universität innsbruck

Forschungsprojekt I-GIT

Auswirkungen sich verändernder Wertschöpfungsketten im Finanzsektor auf die IT-Sicherheit

Rainer Böhme* Paulina Jo Pesch† Verena Fritz‡

Projektbericht
Stand: Juli 2022

1 Motivation und Zielsetzung

Im Zuge der fortschreitenden Digitalisierung wird sich die bereits seit längerer Zeit beobachtbare Ausdifferenzierung der Wertschöpfungsketten des Finanzmarkts noch weiter verstärken. Flankiert wird diese Entwicklung von den gesetzlichen Neuregelungen zur Verbesserung des Wettbewerbs im Zahlungsverkehr. Es ist absehbar, dass diese, z. B. die PSD2, weitreichende Veränderungen der Geschäftsmodelle von Banken im Privatkundengeschäft verursachen oder bereits beobachtbare Veränderungsprozesse beschleunigen. Die mit der fortschreitenden Digitalisierung einhergehende Internationalisierung und Komplexitätssteigerung im Finanzsektor wird auch Weiterentwicklungen der Aufsicht erforderlich machen. Neue Technologien, veränderte Erwartungen und Gewohnheiten von Nutzerinnen[1] sowie die ökonomischen Gesetzmäßigkeiten der Software- und Internet-Industrie werden diese Prozesse maßgeblich beeinflussen. Dies hat unmittelbare Folgen für die Informationssicherheit und die Ausfallsicherheit der Zahlungssysteme. In einer weitgehend digitalisierten Gesellschaft berühren diese beiden Aspekte sowohl den Verbraucherschutz als auch die Stabilität des Zahlungsverkehrs bzw. Wirtschaftssystems. Sie rücken damit in den Kernbereich der Finanzaufsicht. Im Rahmen der IT-Aufsicht konkretisiert die Finanzaufsichtsbehörde die gesetzlichen Vorgaben u. a. an die Informationssicherheit und überwacht deren Einhaltung.

Ziel der Forschungsarbeit ist eine strukturierte Auseinandersetzung mit den Auswirkungen für die IT-Aufsicht, welche sich aus den möglichen zukünftigen Entwicklungen im Finanzsektor

* Rainer Böhme ist Professor für Informatik mit Schwerpunkt Datensicherheit und Datenschutz. Er war unter anderem für die EZB tätig.
† Paulina Jo Pesch ist Juristin mit Schwerpunkt IT-Recht. Sie hat zu virtuellen Kryptowährungen promoviert.
‡ Verena Fritz ist Ökonomin mit Berufserfahrung bei einem Kreditinstitut. Sie hat ein Erweiterungsstudium in Informatik abgeschlossen.
[1] In diesem Bericht wird aus Gründen der besseren Lesbarkeit das generische Femininum verwendet. Sofern auf natürliche Personen Bezug genommen wird, sind Personen männlichen und anderen Geschlechts als von der weiblichen Form erfasst anzusehen.

ergeben (sowohl im Zahlungsverkehr als auch bei anderen und neuen Finanzdiensten, etwa im Bereich von Kryptoverwahrgeschäften). Neuordnungen des zu erwartenden Ausmaßes sind grundsätzlich schwer prognostizierbar. Die internationale Vernetzung des Finanzsektors sowie die außergewöhnlich hohe Entwicklungsdynamik im Technologiebereich stellen zusätzliche Herausforderungen dar. Um trotz dieser Schwierigkeiten nach wissenschaftlichen Kriterien vertretbare und gleichzeitig konkrete Aussagen treffen zu können, wurde die Szenario-Methode angewandt. Bei dieser werden Thesen zur möglichen künftigen Entwicklung im Finanzsektor in Szenarien übersetzt, welche anschließend validiert werden. Ausgangsbasis für die im Projekt entwickelten Szenarien waren die aktuelle Gesetzeslage sowie Detailkenntnisse von Technologien mit Markreife und Marktdurchdringung.

Dieser Bericht gliedert sich wie folgt. Zur Kontextualisierung der Szenarien wird zunächst die Ausgangslage dargestellt (siehe Abschnitt 2). Dann wird jedes entwickelte Szenario skizziert und entlang seiner charakteristischen Aspekte diskutiert (siehe Abschnitt 3). Die der jeweiligen These zur künftigen Entwicklung zugrunde liegenden Tatsachen und Wertungen werden erläutert. Anschließend folgt die Darstellung der Validierung durch Interviews mit Marktvertreterinnen (siehe Abschnitt 4). Der Darstellung der Ergebnisse der Validierung schließt sich eine Erörterung der Konsequenzen der validierten Szenarien für die IT-Aufsicht an (siehe Abschnitt 5).

2 Darstellung der Ausgangslage

Die Ausgangslage für die unten in Abschnitt 3 beschriebenen Szenarien ergibt sich aus den rechtlichen Rahmenbedingungen und den bereits beobachtbaren Veränderungen am Finanzmarkt. Diese Darstellung legt einen Fokus auf Informationssicherheit und führt eine Terminologie ein, welche die Beschreibung der Szenarien unterstützt.

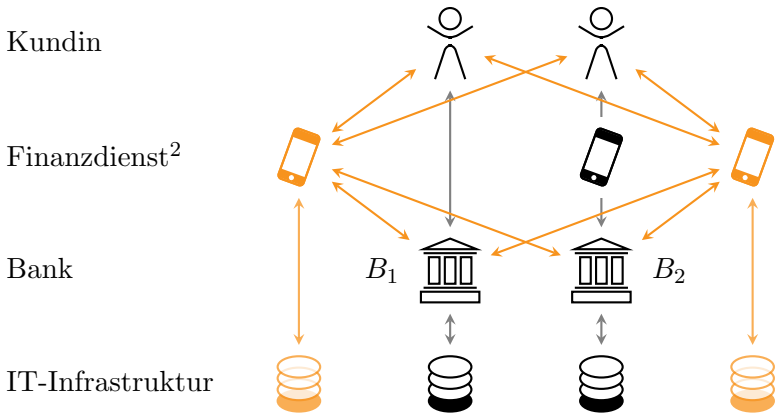

Abbildung 1: Ausdifferenzierung und Flexibilisierung der Wertschöpfungskette: Farblich hervorgehobene Akteurinnen und Beziehungen sind neu hinzugekommen.

Die Ausdifferenzierung und Flexibilisierung der Wertschöpfungskette bringt neue Akteurinnen in den Zahlungsverkehr. Abbildung 1 veranschaulicht diese Entwicklung.

Während vor wenigen Jahren Bankkundinnen hauptsächlich persönlich in der Filiale (B_1) und zunehmend über von ihrer Bank zur Verfügung gestellte digitale Kanäle (B_2) Bankgeschäfte tätigten, haben sie heute die Möglichkeit, für bestimmte Dienstleistungen dritte Finanzdienste einzuschalten. Die Wertschöpfungstiefe der Bank wird somit reduziert und die Bank zum Teil durch neue Markteilnehmerinnen ersetzt. Diese greifen z. B. im Auftrag der Kundin auf die Bankdaten zu und tätigen Geschäfte. Dabei bleibt zur Nutzung dritter Finanzdienste ein Konto bei einer Bank erforderlich, sodass beim Einsatz eines Finanzdienstes stets mindestens eine (weitere) Bank beteiligt ist.

In Umsetzung der PSD2 sind erlaubnispflichtige Zahlungsauslösedienste (ZAD) und registrierungspflichtige Kontoinformationsdienste (KID) im Sinne von § 1 Abs. 1 Satz 2 Nr. 7 und 8 des Zahlungsdiensteaufsichtsgesetzes (ZAG) eingeführt worden. Diese neuen Dienste arbeiten ausschließlich digital und nutzen eigene, nicht von den Banken kontrollierte IT-Infrastrukturen, die an die Infrastruktur der Banken durch von diesen bereitgestellte Schnittstellen angebunden sind.

2.1 Neue Schnittstellen, neue Risiken

Nicht nur der Eintritt neuer Akteurinnen, sondern insbesondere auch die damit verbundene Zunahme unterschiedlicher Schnittstellen erhöht die Anzahl möglicher Fehlerquellen. In der

[2] Der Begriff des Finanzdiensts ist untechnisch für im Finanzsektor gegenüber Endkundinnen erbrachte Dienste zu verstehen, ohne Rücksicht darauf, ob diese von Banken, anderen Kreditinstituten oder Fintech-Unternehmen (ohne Bankenlizenz) erbracht werden.

Softwaretechnologie birgt jede Fehlerquelle eine potenzielle Sicherheitslücke. Die Zunahme betrifft neben technischen Schnittstellen – oft über APIs[3] realisierte Übergabepunkten für Daten zwischen den IT-Systemen verschiedener Stufen der Wertschöpfungskette – auch die Benutzungsschnittstellen. Menschen machen leichter Fehler, wenn sie mit ungewohnten Benutzungsschnittstellen oder ihnen unbekannten Prozessen interagieren. Je mehr unterschiedlichen Benutzungsschnittstellen oder neuen Prozessen Endnutzerinnen ausgesetzt sind, umso größer ist die Gefahr von Social-Engineering-Angriffen, d. h. der Ausnutzung der „Schwachstelle Mensch“ durch Cyberkriminelle, wie z. B. Phishing-Angriffe. Im Folgenden wird der Begriff „Schnittstellenkomplexität“ verwendet, um die Anzahl und Variabilität (zwischen Systemen und im Zeitverlauf) von Schnittstellen aller Art sowie die damit einhergehenden Fehlerquellen zu beschreiben.

Den durch die Schnittstellenkomplexität verursachten, neuen Informationssicherheitsrisiken sind wirksame Sicherheitsmaßnahmen entgegenzustellen. Grundsätzlich wünschenswert wäre es, wenn der Markt selbst ein angemessenes Niveau an Informationssicherheit fände. Die Literatur zur ökonomischen Analyse von Informationssicherheit nennt jedoch eine Reihe von Gründen, aus denen der Markt an dieser Stelle versagen kann (Anderson und Moore, 2006). Ein offensichtliches Hindernis besteht, wenn diejenige Partei, die über den Einsatz einer Sicherheitsmaßnahme entscheidet und deren Kosten trägt, nicht die gleiche Partei ist, die auch im Schadensfall haftet, oder zumindest praktisch nicht in Anspruch genommen wird. Derartige Konstellationen können bei erhöhter Schnittstellenkomplexität eintreten. Durch die Zerteilung von Wertschöpfungsketten im Zahlungssektor könnten finanzielle Risiken und Möglichkeiten zum technischen Risikomanagement (insb. Risikoreduktion) in unterschiedliche Verantwortungsbereiche fallen. Abbildung 2 illustriert dies beispielhaft.

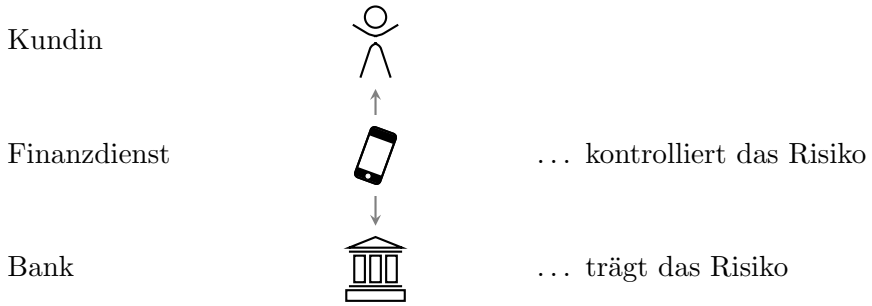

Abbildung 2: Verteilung von Risiko und Riskomanagement auf mehrere Parteien

Bei Zahlungsdiensten richtet sich die Haftung der Beteiligten nach den §§ 675u ff. BGB. Neben kontoführenden Zahlungsdienstleisterinnen (Banken) können weitere Zahlungsdienstleisterinnen eingeschaltet werden. Bei diesen kann es an Anreizen für Investitionen in Informationssicherheitsmaßnahmen fehlen, wenn sie gegenüber den Zahlungsdienstnutzerinnen nicht unmittelbar haften. So haftet gegenüber der Zahlungsdienstnutzerin bei der Einschaltung von Zahlungsauslösediensten weiterhin die kontoführende Zahlungsdienstleisterin (§ 675u Satz 5 BGB). Allerdings kann die unmittelbar haftende kontoführende Zahlungsdienstanbieterin den Zahlungsauslösedienst nach Maßgabe des § 676a BGB in Regress nehmen. Hier trägt jedoch die kontoführende Zahlungsdienstleisterin die Beweislast dafür, dass der Zahlungsvorgang im eigenen Verantwortungsbereich ordnungsgemäß abgelaufen ist, die Störung des Zahlungsvorgangs also auf Seiten der dritten Zahlungsdienstleisterin eingetreten ist.[4]

[3] Application Programming Interface oder Programmierschnittstelle.
[4] Linardatos, in MüKoHGB (4. Aufl 2019), Bd. 6, K. Online-Banking, Rn. 321 f.

Zu berücksichtigen ist auch, dass Zahlungsdienstleisterinnen unter dem Druck der Öffentlichkeit stehen, potenzielle Sicherheitsschwachstellen abzusichern, um einen Reputationsschaden zu vermeiden. Möglicherweise messen Kundinnen dem allerdings weniger Bedeutung bei als der Benutzungsfreundlichkeit des Zahlungsdienstes, weil ihnen durch den Anspruch gegenüber der jeweiligen kontoführenden Zahlungsdienstleisterin kein finanzieller Verlust droht.

Weil es an haftungsrechtlichen und faktischen Anreizen für Informationssicherheitsmaßnahmen fehlen kann, ist es erforderlich, dass die gesetzlichen Regelungen die Einhaltung angemessener Informationssicherheit bei jeder Teilnehmerin der Wertschöpfungskette flankieren. Dies wird bei erlaubnispflichtigen Anbieterinnen, wie insbesondere Zahlungsauslösediensten, im Erlaubnisverfahren berücksichtigt und regelmäßig überprüft. Im Erlaubnisverfahren liegt ein deutlicher Fokus auf der Informationssicherheit.[5] Entsprechende Vorgaben sind die gesetzlichen Grundlagen (Kreditwesengesetz (KWG), ZAG sowie die Auslegungen und Rundschreiben der Verwaltung, die Mindestanforderungen an das Risikomanagement „MaRisk“ (BaFin, 2017b) und die BAIT (BaFin, 2017a). Allerdings können technische Vorgaben und Regeln praktisch nicht sämtliche gegenwärtigen und zukünftigen Risiken abdecken. Denn einzelne Risiken können leicht übersehen werden, künftige Risiken ggfs. im Vorhinein nicht absehbar sein.

2.2 Arten von Abhängigkeiten zwischen Akteurinnen

Technische Schnittstellen sind primär als Kommunikationsangebot oder -möglichkeit zu verstehen. Für die Betrachtung von Risiken ist jedoch erheblich, ob tatsächlich eine Kommunikationsbeziehung zustande kommt, in welcher eine Abhängigkeit technischer oder finanzieller Art zwischen Akteurinnen begründet ist, und wie diese rechtlich einzuordnen ist.[6]

Im Folgenden wird zwischen *statischen* und *dynamischen* Abhängigkeiten unterschieden. Erstere beruhen immer auf einer Vertragsbeziehung und werden oft langfristig aufrecht erhalten. Letzteren können Vertragsbeziehungen zugrunde liegen, dies ist aber nicht zwingend der Fall. So setzt etwa die Nutzung der PSD2-Schnittstellen ausdrücklich keine Vertragsbeziehung voraus (vgl. § 48 Abs. 2 und § 50 Abs. 2 ZAG). Dynamische Abhängigkeiten entstehen, wenn Systeme im Verfahrensablauf auf (u. a. gesetzlich vorgesehene) Schnittstellen zugreifen und der weitere Verfahrensablauf von der Reaktion des zugegriffenen Dienstes abhängt.

Abbildung 3 illustriert den Unterschied zwischen statischen und dynamischen Abhängigkeiten. Kundin K erwirbt ein Produkt bei Händlerin H. Diese Beziehung ist eine statische Abhängigkeit, da ein Kaufvertrag zwischen H und K vorliegt. H bietet die Zahlung über einen Finanzdienst (Z) an, welcher den Zahlungsfluss vom Konto der Kundin K bei der Bank B_1 auf das Konto von H bei der Bank B_2 auslöst. Banken stehen mit ihren Kundinnen in einer Vertragsbeziehung, deshalb handelt es sich um statische Abhängigkeiten. Diese sind der Vollständigkeit halber in Abbildung 3 eingezeichnet, auch wenn es weder beim Kauf noch bei der Zahlung zu direkter technischer Kommunikation zwischen den Parteien kommen muss. Diese wird vollständig über Z vermittelt. K steht mit Z in einer Vertragsbeziehung. Daraus folgt die statische Abhängigkeit zwischen K und Z. Der Beziehung zwischen Z und B_1 liegt hingegen keine vertragliche Beziehung zugrunde, diese Parteien stehen in dynamischer Abhängigkeit zueinander.

[5] Vgl. etwa EBA Guidelines on ICT and security risk management, EBA/GL/2019/04 sowie EBA Leitlinien zu den Informationen, die für die Zulassung von Zahlungsinstituten und E-Geld-Instituten sowie für die Eintragung von Kontoinformationsdienstleisterinnen gemäß Artikel 5 Absatz 5 der Richtlinie (EU) 2015/2366 zu übermitteln sind, EBA/GL/2017/09.

[6] Zu den zunehmend komplexen Abhängigkeiten siehe Financial Stability Board FSB (2019, p. 4 f.).

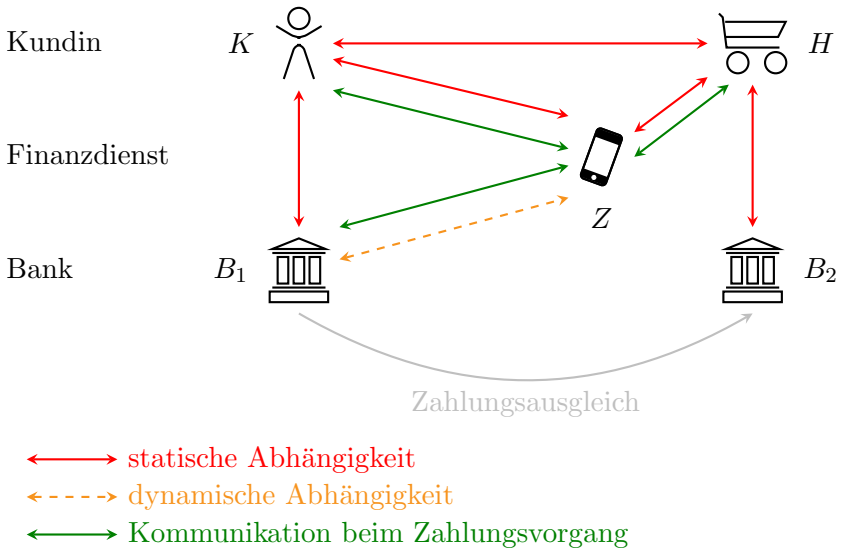

Abbildung 3: Unterscheidung von statischen und dynamischen Abhängigkeiten am Beispiel einer 4-Punkt-Zahlung mit Intermediärin

Statische und dynamische Abhängigkeiten unterscheiden sich bezüglich ihres Risikos und der Sichtbarkeit für die Aufsicht.

Bei **statischen Abhängigkeiten** ist davon auszugehen, dass beide Vertragspartnerinnen am Markt zueinander gefunden und sich bewusst zur Zusammenarbeit entschieden haben. Darüber hinaus haben sie in der Regel ihre Schnittstellen technisch abgestimmt und können auf Unwägbarkeiten reagieren. Zur Haftung im Fehlerfall gibt es regelmäßig vertragliche Regelungen. Beaufsichtigte sind dafür verantwortlich, Auslagerung und Weiterverlagerung vertraglich so zu regeln, dass alle Vertragspartnerinnen ein angemessenes Niveau an Informationssicherheit einhalten und die Kontrollmöglichkeiten sowohl seitens der Beaufsichtigten als auch der Aufsicht nicht beschränkt sind (BaFin, 2018b, S. 11–12). Trotzdem ist die Gesamtheit z. B. durch Weiterverlagerung tief verschachtelter Abhängigkeiten für die Aufsicht nicht unmittelbar „ersichtlich“. Sie kann bestenfalls mit zeitlichem Verzug erhoben werden. Probleme können bei statischen Abhängigkeiten insbesondere dann entstehen, wenn die technische und organisatorische Realität von der zugrunde liegenden vertraglichen Regelung abweicht. Ein Beispiel bilden vertraglich nicht vorgesehene Datenflüsse, etwa an Dritte. Da dies nie gänzlich auszuschließen ist sowie im Zusammenspiel mit dynamischen Abhängigkeiten neue Konstellationen eintreten können, erfordert auch die Anzahl und Verflechtung statischer Abhängigkeiten Aufmerksamkeit.

Parteien in **dynamischen Abhängigkeiten** haben mitunter selten miteinander zu tun. Es kann nicht davon ausgegangen werden, dass sie sich bewusst zu einer Zusammenarbeit entschlossen haben oder eine Abstimmung von technischen Schnittstellen bzw. zu Kontaktmöglichkeiten im Fehlerfall erfolgt ist. Sofern die Schnittstellen eIDAS[7] unterstützen und korrekt implementieren, ist lediglich die gegenseitige Identifizierung als gegeben anzusehen. Dies impliziert aber nicht notwendigerweise eine Vertragsbeziehung. In bestimmten Fällen, etwa den PSD2-Schnittstellen, ist diese vom Gesetz explizit nicht vorgesehen. Die Haftung im Falle nicht autorisierter Zahlungen beruht auf gesetzlichen Vorgaben und könnte im Einzelfall mit Durchsetzungsrisiken verbunden

[7] Die eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014) schafft eine gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen.

sein.

Die Entscheidung, auf welche Schnittstellen von welchen Parteien dynamisch zugegriffen wird, basiert auf der Kombination mehrerer Faktoren wie insbesondere Benutzungsverhalten oder Programmlogik. Es ist auch denkbar, dass Systeme Dritter die Auswahlentscheidung leiten, z. B. wenn ein System zur Entscheidungsunterstützung die Zahlungsmethode aufgrund einer Risikoabschätzung auswählt. Deshalb ist davon auszugehen, dass dynamische Abhängigkeiten im zeitlichen Verlauf sehr unterschiedlichen Mustern folgen. Sie können einmalig, wiederholt, aber auch dauerhaft sein.

Die bereits oben angesprochenen Schwierigkeiten kommen bei dynamischen Abhängigkeiten verstärkt zum Tragen. Bei diesen fehlt es an einer vertraglichen Regelung im Vorfeld, was Abweichungen von der gewollten Situation wahrscheinlicher macht. Bezüglich der Einhaltung des notwendigen Niveaus an Informationssicherheit müssen sich die Parteien auf die Einhaltung der gesetzlichen Vorgaben verlassen, denn es bestehen in der Regel keine direkten Kontrollmöglichkeiten für die betroffenen Parteien. Sofern es sich bei den Parteien um Beaufsichtigte handelt, bestehen gewisse Kontrollmöglichkeiten für die jeweils zuständige Aufsichtsbehörde.

Allerdings erhält die Aufsicht keine Informationen über tatsächlich eingegangene Abhängigkeiten aus der vorgelegten Dokumentation wie Verträgen oder Anwendungsdokumentationen, sondern allenfalls durch die (aufwändige) Analyse von technischen Protokolldaten als Laufzeitinformationen. Die Dokumentation bildet die tatsächliche Implementierung möglicherweise nicht vollständig oder nicht korrekt ab. Insgesamt sind dynamische Abhängigkeiten mit größeren Unsicherheiten behaftet. Über dynamische Abhängigkeiten lässt sich schwerer ein Überblick gewinnen. Die Perspektive der Aufsicht ist hier im Ausgangspunkt fragmentiert, was eine Gesamtschau praktisch erschwert. Dies gilt etwa für die Beziehung zwischen Z und B_1 in Abbildung 3.

