gunnar; Müller, Stephan (2011), Serververlagerungen im Konzern, in: Computer und Recht (CR), Zeitschrift für die Praxis des Rechts der Informationstechnologien, Heft 7, Köln: Verlag Dr. Otto Schmidt KG.

Hildebrand, Knut; Meinhardt, Stefan (Hrsg.) (2014), Systemkonsolidierung & -migration, HMD – Praxis der Wirtschaftsinformatik, Heft 296, 1. Auflage, Heidelberg: Springer Verlag.

Hoeren, Thomas (2015), Datenschutz in der Cloud: Probleme der Werbewirtschaft bei der Auslagerung von Daten auf amerikanische Cloud-Anbieter, in: Konitzer, Michael-A. (Hrsg.), Annual Multimedia, Berlin: Walhalla und Praetoria Verlag.

IBM Institute for Business Value; Saïd Business School (University of Oxford) (2012), Analytics: Big Data in der Praxis, Wie innovative Unternehmen ihre Datenbestände effektiv nutzen, online unter: http://www-935.ibm.com/services/de/gbs/thought leadership/GBE03519-DEDE-00.pdf [Abruf: 20.04.2015].

Institut für Mittelstandsforschung Bonn (IfM-Bonn) (2015), KMU-Definition der Europäischen Kommission, online unter: http://www.ifm-bonn.org/mittelstandsdefinition/ definition-kmu-der-eu-kommission/ [Abruf: 27.03.2015].

IfM-Bonn (2015), KMU-Definition des IfM-Bonn, online unter: http://www.ifm-bonn.org/mittelstandsdefinition/definition-kmu-des-ifm-bonn/ [Abruf: 27.03.2015].

IfM-Bonn (2014), Mittelstand im Wandel, IfM-Material Nr. 232, online vom Oktober 2014 unter: http://www.ifm-bonn.org/fileadmin/data/redaktion/publikationen/ ifm_ materialien/dokumente/IfM-Materialien-232_2014.pdf [Abruf: 22.01.2015].

International Data Corporation (IDC); TA Triumph-Adler GmbH (2015), Future Business World 2025 – Wie die Digitalisierung unsere Arbeitswelt verändert, online vom März 2015 unter: https://www.talking-future.de/downloads/idc-ta-white-paper-future-business-world-de.pdf [Abruf: 19.04.2015].

Jones, Chris (2014), OneDrive delivers unlimited cloud storage to Office 365 subscribers, in: The OneDrive Blog, online vom 27.10.2014 unter: https://blog. onedrive.com/office-365-onedrive-unlimited-storage/ [Abruf: 20.05.2015].

Kienbaum Management Consultants GmbH; BMWi (2014), Berücksichtigung von KMU-Belangen in der Gesetzesfolgenabschätzung, Endbericht, online vom 04.06.2014 unter: http://www.bmwi.de/DE/Mediathek/publikationen,did=645686.html [Abruf: 09.01.2015].

KPMG (2014), Ein Meer an Daten, ein Mehr an Wissen, Eine empirische Studie zum Einsatz von Big Data im Controlling, online vom 18.11.2014 unter: http://www.kpmg.com/DE/de/Documents/Big-Data-Studie_Meer-An-Daten-sec.pdf [Abruf: 14.04.2015].

Krüger, Alfred (2015), Schutz vor Datenklau: Forscher simulieren Pishing-Angriffe auf Firmen, in: ZDF heute, online vom 21.02.2015 unter: http://www.heute.de/schutz-vor-datenklau-forscher-simulieren-phishing-angriffe-auf-unternehmen-37269082.html [Abruf: 18.05.2015].

Kunisch, Matthias (2015), Drei Modelle für Cloud-Marktplätze, in: ComputerWoche, online vom 11.03.2015 unter: http://www.computerwoche.de/a/drei-modelle-fuer-cloud-marktplaetze,3090119 [Abruf: 16.05.2015].

Labes, Stine; Zarnekow, Rüdiger (Hrsg.) (2013), Rechtliche Rahmenbedingungen von Cloud Computing, rechtliche Situation im Öffentlichen Sektor, Projektberichte IKM, Band 10, Technische Universität Berlin, online vom 22.11.2013 unter: https://opus4.kobv.de/opus4-tuberlin/files/4131/projektberichte_IKM_10.pdf [Abruf: 07.01.2015].

