Judith Jaisle / Andreas Bruckner

Die neue **Risikowahrnehmung**

Die beiden vergangenen Jahre stellten für die Unternehmen der Finanzindustrie eine unvergleichliche Herausforderung dar. Besonders gefordert waren die IT-Spezialisten, denn in kürzester Zeit mussten Arbeitsplätze in den Wohnzimmern der Mitarbeiter eingerichtet werden. Dies war nicht nur unter logistischen Gesichtspunkten eine massive Anstrengung, sondern auch im Hinblick auf Sicherheitsaspekte.

Schließlich öffneten die Verbindungen zwischen Homeoffice und Firmenrechnern viele potenzielle Einfallstore. Hacker und andere Cyberkriminelle nutzen diese Gelegenheit weidlich aus: 2020 war ein massiver Anstieg registrierter IT-Sicherheitsvorfälle zu verzeichnen. Dieser Trend setzte sich 2021 fort.

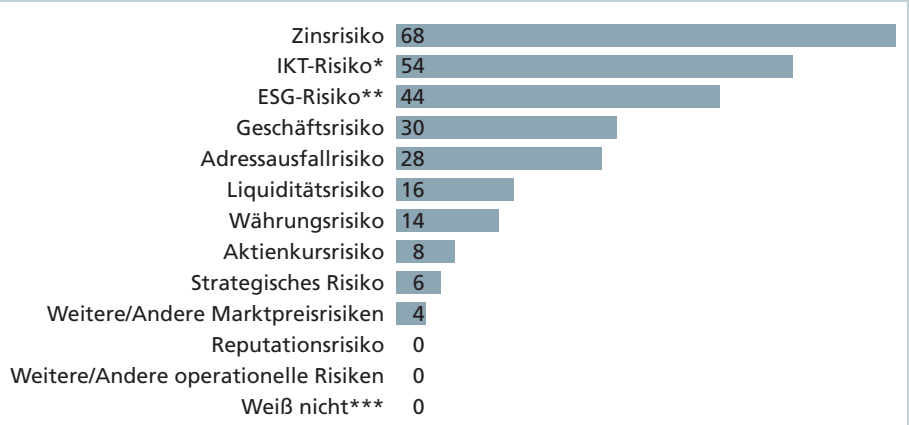
Verteilung knapper Ressourcen

Besonders gefährdet sind Branchen mit einem hohen Digitalisierungsgrad, vor allem wenn diese aufgrund wertvoller Kundendaten zugleich ein lohnenswertes Ziel für Verbrecher darstellen – eben wie die Finanzindustrie. Diese Feststellung führt unweigerlich zu der Frage, wie gut die Finanzdienstleister auf mögliche Cyberattacken vorbereitet sind. Das Hamburger Beratungs- und Softwarehaus PPI AG hat für seine aktuelle Studie „Paradigmenwechsel in der Risikostrategie" Entscheidungsträger deutscher Banken zu diesem Thema interviewt. Eine wichtige Erkenntnis aus den Antworten ist eine klare Verschiebung der Risikowahrnehmung der Institute. So wird zwar das Zinsrisiko nach wie vor als die prioritäre Herausforderung der kommenden zwei Jahre gesehen, aber bereits unmittelbar dahinter folgen Risiken aus der Informations- und Kommunikationstechnologie.

Für diese vorrangigen Risikosegmente müssen in einem hochdynamischen Marktumfeld ausreichend Ressourcen bereitgestellt werden, um die Wahrscheinlichkeit des Schadenereignisses möglichst gering zu halten. Dabei führt der spürbare Kostendruck auch zu Trends, die wieder IKT-Risiken schaffen. Ein Beispiel dafür ist die Tendenz, immer mehr IT-Services von externen Dienstleistern zu beziehen. Knapp drei Viertel der für die Studie befragten Institute haben zumindest Teile der eigenen IT ausgelagert. Dies betrifft auch existenzielle Kernfunktionen der Institute, was ein enormes Vertrauen gegenüber dem jeweiligen Partner erfordert. Entsprechend genau müssen die Finanzdienstleister bei Outsourcing-Projekten hinschauen, zumal die Verantwortung für die ausgelagerte Tätigkeit grundsätzlich bei ihnen verbleibt. Darüber hinaus steigen mit dem Digital Operational Resilience Act (DORA) die Anforderungen an die Outsourcing-Dienstleister hinsichtlich eigener Vorkehrungen zum Business Continuity Management (BCM) und zu Desaster-Recovery-Plänen. Diese Anforderungen sind wahrscheinlich nicht von allen Anbietern erfüllbar und führen auf jeden Fall zu höheren Outsourcing-Kosten.