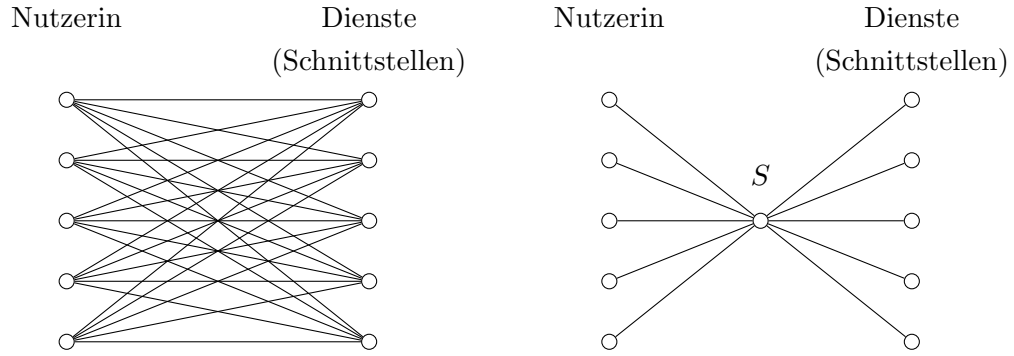

Abbildung 4: Illustration der netzwerkökonomischen Betrachtung: Angenommen, es entstehen Anpassungskosten bei jeder Nutzerin für jede unterstützte Schnittstelle, dann steigen die sozialen Kosten (= Anzahl der Verbindungen) quadratisch in der Anzahl der Parteien (links). Ein gemeinsamer Standard (angeboten durch eine zusätzliche Partei S) reduziert die sozialen Kosten auf eine lineare Funktion der Anzahl an Parteien (rechts). Die Differenz zwischen der linken und der rechten Seite ist der Wohlfahrtsgewinn durch Koordination auf einen Standard, welcher teilweise von der standardisierenden Intermediärin S abgeschöpft werden kann.

2.3 Auslagerung von Schnittstellendiensten

Elementare netzwerkökonomische Überlegungen legen nahe, dass für eine wohlfahrtsmaximierende Lösung die Anzahl unterschiedlicher Schnittstellen gering zu halten ist. In Katz und Shapiro (1985) wird ausgeführt, dass die Etablierung einer Schnittstelle mit Fixkosten verbunden ist, die unabhängig von der Anzahl der diese Schnittstelle benutzenden Nutzerinnen und damit unabhängig vom Nutzen der Schnittstelle sind (je größer das Netzwerk, umso größer der Nutzen). Die Vermeidung dieser Fixkosten wird in der Regel durch Standardisierung erreicht (siehe Abbildung 4). Allerdings ist der Weg zur Etablierung eines Standards allein durch Marktkräfte oft langwierig und ineffizient. Vielfach setzt sich nicht der beste Standard durch, sondern derjenige, der als erstes eine kritische Masse erreicht (Shapiro und Varian, 1998). Fast immer werden in so einem Wettlauf nicht direkt messbare und „unbequeme“ Aspekte, wie insbesondere Informationssicherheit, vernachlässigt. Im Finanzsektor bleibt bei Beobachtung von Standardisierungsbemühungen und ihrer Entwicklung abzuwarten, ob Entsprechendes eintritt. Bislang ist die Vernachlässigung von Informationssicherheitsaspekten bei Standardisierungsbemühungen noch nicht ersichtlich.

Für Banken, die zur Bereitstellung von Schnittstellen verpflichtet sind, diese aber nicht als ihre Kernkompetenz verstehen, ist es insbesondere in der Phase der Standardfindung wirtschaftlicher, die Bereitstellung der Schnittstelle an eine spezialisierte Dienstleisterin auszulagern. Damit erhöhen sich die Anzahl der Schnittstellen und die Komplexität der Abhängigkeitsbeziehungen zusätzlich. Denn auch die Verbindung zwischen Bank und Dienstleisterin erfordert eine technische Schnittstelle. Aus der Vertragsbeziehung ergibt sich eine statische Abhängigkeit. Technisch stellen diese Dienstleisterinnen eine Übersetzung der Bank-internen Datenformate auf, die nach außen sichtbare API bereit und pflegen diese im Zeitverlauf. Durch ihre Spezialisierung können sie die Entwicklungen genau beobachten. Weiterhin können sie durch die Bereitstellung von Schnittstellen für mehrere Banken Skalenvorteile realisieren und teilweise an ihre Kundinnen weitergeben. Inwieweit diese Dienstleisterinnen die Verhandlungsposition ihrer Kundinnen in der Suche nach einem Standard stärken, wird sich zeigen.

Abbildung 5 illustriert die Auslagerung von Schnittstellendiensten, indem sie Abbildung 3 um die Sicht auf die IT-Infrastruktur erweitert. Beide Banken, B_1 und B_2, betreiben oder beauftragen Rechenzentren, R_{B_1} bzw. R_{B_2}. Die Bereitstellung der Schnittstellen hat B_1 an die spezialisierte Dienstleisterin S_{B_1} ausgelagert. Diese steht durch ihre Vertragsbeziehung in einer statischen Abhängigkeit mit B_1. Zu Z und indirekt zum Zahlungsvorgang zwischen K und H besteht eine dynamische Abhängigkeit. Der Datenfluss und die dazu erforderliche technische Abstimmung erfolgen einerseits in Richtung Z und andererseits zum Rechenzentrum R_{B_1}.

An dieser Stelle sei in Erinnerung gerufen, dass Abbildung 5 immer noch eine starke Vereinfachung des tatsächlichen Geflechts an Abhängigkeiten darstellt. Sie blendet nicht nur das gesamte, hinter dem Begriff „Zahlungsausgleich“ stehende, konventionelle Zahlungssystem aus. Vielmehr lagert auch Z seine IT-Infrastruktur an verschiedene Dienstleisterinnen aus. Außerdem ließe sich die Abwicklung der starken Kundenauthentifizierung (SKA) an Dienstleisterinnen auslagern, um diese nicht Z zu überlassen. Solche Konstellationen erschweren es allen beteiligten Akteurinnen – sowohl den Beaufsichtigten, als auch der Aufsicht –, potenzielle Schwachstellen zu erkennen und die damit verbundenen Informationssicherheitsrisiken zu bewerten.

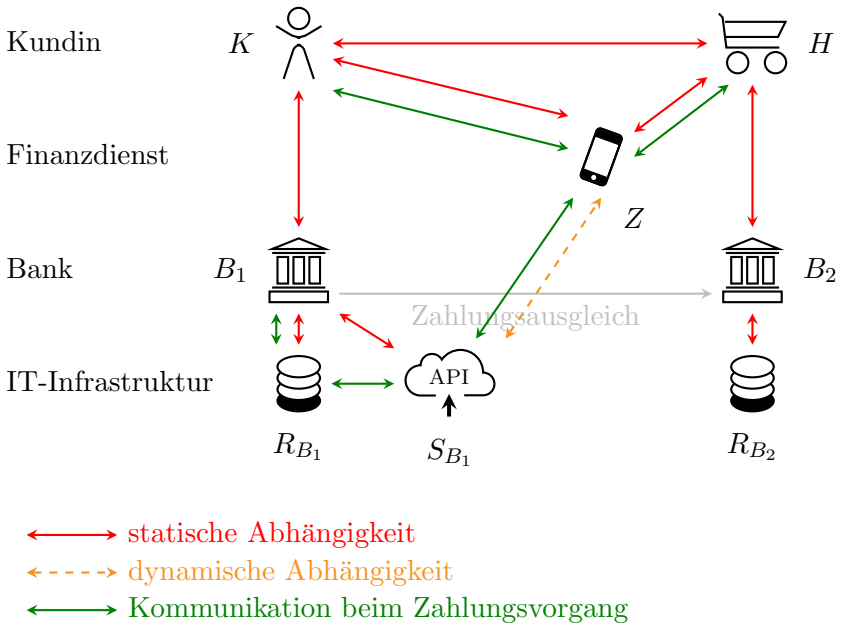

Abbildung 5: Auslagerung von Schnittstellendiensten: Erweiterung von Abbildung 3 um die Sicht auf die IT-Infrastruktur.

2.4 Relevanz der Schnittstellen-Topologie

Der IT-Aufsicht könnte es durch ihren Fokus auf einzelne Beaufsichtigte und deren (nicht direkt beaufsichtigte) IT-Dienstleisterinnen schwer fallen, Schwachstellen und systemische Risiken effizient zu identifizieren, auch wenn der Aufsicht hierzu Instrumente[8] zur Verfügung stehen.

Direkte Prüfungen der IT-Dienstleisterinnen und der ergänzende Nachweis von Prüfzertifikaten für bestimmte Dienstleistungen versprächen im Falle zentraler IT-Dienstleisterinnen Effizienzvorteile gegenüber Einzel- und Mehrfachprüfungen über den jeweiligen Umweg der beaufsichtigten Unternehmen. Beispielsweise könnte die Anbieterin S_{B_1} aus Abbildung 5 in der Gesamtschau aller beaufsichtigten Auftraggeberinnen geprüft werden und die Prüfungsergebnisse der Aufsicht könnten allen abhängigen Parteien zur Verfügung gestellt werden. Eine entsprechende Weitergabe von unternehmensinternen Informationen ist der Aufsicht aber aktuell rechtlich nicht möglich. Beaufsichtige Unternehmen stellen der Aufsicht teilweise gebündelt Berichte der Revisoren ihrer IT-Dienstleisterinnen zur Verfügung. Solche Sammelprüfungen werden letztlich nur auf Initiative der Beaufsichtigten durchgeführt. Zertifizierungen, denen indes nur ergänzende Aussagekraft zukommt, kommen nur auf Initiative derer Dienstleisterinnen zum Einsatz.

Die Aufsicht erhält lediglich, vermittelt über Beaufsichtigte, Einsicht in Prüfergebnisse und kann damit ggfs. Rückschlüsse ziehen und Maßnahmen ableiten, die mehrere Marktteilnehmerinnen betreffen. Allerdings helfen auch Sammelprüfungen oder Zertifizierungen nicht über die mit dynamischen Abhängigkeiten einhergehenden Schwierigkeiten hinweg. Potenzielle Risiken durch dynamische Abhängigkeiten – die per se schwieriger zu überblicken sind (siehe Abschnitt 2.2) – können möglicherweise nur unzureichend oder nicht rechtzeitig erhoben werden.

Abbildung 6 skizziert dies für ein fiktives Szenario (zu einem Zeitpunkt). Auf der linken Seite ist

[8] Siehe etwa EBA/GL/2017/05 v. 11. Mai 2017, Final Report, Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP).

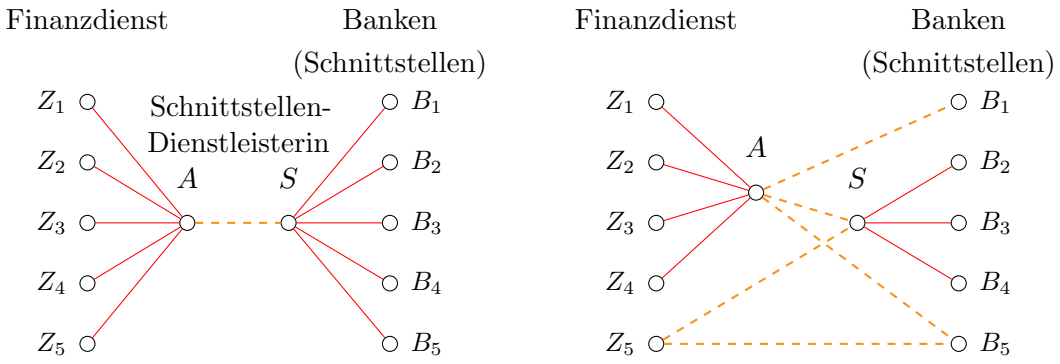

Abbildung 6: Schematische Darstellung der Schnittstellen-Topologie im Zahlungssektor. Links: Idealisierte Auslagerung an jeweils eine Schnittstellen-Dienstleisterin auf der Seite der Finanzdienste (A) bzw. Banken (S). Rechts: Realistischere Situation mit partieller Unterstützung und strategischer Inkompatibilität. Nicht alle Banken lagern ihr API-Angebot aus und einzelne Finanzdienste umgehen Schnittstellen-Dienstleisterinnen unter Verzicht auf volle Abdeckung aller Banken.

die am Markt beobachtbare Standardisierungsbemühung in Idealform dargestellt. Im Unterschied zur „Lehrbuch-Topologie“ in Abbildung 4 (rechts) ist hier berücksichtigt, dass sowohl Banken als auch dritte Finanzdienste Schnittstellen auslagern (an S) bzw. Schnittstellen einkaufen (von A). Diese Entwicklung hat sich bereits im Vorfeld der gesetzlichen Neuregelungen abgezeichnet und seitdem weiter entwickelt.

Allerdings weicht die Realität von der Idealform ab und gleicht eher der Darstellung auf der rechten Seite in Abbildung 6. Da Schnittstellen-Dienstleisterinnen bei hohen Anpassungskosten zu natürlichen Monopolen werden, könnte deren Preisgestaltung einige Banken und FinTech-Unternehmen zur Umgehung motivieren.

Banken, die S umgehen (wie B_1 und B_5 in Abbildung 6), müssen die gesetzlichen Minimalanforderungen an die Schnittstelle selbst implementieren und diese warten. Das Gesetz gibt aber lediglich die zur Verfügung zu stellenden Funktionen vor, nicht jedoch die technische Spezifikation der Schnittstelle. Wenn ein signifikanter Anteil der Banken die gesetzlichen Anforderungen mit eigenen Implementierungen erfüllt, steigt der Wert von A für Finanzdienste, für die die Nutzung einer einheitliche Schnittstelle wirtschaftlicher ist.

Finanzdienste, die A umgehen (wie Z_5 in Abbildung 6) sind dagegen nicht gezwungen, Kompatibilität zu allen Banken herzustellen. Dies kann zu Abdeckungslücken führen, welche für am Markt wenig nachgefragte Relationen (d.h. Kombinationen aus Banken, Zahlungsdiensten und Schnittstellendiensten) am ehesten zu erwarten sind. Sollte allerdings eine Teilnehmerin Marktmacht besitzen, könnten derartige Lücken durch Inkompatibilität prinzipiell auch strategischer Natur sein. Die Konsequenzen solcher Lücken sind schwer quantifizierbar, da sie sich in erster Linie in unzufriedenen Nutzerinnen der Finanzdienste ausdrücken. Ein nicht erwartungskonformes Benutzungserlebnis ist stets potenzielles Einfallstor für Informationssicherheitsrisiken, da Kundinnen oft nicht in der Lage sind, die Funktionsweise neuartiger Sicherheitsmechanismen zu verstehen, und damit leichter auf Täuschungsversuche hereinfallen (Downs et al., 2007). Nehmen Abdeckungslücken überhand, könnte das Vertrauen in Teile des Zahlungssektors erodieren und andere elektronische Zahlungsmethoden Marktanteile gewinnen.

2.5 Zusammenfassung

Die Veränderungen im Zahlungssektor bringen neue Akteurinnen ins Spiel, welche miteinander über eine Vielzahl statischer (d. h. vertraglich geregelter) und dynamischer Abhängigkeiten verflochten sind. Die Art und Anzahl der Verflechtungen nimmt insbesondere durch die Auslagerung von IT deutlich zu. Keine Marktteilnehmerin und keine Behörde hat darüber jederzeit vollständige Information. Erschwerend kommt hinzu, dass IT-Dienstleisterinnen oft nicht direkt beaufsichtigt werden und die Effektivität der mittelbar über die Beaufsichtigten wirkenden Aufsicht mit zunehmender Auslagerungstiefe abnehmen könnte. Mit der Verteilung von Wertschöpfungsketten auf viele Akteurinnen geht eine Zerstückelung von Prozessen einher. Dies erschwert die Identifikation von potenziellen Schwachstellen und die finanzielle und technische Risikokontrolle. Wenn Risiken und Kontrollmöglichkeiten auf unterschiedliche Akteurinnen verteilt sind, besteht die Gefahr des Marktversagens bei der Bereitstellung eines angemessenen Sicherheitsniveaus.

3 Szenarien

Im Folgenden werden die drei zur anschließenden Validierung entwickelten Szenarien dargestellt. In jedem der drei Unterabschnitte 3.1, 3.2 und 3.3 wird zunächst das jeweilige Szenario beschrieben und anschließend begründet. Die ersten beiden Szenarien beschreiben näherliegende Szenarien, nämlich die Förderung von Cyberkriminalität (siehe 3.1) sowie die Konzentration von IT-Infrastruktur (siehe 3.2). Das dritte Szenario (siehe 3.3) beschreibt mit einer Machtverschiebung auf IT-Unternehmen eine zugespitzte, weiter in der Zukunft liegende mögliche Entwicklung, die auf der im zweiten Szenario beschriebenen Konzentration beruht. Die ausführliche Beschreibung der Szenarien in den folgenden Unterabschnitten wurde ausschließlich projektintern verwendet (zu der den Interviewpartnern zur Verfügung gestellten Fassung der Szenarien siehe 4.1 mit Verweis auf Anhänge 2a und 2b).

3.1 Szenario 1: Neue Schnittstellen fördern Cyberkriminalität

Szenario: Stark arbeitsteilig, international und bandenmäßig organisierte Cyberkriminelle werden die neue Situation nutzen, um Straftaten zu begehen. Die erhöhte Komplexität gepaart mit ggfs. fehlenden Anreizen zu IT-Sicherheitsmaßnahmen der Zahlungsdienste führt auch zum Einfallstor für neuartige Modi Operandi. Insbesondere werden Cyberkriminelle die Authentifikationsmechanismen der Banken für dritte Zahlungsdienstleisterinnen umgehen. Soweit sie nicht mit einer Inanspruchnahme durch die für nicht autorisierte Zahlungsvorgänge gegenüber den Kundinnen haftenden Banken oder Reputationsverlusten rechnen, werden Zahlungsdiensteanbieterinnen von IT-Sicherheitsmaßnahmen zur Verhinderung nicht autorisierter Zahlungen in ihrem Einflussbereich absehen und Cyberkriminelle dadurch bestehende Schwachstellen gezielt ausnutzen. Finanzdienstleisterinnen werden Risiken in bestimmten Umfang akzeptieren und in Form höherer Kosten auf Kundinnen umlegen, statt ihre Ursachen zu erfassen und zu beheben.

Die Wirkung von ausdifferenzierten Wertschöpfungsketten auf Kriminalität **gründet auf** den folgenden, sich gegenseitig verstärkenden Faktoren, auf die anschließend in den Unterabschnitten im Einzelnen eingegangen wird: Die zunehmende Schnittstellenkomplexität vergrößert die Angriffsfläche (3.1.1). Bekannte Sicherheitstechnologien sind nur bedingt zur Verteidigung stark arbeitsteilig und dynamisch organisierter Wertschöpfungsketten geeignet (3.1.2). Transaktionskosten bei der Aufklärung von Straftaten und der Schadensregulierung führen zu dysfunktionalen Verhaltensanpassungen (3.1.3).

Die Betrachtung hier konzentriert sich auf Betrug und im weitesten Sinne Identitätsdiebstahl. Bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung handelt es sich um weitere relevante Aspekte, die hier allerdings nicht im Mittelpunkt stehen.

3.1.1 Vergrößerung der Angriffsfläche

Je verteilter ein System realisiert ist, desto schwieriger ist es gegen Angriffe zu schützen. Jede Schnittstelle ist als potenzielle Fehlerquelle anzusehen. Dies lässt sich am Beispiel von – auf höchste Sicherheitsanforderungen ausgelegten – HSMs[9] aufzeigen. Bei HSMs konnte kryptographisches Schlüsselmaterial durch geschickte Kombination von Anfragen an deren Schnittstelle unberechtigt ausgelesen werden (Anderson, 2008, Kap. 18). Dies gelang, obwohl die Schnittstellen

[9] Hardware Security Modules bezeichnen Spezialhardware zum Schutz kryptographischer Schlüssel gegen physische Angreiferinnen.

bewusst überschaubar gehalten waren und jede Anfrage für sich genommen für sicher befunden werden konnte. Der bekanntgewordene Schaden war in diesen Beispielen gering, mutmaßlich weil diese Systeme nur mit bankinternen Netzen verbunden waren und im Wesentlichen als Schutz gegen den Zugriff von Insidern z. B. auf Karten-PINs dienten.

Die mit den Neuregelungen einhergehende Bereitstellung von Schnittstellen für eine nicht vorab spezifizierte Menge an Finanzdiensten erfordert, dass die neuen Schnittstellen, anders als HSM-Schnittstellen, vom Internet aus erreichbar, also offen sind. Damit sind sie im Unterschied zu HSMs mit einer Angriffsoberfläche weltweiter Dimension exponiert. Dies gilt auch für nur zur internen Kommunikation bestimmte offene Schnittstellen.

Überträgt man das Gefahrenpotenzial bekannter HSM-Schwachstellen in das Szenario ausdifferenzierter Wertschöpfungsketten im Zahlungsverkehr, ist damit zu rechnen, dass Cyberkriminelle versuchen werden, die Authentifikationsmechanismen für dritte Zahlungsdienstleisterinnen bei kontoführenden Zahlungsdienstleisterinnen zu umgehen – möglicherweise indirekt durch Umgehung der Authentifikation einer Dienstleisterin der dritten Zahlungsdienstleisterin. Dies wäre etwa denkbar bei einer Kompromittierung einer Anbieterin von eIDAS-Zertifikaten, aber auch einem Angriff auf andere IT-Dienstleisterinnen, über welche die Zahlungsdienstleisterinnen mit Banken kommunizieren, z. B. Schnittstellen-Dienstleisterinnen.

Damit könnten sie die Schnittstelle der kontoführenden Zahlungsdienstleisterin mit den Berechtigungen einer (impersonifizierten) dritten Zahlungsdienstleisterin nutzen. Ein solcher Angriff ist für die Bank zunächst praktisch nicht erkennbar. Selbst die Verfolgung der Täterinnen durch eine forensische Analyse der Netzwerk-Daten kann ins Leere führen, da Cyberkriminelle in der Regel kompromittierte Rechner Unbeteiligter als Zwischenstationen nutzen.

Gemeinsame Fehlerursache der genannten Schwachstellen von HSMs war „Featuritis“, die schrittweise Ergänzung von Funktionen, welche in ihrem Zusammenspiel unüberschaubar und fehlerträchtig werden. Eine kombinatorische Abschätzung ergibt, dass die Anzahl der Kombinationsmöglichkeiten mindestens quadratisch mit der Anzahl der Funktionen einer Schnittstelle wächst. Die Sicherheit ist bereits dann gefährdet, wenn eine einzige von allen möglichen Kombinationen unberechtigten Zugriff ermöglicht. Selbst die in der modernen Softwareentwicklung empfohlenen – jedoch keineswegs weit verbreiteten – automatisierten Tests können derartige Fehler nicht oder nur mit erheblichem Aufwand aufspüren.

Es liegt nahe, dass die neuen Schnittstellen im Finanzsektor nicht minimal konzipiert werden: Zwar besteht seitens der Banken, isoliert betrachtet, kein Interesse daran, über die gesetzlichen (Mindest-)Anforderungen hinausgehende Schnittstellen anzubieten. Allerdings haben andere Akteurinnen, nämlich Anbieterinnen von Finanzdiensten oder auf deren Seite eingeschaltete Schnittstellen-Dienstleisterinnen, Interesse an einer Vielzahl an Schnittstellen, um Endkundinnen eine Vielzahl verschiedener Funktionen anbieten zu können. Hierdurch wächst Druck auf die Banken, entsprechend umfangreiche Schnittstellen anzubieten. Hierbei könnte sich eine Tendenz zugunsten der Funktionalität und Benutzungsfreundlichkeit und zulasten der IT-Sicherheit der Zahlungssysteme ergeben. Kosten- und Zeitdruck, getrieben durch die Aussicht auf First-Mover-Vorteile, führen in der Softwareentwicklung traditionell zu einer Priorisierung funktionaler Eigenschaften zu Lasten nicht-funktionaler Eigenschaften wie Sicherheit (Anderson und Moore, 2006).