Leonhard, Woody (2015), Gescheiterte Office-Suiten: Diese Konkurrenten vernichtete Microsoft Office, online vom 08.02.2015 unter: http://www.pcwelt.de/ratgeber/ Diese_Konkurrenten_vernichtete_Microsoft_Office_-Gescheiterte_Office-Suiten-8774535.html [Abruf: 24.04.2015].

Maier, Astrid; Student, Dietmar (2015), Industrie 4.0 – der große Selbstbetrug, online vom 13.02.2015 unter: http://www.manager-magazin.de/magazin/artikel/digitale-revolution-industrie-4-0-ueberfordert-deutschen-mittelstand-a-1015724-4.html [Abruf: 16.03.2015].

Manhart, Klaus (2015), Was ist was bei der Cloud-Zertifizierung?, online vom 14.01.2015 unter: http://www.cio.de/a/was-ist-was-bei-der-cloud-zertifizierung, 3101823 [Abruf: 06.03.2015].

Matzer, Michael (2014), Der deutsche Cloud-Markt wächst, doch die Fertigungsindustrie hinkt hinterher, online vom 05.09.2014 unter: http://www.vdi-nachrichten.com/Technik-Wirtschaft/Der-deutsche-Cloud-Markt-waechst-Fertigungsindustrie-hinkt-hinterher [Abruf: 19.01.2015].

Metzger, Christian; Reitz, Thorsten; Villar, Juan (2011), Cloud Computing, Chancen und Risiken aus technischer und unternehmerischer Sicht, München: Carl Hanser Verlag.

Microsoft (2015), Das Unternehmen Microsoft / Fast Facts, online unter: http://www.microsoft.com/de-de/corporate/ueber-uns/ [Abruf: 15.04.2015].

Microsoft (2015), Hilfe und Support / Alle Produkte, online unter: https://support. microsoft.com/de-de/product/allproducts [Abruf: 15.04.2015].

Microsoft (2015), Microsoft Office 365 - Datenblatt, online unter: http://officecloud. de/docs/Office365_Datenblatt.pdf [Abruf: 15.04.2015].

Microsoft (2015), Office 365 / Häufig gestellte Fragen zu Office 365, online unter: http://products.office.com/de-de/microsoft-office-for-home-and-school-faq [Abruf: 15.04.2015].

Microsoft (2015), Office 365 / Häufig gestellte Fragen zu Office 365 Business, online unter: http://products.office.com/de-de/business/microsoft-office-365-frequently-asked-questions [Abruf: 15.04.2015].

Moutafis, Jannis (2014), Der lange Weg zum EU-weiten Cloud-Recht, online vom 23.11.2014 unter: http://www.computerwoche.de/a/der-lange-weg-zum-eu-weiten-cloud-recht,3066024 [Abruf: 26.02.2015].

Müller, Klaus-Rainer (2008), IT-Sicherheit mit System: Sicherheitspyramide, Sicherheits-, Kontinuitäts- und Risikomanagement, Normen und Practices, SOA und Softwareentwicklung, 3. erweiterte und aktualisierte Auflage, Wiesbaden: Vieweg+Teubner Verlag.

Nationale Initiative für Informations- und Internet-Sicherheit e. V. (NIFIS) (2014), Studie: IT-Sicherheit und Datenschutz 2015, online vom 26.11.2014 unter: http://www.nifis.de/fileadmin/docs/NIFIS_Studie_IT-Sicherheit_und_Datenschutz_2015.pdf [Abruf: 26.02.2015].

NetApp Deutschland (2014), Kalkuliertes Risiko? Datensicherheit im Mittelstand überraschend fahrlässig, online vom 08.12.2014 unter: http://www.netapp.com/de/ company/news/press-releases/news-rel-20140812-520909.aspx [Abruf: 12.05.2015].

Niemann, Fabian; Paul, Jörg-Alexander (2009), Bewölkt oder wolkenlos – rechtliche Herausforderung des Cloud Computings, in: Kommunikation & Recht (K&R), Heft 7/8, Frankfurt a. M.: Deutscher Fachverlag

Nägele, Thomas; Jacobs, Sven (2010), Rechtsfragen des Cloud Computing, in: Zeitschrift für Urheber- und Medienrecht (ZUM), Heft 4, München: Nomos Verlag.

