VÖB DIGITAL

Cybersicherheit – gegen die dunkle Seite der Digitalisierung

1 Cybersicherheitsvorfälle können jeden treffen

Schon lange sind Hackerangriffe keine Fantasien von Drehbuchautoren mehr, sondern Realität. Die weltweiten Sicherheitsvorfälle nehmen im Zuge der Digitalisierung stetig zu. Der kürzlich in Deutschland bekannt gewordene Hackerangriff auf Politiker und Prominente zeigt, dass es jeden treffen kann und alle in ihrer Privatsphäre verletzlich sind.

Dies bestätigt auch der „NotPetya-Angriff“ von Sommer 2017, der besonders gravierend in Erinnerung geblieben ist. Der Erpressungstrojaner (Ransomware) befiel über ein Buchhaltungsprogramm zunächst zahlreiche Rechner in der Ukraine und von dort aus weltweit Tausende weitere Computer. Geschädigte bekannte Unternehmen waren unter anderem Merck und FedEx. Doch am schwerwiegendsten traf es den dänischen Großkonzern Maersk, dessen gesamtes Netzwerk vorübergehend lahmgelegt wurde. Die weltgrößte Reederei bezifferte den entstandenen Schaden auf etwa 200 Millionen Euro.

Vor gut zwei Jahren raubten zudem Cyberkriminelle 81 Millionen US-Dollar von der Zentralbank von Bangladesch durch Überweisungen an ausländische Banken. Zuvor hatten die Hacker die internen Prozesse der Zentralbank ausspioniert, um sich Zugang zum Zahlungsverkehrsnetzwerk SWIFT zu verschaffen. Spätestens seit diesem Vorfall ist in der Finanzdienstleistungsbranche ebenfalls nicht mehr zu leugnen, dass Cyberrisiken eine reale Bedrohung darstellen.

2 Digitale Transformation erfordert kontinuierliches Nachjustieren

Kriminelle Angriffe im Cyberraum kennen weder Sektoren- noch Ländergrenzen. Hinter den Attacken stehen unterschiedliche – häufig finanziell oder politisch motivierte – Interessen. Infolge der weltweiten digitalen Vernetzung können Cyberattacken zukünftig vergleichsweise noch größere Wirkung als die bisher bekannten Fälle entfalten und somit noch mehr Schaden anrichten. Mit der digitalen Transformation des Finanzsektors und der Entwicklung innovativer Technologien entsteht also nicht nur ein erweitertes Spektrum an Möglichkeiten, sondern zugleich auch eine zunehmend große Vielfalt an Gefahren und Risiken. Besonders die Institute und deren IT-Dienstleister stehen deshalb heute und in Zukunft vor der Herausforderung, ihre präventiven Sicherheitsmaßnahmen und laufenden Kontrollen so schnell wie möglich an die technologischen Entwicklungen anzupassen. Hersteller und IT-Dienstleister sollten daher bereits frühzeitig beim Design neuer Produkte und Dienstleistungen Cybersicherheitsrisiken und -anforderungen („Security by Design“) berücksichtigen. Diese sollten einen vergleichbaren Stellenwert wie funktionale und ökonomische Faktoren einnehmen, um von Beginn an ausreichende Berücksichtigung zu erfahren.

Zudem sollten IT-Sicherheitsstandards für internetfähige Produkte weiterentwickelt und etabliert werden. Weiterhin können Verbraucher-Gütesiegel, die zeigen, dass gesetzliche Mindeststandards eingehalten werden, einen wichtigen Beitrag leisten.

Ebenso sinnvoll wäre es, wenn sich Hersteller und Anbieter verpflichten, Sicherheitslücken digitaler Produkte und Dienstleistungen bekanntzumachen und zu beheben. Die Bundesregierung hat im Rahmen des Koalitionsvertrages vom Frühjahr 2018 grundsätzlich die Absicht erklärt, hier in Deutschland stärker aktiv zu werden. Von besonderer Bedeutung ist dabei, dass alle Käufer bzw. Nutzer (unter anderem Banken, Sparkassen und Privatpersonen) Hard- und Softwareprodukte in Bezug auf deren (Cyber-)Sicherheit besser vergleichen können. Dazu müssen Hersteller zumindest verpflichtend angeben, wann, wie häufig und in welchem Umfang sie Sicherheits- und Firmware-Updates im Rahmen der Produktpflege garantieren.