Auch der FinTech-Sektor unterliegt dieser Logik. Schnittstellen-Dienstleisterinnen wie A in Abbildung 6 sind prädestiniert, Funktionen anzubieten, die über das gesetzlich vorgeschriebene Minimum hinausgehen.

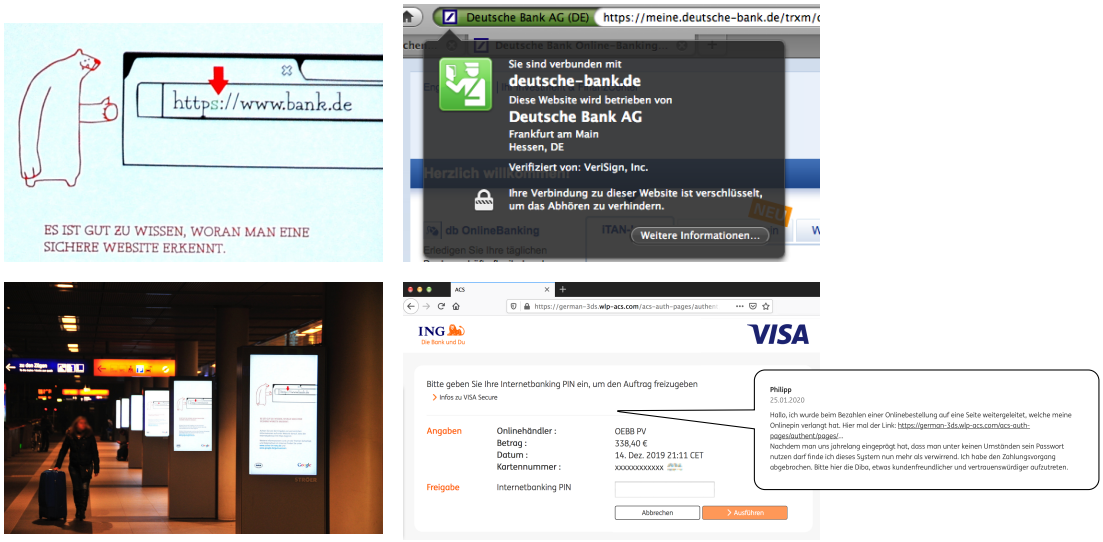

Abbildung 7: Beispiel für inkonsistentes Benutzungserlebnis mit Sicherheitsverlust: Außenwerbung zur Erklärung der Sicherheitsmerkmale von HTTPS (Berlin Hbf, 2011, links); Darstellung einer mit EV-Zertifikat gesicherten HTTPS-Verbindung im Browser (ca. 2012, oben rechts); überraschende Aufforderung zur Eingabe der Online-Banking-PIN im Zahlungsprozess einer Händlerin auf einer nicht offensichtlich mit der Bank zusammenhängenden Domain einer Drittanbieterin (unten rechts, 2019); Beispiel für Kundenreaktion (Sprechblase).

Die Angriffsfläche wächst nicht nur auf der technischen Dimension. Die Sicherheit von an Verbraucherinnen gerichteten Zahlungssystemen hängt maßgeblich davon ab, dass Benutzerinnen die den Sicherheitsmechanismen zugrunde liegende Logik zumindest ansatzweise verstehen und sich auch dann richtig verhalten, wenn Cyberkriminelle zu Fehlverhalten anstiften. Phishing-Angriffe auf Bankkundinnen gibt es seit der ersten Stunde des Online-Bankings. Sie verursachen erhebliche Kosten, monetär in Form von Sicherheitsinvestitionen sowie dem Ersatz von Kundenguthaben und nicht-monetär in Form eines Vertrauensverlusts in Online-Banking (Riek et al., 2016; Böhme, 2018). Bisherige Investitionen in Aufklärung und Anleitungen zum sicheren Verhalten im Internet sind nutzlos, wenn die mühsam erlernten Regeln aus für Endkundinnen nicht nachvollziehbaren Gründen plötzlich nicht mehr gelten (Abbildung 7). Zudem ist die Erstellung allgemein gültiger Anleitungen wegen der Vielzahl unterschiedlicher Endgeräte mit unterschiedlicher Software seitens der Endkundinnen kaum mehr möglich, näher beschrieben in 3.1.2.

3.1.2 Schwierigkeit effektiver Verteidigung

Je ausdifferenzierter Wertschöpfungsketten sind, desto schwerer lassen sie sich gegen Angriffe absichern. Beginnend mit der Benutzerinnensicht, machen es unterschiedliche Benutzungserlebnisse zwischen (Kombinationen von) Anbieterinnen sowie im Zeitverlauf praktisch unmöglich, allgemein gültige Anleitungen zu formulieren und in einschlägigen Medien zu verbreiten. Auch fällt es selbst fachlich versierten Personen schwerer, verbindliche Handlungsanweisungen an Menschen in ihrem Umfeld weiterzugeben. Das Haupteinfallstor bei z. B. Pishing ist nach wie vor die Unwissenheit der Benutzerinnen; so werden Warnhinweise wie z. B. durch den Browser ignoriert (Downs et al., 2007). Passende Anti-Pishing-Trainings sind nicht immer verfügbar oder

haben Verbesserungsbedarf. Beispielsweise wären angewandte Trainings („embedded trainings“) am effektivsten (Jansen und Leukfeldt, 2015). Das alleinige Hinweisen auf Pishing über Webseiten ist unzureichend, um Endnutzerinnen aufzuklären (Wash und Cooper, 2018). Wenn Quellen für verlässliche Informationen wegfallen bzw. die Verlässlichkeit nicht mehr gut einschätzbar ist, wird es für Cyberkriminelle leichter, unbemerkt auf Seiten von Benutzerinnen in Zahlungsvorgänge einzugreifen.

Auch aus technischer Sicht lässt sich ein Ökosystem mit vielen offenen Schnittstellen kaum effektiv absichern. Netzarchitekturen mit klarer Trennung zwischen vertrauenswürdigem internen und nicht vertrauenswürdigem externem Netz, mit kontrollierten und durch technische Maßnahmen abgesicherten Übergabepunkten (Paketfilter[10], DMZ[11], DDoS-Abwehr[12]), konnten in der bisherigen Praxis interne Schnittstellen weitgehend abschirmen. Diese sogenannte Perimeter-Sicherheit ist nicht vereinbar mit der Idee offener Schnittstellen. Vielmehr muss nunmehr jede einzelne Schnittstelle durch technische Maßnahmen abgesichert werden. Dadurch erhöhen sich die Komplexität, das Risiko von Sicherheitslücken durch Fehlkonfigurationen und die Kosten.

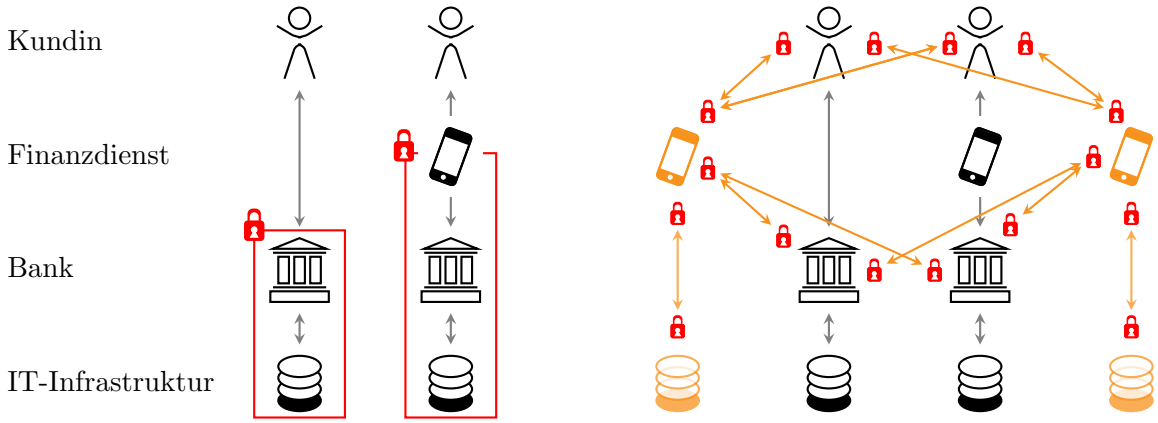

Abbildung 8: Visualisierung des Unterschieds zwischen der Absicherung von internen Schnittstellen (linkes Bild) und offenen Schnittstellen (rechtes Bild)

Beispielsweise kommen in ausdifferenzierten Wertschöpfungsketten eine Vielzahl von Berechtigungsmanagementsystemen (BaFin, 2017a, S. 11–12) zum Einsatz. Diese implementieren verschiedene Zugriffskontrollmodelle, folgen keiner einheitlichen Terminologie und grenzen Rollen von Berechtigten unterschiedlich ab. Zwar wird jedes Berechtigungsmanagementsystem für sich genommen direkt (bei Beaufsichtigten) oder indirekt (bei Auslagerungen an nicht beaufsichtigte Marktteilnehmerinnen) von der IT-Aufsicht geprüft. Trotzdem besteht fallweise das Risiko, dass eine vollständige Gesamtschau unter Berücksichtigung aller Beteiligten und ihrer Abhängigkeiten untereinander nicht stattfinden kann. Ohne diese lässt sich nicht beurteilen, ob ein System, das heißt die Gesamtheit der an einem Zahlungsvorgang beteiligten technischen Komponenten, tatsächlich sicher ist. Die Tatsache, dass jede einzelne Teilnehmerin hohe Vorgaben erfüllt, ist notwendig, aber nicht hinreichend für die Gesamtsicherheit.[13] Dies lässt sich vergleichen mit der

[10] Paketfilter (oder Netzwerkfilter) filtern den ein- und ausgehenden Datenverkehr in einem Netz und werden auch als Firewalls bezeichnet.

[11] Als DMZ (demilitarisierte Zone) wird ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server bezeichnet.

[12] Als DDoS (Distributed-Denial-of-Service) wird ein Angriff auf die Verfügbarkeit, verursacht durch Anfragen einer Vielzahl von Quellen, bezeichnet.

[13] Beispiele hierfür siehe Canetti (2001).

Beurteilung der Verträglichkeit eines Medikaments, das gemeinsam mit anderen Medikamenten eingenommen wird. Schädliche Wechselwirkungen zeigen sich nur in der Gesamtschau.

Die Erkennung von Mustern und Anomalien mittels spezifischer Verfahren (BaFin, 2018a, Kapitel 3.2.2 und 7.1.2) kann die Verteidigung gegen Angriffe auf Ebene des Netzwerkes sowie die Betrugserkennung unterstützen. Diese erfordern eine große und möglichst homogene Informationsbasis über legitime Transaktionen sowie detaillierte Informationen über auffällige Transaktionen zur Echtzeit. Kleinteilige Wertschöpfungsketten erschweren mitunter den Blick auf nützliche Daten. Zeitliche Variabilität in der Nutzung dynamischer Abhängigkeiten reduziert die Menge homogener Transaktionen, z. B. weil Marktteilnehmerinnen die Informationen als Geschäftsgeheimnisse betrachten oder die datenschutzrechtliche Grundlage zur Weitergabe nicht eindeutig vorhanden ist. Dies führt zu einer geringeren Sensibilität automatischer Detektionsverfahren. Auch die Spezifität ist reduziert, wenn Umkonfigurationen der Wertschöpfungskette fälschlich als Anomalien klassifiziert werden. Wie für alle Formen automatischer Angriffs- und Betrugserkennung gilt auch für Muster-basierte Verfahren, dass sich ihre Güte durch hohe Sensibilität bei gleichzeitig hoher Spezifität bestimmt.

3.1.3 Transaktionskosten in der Aufarbeitung

Die gesetzliche Haftungsverteilung sowie die aufsichtsrechtlichen Vorgaben an die IT-Sicherheit (siehe Abschnitt 2.1) für Dienste nach der PSD2 sind im Prinzip geeignet, die Marktteilnehmerinnen dahingehend zu disziplinieren, dass die Angriffsfläche nicht übermäßig wächst sowie effektive Sicherheitstechnologien entwickelt und eingesetzt werden. Trotzdem unvermeidbare Restrisiken werden auf die verursachende Partei bzw. deren Versicherung übertragen.

Die Steuerungswirkung der gesetzlichen Haftungsregelungen, wie z. B. dem Ausgleichsanspruch von Banken gegen Zahlungsdienstleisterinnen aus § 676a Abs. 1 BGB auf Ersatz des durch die Rückererstattung an Kundinnen im Falle nicht-autorisierter Zahlungen gem. § 675u BGB entstandenen Schadens, hängt aber von der effizienten Durchsetzbarkeit der rechtlichen Ansprüche ab.[14] Ist so ein Anspruch strittig und nur gerichtlich durchsetzbar, können die Transaktionskosten um ein Vielfaches höher als der Anspruch sein. Der Rechtsweg lohnt sich dann nur in sich wiederholenden Fällen, z. B. bei systematischem Fehlverhalten oder wenn Cyberkriminelle eine Informationssicherheitslücke in der Wertschöpfungskette entdecken und gezielt vermehrt ausnutzen. Der Rechtsweg könnte sich selbst in diesen Fällen als ungeeignet erweisen. Denn es besteht die Gefahr, dass die zur Zahlung verpflichteten Marktteilnehmerinnen im Laufe des Prozesses aus dem Markt ausscheiden. Dies kann unter anderem dann passieren, wenn die Beklagte den finanziellen Verlust nicht selbst verursacht hat, sondern ihn wiederum von Dritten (z. B. unregulierte oder gar unerlaubt tätige Dienstleisterinnen) einfordern muss und der zwischenzeitliche Liquiditätsabfluss zur Insolvenz führt. Insgesamt bleibt zu erwarten, dass die Beteiligten solche Risiken in gewissem Umfang akzeptieren (und in Form höherer Kosten auf Kundinnen umlegen), statt ihre Ursachen zu ermitteln und Maßnahmen zur Vermeidung ihres Eintritts zu treffen.

Noch deutlicher wird das Problem der Transaktionskosten im internationalen Kontext. Cyberkriminelle agieren bewusst international, um die Strafverfolgung zu behindern und Durchset-

[14] Nicht autorisierte Zahlungen waren auch vor den Neuregelungen zu erstatten. Im Kontext von Cyberkriminalität entstehen viele Verluste durch betrügerisch bzw. missbräuchlich initiierte Zahlungen. Dabei hatten es die Institute selbst in der Hand, Anzeichen für Betrug auszuwerten und Zahlungen zurückzuhalten. Diese Prozesse verteilen sich nach den Neuregelungen auf mehrere Marktteilnehmerinnen.

zungslücken auszunutzen (Anderson et al., 2008). Zwar gelten innerhalb des EWR aufgrund der vollharmonisierten Richtlinie identische Vorgaben. Dies begrenzt die Möglichkeit zur regulatorischen Arbitrage theoretisch. Im Inland beaufsichtigte Banken und FinTech-Unternehmen können diesen Risiken ausgesetzt sein, wenn Teile der Wertschöpfungskette aus Drittstaaten operieren.

Jedoch erhöhen sich die Transaktionskosten der Durchsetzung bis hin zu faktischen Durchsetzungslücken. Laut Eoyang (2018) gab es in weniger als 1% der jährlichen Fälle an Cyberkriminalität in den Vereinigten Staaten eine Festnahme. Cyberkriminelle können sich angesichts der weitgehend fehlenden Rechtsdurchsetzung nahezu sicher sein, nicht zur Rechenschaft gezogen zu werden (Peters und Jordan, 2019).

3.2 Szenario 2: Konzentration der IT-Infrastruktur

Szenario: Die IT-Infrastruktur, d. h. die Gesamtheit von Software und Hardware, des Finanzsektors wird sich in verschiedenen Auslagerungstiefen konzentrieren. Sowohl Banken als auch andere Zahlungsdienstleisterinnen werden gleichermaßen an branchenspezifische IT-Dienstleisterinnen auslagern. Um branchenspezifische IT-Dienstleisterinnen handelt es sich z. B. bei Anbieterinnen spezifischer Schnittstellen oder von Banking-as-a-Service-Plattformen. Diese nutzen wiederum über eine oder mehrere Ebenen die gemeinsame Infrastruktur internationaler dritter IT-Dienstleisterinnen, insb. Cloud-Anbieterinnen. Eine Konzentration tritt auch bei spezialisierten IT-Unternehmen, z.B. im Bereich des App-Hardenings[15] ein. Schnittstellen-Dienstleisterinnen werden Schnittstellen nicht minimal konzipieren und Komplexitätssteigerungen bewirken, die die in Szenario 1 beschriebenen Entwicklungen begünstigen.

Dem liegen **folgende Erwägungen** zugrunde, die in den Unterabschnitten näher ausgeführt werden. Einerseits besteht im IT-Sektor eine allgemeine Tendenz zur Auslagerung von IT-Infrastruktur an große IT-Dienstleisterinnen. Andererseits wird diese Entwicklung begünstigt durch eine speziell für den Finanzsektor angenommene Steigerung der Komplexität von Dienstleistungen.

3.2.1 IT-Sektor-typische Auslagerung

Die im gesamten IT-Sektor zu beobachtende Tendenz zur Auslagerung von IT-Infrastruktur an IT-Dienstleisterinnen, insb. Cloud-Anbieterinnen, beruht auf der kostengünstigen Skalierbarkeit von IT-Diensten. Die für den IT-Sektor charakteristische Kostenstruktur aus hohen Fixkosten, z. B. in der Softwareentwicklung, gepaart mit niedrigen variablen Kosten begünstigt Konzentration auf der Angebotsseite (FSB, 2019, S. 8 ff.).

Internationale Cloud-Dienstanbieterinnen können besonders attraktive Auslagerungen anbieten, weil ihre Kapitalausstattung eine langfristige Wachstumsstrategie ermöglicht, die Larkin (2008) als "Bargains-then-Ripoffs"-Strategie bezeichnet. Er bezieht sich dabei auf das von Shapiro und Varian (1998) beschriebene Vorgehen, in welchem IT-Unternehmen Dienstleistungen anfänglich preisgünstig oder sogar kostenlos anbieten, bis sie so etabliert sind, dass der Markt fast nicht mehr oder nur noch schwer auf sie verzichten kann. Erst dann wird die Dienstleistung bepreist bzw. der Preis angehoben.

[15] Unter App-Hardening wird die programmiertechnische Absicherung der Integrität der Ausführungsumgebung einer App verstanden (Haupert et al., 2018, Kapitel 2).

Zahlungsdienstleisterinnen (sowie ggfs. deren IT-Dienstleisterinnen), die in der „Bargain"-Phase an (andere) IT-Dienstleisterinnen auslagern, beziehen Leistungen oft unter deren Entwicklungs- und Betriebskosten. Interne Alternativen erscheinen dazu im Vergleich zunächst unwirtschaftlicher. Allerdings sind anfängliche Kostenvorteile möglicherweise nur kurzfristig realisierbar, denn die Preise in der „Ripoff"-Phase orientieren sich an den Wechselkosten der Kundin. Diese können sehr hoch sein, wenn die Kundin auf die Dienstleistung angewiesen ist, ihre Software und Daten aus technischen oder rechtlichen Gründen nicht leicht portierbar sind oder die IT-Dienstleisterin derartige Marktmacht erlangt hat, dass praktisch keine Alternativen zur Verfügung stehen.

Beispiele für die Anwendung solcher „Bargains-then-Ripoffs"-Strategien gibt es viele. So stiegen die Preise für das Einbetten der *Google Maps*-API in Webseiten sprunghaft an.[16] Die Schnittstelle war zunächst kostenlos zu nutzen, was zahlreiche Entwicklerinnen von Apps mit Karten- und Navigationselementen (beispielsweise für Hotel- oder Tagungsbesucher) zur Anbindung veranlasste. Diese Entwicklerinnen sahen sich daraufhin einer Preissteigerung um ein Vielfaches ausgesetzt. Nicht nur private Akteurinnen, sondern auch solche des öffentlichen Sektors sind hiervon betroffen. So wurde etwa der Lock-In von Strafverfolgungsbehörden durch den Informationsdienst *Palantir* durch die Fachmedien bekannt:[17] Zu den Kundinnen der auf Big-Data-Analysen spezialisierten Anbieterin forensischer Software und Dienstleistungen gehören neben privaten Kundinnen insbesondere US-amerikanische Polizeibehörden, Nachrichtendienste und weitere Behörden wie etwa Europol[18]. Diese wurden durch niedrige Preise und die Datenbasis des Dienstes zur Nutzung des Dienstes einschließlich der Preisgabe ihrer Daten bewegt, was schließlich zu einer Abhängigkeit der Behörden von dem Dienst für die Erfüllung wesentlicher Aufgaben geführt hat. Neben Problemen mit Datenschutz und Geheimhaltung sahen sich die Behörden daraufhin Qualitätsmängeln und angestiegenen Preisen ausgesetzt. Dabei ist der Wechsel der Cloud-Anbieterin häufig nicht möglich, weil Daten nicht von einer Cloud-Anbieterin zu einer anderen übertragbar sind (mangelnde Datenportabilität) oder Daten und Anwendungen auf dem System einer anderen Cloud-Anbieterin nicht ohne weiteres verwendbar sind (mangelnde Interoperabilität).

In solchen Fällen ist die Kundin laut Shapiro und Varian (1998) eingesperrt („Lock-In") und für das IT-Unternehmen besonders wirtschaftlich.[19] Ergebnisse einer Studie von Arce (2022) zeigen, dass Cloud-Anbieterinnen sich durch langfristige Kundenbindung einen größeren Vorteil am Markt verschaffen können als über Preisstrategien. Dabei werden Kundinnen gezielt in eine Situation gedrängt, in der ein Wechsel der Cloud-Anbieterin aufgrund mangelnder Datenportabilität und Interoperabilität unwirtschaftlich oder sogar unmöglich ist. Das geht so weit, dass angebotene Sicherheitsmaßnahmen nicht zur Absicherung gegen Cyberangriffe durch Dritte, sondern zur weiteren Verstärkung der Kundenbindung eingesetzt werden. Für Kundinnen stellen die Sicherheit ihrer Daten sowie die Erreichbarkeit im Falle eines Ausfalls der Cloud-Anbieterin essentielle Faktoren dar. Dieses Vorgehen wird als "Security-induced Lock-in" bezeichnet (Lookabaugh und Sicker, 2004). Maßnahmen, die diese strategischen Optionen einschränken, wie etwa die

[16] Singh, Insane, shocking, outrageous: Developers react to changes in Google Maps API (2018), abrufbar unter `https://geoawesomeness.com/developers-up-in-arms-over-google-maps-api-insane-price-hike/` (letzter Abruf: 18.07.2022).

[17] Harris, How Peter Thiel's Secretive Data Company Pushed Into Policing (2017), abrufbar unter `Https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/` (letzter Abruf: 18.07.2022).

[18] Europäisches Parlament, Parlamentarische Anfrage E-000173/2020(ASW), Antwort von Frau Johansson im Namen der Europäischen Kommission `https://www.europarl.europa.eu/doceo/document/E-9-2020-000173-ASW_EN.html` (letzter Abruf: 18.07.2022)

[19] Zur Lock-In-Problematik siehe auch FSB (2019, p. 12 ff.).

Vereinheitlichung von Schnittstellen und Einführung von homogenen Standards, sind daher für IT-Dienstleisterinnen wie insbesondere Cloud-Anbieterinnen unattraktiv. Vielmehr versuchen sie sich durch immer komplexere und noch individuellere Lösungen von der Konkurrenz abzuheben.

Für Banken und andere Finanzdienstleisterinnen, die in diesem Umfeld unter Zeit- und Kostendruck Angebote schaffen wollen, ist die Auslagerung von IT-Dienstleistungen attraktiv. Sie verspricht Flexibilität und bindet nur wenig Personal in Prozessen jenseits des Kerngeschäfts. Eingekaufte IT-Dienste sind bereits dann günstiger als Eigenentwicklungen, wenn die IT-Dienstleisterin ihre Fixkosten auf mehrere Kundinnen verteilen kann. Zudem können Lohnkostenunterschiede zwischen branchenspezifischen Tarifverträgen zum Tragen kommen. Im internationalen Kontext können darüber hinaus unterschiedliche Lohnniveaus der weltweit verteilten Mitarbeiterinnen von Dienstleisterinnen zur Kostensenkung ausgenutzt werden.

