RECHTLICHE ASPEKTE VON CLOUD COMPUTING IN DER FINANZ- UND VERSICHERUNGSWIRTSCHAFT

Aljoscha Dietrich / Christoph Sorge

Wissenschaftlicher Mitarbeiter, juris-Stiftungsprofessur für Rechtsinformatik und CISPA / Deutsches Forschungsinstitut für öffentliche Verwaltung Speyer
Campus E 9 1, 66123 Saarbrücken, DE / Freiherr-vom-Stein-Str. 2, 67346 Speyer, DE
aljoscha.dietrich@uni-saarland.de

Universitätsprofessor, juris-Stiftungsprofessur für Rechtsinformatik und CISPA, Universität des Saarlandes
Campus E 9 1, 66123 Saarbrücken, DE
christoph.sorge@uni-saarland.de

Schlagworte: ***Cloud Computing, IT-Sicherheitsgesetz, Datenschutz***

Abstract: *Cloud Computing findet immer breitere Verwendung. Dies gilt auch für die Finanzbranche, «FinTechs» fordern dabei traditionelle Geschäftsmodelle heraus. Cloud Computing ist häufig ein zentraler Baustein. Der Einsatz von Cloud Computing in regulierten Unternehmen aus der Finanz- und Versicherungswirtschaft kann jedoch zu aufsichtsrechtlichen Herausforderungen führen. Daneben können eine Vielzahl von Normen sowie Standards von Branchenverbänden herangezogen werden. Der Beitrag wird die rechtlichen Aspekte von Cloud Computing für Finanzanwendungen näher darstellen und untersuchen.*

1. Einführung und Motivation

Die fortschreitende Digitalisierung hat Einfluss auf nahezu alle Lebensbereiche und macht daher auch nicht vor konservativen Branchen wie der Finanz- und Versicherungswirtschaft halt. Im Finanz- und Bankenumfeld hat sich in den letzten Jahren der Begriff FinTech etabliert. Damit sind junge Start-Ups gemeint, die neue und innovative Produkte entwickeln und anbieten.

Neben neuen Produkten geht es jedoch auch um eine effizientere Gestaltung und Umsetzung bisheriger Technologien und Prozesse. Ein großer allgemeiner IT-Trend der letzten Jahre ist die Verlagerung von Diensten in Cloud-Umgebungen. Dieser Trend geht bisweilen soweit, dass Unternehmen ihre eigenen Rechenzentren abschaffen und vollständig in eine Cloud-Umgebung verlagern. Solche Bestrebungen machen auch vor der Finanz- und Versicherungswirtschaft nicht halt, sind dort aber im Vergleich zu anderen Branchen aufgrund von hohen gesetzlichen und regulatorischen Anforderungen schwieriger umzusetzen.

2. Branchenstandards und regulatorischer Überblick

In der Regel sind gesetzliche Rahmenbedingungen nur schwer zu ändern und zu beeinflussen, insbesondere wenn diese auf europäischen Richtlinien oder Verordnungen basieren. Häufig verweisen diese Regelungen auf den Stand der Technik, um keine zu konkreten Vorgaben treffen zu müssen. In der praktischen Umsetzung bereitet dies jedoch bei der Auslegung Probleme. Um den Begriff «Stand der Technik» mit Inhalt zu füllen, wird daher häufig auf Standards zurückgegriffen. In der Regel haben die betroffenen Branchen selbst die Möglichkeit, Standards zu entwickeln oder auf diese einzuwirken. Besonders deutlich wird dies bei Betrachtung des IT-Sicherheits- bzw. BSI-Gesetzes, auf das in Abschnitt 3 noch näher eingegangen wird. Es sieht vor der Festlegung von branchenspezifischen Standards eine Mitwirkung von Vertretern der betroffenen Betreiber und Wirtschaftsverbände vor, so dass man hier von einem formalisierten Prozess zur Feststellung des Stands der Technik reden kann.