Insgesamt wird der Nutzen aus der Digitalisierung nur dann dauerhaft Bestand haben können, wenn Cybersicherheitsaspekte und -anforderungen im Sinne einer bestmöglichen Informationssicherheit grundlegend verankert werden können. Dies ist zugleich eine wichtige Voraussetzung für einen wirkungsvollen Datenschutz, der ohne ausreichende Informations- bzw. Datensicherheit nicht gelingen kann.

3 Viel erreicht, aber noch lange nicht am Ziel

Positiv festzuhalten ist, dass insbesondere die in Deutschland ansässigen Finanzinstitute Cyberbedrohungen als Gefahrenpotenzial und bedeutendes Thema erkannt haben. So belegen aktuelle Studien, dass das Bewusstsein für Cyberrisiken in den Vorstandsetagen – auch anderer Branchen – zunimmt (siehe Abbildung 1). Entscheider beschäftigen sich vermehrt mit notwendigen Lösungen und Verbesserungen. Die Banken arbeiten bereits seit vielen Jahren gemeinsam mit den beauftragten IT-Dienstleistern an passenden Lösungen zur Prävention und Behandlung von Informationssicherheitsrisiken. Fortlaufend entwickeln und verbessern sie geeignete Banksoftware oder implementieren neue Prozesse, die zu verbesserter Cybersicherheit beitragen.

Auch die Gesetzgeber und Aufsichtsbehörden in Europa und Deutschland haben ihrerseits einen wesentlichen Beitrag geleistet, indem sie umfassende Rahmenbedingungen und Begleitmaßnahmen entwickelt haben, mit denen die Cybersicherheit grundsätzlich verbessert werden konnte. Hervorzuheben sind dabei die europaweit und sektorenübergreifend geltenden Richtlinien zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS). In Deutschland tragen das Umsetzungsgesetz und das IT-Sicherheitsgesetz (IT-SiG) bereits seit Mitte 2017 diesem Ziel Rechnung. Ergänzend kommt die sogenannte KRITIS-Verordnung hinzu, die ebenfalls sektorenübergreifend Anforderungen an Betreiber kritischer Infrastrukturen beinhaltet. Zudem adressieren verschiedene Gesetze, Rahmenwerke und Richtlinien sowohl auf europäischer als auch nationaler Ebene umfänglich die Anforderungen an den Finanzsektor zur Erhöhung der Cyberresilienz sowie zur Informationssicherheit und zum Management damit verbundener Risiken in Banken. Dies erfolgt beispielsweise durch die Zahlungsdiensterichtlinie PSD2 mit spezifischen Vorgaben für

Abbildung 1: Was Entscheider bewegt: Bedeutung von Cyberrisiken nimmt zu

2017		2018	
1. Überregulierung	42 %	1. Überregulierung	42 %
2. Unsicherheit über Wirtschaftswachstum	34 %	2. Terrorismus	41 %
3. Wechselkurs-Volatilität	31 %	3. Geopolitische Unsicherheiten	40 %
4. Mangel an Schlüsselqualifikationen	31 %	4. Cyberrisiken	40 %
5. Geopolitische Unsicherheiten	31 %	5. Mangel an Schlüsselqualifikationen	38 %
6. Geschwindigkeit des technischen Wandels	29 %	6. Geschwindigkeit des technischen Wandels	38 %
7. Zunehmende Steuerbelastungen	29 %	7. Zunehmende Steuerbelastungen	36 %
8. Verändertes Konsumentenverhalten	26 %	8. Populismus	35 %
9. Soziale Instabilität	24%	9. Klimawandel und Umweltschäden	31 %
10. Cyberrisiken	24 %	10. Wechselkurs-Volatilität	29 %
11. Volatile Rohstoffpreise	20 %	11. Soziale Instabilität	29 %
12. Terrorismus	20 %	12. Protektionismus	29 %
13. Unzureichende Infrastruktur	20 %	13. Unsicherheit über Wirtschaftswachstum	26 %
14. Protektionismus	19 %	14. Unzureichende Infrastruktur	26 %
15. Mangel an Vertrauen in die Wirtschaft	19 %	15. Verändertes Konsumentenverhalten	26 %