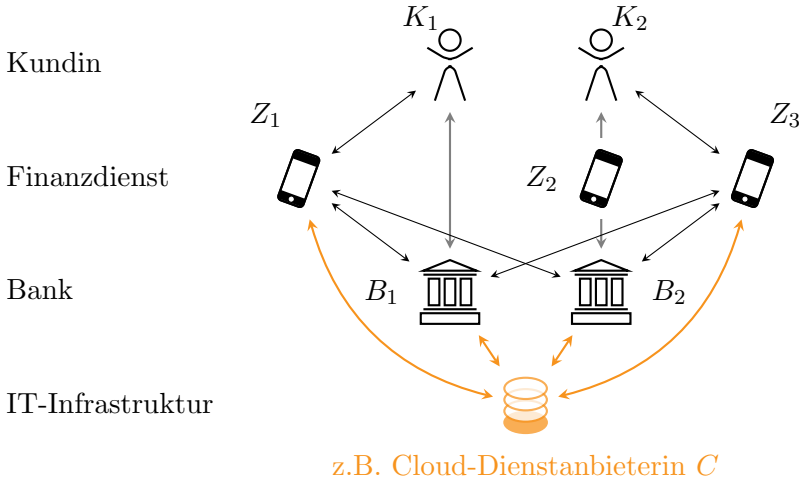

Abbildung 9: Szenario 2 – Konzentration der IT-Infrastruktur

Abbildung 9 veranschaulicht das Szenario der Auslagerung auf große IT-Dienstleisterinnen. Sowohl Banken, als auch (andere) Anbieterinnen von Finanzdiensten benutzen hier dieselbe IT-Infrastruktur. Sowohl Bank B_1 als auch Bank B_2 lagern z. B. die Bezahlung am PoS[20] via App an dritte Finanzdienste (Z_1, Z_2, Z_3) aus.

Eine Konzentration von IT-Infrastruktur kann nicht nur bei Cloud-Anbieterinnen, sondern auch – weniger offenkundig – bei speziellen, in der Öffentlichkeit weniger wahrgenommenen IT-Dienstleisterinnen entstehen. Im Zusammenhang mit Apps ist eine Konzentration von IT-Dienstleistungen bei der Programmierung zu verzeichnen, nämlich beim App-Hardening. Ziel ist es, dass nur benötigte Software eingesetzt wird, deren korrekter Ablauf weitgehend garantiert werden kann. Das System soll daher besser vor Angriffen geschützt sein. So sollen Nutzerinnen etwa außerstande versetzt werden, Apps auf Smartphones zu verwenden, bei denen Beschränkungen des Betriebssystems umgangen worden sind.[21] Denn solche Veränderungen des Betriebssystems reduzieren die IT-Sicherheit des Endgeräts. Durch das App-Hardening werden also Angriffsvektoren reduziert, die die von den Nutzerinnen kontrollierten Endgeräte betreffen. Problematisch ist indes, dass das Hardening einer Vielzahl von Apps von denselben IT-Dienstleisterinnen vorgenommen wird. Es existieren wenige auf das App-Hardening spe-

[20] Der PoS (Point of Sale) bezeichnet die Verkaufsstelle.
[21] Dies wird auch als Jailbreak bezeichnet, siehe dazu Kellner et al. (2019).

zialisierter Unternehmen, weshalb sich Banken und andere Finanzdienstleisterinnen vielfach derselben Anbieterinnen für das Hardening ihrer Apps bedienen. Dies geht mit dem Risiko einher, dass im Falle fehlerhaften Programmcodes der IT-Dienstleisterinnen App-basierte Finanzdienste institutsübergreifend ausfallen. Eine besondere Anfälligkeit resultiert daraus, dass App-Hardening-Techniken undokumentierte Softwarefunktionen nutzen.

Bei bestimmten Kreditinstituten, nämlich den Genossenschaftsbanken und Sparkassen, sind **Konzentrationsentwicklungen bereits zu beobachten**.[22] Die IT-Infrastruktur der mehr als 900 Genossenschaftsbanken wird von zwei Unternehmen des Finanzverbundes betreut (*Atruvia*, vormals *Fiducia & GAD IT* mit Sitz in Frankfurt, *Sopra Financial Technology* mit Sitz in Nürnberg), die der knapp 400 Sparkassen von der *Finanz Informatik*-Unternehmensgruppe mit Sitz in Frankfurt. Diese Strukturen entstanden durch mehrere Fusionen von IT-Unternehmen und Rechenzentren in den letzten 20 Jahren: 2015 durch die Fusion von *Fiducia IT* (Karlsruhe) und *GAD* (Münster) und 2019 durch die Übernahme der *Sparda*-Datenverarbeitung (SDV) durch die französische IT-Beratung *Spora Steria SA*. Dieses Unternehmen entstand durch den Zusammenschluss von insgesamt 11 unabhängigen Rechenzentren in den Jahren 1998–2008. Die Entwicklung bei den Sparkassen und Genossenschaftsbanken kann einerseits als Anzeichen für eine entsprechende Entwicklung auch bei anderen Banken gesehen werden. Andererseits macht diese schon eingetretene Konzentration bei deutschen Unternehmen eine Konzentration von Banken-IT-Infrastruktur bei internationalen IT-Dienstleisterinnen unwahrscheinlicher, soweit nicht die derzeitigen wiederum Infrastruktur auslagern.

3.2.2 Systemrelevanz von IT-Unternehmen

Durch diese Entwicklungen entstehen neue systemrelevante Unternehmen wie z. B. Plattformanbieterinnen. Systemrelevant ist ein IT-Unternehmen, von dessen Produkten oder Dienstleistungen das System als solches abhängt.[23] Das ist der Fall für IT-Unternehmen, die nicht nur kritische Auslagerungsnehmerinnen für ein beaufsichtigtes Institut sind, sondern von denen eine Vielzahl von Instituten gleichermaßen abhängt. Unter diesem Gesichtspunkt sind aber nicht nur einzelne Unternehmen als systemrelevant anzusehen, sondern auch die Verkettung von Dienstleistungen bzw. die Interaktion verschiedener Marktteilnehmerinnen. Benutzt ein Großteil der Marktteilnehmerinnen (direkt oder indirekt über Drittanbieterinnen) dieselbe Infrastruktur, um Dienste auszulagern, wird diese systemrelevant, da bei einem Ausfall ebendieser das System als solches betroffen ist. Folge der wachsenden Systemrelevanz selbst (noch) nicht beaufsichtigter IT-Dienstleisterinnen ist, dass sich die für die Angebote der Beaufsichtigten eingesetzte Infrastruktur einerseits deren Einfluss, andererseits der direkten Aufsicht entzieht.[24] Es besteht dabei das Risiko, dass Erbringerinnen systemrelevanter Dienstleistungen wegen vielfacher Auslagerung auch nicht unmittelbar funktionsrelevanter Dienstleistungen (etwa im oben beschriebenen Fall des App-Hardenings) von der Aufsicht nicht unmittelbar als solche wahrgenommen werden.

[22] Zur Entwicklung Schmitt in (Tatnall und Leslie, 2016), S. 141 ff.

[23] Der hier verwendete Begriff der Systemrelevanz bezieht sich somit nicht auf die Liste systemrelevanter Banken des Financial Stability Board (FSB).

[24] Zur Problematik auch European Systemic Risk Board (ESRB), Systemic cyber risk (Februar 2020), abrufbar unter `https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf` (letzter Abruf: 18.07.2022).

3.2.3 Komplexitätssteigerung im Finanzsektor

Die Zunahme an Komplexität der IT von Zahlungsdienstleisterinnen verstärkt die Entwicklung hin zu einer immer konzentrierteren IT-Infrastruktur. Ursachen für die zunehmende Komplexität sind u. a. **exogene Faktoren**:

Der anhaltende technische Fortschritt ermöglicht kompliziertere Produkte, insb. mit nahezu Echtzeit-Informationen. Es bestehen wirtschaftliche Anreize, solche komplizierten Produkte auch anzubieten. Der gesteigerter Wettbewerbsdruck in der Branche führt zu einer Ausdifferenzierung am Markt, in deren Folge die neuen technischen Möglichkeiten auch genutzt werden. Das ist auf veränderte Erwartungen von Zahlungsdienstenutzerinnen zurückzuführen, die sich aus deren Erfahrungen mit digitalen Technologien in anderen Lebensbereichen, insb. Unterhaltungsindustrie und Medien, speisen. Sektorübergreifend ist dabei ein Trend hin zu einer Vielzahl interoperabler Dienste zu verzeichnen. Im Finanzsektor wird diese Entwicklung flankiert durch die gesetzlichen Vorgaben zur Interoperabilität (zur Schnittstellen-Problematik siehe Abschnitt 3.1). So sind kontoführende Zahlungsdienstleisterinnen nach Maßgabe des § 48 ZAG dazu verpflichtet, Zahlungen von den bei ihn geführten Konten unter Einschaltung von Zahlungsauslösediensten zu ermöglichen, und dürfen Kontoinformations- und Zahlungsauslösedienstleisterinnen nur in den Grenzen des § 52 ZAG Zugang zu den bei ihnen geführten Konten verweigern.

Außer der oben beschriebenen, exogen verursachten Komplexität kommt es auch zu einer **endogenen, taktischen Komplexitätssteigerung** . Die Zunahme an Schnittstellen öffnet den Markt für spezialisierte IT-Unternehmen, die die Unübersichtlichkeit der Schnittstellenlandschaft zu ihrem Vorteil nutzen. Sie bündeln die vorhandenen Schnittstellen und bieten diese den kontoführenden Zahlungsdienstleisterinnen als Paket an (vgl. Abbildung 6 Schnittstellen-Topologie).

Wenn die Anzahl der benötigten Schnittstellen seitens der kontoführenden Zahlungsdienstleisterinnen eine gewisse Größe erreicht hat, ist es günstiger, diese über eine solche Anbieterin zu beziehen. Diese spezialisierten Unternehmen haben insofern keinen Anreiz, die komplexe Struktur zu vereinfachen, sondern profitieren davon, gegenteilig zu agieren, die Schnittstellen also nicht minimal, sondern absichtlich kompliziert zu konzipieren. Der bewusste Einsatz dieser Taktik wird sich in der Regel nicht nachweisen lassen, da über lange Zeit in Arbeitsteilung entwickelte und dabei inkrementell verbesserte Softwaresysteme tendenziell sehr komplex werden. Denn vielfach ist es technisch einfacher und kurzfristig rentabler, etwas Neues hinzuzufügen als Bestehendes zu konsolidieren.

Eine hohe Komplexität flankiert wiederum die bereits oben genannten Preisstrategien von IT-Dienstleisterinnen. Mehrere Markteilnehmerinnen ziehen demnach einen Nutzen daraus, die Komplexität zu erhalten bzw. noch weiter zu steigern. Das ist insofern problematisch, als in dieser Hinsicht kaum Anreize zur Reduktion der Komplexität gegeben sind.

3.3 Szenario 3: Reduktion der Bank auf eine Risiko-Hülle

Szenario: Infolge der in Szenario 2 beschriebenen Konzentration der Finanzdienstleistungslandschaft auf einzelne IT-Unternehmen wird eine Reduzierung von Banken auf bloße Risikohüllen eintreten. Konkret wird es dazu kommen bei der Auslagerung an große, internationale IT-Unternehmen, die jeweils von einer Mehrzahl von Banken genutzt werden – im denkbaren Extremfall ein einziges IT-Unternehmen, an das sämtliche Banken auslagern. Dabei verbleiben Banken als relativ machtloser (da austauschbarer) beaufsichtigter Teil einer ansonsten zentral gesteuerten Zahlungs- und Finanzdienstleistungslandschaft.

Die Entwicklung wird dadurch begünstigt, dass die IT-Unternehmen einerseits die Kontrolle über die Kundenschnittstelle innehaben und andererseits über die Schnittstelle zu ihren Auftraggeberinnen Know-how erlangen. Abbildung 10 veranschaulicht das Szenario. Erneut deutet sich an, dass Komplexität strategisch einsetzbar sein könnte, was die Aufsicht vor neue Herausforderungen stellen könnte.

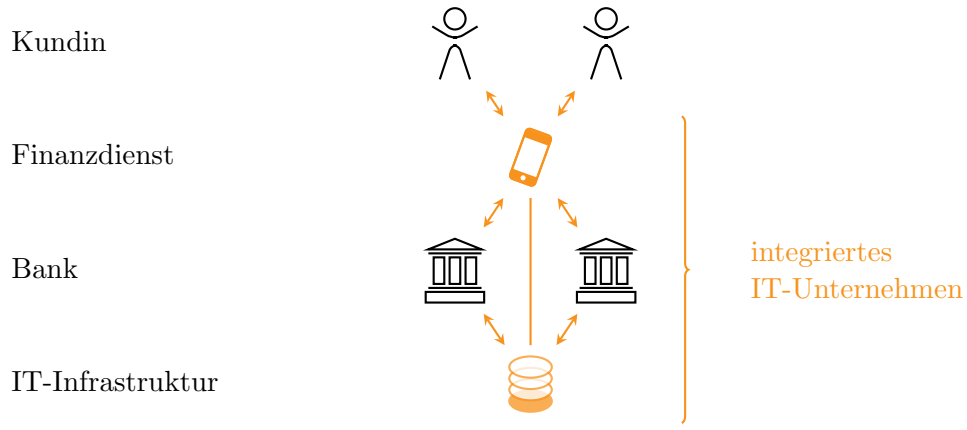

Abbildung 10: Szenario 3 – Entkopplung der Bank von Kundenschnittstelle und IT-Infrastruktur

3.3.1 De-facto Kontrolle der Kundenschnittstelle durch IT-Unternehmen

Die **Schnittstelle Endkundin–Bank** ist in mehrfacher Hinsicht relevant. Sie wird nicht von der Bank, sondern von dem IT-Unternehmen betrieben.[25] Durch entsprechende Gestaltung (z. B. Dialogführung, Anordnung und Farbgebung visueller Elemente) können Kundenentscheidungen in bestimmte Richtungen beeinflusst werden und in einem gewissen Rahmen Geschäftsvorfälle gesteuert sowie auf Marktteilnehmerinnen verteilt werden.[26]

Ein Beispiel, bei dem dies bereits heute sichtbar ist, sind Voreinstellungen von Zahlungsmethoden im Online-Handel. Dies kann mit einer engen Verzahnung der von der Bank erbrachten Finanzdienstleistung mit anderen Leistungen des IT-Unternehmens einhergehen. Beispielsweise können Verbraucherkredite direkt in den Bestellvorgang einer Online-Händlerin integriert werden. Auf diese Weise könnte die Bank in der Wahrnehmung der Verbraucherinnen in den Hintergrund rücken, da die Interaktion lediglich über die Webseite, App oder das Gerät des IT-Unternehmens abläuft.

Zwar könnten Banken in ihrer Stellung als Auftraggeberinnen im Prinzip diese Praktiken unterbinden oder kontrollieren. Dies erfordert aber belastbare vertragliche Regelungen sowie mehrstufige Kommunikationsketten, denn in der Regel wird das IT-Unternehmen seinerseits der Bank keine technische Schnittstelle anbieten, mit der Mitarbeiterinnen der Bank die Kundenschnittstelle frei programmieren können. Würde die Bank dies vertraglich fordern, bliebe ungewiss, ob das IT-Unternehmen angesichts seiner Marktstellung darauf eingehen würde. Eine gesetzliche Verpflichtung zur Bereitstellung von Schnittstellen gibt es für IT-Unternehmen im Gegensatz zu Banken nicht.

[25] Siehe hierzu auch BaFin (2018a, S. 66 ff.) im Folgenden: BDAI-Studie, abrufbar unter `https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html?nn=7846960` (letzter Abruf: 18.07.2022).

[26] Siehe etwa im Kontext von Cookie-Einwilligungen Machuletz und Böhme (2020).

Die einseitige Pflicht zur Bereitstellung von Schnittstellen im Zuge der PSD2 kann dazu führen, dass IT-Unternehmen bestimmte Dienstleistungen von Banken ohne vertragliche Grundlage und ggf. gegen die Interessen der Bank in ihr Angebot einbinden. Dabei können IT-Unternehmen versuchen, Bankkundinnen den Zugang zu weiteren eigenen Leistungen (z. B. Online-Handel, Streaming-Dienst) zu erleichtern.

Konkret könnten IT-Unternehmen zusätzlich zu den gewünschten Waren und Dienstleistungen eine eigene Bezahlungsmethode anbieten.[27] Beispiele für Dienstleistungen im Zahlungsverkehr von IT-Unternehmen bilden etwa Amazon Pay[28] oder Apple Pay.[29] Gegenüber der Kundin tritt das IT-Unternehmen als Zahlungsdienst auf, im Hintergrund steht die Bank als Abwicklerin, die aber diese Dienstleistungen ohnehin weitgehend ausgelagert hat. Erwähnenswert sind in dem Zusammenhang auch die Pläne von *Facebook* zur Schaffung des Blockchain-basierten Online-Bezahlsytems *Diem* (vormals *Libra*).[30] Die Anwendbarkeit dieser Strategie ist nicht auf Dienstleistungen im Zahlungsverkehr beschränkt. Möglich ist auch darüber hinaus die Erbringung weiterer Finanzdienste durch IT-Unternehmen, etwa in den Bereichen Finanzierung und Beratung.

Eine ähnliche Asymmetrie bestimmt den Zugang zu neuen Kundengruppen insb. jungen Kundinnen. Während Banken gesetzlich verpflichtet sind, die Identität ihrer Kundinnen zweifelsfrei festzustellen, sind die Anforderungen an die Eröffnung von Konten bei IT-Unternehmen in der Regel niederschwelliger. Oftmals findet überhaupt keine Zuordnung zu einer natürlichen oder juristischen Person statt. Freilich sind diese Online-Konten nicht für Bankgeschäfte verwendbar; die Identifikation muss beim ersten Bankgeschäft von der Bank nachgeholt werden. Trotzdem ist davon auszugehen, dass mittelfristig Verbraucherinnen stärker an ihre Online-Konten gebunden sind als an Bankkonten. Online-Konten, die in den Social-Media-Angeboten sichtbar erscheinen, unterstützen diese Bindung. Auch dies stärkt die Verhandlungsposition und den Gestaltungsspielraum von IT-Unternehmen gegenüber Banken.

3.3.2 Know-how-Transfer über den Zugang zu Geschäftsdaten durch IT-Unternehmen

Zweitens gibt es die **Schnittstelle Bank–IT-Unternehmen**. Über diese erbringt das IT-Unternehmen Dienstleistungen wie etwa die Verwaltung von Kundendaten, die Steuerung von Geschäftsprozessen oder die Kommunikation mit anderen Marktteilnehmerinnen und der Aufsicht.

Durch Auslagerungen auf ein IT-Unternehmen hat dieses über die genannte Schnittstelle Zugriff auf die Daten und Geschäftslogik der Bank. Weil das IT-Unternehmen seine Dienste für eine Mehrzahl von Banken – im Extremfall alle beaufsichtigten Banken – erbringt, erlangt das IT-Unternehmen Wissen über den Finanzmarkt, das über das einzelner Banken hinausgeht. Selbst wenn es Zusicherungen gibt, dass Daten von Kundinnen auf technischer Ebene vor dem Zugriff durch Mitarbeiterinnen des IT-Unternehmens geschützt sind, sind diese sachlich und bezüglich ihrer Wirksamkeit zu hinterfragen.

So enden diese Zusicherungen immer dann, wenn das IT-Unternehmen gesetzlich verpflichtet ist, Daten herauszugeben. Ähnlich gelagert sind Fälle, in denen das IT-Unternehmen Daten

[27] So auch BaFin, BDAI-Studie, S.68, abrufbar unter `Https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html?nn=7846960` (letzter Abruf: 18.07.2022).
[28] Siehe `https://pay.amazon.de/` (letzter Abruf: 18.07.2022).
[29] Siehe `https://www.apple.com/de/apple-pay/` (letzter Abruf: 18.07.2022).
[30] Siehe `https://www.diem.com/en-us` (letzter Abruf: 18.07.2022).

heranziehen muss, etwa um Cyberangriffen vorzubeugen, laufende Angriffe abzuwehren oder erfolgte Angriffe aufzuklären. Diese Ausnahmen sind oft vertraglich – wenn nicht gesetzlich – geregelt. Im Zusammenhang mit Wartungsarbeiten oder vom IT-Unternehmen angebotenen Kundendienstleistungen (z. B. Assistenz bei der Fehlersuche) ist der technische Zugriff auf Kundendaten in der Regel möglich. Allerdings sind die Mitarbeiterinnen des IT-Unternehmens sowie dessen mit Administrationsaufgaben betrauten Dienstleisterinnen zur Vertraulichkeit verpflichtet. Eine vollständige Abschirmung der Kundendaten ist technisch anspruchsvoll und erfolgt nur, wenn die Voreinstellungen erheblich angepasst werden. Sie erfordert, dass ausgewählte Komponenten der IT-Infrastruktur (z. B. HSMs) bei der Bank und unter deren Kontrolle vorgehalten werden. Dieser Mehraufwand steigert die Kosten der Auslagerung erheblich. IT-Unternehmen gestalten ihre Verträge so, dass die Verantwortung für diese Maßnahmen vollständig den Banken obliegt, was derartige Bestrebungen – sofern sie die Aufsicht nicht fordert – noch unattraktiver macht.

Selbst wenn die Zusicherungen eingehalten werden, bleibt deren Wirksamkeit fraglich. Markttrends lassen sich oft aus Metadaten erschließen und erfordern keinen unerlaubten Einblick in die Geschäftsprozessdaten. Denn das IT-Unternehmen ist nicht an Einzelfällen interessiert (z. B. an Bonitätsauskünften zu bestimmten Personen), sondern es möchte neue Entwicklungen abschätzen und Möglichkeiten zur Effizienzsteigerung frühzeitig erkennen. Indikatoren wie die Unzufriendenheit von Kundinnen erfährt es durch seine Präsenz an der Kundenschnittstelle aus erster Hand und bei Bedarf in Form strukturierter Daten. Beispiele hierfür sind Funktionen zur Bewertung oder das Melden von Problemen. Sind die Wertschöpfungsketten fragmentiert und mehr als eine Marktteilnehmerin an einem Geschäftsprozess beteiligt, dann entstehen Metadaten über Kommunikationsverläufe zwischen Finanzdienstleisterinnen, welche aufschlussreich sein können. Wenn alle Beteiligten an das gleiche IT-Unternehmen auslagern, so erhält dieses ein genaues Bild über die Zusammenhänge. Schließlich ist die Nachfrage nach neuen Funktionen seitens der Kundinnen ein valider Marktindikator, der sich leichter interpretieren lässt als eine Vielzahl von Prozess-Mikrodaten. Angesichts der Tatsache, dass IT-Unternehmen auch Experten und Führungskräfte aus dem Finanzsektor rekrutieren, steht außer Frage, dass sie in der Lage sind, die ihnen zur Verfügung stehenden Informationen auch im Rahmen der gemachten Zusicherungen profitbringend zu nutzen.

3.3.3 Verlust von Gestaltungsmacht und Kontrolle der beaufsichtigten Banken

Die Abhängigkeit von IT-Unternehmen an beiden Schnittstellen (Endkundenschnittstelle und Schnittstelle Bank–IT-Unternehmen) führt zu einer Situation, in der bei der Bank faktisch keine Gestaltungsmacht und Kontrolle über den der Endkundin gegenüber erbrachten Dienst verbleibt. Denn die Verhandlungsmacht liegt bei dem IT-Unternehmen. Dies entspricht den Machtverhältnissen bei der Auftragsverarbeitung im Sinne von Art. 28 der Datenschutzgrundverordnung (DSGVO): Der gesetzlichen Regelung nach handelt es sich bei Auftragsverarbeiterinnen um weisungsabhängige Auftragnehmerinnen der für die Verarbeitung Verantwortlichen. Faktisch als Auftragsverarbeiterinnen eingesetzt werden aber große IT-Unternehmen, die durch ihre AGB die Vertragsbedingungen einseitig diktieren.