Anders gestaltet sich dies jedoch bei Standards, die von den Branchenverbänden selber entwickelt wurden bzw. Produkt eines Verhandlungsprozesses sind. Entsprechende Standards wurden von der Deutschen Kreditwirtschaft (DK) für die Zahlung mit electronic-cash-Karten entwickelt. Analog hierzu ist der Standard für die Verwendung von Kreditkarten zu nennen, der Payment Card Industry Security Standard (PCI DSS), entwickelt von dem Payment Card Industry Security Standards Council (PCI SSC). Auch diese Standards können aber herangezogen werden, wenn der Gesetzgeber implizit oder explizit die Beachtung des Stands der Technik vorschreibt. Ein Beispiel findet sich etwa im Kreditwesengesetz: Für den automatisierten Abruf von Kontoinformationen beschreibt § 24c Abs. 6 KWG, dass der Stand der Technik von der Bundesanstalt [für Finanzdienstleistungsaufsicht] im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik in einem von ihr bestimmten Verfahren festgestellt wird.

Der Einsatz von Cloud Computing in den regulierten Unternehmen aus der Finanz- und Versicherungswirtschaft kann zu aufsichtsrechtlichen Herausforderungen führen. Je nach Art der Unternehmung können u.a. die Regeln des Kreditwesengesetzes (KWG), Versicherungsaufsichtsgesetzes (VAG), Wertpapierhandelsgesetzes (WpHG), Zahlungsdiensteaufsichtsgesetzes (ZAG), Kapitalanlagegesetzbuchs (KAGB) und des Börsengesetzes (BörsG) zum Tragen kommen. Allgemein ergeben sich hieraus Anforderungen an die Integrität und die Organisation der einzelnen Unternehmen.[1] Diese Auflistung ist aber weder abschließend noch stellt sie das Ende der Entwicklung dar. Ganz im Gegenteil, die Finanz- und Versicherungsbranche fällt beispielsweise auch in den Bereich des IT-Sicherheitsgesetzes (IT-SiG) und der NIS-Richtlinie[2] zum Schutz von kritischen Infrastrukturen (KRITIS) sowie weiterer europarechtlicher Regulierung. Zu nennen ist hier die RL 2015/2366 über Zahlungsdienste im Binnenmarkt. Des Weiteren sind beim Einsatz von Cloud Computing auch weitere allgemeine Gesetze wie z.B. die Datenschutzgesetze zu beachten. Dieser Beitrag soll jedoch vor allem die spezifischen Regelungen der Finanzwirtschaft behandeln. Auch die Versicherungswirtschaft soll hier nur insoweit betrachtet werden, als sie nicht durch Regelungen der Finanzbranche miterfasst wird.

3. Kritische Infrastrukturen

Wie eingangs erwähnt, können die IT-Systeme des Finanz-, Versicherungs-, und Börsenwesen zu den kritischen Infrastrukturen (KRITIS) zählen. KRITIS zeichnen sich dadurch aus, dass sie «von hoher Bedeutung für das Funktionieren des Gemeinwesens [sind], da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden».[3] Zur Abwehr dieser Gefahren hat der Gesetzgeber die Notwendigkeit zur Schaffung des IT-SiG gesehen – ein Artikelgesetz, mit dem u.a. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG) angepasst und die Kompetenzen des BSI erweitert wurden. Ziel ist die Verpflichtung zur Schaffung eines hohen Sicherheitsniveaus für KRITIS Betreiber. Eine Festlegung von Messgrößen und Schwellwertung zur Bestimmung von KRITIS hat der Gesetzgeber gemäß § 10 Abs. 1 BSIG in eine Rechtsverordnung ausgelagert, die sogenannte BSI-KritisV. Insgesamt wurden hier die Bestimmungen für KRITIS in 8 Branchen getroffen und in zwei Körben veröffentlicht. Die Bestimmungen für das Finanz- und Versicherungswesen finden sich im zweiten Korb, welcher zum 30. Juni 2017 in Kraft trat. Die relevanten Dienstleistungen umfassen die Bargeldversorgung, den kartengestützten und konventionellen Zahlungsverkehr, die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften sowie Versicherungsdienstleistungen.[4] Die weiteren Absätze konkretisieren die Dienstleistungen mit Verweis auf entsprechende EU-Richtlinien, Absatz 7 schließlich verweist auf Anhang 6, welcher die Zuordnung zu den genannten Kategorien sowie Schwellwerte beschreibt.

