LÜNENDONK

Lünendonk®-Studie 2022

Von Cyber Security zur Cyber Resilience

Wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Eine Studie der Lünendonk & Hossenfelder GmbH
in Zusammenarbeit mit

KPMG

Inhaltsverzeichnis

Vorwort

Mario Zillmann
Partner

Liebe Leserinnen, liebe Leser,

mit zunehmender Digitalisierung nehmen auch die potenziellen Angriffspunkte für Hackerinnen und Hacker zu, weshalb die Absicherung der Unternehmensnetze für fast alle Unternehmen höchste Priorität haben sollte. Die Realität zeigt aber leider oft ein ganz anderes Bild. So ist seit Ausbruch der Corona-Krise nochmals ein deutlicher Anstieg der Cyberkriminalität zu verzeichnen gewesen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verzeichnet in seinem aktuellen Bericht zur „Lage der IT-Sicherheit in Deutschland 2021" demnach auch eine Bedrohungslage zwischen „angespannt und kritisch". Vor allem die Anzahl und Vielfältigkeit cyberkrimineller Erpressungsmethoden sind stark angestiegen. So gab es im Jahr 2021 vier Security-Fälle, die vom BSI mit „Alarmstufe rot", also als besonders schwerwiegend, eingestuft wurden.

Zwei besonders prominente Fälle mit schwerwiegenden Auswirkungen auf die Datensicherheit von Unternehmen – auch auf Finanzdienstleister – waren zunächst im März 2021 eine Schwachstelle im Microsoft-Exchange-Server und dann im Dezember 2021 eine von Hackerinnen und Hackern identifizierte Schwachstelle in Open-Source-Java-Anwendungen, besser bekannt als Log4j.

Gerade für Finanzdienstleister, an die sich diese Lünendonk®-Studie richtet, ist der Schutz vor Cyberangriffen ein zentrales Thema – unter anderem weil sie als Betreiber kritischer Infrastrukturen und Verarbeiter sehr sensibler kundenbezogener Daten an regulatorische und gesetzliche Vorgaben gebunden sind.

Durch die sich forcierende digitale Transformation nimmt jedoch die Bedrohungslage immer mehr zu. So investieren Finanzdienstleister immer stärker in die Digitalisierung ihrer Kundenschnittstellen und in neue, digitale Geschäftsmodelle und nutzen die Innovationskraft von Cloud-Anbietern, um ihre Geschäftsprozesse effizienter und effektiver zu gestalten. Darüber hinaus verändern neue Formen der Zusammenarbeit die Anforderungen an die Cybersicherheit. So verlagern sich die Arbeitsumgebungen immer mehr in private und oft nicht besonders gut geschützte Internetnetzwerke (Digital Workplace).

Cyber Security sollte daher aufgrund dieser Entwicklungen die Aufmerksamkeit der obersten Managementebene haben und nicht nur technologisch, sondern vielmehr als wertschöpfende Aufgabe des gesamten Unternehmens betrachtet werden.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Bei Cyber Security geht es allerdings nicht nur um die Einführung von Security-Software oder die technische Absicherung der Unternehmensnetzwerke; vielmehr erkennen immer mehr Finanzdienstleister, dass in ihren historisch gewachsenen IT-Kernsystemen häufig große Security-Mängel schlummern, beispielsweise aufgrund von veralteten Codes, Konfigurations- oder Programmierfehlern oder fehlenden Sicherheitsfunktionen in der Legacy-IT – die sogenannten technischen Schulden. Daher stehen IT-Modernisierungsprojekte auch stets im Kontext einer Verbesserung der IT-Security-Standards. Die Modernisierung der IT-Landschaften und der (teilweise) Umbau zu Cloud-native-IT-Architekturen können helfen, technische Schulden der Vergangenheit abzubauen und das Security-Niveau zu verbessern.

Tatsächlich gehört das Thema Cyber Security laut der Lünendonk®-Studie 2021 „Der Markt für IT-Dienstleistungen in Deutschland" für 85 Prozent der Finanzdienstleister für das Jahr 2022 zu den wichtigsten Investitionsschwerpunkten – gemeinsam mit Themen wie IT-Modernisierung und Cloud-Transformation. Analog zu den geplanten Investitionen in neue Technologien, in Innovationen und ganz allgemein in die Digitalisierung werden die IT-Budgets für Security im Jahr 2022 folglich auch mehrheitlich steigen.

Die vorliegende Lünendonk®-Studie wirft einen umfassenden Blick auf den Stand der Cyber Resilience im Finanzdienstleistungssektor. Dabei steht die zentrale Frage im Mittelpunkt, vor welchen Herausforderungen Finanzdienstleister stehen und worauf es für den Aufbau einer starken Cyber Resilience wirklich ankommt. Die Studie betrachtet dazu nicht nur einen Ausschnitt, sondern den gesamten Finanzdienstleistungssektor und stellt Unterschiede in den einzelnen Segmenten heraus. 100 Verantwortliche aus Banken, Versicherungsunternehmen und Vermögensverwaltungen wurden telefonisch befragt.

Diese Lünendonk®-Studie ist in Kooperation und fachlicher Zusammenarbeit mit KPMG entstanden. Wir wünschen Ihnen eine interessante und nützliche Lektüre!

Herzliche Grüße

Mario Zillmann

Management Summary

- Neun von zehn der untersuchten Banken, Versicherungen und Vermögensverwaltungen sind laut den Antworten im Rahmen der Studie gut gegen Cyberangriffe geschützt. Dennoch rechnen sieben von zehn Befragten damit, dass ihre Unternehmen in den kommenden zwei Jahren infolge von Phishing-Attacken zum Opfer eines schwerwiegenden Angriffs werden. Auch das Risiko von DDoS-Angriffen (Distributed Denial of Service) schätzen 55 Prozent als hoch ein.

- 97 Prozent der Befragten gehen im Falle eines Cyberangriffs von einem schwerwiegenden Schaden für ihr Unternehmen aus. Vor allem befürchten sie den Abfluss von Kunden- und Unternehmensdaten sowie Image- und Reputationsschäden. Dennoch überprüfen nur sieben von zehn der untersuchten Finanzdienstleister regelmäßig die Wirksamkeit ihrer IT-Security-Strategie. Eine Überprüfung der IT-Systeme auf Schwachstellen findet sogar nur in sechs von zehn der untersuchten Finanzdienstleister statt.

- Trotz zunehmender Digitalisierung der Kundenschnittstellen und dem Trend zu unternehmensübergreifenden Geschäftsmodelle (z. B. Open Banking) enden IT-Security-Strategien in 46 Prozent der befragten Unternehmen an den eigenen Unternehmensgrenzen. Ebenso ist Security by Design, also die Berücksichtigung von Security-Elementen bereits während der Produktentwicklung, bisher nur für 44 Prozent ein fester Bestandteil bei der Entwicklung von digitalen Produkten und Softwarelösungen

- 95 Prozent der untersuchten Finanzdienstleister verfügen bereits über eine Cloud-Strategie beziehungsweise werden bis 2023 eine klare Cloud-Strategie entwickelt und umgesetzt haben. Aus der zunehmenden Cloud-Nutzung ergibt sich aus Sicht von 55 Prozent der Befragten zwar eine Erhöhung des IT-Sicherheitsniveaus, aber auch gleichzeitig die Notwendigkeit, in die IT-Sicherheit und den Aufbau einer ganzheitlichen IT-Sicherheitsarchitektur zu investieren.

92 %

schätzen die eigene Cyber-Security-Resilienz als sehr oder eher hoch ein.

44 %

berücksichtigen Security-Elemente während der Produktentwicklung.

95 %

verfügen über eine Cloud-Strategie bzw. haben diese bis 2023 umgesetzt.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

- Infolge der zunehmenden Bedrohungslage, aber auch aufgrund von schärferen gesetzlichen und regulatorischen Vorschriften, die es mit zunehmender Cloud-Nutzung einzuhalten gilt, steigen die Budgets für IT-Security in den kommenden zwei Jahren teilweise sehr stark an. Die größten Zuwächse finden sich im Bereich der Identifizierung von Schwachstellen: 74 Prozent der befragten Unternehmen werden ihre Budgets für die Früherkennung potenzieller Cyberrisiken und -angriffe um bis zu 10 Prozent erhöhen. Den zweiten großen Block für Budgeterhöhungen bildet die Prävention, also die Antizipation und Abwehr von Cyberangriffen.

- Thematisch setzen die untersuchten Finanzdienstleister in den kommenden Jahren vor allem darauf, Schwachstellen früher zu erkennen, noch bevor Schäden eintreten, und Cyberangriffe besser aufzudecken. Den größten Fokus setzen sie dabei auf das Identity & Access Management, das Security Monitoring und auf Business Continuity & Disaster Recovery.

- Jedes zweite Unternehmen verfügt bereits über ein Security Operations Center (SOC) beziehungsweise befindet sich zum Zeitpunkt der Studienerstellung inmitten des Aufbaus eines solchen. Erfreulicherweise decken die SOCs in fast allen befragten Unternehmen alle relevanten Aufgaben für eine hohe Cyberresilienz ab.

- Aufgrund der Vielzahl von Aufgaben und eines gleichzeitigen Mangels an Inhouse-Expertise setzen die untersuchten Unternehmen auf die Zusammenarbeit mit externen Beratungs- und IT-Dienstleistern. Besonders häufig arbeiten die Unternehmen in den Aufgabenfeldern Cloud Security, Security Monitoring, Security Incident & Event Management und KI-gestützte Cyberabwehr mit solchen Anbietern zusammen.

Um bis zu 10 %

wollen die meisten Finanzdienstleister ihr extern vergebenes Budget für Cyber-Security-Maßnahmen erhöhen.

Fokus der Finanz-dienstleister

Identity & Access Management (IAM), Security Monitoring, Business Continuity & Disaster Recovery.

Jedes 2. Unternehmen

verfügt über ein SOC bzw. befindet sich im Aufbau eines SOCs.

Methodik

Diese Studie basiert auf 100 Gesprächen vor allem mit CIOs, CTOs und CISOs aus dem Finanzdienstleistungssektor. Die Gespräche fanden ausschließlich telefonisch statt. Neben der Perspektive der IT-Verantwortlichen wurden auch für das operative Geschäft verantwortliche Managerinnen und Manager befragt.

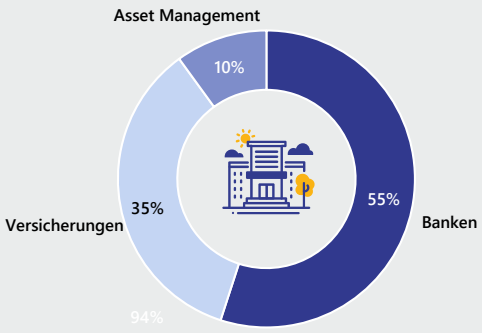
Untersucht wurden Asset-Management-Gesellschaften (Vermögensverwaltungen), Banken und Versicherer. Der Schwerpunkt der Interviews lag allerdings auf Banken und Versicherungen. Für diese beiden Sektoren der Finanzwirtschaft wurde auf eine ausgewogene Verteilung der geführten Interviews geachtet, um die Ergebnisse beider Branchen aussagekräftig einander gegenüberstellen zu können.

100
Gespräche mit Finanzdienstleistern wurden im Zuge der Studie geführt.

Die befragten Unternehmen repräsentieren zu großen Teilen die jeweilige Marktstruktur: So verteilen sich die untersuchten Banken zu 44 Prozent auf Privatbanken und zu 56 Prozent auf die öffentlich-rechtlichen Sparkassen und die Genossenschaftsbanken. Da bei den Sparkassen und Genossenschaftsbanken Themen rund um Digitalisierung, IT-Strategie und Cyber Security im Wesentlichen durch die zentralen IT-Dienstleister abgedeckt werden, wurden diese ebenfalls in dieser Studie berücksichtigt.

METHODIK DER STUDIE (1/3)

Branchenverteilung



Funktionsverteilung

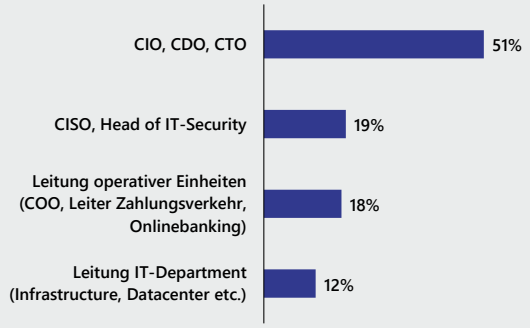


Abb. 1: Branchenverteilung und Funktionsverteilung; Alle Teilnehmer; n = 100

Der Fokus der Studie liegt auf den führenden Finanzdienstleistern in ihren jeweiligen Märkten. So haben 37 Prozent der befragten Banken eine Bilanzsumme von mehr als 50 Milliarden

Euro und 60 Prozent der Versicherungen Beitragseinnahmen von über 2 Milliarden Euro.
70 Prozent der Asset Manager verwalten jeweils Geldanlagen von mehr als 50 Milliarden Euro.