Dabei könnte, wenn die Bank **an beiden Schnittstellen** an dasselbe IT-Unternehmen auslagert, dieses sogar ganz ohne Bank auskommen. Aus Sicht des IT-Unternehmens läge hierin die Vollendung einer Divide-and-Conquer-Strategie, welche bedingt durch die im Ausgangspunkt vergleichsweise geringe Konzentration im Bankensektor weitgehend ohne „Divide“ auskommen kann. Den IT-Unternehmen kommt es aber zugute, wenn die Bank als Adressatin regulatorischer

Verpflichtungen als Risikohülle verbleibt. Beim Eintritt dieses Szenarios würde die Perspektive der Aufsicht zunehmend mittelbar. Denn diese würde nicht bei dem die Infrastruktur betreibenden und faktisch Finanzdienste bereitstellenden IT-Unternehmen, sondern bei den von diesem als Risikohüllen genutzten Banken ansetzen.

3.3.4 Komplexitätssteigerung für die Aufsicht

Eine solche Situation kann ebenfalls zu wachsender Komplexität führen. Einerseits sind hochelastische, mehrmandantenfähige verteilte Systeme technisch sehr komplex. Diese Tatsache wird vor den Kundinnen oft versteckt, da sie nur eine Sicht auf das Gesamtsystem erhalten. Erst im Falle von Fehlern und ungewöhnlichen Kaskaden von Ausfällen wird diesen das Geflecht an Abhängigkeiten bewusst.

Andererseits bestehen für das IT-Unternehmen Anreize zur Komplexitätssteigerung. Das IT-Unternehmen profitiert von einer großen Zahl unterschiedlicher, ausdifferenzierter Dienste, deren fixe Entwicklungskosten es durch den weltweit standardisierten Einsatz amortisieren kann. Das IT-Unternehmen kann dabei versuchen, den Banken die von diesen genutzten Funktionalitäten nicht möglichst simpel, sondern durch eine Vielzahl ausdifferenzierter Dienste bereitzustellen, um damit die Entwicklung von (eigenen) Alternativen zu erschweren. Außerdem gewöhnen sich die Kundinnen der Banken an die bereitgestellten Funktionen, sodass ein Wechsel des IT-Unternehmens (oder eine Reduktion des Dienstumfangs) wirtschaftlich riskant wäre. Das IT-Unternehmen festigt also seine Marktposition durch den Lock-In der Kundinnen seiner Kundinnen.

Steigt die Komplexität der Zahlungs- und Finanzdienstleistungslandschaft, erschwert schon dies für sich genommen der Aufsicht die Überprüfung der IT-Sicherheit erheblich, insbesondere wenn eine Gesamtschau auf das IT-Unternehmen mit allen seinen beaufsichtigen Kundinnen verwehrt ist und stattdessen der Informationsfluss stets indirekt über einzelne Beaufsichtigte verläuft. Die Aufsichtsbehörde muss dementsprechend vielfach redundante Informationen erheben und auswerten. Die Erfassung des Gesamtsystems und Kombinatorik sämtlicher Möglichkeiten von Interaktion ist aber für die Beurteilung seiner Sicherheit entscheidend (siehe Abschnitt 3.1.2). Dabei besteht in dem Szenario bereits ein eingeschränkter, weil über die gegenüber dem IT-Unternehmen einflussschwache Bank vermittelter, Einblick in die vom IT-Unternehmen kontrollierte für die Bank bereitgestellte Infrastruktur. Das heißt, bereits die Überprüfung der Sicherheit einzelner Komponenten der gesamten Infrastruktur ist erschwert, obwohl diese an sich selbst bei Sicherheit aller einzelnen Komponenten nicht als sicher betrachtet werden kann. Bei etwaigen Einwänden könnte es passieren, dass die Bank ihre Änderungswünsche nicht umsetzen kann, weil sich das IT-Unternehmen auf die Gangbarkeit der von ihm angebotenen Lösung bei anderen internationalen Kundinnen berufen könnte, oder dass die Umsetzung unverhältnismäßig teuer ist, da das IT-Unternehmen der nachfragenden Bank die kompletten Entwicklungskosten in Rechnung stellt.

Im Extremfall verbliebe nur die Möglichkeit, der Nutzung der Infrastruktur des IT-Unternehmens durch die Banken insgesamt eine Absage zu erteilen. Dies erscheint allerdings insofern wenig praktikabel, als bei einer gewissen Marktmacht des IT-Unternehmens deutsche bzw. europäische Finanzdienstleisterinnen in andere Jurisdiktionen gedrängt und so der hiesigen Aufsicht ganz entzogen würden.

4 Validierung

4.1 Methode

Um zu erwartende Entwicklungen auf Grundlage der Szenarien zu antizipieren, war es notwendig, diese in Gesprächen mit Vertreterinnen unterschiedlicher Marktteilnehmerinnen zu validieren. Hierzu haben die Projektpartnerinnen im Zeitraum von Juli bis November 2020 Banken, Finanzdienstleisterinnen sowie sowohl sektorspezifische als auch allgemeine IT-Unternehmen und Händlerinnen kontaktiert, über Projektziel und Methode informiert und um Interviews gebeten (siehe die deutschsprachige Fassung des Anschreibens in Anhang 1a sowie die englischsprachige Fassung in Anhang 1b). Den potenziellen Interviewpartnerinnen wurde eine Kurzfassung der zu validierenden Szenarien übersandt (siehe die deutschsprachige Kurzfassung in Anhang 2a sowie die englischsprachige Kurzfassung in Anhang 2b). Dabei wurde in der Einleitung der Kurzfassung darauf hingewiesen, dass die Szenarien bewusst überspitzt (in der englischen Fassung „provoking“) angelegt und nicht als Prognosen zu verstehen seien.

Schließlich wurden im Rahmen des Projekts im Zeitraum von August bis Dezember 2020 neun Interviews mit Vertreterinnen von Banken, Finanzdienstleisterinnen und IT-Unternehmen in Form von Videokonferenzen geführt. Im Rahmen der neun Interviews wurden insgesamt 21 Personen interviewt, von denen über die Hälfte im Managements des jeweiligen Unternehmens tätig war. Unter den Gesprächspartnerinnen waren solche mit wirtschaftswissenschaftlichem, kaufmännischem, mathematischem, juristischem und informationstechnischem Hintergrund. Eines der Gespräche wurde in englischer Sprache, die übrigen in deutscher Sprache geführt. Als Grundgerüst für die Gespräche diente ein zuvor von den Projektpartnerinnen erarbeiteter Leitfaden (Anhang 3). Mit Ausnahme eines Interviews wurde den Interviewpartnerinnen der Leitfaden weder vollständig noch teilweise zur Verfügung gestellt. Die Interviews wurden in Gedächtnisprotokollen auf Grundlage schriftlicher Notizen der Projektpartnerinnen dokumentiert (Anhang 4 – nicht öffentlich).

4.2 Ergebnisse der Interviews

Insgesamt haben die Gespräche mit den Marktteilnehmerinnen ergeben, dass diese die erstellten Szenarien als nicht unrealistisch und weitgehend vollständig bewerten. Erwartungsgemäß wurde nicht jeder Einzelaspekt der bewusst überspitzt formulierten Szenarien unterstützt, sodass bei der Formulierung der empfohlenen Konsequenzen für die IT-Aufsicht insbesondere nach Dringlichkeit differenziert wird. Für einzelne Ergebnisse der Interviews wird im Folgenden auf die Abschnitte und Zeilennummern der Dokumentation in Anhang 4 verwiesen. In den Fußnoten werden neben den konkreten Verweisen auch zentrale Aussagen der Marktteilnehmerinnen wiedergegeben. Dabei ist darauf hinzuweisen, dass nicht in jedem Interview Aussagen zu allen Einzelfragen getroffen wurden.

Konkret zeigte sich bei **Szenario 1** eine sehr hohe Spannbreite an Reaktionen auf die Hypothese, mehr Schnittstellen würden zu weniger Sicherheit führen. Die Kommentare reichten von nachdrücklicher Zustimmung („das ist offensichtlich“)[31] bis zur deutlichen Ablehnung.[32] Die Gefährlichkeit von Schnittstellen ablehnende und einschränkende Aussagen wurden mit der Überzeugung begründet, dass reife Sicherheitsmechanismen zum Einsatz kämen.[33] Tenden-

[31] Interviews, 1.2., Z. 1 f., siehe auch 4.2, Z. 35 f., 5.2., Z. 32 f.
[32] Interviews, 3.2., Z. 54 f., 6.2., Z. 13 f., 8.2., Z. 32 f.
[33] Interviews, 6.2, Z. 14 f., 8.2., Z. 33 f., 9.2, Z. 15

ziell stimmten Gesprächspartnerinnen mit technischem Hintergrund – und damit solche mit größerer Expertise in den im Szenario im Fokus stehenden technischen Fragen – eher zu als Gesprächspartnerinnen mit nicht-technischem Hintergrund.

Konsens herrschte darüber, dass die neuen technischen Schnittstellen nicht das schwächste Glied seien und Cyberkriminelle derzeit mit einfacheren Methoden Erfolg hätten.[34] Dies gelte derzeit in absehbarer Zukunft.

Auch sei es eher unrealistisch, dass Cyberkriminelle eine Organisation gründen, um an gültige Zertifikate zu kommen.[35] Dass Zertifikate von lizenzierten Marktteilnehmerinnen in die Hände von Cyberkriminellen fallen und missbraucht werden könnten, sei dagegen plausibel, wenngleich noch keine Vorfälle bekannt seien.[36] Die Marktteilnehmerinnen haben bestätigt, dass – gesetzliche und vertragliche – Haftungsregeln entscheidende Anreize für IT-Sicherheit setzen könnten.[37] Uneinigkeit bestand bezüglich der Frage, ob für die Banken eine Prüfung auffälliger Zahlungen im Rahmen der SEPA-Fristen möglich sei.[38]

Bei **Szenario 2** hat sich ergeben, dass die Frage systemischer Risiken der Cloud-Technologie stark polarisiert. Wir erfuhren zunächst von einer Vielzahl teils noch nicht berücksichtigter Faktoren,[39] die den Druck zur Migration in die Cloud[40] erhöhen würden. Der Trend zur Cloud betrifft aber zunächst Office-Umgebungen und unterstützende Systeme und eher weniger den Kern der Zahlungssysteme.[41] Unsere Hypothesen zu den Preisstrategien der Cloud-Anbieterinnen lösten gemischte Reaktionen aus. Zwei Marktteilnehmerinnen bestätigten, Preisstrategien mit dem Ziel des Lock-ins seien realistisch,[42] wobei eine Marktteilnehmerin ergänzte, die Strategie werde jedenfalls von einer großen Cloud-Anbieterin nicht angewandt.[43] Mit Bezug auf dieselbe Cloud-Anbieterin wies eine andere Marktteilnehmerin darauf hin, der Preis sei kein relevanter Entscheidungsfaktor.[44] Eine Marktteilnehmerin wies eigene Pricing-Strategien mit dem Ziel des Lock-ins zurück.[45] Zur Frage der Verhandlungsposition von Kundinnen gab es unterschiedlich Nuancen.[46] Systemische Risiken durch Infrastrukturanbieterinnen wurden vielfach bejaht,[47]

[34] Interviews, 1.2., Z. 2 ff., 2.2., Z. 61 ff., 3.2., Z. 54 ff., 5.2. Z. 32 ff., 6.2., Z. 15 f., 7.2., Z. 17 ff., 8.2., Z. 37 f.

[35] Interviews, 5.2., Z. 38, 6.2., Z. 29 f., „schwierig“ laut 9.2., Z. 24 f.

[36] Interviews, 5.2., Z. 38 ff., jedoch “schwierig“ laut 4.2., Z. 29 f. und 9.2., Z. 25, „unwahrscheinlich“ laut 6.2., Z. 28 f.

[37] Interviews, 1.2, Z. 60 f. (es bestehe kein Anreiz, auffällige Zahlungen nicht durchzuleiten seitens nicht unmittelbar haftender Zahlungsdienstleisterinnen), 4.2., Z. 57, 5.2., Z. 47, anders nur 7.2., Z. 16 (Haftung sei kein entscheidender Faktor für IT-Sicherheit).

[38] Interviews, 1.2., Z. 58 f. (sei nicht möglich); dagegen 3.2., Z. 76 (Klärung sei in der Regel möglich).

[39] Interviews, 2.2., Z. 127 f. (alle würden Cloud nutzen), 130 f. (Benutzungsfreundlichkeit sei wichtiger als ökonomische Faktoren), 3.2., Z. 84 ff. (Ausfallsicherheit, Qualität, Verfügbarkeit, flexibles Scaling), 4.2., Z. 140 ff. (Compliance-Level der Cloud-Anbieterinnen), 9.2., Z. 41 ff.

[40] Interviews, 1.2., Z. 101, 2.2., Z. 124 ff., 3.2., Z. 82 ff., 4.2., 21 f., 9.2., 41 ff. (schnellere Umsetzung neuer Sicherheitsanforderung durch die Software-Anbieterinnen für die Cloud).

[41] Interviews, 2.2., Z. 124 f., 128 f., 5.2., Z. 115 ff., 9.2., Z. 33 ff., aber Z. 40, geplante Auslagerung des Zahlungsverkehrs gem. 3.2., Z. 86 f., 4.2., Z. 147 ff.

[42] Interviews, 7.2., Z. 33 ff., „valide“ laut 9.2, Z. 54.

[43] Interviews, 9.2., Z. 54.

[44] Interviews, 6.2., Z. 39 f.

[45] Interviews, 5.2., Z. 124 f.

[46] Verhandlungspositionen ggü. existierenden „Oligo-, Duo- und sogar Monopolen“ seien nur durch Zusammenschlüsse von Akteurinnen mit gemeinsamen „Audit-Interessen“ zu stärken laut Interviews, 1.2., Z. 101 ff., Vertragsverhandlungen mit AWS nicht möglich laut 6.2., Z. 39, möglich dagegen laut 7.2., 35 ff., allerdings mit geringerer Verhandlungsmacht; stärkere Verhandlungsposition großer Cloudabieterinnen ggü. dritten Softwareherstellerinnen laut 9.2., Z. 41 ff.

[47] Interviews, 4.2., Z. 16 ff., 7.2., Z. 27 ff., einschränkend 8.2., Z. 59 ff., 9.2., Z. 50 ff., implizit 2.2., Z. 132 ff.

wenngleich zwischen Verfügbarkeits- und Vertraulichkeitsaspekten zu differenzieren ist: Während die redundante Speicherung von Daten deren Verfügbarkeit und Integrität fördert, steht sie mit dem Ziel der Vertraulichkeit in einem Spannungsverhältnis.[48] Die drei Marktteilnehmerinnen, die ein systemisches Risiko durch die breite Nutzung von Cloud-Technologien explizit oder implizit zurückgewiesen haben, haben sich auf die geringere absolute Eintrittswahrscheinlichkeit von Vorfällen im Cloud-Szenario bezogen.[49] Damit nicht zurückgewiesen wurde das systemische Risiko durch die Korrelation (Gleichzeitigkeit des Eintritts) von Vorfällen bei Nutzung einer Anbieterin durch eine Vielzahl von Finanzmarktakteurinnen.[50]

Systemische Risiken können auch auch von kleinen und damit leicht übersehbaren Dienstleisterinnen ausgehen, die in einem sehr engen und damit konzentrierten Markt arbeiten. Dies wurde weitgehend bestätigt,[51] allerdings wirken Marktteilnehmerinnen Konzentrationsrisiken nicht unbedingt entgegen, wenn so ein Problem erkannt ist.[52] Einige, aber nicht alle Marktteilnehmerinnen würden den Aufwand betreiben, eine Multi-Sourcing-Strategie umzusetzen.[53] Einige, nicht aber alle Marktteilnehmerinnen würden über konkrete Exit-Strategien verfügen.[54]

Vielfältige Einsichten konnten an der Schnittstelle zwischen **Szenario 2 und Szenario 3** zu Fragen der Komplexität gewonnen werden. Unterschiedlich äußerten die Marktteilnehmerinnen sich auch zu strategischen Komplexitätssteigerungen (Abschnitt 3.3.4)[55] bzw. systemischen Risiken durch Komplexität.[56] Eine Marktteilnehmein räumte ein, man versuche Kundinnen durch eine Vielzahl von Services von einem Wechsel zu Konkurrentinnen abzuhalten.[57] Zustimmung erhielt dabei die These, dass eine hohe Komplexität die Erfüllung der Aufgaben der IT-Aufsicht erschwere.[58] In einem Interview wurde problematisiert, dass Komplexität vielfach außerhalb des

[48] Siehe zu diesem Einwand die Aussage in Interviews, 8.2., 64 ff., Cloud sei nicht perfekt, mache es aber auch nicht schlimmer.

[49] Interviews, 3.2., Z. 84 ff., 8.2., 60 ff., 9.2., Z. 51 f.

[50] Interviews, 9.2., Z. 52 f. (Verweis auf einen großen Vorfall bei *AWS*).

[51] Vgl. zum App Hardening Interviews, 1.2., Z. 109 ff., 2.2., Z. 90 ff., 5.2., Z. 134 ff., 9.2., 63 ff.

[52] Interviews, 2.2., Z. 90, 5.2., Z. 134 ff., vgl. auch 3.2., Z. 129 f., 136 f., anders nur 1.2., Z. 111 f.

[53] Für Cloud-Anbieterinnen siehe Interviews, 4.2., Z. 17 f., 157 (die meisten Akteurinnen würden auf mehr als eine Anbieterin setzen), dagegen sei die Möglichkeit einer zweiten Cloud-Anbieterin „schwierig, nicht einmal theoretisch interessant laut 1.2., Z. 105 f., implizit verneinend auch 6.2., Z. 37 f., 44 ff. (nicht einmal Möglichkeit eines Wechsels betrachtet); zum App-Hardening 2.2., Z. 90 ff. (Anbieterin sei konkurrenzlos), 5.2., Z. 135 f. (zwei Anbieterinnen heranzuziehen verursache zu großen Aufwand).

[54] Interviews, 1.2., Z. 116 ff. (umgehender Wechsel auf eigene Hardware), 4.2., Z. 18 f. (meiste Anbieterinnen hätten Exit-Strategien). 6.2., Z. 37 f., 44 ff. (kein konkretes Konzept für eine andere Anbieterin), konkrete Exit-Strategien der Kundinnen nicht ersichtlich laut 5.2., Z. 121 ff. und 2.2., Z. 40 ff.; siehe auch 2.2., Z. 90 ff. (Konkurrenzlosigkeit der genutzten App-Hardening-Anbieterin).

[55] Interviews, 3.2., Z. 48 ff. (man verfolge das Ziel, alles „super-einfach“ zu halten, stelle aber zur Bedienung unterschiedlicher Bedürfnisse eine Vielzahl von Einzeldiensten modular bereit), 4.2., Z. 63 ff. (häufig – implizite – Strategien zur Komplexitätsreduktion technisch nicht umgesetzt, insb. wegen der Neigung zu komplexitätssteigernden Technologien auf Management-Ebene), 5.2., Z. 56 ff. (Bemühung um Einfachheit, aber Kompromisse, wenn „schnell eine fancy Schnittstelle hermüsse“) sowie Z. 124 ff. (keine Komplexitätsstrategie zur Kundenbindung, da diese „nicht blöd“ seien und Komplexität auch eigene Kosten von IT-Dienstleisterinnen erhöhe), 6.2., Z. 51 f. (Vielzahl von Services, um Kundinnen von einem Wechsel abzuhalten), 8.2., Z. 20 ff. (keine Komplexitätsstrategie, weil der Adaption abträglich, aber Vielfalt von Diensten zweck Flexibilität, Agilität und Adaptivität).

[56] Interviews, 1.2., Z. 94 f. (aus Sicht der Bank nicht von großem Interesse); 2.2., Z. 109 (f. naturgemäße, grundlegend riskante Komplexität durch Whitelabel-Banken und Aggregatoren), 4.2., Z. 38 ff. (wachsende Komplexität sei Herausforderung für IT-Sicherheit) sowie Z. 75 ff. (Förderung von Abhängigkeit durch Komplexität als Strategie), 9.2., Z. 98 f. (inhärente und steigende Risiken durch Komplexität, unabhängig davon, ob Cloud genutzt werde oder nicht).

[57] Interviews, 6.2., Z. 51 f.

[58] Interviews, 1.2., Z. 98 f., 4.2., Z. 41 f., 43 ff., 163 ff.

Einflussbereichs von Banken erzeugt werde, diese aber die Adressatinnen der IT-Aufsicht seien.[59]

Ob und inwieweit die Komplexität von IT-Landschaften exogen bedingt ist, also die Komplexität der darin abgebildeten Prozesse lediglich reflektiert, oder endogen durch inhärente Eigenschaften der Technologie bzw. taktische und strategische Handlungen von Marktteilnehmerinnen entsteht, ist eine in der wissenschaftlichen Literatur selten gestellte und auch nach den durchgeführten Interviews weitgehend unbeantwortete Frage. Wir sind der Auffassung, dass diese Frage jedoch in Zukunft zentral werden könnte.

Szenario 3 fand im Ergebnis überwiegend Zustimmung,[60] nicht jedoch bezüglich des Wegs dorthin. Insbesondere die Hypothese, Infrastruktur-Anbieterinnen würden aus den Informationen ihrer Kundinnen lernen, wurde zurückgewiesen.[61] Als plausible Begründung wurde insb. vorgebracht, dass es nicht viel zu lernen gäbe.[62] Auch wurde impliziert, dass andere Wege einfacher seien, wie etwa der Einkauf von Know-how über die Rekrutierung von Branchen-Expertinnen[63]. Tenor war, Finanzdienstleistungen seien global sehr ähnlich.[64] Lokale Strukturen und Regulierung verzögere die Konzentration lediglich, aber werden sie nicht aufhalten.[65]

[59] Interviews, 1.2., Z. 98 f.

[60] Interviews, 2.2., Z. 111 ff., 117 ff. (weitere Herrschaftsverschiebung auf Cloud-Anbieterinnen sei erwartbar), 5.2., Z. 165 ff. (von *AWS* gehe große Gefahr aus; es sei attraktiv, den Hauptteil des Marktes „ohne den aufsichtsrechtlichen Stress“ zu kontrollieren), 6.2., Z. 58 f. (für *AWS* möglich, noch wahrscheinlicher agiere *Google* so), 8.2., Z. 73 f. (Realisierung einer solchen Strategie für Tech-Companies schwierig, aber möglich); einschränkend 4.2., Z. 151, insb. 160 f. (mögliche Händlerstrategie, z.B. *Amazon* statt *AWS*), dagegen 1.2., Z. 106 („sei theoretisch möglich, aber praktisch irrelevant“), 3.2., Z. 91 ff. (nicht angestrebt von den Tech-Companies).

[61] Interviews, 8.2., Z. 67 ff., 9.2., Z. 82 ff. Anders etwa: BIS, FSI Briefs No. 12 (March 2021), Big techs in finance: regulatory approaches and policy options, S. 4.

[62] Interviews, 8.2., Z. 67 ff.

[63] Interviews, 8.2., Z. 77 ff.

[64] Interviews, 9.2., Z. 87 f. (die „Use Cases [sind] international“).

[65] Interviews, 9.2., Z. 86 ff.

5 Konsequenzen für die IT-Aufsicht

Aus den in den Interviews gewonnen Erkenntnissen kann die IT-Aufsicht Konsequenzen ableiten. Zu PSD2-Schnittstellen sollten weitere Informationen gewonnen werden (siehe 5.1). Die Möglichkeit der Entstehung systemischer Risiken durch Cloud-Anbieterinnen, aber auch andere in die Wertschöpfungsketten eingeschaltete Unternehmen, machen es zunächst erforderlich, dass die IT-Aufsicht die Wertschöpfungsketten umfassend und zeitnah erfasst (siehe 5.2). Im Hinblick auf eine effiziente Verarbeitung sowohl der IT-Aufsicht bereits zur Verfügung stehender, als auch von ihr noch zu erhebender Daten ist es erforderlich, zu verstehen, welche Daten der IT-Aufsicht nützlich sind (siehe 5.3). Das überspitzte dritte Szenario und die hierzu gewonnenen Erkenntnisse verleiten zur gleichsam visionären Zukunftsidee einer eigenen Cloudlösung der IT-Aufsicht (siehe 5.4). Auch ist eine engere Zusammenarbeit mit anderen Aufsichtsbehörden angezeigt, um Synergien zu nutzen und den Aufwand für die Beaufsichtigten gering zu halten (siehe 5.5).