---

1 Eckhold, Thomas, § 24: In Borges, Georg/Meents, Geert (Hrsg.): Cloud Computing – Rechtshandbuch, Rn. 1.

2 Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, ABl L 194/1 vom 19. Juli 2016, in Deutschland umgesetzt mit dem Gesetz zur Umsetzung der NIS-Richtlinie vom 23. Juni 2017.

3 § 2 Abs. 10 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG); Vgl. auch Eckhold (Fn. 1), Rn. 2.

4 § 7 Abs. 1 BSI-KritisV.

Die Berechnung der Schwellwerte hat jeweils 500‘000 betroffene Personen zur Grundlage. Maßgeblich zur Bestimmung der verantwortlichen Stelle ist im Finanz- und Versicherungswesen, wer die tatsächliche Sachherrschaft ausübt, unabhängig von rechtlichen und wirtschaftlichen Umständen.[5]

Im Falle einer Zuordnung zu kritischen Infrastrukturen sind vom Betreiber «angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit [der] informationstechnischen Systeme, Komponenten und Prozesse zu treffen». Ein Nachweis ist insbesondere durch Sicherheitsaudits, Prüfungen oder Zertifizierungen zu erbringen. Der Nachweis ist mindestens alle zwei Jahre zu erbringen.[6] Auch sind erhebliche Ausfälle oder Beeinträchtigungen der Funktionsfähigkeit dem BSI unverzüglich zu melden. Um dem nachzukommen, ist der KRITIS-Betreiber zur Einrichtung einer Kontaktstelle mit jederzeitiger Erreichbarkeit verpflichtet.[7] Nach § 8a Abs. 4 BISG kann die Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Anhörung der betroffenen Betreiber und Wirtschaftsverbände durch das BSI in sogenannten branchenspezifischen Sicherheitsstandards (B3S) festgelegt werden. Für die Finanzbranche ist eine Erweiterung der «Bankenaufsichtlichen Anforderungen an die IT» (BAIT)[8] um ein optional anwendbares KRITIS-Modul im Gespräch. B3S könnten so in den BAIT verankert werden.[9] § 14 BSIG sieht Geldbußen von bis zu 100‘000 € bei Verstößen vor.

4. Auslagerung an Dienstleister

Bei der Nutzung von Community-, Public- oder Hybridclouds kann von einem sogenannten Outsourcing ausgegangen werden, also davon, dass die Cloud von einem beauftragen Unternehmen verwaltet wird. Ein Outsourcing von IT-Infrastruktur kann in regulierten Unternehmen nur bedingt durchgeführt werden, sofern in diesem Fall die erlaubnisspezifischen Geschäftsbereiche wesentlich betroffen sind.[10]

Es gelten wesentliche Anforderungen an den Dienstleister, welcher mit der Auslagerung beauftragt wurde. Der Dienstleister muss die Qualifikation und Quantität (also ausreichende Ressourcen) vorweisen können, um die übertragenen Aufgaben ordnungsgemäß wahrnehmen zu können.[11] Dies umfasst in der Sache eine sorgfältige Auswahl und Überprüfung, welche u.a. die Feststellung von ausreichenden personellen, sachlichen und finanziellen Ressourcen beinhaltet. Auch müssen die Auslagerungsunternehmen jederzeit wirksam überwacht werden können.[12] Die regulierten Unternehmen bleiben auch bei der Auslagerung letztverantwortlich für die Einhaltung der gesetzlichen Regelungen.[13]

5. Konkretisierte Anforderungen

Eine Konkretisierung der Regelungen bzgl. des Risikomanagements wurde bereits 2005 durch die BaFin für Kreditinstitute und für Finanzdienstleistungsinstitute im Rahmen eines Rundschreibens veröffentlicht: «Mindestanforderungen an das Risikomanagement (MaRisk)».[14] Dies sollte den Instituten mehr Freiräume für individuelle Umsetzungslösungen gewähren, indem die Vorgaben für wesentliche (IT-)Auslagerungen im Ver-

---

5 Vgl. § 7 Abs. 8 BSI-KritisV.

6 § 8a Abs. 1 S. 1 BSIG.