Quelle: PwC CEO Survey 2018, eigene Darstellung

die Meldung kritischer Sicherheitsvorfälle im Zahlungsverkehr oder die Bankaufsichtlichen Anforderungen an die IT, kurz BAIT, die die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) veröffentlicht hat und zuletzt um ein optional anwendbares Kapitel für die KRITIS-Betreiber im Finanzsektor ergänzt wurde. Von staatlicher Seite wurden damit die grundlegenden Maßnahmen zur Erhöhung der Cybersicherheit bereits eingeführt.

Auch deutsche Aufsicht forciert Cybersicherheit

Die deutsche Bankaufsichtsbehörde BaFin stellt sich mit Blick auf Cyberrisiken neu auf und erweitert ihre Kapazitäten entsprechend. Hinter dem Kürzel GIT steht beispielsweise die Gruppe IT-Aufsicht/Zahlungsverkehr/Cybersicherheit, die derzeit in vier Referaten zusätzlich besonders die IT-sicherheitsrelevanten Themen und Aspekte bankaufsichtlich begleitet und bearbeitet. Ende September 2018 meldete die BaFin, dass sie von den rund 420 im Zahlungsverkehr gemeldeten Sicherheitsvorfällen rund ein Drittel als mittelschwere und schwere Vorfälle eingestuft hat. Der Großteil der Meldungen ergebe sich jedoch nicht aufgrund von Cyberangriffen, sondern infolge von Software- und Hardwarestörungen oder Fehlern bei Tests oder Anpassungen.

Insgesamt sieht die deutsche Aufsicht mangelnde „Cyberhygiene“, das heißt das Fehlen ausreichender organisatorisch-prozessualer Vorkehrungen, als eine ganz wesentliche Ursache für Sicherheitsvorfälle. Weitere Gründe liegen ihres Erachtens darin, dass Dienstleister unzureichend überwacht würden, Prozesse, Technologien und Personen nur ungenügend getestet würden und insgesamt zu wenig in die Fähigkeiten, Cyberangriffe zu entdecken und Bedrohungen zu identifizieren, investiert werde. Insgesamt sei laut BaFin der Fokus gelegentlich zu technikzentriert, während der Faktor Mensch manchmal noch vernachlässigt werde. So können nicht ausreichend sichere Passwörter genauso problematisch wie das unbedachte Weitergeben sensibler Informationen sein.

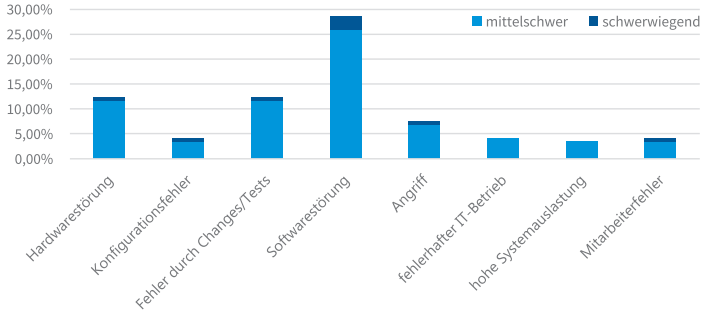
Die Aufsicht stellt aber dennoch fest, dass verheerende Cyberangriffe im Finanzsektor und in Europa bisher glücklicherweise ausblieben. Zudem sei die Anzahl der in der ersten Jahreshälfte 2018 in Deutschland gemeldeten IT-Sicherheitsvorfälle bei Betreibern kritischer Infrastrukturen im Finanz- und Versicherungswesen mit rund zwei Dutzend rein quantitativ überschaubar.