5.1 PSD2-Schnittstellen – Messungen und Tests

Zwar hat der Markt die Vermutung nicht bestätigt, dass PSD2-Schnittstellen Cyberkiminellen bereits verbreitet als Einfallstor für Angriffe dienen. Lediglich die mit der Umstellung der Authentifizierungverfahren einhergehende Unsicherheit der Kundinnen wurde für Angriffe ausgenutzt. Allerdings dürften bezüglich der Schnittstellen Informationsdefizite herrschen. Auch wenn etwaige Schwachstellen von PSD2-Schnittstellen bislang nicht ausgenutzt worden sein mögen, gibt es Hinweise darauf, dass sie unsicherer sein könnten als die Marktteilnehmerinnen annehmen. Es gibt zahlreiche Fälle von IT-Angriffen, die nicht vorhergesehen oder für wahrscheinlich gehalten worden sind. Ein Beispiel bildet die aktuelle Versionen von Android und iOS betreffende Spähsoftware Pegasus.[66] Ein anderes Beispiel bilden Fehler in TLS-Bibliotheken, die im Vergleich zu Finanzmarktinfrastruktur einfacher aufgebaut und weiter verbreitet sind – allein im Jahr 2021 bekannt wurden etwa ALPACA[67], CVE-2021-3450[68] und Sicherheitslücken bei STARTTLS.[69] Auch wenn die Validierung insofern keinen dringenden Handlungsbedarf ergeben hat, sollte die IT-Aufsicht der möglichen Ausnutzung von PSD2-Schnittstellen durch Cyberkriminelle vorbeugend begegnen. Für die IT-Aufsicht ist im Zusammenhang mit PSD2-Schnittstellen insbesondere relevant, ob diese den gesetzlichen Anforderungen an Funktionalität, Verfügbarkeit und Leistung entsprechen. Diese ergeben sich aus der delegierten Verordnung (EU) 2018/389.[70] Deren Art. 30 regelt die Pflicht kontoführender Zahlungsdienstleisterinnen zur Bereitstellung mindestens einer Schnittstelle mit den in der Vorschrift aufgelisteten Funktionalitäten und enthält weitere Anforderungen. Weiterhin bestimmt Art. 32 Abs. 1 der Verordnung, dass die Schnittstellen denselben Grad an Verfügbarkeit und Leistung, einschließlich Unterstützung aufweisen müssen,

[66] Biermann et. al., Cyberangriff auf die Demokratie (2021), abrufbar unter `https://www.zeit.de/politik/ausland/2021-07/spionage-software-pegasus-cyberwaffe-ueberwachung-menschenrechte-enthuellung` (letzter Abruf: 18.07.2022).

[67] Brinkmann et. al., ALPACA, Application Layer Protocol Confusion – Analyzing and Mitigating Cracks in TLS Authentication (2021), abrufbar unter `https://www.usenix.org/system/files/sec21-brinkmann.pdf` (letzter Abruf: 18.07.2022).

[68] Siehe `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3450` (letzter Abruf: 18.07.2022).

[69] Poddebniak/Ising, Why TLS is better without STARTTLS; A Security Analysis of STARTTLS in the Email Context (2021), abrufbar unter `https://www.usenix.org/conference/usenixsecurity21/presentation/poddebniak` (letzter Abruf: 18.07.2022).

[70] Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation.

der Zahlungsdienstnutzerinnen für den direkten Online-Zugriff auf ihre Zahlungskonten zur Verfügung steht.

Die IT-Aufsicht könnte einer tatsächlichen Ausnutzung von PSD2-Schnittstellen durch Cyberkriminelle zuvorkommen, indem sie Risikoübungen durchführt. Beispielsweise könnte in einem Pilotprojekt versucht werden, auf die Schnittstellen mittels gefälschter sowie mittels echter, aber widerrufener eIDAS-Zertifikate zuzugreifen. Dabei könnten Erkenntnisse zu Sicherheitslücken gewonnen und deren Ausnutzung gezielt vorgebeugt werden. Ein weiterer Ansatz wäre die Organisation von "Bug Bounties" an Testsystemen, die typische Schnittstellen implementieren. Offene Wettbewerbe zur Untersuchung der Sicherheit von Softwaresystemen haben inzwischen einen festen Platz in der Softwareindustrie. Forschungsergebnisse deuten darauf hin, dass solche Aufrufe komplementär zu internen Tests sind und neue Informationen liefern.[71] Voraussetzung ist allerdings eine sichere Organisation mit klaren Regeln, welche ausschließen, dass sich Teilnehmerinnen strafbar machen, wenn sie an Schnittstellen experimentieren. Genau dies ist bei eigenständiger Untersuchung von Schnittstellen durch Dritte derzeit nicht ausgeschlossen und wirkt der erforderlichen Transparenz entgegen (siehe etwa Klaas (2022)). Bereits die Ankündigung von "Bug-Bounties" kann disziplinierend auf die Softwareentwicklung wirken.

5.2 Sektorlandkarte

Im Hinblick auf mögliche systemische Risiken ist für eine wirksame IT-Aufsicht ein Überblick über die Beziehungen und Abhängigkeiten der Beaufsichtigten und weiterer relevanter Akteurinnen erforderlich. Diese ließen sich mit der Struktur eines Graphen (im mathematischen Sinne) erfassen. Abbildung 11 illustriert eine solche beispielhaft und stark vereinfacht.

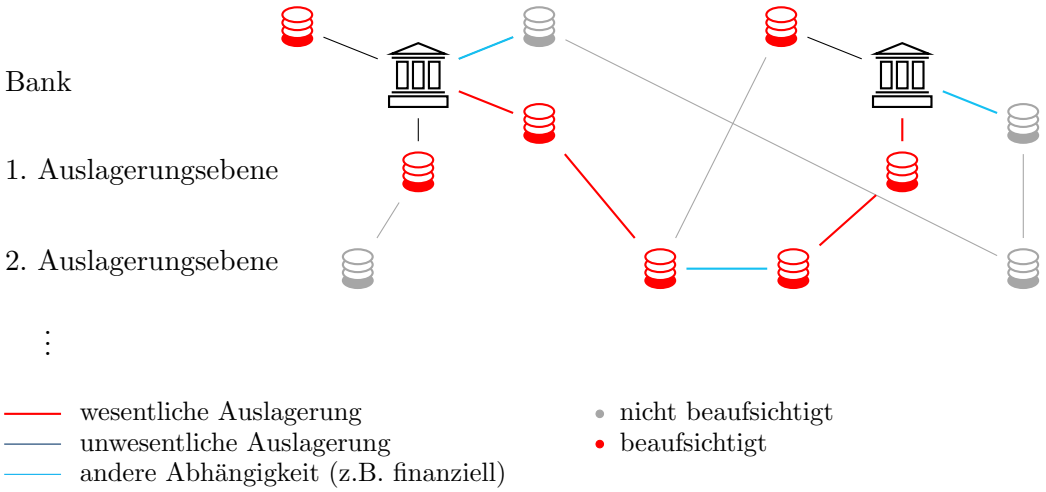

Abbildung 11: Sektorlandkarte

Für die Identifikation von Konzentrationsrisiken ist die Erfassung bestehender Beziehungen und Abhängigkeiten im Sinne einer „Sektorlandkarte" erforderlich. Hierfür benötigt die IT-Aufsicht eine Vielzahl relevanter Daten. Ein seitens der IT-Aufsicht geführtes Register, in dem von den Beaufsichtigten angezeigte Auslagerungen erfasst werden, genügt zur Durchdringung

[71] Siehe Sridhar und Ng (2021) sowie Sivagnanam et al. (2021).

der relevanten bestehenden Beziehungen und Abhängigkeiten nicht, wie im Folgenden näher ausgeführt wird.

§ 24 KWG alter Fassung hatte nicht vorgesehen, dass Institute Auslagerungen anzuzeigen haben. Mit dem Gesetz zur Stärkung der Finanzmarktintegrität (im Folgenden: FISG)[72] wurde die Vorschrift allerdings um die Pflicht zur Anzeige bestimmter Auslagerungen erweitert. § 24 Abs. 1 Nr. 19 KWG-neu sieht vor, dass die Institute „die Absicht einer wesentlichen Auslagerung und deren Vollzug sowie wesentliche Änderungen und schwerwiegende Vorfälle im Rahmen von bestehenden wesentlichen Auslagerungen, die einen wesentlichen Einfluss auf die Geschäftstätigkeit des Instituts haben können," unverzüglich anzuzeigen haben. § 28 Abs. 1 Nr. 10 ZAG alter Fassung, der eine Anzeigepflicht für Auslagerungen und den Vollzug von Auslagerungen bereits vorgesehen hatte, wurde erweitert um eine Anzeigepflicht für „wesentliche Änderungen und schwerwiegende Vorfälle im Rahmen von bestehenden wesentlichen Auslagerungen, die einen wesentlichen Einfluss auf die Geschäftstätigkeit des Instituts haben können", § 28 Abs. 1 Nr. 10 ZAG-neu.

Als Auslagerungsunternehmen sind solche Unternehmen zu verstehen, „auf die ein Institut oder ein übergeordnetes Unternehmen Aktivitäten und Prozesse zur Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen ausgelagert hat, sowie deren Subunternehmen bei Weiterverlagerung von Aktivitäten und Prozessen, die für die Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen wesentlich sind", § 1 Abs. 10 KWG-neu. Eine entsprechende Regelung enthält § 1 Abs. 10a ZAG-neu, wobei übergeordnete Unternehmen nicht von der Regelung erfasst sind. Die Definition entspricht dem Auslagerungsbegriff nach AT9, Rn. 1 Satz 1 MaRisk.[73]

Einerseits erfasst die durch das FISG erweiterte Anzeigepflicht nicht alle Auslagerungen. So sind erstens von § 24 Abs. 1 Nr. 19 KWG-neu nur wesentliche Auslagerungen erfasst. Während die Beaufsichtigten zur Führung interner Auslagerungsregister verpflichtet werden sollen, die sämtliche wesentlichen und nicht wesentlichen Auslagerungen umfassen, § 25b Abs. 1 Satz 4 KWG-neu, ist eine Anzeigepflicht nur für wesentliche Auslagerungen vorgesehen. Der Begriff der wesentlichen Auslagerung ist bereits nach geltendem Recht in § 25b Abs. 1 Satz 1 KWG definiert als „eine Auslagerung von Aktivitäten und Prozessen auf ein anderes Unternehmen, die für die Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen wesentlich sind." Nach MaRisk müssen die Institute auf der Grundlage einer Risikoanalyse eigenverantwortlich festlegen, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen).[74] Die Unterscheidung zwischen wesentlichen und nicht wesentlichen Auslagerungen erscheint insofern problematisch, als sie die Gefahr einer zu isolierten Betrachtung von Einzelkomponenten birgt. Denn entscheidend für einen Prozess ist das Zusammenspiel aller Einzelkomponenten, sodass auch der Ausfall einzelner, für sich genommen unwesentlicher Komponenten sich auf den Prozess als solchen auswirken kann, beispielsweise die Ableitung der BIC aus der IBAN bei einem Überweisungsvorgang. Ideal wäre, wenn bezüglich der Meldepflicht nicht zwischen wesentlicher und unwesentlicher Auslagerung unterschieden würde. Unter dem bestehenden Rechtsrahmen, der diese Unterscheidung trifft, liegt eine mögliche Lösung in einer Konkretisierung des Wesentlichkeitsbegriffs durch die IT-Aufsicht auf Grundlage einer sehr weiten Interpretation von Wesentlichkeit. Es sollte grundsätzlich von der

[72] Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG) vom 03.06.2021, abrufbar unter `https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_Finanzmarktintegritaet.pdf?__blob=publicationFile&v=2` (letzter Abruf: 18.07.2022).

[73] Rundschreiben 09/2017 (BA) zu den Mindestanforderungen an das Risikomanagement.

[74] MaRisk AT9, Rn. 2.

Wesentlichkeit aller Auslagerungen ausgegangen werden und eine Auslagerung nur ausnahmsweise bei Nachweisbarkeit ihrer Unwesentlichkeit von der Erfassung ausgenommen werden. Jedenfalls sollten in eine Sektorlandkarte nicht nur wesentliche, sondern alle Auslagerungen aufgenommen werden, die Kommunikation zwischen technischen Systemen implizieren (siehe Abbildung 11).

Zweitens gelten die Regelungen nicht rückwirkend. Zwar sollen die von den Beaufsichtigten geführten Auslagerungsregister alle bestehen Auslagerungen erfassen. Die geplante Anzeigepflicht betrifft aber nur die Absicht und den Vollzug wesentlicher Auslagerungen sowie wesentliche Änderungen und schwerwiegende Vorfälle. Die IT-Aufsicht sollte bei den Beaufsichtigten ergänzend Informationen über bereits bestehende Auslagerungen abfragen und diese in die Sektorlandkarte aufnehmen.

Drittens werden Auslagerungen der Auslagerungsunternehmen an Dritte nur eingschränkt erfasst. Denn nach § 1 Abs. 10 KWG-neu sind nur solche Subunternehmen vom Auslagerungsbegriff erfasst, bei denen es sich um Subunternehmen von Auslagerungsunternehmen handelt, auf die „Aktivitäten und Prozessen, die für die Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen wesentlich sind“ weiterverlagert sind, § 1 Abs. 10 KWG-neu. Wie Abbildung 11 verdeutlicht, muss sich die Erfassung von Auslagerungen nicht auf zwei Ebenen beschränken.

Andererseits lässt ein reines Auslagerungsregister einige Arten von Akteurinnen ganz außer Acht. Dem Auslagerungsbegriff unterfallen beispielsweise nicht App-Hardening-Unternehmen. Diese bieten Software bzw. Dienstleistungen für den Softwareentwicklungsprozess im Bereich mobiler Apps an. Dabei werden Softwaremodule der App-Hardening-Unternehmen in den Programmcode eines Softwareprodukts (z. B. Banking-App für Endkundinnen) eingebracht bzw. der Programmcode der Kundinnen für diese umgeschrieben. Die in den Interviews gewonnene Erkenntnis, dass auch weniger offensichtlich in die Wertschöpfungskette eingebundene Akteurinnen wie beispielsweise App-Hardening-Unternehmen Risiken mit sich bringen können, legt es für die IT-Aufsicht nahe, sich auf die Identifikation von neuen und unbekannten Risiken dieser Art zu konzentrieren. Notwendig erscheint die umfassende Erfassung nicht nur sämtlicher Auslagerungen, sondern aller relevanten Beziehungen bzw. Abhängigkeiten. Dabei sollte im Hinblick auf die Ermittlung von Konzentrationsrisiken die Art der Abhängigkeit erfasst werden (z.B. technisch, finanziell) und sollte die Erfassung nicht auf vertragliche Abhängigkeiten begrenzt sein. Außerdem sollten Abhängigkeiten nicht nur der Beaufsichtigten zu Dritten (z.B. Auslagerungsunternehmen), sondern auch der Dritten untereinander erfasst werden (siehe Abbildung 11). Dabei stellt sich die Frage, inwieweit derartige Informationen von der IT-Aufsicht zu erlangen sind. Diese kann jedenfalls bei den Beaufsichtigten vorliegende Informationen anfordern. Im Rahmen von Auslagerungsverhältnissen ist aufgrund der Regelungen über die Auftragsdatenverarbeitung davon auszugehen, dass Beaufsichtigte über Unterauftragsverarbeiterinnen informiert ist oder entsprechende Informationen von ihren Auftragsverarbeiterinnen erlangen können (Art. 28 Abs. 3 lit. h, Abs. 4 DSGVO). Optimal wäre es, wenn sich die Informationsgewinnung insoweit nicht auf eine Auflistung von Vertragsverhältnissen oder Sammlung von Vertragswerken beschränken würde, sondern die IT-Aufsicht überprüfen könnte, was auf der Grundlage von Verträgen (statischen Abhängigkeiten) tatsächlich (dynamisch) passiert. Denn auf der Grundlage von Verträgen lassen sich tatsächliche Abweichungen vom vertraglich Vereinbarten nicht feststellen. So können zum Beispiel nicht im Vertrag genannte Dienstleisterinnen der vom Beaufsichtigten eingeschalteten Dienstleisterinnen in Prozesse eingebunden werden. Die IT-Aufsicht sollte Informationsflussdiagramme erstellen, in denen die in Prozessen verwendete Komponenten und eingeschaltete Dienstleisterinnen dargestellt werden. Dabei wären nicht nur

übliche Fälle, sondern auch Ausnahmefälle wie Fallback-Strategien für den Fall, dass einzelne Anbieterinnen ausfallen oder Komponenten versagen, zu berücksichtigen. Die Grundlage für solche Informationsflussdiagramme können von den Beaufsichtigten zu führende manipulationssichere Log-Dateien oder von der IT-Aufsicht an den Schnittstellen zwischen Beaufsichtigten und ihren Dienstleisterinnen selbst erhobene Daten sein. Hierzu könnten allerdings weitreichendere gesetzliche Befugnisse der IT-Aufsicht (gegenüber IT-Unternehmen) und eine engere Zusammenarbeit mit anderen Aufsichtsbehörden wie etwa den Datenschutzbehörden erforderlich sein (siehe hierzu Abschnitt 5.5).

Berücksichtigung finden sollte auch, als wie zuverlässig die der IT-Aufsicht zur Verfügung stehenden, in die Sektorlandkarte eingehenden Informationen zu bewerten sind. Hierzu sollten Beziehungen mit einem Konfidenzmaß annotiert werden. Die Bildung eines solchen Konfidenzmaßes erfordert die Erfassung der Informationsquelle(n) (z.B. Anzeige durch einen oder mehrere Beaufsichtigte(n), Presse, Ergebnis technischer Analyse).

Die Ermittlung von Konzentrationsrisiken profitiert erheblich von einer Prozessbetrachtung, d.h. einer Erfassung von Prozessen und der Annotation der in der Sektorlandkarte dargestellten Beziehungen mit den von ihnen betroffenen Prozessen. Hierdurch würde die Sektorlandkarte mit einem zusätzlichen Attribut versehen und verfeinert. Sollte eine Beschränkung auf wesentliche Prozesse erfolgen, ist – wie auch bei Auslagerungen – grundsätzlich von der Wesentlichkeit aller Prozesse ausgegangen und ein Prozess nur ausnahmsweise bei Nachweisbarkeit seiner Unwesentlichkeit von der Erfassung ausgenommen werden. Die Erfassung der von den Beaufsichtigten angewandten Prozesse ist effizient zu gestalten. Um die Effizienz und Automatisierbarkeit der Risikoermittlung zu gewährleisten, ist eine gewisse Vereinheitlichung von Prozessdefinitionen notwendig. Hierzu sollte die IT-Aufsicht einen Katalog möglicher Prozesse und eine entsprechende Terminologie vorgeben. Die Bestimmung der von den Beaufsichtigten tatsächlich angewandten Prozesse sollte dann den Beaufsichtigten selbst überlassen werden und die digitale Eingabe in einem vordefinierten Format obligatorisch sein.

Um Konzentrationsrisiken zu ermitteln und ihnen entgegenzutreten, sind auch konkrete Exit-Strategien (bezogen auf einen konkreten Anbieterwechsel oder den Wechsel von einer Anbieterin auf eigene Infrastruktur) der Beaufsichtigten relevant (siehe hierzu auch MaRisk AT9 Nr. 6). Hier sollte die IT-Aufsicht erstens fordern, dass solche Strategien existieren, um Lock-in-Risiken zu begegnen. Zweitens sollten Exit-Strategien, die den Wechsel zu einer anderen Anbieterin vorsehen, bei der Risikobewertung im Hinblick auf eine Konzentration bei der Verlagerung berücksichtigt werden.

Für eine vollständige Sektorlandkarte ist hinsichtlich der PSD2-Schnittstellen deren tatsächliche Nutzung zu erfassen. Die Erfassung der tatsächlichen Nutzung von PSD2-Schnittstellen ist mit relativ geringem Aufwand für die IT-Aufsicht zu bewerkstelligen. Während die IT-Aufsicht mittels Testzugängen das Vorhandensein von Schnittstellen, deren Funktionalität, Verfügbarkeit und Leistung selbst messen kann (siehe dazu Abschnitt 5.1), ist sie für die Erfassung der tatsächlichen Nutzung der Schnittstellen auf die Beaufsichtigten oder deren Dienstleisterinnen angewiesen, die Protokolldaten über die Nutzung der Schnittstellen einschließlich der von den PSD2-Dienstleisterinnen genutzte Zertifikate führen. Die IT-Aufsicht sollte diese Daten erheben und auf diese Weise die dynamischen Abhängigkeiten in der Sektorlandkarte erfassen. Dadurch gewänne die IT-Aufsicht Einblicke in die Intensität der Beaufsichtigten untereinander.

Zweifellos bedeutet die Erstellung einer Sektorlandkarte einen hohen Aufwand. Diesen zu rechtfertigen ist mit der Schwierigkeit behaftet, dass sich ihr Mehrwert erst dann ergibt, wenn Schnitt-

mengen der erfassten Abhängigkeiten zu sehen sind, d.h. eine große Zahl von Abhängigkeiten erfasst ist. Insofern ist eine zügige Erhebung, die sich nicht nur auf Meldungen zu Änderungen am Status Quo stützt, zu bevorzugen. Steht der IT-Aufsicht eine umfassende Sektorlandkarte zur Verfügung, bietet diese einen Überblick über Abhängigkeiten und Konzentration. Die IT-Aufsicht kann auf dieser Grundlage mögliche Szenarien simulieren und Risiken einschätzen. Auf Grundlage ihrer Risikoeinschätzung kann die Aufsicht dann bestimmte Beaufsichtigte und Prozesse priorisieren und bei einem als hoch erkannten Risiko engmaschig beaufsichtigen. Wo die IT-Aufsicht zu dem Ergebnis gelangt, dass eine Konzentration unter Risikogesichtspunkten nicht tragbar ist, kann sie auf eine Entflechtung hinwirken.

5.3 Verbesserung der Verfügbarkeit relevanter Daten

Die Datenerhebung ist effizient zu gestalten und überdies an Nützlichkeitskriterien zu orientieren.

Bei der **Erhebung von Daten bei den Beaufsichtigten**, etwa der in einer Sektorlandkarte zu erfassenden Daten (siehe Abschnitt 5.2) sind diese angemessen in den Datenerhebungsvorgang einzubeziehen. Den Beaufsichtigten die Zuordnung von Prozessen und Abhängigkeiten auf Grundlage vordefinierter Kategorien und in vordefinierten Formaten zu überlassen, erspart der IT-Aufsicht – gegebenenfalls nicht zu bewältigende – Arbeit. Insbesondere schützt diese Vorgehensweise die IT-Aufsicht davor, Komplexität bewältigen zu müssen, die sie selbst nicht reduzieren kann. Ein Grundsatz sollte sein, dass diejenigen, welche von hoher Komplexität profitieren, der IT-Aufsicht gegenüber Transparenz herstellen. Die IT-Aufsicht sollte bei der Entwicklung ihrer Maßnahmen anstreben, dass sich eine Erhöhung der Komplexität für Marktteilnehmerinnen nicht „lohnt“, bspw. indem sie den Aufwand für die Beaufsichtigten im Vergleich zu dem für die IT-Aufsicht überproportional steigert. Dem liegt die Überlegung zugrunde, dass ein großer Hebel zum Erfolg effektiver IT-Aufsicht in der Gestaltung effizient zu beaufsichtigender Systeme liegt. Wenn zum Beispiel eine Beaufsichtigte eine Vielzahl von Diensten oder Varianten von Diensten anbietet, etwa um Kundinnen zu binden, und die IT-Aufsicht dementsprechend eine größere Menge an Daten bei der Beaufsichtigten erhebt, sollte die Erhebung den Aufwand der Beaufsichtigten, nicht aber den Aufwand der IT-Aufsicht steigern. Gegebenenfalls entsteht für die Institute dadurch ein zusätzlicher Anreiz, Komplexität zu reduzieren. Ändern sich Beziehungen und ist eine Differenzmeldung notwendig, ist den Beaufsichtigten auch die Verantwortung für die Zusammenführung der gemeldeten Daten zu übertragen. Das ist beispielsweise möglich, indem nach der Eingabe der Differenzmeldung die aktualisierten Beziehungen oder Prozesse der Beaufsichtigten zur Überprüfung angezeigt und von dieser durch eine elektronische Signatur bestätigt werden, bevor die Aktualisierung der Datenbank erfolgt.