7 Siehe § 8b BSIG.

8 Weiteres zu BAIT findet sich in Abschnitt 5.

9 Bundesverband Öffentlicher Banken Deutschland (VÖB) , Bankaufsichtliche Anforderungen an die IT (BAIT) veröffentlicht, 3. November 2017, https://www.voeb.de/de/themen/bankenregulierung/bankaufsichtliche-anforderungen-an-die-it-bait-veroeffentlicht (alle Websites abgerufen am 7. Januar 2018).

10 Eckhold (Fn. 2), Rn. 17; § 25b KWG.

11 Eckhold (Fn. 2), Rn 20; § 25b Abs. 1, S. 2 KWG.

12 § 25b Abs. 2 S. 2, 3 Abs. 3, S. 3 KWG.

13 §§ 25b Abs. 1 S. 3, Abs. 3, 25c Abs. 4a Nr. 6, Abs. 4b KWG; Eckhold (Fn. 2), Rn. 21.

14 Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Rundschreiben 18/2005 «Mindestanforderungen an das Risikomanagement» in der Fassung vom 20. Dezember 2005, https://www.bundesbank.de/Redaktion/DE/Standardartikel/Aufgaben/Bankenaufsicht/risikomanagement_marisk_2005_rundschreiben.html.

gleich zu einem Vorgänger-Dokument[15] drastisch reduziert wurden. In der Praxis führte dies jedoch zu erhöhter Unsicherheit aufgrund der nun unkonkreteren Anforderungen.[16] Zuletzt wurden die MaRisk im Oktober 2017 aktualisiert und an die europäischen und internationalen Anforderungen angepasst. Wesentliche Neuerungen betreffen die Bereiche Datenaggregation und Risikoberichterstattung, Risikokultur und Auslagerung.[17] Die MaRisk sind jedoch eher norminterpretierend als normkonkretisierend zu verstehen. Daher haben sie keine Bindungswirkung gegenüber dem Normadressaten.[18] Kernelement der IT-Sicherheitsstrategie sind die Sicherstellung von Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit der Daten.[19]

Ausdruck der staatlichen Bemühungen zur Verbesserung der IT-Sicherheit ist das Cyber-Abwehrzentrum (Cyber-AZ). Zeichen der erhöhten Gefährdung von Finanzinfrastrukturen ist die Mitgliedschaft der BaFin im Cyber-AZ neben BSI, BfV, MAD, BND, BKA, ZKA, BPOL und BKK. Das Cyber-AZ ist ein Kernelement der 2011 von der Bundesregierung veröffentlichten IT-Sicherheitsstrategie. Es wurde beim BSI in Bonn angesiedelt und handelt sich um keine eigenständige Behörde, sondern stellt eine Kooperation diverser Behörden dar. Ziel ist eine Zusammenarbeit der zuvor genannten Organe. Gemeinsam sollen alle Informationen zu Cyberangriffen auf kritische Infrastrukturen zusammengeführt, ausgetauscht und bewertet werden.[20]

Die BaFin zählt eine Reihe wichtiger Angriffsziele bei Banken auf.[21] Im Kontext von Cloud-Umgebungen der Finanzwirtschaft sind u.a. Datenbanken und Dateien, buchführende IT-Systeme, Steuerungs- und Controlling-Anwendungen, Anwendungen für Risikomanagement und Risikoberichterstattung, Zahlungsverkehrssysteme, Handelssysteme und Schnittstellen zu Kunden und Geschäftspartnern zu berücksichtigen.