METHODIK DER STUDIE (2/3)

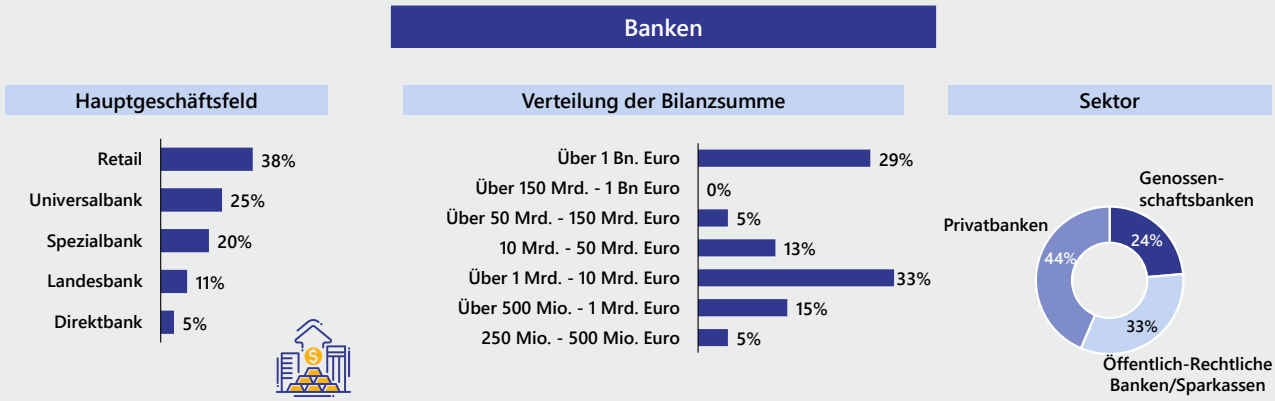


Abb. 2: Frage: Hauptgeschäftsfeld, Verteilung der Bilanzsumme, Sektoren; Banken; n = 55

METHODIK DER STUDIE (3/3)

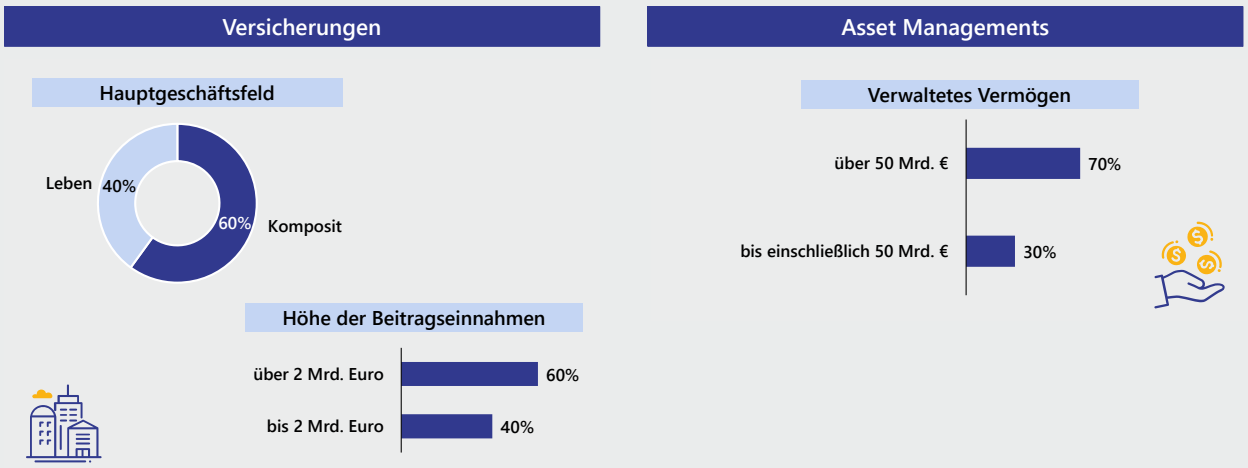


Abb. 3: Frage: Hauptgeschäftsfeld, Höhe der Beitragseinnahmen; Versicherungen; n = 35
Frage: Verwaltetes Vermögen; Asset Management; n = 10

Finanzdienstleister im Fokus von Cyberkriminalität

Cyberkriminalität hat sich mit fortschreitender Digitalisierung zu einer der größten Bedrohungen für Finanzdienstleister entwickelt. Laut dem Allianz Global Corporate & Specialty Report aus dem Jahr 2021 stellen Cybervorfälle das größte Risiko für den Finanzdienstleistungssektor dar – sogar noch vor den gewaltigen Risiken infolge der Corona-Pandemie. Sie sind die häufigste Schadensursache, die Schäden durch IT-Systemausfälle oder Datenschutzverletzungen nehmen stark zu. Auch die Finanzaufsicht (BaFin) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnen regelmäßig vor Cyberrisiken. Eine große Angriffswelle gab es im Dezember 2021 durch eine Sicherheitslücke in der Protokollierungsbibliothek für Java-Anwendungen, besser bekannt unter Log4J. Diese Sicherheitslücke gilt als eine der größten bisher entdeckten Schwachstellen in der Geschichte des Internetzeitalters. Besonders bedrohlich war, dass sich Hackerinnen und Hacker sehr einfach Zugang zu den Servern und Daten verschaffen und massiv Daten abziehen konnten.

Dieses Beispiel zeigt, dass Hackerangriffe Unternehmen mitten in ihre Lebensader treffen und Systeme und komplette Prozesse für eine lange Zeit stilllegen können. Gerade für Banken und Versicherungen als Betreiber kritischer Infrastrukturen ist die IT-Sicherheit ein besonders hohes Gut und Teil der aufsichtsrechtlichen Überprüfung.

Die Cybergefahr kommt von vielen Seiten – von innen wie auch von außen – und die Angriffe verfolgen sehr unterschiedliche Ziele. Während es kriminellen Organisationen darum geht, die Server ihrer Ziele in ihre Gewalt zu bekommen und Lösegeld zu erpressen, wollen Staaten oder Wettbewerber beispielsweise an sensible Informationen gelangen oder ganz gezielt konkurrierenden Unternehmen schaden. Aber auch von den Beschäftigten der Unternehmen selbst gehen Gefahren aus – bewusst oder auch unbewusst.

Im Bereich der kritischen Infrastrukturen (KRITIS), zu denen der Finanzdienstleistungssektor gehört, kamen im Jahr 2020 65 von 419 Meldungen von Cyberangriffen von Finanzdienstleistern. Vor allem DDoS-Angriffe auf IT-Infrastrukturen und Online-Dienste von Banken, Versicherungen und Vermögensverwaltungen waren zu beobachten. Aufgrund der hohen Brisanz von Lösegelderpressungen oder dem Diebstahl sensibler Kundendaten werden Cyberangriffe nicht immer den Behörden gemeldet beziehungsweise gelangen nur selten an die Öffentlichkeit. Die Dunkelziffer ist demnach deutlich höher. In der Corona-Pandemie hat – unter anderem aufgrund von mehr Online-Geschäften und Heimarbeitsplätzen – die Zahl der Cyberangriffe zugenommen und auch die verwendeten Angriffstechnologien erlangen ein immer breiteres Spektrum (Quelle: VMware-Studie 2021 „Modern Bank Heists 4.0“).

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

TOP 5 RISIKEN IM BEREICH FINANZDIENSTLEISTUNGSSEKTOR

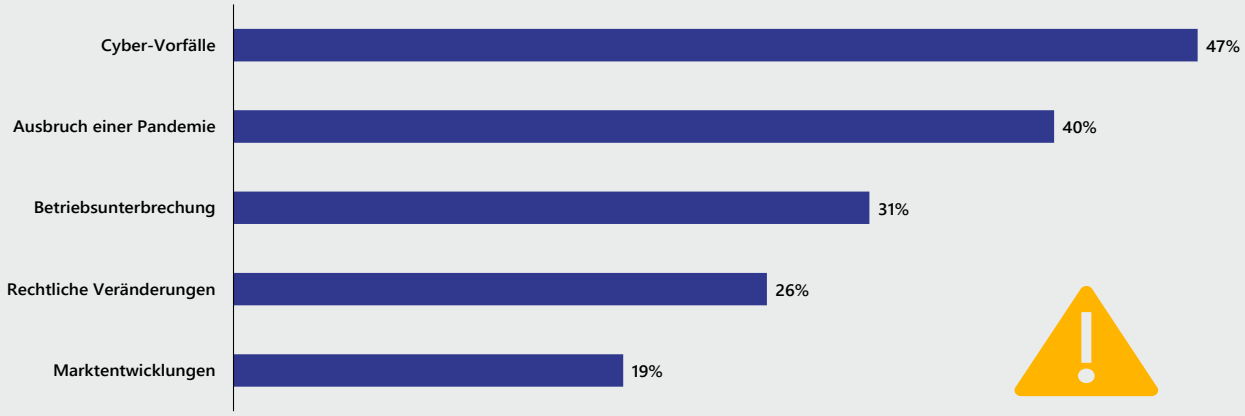


Abb. 4: Die Zahlen geben als Prozentsatz an, wie oft ein Risiko ausgewählt wurde. Die Zahlen addieren sich nicht zu 100 %, da bis zu drei Risiken ausgewählt werden konnten; Häufigkeitsverteilung, n = 931. Quelle: Allianz Global Corporate & Specialty SE

Ein Blick auf einige Beispiele verdeutlicht die Brisanz von Cyberkriminalität im Finanzdienstleistungssektor:

- Jeweils im Januar und im Mai 2020 gab es eine DDoS-Attacke auf die Server des zentralen IT-Dienstleisters der Sparkassen und Landesbanken. Dieser Angriff hatte zur Folge, dass die Webseite der DKB, die zur BayernLB gehört, zeitweise lahmgelegt wurde.

- Bei einem Hackerangriff auf die Haftpflichtkasse mit ca. 2 Millionen betreuten Verträgen im Sommer 2021 wurden ebenfalls die Systeme lahmgelegt und Daten abgezogen.

Laut einer Studie des Digital- und IT-Branchenverbandes Bitkom beginnt der Großteil der Angriffe mit dem sogenannten Social Engineering, worunter die Manipulation von Beschäftigten verstanden wird. Die Angreifenden versuchen mithilfe gefälschter E-Mails oder Telefonanrufen an sensible Daten wie Passwörter zu gelangen. Besonders „beliebt" sind Phishing Mails und CEO Fraud.

Das Problem bei vielen Cyberattacken ist jedoch, dass sie zu spät erkannt werden – nämlich erst dann, wenn der Angriff auf die Server und Rechenzentren erfolgt. Das Ausspähen der Ziele, die Vorbereitungen und das tatsächliche Eindringen in die IT-Systeme finden jedoch oft mehrere Monate vor dem tatsächlichen Angriff statt.

Die Folge: Unternehmen wiegen sich oft in trügerischer Sicherheit, obwohl Cyberkriminelle längst in ihre IT-Systeme vorgedrungen sind und unbemerkt Schadsoftware installieren konnten.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Eine gefühlte Sicherheit entsteht häufig auch dadurch, dass entsprechende organisatorische, technologische und prozessuale Maßnahmen wie 2-Faktor-Identifizierung, Aufbau von Security Operation Centers, die Einführung einer Cloud Security Governance oder Security-Monitoring-Systeme eingeführt sind. In einer digitalisierten und global vernetzten Welt reichen diese Maßnahmen jedoch nicht mehr aus. Die großen Hackerangriffe der jüngeren Vergangenheit zeigen, dass Unternehmen den Angreiferinnen und Angreifern immer einen Schritt voraus seien müssen – sich also viel stärker auf das frühzeitige Identifizieren möglicher Angriffe fokussieren sollten.

Unternehmen fühlen sich gleichzeitig geschützt und bedroht

Gleich zu Beginn der Studie tut sich ein interessantes Spannungsfeld auf: 92 Prozent der befragten C-Level-Verantwortlichen sehen ihre Unternehmen gut gegen Cyberangriffe geschützt. Besonders sicher fühlen sich diejenigen aus dem Banksektor: 55 Prozent sehen sich mit einer sehr hohen Kompetenz in der Lage, Bedrohungen durch Hackerangriffe frühzeitig zu identifizieren und somit eine hohe Cyber Security zu gewährleisten. Unter den ebenfalls befragten Versicherungen sehen dagegen nur 31 Prozent eine sehr hohe Kompetenz in der Früherkennung.

22 Prozent der Banken mit einer Bilanzsumme zwischen 1 und 10 Milliarden Euro – die immerhin 46 Prozent aller befragten Banken ausmachen – haben laut den Studienergebnissen eine geringe Kompetenz in der Cyberabwehr. Vor allem in Bezug auf DDoS-Attacken, Ransomware, Phishing und die seit der Corona-Krise stark zugenommenen Zahl an Heimarbeitsplätzen (Digital Workplace) machen die Befragten Schwachstellen aus. Ebenso zeigt sich in den Ergebnissen, dass die untersuchten Genossenschaftsbanken häufiger als der Durchschnitt Schwächen in der Einschätzung der Bedrohungslage aufweisen: So sehen sich 23 Prozent der befragten Genossenschaftsbanken derzeit nicht gut aufgestellt, um Cyberbedrohungen frühzeitig zu erkennen – was unter anderem eine unmittelbare Folge der DDoS-Attacke auf die Server des zentralen IT-Dienstleisters der Volks- und Raiffeisenbanken im Sommer 2021 sein kann. So hat dieser Angriff der Branche aufgezeigt, wie stark die Bedrohung trotz getroffener Sicherheitsmaßnahmen ist und wie schwerwiegend die Folgen sein können.

92 %
der Unternehmen sehen sich gut gegen Cyberangriffe geschützt.

Auch bei den untersuchten Versicherungen sieht ein Teil der Befragten (14 %) eine geringe Cyber-Security-Kompetenz. Den Gesellschaften mit mehr als 2 Milliarden Euro an Beitragseinnahmen bescheinigen jedoch 71 Prozent der Befragten hier eine eher hohe Kompetenz. Hier sind es DDoS-Attacken und Phishing, bei denen sie ein geringes Schutzniveau erkennen.