Die Richtigkeit der Daten ist abzusichern. Dies ist insbesondere bei in eine Sektorlandkarte (siehe Abschnitt 5.2) eingehenden Daten wichtig. Bei von den Beaufsichtigten gemeldeten Daten ist deshalb eine Eingangskontrolle bzw. echte Plausibilitätsprüfung durchzuführen. Beschränkt sich die Prüfung auf die Bildung von Prüfsummen von Identifikatoren, fällt dabei nicht auf, wenn diese veraltet sind, etwa weil es zum Verlust gekommen und dem Berechtigten ein neuer Identifikator zugeordnet worden ist.

Die Erhebung von Daten aus **anderen Datenquellen** ist auf solche Daten zu begrenzen, die der IT-Aufsicht tatsächlich nutzen. Auch nicht bei den Beaufsichtigten erhobene, sondern aus öffentlichen Quellen stammende Daten können einen Mehrwert für die IT-Aufsicht bilden. Dabei verspricht nicht jede öffentliche Quelle einen Mehrwert für die IT-Aufsicht. So würden etwa bei der breiten, nicht auf spezifische Accounts begrenzten Erhebung von Daten aus den sozialen

Medien (beim „Social Media Scraping“) anlasslos große Mengen nicht relevanter Daten erhoben, die aufwändig automatisiert zu filtern wären. Die hiermit verbundene massenhaften Verarbeitung personenbezogener Daten ist datenschutzrechtlich fragwürdig und zöge mindestens einen erhöhten Aufwand zur Einhaltung der datenschutzrechtlichen Vorgaben nach sich. Bereits das Vorliegen einer datenschutzrechtlich notwendigen Rechtsgrundlage ist zweifelhaft (vgl. Art. 5 Abs. 1 lit. a DSGVO). Außerdem ist die Erhebung und Verarbeitung personenbezogener Daten nur zulässig, soweit die Daten dem Verarbeitungszweck angemessen und erheblich sowie ihre Verarbeitung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist (vgl. Art. 5 Abs. 1 lit. c DSGVO). Insoweit findet eine Verhältnismäßigkeitsprüfung statt. Eine derartige automatisierte Erhebung erscheint deshalb nicht ratsam. Aber auch abgesehen von den genannten Bedenken wären bei einer Erhebung von Daten aus den sozialen Medien Potenziale für eine mögliche Beeinflussung der IT-Aufsicht zu bedenken. Es ist bekannt, dass Kommunikationskanäle von Unternehmen zu Marktteilnehmerinnen strategisch genutzt werden (Lansford, 2006). Das betrifft auch die Informationspolitik von Unternehmen im Bereich von IT-Sicherheitsvorfällen (Gay, 2017). Diejenigen Daten in den sozialen Medien, die als für die IT-Aufsicht relevant zu bewerten sind, finden sich vielfach auch in der Presse, gegebenenfalls mit einer gewissen Verzögerung. Aus den genannten Gründen verspricht die Erhebung in der Presse veröffentlichter Informationen zu Beaufsichtigten und mit diesen verbundenen Akteurinnen gegenüber der Erhebung von Daten aus den sozialen Medien einen größeren Mehrwert.

Im Bereich von Kryptoverwahrung ist es gut möglich, öffentliche Ledger-Daten wie bspw. Blockchain-Daten zu erheben und automatisiert zu verarbeiten. So kann die IT-Aufsicht etwa in Echtzeit Hinweise auf Angriffe erhalten, z.B. solche, bei denen beaufsichtigten Kryptoverwahrerinnen verwahrte Werteinheiten entzogen werden. Notwendig erscheinen spezifische „Responsible Disclosure“-Verfahren und eine internationale Kooperation von Finanzaufsichtsbehörden; nachzudenken ist außerdem über die Ausnutzung der Sicherheitslücke und Sicherstellung von durch die Sicherheitslücke gefährdeter Kryptobestände auf staatlichen Wallets (Böhme et al., 2020, S. 69 f.). Weil es sich um begrenzte Datenmengen mit einem hohen Formalisierungsgrad handelt, verspricht deren automatisierte Verarbeitung mehr Erfolg als die vieler anderer öffentlich zugänglicher Daten, wie z.B. Social-Media-Daten. Jedoch ist der Wartungs- und Interpretationsaufwand nicht zu unterschätzen. Zu dessen Bewältigung dürfte es eines kleinen Teams bedürfen, das idealerweise rund um die Uhr tätig ist. Um den Aufwand für die BaFin zu begrenzen, ist zu überprüfen, inwieweit eine Kooperation mit anderen Behörden in Betracht käme, bspw. mit dem BSI oder der Finanzverwaltung.

Der Nutzen einiger Daten, auch solcher, die der IT-Aufsicht bereits vorliegen, ist noch näher zu ermitteln. So ist der Mehrwert automatisierter Textanalysen von Vertragsdokumenten (z.B. Auslagerungsvereinbarungen) noch nicht einzuschätzen. Es erscheint aber wegen typischer Vertragselemente (z.B. Regelungen zur Laufzeit, Verfügbarkeit und Kündigung) denkbar, dass die IT-Aufsicht sich die automatisierte Analyse von Vertragsdokumenten zunutze machen kann, etwa was die Anforderungen von MaRisk AT9 zu Auslagerungen anbetrifft. Allerdings stellen sich hier zwei Probleme: Erstens stellt die bloße Analyse von Vertragswerken nicht sicher, dass die Wirklichkeit den regulatorischen Vorgaben entspricht. Zweitens ist bei der automatisierten Analyse von Verträgen zu beachten, dass jedes automatisierte (Text-)Analyseverfahren Fehlerquoten aufweist, also falsche Negative und falsche Positive produziert. Im Hinblick darauf ist der Einsatz entsprechender Analyseverfahren kritisch unter Effizienzgesichtspunkten zu hinterfragen. In einem Projekt könnte der Mehrwert automatisierter Vertragstextanalysen untersucht werden.

Mit neuen Datenquellen und zunehmenden Datenmengen wächst die Verantwortung, diese

zeitnah zu verarbeiten und Schlüsse aus den Daten abzuleiten. Andernfalls droht eine Anhäufung unüberschaubarer Datenmengen, die wenig Nutzen versprechen. Zur Vereinfachung der Datenverarbeitung ist die Anzahl unterschiedlicher Datenformate so weit wie möglich einzuschränken. Dabei sollten grundsätzlich offene Formate (im Gegensatz zu proprietären Formaten wie docx) eingesetzt werden, um zu gewährleisten, dass sowohl die IT-Aufsicht als auch die Beaufsichtigten die Formate dauerhaft handhaben können.

5.4 „BaFin-Cloud"?

Das stark überspitzte dritte Szenario verleitet zu der gleichermaßen ambitionierten Überlegung, dass die IT-Aufsicht bzw. die IT-Aufsicht in Kooperation mit anderen nationalen oder europäischen Behörden selbst als Cloud-Anbieterin auftreten könnte. Damit könnte sie Skaleneffekte im Wirtschaftsraum erzielen und wäre in der operativen IT-Aufsicht nicht auf die Kooperation mit nicht direkt beaufsichtigten IT-Unternehmen angewiesen. Diese Vorteile wären aber gegen die Nachteile eines möglicherweise reduzierten Innovationstempos bei öffentlicher Bereitstellung gegenüber einer privatwirtschaftlichen Organisationsform abzuwägen. Das notwendige Kapital, technische Know-how und hochqualifizierte Personal für eine eigene Cloud-Lösung lassen diesen Weg jedenfalls kurz- und mittelfristig kaum gangbar erscheinen. Insbesondere hinsichtlich der Gehälter von Personal mit großer technischer Expertise dürfte kaum eine fortdauernde Wettbewerbsfähigkeit im Verhältnis zu großen Cloud-Unternehmen gegeben sein. Auch könnten im Falle einer von der BaFin selbst betriebenen Cloud Interessenkonflikte eine wirksame IT-Aufsicht beeinträchtigen.

5.5 Ausblick: Engere Zusammenarbeit mit der Datenschutzaufsicht und der Wettbewerbsaufsicht

Bei der Betrachtung der Geschäftsmodelle der Interviewpartnerinnen hat sich zudem abgezeichnet, dass eine engere Zusammenarbeit der IT-Aufsicht mit anderen Aufsichtsbehörden angezeigt ist. Wünschenswert wäre eine Kooperation im Sinne einer Verzahnung, also mit täglicher Kommunikation und (insbesondere zeitlicher) Synchronisierung der Aufsichtsaufgaben. Eine Kooperation ist insbesondere mit Aufsichtsbehörden zweier anderer Bereiche, nämlich einerseits den Datenschutz-, andererseits den Wettbewerbsbehörden notwendig.[75]

Bei den von den Beaufsichtigten erhobenen Daten, insb. denen zu Prozessen und Auslagerungen, bestehen Synergien mit den **Datenschutzbehörden**. Denn personenbezogene Daten eröffnen Finanzmarktakteurinnen Geschäftsmodelle, bei denen die sekundäre Nutzung der im Transaktionsvorgang erhobenen Daten Transaktionskosten substituiert oder personenbezogene Daten die effizientere Ermittlung der Kreditwürdigkeit von Endkundinnen erlauben.[76] Kopien dieser Daten liegen gegebenenfalls bei jeder an der Wertschöpfungskette beteiligten Akteurin und deren Auslagerungsunternehmen. Datengetriebene Geschäftsmodelle im Finanzbereich werden begünstigt, wenn eine Beaufsichtigung betreffender Unternehmen oder deren Finanzaktivitäten allein durch die Finanzmarktaufsicht bzw. die IT-Aufsicht erfolgt. Denn diese stellt sicher, dass sichere Kundenauthentifizierung und hohe Sicherheitsstandards eingesetzt werden. Das schützt auch bei ausdifferenzierten Wertschöpfungsketten vor Betrug und Geldwäsche, nicht aber vor dem Missbrauch personenbezogener Daten, sodass die Beaufsichtigung durch die IT-Aufsicht eine

[75] BIS, FSI Briefs No. 12 (March 2021), Big techs in finance: regulatory approaches and policy options, S. 8, 11 f.
[76] Zu Bigtech-Unternehmen BIS Working Papers, No 779, S. 9; BIS, FSI Briefs No. 12 (March 2021), Big techs in finance: regulatory approaches and policy options, S. 2.

Datenschutzaufsicht über IT-Sicherheitsmaßnahmen etwa im Sinne von Art. 58 Abs. 1, Art. 32 DSGVO im Speziellen sowie über die Einhaltung der datenschutzrechtlichen Vorschriften im Allgemeinen (vgl. Art. 57 Abs. 1 lit. a DSGVO) nicht ersetzen kann. Kommt es zu Datendiebstählen, dürfte in der öffentlichen Wahrnehmung die Verantwortung auch bei der Finanzaufsicht gesucht werden, obwohl ihr die Aufsicht über die Einhaltung personenbezogener Daten nicht obliegt. Insoweit treffen die IT-Aufsicht Reputationsrisiken.

Die Zuständigkeit der Landesdatenschutzbehörden für die Datenschutzaufsicht über Privatunternehmen macht die engere Zusammenarbeit zwischen IT-Aufsicht und Datenschutzbehörden zu einer besonderen Herausforderung. Die IT-Aufsicht müsste mit 16 Landesdatenschutzbehörden zusammenarbeiten, die gegebenenfalls unterschiedliche Auffassungen zu Einzelfragen vertreten. Jedenfalls müssen bei einer Kooperation die Zuständigkeiten der Aufsichtsbehörden und ihre Unabhängigkeit gewahrt bleiben.

Dabei können Datenschutzverstöße unmittelbar relevant für die Aufsicht der BaFin sein. Mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) besteht seit 2013 eine Sprachregelung für Datenschutzverstöße wie insbesondere die übermäßige Erhebung personenbezogener Daten oder ihre Verarbeitung ohne hinreichende Rechtsgrundlage. Nach dieser „berücksichtigt [die BaFin] systematische oder über den Einzelfall hinausgehende bedeutende Datenschutzverstöße im Rahmen ihrer aufsichtlichen Tätigkeit, sofern sie auf eine nicht ordnungsgemäße Geschäftsorganisation hindeuten“. Im Übrigen verweist die BaFin in ihrer Arbeitspraxis Beschwerdeführerinnen und Unternehmen auf die Datenschutzbehörden, wenn und soweit ihr datenschutzrechtlicher Klärungsbedarf bekannt wird.

Auch mit der **Wettbewerbsaufsicht** dürften Synergien bestehen, die die Intensivierung der Kooperation nahelegen.[77] Diese Synergien betreffen zwar nicht die unmittelbar Beaufsichtigten, aber die Konzentration deren IT-Infrastruktur bei großen IT-Unternehmen. Die zunehmende Konzentration von IT-Infrastruktur und Marktmacht großer IT-Unternehmen geht einerseits mit systemischen Risiken für Finanzstabilität einher. Andererseits sind mangelnder Wettbewerb und sogar der Missbrauch von marktbeherrschenden Stellungen zu befürchten.[78] Insbesondere könnten Bigtech-Unternehmen anderen Unternehmen den Markteintritt erschweren.[79]

[77] BIS, FSI Briefs No. 12 (March 2021), Big techs in finance: regulatory approaches and policy options, S. 8, 11 f.
[78] Carsten, Big tech in finance and new challenges for public policy, S. 9
[79] Carsten, Big tech in finance and new challenges for public policy, S. 9; BIS, FSI Briefs No. 12 (March 2021), Big techs in finance: regulatory approaches and policy options, S. 9.

Literatur

Ross Anderson. *Security Engineering*. Wiley, second edition, 2008.

Ross Anderson und Tyler Moore. The economics of information security. *Science*, 314:610–613, 2006.

Ross Anderson, Rainer Böhme, Richard Clayton, und Tyler Moore. *Security Economics and the Internal Market*. ENISA, Heraklion, 2008.

Daniel Arce. Security-induced lock-in in the cloud. *Business & Information Systems Engineering*, 2022.

BaFin. *Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018, Bankaufsichtliche Anforderungen an die IT (BAIT)*. Bundesanstalt für Finanzdienstleistungsaufsicht, 2017a.

BaFin. *Rundschreiben 09/2017 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk*. Bundesanstalt für Finanzdienstleistungsaufsicht, 2017b.

BaFin. *Big Data trifft auf künstliche Intelligenz, Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen*. Bundesanstalt für Finanzdienstleistungsaufsicht, 2018a.

BaFin. *Merkblatt - Orientierungshilfe zu Auslagerungen an Cloud-Anbieter*. Bundesanstalt für Finandienstleistungsaufsicht, 2018b.

Rainer Böhme. The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4(1), 2018.

Rainer Böhme, Lisa Eckey, Tyler Moore, Neha Narula, Tim Ruffing, und Aviv Zohar. Responsible vulnerability disclosure in cryptocurrencies. *Communications of the ACM*, 63(10), 2020.

R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145, 2001.

Julie S. Downs, Mandy Holbrook, und Lorrie Faith Cranor. Behavioral response to phishing risk. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit*, eCrime '07, page 37–44, New York, NY, USA, 2007. Association for Computing Machinery.

Mieke Eoyang. *To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors*. Third Way, 2018.

FSB. *Third-party dependencies in cloud services – Considerations on financial stability implications*. Financial Stability Board (FSB), 2019.

Sebastien Gay. Strategic news bundling and privacy breach disclosures. *Journal of Cybersecurity*, 3(2), 2017.

Vincent Haupert, Dominik Maier, Nicolas Schneider, Julian Kirsch, und Tilo Müller. Honey, i shrunk your app security: The state of Android app hardening. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 69–91. Springer, 2018.

J. Jansen und R. Leukfeldt. How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In *2015 Workshop on Socio-Technical Aspects in Security and Trust*, pages 24–31, 2015.

Michael L. Katz und Carl Shapiro. Network externalities, competition, and compatibility. *The American Economic Review*, 75(3):424–440, 1985.

Ansgar Kellner, Micha Horlboge, Konrad Rieck, und Christian Wressnegger. A study on the effectivity of jailbreak detection in banking apps. In *Proceedings 4th IEEE European Symposium on Security and Privacy (EuroS&P)*, June 2019.

Arne Klaas. „White Hat Hacking“ – Aufdecken von Sicherheitsschwachstellen in IT-Strukturen. *Multimedia und Recht*, 2022:187–192, 2022.

Benjamin Lansford. Strategic coordination of good and bad news disclosures: The case of voluntary patent disclosures and negative earnings surprises. *SSRN*, 2006.

Ian Larkin. Bargains-then-ripoffs: Innovation, pricing and lock-in in enterprise software. Academy of Management Annual Meeting Proceedings, Februar 2008.

Tom Lookabaugh und Douglas C. Sicker. Security and lock-in. *Economics of Information Security. Norwell, MA: Kluwer Academic*, pages 225–245, 2004.

Dominique Machuletz und Rainer Böhme. Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020:481–498, 04 2020. doi: 10.2478/popets-2020-0037.

Allison Peters und Amy Jordan. Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *J. Nat'l Sec. L. & Pol'y*, 10:487, 2019.

Markus Riek, Rainer Böhme, und Tyler Moore. Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13 (2):261–273, 2016.

Carl Shapiro und Hal R. Varian. *Information Rules. A Strategic Guide to the Network Economy.* Harvard Business School Press, 1998.

Amutheezan Sivagnanam, Soodeh Atefi, Afiya Ayma, Jens Grossklags, und Aron Laszka. On the benefits of bug bounty programs: A study of Chromium vulnerabilities. In *Workshop on the Economics of Information Security (WEIS)*, 2021.

Kiran Sridhar und Ming Ng. Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. *Journal of Cybersecurity*, 7(1), 03 2021. ISSN 2057-2085. doi: 10.1093/cybsec/tyab007. URL `https://doi.org/10.1093/cybsec/tyab007`. tyab007.

Arthur Tatnall und Christopher Leslie. *International Communities of Invention and Innovation: IFIP WG 9.7 International Conference on the History of Computing, HC 2016, Brooklyn, NY, USA, May 25-29, 2016, Revised Selected Papers*, volume 491. Springer, 2016.

Rick Wash und Molly M. Cooper. Who provides phishing training? Facts, stories, and people like me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–12, New York, NY, USA, 2018. Association for Computing Machinery.

universität innsbruck

Forschungsprojekt I-GIT

Anhang 1a: Anschreiben (deutsch)

Innsbruck/Bonn März 2020

Sehr geehrte Damen und Herren,

aufgrund der Digitalisierung entstehen neue Geschäftsmodelle und Möglichkeiten im Finanzsektor, wodurch sich dieser wandelt und sich auch Veränderungen der Wertschöpfungsketten abzeichnen. Dies hat unmittelbare Folgen für die IT-Sicherheit und die Ausfallsicherheit der Zahlungssysteme. In einer weitgehend digitalisierten – in einigen Bereichen nahezu bargeldlosen – Gesellschaft berühren diese Entwicklungen die Stabilität des Zahlungsverkehrs bzw. Wirtschaftssystems. Deshalb haben wir, die Universität Innsbruck und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), gemeinsam eine Forschungskooperation angestoßen um mit Hilfe von Szenarien zukünftige Entwicklungen zu antizipieren und mögliche Folgen für den Finanzsektor abzuschätzen.

Um die Relevanz und Korrektheit der Szenarien zu überprüfen, möchten wir gerne mit ausgewählten Unternehmen des Finanzsektors Gespräche in Form von informellen Interviews durchführen. Basis für das Gespräch wären drei Szenarien, welche die Forschungskooperation erarbeitet hat und den teilnehmenden Personen im Vorfeld des Gesprächs zur Verfügung stellen wird.

Wir würden uns sehr freuen, wenn Sie sich uns für dieses Forschungsprojekt im Rahmen eines Interviews durch die Universität Innsbruck und die BaFin zur Verfügung stellen.

Es handelt sich hierbei ausdrücklich nicht um ein aufsichtliches Gespräch, sondern es dient dem Zweck Ihre Expertise in das Forschungsprojekt einfließen zu lassen. Die Teilnahme am Gespräch ist freiwillig. Die Ergebnisse jedes Einzelgesprächs werden anonymisiert in die Finalisierung der Szenarien eingearbeitet. Eine spätere Veröffentlichung der Forschungsergebnisse ist avisiert und wird Ihnen nach Fertigstellung gerne zur Verfügung gestellt.

Da es sich bei der Arbeit um eine perspektivische Einschätzung der zukünftigen Entwicklung des Finanzsektors handelt, halten wir die Teilnahme einer hochrangigen Person mit strategischer Cyber-Expertise aus Ihrem Haus (z.B. CIO) für hilfreich. Daneben wäre die Teilnahme weiterer Personen mit technischer Expertise geeignet.

Für das Interview stellen wir uns einen Rahmen von drei Stunden vor. Wir passen uns hier aber sehr gerne Ihren Verfügbarkeiten an. Um Ihren Aufwand möglichst gering zu halten, können wir das Gespräch gerne bei Ihnen führen.

Wir wären Ihnen für eine kurze Rückmeldung, telefonisch oder per E-Mail, direkt an Herrn Prof. Rainer Böhme von der Universität Innsbruck unter rainer.boehme@uibk.at oder +43 (512) 507-53202 innerhalb der nächsten zwei Wochen sehr dankbar.

Für Rückfragen zu dem Hintergrund des Forschungsprojekts, den Gesprächsteilnehmenden können Sie sich gern an folgende Personen wenden:

universität innsbruck

Forschungsprojekt I-GIT

Anhang 1b: Anschreiben (englisch)

Innsbruck/Bonn, September 2020

Dear . . . ,

Increasing digitalization gives rise to new business models and causes further changes in the financial sector, in particular a reorganisation of value chains. This affects both the security and resilience of payment systems and in a digitalized world, consequently the stability of payments and the financial market themselves.

In light of these considerations, we – the German Federal Financial Supervisory Authority and the University of Innsbruck – entered into a research cooperation. We aim to anticipate future trends in the payments market and derive possible consequences for the financial sector and the prudential supervision.

We developed three scenarios describing potential future developments to be evaluated through semi-structured interviews with representatives of various financial market actors, including not only banks and financial service providers but also IT providers and merchants. Based on our findings, in a second step, we will derive consequences and develop potential strategies for financial supervision.

We would appreciate the opportunity to interview you. The attached scenarios provide a concise summary of the starting point for our discussion. We believe your opinions on the scenarios would add great value to our research project. Furthermore, we encourage you to contribute your own scenarios or future expectations in addition to our scenarios.

The participation of one of your employees with an expertise in strategic cyber security would be very helpful. Employees with technical expertise would also be suitable participants.

The interviews will be carried out via video conferences. For each interview, we usually schedule three hours but are able to adapt based on your availability. Please contact Dr. Paulina Jo Pesch (University of Innsbruck) for any further steps via e-mail to paulina.pesch@uibk.ac.at or by telephone under the mobile number +49 1511 634 8344.

All responses from participants will be anonymized in any publications based on this research.

If you have any questions, please do not hesitate to contact one of the following project members:

[redacted]

Sincerely,

. . .

universität innsbruck

Forschungsprojekt I-GIT

Anhang 2a: Kurzfassung der Szenarien (deutsch)

Die folgenden im Projekt zu validierenden Szenarien basieren auf kontroversen, teils überspitzten Thesen zur künftigen Finanzmarktentwicklung, insbesondere im Zahlungsverkehr. Sie sind nicht als Prognose der Projektkooperation zu verstehen.