Der jüngste Bericht der „Bank of England“ zeigt, dass Banken verstärkt davon ausgehen, dass Cyberrisiken im Vergleich zu anderen für das Bankgeschäft typischen Risiken wesentlich schwieriger zu verhindern bzw. bei Eintritt zu bewältigen sind. Im besonderen Maße könnte das für den international stattfindenden interoperablen Zahlungsverkehr gelten. So sind beispielsweise Bankinstitute durch die PSD2 verpflichtet, Schnittstellen für andere Zahlungsdiensteanbieter zu öffnen. Insgesamt bedeutet die zunehmende globale Vernetzung also ein grundsätzlich erhöhtes Informationssicherheitsrisiko, da Strukturen immer komplexer werden, die Anzahl an Beteiligten zunimmt und es so immer mehr Einfallstore für potenzielle Cyberangriffe gibt. Finanzinstitute müssen diese Risiken in ihrer Cybersicherheitsstrategie immer mit einkalkulieren.

4 Internationale Initiativen treiben Cybersicherheit aktiv voran

Ohne international koordinierte Zusammenarbeit kann Cybersicherheit nicht „funktionieren“. Daher messen auch die G7-Staaten dem Thema Cybersicherheit im Finanzsektor schon seit geraumer Zeit eine hohe Bedeutung bei. Besonders unter Anbetracht der weltweiten Vernetzung der Finanzsysteme wurde die strategische Bündelung von Cybersicherheitsaktivitäten auf internationaler Ebene vorangetrieben. Bereits im Oktober 2016 wurden mit dem Rahmenwerk „G7 Fundamental Elements of Cybersecurity“ Mindeststandards für die Cybersicherheit in der Finanzdienstleistungsbranche veröffentlicht, die Verbraucher, Institute, Daten und Infrastrukturen schützen sollen. Es

Abbildung 2: Ursachen für Sicherheitsvorfälle – Erkenntnisse aus dem Meldewesen



- Seit 2017 rund 420 Sicherheitsvorfallsmeldungen (MaSi* bzw. PSD2), davon ein Drittel mittelschwere und schwerwiegende Vorfälle
- Mängel im Bereich der „Cyberhygiene“ als eine wesentliche Ursache
- Nur wenige Vorfälle durch Cyberangriffe verursacht

Quelle: BaFin, eigene Darstellung
* Mindestanforderungen an die Sicherheit von Internetzahlungen

umfasst zentrale Grundelemente der Cybersicherheit, so etwa wesentliche Anforderungen an Cybersicherheitsstrategien und Rahmenwerke und das Risiko-Controlling.

Auch das Europäische Parlament und die Europäische Kommission haben neben der bereits genannten NIS-Richtlinie verschiedene spezifische Maßnahmen und Aktivitäten auf den Weg gebracht, die die Cybersicherheit im Finanzsystem erhöhen sollen. So veröffentlichte die EU-Kommission im März 2018 den EU-FinTech-Aktionsplan, der Innovationen in einem stabilen Finanzsektor fördern soll und Cybersicherheit als Querschnittsthema deklariert. Sowohl die Europäische Bankenaufsichtsbehörde (EBA) als auch die Europäische Zentralbank (EZB) leiten daraus unterschiedliche Maßnahmen für ihr Mandat ab.