DIE GEFAHR KOMMT AUCH VON INNEN

Obwohl sich die meisten der untersuchten Finanzdienstleister als gut gegen Hackerangriffe und Datendiebstahl geschützt sehen, rechnet gleichzeitig aber ein ebenso hoher Teil der Befragten damit, dass ihre Unternehmen Opfer schwerwiegender Cyberangriffe werden können, die wiederum schwere Folgen nach sich ziehen.

Eine besonders große Gefahr geht laut den Befragten von Ransomware/Phishing-E-Mails (68 %) und der Nutzung unautorisierter Devices (66 %) aus. Der Faktor Mensch

FINANZDIENSTLEISTER FÜHLEN SICH IN BEZUG AUF CYBERBEDROHUNGEN SICHER

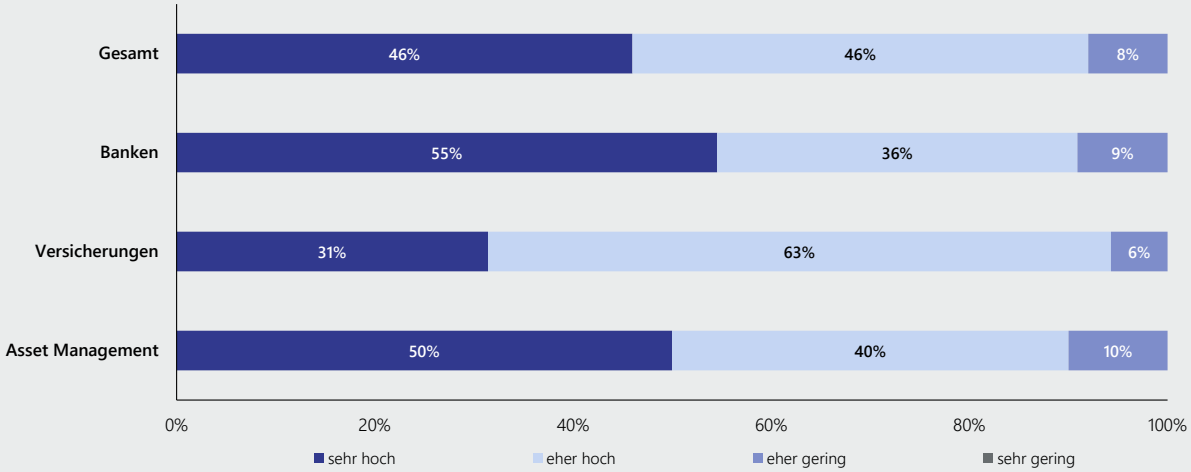


Abb. 5: Frage: Wie schätzen Sie die Fähigkeit Ihres Unternehmens ein, Bedrohungen durch Hackerangriffe zu identifizieren und somit eine Früherkennung von Cyberangriffen zu gewährleisten?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 55; Versicherungen: n = 35; Asset Managements: n = 10

ist demnach aus Sicht der befragten IT- und Security-Verantwortlichen das größte Sicherheitsrisiko. Tatsächlich erfolgen laut Microsoft Security Report 2021 über zwei Drittel der Cyberangriffe durch Social Engineering, also den Versand täuschend echt anmutender E-Mails (Phishing-Mails) an Mitarbeitende, um diese dazu zu bringen, unabsichtlich Schadsoftware zu nutzen. Die Angriffsmethoden sind mittlerweile sehr ausgereift und reichen von Phishing Mails bis hin zum CEO Fraud.

55 Prozent der Befragten befürchten ferner, dass DDoS-Attacken schwerwiegende Folgen haben können. Tatsächlich zielen diese Angriffe darauf ab, die Geschäftsaktivitäten der Opfer lahmzulegen und sie dadurch massiv zu schädigen. DDoS-Angriffe kommen zwar im Vergleich zu Phishing-Angriffen seltener vor, dennoch ist der durch sie verursachte Schaden deutlich größer, wie der DDoS-Angriff auf den IT-Dienstleister Fiducia & GAD (heute: Atruvia) im Sommer 2021 gezeigt hat.

Eine unzureichende Absicherung und Kontrolle der Unternehmensnetzwerke sehen nur 28 Prozent der Befragten als mögliche Ursache von Cyberangriffen. Dagegen halten es immerhin 49 Prozent für wahrscheinlich, dass sich aufgrund von technischen Schwachstellen in den IT-Systemen Sicherheitslücken auftun, die genutzt werden, um unbemerkt an die Server und Daten vorzudringen. Gerade dieser Aspekt ist in den letzten Jahren mit zunehmender Digitalisierung der Kundenschnittstellen und der damit verbundenen Anbindung von digitalen Frontend-Lösungen zu einem großen Problem für Finanzdienstleister geworden. So finden sich besonders in diesem Sektor sehr viele historisch gewachsene IT-Legacy-Systeme, die nicht selten neben veralteten Codes vor allem Mängel im Design und

in der Konfiguration aufweisen und damit über die Anbindung an die modernen Frontend-Lösungen ein attraktives Angriffsziel darstellen.

In den Ergebnissen spiegelt sich auch das bekannte Problem wider, dass viele Unternehmen IT-Security und auch die IT-Risikobewertung noch sehr stark aus einer technischen Perspektive heraus betrachten, indem sie sich überwiegend auf die technologische Absicherung ihrer eigenen Netzwerke konzentrieren. Dagegen ist für den Schutz vor Malware wie beispielsweise Ransomware eine hohe Kompetenz in der Früherkennung (Identification, Detection) notwendig – was neben technologischen Aspekten vor allem die Sensibilisierung der Beschäftigten, organisatorische Maßnahmen wie den Aufbau eines wirkungsvollen SOC oder regelmäßige Penetration Tests sowie Schulungen aller Beschäftigten einschließlich der Führungskräfte in Bezug auf Phishing Mails und CEO Fraud erfordert. Wie an späterer Stelle in dieser Studie jedoch noch deutlich wird, finden entsprechende Überprüfungen der IT-Systeme auf Security-Lücken bei einigen der untersuchten Finanzdienstleister noch gar nicht statt.

BESONDERS GEFÜRCHTET: ABFLUSS VON KUNDEN- UND UNTERNEHMENSDATEN

Nahezu alle untersuchten Banken, Versicherungen und Vermögensverwaltungen (97 %) rechnen im Falle eines Cyberangriffs mit schwerwiegenden Schäden für ihre Unternehmen infolge einer massiven Kompromittierung der IT-Infrastruktur.

Besonders große Sorge haben die Befragten vor einem Abfluss von Kundendaten (73 %) und kritischen Unternehmensinformationen (67 %). Insbesondere bei den sensiblen Kundendaten stehen Finanzdienstleister unter besonderer Beobachtung der Finanzaufsicht, da sie besonderen Geheimhaltungsbedingungen unterliegen und somit als besonders schützenswert gelten, aber auch unter der EU-DSGVO-Regelung stehen. So gelten beispielsweise unter anderem aufgrund der bank-, versicherungs- und kapitalverwaltungsrechtlichen Anforderungen an die IT (BAIT, VAIT und KAIT) konkrete Vorgaben für das Identity and Access Management zum Schutz vor Datenzugriff durch unbefugte Beschäftigte, aber auch für die Absicherung der Datenbanken gegenüber externen Angriffen. Immer mehr Finanzdienstleister stellen den Zugriff zu ihren sensiblen Kundenportalen durch die 2-Faktor-Authentifizierung sicher -was nebenbei auch die Akzeptanz der Kundinnen und Kunden für digitale Kundenschnittstellen deutlich erhöht.

Als unmittelbare Folge eines möglichen Datendiebstahls befürchten 59 Prozent der Befragten hohe Image- und Reputationsschäden für ihre Institute. Um finanzielle Risiken macht sich dagegen nur ein Drittel von ihnen Sorge. Während 33 Prozent der Befragten mit der Wahrscheinlichkeit hoher Lösegeldforderungen rechnen, erwarten 31 Prozent Umsatzeinbußen, beispielsweise durch das Abschalten der Online-Kanäle oder der

EIN GROSSER TEIL DER STUDIENTEILNEHMER RECHNET MIT CYBERATTACKEN AUF IHR UNTERNEHMEN

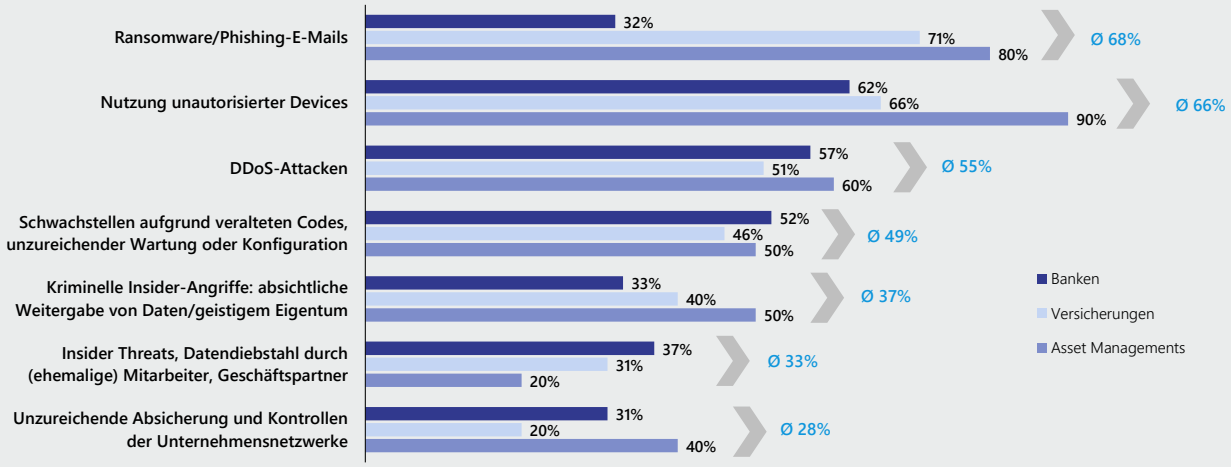


Abb. 6: Frage: Für wie wahrscheinlich halten Sie es, dass Ihr Unternehmen in den kommenden zwei Jahren aufgrund der folgenden Ereignisse einem schwerwiegenden Angriff zum Opfer fällt, durch....?; Alle Teilnehmer; Häufigkeitsverteilung; Werte beziehen sich auf die Antworten „sehr wahrscheinlich" und „eher wahrscheinlich"; Banken: n = 53; Versicherungen: n = 35; Asset Managements: n = 10

IT-Kernsysteme durch Hackerinnen und Hacker, sodass zeitweise keine Geschäftsaktivitäten mehr möglich sind. Im Branchenvergleich zeigt sich, dass die befragten Versicherungen deutlich häufiger den Abfluss kritischer Unternehmensdaten befürchten (77 %) als Banken (54 %). Dagegen halten es signifikant mehr Banken (41 %) als Versicherungen (26 %) für wahrscheinlich, dass nach einem Cyberangriff hohe Lösegeldforderungen auf sie zukommen. Diese überdurchschnittlich häufig geäußerten Befürchtungen seitens der befragten Banken können mit deren hoher Systemrelevanz beispielsweise für den Zahlungsverkehr zusammenhängen.

FINANZDIENSTLEISTER FÜRCHTEN UNTER ANDEREM DEN ABFLUSS VON KUNDENDATEN UND REPUTATIONSSCHÄDEN

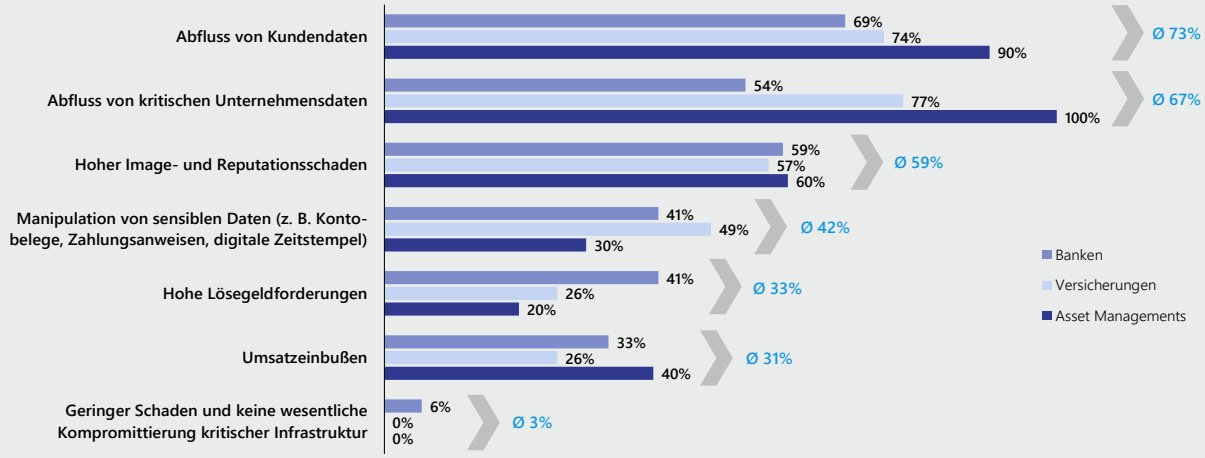


Abb. 7: Frage: Welche konkreten Folgen hätte aus Ihrer Sicht ein Cyber-Angriff für Ihr Unternehmen?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 54; Versicherungen: n = 35; Asset Managements: n = 10

Mehr Innovation durch Cloud-Nutzung – aber auch ein neues Bedrohungspotenzial

Angesichts des immer schnelleren Wandels von Markt- und Kundenanforderungen ist eine moderne, schnittstellenoffene und leistungsfähige IT-Infrastruktur inzwischen essenziell für die Wettbewerbsfähigkeit von Finanzdienstleistern. Gleichzeitig führt die Umstellung auf digitale Arbeitsplätze seit der Corona-Krise zu einem starken Anstieg der Nutzung von Public-Cloud-Diensten wie Microsoft 365 und anderen Collaboration Tools und ebenfalls zu einem Anstieg von Remote-Zugriffen auf die Firmennetzwerke. Aber auch infolge der Digitalisierung der Kundenschnittstellen und der Einführung von immer mehr digitalen Geschäftsmodellen werden nun deutlich mehr Cloud-Lösungen eingesetzt, um die hohen Anforderungen an Skalierbarkeit, Reaktionszeiten und Interoperabilität durch die IT zu erfüllen.