Auch bei einem so sicherheitsrelevanten Thema wie dem Identity- und Accessmanagement (IAM) ist die wirtschaftliche

Abbildung 1: Wesentliche Risiken für Banken in den kommenden Jahren (in Prozent)



Die Risikopriorisierung deckt sich nur im ersten Punkt mit der Bewertung der Herausforderungen insgesamt. IKT-Risiken werden bereits an zweiter Stelle genannt und haben dadurch eine deutlich höhere Priorität, als die Einschätzung der Makrotrends vermuten lässt.

Maximal drei Antworten möglich. * Unter anderem Cyberrisiken/Informations- und Kommunikationstechnologie, ** Environmental, Social and Governance, *** Exklusive Antwortoption
Quelle: PPI AG

Judith Jaisle

Senior Manager, PPI AG, Hamburg

Andreas Bruckner

Manager, PPI AG, Hamburg

Die Frage ist längst nicht mehr ob, sondern wann und wie schlimm. Die Mehrheit der deutschen Finanzinstitute geht mittlerweile davon aus, in den kommenden Jahren Zielscheibe eines Cyberangriffs. Entsprechend hat sich die Risikowahrnehmung der Institute verschoben, hinter dem Zinsrisiko als der weiterhin prioritären Herausforderung der kommenden beiden Jahre folgen nun schon Risiken aus der Informations- und Kommunikationstechnologie. Das ist das zentrale Ergebnis einer Studie der PPI AG. Die Gründe für die verstärkte Anfälligkeit gegenüber Cyberkriminalität sind laut den Autoren vielfältig. Da sind offene Flanken durch die Verbindungen von Homeoffice zu Firmencomputern. Da ist der zunehmende, vor allem kostenseitig beförderte Trend zur Auslagerung wichtiger IT-Services an externe Dienstleister. Da ist die stetig wachsende Komplexität aufgrund des derzeitigen Trends zum Cloud Computing. Und da ist natürlich der Mangel an IT-Fachkräften. Interessanterweise beurteilen die befragten Institute ihre Fahigkeiten, Cyberangriffe zu erkennen und abzuwehren trotz allem als gut bis sehr gut. Die Autoren sind etwas skeptischer und sehen die Resilienz als entscheidenden Faktor, also die Fähigkeit, sich nach einer Attacke möglichst schnell wieder zu erholen. (Red.)

Anspannung des Marktes fühlbar. So halten zwar sämtliche Studienteilnehmer ihr IAM-System für State of the Art, knapp die Hälfte empfindet die Kosten dafür allerdings als zu hoch. Zwar können Zukunftstechnologien wie Blockchain oder künstliche Intelligenz (KI) Prozesse vermehrt optimieren und damit zu Kostensenkungen beitragen. Ihre Einführung sowie neue aufsichtsrechtliche Anforderungen zum Management privilegierter Accounts machen aber Anpassungen der aktuellen Systeme notwendig.

Gleiches gilt für die langfristige Bekämpfung von Betrugsversuchen. Obwohl sich deutsche Institute in diesem Bereich gut aufgestellt sehen, belasten neue regulatorische Vorgaben die bei vielen Instituten heterogene und zunehmend veraltete IT. In deren Modernisierung werden Banken verstärkt investieren müssen, auch wenn die Amortisation erst auf den zweiten Blick ersichtlich wird: Verhinderte beziehungsweise in Echtzeit erkannte Betrugsfälle und geringere Kosten für den Systemunterhalt sind die greifbaren Vorteile.