Ohlhorst, Frank (2013), Big Data Analytics, New Jersey (USA): John Wiley & Sons, Inc.

Pierre Audion Consultants (PAC) (2014), Arbeitsplätze in der Wolke?! Cloud-basierte Kommunikation und Zusammenarbeit in deutschen Unternehmen, Executive Summary, online vom 21.10.2014 unter: http://blog.qsc.de/wp-content/uploads/ 2014/10/ PAC_Studie_Arbeitsplaetze_in_der_Wolke _ExecutiveSummary.pdf [Abruf: 09.05.2015].

Presseportal (2014), 9,23 Mrd. Euro wird das Cloud Computing-Marktvolumen 2015 betragen, online vom 10.07.2014 unter: http://www.presseportal.de/pm/ 23295/2781159 [Abruf: 26.01.2015].

Poguntke, Werner (2007), Basiswissen IT-Sicherheit, Das Wichtigste für den Schutz von Systemen & Daten, Witten: W3L GmbH.

Pohle, Jan; Ammann, Thorsten (2009), Über den Wolken… - Chancen und Risiken des Cloud Computing, in: Computer und Recht (CR), Zeitschrift für die Praxis des Rechts der Informationstechnologien, Heft 5, Köln: Verlag Dr. Otto Schmidt KG.

Ponemon Institute; SafeNet (2014), The Challenges of Cloud Information Governance: A Global Data Security Study, online vom Oktober 2014 unter: http://www2.safenet-inc.com/cloud-security-research/SafeNet-Cloud-Governance.pdf?utm_source=102714-pr&utm_medium=pr&utm_campaign=cloud-security-study [Abruf: 12.02.2015].

PricewaterhouseCoopers (PwC) (2013), Cloud Computing – Evolution in der Wolke, online vom März 2013 unter: http://www.pwc.de/de_DE/de/prozessoptimierung/ assets/evolution-in-der-wolke-reifegrad-der-cloud-services-steigt2.pdf [Abruf: 07.02.2015].

Projektträger für das Bundesministerium für Bildung und Forschung (2014), Big Data, online vom 29.08.2014 unter: http://www.pt-it.pt-dlr.de/de/big-data.php [Abruf: 07.05.2015].

Pröhl, Thorsten; Repschläger, Jonas; Erek, Koray; Zarnekow, Rüdiger (2012), IT-Servicemanagement im Cloud Computing, in: Fröschle, Hans-Peter (Hrsg.): Cloud-Service-Management – HMD – Praxis der Wirtschaftsinformatik, Heft 288, 1. Auflage, Heidelberg: dpunkt.verlag.

PwC (2014), Industrie 4.0 – Chancen und Herausforderungen der vierten industriellen Revolution, online vom Oktober 2014 unter: https://www.pwc.de/de/publikationen/paid_pubs/PwC_Studie_Industrie_4.0_141022_SCREEN_GESCHUETZT.pdf [Abruf: 10.03.2015].

PwC (2014), Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security Survey 2015, online vom 30.09.2014 unter: https://www.pwc.de/de/publikationen/paid_pubs/pwc_managing_cyber_risks_in_an_interconnected_world_2014.pdf [Abruf: 05.05.2015].

PwC (2014), Revolution Big Data, online vom Mai 2014 unter: https://www.pwc.de/de/publikationen/paid_pubs/pwc_revolution_big_data_2014.pdf [Abruf: 27.04.2015].

PwC (2015), Tax4Cloud: Steuerrechtliche Herausforderungen des Cloud-Computing, online unter: http://www.pwc.de/de/technologie-medien-und-telekommunikation/tax4cloud_steuerrechtliche-herausforderungen-des-cloud-computing.jhtml [Abruf: 30.04.2015].

Ramli, David (2013), Adobe cuts Australian prices after inquiry summons, in: The Australian Financial Review, online vom 12.02.2013 unter: http://www.afr.com/ technology/enterprise-it/adobe-cuts-australian-prices-after-inquiry-summons-20130212-ji8wb [Abruf: 03.04.2015].