Aus all diesen Gründen ist die Nutzung von Cloud-Technologien für die IT-Modernisierung und die Ausrichtung der IT auf veränderte Business-Anforderungen von zentraler Bedeutung. Auch die Aufsichtsbehörden stehen der Cloud-Nutzung aufgeschlossener gegenüber und haben mit den rechtlichen Anforderungen an die IT (BAIT, VAIT und KAIT) für mehr Klarheit in der Nutzung von Cloud-Services gesorgt.

41 %
der Finanzdienstleister beziehen einen Großteil der Anwendungen aus der Public Cloud.

EXKURS: CYBER SECURITY IST ZENTRALES DIGITALISIERUNGSTHEMA

Die Lünendonk®-Studie 2021 „Der Markt für IT-Beratung und IT-Service in Deutschland“ zeigt, dass für 59 Prozent der darin befragten Banken und Versicherungen 2022–2023 die Cloud-Transformation, also der Umbau von Teilen der IT-Landschaft zu einer Cloud-native-IT-Architektur, eines der wichtigsten Investitionsthemen ist. Mit Blick auf die kommenden Jahre erwarten laut dieser Studie 37 Prozent der befragten CIOs aus der Finanzbranche, dass der überwiegende Teil der IT-Services aus einer Cloud-Infrastruktur bezogen wird, und sogar jede zweite Bank oder Versicherung wird neue Softwarelösungen auf der Grundlage einer Cloud-native-Architektur entwickeln. 41 Prozent der untersuchten Finanzdienstleister beziehen einen großen Teil ihrer Anwendungen bereits aus der Public Cloud, zwei Drittel setzen sehr stark auf hybride Cloud-Modelle. Aber noch deutlicher spiegelt den Cloud-Trend im Finanzdienstleistungssektor die Tatsache wider, dass zwei Drittel (66 %) der befragten Banken und Versicherer in Zukunft Software überwiegend als Software as a Service (SaaS) bereitstellen werden. Da SaaS-Modelle darauf basieren, dass die zugehörige IT-Infrastruktur durch die Softwareanbieter betrieben wird, handelt es sich bei SaaS in der Regel um Public-Cloud-Services.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

IT-INVESTITIONSSCHWERPUNKTE FÜR 2022 UND 2023

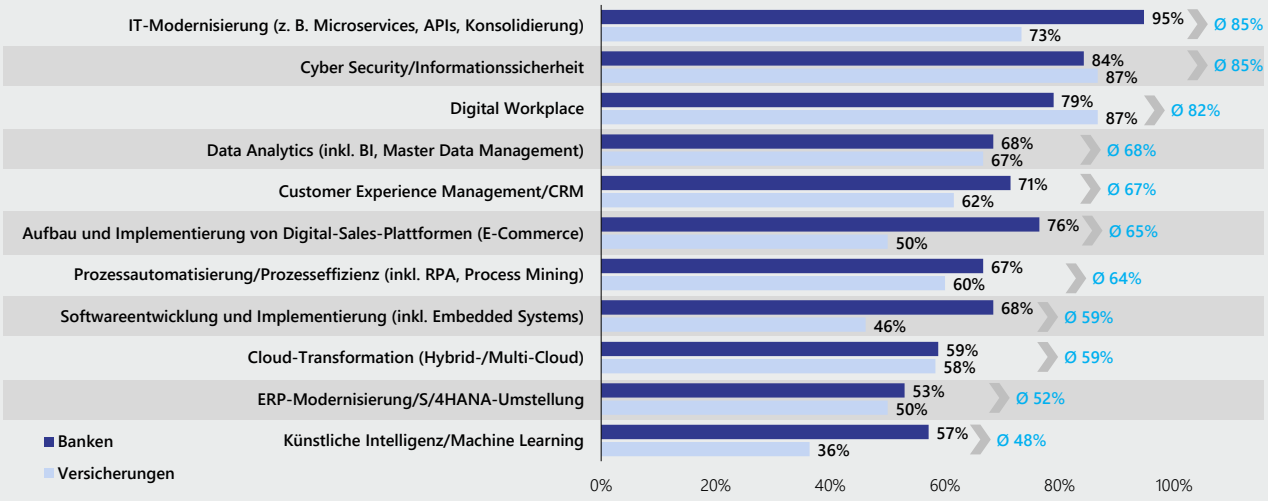


Abb. 8: Frage: In welche Themen investiert Ihr Unternehmen in den kommenden zwei Jahren? Mittelwerte; Skala von -2 = „gar nicht" bis +2 = „sehr stark"; Werte beziehen sich auf die Antworten +2 (sehr stark) und +1 (eher stark); n = 14-19 (Banken); n = 11-15 (Versicherungen), Quelle: Lünendonk-Studie 2021: Der Markt für IT-Beratung und IT-Service in Deutschland

ZWEI VON DREI FINANZDIENSTLEISTERN HABEN EINE CLOUD-STRATEGIE

Trotz der hohen regulatorischen Anforderungen, die die Aufsichtsbehörden an die Cloud-Nutzung stellen, verfolgen 29 Prozent der untersuchten Unternehmen eine Cloud-first-Strategie, prüfen also bei jedem Projekt, ob es sich mithilfe von Cloud-Services umsetzen lässt. Jedoch ist der Anteil der Versicherer, die eine solche Strategie verfolgen, mit 41 Prozent deutlich höher als im Bankensektor (25 %). Das hängt damit zusammen, dass nur jede zehnte befragte Sparkasse und Genossenschaftsbank angab, eine Cloud-first-Strategie zu verfolgen. Da sich aus ganz unterschiedlichen Gründen nicht alle traditionellen IT-Kernsysteme in die Cloud migrieren (Lift & Shift) oder zu Cloud-native-Services umbauen lassen, zeigt sich in der Praxis meist eine hybride IT-Architektur aus den traditionellen IT-Kernsystemen und Cloud-Anwendungen. Eine sogenannte Cloud-too-Strategie, also die Verlagerung einzelner Anwendungen in die Cloud beziehungsweise den Bezug einzelner Anwendungen als Software as a Service, nutzen vor allem Banken (42 %) und Vermögensverwaltungen (50 %).

DER TREND GEHT ZUR PUBLIC CLOUD – ABER GENAU DORT SIND DIE DATEN NOCH NICHT GUT GENUG GESCHÜTZT

Diejenigen Finanzdienstleister, die bereits über eine Cloud-Strategie verfügen, wurden gefragt, für wie sicher sie ihre Daten in den unterschiedlichen Cloud-Varianten halten. Am sichersten ist aus Sicht der Befragten – wenig überraschend – die Private Cloud. 65 Prozent sehen in der Private Cloud ein sehr hohes Schutzniveau vor Cyberangriffen. Nur 11 Prozent erachten ihre Daten in der Private Cloud als nicht sicher.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Ein hohes Schutzniveau ihrer Daten verorten die befragten IT-Entscheiderinnen und -Entscheider auch in der Hybrid Cloud. Allerdings ist der Anteil derer, für die die Hybrid Cloud ein „sehr hohes Schutzniveau" bietet, mit 42 Prozent geringer als bei der Private Cloud. Dennoch bieten hybride Umgebungen aus Sicht von 48 Prozent der Befragten noch ein „eher hohes Schutzniveau". Die Analyse nach Sektoren zeigt, dass Banken das Schutzniveau in der Private Cloud und in Hybrid-Cloud-Umgebungen deutlich häufiger als hoch einschätzen als die befragten Versicherungen (siehe Abbildung 10). Dagegen sind die untersuchten Versicherungen der Public Cloud gegenüber etwas aufgeschlossener. Während 75 Prozent der Versicherungen ihre Daten in der Public Cloud als sicher erachten, liegt der Durchschnitt über alle befragten Finanzdienstleister mit 69 Prozent deutlich darunter. In Zukunft erwartet Lünendonk eine noch stärkere Nutzung von Public-Cloud-Diensten – unter anderem weil der Aufbau von Private-Cloud-Umgebungen insbesondere für kleinere und mittlere Institute zu hohe Kosten verursacht, ebenso wie das Management hybrider IT-Landschaften einen hohen Ressourcenaufwand in der IT-Organisation erfordert.

NAHEZU ALLE FINANZDIENSTLEISTER VERFOLGEN EINE CLOUD-STRATEGIE

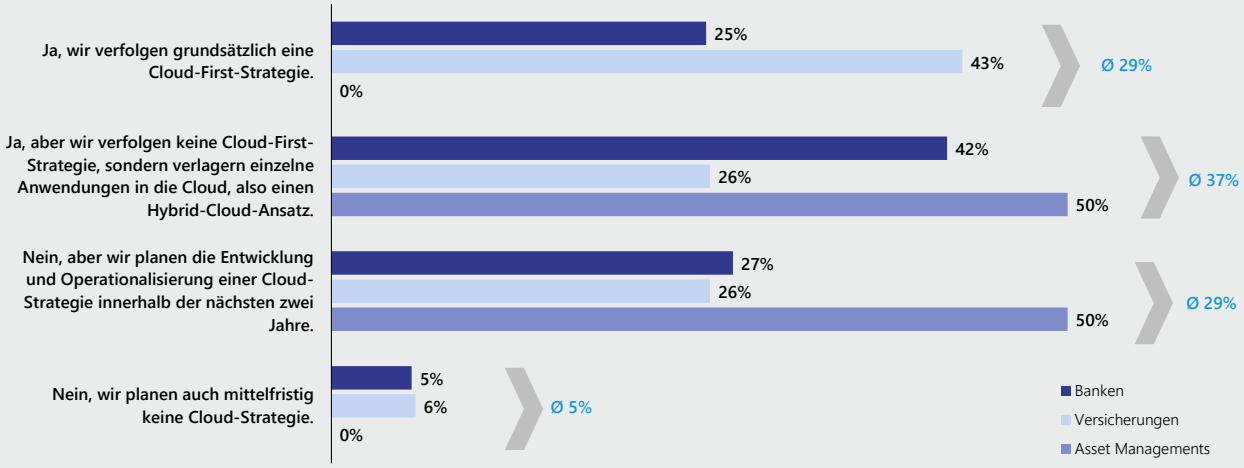


Abb. 9: Frage: Hat Ihr Unternehmen eine Cloud-Strategie?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 55; Versicherungen: n = 35; Asset Managements: n = 10

UNTERNEHMEN MIT CLOUD-FIRST-STRATEGIE PRÄFERIEREN DIE PUBLIC CLOUD

Von denjenigen Finanzdienstleistern, die eine Cloud-first-Strategie verfolgen, schätzen dagegen 86 Prozent die Public Cloud als sicher ein, was aus Sicht von Lünendonk vor allem damit zusammenhängt, dass diese Unternehmen bereits entsprechende Governance- und Risk-Konzepte für die Public-Cloud-Nutzung umsetzen – beispielsweise eine Multi-Cloud-Provider-Steuerung oder sie verfügen über ein wirkungsvolles Security Operation Center.

86 %
der Finanzdienstleister schätzen die Public Cloud als sicher ein.

IN DER PUBLIC CLOUD FÜHLEN SICH DIE BEFRAGTEN FINANZDIENSTLEISTER ZWAR NOCH NICHT AM SICHERSTEN – ABER DENNOCH NIMMT DAS SECURITY-NIVEAU ZU

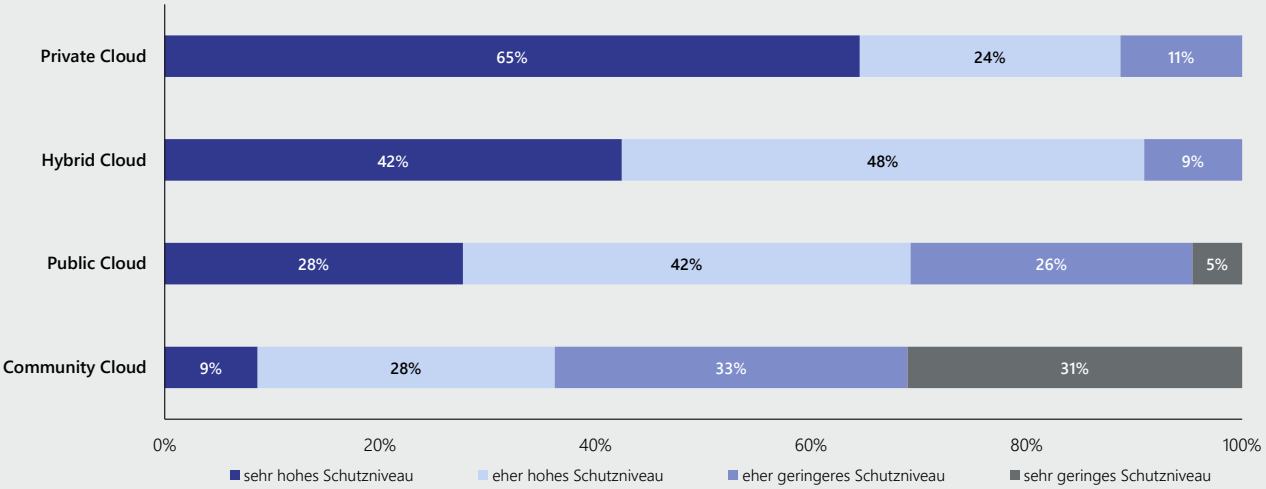


Abb. 10: Frage: Hat Ihr Unternehmen eine Cloud-Strategie?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 55; Versicherungen: n = 35; Asset Managements: n = 10