Resilienz rückt in den Fokus

Die Mehrheit der Finanzinstitute geht davon aus, in den kommenden Jahren Zielscheibe eines Cyberangriffs zu werden. Die Frage ist nur noch, wann. Daher rückt das Thema Cyberresilienz immer stärker in den Fokus, und zwar sowohl in der Branche selbst als auch bei den Aufsichtsbehörden. Unter diesem Begriff wird eine Reihe vor, während und nach einem Angriff notwendiger Maßnahmen subsumiert. Gemeint ist also faktisch die Fähigkeit, Cyberattacken im Vorfeld abzuwehren oder aber, wenn diese bereits stattfinden, zu erkennen, abzuschwächen und die eigene Systemlandschaft schnell wieder funktionsfähig zu machen. Beim Aufbau effektiver, resilienter Strukturen ergeben sich neue Kernfragen: „Wie reagiere ich, wenn etwas passiert?“ Und: „Wie schnell erkenne ich überhaupt, dass etwas passiert ist?“

Neuere Vorschriften wie DORA und TIBER (Threat Intelligence-based Ethical Red Teaming), ein Rahmenwerk für bedrohungsgeleitete ethische Hacking-Übungen, legen inzwischen größeren Wert auf die Resilienz einer Organisation.

Die deutsche Bankenbranche beurteilt ihre diesbezüglichen Sicherheitsmaßnahmen mit wenigen Ausnahmen als gut oder sehr gut. Allerdings dürften die nächsten Jahre in puncto Cyberangriffe komplex werden, insbesondere aufgrund des derzeitigen Trends zum Cloud Computing. Viele Banken betreten hier Neuland und sind sich der Gefahren kaum bewusst. Ein weiteres Problem für die Finanzbranche liegt im aktuellen Mangel an IT-Fachkräften. Bereits zum jetzigen Zeitpunkt bezeichnen 44 Prozent der befragten Institute die Einstellung qualifizierter Fachkräfte als herausfordernd. Nach unterschiedlichen Schätzungen fehlen in Deutschland zurzeit rund 80 000 IT-Spezialisten, Tendenz steigend. Die Banken müssen Lösungen für diese und andere Schwierigkeiten finden, wenn sie ihrer guten Selbsteinschätzung treu bleiben wollen.

Zentrale Statuserfassung

Die staatliche Aufsicht wird dabei sehr genau hinsehen. Denn deren Albtraum ist ein von IT-System zu IT-System überspringender Flächenbrand von Cyberattacken, der bis zu einem vollständigen oder teilweisen Ausfall des ganzen Finanzsystems führen kann. Untersuchungen der Europäischen Zentralbank zufolge hat die Zahl der kritischen IT-Befunde bei Banken in den vergangenen zwei Jahren deutlich abgenommen. Aber nach wie vor gibt es zu viele potenzielle Angriffsflächen für Cyberkriminelle.

„Die Bankenbranche beurteilt ihre Sicherheitsmaßnahmen mit wenigen Ausnahmen als gut oder sehr gut. “

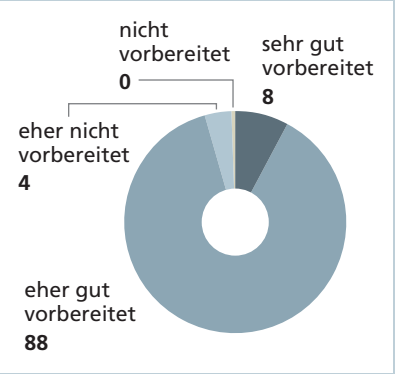
Um Schwachstellen in den eigenen Systemen zu vermeiden, ist ein funktionierendes IT-Assetmanagement unerlässlich. Darunter ist die Administration der verwendeten Hardware und Software bis zu den Peripheriegeräten innerhalb von Banken und Unternehmen zu verstehen. Nur mit einer zentralen Verwaltung, Speicherung und Archivierung der hierü-

ber vorhandenen Informationen lassen sich diese Komponenten im Sinne der IT-Sicherheit optimal aufeinander abstimmen.

Die für die Studie befragten Banken sehen sich in diesem Bereich ausnahmslos gut bis sehr gut aufgestellt. Dafür gibt es zwei Gründe. Zum einen sind dies handfeste betriebswirtschaftliche Erwägungen. Längst ist die IT in Banken und Versicherungen ein Wettbewerbsfaktor geworden, spätestens seit dem Aufkommen von reinen Onlinebanken. Eine zentrale Datenbank, wie etwa eine Configuration Management Database (CMDB), macht die permanente Kontrolle zentraler Parameter wie Auslastung und Kosten über alle Einsatzfelder hinweg möglich. Daraus ergeben sich in der Regel Einsparpotenziale.