Szenario 1: Neue Schnittstellen fördern Cyber-Kriminalität

Im Zuge der fortschreitenden Digitalisierung werden zunehmend neue Finanzdienste entwickelt. Mit diesen treten neue Akteure in den Finanzmarkt ein, für die Banken Schnittstellen bereitstellen müssen. Diese müssen vom Internet aus erreichbar, also offen gestaltet sein. Über diese Schnittstellen wird dynamisch, also abhängig vom Reaktionsverhalten der jeweils Beteiligten kommuniziert. Hierdurch steigt die Komplexität der im Finanzsektor verwendeten IT-Infrastruktur. Abbildung 1 veranschaulicht die Ausdifferenzierung der Wertschöpfungskette.

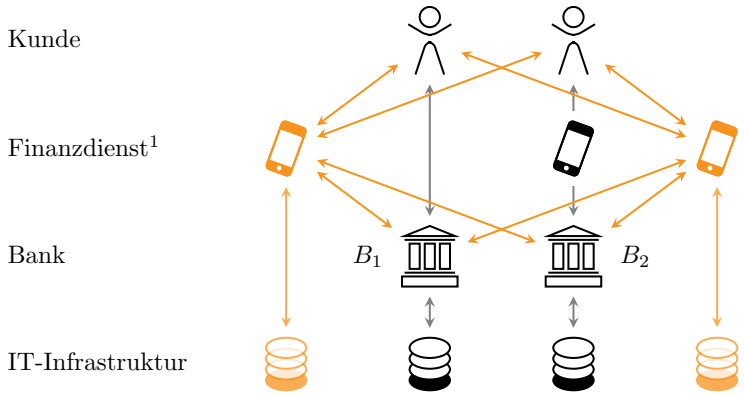

Abbildung 1: Ausdifferenzierung und Flexibilisierung der Wertschöpfungskette: Farblich hervorgehobene Akteure und Beziehungen sind neu hinzugekommen.

Mit jeder offenen Schnittstelle **vergrößert sich die Angriffsfläche** für Cyberkriminelle. Je verteilter ein System realisiert ist, desto schwieriger ist es gegen Angriffe zu schützen. Bekannte Sicherheitstechnologien sind nur bedingt zur Verteidigung stark arbeitsteilig und dynamisch organisierter Wertschöpfungsketten geeignet. Schon die Erfassung der möglichen dynamischen Abhängigkeiten bereitet Probleme. Die herrschenden Rahmenbedingungen setzen zudem nicht in jedem Fall Anreize für die Verbesserung der IT-Sicherheit. Dies liegt auch daran, dass der Einsatz von Schnittstellen-Intermediären durch die Beteiligten uneinheitlich ist. Das veranschaulicht Abbildung 2.

Cyber-Kriminelle werden die Authentifikationsmechanismen von Banken für neue Zahlungsdienstleister umgehen und die Bankenschnittstelle mit den Berechtigungen eines (impersonifizierten) dritten Zahlungsdienstleisters nutzen. Durch steigende Komplexität wächst die Angriffsfläche sowohl in technischer,

[1] Der Begriff des Finanzdiensts ist untechnisch für im Finanzsektor gegenüber Endkunden erbrachte Dienste zu verstehen, ohne Rücksicht darauf, ob diese von Banken, anderen Instituten oder Fin-Tech-Unternehmen (ohne Bankenlizenz) erbracht werden.

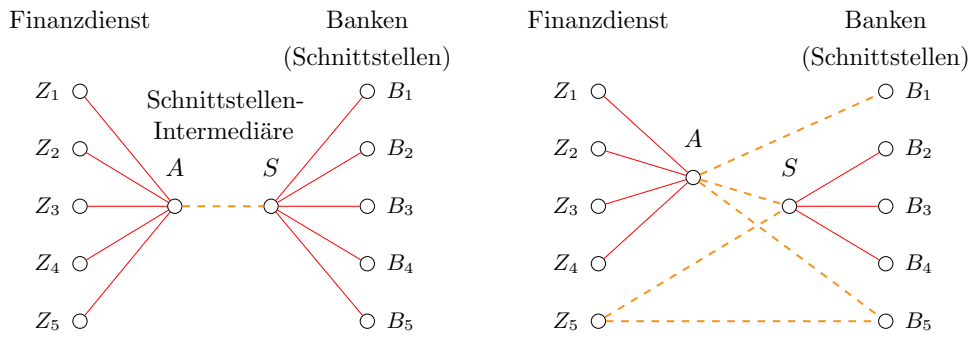

Abbildung 2: Schematische Darstellung der Schnittstellen-Topologie im Zahlungssektor. Links: Idealisierte Auslagerung an jeweils einen Schnittstellen-Intermediär auf Seite der Finanzdienste (A) bzw. Banken (S). Rechts: Realistischere Situation mit uneinheitlicher Einbindung von Schnittstellen-Intermediären.

als auch in sozialer Hinsicht. Die Sicherheit von an Konsumenten gerichtete Zahlungssysteme hängt maßgeblich davon ab, dass Benutzer die den Sicherheitsmechanismen zugrunde liegende Logik zumindest ansatzweise verstehen und sich auch dann richtig verhalten, wenn Cyber-Kriminelle zu Fehlverhalten anstiften.

Szenario 2: Konzentration der IT-Infrastruktur

Neue technische Möglichkeiten, Wettbewerbsdruck und Charakteristika des IT-Sektors fördern die Konzentration von IT-Infrastruktur. Sowohl Banken, als auch Fin-Tech-Unternehmen werden gleichermaßen an **branchenspezifische IT-Dienstleister** auslagern, welche wiederum über eine oder mehrere Ebenen die gemeinsame Infrastruktur dritter IT-Dienstleister nutzen. Zu einer Konzentration von IT-Infrastruktur kommt es bei Cloud-Anbietern, aber auch bei anderen Dienstleistern, etwa im Bereich der Software-Programmierung. Dies wird dadurch begünstigt, dass IT-Dienste kostengünstig skalierbar sind. Große IT-Dienstleister mit entsprechender Kapitalausstattung werden zudem gezielt Strategien zur Gewinnung und Bindung vieler Kunden einsetzen. Sie werden ihre Dienste anfänglich preisgünstig anbieten, bis sie so etabliert sind, dass der Markt fast nicht mehr oder nur noch schwer auf sie verzichten kann. In der Folge tritt eine faktische Bindung der betroffenen Banken und Fin-Tech-Unternehmen durch hohe Wechselkosten ein.

Weil die IT-Dienstleister dann eine Vielzahl von Akteuren bedienen, wirkt sich eine etwaige Unterbrechung der von ihnen erbrachten Dienste auf das ganze System aus. Durch die Konzentration der IT-Infrastruktur werden IT-Dienstleister, z. B. Plattformanbieter, also zunehmend **Systemrelevanz** erlangen.

Szenario 3: Gefahr einer einsetzenden Reduktion der Bank auf eine Risiko-tragende Hülle

In drastischer Zuspitzung führt die in Szenario 2 beschriebene Entwicklung zu einem umfassenden Bedeutungsverlust von Banken. Infolge einer Konzentration der Finanzdienstleistungslandschaft auf einzelne – im äußersten Fall auf nur ein *gemeinsames* internationales – Big-Tech-Unternehmen tritt eine Reduzierung von Banken auf bloße Risikohüllen (Szenario 3) ein. Im Rahmen des Outsourcings auf **IT-Unternehmen**, wie z. B. **Cloud-Anbieter**, erhalten diese Zugriff auf die Daten und Geschäftslogik ihrer Kunden, der beaufsichtigten Banken. Dies ermöglicht es den IT-Unternehmen, weitere Teile derer IT selbst anzubieten und ihren Kunden die weitere Auslagerung zu günstigen Preisen anzubieten. In der Folge bieten Cloud-Anbieter **eigene Finanzdienste** wie insbesondere Zahlungsdienste an.

Dies führt zu einer sukzessiven Verschiebung der Herrschaft nicht nur über die IT-Infrastruktur, sondern auch über die Finanzdienstleistungslandschaft auf IT-Unternehmen, insb. auf Big-Tech-Unternehmen. Gegenüber dem Endkunden tritt das IT-Unternehmen als Zahlungsdienst auf, im Hintergrund steht die Bank als Abwicklerin, die aber diese Dienstleistungen weitgehend auslagert. Dabei verbleiben Banken als relativ machtloser (da austauschbarer) Teil der Zahlungs- und Finanzdienstleistungslandschaft.

universität innsbruck

Research project I-GIT

Anhang 2b: Kurzfassung der Szenarien (englisch)

Disclaimer: The scenarios described below are designed to provoke participants to consider potential future developments of the financial market with a focus on payments and the role of Tech providers. They are not predictions of the project partners and are by no means the most probable developments.

Scenario 1: The more interfaces, the more cybercrime

Increasing digitalisation gives rise to novel financial services provided by new actors entering the financial market. Regulation forces banks to facilitate such services and FinTech firms by providing open APIs. Communication over these APIs is dynamic in that it depends on the involved parties' requests and responses. This increases the complexity of the IT infrastructure that the financial sector relies on. Figure 1 illustrates the disruption in value chains due to new actors and relationships.

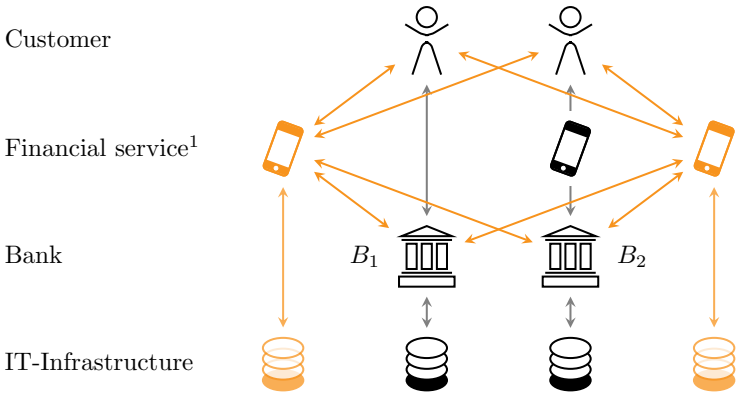

Figure 1: Differentiation and flexibilisation of the value chain. New actors and connections are highlighted in orange.

Each open API **increases the surface exposure** that could be targeted by cybercriminals. Beyond the number of APIs, the fact that they are distributed across many actors, increases the difficulty of effectively protecting against cyberattacks. Comprehensively mapping all possible inter-dependencies and relationships is a hard problem, let alone implementing sufficient security measures. Many existing security technologies were developed under the assumption a centralized IT department can oversee security risk. Clearly this breaks down when the payments ecosystem consists of a range of actors whose systems are interconnected via open APIs. Beyond coordination problems, existing frameworks may not necessarily incentivise financial market actors to implement strong IT security measures. Figure 2 illustrates that the use of intermediaries for interfaces is heterogenous.

Cybercriminals will target the procedures banks use to authenticate legitimate market actors, in particular by impersonating certified payment service providers. Increasing complexity gives rise not only to attacks on the technical level but also to social engineering attacks. For the security of payment systems, it is

[1] The term financial service is meant nontechnical. It is used to describe services provided for retail customers in the financial sector. Providers can be banks, other institutes or fintech companies (without a banking license).

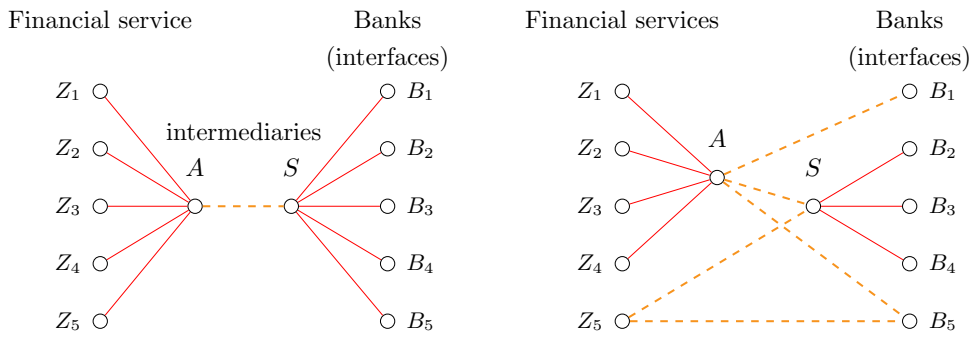

Figure 2: Schematic illustration of the interface topology in the financial sector. Left side: idealistic outsourcing from financial services (A) or banks (S) to each one intermediary for interfaces. Right side: more realistic situation with mixed outsourcing to intermediaries for interfaces.

crucial for end users to have a basic understanding of the security measures in place and how to properly behave when targeted by cybercriminals.

Scenario 2: Concentration of IT infrastructure

New technologies, competitive pressure, and characteristics of the IT sector encourage the concentration of IT infrastructure. Financial market actors outsource functionality to **sector-specific IT providers** who themselves will outsource their infrastructure to IT providers.

Over time this market logic will lead to the migration of financial infrastructures to cloud providers. Beyond hardware, we are also likely to see significant concentration in software provision. Information economics shows how market concentration in this area is intensified by intentional market strategies to increase network effects and customer lock-in. One such strategy is to initially under-price products to gain a large customer base who become habituated to the product and rely on it to relate to other users or companies. If these dynamics which have already been realized in consumer products play out in financial markets, banks and other financial institutions will find themselves locked-in due to high switching costs.

Any failure of one providers' services used by a majority of financial market actors will affect the financial system as a whole. Consequently, IT providers become **systemically relevant** financial market actors and an accumulation point for risks to financial stability.

Scenario 3: Banks as mere regulatory risk-bearers

In a worst-case scenario, concentration could cause a far-reaching loss of influence for banks. If a variety of banks decides to outsource their IT infrastructure to the same few IT companies, these companies gain insights into their customers' business logic and customer bases. Over time this data may provide a strategic insights into the financial market as a whole. This enables **IT companies**, especially **large cloud service providers**, to **develop their own financial services** (e.g. payment services). Such companies could use the network of consumers from 'traditional' technology products to facilitate entry into financial services. This may involve strategies such as cross-subsidisation, nudges (e.g. control over defaults), and inter-operability. Such a scenario would see tech companies slowly take control over the financial sector, while leaving the usurped financial institutions as mere regulatory risk-bearers in order to provide regulated payments services.

universität innsbruck

Forschungsprojekt I-GIT

Anhang 3: Interview-Leitfaden

Guten Tag... vielen Dank, dass Sie sich die Zeit nehmen, mit uns über Entwicklungen des Finanzmarktes zu sprechen. Bevor wir mit dem Interview beginnen, möchten wir uns vorstellen. ... Bei I-GIT handelt es sich um ein Forschungsprojekt der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und des Security und Privacy Lab der Universität Innsbruck. Das Projekt hat sich zum Ziel gesetzt, künftige Entwicklungen des Finanzmarktes zu untersuchen. Hierfür haben wir teils überspitzte Thesen zu künftigen Entwicklungen erarbeitet und in Szenarien übersetzt. Diese möchten wir nun im Rahmen von Interviews mit Vertretern verschiedener Finanzmarktakteure validieren.

Wir freuen uns, dass Sie bereit sind im Namen der/des... mit uns zu sprechen. Wir werden das Gespräch zu internen Zwecken aufzeichnen und transkribieren. ...

Unser Interview wird folgendermaßen strukturiert sein. Im ersten Teil des Interviews möchten wir zunächst wissen, inwieweit unsere Szenarien Ihre Erwartungen reflektieren. Dabei werden wir Ihnen auch Gelegenheit geben, anderweitige Ihrer Meinung nach wahrscheinliche oder mögliche Entwicklungen anzusprechen. Anschließend werden wir Ihnen in Teil 2 des Interviews konkrete, vertiefende Fragen zu den Szenarien stellen.

1 Szenarien und allgemeine Erwartungen

1.1 Alle

a) Zunächst möchten wir wissen, ob Sie sich mit den Szenarien schon vorab vertraut gemacht haben.
   i) Falls nicht, ...
   ii) Falls das der Fall ist, haben Sie auch die Langfassung gelesen oder sich auf deren Grundlage intern briefen lassen?

b) Halten Sie die Szenarien für plausibel?

c) Wie hoch bewerten Sie die Wahrscheinlichkeit, dass diese so eintreffen?

d) Rechnen Sie mit abweichenden oder sogar gegenteiligen Entwicklungen?

e) Haben Sie anderweitig, ganz unabhängig von den von uns beschriebenen Szenarien, Erwartungen, wie sich der Finanzmarkt künftig entwickeln wird?

2 Schnittstellenvielfalt und -dienste/-dienstleister

2.1 Banken

a) Wieviele offene Schnittstellen für wieviele Berechtigte stellen Sie bereit?

b) Seit wann stellen Sie Schnittstellen bereit?

c) Wie behalten Sie den Überblick über Schnittstellen und Berechtigte?

d) Nutzen Sie einen Schnittstellendienst?
   i) Haben Sie vertragliche Abreden zur Haftung getroffen?

ii) Ist Ihnen bekannt, welche Anbieter Wettbewerber (Banken oder FinTechs) nutzen / welche Wettbewerber denselben Dienst nutzen?

e) Haben Sie Strategien zur Reduktion von Komplexität oder zur Vermeidung von Komplexitätssteigerungen?

2.2 FinTech-Unternehmen

a) Die Schittstellen wie vieler Banken nutzen Sie?

b) Seit wann?

c) Wieviele Wettbewerber nutzen Ihrer Einschätzung nach dieselben Schnittstellen?

d) Nutzen Sie einen Schnittstellendienst?

i) Haben Sie vertragliche Abreden zur Haftung getroffen?

ii) Ist Ihnen bekannt, welche Anbieter Wettbewerber (Banken oder FinTechs) nutzen / welche Wettbewerber denselben Dienst nutzen?

e) Haben Sie Strategien zur Reduktion von Komplexität oder zur Vermeidung von Komplexitätssteigerungen?

2.3 IT-Dienstleister

a) Bieten Sie Schnittstellen-Dienste an?

i) Für wieviele Banken und FinTech-Unternehmen stellen Sie diese bereit? Wie groß ist hier Ihr Marktanteil? Welche wichtigen Wettbewerber haben Sie?

ii) Wie viele Schnittstellen entfallen im Schnitt etwa auf eine einzelne Bank bzw- ein einzelnes Fin-Tech-Unternehmen?

iii) Wieviele Berechtigte entfallen im Schnitt etwa auf eine einzelne Schnittstelle?

iv) Auf wessen Initiative werden konkrete Schnittstellen implementiert? Wie kommt die konkrete Entscheidung, eine bestimmte Schnittstelle zu programmieren, zustande?

v) Haben Sie vertragliche Abreden zur Haftung getroffen?

vi) Haben Sie Interesse an einer Reduktion von Komplexität oder einer Vermeidung von Komplexitätssteigerungen? Haben Sie in diesem Fall Strategien?

vii) Wie einfach könnten die Banken und FinTechs, die Ihre Dienste nutzen, zu einem anderem Anbieter wechseln?

b) Im Übrigen: Welche Dienste bzw. Produkte bieten Sie an? (z.B. App Hardening, Chipkartenleser-Hersteller)

i) Für wieviele Banken und FinTech-Unternehmen stellen Sie diese bereit? Wie groß ist hier Ihr Marktanteil? Welche wichtigen Wettbewerber haben Sie?

ii) Haben Sie vertragliche Abreden zur Haftung getroffen?

iii) Haben Sie Interesse an einer Reduktion von Komplexität oder einer Vermeidung von Komplexitätssteigerungen? Haben Sie in diesem Fall Strategien?

iv) Wie einfach könnten die Banken und FinTechs, die Ihre Dienste nutzen, zu einem anderem Anbieter wechseln?

2.4 Händler

a) Auf wieviele Schnittstellen von Banken und FinTechs greifen Sie zu, um Ihren Nutzer*innen die Zahlung mittels neuer Zahlungsdienste anzubieten?

b) Sind Sie oder ein Ihrem Konzern angehöriges Unternehmen in diesem Zusammenhang zugleich anderweitig in die Wertschöpfungskette integriert (z.B. als Cloud-Anbieter von Banken oder FinTech-Unternehmen)?

c) Planen oder erwägen Sie eigene Dienstleistungen oder Produkte für den Finanzmarkt oder eigene Finanzdienste anzubieten?

2.5 Sonstige

3 IT-Sicherheit und Cybercrime

3.1 Alle

a) Reagieren Sie mit bestimmten technischen IT-Sicherheitsmaßnahmen auf neuartige Bedrohungen, insb. durch neue Zahlungsdienste? Verfolgen Sie angesichts neuartiger Bedrohungen Strategien zur Vermeidung von Social Engineering (der Ausnutzung der Schwachstelle "Mensch"?

b) Informieren Sie Kunden regelmäßig über neue Sicherheitsmechanismen / Modi Operandi von Angreifern?

   i) Wie gut funktioniert das Ihrem Eindruck nach?

   ii) Wird das von den Kunden angenommen oder gibt es Klagen über mangelnde Nutzerfreundlichkeit / Usability?

   iii) Hat sich hier etwas geändert, seit Sie für Wettbewerber offene Schnittstellen anbieten?

c) Was sind Ihre Motive / Abwägungsfaktoren für IT-Sicherheitsmaßnahmen? (insb. Haftung/Reputation)

d) Welche Rolle spielt, Ihrem Eindruck nach, IT-Sicherheit im Verhältnis zu Nutzerfreundlichkeit für die Reputation?

e) Hat Ihrer Einschätzung nach die Zahl von IT-Sicherheitsvorfällen im Finanzsektor mit neuen Diensten wie insbesondere Zahlungsauslösediensten zugenommen?

f) Haben Sie neue Arten / eine Häufung von Cyberangriffen erlebt, seit eine Vielzahl von neuen Diensten, insb. Zahlungsdiensten, Bankenschnittstellen nutzt?

g) Sehen Sie eine Korrelation zwischen der Zahl der für neue Dienste bereitgestellten Schnittstellen und Cyberagriffen/IT-Sicherheitsvorfällen?

3.2 Banken

a) Falls es im Zusammenhang mit dritten Finanzdiensten zu Haftungsfällen aufgrund nicht authorisierter Zahlungen gekommen ist: Konnten Sie den Anbieter des Finanzdienstes (oder einen Dritten) erfolgreich in Regress nehmen?

b) Falls ja: Gerichtlich oder außergerichtlich?

c) Falls nein: Wie schätzen Sie die Erfolgsaussichten in solchen Fällen ein?

4 Cloud-Dienste (Banken und FinTechs)

a) Nutzen Sie einen oder mehrere Clouddienste? (Wenn mehrere, warum?)

   i) Nach welchen Kriterien haben Sie diese ausgewählt?

ii) Nutzen Sie Techniken, damit Anbieter möglichst wenig Einblick in Ihre Geschäftsprozesse und -daten erhalten?

iii) Könnten Sie leicht zu einem anderen Anbieter wechseln?

iv) Ist Ihnen bekannt, welche Anbieter Wettbewerber nutzen / welche Wettbewerber denselben Dienst nutzen?

b) Welche anderen Intermediäre/dritte Dienste nutzen Sie (Programmierung, zB App)

i) Könnten Sie leicht zu einem anderen Anbieter wechseln?

ii) Ist Ihr Unternehmen aufgrund des Geschäftsmodells auf einen bestimmten Dienstleister angewiesen?

iii) Ist Ihnen bekannt, welche Anbieter Wettbewerber nutzen / welche Wettbewerber denselben Dienst nutzen?

c) Bieten Sie Finanzdienste an?

i) Welche Finanzdienste bieten Sie an?

ii) Arbeiten Sie mit einer Bank zusammen?

iii) Planen Sie das Angebot weiterer Finanzdienste?

5 Schluss

Damit sind wir am Ende. Haben Sie abschließende Gedanken, Anregungen oder Anmerkungen? Wir danken Ihnen. ...