Aber auch die Größe der Unternehmen scheint einen Einfluss auf die Wahrnehmung der unterschiedlichen Cloud-Modelle zu haben: So betrachten 86 Prozent der Befragten aus Versicherungen mit mehr als 2 Milliarden Euro Beitragseinnahmen die Public Cloud als sicheren Ort für ihre Daten. Im Banksektor stufen dagegen alle untersuchten Institute mit

BRANCHENVERGLEICH: ALLE DREI BRANCHEN SEHEN IN DER PRIVATE CLOUD DAS HÖCHSTE SICHERHEITSNIVEAU

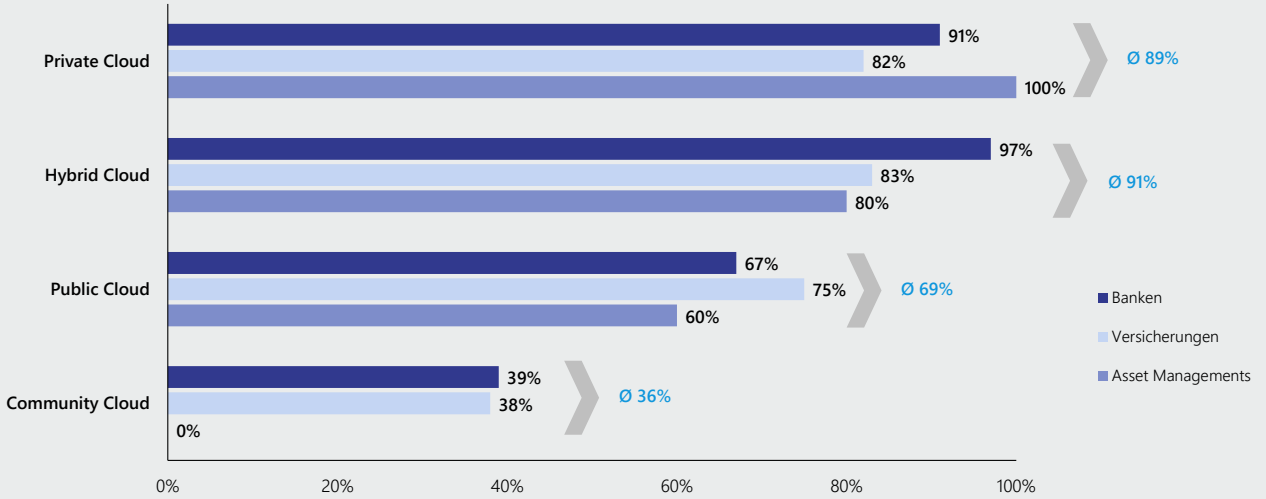


Abb. 11: Frage: Wie schätzen Sie den derzeitigen Schutz Ihrer Daten in den einzelnen Cloud-Deployments ein?; Alle Teilnehmer; Häufigkeitsverteilung; Werte beziehen sich auf die Antworten „sehr hohes Schutzniveau“ und „eher hohes Schutzniveau““; Banken: n = 33; Versicherungen: n = 21; Asset Managements: n = 4

mehr als 50 Milliarden Bilanzsumme die Private Cloud wie auch Hybridumgebungen als sichere Cloud-Modelle ein. Diese Einschätzung liegt zum Teil darin begründet, dass Banken in dieser Größe über ausreichend Ressourcen und Kapital verfügen, um Private Clouds und hybride Bereitstellungsmodelle aufzubauen und vor allen nach den Anforderungen der Regulierungsbehörden zu managen – was für kleinere Institute oft aus rein wirtschaftlichen Gründen eher schwer ist. Darüber hinaus sind besonders in den großen Universalbanken Kernbanksystemlandschaften anzutreffen, die mehr als ein Jahrzehnt alt sind und eine hohe technologische Komplexität aufweisen, sodass man sie nicht ohne massive Investitionen zu einer Cloud-Architektur umbauen kann. Solche Systemlandschaften werden allein schon aus Kostengründen in Private Clouds migriert (Lift & Shift).

ZAHL DER CLOUD-PROVIDER, MIT DENEN EIN WORKLOAD BETRIEBEN WIRD, NIMMT ZU

Dem Innovationsdruck, den Finanzdienstleister in den kommenden Jahren zu bewältigen haben, werden sie nur durch konsequente Digitalisierung und Einsatz der Cloud standhalten können. Unter anderem deshalb beziehen Banken, Versicherungen und Vermögensverwaltungen nun deutlich stärker Software aus dem Internet (Software as a Service) oder entwickeln und betreiben digitale Produkte in Cloud-native-Umgebungen (Platform as a Service).
Um einen möglichst effizienten IT-Betrieb zu gewährleisten, aber auch um Exit-Strategien bei einem Providerwechsel umzusetzen, setzen immer mehr Finanzdienstleister auf Multi-Cloud-Betreibermodelle und lassen ihre Prozesse in den Clouds mehrerer Anbieter laufen. Durch die daraus resultierende steigende Zahl der Cloud- und Managed-Service-Provider, von denen Cloud-Services bezogen werden, erhöht sich auch das Risiko, durch mögliche

TROTZ HOHER CLOUD-NUTZUNG UND VORGABEN DURCH DIE AUFSICHT: MULTI-PROVIDER-STRATEGIE IST IM FINANZDIENSTLEISTUNGSSEKTOR NOCH NICHT ÜBERALL IMPLEMENTIERT

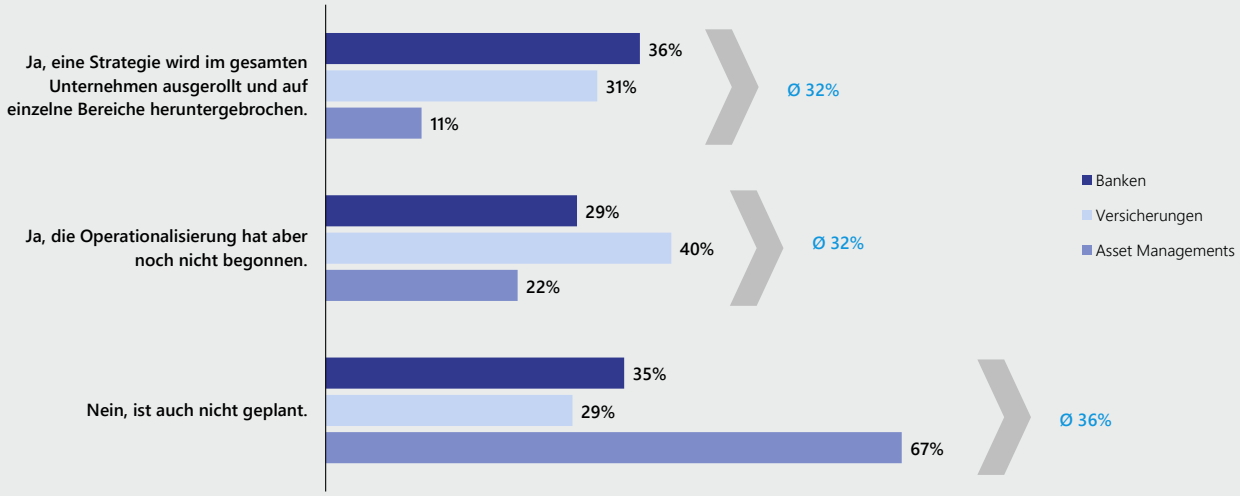


Abb. 12: Frage: Verfolgt Ihr Unternehmen beim Bezug von Cloud Services eine Multi-Provider-Strategie?; Alle Teilnehmer; Häufigkeitsverteilung; n = 99

Schwachstellen in deren IT-Landschaften zum Ziel von Cyberattacken zu werden. Zwei von drei der untersuchten Finanzdienstleister (64 %) verfolgen beim Bezug von Cloud-Services bereits eine Multi-Provider-Strategie. 36 Prozent setzen dagegen auf einen zentralen Cloud-Provider oder Managed-Service-Dienstleister – zumindest innerhalb der einzelnen Leistungsbereiche wie IT-Infrastruktur, SAP-Betrieb oder im Datacenter.

Multi-Provider-Strategien werden vor allem von den befragten Finanzdienstleistern genutzt, um die Business Continuity sicherzustellen, sollte ein Cloud-Provider ausfallen oder einen bestimmten Service einstellen. Diesen Aspekt sehen 70 Prozent der Befragten als einen wesentlichen Grund, warum ihre Unternehmen auf Multi-Provider-Strategien setzen, und er ist gleichzeitig auch eine zentrale regulatorische Vorgabe für besonders kritische Services. Ein weiterer Grund sind für 61 Prozent der Befragten die Kosteneinspareffekte, beispielsweise weil Workloads effizienter verteilt und Skalierungsvorteile genutzt werden können. Nicht selten kommt es auch vor, dass bestimmte Funktionalitäten durch einen Cloud-Provider besonders gut oder überhaupt abgedeckt werden. So sehen 55 Prozent der Befragten diesen Aspekt ebenfalls als einen wichtigen Grund für Multi-Provider-Strategien.

CLOUD-NUTZUNG ERHÖHT DAS SECURITY-NIVEAU – FÜHRT ABER AUCH ZU HÖHEREN INVESTITIONEN IN DIE IT-SICHERHEIT

Welche Folgen hat aber nun der stärkere Bezug von Cloud-Services – zumindest aus Sicht derjenigen Unternehmen, die bereits über eine Cloud-Strategie verfügen?

Neben einem Umbau der IT-Architektur zur Nutzung hybrider und multipler Cloud-Services (73 %) sehen 56 Prozent der Befragten die Notwendigkeit, mehr in die IT-Sicherheit zu investieren.

Nicht nur neue Möglichkeiten der Kundenzentrierung, mehr Prozesseffizienz und geringere Kosten sind wichtige Argumente für die Verlagerung von IT-Infrastruktur und Anwendungen in die Cloud, sondern auch immer häufiger das hohe Sicherheitsniveau, das Cloud-Provider bieten.

So sind 55 Prozent der Befragten der Meinung, dass ihre Daten in der Cloud grundsätzlich besser geschützt sind als im traditionellen On-Premise-Rechenzentrumsbetrieb. Diesen Eindruck bestätigen auch zwei Drittel der Befragten aus dem Sparkassensektor. Beispielsweise verfügen viele der Cloud-Provider über eigene SOCs, um ihre Cloud-Landschaften in Echtzeit überwachen zu können. Dazu nutzen sie unter anderem in größerem Umfang Künstliche Intelligenz wie Machine Learning, um beispielsweise Datenströme in Echtzeit analysieren und Netzwerkanomalien im Datenstrom erkennen zu können, bevor ein Sicherheitsfall überhaupt eintritt. Darüber hinaus investieren die Cloud-Provider oder die Managed-Cloud-Service-Provider massive Summen in den Schutz ihrer Cloud-

Infrastrukturen. Folglich sind Daten in den hochmodernen Rechenzentren grundsätzlich besser vor Cyberangriffen geschützt als in den klassischen On-Premise-Rechenzentren.

Trotz der höheren wahrgenommenen Sicherheit in der Cloud sehen 56 Prozent der befragten IT-Entscheiderinnen und Entscheider dennoch die Notwendigkeit, mehr in die IT-Sicherheit zu investieren, während 49 Prozent den Aufbau einer ganzheitlichen Security-Architektur für notwendig erachten. In diesen Einschätzungen spiegeln sich die gestiegenen regulatorischen Anforderungen durch die neuen Freiräume in der Cloud-Nutzung unmittelbar wider.

Etwas überraschend – auch vor dem Hintergrund der schwerwiegenden Cyberattacke auf das Rechenzentrum des zentralen IT-Dienstleisters der Genossenschaftsbanken – sehen dagegen nur 38 Prozent der Befragten aus dem Genossenschaftssektor die Notwendigkeit, die Investitionen in die IT-Sicherheit infolge von mehr Cloud-Nutzung zu erhöhen. Und nur 44 Prozent sehen Bedarf, eine ganzheitliche Security-Architektur aufzubauen, um besser gegen Cyberangriffe geschützt und vorbereitet zu sein. Diese Sichtweise aus dem Genossenschaftsbankensektor überrascht etwas vor dem Hintergrund der Bedrohungslage durch Cyberkriminalität im Bankensektor und der zunehmenden Digitalisierung der Branche.