Jüngstes Beispiel ist TIBER-EU. Der Begriff steht für „Threat Intelligence-based Ethical Red Teaming". Das europäische Rahmenwerk wurde von der EZB unter Mitwirkung der Bundesbank und anderen nationalen Zentralbanken entwickelt und im Mai 2018 veröffentlicht. TIBER-EU soll mittels beauftragter „echter" Cyberangriffe durch sogenannte „Red Teams" die Widerstandsfähigkeit von Akteuren im Finanzbereich testen und vorhandene Schwachstellen ermitteln. Unter einem „Red Team" wird in diesem Zusammenhang eine Gruppe von Spezialisten verstanden, die versucht, in den Kern eines (IT-)Systems vorzudringen, und dazu Taktiken und Vorgehensweisen von echten Hackern verwendet. Ziel ist, dass die europäischen Behörden über Landesgrenzen hinweg in Cyberübungen zusammenarbeiten und Erkenntnisse zur Bedrohungslage sammeln und auswerten. In Deutschland haben die BaFin und das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor kurzem damit begonnen, über eine mögliche nationale Implementierung zu beratschlagen. Erörtert werden muss insbesondere, welcher Sorgfaltserfordernisse es bei der Durchführung bedarf und wie ein geeignetes Risikomanagement aussehen kann, um potenziellen Gefährdungen produktiver Systeme und weiteren Negativauswirkungen angemessen begegnen zu können. Die weitere Entwicklung und grundlegende Konkretisierung zur möglichen Umsetzung in Deutschland bleiben vorerst abzuwarten. Darunter fällt auch die Klärung der Frage, ob und für wen genau Maßnahmen aus TIBER-EU verpflichtend werden.

Der zuständige Ausschuss des EU-Parlamentes hat gefordert, den Entwurf der EU-Verordnung zur „EU-Cybersicherheitsagentur" (ENISA) sowie zur Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit") zu verschärfen. So sollte für Betreiber kritischer Infrastrukturen die Zertifizierung von sicherheitsrelevanten Produkten in der Informations- bzw. Kommunikationstechnologie bindend werden. Bereits heute sind die entsprechenden Betreiber gesetzlich verpflichtet, diese Systeme oder Produkte, etwa Chipkarten im Zahlungsverkehr, abzusichern. Eine durchgehende Zertifizierungspflicht würde aber den Wettbewerb auf Anbieterseite und letztlich den Handlungsspielraum, Cybergefahren zu begegnen, einschränken, wenn ausschließlich zertifizierte Leistungen und Produkte eingesetzt werden dürften. Zudem haben die Infrastrukturbetreiber keinen Einfluss darauf, ob die Produkthersteller, die zudem häufig nicht aus der EU stammen, den entsprechenden Zertifizierungsprozessen für den europäischen Markt unterliegen. Das Ergebnis der nunmehr abgeschlossenen Verhandlungen in der EU sieht zwar keine grundsätzliche Verpflichtung durch den Rechtsakt zur Cybersicherheit vor, lässt aber für die Umsetzung durch die ENISA bzw. die dafür zukünftig zuständige europäische Aufsichtsgruppe ECCG (european cyber security certification group) Spielraum, Zertifizierungsanforderungen festzulegen und zu beaufsichtigen. Das kann auch bedeuten, dass Zertifizierungen für einzelne Leistungen, Komponenten oder Produkte in Europa letztlich verpflichtend würden.

5 Alle Beteiligten sind in der Pflicht

Die Gesamtheit der bisherigen Maßnahmen und Aktivitäten hat die Cybersicherheit deutlich gestärkt. Aufgrund der hohen Transformationsgeschwindigkeit im Finanzsektor muss das Thema aber weiterhin oberste Priorität haben und die Maßnahmen müssen laufend an die sich verändernden Erfordernisse angepasst werden.

Gerade Banken stehen deshalb weiterhin vor der Herausforderung, für alle Geschäfts- und Transaktionsbereiche Cyberrisiken zentral zu koordinieren und diesen insgesamt auf möglichst effektive Weise zu begegnen. Dies gilt umso mehr, als dass der Schutz vor Cyberrisiken nicht nur Sache der einzelnen Institute ist, sondern ein koordiniertes Vorgehen aller Beteiligten erfordert. Es kann daher notwendig werden, dass europäische Initiativen und nationale Umsetzungsmaßnahmen fortgesetzt werden müssen. Im Rahmen ihrer Entscheidungsfindung sollten Gesetzgeber und Aufsichtsbehörden aber mögliche Aus- und Wechselwirkungen berücksichtigen. Im eigenen Interesse werden Unternehmen des Finanzsektors konsequent und fortlaufend überprüfen, ob die bereits getroffenen Schutzmaß-

nahmen für die bestehende bzw. zu erwartende Bedrohungslage ausreichen und diese ggf. anpassen bzw. weiterentwickeln. Cybersicherheit muss dabei immer auch als operationelles Risiko verstanden und behandelt werden. Die beste Strategie, um Cybersicherheitsrisiken zu reduzieren, liegt darin, die Sicherheitsorganisationen und -prozesse systematisch zu standardisieren und zu automatisieren. Vor allem aber sollte der manchmal noch vernachlässigte Faktor „Mensch“ stärker in den Sicherheitsstrategien berücksichtigt werden.