Die Anforderungen der BaFin zur Gewährleistung der Cybersicherheit gehen über die bereits bestehenden Anforderungen aus dem KWG hinaus. Nach § 25a Absatz 1 KWG ist eine Notfallvorsorge zu treffen. Übliche Maßnahmen, wie Ausweichrechenzentren, können zwar einen Schutz gegen Naturkatastrophen oder Bombenanschläge bieten, gelten jedoch bei Cyberangriffen als nicht ausreichend. Um einen weitergehenden Schutz zu erreichen, verpflichtet die MaRisk die verantwortliche Stelle daher zur Umsetzung von gängigen Standards (AT 7.2). Eine weitere Präzisierung nehmen die Bankenaufsichtlichen Anforderungen an die IT (BAIT) der BaFin vor. Der Adressatenkreis findet sich in den MaRisk, AT 2.1 und gilt auch entsprechend für die BAIT. Die IT-Berechtigungsvergabe wird in den MaRisk besonders hervorgehoben. Die Mitarbeiter sollen nur über solche Rechte verfügen, die sie zur Ausübung ihrer Tätigkeit benötigen. Die Erläuterungen der BaFin zählen bei den gängigen Standards die IT-Grundschutzkataloge des BSI und die internationalen Sicherheitsstandards ISO/IEC 2700X auf. Zum einen ist diese Liste jedoch offen formuliert, d.h. weitere Standards können hinzugefügt werden. Zum anderen wird jedoch ausdrücklich erwähnt, dass «Das Abstellen auf gängige Standards [...] nicht auf die Verwendung von Standardhardware beziehungsweise -software ab[zielt]. Eigenentwicklungen sind grundsätzlich ebenso möglich».[22]

Speziell für Zahlungsdienste im Binnenmarkt wurde die EU-Richtlinie 2015/2366, Payment Service Directive 2 (PSD 2) erlassen, welche eine Reihe von Regelungen enthält, um die Sicherheit im Zahlungsverkehr zu erhöhen und weiteren Wettbewerb zu ermöglichen.[23] Von den nationalen Gesetzgebern ist diese bis zum 13. Januar

---

15 Bundesaufsicht für das Kreditwesen (BAKred), Rundschreiben 11/2001 «Auslagerung von Bereichen auf ein anderes Unternehmen gem. § 25a Abs. 2 KWG» vom 6. Dezember 2001.

16 Lensdorf, Lars, Aufsichtsrechtliche Anforderungen an die IT von Kredit- und Finanzdienstleistungsinstituten – eine Tour d'horizont von der Einführung des § 25a KWG zur MaRisk 2017 und den BAIT 2017, CR 2017, S. 754 ff.

17 https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171027_marisk.html.

18 Vgl. Eckhold (Fn. 2), Rn. 25.

19 BaFin (Fn. 14), AT 7.2, Tz. 2; Eckhold (Fn. 2) Rn. 26.

20 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html; https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/BaFin_CyberAZ_31032017.html.

21 https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2015/fa_bj_1502_cyber_angriffe.html.

22 Anlage 1: Erläuterungen zu den MaRisk in der Fassung vom 27. Dezember 2017, Seite 28.

23 Bundesbank, Unbarer Zahlungsverkehr – der rechtliche Rahmen, https://www.bundesbank.de/Redaktion/DE/Standardartikel/Aufgaben/Unbarer_Zahlungsverkehr/der_rechtliche_rahmen.html.

2018 in nationales Recht umzusetzen. Der deutsche Gesetzgeber hat dies mit dem «Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie» (ZDUG) vom 1. Juni 2017 beschlossen. Art. 94 Abs. 3 RL 2015/2366 fordert von der Europäischen Bankenaufsichtsbehörde (EBA), in Zusammenarbeit mit der Europäischen Zentralbank (EZB) und nach Anhörung aller maßgeblichen Akteure, die Erstellung von Leitlinien für die Festlegung, Anwendung und Überwachung der Sicherheitsmaßnahmen. Diese finden sich in den «Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)». Die EBA geben mit dieser Orientierungshilfe einen Rahmen zur Absicherung der IT-Systeme vor, welche u.a. Risikomanagement, Risikobewertung, (IT-)Sicherheitsmaßnahmen, Monitoring, Betriebskontinuitätsmanagement, Tests der Sicherheitsmaßnahmen sowie ständige Evaluierung umfassen. Dieses Vorgehen erinnert stark an die Sicherheitsstandards ISO/IEC 2700X.