DIE CLOUD ERHÖHT AUS SICHT JEDES ZWEITEN BEFRAGTEN FINANZDIENSTLEISTERS DAS SECURITY-NIVEAU

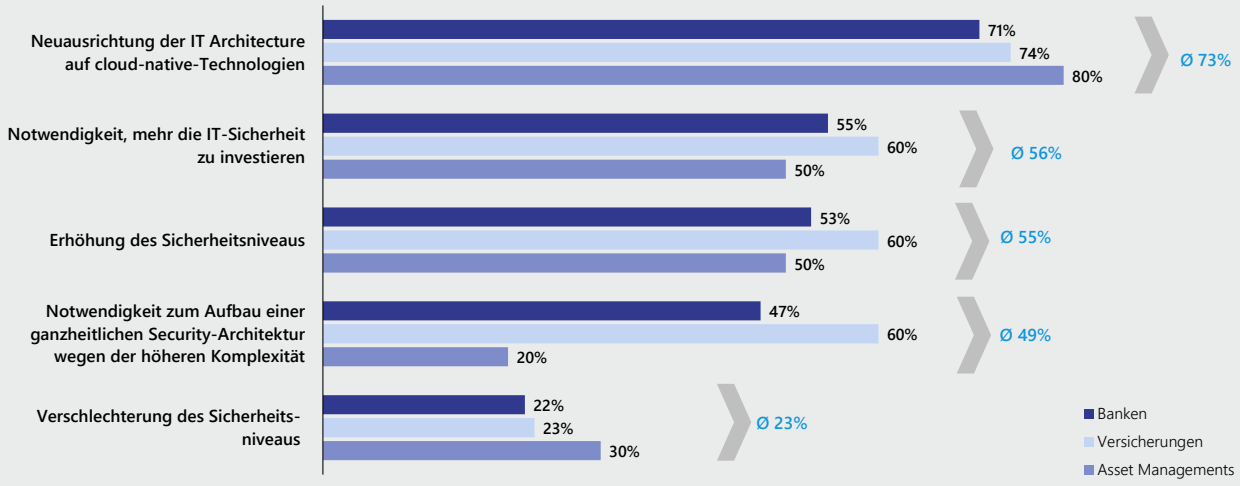


Abb. 13: Frage: Welche Folgen hat Ihrer Ansicht nach der stärkere Bezug von Cloud-Services für die IT-Sicherheit?; Alle Teilnehmer; Banken: n = 55; Versicherungen: n = 35; Asset Managements: n = 10

Ausrichtung der Cyber-Security-Strategie auf eine veränderte digitale Welt

Der Schutz von Cyberangriffen ist fester Bestandteil der digitalen Transformation, gilt als wertschöpfend, stellt aber auch einen großen Kostenfaktor dar. So lässt sich die Sichtweise auf Cyber Security in den untersuchten Finanzdienstleistern zusammenfassen. Demnach gilt Cyber Security in 87 Prozent der Unternehmen zwar als Wertschöpfungsfaktor und ist somit vermutlich auch als wichtiger Faktor in die Digitalisierungsstrategien eingebettet; dennoch nehmen 79 Prozent der Unternehmen Cyber Security weiterhin als Kostenfaktor wahr.

In einem solchen Spannungsfeld zwischen Wertschöpfungs- und Kostenfaktor bei gleichzeitigem Kostendruck im Finanzdienstleistungssektor kann es schnell passieren, dass Unternehmen sich eher auf die von der Finanzaufsicht geforderten Mindestanforderungen konzentrieren, um ihre Netzwerke und IT-Infrastrukturen technologisch abzusichern. Notwendige organisatorische und kulturelle Transformationsmaßnahmen sowie Investitionen in neue digitale Technologien im Sinne von Cyber-Früherkennungen laufen somit Gefahr, nicht hoch genug priorisiert zu werden, weil der Business-Nutzen nicht erkannt wird.

79 %
der Unternehmen sehen Cyber Security als Kostenfaktor.

SECURITY-KONZEPTE MACHEN NOCH OFT AN DEN EIGENEN UNTERNEHMENSGRENZEN HALT

Tatsächlich richten sich IT-Security-Strategien bei 46 Prozent der befragten Finanzdienstleister nach aktuellem Stand noch ausschließlich auf die eigenen Unternehmensnetzwerke. Vor allem bei den untersuchten Sparkassen und Genossenschaftsbanken enden IT-Security-Strategien noch vergleichsweise oft an den eigenen Unternehmensgrenzen. Der hohe Anteil von Banken, bei denen sich IT-Security-Strategien ausschließlich auf die eigenen Unternehmensnetzwerke beziehen, kommt vor dem Hintergrund der Zahlungsdiensterichtlinie (Payment Service Directive 2, kurz: PSD2) etwas überraschend. Banken sind durch die PSD2 verpflichtet, ihre Schnittstellen (APIs) gegenüber Drittanbietern zu öffnen (Open Banking). Somit können beispielsweise die Kundinnen und Kunden einer traditionellen Bank auf digitale Angebote von Drittanbietern zugreifen. Beispiele sind die Erstellung von Anlageplänen auf der Basis der Kontoinformationen durch Robo Advisors wie Scalable oder die mobile Bezahlfunktion Apple Pay. Durch die PSD2 werden Banken nun getrieben, ihre traditionellen Silostrukturen und die funktionale Trennung der Bankorganisation aufzulösen und sich als ein wie auch immer gearteter Teil digitaler Plattformen und Ökosysteme weiterzuentwickeln.
Dazu gehören aber eben auch IT-Security-Konzepte, die auf die Plattformökonomie ausgerichtet sind und die Zunahme an Angriffspunkten berücksichtigen.

Immerhin 58 Prozent der Unternehmen stellen dagegen bereits ihr gesamtes Ökosystem in den Fokus der Cyberabwehr, die vor allem die Vielzahl von Third-Party-Lösungen an der Kundenschnittstelle in den Blick nehmen wird.

PRIVATBANKEN UND VERSICHERUNGEN BETRACHTEN HÄUFIGER DAS GESAMTE ÖKOSYSTEM IN IHREN SECURITY-KONZEPTEN

Unter den befragten Banken sind vor allem die Privatbanken diejenigen, die bereits entsprechende Sicherheitsarchitekturen zum Schutz ihrer unternehmensübergreifenden Geschäftsaktivitäten aufgebaut haben. Zwei Drittel verfolgen entsprechende ganzheitliche Security-Strategien, während sich 55 Prozent der Sparkassen und Genossenschaftsbanken noch ausschließlich auf die Überwachung ihrer eigenen IT-Infrastruktur konzentrieren. Auch 66 Prozent der untersuchten Versicherungen richten ihre IT-Security auf die Überwachung ihres gesamten Ökosystems aus. Allerdings etablieren sich – auch im öffentlich-rechtlichen Bankenumfeld – immer mehr Plattformökosysteme im Finanzdienstleistungssektor, was zu neuen Angriffsflächen und somit zu einem hohen Handlungsdruck führt.

POSITIV: IT-SECURITY HAT SICH ZUM WERTSCHÖPFUNGSFAKTOR ENTWICKELT. NEGATIV: IN DER WAHRNEHMUNG IST IT-SECURITY IMMER NOCH EIN KOSTENFAKTOR

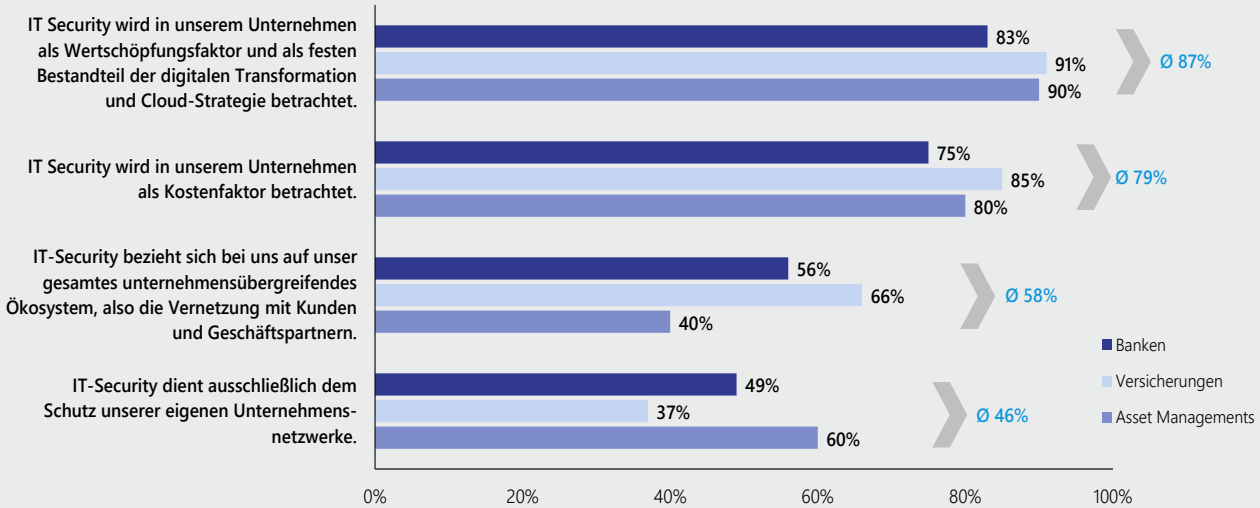


Abb. 14: Frage: Wie wird IT-Security in Ihrem Unternehmen wahrgenommen?; Alle Teilnehmer; Häufigkeitsverteilung; Werte beziehen sich auf die Antworten „stimme voll zu" und „stimme eher zu""; Banken: n = 54; Versicherungen: n = 35; Asset Managements: n = 10

PLATTFORMÖKONOMIE ERFORDERT NEUE SECURITY-ARCHITEKTUREN

Diejenigen Unternehmen, die bisher IT-Security noch ausschließlich in ihren eigenen Unternehmensgrenzen betrachten, sind gefordert, ihre Security-Architekturen und Konzepte an der aufkommenden Plattformökonomie auszurichten. Vor allem plattformbasierte Geschäftsmodelle gewinnen im Finanzdienstleistungssektor an Bedeutung.

Dabei geht es für Banken, Versicherungen oder Vermögensverwalter darum, sich näher an den Lebenswelten ihrer Kundinnen und Kunden zu orientieren. Dazu bauen sie entweder als Plattform-Owner eigene Ökosysteme auf und binden andere Drittanbieter an ihre IT-Infrastruktur an oder sie integrieren ihre Produkte in bereits bestehende Ökosysteme. In jedem Fall erweitern sie durch die Vernetzung mit anderen Unternehmen die Projektionsfläche ihrer IT-Infrastruktur für potenzielle Cyberangriffe.

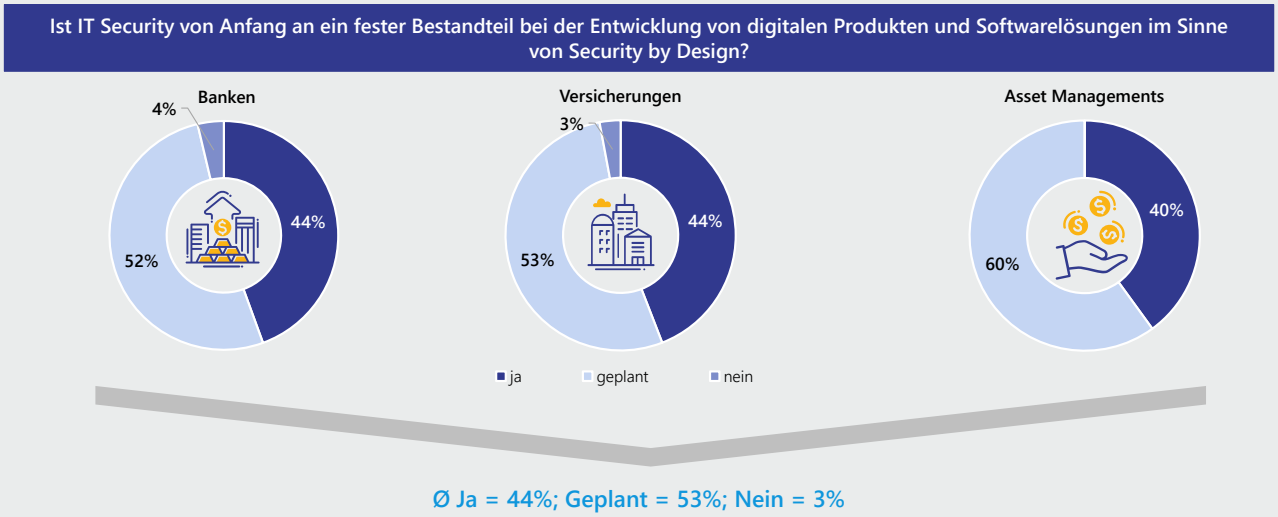
So zeigt die Lünendonk®-Studie „Kunden im Mittelpunkt –Kundenzentrierung als wesentlicher Erfolgsfaktor im Finanzdienstleistungssektor", dass bereits jeder dritte Finanzdienstleister in Plattformökosystemen vertreten ist. Laut dieser Studie arbeiten 63 Prozent bereits daran, die Angebote von rein digitalen Wettbewerbern zu übertreffen, und rund 25 Prozent wollen ihre digitalen Kundenschnittstellen massiv ausbauen. Ebenso werden neue Produkte und Services in Zukunft immer stärker vom Kunden beziehungsweise von der Kundin ausgehend entwickelt, um sie in seine respektive ihre Alltagssituationen einzubetten. Dazu wollen 89 Prozent der untersuchten Finanzdienstleister rund um den bestehenden Produktkern immer mehr digitale Zusatzservices anbieten, beispielsweise Portale zu Themen wie Familie, Wohnung, Immobilienkauf, Baufinanzierung oder Vermögensaufbau.

SECURITY BY DESIGN: DIGITALISIERUNG DER KUNDENSCHNITTSTELLEN FÜHRT ZU ERHÖHTEM SCHUTZ VON KUNDEN- UND UNTERNEHMENSDATEN

Zu diesem Zweck investieren Banken, Versicherer und Vermögensverwaltungen intensiver in digitale Produkte wie Kunden-Apps, Online-Portale oder in plattformbasierte Ökosysteme – kurzum in die Digitalisierung der Customer Journey. Immer mehr solcher Anwendungen werden in BizDevOps-Teams (Business & DevOps) und auf der Grundlage einer Cloud-native-Architektur entwickelt, woraus sich wiederum hohe Anforderungen an den Schutz der gesammelten personenbezogenen Daten ergeben. Insbesondere die Finanzaufsichtsbehörden fordern die Erfüllung bestimmter Sicherheitsstandards bei der Entwicklung digitaler Produkte.