UNSERE POSITION

Wir begrüßen, dass alle beteiligten Akteure Cyberrisiken als Gefahrenpotenzial erkannt haben. Um der Bedrohungslage gerecht zu werden, bedarf es nun einer Regulierung mit Augenmaß.

Wir setzen daher mit Blick auf europäische und nationale Aktivitäten auf eine Regulierung, die alle Faktoren und mögliche Auswirkungen einbezieht und berücksichtigt. Nur so können TIBER-EU und die geplante Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik am Ende zu mehr Cybersicherheit beitragen.

Wir befürworten grundsätzlich Initiativen zur Etablierung europaweit einheitlicher IT-Sicherheitsstandards und Aufsichtspraktiken, die die Cybersicherheit verbessern sollen. Diese sollten sich aber am Vorbild der deutschen Praxis orientieren. Beispielsweise sind die Anforderungen an das IT-Informationssicherheits(risiko)management in den deutschen BAIT bereits ausreichend verankert.

Wir sind im Wesentlichen für die Unterstützung von Cybersicherheit durch Zertifizierung ausgesuchter IT-Produkte oder Leistungen (beispielsweise durch die optionale Zertifizierung von Cloud-Diensten im Auslagerungsfall), die für die IT-Sicherheit in besonderem Maße relevant sind. Eine verpflichtende Zertifizierung von (sicherheitsrelevanten) Produkten und Leistungen lehnen wir aber ab.

Wir fordern eine transparente und ausgewogene Regulierung, die entlang der sich neu bildenden Wertschöpfungsketten faire Wettbewerbsbedingungen für alle Markbeteiligten in Europa sicherstellt. Insbesondere die Verpflichtung, wesentliche Infrastrukturen („open everything“) und Schnittstellen im Zahlungsverkehr zu öffnen, muss für alle Marktbeteiligten gleichermaßen gelten. Nur so können funktionierende digitale Ökosysteme geschaffen und kann sichere branchenübergreifende Interoperabilität auf Basis von Standards realisiert werden.

Über VÖB Digital

Die Digitalisierung verändert das Bankgeschäft tiefgreifend und stellt Banken vor enorme Herausforderungen, denen es aktiv zu begegnen gilt. Diesen Transformationsprozess wollen wir mit unserem Newsletter VÖB Digital beleuchten – aber auch aktiv mitgestalten. Mit VÖB Digital zeigen wir nicht nur Risiken, sondern auch Chancen auf, suchen nach Lösungen und stellen Entwicklungsperspektiven dar.

Sie wollen VÖB Digital abonnieren?

*Dann schreiben Sie bitte eine E-Mail an **presse@voeb.de**. Geben Sie einfach den Betreff „Anmeldung VÖB Digital“ an. Alle VÖB-Newsletter können Sie zudem unter **www.voeb.de/de/publikationen/newsletter** bestellen und abbestellen. Weitere VÖB-Publikationen finden Sie online unter **www.voeb.de/de/publikationen**.*

IMPRESSUM
Bundesverband Öffentlicher Banken Deutschlands, VÖB
Lennéstraße 11, 10785 Berlin
Telefon: 030 8192 0 | Telefax : 030 8192 222
E-Mail: presse@voeb.de | Internet: www.voeb.de
Redaktion: Silke Birkholz
Redaktionsschluss: 21. Januar 2019
Foto: shutterstock, whiteMocca
Registernummer im Transparenz-Register der EU: 0767788931-41