Research in Motion (RIM) (2013), Die Kontrolle über ihre Cloud Apps zurückgewinnen: Welche SLAs bieten ihnen wirklich Schutz?, online vom Dezember 2013, unter: http://www.compuware.com/content/dam/compuware/apm/assets/pdfs/Cloud-Studie_Welche%20SLAs_bieten%20Ihnen_wirklich%20Schutz_WP_DE.pdf [Abruf: 10.02.2015].

Rieth, Sabine (2013), Europäischer Datenschutztag 2013 – Risiken bei Cloud Service-Angeboten genau prüfen (Pressemitteilung der TÜV Rheinland AG), online vom 24.01.2013, unter: http://www.presseportal.de/pm/31385/2403444/europaeischer-datenschutztag-2013-risiken-bei-cloud-service-angeboten-genau-pruefen-tuev-rheinland [Abruf: 21.02.2015].

Ritall (2014), Whitepaper von IDC und Rittal: Rechenzentren werden immer mehr zum Wettbewerbsfaktor, online vom 23.07.2014, unter: http://www.rittal.com/de-de/content/de/unternehmen/presse/pressemeldungen/pressemeldung_detail_63104.jsp [Abruf: 31.01.2015].

Rubin, Aviel (2002), Hackerabwehr und Datensicherheit, Angriff, Diagnose, Abwehr., Bonn: Addison-Wesley.

Sage Pressemitteilung (2014), Sage-Studie: Deutsche Unternehmer schöpfen Potenzial der Cloud noch nicht aus, online vom 25.09.2014, unter: http://www.sage.de/header/presse/pressemitteilungen/2014/09/25/cloud-studie [Abruf: 09.02.2015].

Schlak, Martin (2015), Industrie 4.0: Was die Roboter der Zukunft können, in: Spiegel Online, online vom 13.04.2015, unter: http://www.spiegel.de/wirtschaft/ unternehmen/hannover-messe-industrie-4-0-und-internet-der-dinge-a-1027553.html [Abruf: 17.04.2015].

Schneider, Jochen (Hrsg.) et al. (2015), ENISA: Empfehlungen für Privacy by design, in: Zeitschrift für Datenschutz (ZD): 5. Jahrgang, Heft 2, 31.01.2015, München: Verlag C. H. Beck.

Schonschek, Oliver (2014), Cloud-Zertifizierung: Noch keine Einheitlichkeit in Sicht, online vom 30.06.2014, unter: https://www.datenschutz-praxis.de/fachartikel/cloud-zertifizierung-keine-einheitlichkeit/ [Abruf: 07.03.2015].

Schuster, Fabian; Reichl, Wolfgang (2010), Cloud Computing & SaaS: Was sind die wirklichen neuen Fragen?, in: Computer und Recht (CR), Zeitschrift für die Praxis des Rechts der Informationstechnologien, Heft 1, Köln: Verlag Dr. Otto Schmidt KG.

Schödwell, Björn; Labes, Stine; Zarnekow, Rüdiger (2014), Herausforderungen und Erfolgsfaktoren der Migration in eine Community Cloud für die öffentliche Verwaltung, in: Hildebrand, Knut; Meinhardt, Stefan (Hrsg.): Systemkonsolidierung & -migration, HMD – Praxis der Wirtschaftsinformatik, Heft 296, 1. Auflage, Heidelberg: Springer Verlag.

Sophos Pressemitteilung (2015), IT-Sicherheit in KMU: am liebsten schlicht und ergreifend, online vom 26.03.2015, unter: https://www.sophos.com/de-de/press-office/press-releases/2015/03/securitysurvey_dach.aspx [Abruf: 15.05.2015].

Söllner, René (2014), Die wirtschaftliche Bedeutung kleiner und mittlerer Unternehmen in Deutschland, in: Statistisches Bundesamt (Hrsg.): Wirtschaft und Statistik (WiSTa) - das Wirtschaftsmagazin, Ausgabe 01/2014, online vom Januar 2014, unter: https://www.destatis.de/DE/Publikationen/WirtschaftStatistik/UnternehmenGewerbeanzeigen/BedeutungKleinerMittlererUnternehmen_12014.pdf?__blob=publication File [Abruf: 12.01.2015].

Spiegel Online (2013), Adobe Creative Cloud: Photoshop gibt es bald nur noch im Abo, online vom 07.05.2013, unter: http://www.spiegel.de/netzwelt/web/adobe-creative-cloud-photoshop-gibt-es-bald-nur-noch-im-abo-a-898494.html [Abruf: 28.03.2015].