Security by Design, also die Berücksichtigung von Security-Elementen bereits während der Produktentwicklung, ist folglich eine wichtige Kernanforderung, die Finanzdienstleister bereits bei der Entwicklung digitaler Produkte und Schnittstellen zu berücksichtigen haben. Dabei geht es unter anderem um eine Minimierung der Angriffsfläche, den Einsatz von Verschlüsselungstechnologien und um ein wirkungsvolles Identity & Access Management beispielsweise mithilfe einer 2-Faktor-Authentifizierung. Obwohl nahezu alle größeren Finanzdienstleister mittlerweile digitale Frontend-Anwendungen anbieten, finden IT-Security-Anforderungen bisher nur bei 44 Prozent der befragten Finanzdienstleister im Design digitaler Produkte Berücksichtigung. Allerdings planen nahezu alle anderen befragten Unternehmen, in Zukunft Security by Design in der Softwareentwicklung als integralen Bestandteil zu berücksichtigen.

SECURITY BY DESIGN IST ALS FESTER BESTANDTEIL BEI DER ENTWICKLUNG VON PRODUKTEN UND SOFTWARELÖSUNGEN GEPLANT



Ø Ja = 44%; Geplant = 53%; Nein = 3%

Abb. 15: Frage: Ist IT Security von Anfang an ein fester Bestandteil bei der Entwicklung von digitalen Produkten und Softwarelösungen im Sinne von Security by Design?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 54; Versicherungen: n = 35; Asset Managements: n = 10

DIE ZUNEHMENDE CLOUD-NUTZUNG VERÄNDERT DIE SICHERHEITSLAGE

Aber nicht nur die Digitalisierung der Kundenschnittstellen und Plattformökosysteme erhöht das Risiko von Cyberangriffen, sondern auch die immer stärkere Nutzung von Cloud-Services. 97 Prozent der befragten Business- und IT-Verantwortlichen sehen in der zunehmenden Komplexität der IT durch Cloud-Services einen wesentlichen Einflussfaktor auf die IT-Security in ihren Unternehmen. Neun von zehn Befragten sehen ferner in dem stärkeren Bezug von Software as a Service und in der Entwicklung digitaler Produkte auf der Basis von Cloud-native-Technologien weitere Security-Risiken, denen es zu begegnen gilt.
Eine größere Bedrohungslage für die IT-Sicherheit stellen für 84 Prozent der Befragten die bereits erwähnten cloudbasierten Plattformökosysteme dar und für 83 Prozent der allgemeine Trend zur zunehmenden Cloud-Nutzung. Infolge der übereinstimmenden Bedrohungslage durch mehr Cloud-Nutzung überrascht es jedoch, dass sich für nur 79 Prozent der an der Studie teilnehmenden Unternehmen die stärkere Auslegung der regulatorischen Vorgaben für die Nutzung von Cloud-Services auf ihre IT-Security-Strategien auswirkt.

Obwohl sich gerade in den befragten Genossenschaftsbanken und Sparkassen die IT-Security-Strategien noch sehr stark auf die eigenen IT-Infrastrukturen anstatt auf unternehmensübergreifende Sicherheitskonzepte beziehen, sehen rund 90 Prozent von ihnen in der Nutzung cloudbasierter Plattformökosysteme eine größere Bedrohungslage. Zum Vergleich:

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Unter den befragten Privatbanken sehen „nur“ 80 Prozent eine größere Bedrohungslage durch die aufkommende Plattformökonomie, was zu dem vorsichtigen Schluss führt, dass sich einige der untersuchten Privatbanken mit ihrer IT-Security-Strategie für plattformbasierte Geschäftsmodelle als gut aufgestellt einschätzen.

AUSWIRKUNGEN DER ZUNEHMENDEN CLOUD-NUTZUNG AUF DIE IT-SECURITY

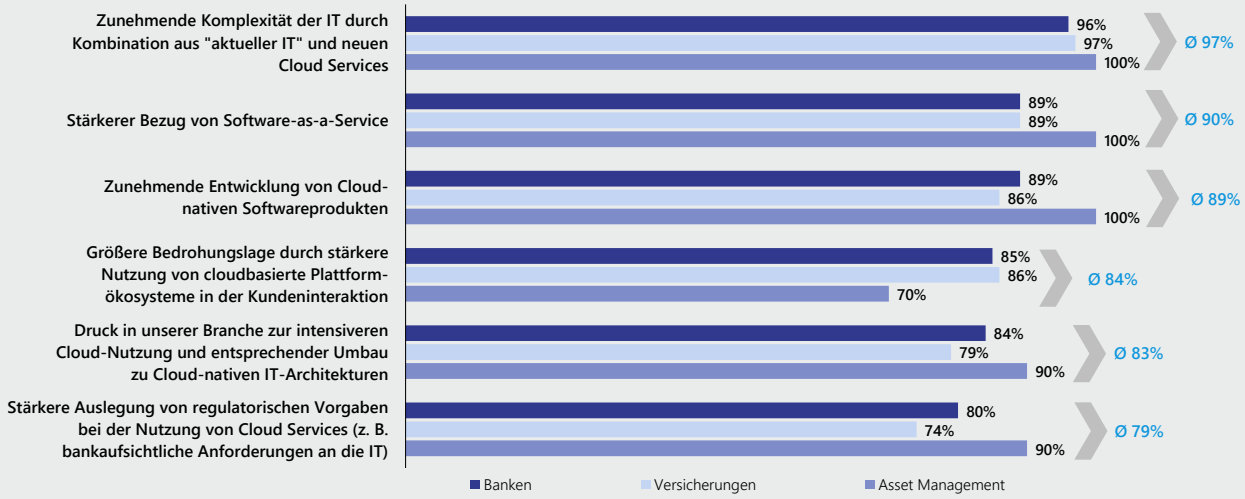


Abb. 16: Frage: Was sind die wesentlichen Einflussfaktoren für IT-Security in Ihrem Unternehmen?; Alle Teilnehmer; Häufigkeitsverteilung; Werte beziehen sich auf die Antworten „sehr großer Einfluss“ und „eher großer Einfluss“; Banken: n = 54; Versicherungen: n = 34; Asset Managements: n = 10

DREI VON ZEHN FINANZDIENSTLEISTERN ÜBERPRÜFEN IHRE IT-SECURITY-STRATEGIE NICHT AUF WIRKSAMKEIT

Infolge der zunehmenden Nutzung von Cloud-Services im Finanzdienstleistungssektor können die gesetzlichen oder regulatorischen Mindestanforderungen nur ein Mindestmaß darstellen. Und auch die Verantwortung an die eigene IT oder die Outsourcing-Partner abzugeben, reicht in Zeiten der Digitalisierung und der täglichen Bedrohung durch Cyberkriminalität längst nicht mehr aus.

Vor allem wenn (richtigerweise) immer mehr Public-Cloud-Dienste genutzt werden, müssen höchste Anforderungen an die Datensicherheit erfüllt sein. Wie das erste Kapitel gezeigt hat, sorgen sich die untersuchten Unternehmen nicht nur um den Abfluss von Daten an Hackerorganisationen, sondern auch um ihre Reputation sowie um Störungen im Geschäftsbetrieb und damit um Umsatzeinbußen.

Im Sinne der Umsetzung regulatorischer Vorgaben vor allem durch die BAIT, die VAIT und die KAIT sind bestimmte Anforderungen im Rahmen der Cloud-Governance zu erfüllen. Dazu gehört es unter anderem auch, die IT-Security-Strategie und -Prozesse auf ihre Wirksamkeit

hin zu überprüfen. Aber nur sieben von zehn der befragten Finanzdienstleister überprüfen regelmäßig die Wirksamkeit ihrer Cyber-Security-Strategie. Hier liegen die befragten Versicherungen noch deutlich hinter den Banken, denn nur 63 Prozent der Versicherer messen regelmäßig den Cyber-Security-Status, während dies 74 Prozent der Banken tun. Bei den Versicherungen messen interessanterweise die kleineren Gesellschaften mit bis zu 2 Milliarden Euro an Beitragseinnahmen deutlich häufiger den Security-Status (79 %) als die größeren Gesellschaften mit mehr als 2 Milliarden Euro Beitragseinnahmen (52 %). Sogar noch seltener werden Penetration-Tests, kurz Pentests, durchgeführt. Nur sechs von zehn Finanzdienstleistern überprüfen ihre IT-Systeme regelmäßig mithilfe von Pentesting. Dabei werden die IT-Systeme einem empirischen Sicherheitscheck unter definierten Rahmenbedingungen unterzogen. Die Ergebnisse werden in einem Bericht zusammengefasst und die identifizierten Schwachstellen, Konfigurationsfehler und Best-Practice-Empfehlungen aufgelistet

70 %
der Unternehmen überprüfen die Wirksamkeit ihrer Cyber-Security-Strategie

FEHLENDE ÜBERPRÜFUNG: EIN TEIL DER FINANZDIENSTLEISTER KANN DEN REGULATORISCHEN ANFORDERUNGEN NOCH NICHT GERECHT WERDEN

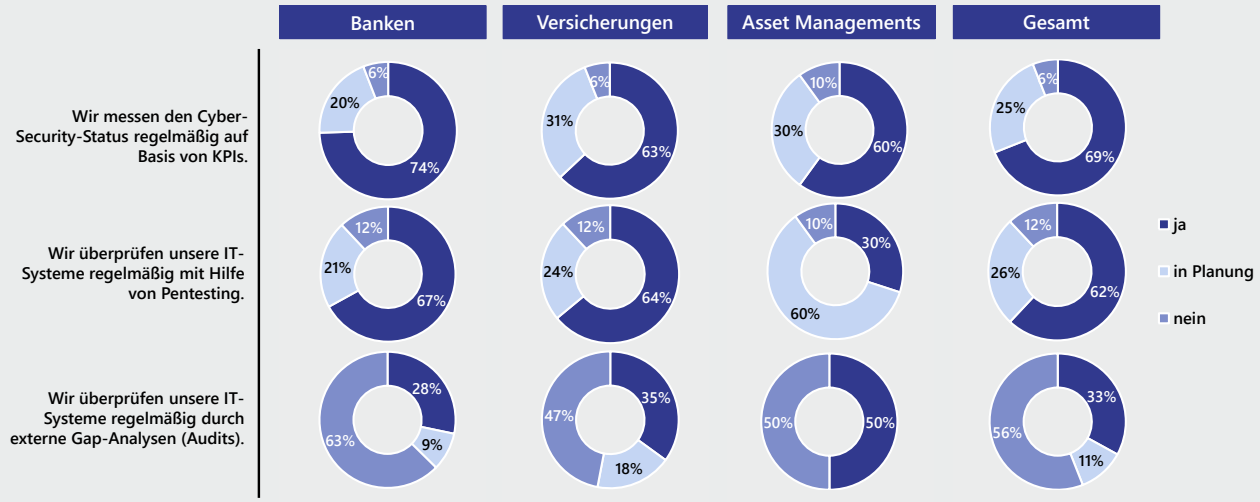


Abb. 17: Frage: Wie überprüfen Sie in Ihrem Unternehmen die Wirksamkeit/Resilienz Ihrer IT-Security?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 52; Versicherungen: n = 33; Asset Managements: n = 10

WIDERSPRUCH ZWISCHEN ANSPRUCH UND WIRKLICHKEIT

Die Ergebnisse zeigen, dass ein signifikanter Teil der befragten Finanzdienstleister derzeit nicht in der Lage ist, vollständige Auskunft über seinen Security-Status zu geben – einfach weil keine entsprechenden Überprüfungen stattfinden. Hier deutet sich ein klarer Widerspruch zur Wahrnehmung der eigenen Cyber-Resilienz an (siehe Abbildung 5), denn neun von zehn Finanzdienstleistern schätzen die Fähigkeit ihres Unternehmens, Bedrohungen durch Hackerangriffe zu identifizieren und somit eine Früherkennung von Cyberangriffen zu gewährleisten, als hoch ein.

Budget für Cyber Security

In Kapitel 1 wurde gezeigt, dass neun von zehn der untersuchten Finanzdienstleister Cyber Security mittlerweile als Wertschöpfungsfaktor wahrnehmen – unter anderem auch weil, wie Kapitel 2 zeigte, die Cloud ein strategisches Element für Finanzdienstleister auf dem Weg ihrer digitalen Transformation ist und die Zahl der eingesetzten Cloud-Lösungen sowie auf Cloud-Technologien basierender Geschäftsmodelle folglich kontinuierlich ansteigt.

Obwohl immer noch ein (zu großer) Teil der befragten Banken, Versicherer und Vermögensverwalter die IT-Sicherheit weiterhin als Kostenfaktor betrachtet, werden die Ausgaben für den Schutz vor Cyberangriffen in Zukunft steigen. Steigende Ausgaben für die IT-Sicherheit ergeben sich aus den steigenden Compliance- und Risk-Anforderungen, unter anderem infolge der durch die Finanzaufsichtsbehörden gestellten Mindestanforderungen an die IT-Sicherheit. Aber auch Reputationsschäden und hohe Strafzahlungen beispielsweise durch den Verlust von Kundendaten führen immer mehr zu einem Umdenken bei Finanzdienstleistungen, mehr in den Schutz der IT-Systeme zu investieren. Da die Zahl der Cyberangriffe mit hoher Zuverlässigkeit stetig ansteigt und die Digitalisierung der Geschäftsmodelle im Finanzdienstleistungssektor längst in vollem Gang ist, müssen entsprechende Maßnahmen in die Absicherung der verletzlichen IT-Infrastrukturen sowie der sensiblen Kunden- und Unternehmensdaten auch getroffen werden.