Weitere Empfehlungen und Anforderungen ergeben sich auch aus dem Payment Card Industry Data Security Standard (PCI DSS). Hierbei handelt es sich um einen Standard für die Verwendung und Nutzung von Kreditkarten, wie Visa, MasterCard und American Express. Vom Payment Card Industry Security Standards Council (PCI SSC) wurden u.a. die Information Supplement: PCI DSS Cloud Computing Guidelines herausgegeben, die aktuell in der Version 2.0 vom Februar 2013 vorliegen. In diesem Dokument werden Praxisaspekte bzw. konkrete Umsetzungsmöglichkeiten dargestellt. So werden unterschiedliche Cloudmodelle (Software as a Service – SaaS/ Platform as a Service – PaaS / Infrastructure as a Service – IaaS) beschrieben und die entsprechenden Kontrollmöglichkeiten bzw. Verantwortlichkeiten dargestellt. Ähnlich, wie auch in den bundesrechtlichen Normen,[24] wird die Gefahr eines Kontrollverlusts bei einer Auslagerung erkannt. Ein Kontrollverlust ist zu verhindern. Auch wird verdeutlicht, wie sich nach PCI DSS die Verteilung der Kontrolle über die einzelnen Cloud Layer zwischen Klient und Cloud Service Provider (CSP) darstellen kann. Im weiteren Text der Cloud Computing Guidelines werden die 12 grundsätzlichen Anforderungen (Requirements) des PCI DSS genannt und es wird beispielhaft eine Aufteilung der Verantwortung zwischen den Parteien vorgenommen.

Der PCI DSS empfiehlt weiterhin eine Segmentierung, d.h., der CSP muss sicherstellen, dass die einzelnen Klienten und insbesondere deren Daten voneinander getrennt gehalten werden. Auch beim Einsatz von Virtualisierungen soll also dafür gesorgt werden, dass die Daten möglichst physisch getrennt gespeichert werden. Zudem sollen auch die besonders kritischen Daten, hier Cardholder Data Enviroment (CDE), von anderen Daten getrennt abgelegt werden. Um die Gefahren bzw. den regulatorischen Aufwand gering zu halten, empfiehlt der PCI SSC, dass keine Zahlungsdaten in die Cloud übermittelt, gespeichert oder dort verarbeitet werden. Sind jedoch keine Klartextdaten in der Cloud vorhanden, kann dies die Anforderungen der PCI DSS verringern. Die Abschnitte 4.5 und 6.4.5 gehen näher auf Kryptographie und Schlüsselmanagement ein. Hier wird die Empfehlung ausgesprochen, die Schlüssel getrennt vom Clouddienst, welcher für die Datenablage verwendet wird, abzulegen. Auch wird vor potentiellen Fehlerquellen bei der Ent- bzw. Verschlüsselung in der Cloud gewarnt. So werden die unbeabsichtigte Ablage von Klartext im Arbeitsspeicher oder auch in Snapshot und Backups der Host-Systeme als potentielle Gefahrenquellen genannt. Daher wird die Empfehlung ausgesprochen, Schlüssel und kryptographische Operationen nur auf den Systemen des Kunden zu lagern bzw. durchzuführen. Beim Einsatz von Virtualisierung wird in den Cloud Computing Guidelines die Gefahr aufgezeigt, dass veraltete und unsichere Systeme/Software zum Einsatz kommen können.[25] Dem könnte beispielsweise mit dem Einsatz von Virtualisierungslösungen mit Containern, wie beispielsweise Docker[26], entgegengewirkt werden. Die Container können jederzeit einfach ausgetauscht und aktualisiert werden. Im Zusammenspiel mit den sehr kurzzeitigen Laufzeiten der einzelnen Container kann somit sichergestellt werden, dass nur aktuelle Software eingesetzt wird bzw. auf Sicherheitslücken schnell reagiert werden kann.