Zum anderen ist ein funktionierendes IT-Assetmanagement mit individuellen Schutzbedarfen für jedes einzelne IT-Asset die

Abbildung 2: Vorbereitungsstand auf Cyberrisken (in Prozent)



Quelle: PPI AG

Basis für eine wirtschaftliche Steuerung von IKT-Risiken. Ohne einen Überblick über Hard- und Softwarekomponenten sind Schwachstellen kaum identifizierbar. Ein Beispiel in diesem Zusammenhang sind Patch- und Lifecycle-Prozesse. Über diese wird sichergestellt, dass keine veralteten Softwarekomponenten im Einsatz und alle Anwendungen auf dem neuesten Stand sind.

Die Anforderungen an das IT-Assetmanagement werden in Zukunft nicht weniger, im Gegenteil: Institute müssen künftig auch cloudbasierte Software und Infrastrukturen berücksichtigen. Um diesen und anderen Herausforderungen zu begegnen, ist mehr Automatisierung und Standardisierung notwendig. Ersteres bedingt die Einrichtung von Schnittstellen zwischen den Systemen des IT-Assetmanagements einerseits und den hier erfassten Zielsystemen andererseits. Das Zweite umfasst unter anderem die Vereinheitlichung genutzter Software zur Erfüllung der IT-Governance. Lücken in diesem Bereich können sich schnell zu erheblichen IKT-Risiken ausweiten. Schließlich leiten sich dem Grunde nach sämtliche innerhalb einer Bank getroffenen Maßnahmen hinsichtlich Cybersicherheit und -resilienz hieraus sowie aus der IT-Strategie ab.

„Im digitalen Dschungel ist jede Organisation anfällig und verwundbar."

Strategische Ausgangsbasis

Unter dem Begriff Governance sind in diesem Fall alle Standards und Prinzipien zusammengefasst, die Verantwortlichkeiten, Berichtslinien und interne Kontrollframeworks definieren. Diese münden meist in Vorgaben für IT-Projekte, Systemeinführungen und -betrieb, Outsourcing und Business Continuity Management.

Die IT-Strategie liefert langfristige Leitlinien für die Entwicklung der IT in der Gesamtbank, ausgehend von der jeweiligen Geschäfts- und Risikostrategie eines Instituts. Wesentliches Element ist ein IT-Masterplan, der definiert, welcher Teil des Technologiestacks welche Geschäftsprozesse abdeckt.

Angesichts der ständig wachsenden regulatorischen Anforderungen und der hohen digitalen Transformationsgeschwindigkeit wäre an sich zu erwarten, dass die Banken selbst hier erhebliche Herausforderungen sehen. Die Studienergebnisse zeichnen ein anderes Bild. Die Banken beurteilen ihre Kompetenz in den jeweiligen Bereichen als gut bis sehr gut. Ohne diese Aussage bewerten zu wollen, sind in jedem Fall drei Trends im Bereich IT-Strategie und IT-Governance erkennbar:

– Ein endgültiger Abschied von den bisherigen Hostsystemen und deren Ablösung durch Microservice-Architekturen mit flexiblen Betriebsmodellen.

– Die Fortsetzung des aktuellen Trends zur Migration von IT-Architekturen in die Cloud. Hier ist eine funktionierende Cloud Governance gefragt.

– Ein deutlich stärkeres Zusammenspiel von Geschäfts- und Servicestrategie. So können beispielsweise Bereiche, die nicht mehr dem Kerngeschäft zugeordnet sind, ohne Weiteres in kürzester Zeit ausgelagert werden.

Planen für den Ernstfall

Wollen Banken aktuell und in Zukunft für die Risiken des digitalen Zeitalters gerüstet sein, müssen sie jetzt die Grundlagen dafür schaffen. Denn das digitale Ökosystem aus Kunden, digitalen Dienstleistern und Partnern birgt bei all seinen Vorteilen auch ganz eigene Gefahren. Risiken werden sich auf die eine oder andere Weise manifestieren. Daher wird die Resilienz einer Bank ausschlaggebend für den Erfolg sein. Denn im digitalen Dschungel ist jede Organisation anfällig und verwundbar. Nur diejenigen, die sich schnell erholen, können die Angelegenheiten meistern.

Detaillierte Informationen zur Risikowahrnehmung deutscher Banken im IKT-Bereich sowie zu weiteren Einzelaspekten dieses weiten Themenfelds können Interessierte in der Studie „Paradigmenwechsel in der Risikostrategie" nachlesen. Diese kann auf der Website der PPI AG kostenlos angefordert werden: https://www.ppi.de/studie-ikt-risiken/