Spiegel Online (2014), Erstes Urteil: Microsoft muss US-Ermittlern Daten aus Europa herausgeben, online vom 31.07.2014, unter: http://www.spiegel.de/netzwelt/ netzpolitik/urteil-microsoft-muss-us-ermittlern-daten-aus-europa-geben-a-983921.html# [Abruf: 17.04.2015].

Spiegel Online (2005), Software-Fusion: Adobe kauft Macromedia, online vom 18.04.2005, unter: http://www.spiegel.de/wirtschaft/software-fusion-adobe-kauft-macromedia-a-351904.html [Abruf: 25.03.2015].

Spies, Axel; McCutchen, Bingham (2009), USA: Cloud Computing – Schwarze Löcher im Datenschutzrecht, in: MultiMedia und Recht (MMR), Zeitschrift für Informations-, Telekommunikations- und Medienrecht, Heft 5, München: Verlag C. H. Beck.

Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim (2011), Kryptographie und IT-Sicherheit, Grundlagen und Anwendungen, 2., überarbeitete Auflage,

Statistisches Bundesamt (2014), Nutzung von Informations- und Kommunikationstechnologien in Unternehmen, Unternehmen und Arbeitsstätten, online vom 19.12.2014, unter: https://www.destatis.de/DE/Publikationen/Thematisch/ UnternehmenHandwerk/Unternehmen/InformationstechnologieUnternehmen5529102147004.pdf?__blob=publicationFile [Abruf: 15.01.2015].

Statistisches Bundesamt (2014), Unternehmen mit Nutzung von Cloud Computing (Cloud Services) nach Beschäftigtengrößenklassen im Jahr 2014, Informations- und Kommunikationstechnologien, online vom 19.12.2014, unter: https://www. destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/IKTUnternehmen/Tabellen/06_CloudComputing_IKT_Unternehmen.html [Abruf: 16.01.2015].

Statistisches Bundesamt Pressemitteilung (2014), 12 % der Unternehmen setzen auf Cloud Computing, online vom 19.12.2014, unter: https://www.destatis.de/DE/ PresseService/Presse/Pressemitteilungen/2014/12/PD14_467_52911pdf.pdf?__blob= publicationFile [Abruf: 17.01.2015].

Stögmüller (2013), in: Leupold, Andreas; Glossner, Silke (Hrsg.); Freiherr von dem Bussche, Axel et al.: Münchener Anwaltshandbuch IT-Recht, 3. überarbeitete und erweiterte Auflage, München: Verlag C. H. Beck.

Symantec (2013), Avoiding the hidden costs of cloud 2013, online vom 16.01.2013, unter: https://www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf [Abruf: 10.01.2015].

Taeger, Jürgen; Gabel, Detlev (2010), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 1. Auflage, Frankfurt am Main: Verlag Recht und Wirtschaft.

techconsult GmbH; Hewlett-Packard GmbH (2013), IT-Cloud-Index, Q4/2012, online vom 21.12.2012, unter: http://www.techconsult.de/index.php?option=com_content &view=article&id=237 [Abruf: 15.01.2015].

Telekom (2015), CeBIT 2015: Telekom verschlüsselt Microsoft Office 365, online, unter: http://www.telekom.com/medien/konzern/271530 [Abruf: 12.05.2015].

Telekom (2015), Cloud Computing – Einfach mache, online, unter: Telekom (2015): Cloud-Services für den Mittelstand, online, unter: https://www.telekom.com/ medien/medienmappen/cloud-mittelstand/135550 [Abruf: 10.05.2015].

Telekom (2015), Der Business Marketplace der Deutschen Telekom, online, unter: https://portal.telekomcloud.com/informationen/business-marketplace/ [Abruf: 10.05.2015].

Telekom (2014), Whitepaper: Datenschutz und Datensicherheit beim Cloud Computing, online vom 30.01.2014, unter: https://geschaeftskunden.telekom.de/ blobCache/umn/uti/136378_1415453385000/blobBinary/sicherheit-beim-cloud-computing-ps.pdf [Abruf: 16.05.2015].