---

24 Siehe u.a. § 25b KWG.

25 Siehe Payment Card Industry Security Standards Council (PCI SSC), Information Supplement: PCI DSS Cloud Computing Guidelines, Februar 2013, https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf, S. 28.

26 https://www.docker.com.

6. Bewertung

Der Einsatz von Cloud Computing für sicherheitsrelevante Anwendungen ist zunächst kritisch zu bewerten; die Aufgabe von Kontrolle kann ein erhebliches Risiko implizieren. Gerade die gemeinsame Verarbeitung von Daten verschiedener Klienten auf einem gemeinsamen IT-System erfordert größte Sorgfalt, um deren Vertraulichkeit zu wahren. Sicherheitslücken, durch die Schutzmechanismen wie die Trennung verschiedener virtueller Maschinen überwunden werden könnte, sind in der Vergangenheit mehrfach aufgetreten. Als jüngstes Beispiel sei die Meltdown-Verwundbarkeit genannt, die das Lesen von Speicherbereichen ohne die notwendigen Zugriffsrechte ermöglicht.[27] Andererseits kann die Auslagerung von Diensten in eine Cloud neben einer höheren Effizienz auch durchaus Sicherheitsvorteile durch professionalisiertes Sicherheitsmanagement mit sich bringen. Ein völliger Verzicht auf die Cloud-Nutzung wird daher in vielen Fällen nicht die richtige Antwort sein; die dargestellten Standards zeigen, dass eine Balance zwischen den Sicherheitsanforderungen und ökonomischen Überlegungen durchaus möglich ist. Weitere Forschung kann dazu beitragen, die Cloud für Anwendungen nutzbar zu machen, in denen Sicherheitsbedenken dies bislang – durchaus zu Recht – verhindert haben.

7. Fazit

Zusammenfassend lässt sich feststellen, dass es sich bei dem Einsatz von Cloud-Umgebungen im Finanzsektor um einen stark regulierten und reglementierten Bereich handelt. Im Regelfall dürfte der Einsatz von Cloud-Lösungen als Auslagerung zu interpretieren sein, welche eine Vielzahl von Regularien nach sich zieht. Doch auch der Einsatz Instituts eigener IT wird weiter reguliert. Nicht nur der Gesetzgeber, sondern auch Branchenvertretungen und Standardgeber sind sehr aktiv. Dies führt zum einen zu einer Vielzahl verschiedener Gesetze, Verordnungen und Empfehlungen etc. Zum anderen ist jedoch anzumerken, dass diese sich viele Gemeinsamkeiten teilen und dass es, je nach konkretem Einsatzbereich, lediglich zu unterschiedlichen Ausprägungen kommt. Kryptographie wird allgemein als Lösungsmöglichkeit aufgezeigt. Innovative Lösungen in Cloud-Umgebungen können hier gegebenenfalls nicht nur dem Stand der Technik, sondern auch dem Stand der Forschung entsprechen und neben gehärteten Systemen mit Trusted Computing auch auf fortschrittliche kryptographische Systeme mit feingranularem Rechtemanagement setzen. Vorzugsweise sollten dann das Schlüsselmanagement und damit auch die Datenhoheit beim Kunden verbleiben. Eine solche innovative Lösung könnte sich gut in die rechtlichen und regulatorischen Anforderungen einfügen und zugleich Akzente für zukünftige Entwicklungen und Standards setzen.

8. Danksagung

Diese Arbeit wurde zu Teilen durch das Forschungsprojekt Securing the Financial Cloud (SFC) unterstützt, finanziert durch das Bundesministerium für Bildung und Forschung (BMBF), Fördernummer 16KIS0058K.

[27] https://googleprojectzero.blogspot.de/2018/01/reading-privileged-memory-with-side.html.