TeleTrusT – Bundesverband IT-Sicherheit e. V. Pressemitteilung (2015), Bundesverband IT-Sicherheit warnt vor Absenkung des IT-Sicherheitsniveaus durch TTIP, online vom 09.03.2015, unter: https://www.teletrust.de/uploads/media/PM-150309-TeleTrusT-TTIP.pdf [Abruf: 30.04.2015].

ten Hompel, Michael (Hrsg.); Wolf, Maren-Bianca; Rahn, Jonas (2013), Cloud Computing für Logistik 2, Akzeptanz und Nutzungsbereitschaft der Logistics Mall bei Anwendern und Anbietern, Eine Qualitative und Quantitative Empirische Analyse des Frauenhofer-Institutes für Materialfluss und Logistik IML, Freiburg: Frauenhofer Verlag.

ten Hompel, Michael; Heidenblut, Volker (2011), Taschenlexikon Logistik. Abkürzungen, Definitionen und Erläuterungen der wichtigsten Begriffe aus Materialfluss und Logistik, Berlin: Springer Verlag.

Tipke, Klaus; Kruse, Heinrich Wilhelm (2015), Abgabenordnung – Finanzgerichtsordnung - Kommentar, März 2015, Köln: Verlag Dr. Otto Schmidt KG.

TNS Infratest GmbH (2012), Quo Vadis Big Data - Herausforderungen- Erfahrungen - Lösungsansätze, online vom 20.08.2012, unter: http://www.computerwoche.de/ fileserver/idgwpcw/files/2157.pdf [Abruf: 13.04.2015].

t3n - digital pioneers (2015), Die besten Office-Alternativen für Windows, Mac und Linux, online vom 13.01.2015, unter: http://t3n.de/news/microsoft-office-alternativen-514808/ [Abruf: 25.04.2015].

Vetalio (2014), Microsoft OneDrive Test, online vom 01.03.2014, unter: https://www.vetalio.de/microsoft-onedrive-test [Abruf: 23.05.2015].

Vossen, Gottfried; Haselmann, Till; Hoeren Thomas (2012), Cloud Computing für Unternehmen, Technische, wirtschaftliche, rechtliche und organisatorische Aspekte, 1. Auflage, Heidelberg: dpunkt.verlag.

Wachter, Sabine; Zaelke, Thomas (2014), Systemkonsolidierung und Datenmigration als geschäftskritische Erfolgsfaktoren in: Hildebrand, Knut; Meinhardt, Stefan (Hrsg.) (2014): Systemkonsolidierung & -migration, HMD – Praxis der Wirtschaftsinformatik, Heft 296, 1. Auflage, Heidelberg: Springer Verlag.

Weichert; Thilo (2010), Cloud Computing und Datenschutz, in: Datenschutz und Datensicherheit – DuD, Ausgabe 10, Wiesbaden: Vieweg Verlag.

Wind, Stefan (2012), Cloud Management mit Open-Source-Plattformen, in: Strahringer, Susanne (Hrsg.): Open Source – Konzepte, Risiken, Trends – HMD – Praxis der Wirtschaftsinformatik Heft 283, 1. Auflage, Heidelberg: dpunkt.verlag.

Zentrum für europäische Wirtschaftsforschung (ZEW); prognos; BMWi (2013), Untersuchung von Innovationshemmnissen in Unternehmen - insbesondere KMU - bei der Umsetzung von Forschungs- und Entwicklungsergebnissen in vermarktungsfähige Produkte und mögliche Ansatzpunkte zu deren Überwindung, Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie, online vom 18.10.2013, unter: http://www.bmwi.de/DE/Mediathek/publikationen,did=603754.html [Abruf: 09.01.2015].

Abgeschlossen Juni 2015
www.logos-verlag.de unter ‚Zeitschriften'
www.w-hs.de/ReWir
URN: urn:nbn:de:hbz:1010-opus4-2612 (www.nbn-resolving.de)
URL: https://whge.opus.hbz-nrw.de/frontdoor/index/index/docId/261

Impressum: Westfälische Hochschule, Fachbereich Wirtschaftsrecht, August-Schmidt-Ring 10
D - 45665 Recklinghausen, www.w-hs.de/wirtschaftsrecht

λογος

Vertrieb: Logos Verlag Berlin GmbH
Comeniushof, Gubener Straße 47
10243 Berlin
http://www.logos-verlag.de