74 %
der Unternehmen erhöhen Ihre Budgets für die Früherkennung von Cyberangriffen.

Die wichtigste Nachricht für alle IT- und Security-Verantwortlichen, aber auch für die Kundinnen und Kunden: Bei keinem der untersuchten Finanzdienstleister wird im Jahr 2022 weniger Geld für die IT-Sicherheit ausgegeben. Die größten Zuwächse in den Budgets finden sich erwartungsgemäß im Bereich Identifizieren von Schwachstellen (Identify): 74 Prozent der befragten Unternehmen werden ihre Budgets für die Früherkennung von potenziellen Cyberrisiken und Angriffen um bis zu 10 Prozent erhöhen, unter den befragten Versicherungen sind es sogar 80 Prozent und bei den untersuchten Genossenschaftsbanken noch mehr, nämlich 85 Prozent. Hingegen will ein Drittel der befragten Sparkassen diese Budgets konstant lassen.

Den zweiten großen Block für Budgeterhöhungen bildet die Antizipation und Abwehr von Cyberangriffen (Prevention). 61 Prozent der Studienteilnehmer wollen die Investitionen in diesem zentralen Bereich der Cyberabwehr um bis zu 10 Prozent erhöhen, 17 Prozent sogar um mehr als 10 Prozent. Dieser hohe Anstieg kommt vor allem aus den befragten Privatbanken: 30 Prozent von ihnen werden ihre Budgets für Prevention 2022 um mehr als 10 Prozent erhöhen, aber auch jede fünfte Versicherung, unabhängig von ihrer Größe.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Im Bereich der Erkennung von aktuellen Cyberangriffen und Unregelmäßigkeiten in den IT-Systemen (Detection) werden die Budgets hingegen laut den Investitionsplanungen nicht so stark steigen wie in den Bereichen Identify und Prevention. Die vergleichsweise moderate Entwicklung mag unter anderem damit zusammenhängen, dass viele Finanzdienstleister in den letzten Jahren ihre Rechenzentren technologisch modernisiert, technische Schulden abgebaut und in neue Security-Softwarelösungen zur Gefahrenabwehr investiert haben.

Dennoch wollen 61 Prozent der befragten Unternehmen in ihren Bemühungen, die Gefahr von Hackerangriffen weiter zu reduzieren, nicht nachlassen und ihre Ausgaben für die Erkennung von Cyberangriffen 2022 weiter erhöhen. Vor allem Banken investieren stärker in die Detection als die übrigen befragten Finanzdienstleister: So werden 13 Prozent ihre Budgets um mehr als 10 Prozent erhöhen und weitere 54 Prozent um bis zu 10 Prozent. Dagegen wird jede zweite befragte Versicherung ihr Budget 2022 konstant halten.

Bei der Detection geht es neben technologischen Aspekten aber auch sehr stark um organisatorische und prozessuale Maßnahmen, die es im Falle aufgedeckter Unregelmäßigkeiten zu treffen gilt. Denn gerade durch den digitalen Arbeitsplatz ergibt sich eine Vielzahl neuer Angriffspunkte und es gilt, die Endpoint Security entsprechend nachzuziehen und an die Heimarbeitsplätze anzupassen.

Aber auch das Security Information and Event Management (SIEM) steht mit zunehmender Cloud-Nutzung im Fokus der IT. Je häufiger sich Finanzdienstleister für Multi-Clouds und hybride Umgebungen entscheiden, ist es im Sinne einer wirkungsvollen Security-Strategie ratsam, die Monitoring-Daten aus den einzelnen Cloud-Services an einer zentralen Stelle zusammenlaufen zu lassen. Mit zunehmender Nutzung multipler und hybrider Cloud-Prozesse müssen folglich auch Investitionen in das SIEM nachgezogen werden. Druck zu Investitionen in ein wirkungsvolles SIEM kommt auch durch die BAIT, die VAIT und die KAIT, in denen ein SIEM nahegelegt wird. Organisatorisch und prozessual kommt es hierbei jedoch darauf an, ein zentrales SIEM aufzubauen, das die unterschiedlichen Cloud-Provider beziehungsweise Managed-Service-Provider steuert und somit für die Integration der hybriden Multi-Cloud- und Multi-Provider-Umgebungen in die Security-Prozesse sorgt.

Auch in den Bereich „Response“, bei dem es um das Ergreifen der richtigen Maßnahmen im Falle eines Cyberangriffs geht, wird moderat investiert – allerdings auch hier wieder mehrheitlich von den Versicherungen. Von den befragten Banken hingegen werden 63 Prozent ihre Budgets für Projekte in diesem Bereich erhöhen. Gleiches gilt auch für Recovery-Maßnahmen: Während jede zweite Versicherung die Budgets konstant hält, werden zwei Drittel der Banken (67 %) mehr Geld in diesen wichtigen Teil der Business Continuity stecken.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

ENTWICKLUNG DER BUDGETS FÜR CYBER SECURITY

	um über 10% steigen	um bis zu 10% steigen	konstant
Identify: Identifizieren von Schwachstellen	4%	74%	22%
Prevention: Antizipation und Abwehr von Cyberangriffen	17%	61%	21%
Detection: Erkennung von stattfindenden Angriffen und Unregelmäßigkeiten/Anomalien	9%	52%	39%
Response: Ergreifen der richtigen Maßnahmen bei erfolgten Cyberangriffen	8%	47%	44%
Recovery: Wiederherstellen der Daten und IT-Systeme	2%	58%	40%

Abb. 18: Frage: Wie werden sich im kommenden Jahr die extern vergebenen Budgets in Ihrem Unternehmen voraussichtlich in den folgenden Bereichen verändern?; Alle Teilnehmer; Häufigkeitsverteilung; n = 99

SECURITY SOLLTE DEZENTRALER UND CROSSFUNKTIONALER GESTEUERT WERDEN

Die Analyse der Budgetverantwortung für die Umsetzung von IT-Security-Strategien zeigt einige deutliche Unterschiede in den einzelnen Branchen und lässt auf unterschiedliche Reifegrade in der Digitalisierung und Agilität schließen. Bei der Verantwortung für die IT-Security kommt es einerseits darauf an, einen ganzheitlichen Blick auf die Gesamtheit der IT-Prozesse eines Unternehmens zu haben und die immer komplexeren IT-Landschaften effektiv und effizient zu steuern; andererseits führt die steigende Relevanz von Security by Design dazu, dass bereits während der Produktentwicklung Sicherheitsanforderungen definiert und bei der Konfiguration der IT-Infrastruktur von Beginn an berücksichtigt werden.
Da immer mehr digitale Produkte in BizDevOps entwickelt werden, sollte auch genau hier ein Teil der Verantwortung für den Schutz vor Cyberbedrohungen angesiedelt sein.

Bei jedem fünften der untersuchten Finanzdienstleister (21 %) ist die Verantwortung für Teile des IT-Security-Budgets bereits in solchen crossfunktionalen DevOps-Teams verankert. In dezentralen Einheiten liegt bei 66 Prozent der untersuchten Unternehmen das Budget für IT-Security. Hier hat tatsächlich – unter anderem auch im Zuge von Security by Design – ein Umdenken stattgefunden:

Wenn die einzelnen Fachbereiche mehr Verantwortung für den Schutz vor Cyberangriffen erhalten, ist es möglich, dass einerseits die notwendige Sensibilisierung gegenüber Cyberkriminalität und für Cyber-Risk-Anforderungen vorhanden ist und andererseits Security by Design auch tatsächlich ein fester Bestandteil in den Digitalisierungsstrategien der Fachbereiche und zu einer Selbstverständlichkeit wird.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

DIE VERANTWORTUNG FÜR CYBERABWEHR WIRD AUF MEHRERE FACHBEREICHE VERTEILT

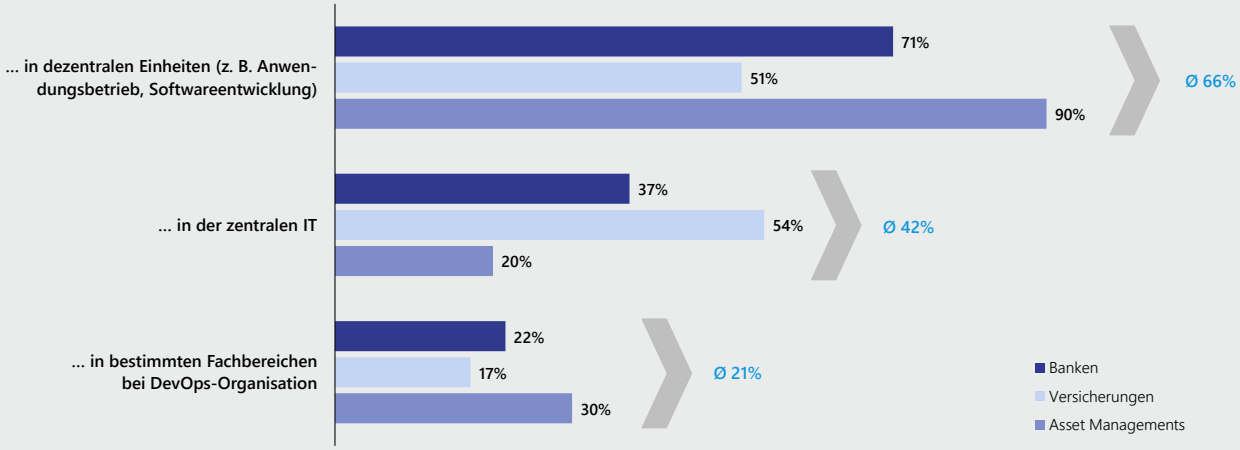


Abb. 19: Frage: Liegt das Budget für Cyber Security in Ihrem Unternehmen...?; Alle Teilnehmer; Banken: n = 49; Versicherungen: n = 34; Asset Managements: n = 8

Geplante Security-Maßnahmen und -Investitionen

Digitalisierte Kundenschnittstellen und Prozesse, mehr Cloud, neue Bedrohungsszenarien, veränderte Anforderungen an Daten- und IT-Sicherheit und steigende Budgets: Die befragten Finanzdienstleister stellen sich in den kommenden Jahren der neuen Realität in der IT-Sicherheit und investieren in die bessere Absicherung ihrer IT-Infrastruktur und digitaler Geschäftsmodelle.

SCHWACHSTELLEN ERKENNEN, BEVOR SCHÄDEN EINTRETEN: UNTERNEHMEN SETZEN FOKUS AUF FRÜHERKENNUNG

Da Hackerinnen und Hacker oft bereits zu einem sehr frühen Zeitpunkt und unbemerkt im Unternehmen sind, bevor der eigentliche Angriff passiert, liegt der größte Fokus der Unternehmen in den Jahren 2022–2023 auf Investitionen im Bereich „Identify", also dem Identifizieren von Schwachstellen und Sicherheitslücken. Hierbei ist ein hochprofessionelles Vorgehen unter Einsatz modernster Technologien und wirksamer Prozesse notwendig, um größere Schäden abzuwenden. So legen 48 Prozent der Unternehmen einen sehr starken und weitere 34 Prozent einen eher starken Fokus auf das Vulnerability Management, also die präventive Erkennung und Behebung von Schwachstellen in der eigenen IT-Infrastruktur beziehungsweise im gesamten Ökosystem. Noch stärker im Fokus steht aber mit Blick auf die kommenden zwei Jahre das Identity & Access Management (IAM), also die Verwaltung der Benutzerkonten und Zugriffsberechtigungen. Hier wollen sogar 94 Prozent der befragten Unternehmen einen Fokus setzen.

94 %
der Unternehmen setzen ihren Fokus auf Identify & Access Management (IAM).

Eine hohe Relevanz erlangt das IAM durch den Trend zu Multi-Cloud-Prozessen. Eine der Kernfunktionen ist die Authentifizierung und Autorisierung des Users, weshalb IAM auch eine zentrale Zugriffskontrolle für Webdienste wie Online-Banking, Online-Zahlungsverkehr, Wertpapierhandel oder den Zugriff auf Kundeninformationen in Web-Portalen beinhaltet (Stichwort: 2-Faktor-Authentifizierung). Eine weitere Kernfunktion moderner IAM-Softwarelösungen ist die zentrale Verwaltung der Zugriffsberechtigungen, also rollenbasierte Regelungen, auf welche Informationen eine Mitarbeiterin beziehungsweise ein Mitarbeiter Zugriff hat und auf welche eben nicht. Einen stets aktuellen Überblick über die Berechtigungen und Zugriffe zu haben ist vor allem infolge der zunehmenden Zahl von Public-Cloud-Diensten und entsprechend mehr potenzieller Angriffspunkte wichtiger denn je.

NACHHOLBEDARF AUCH IN DER PRÄVENTION VON CYBERANGRIFFEN

Ebenfalls stark im Fokus der Maßnahmen für mehr Cyberresilienz soll das Security-Monitoring stehen. 94 Prozent der untersuchten Finanzdienstleister legen in den Jahren 2022–2023 hierauf einen starken Fokus. Wie Kapitel 3 gezeigt hat, überprüfen nur sieben von zehn der be-

fragten Unternehmen regelmäßig ihre IT-Systeme auf Security-Vorfälle (siehe Abb. 16). Daher überrascht es nicht, dass infolge der größeren Bedrohungslage einerseits sowie steigender regulatorischer und gesetzlicher Anforderungen andererseits die Finanzdienstleister nun ihre Anstrengungen im Security-Monitoring erhöhen.

Auch die steigenden Datenmengen und die Komplexität im Cyber-Security-Tracking stellen viele Security-Abteilungen vor große Herausforderungen, die Flut an Gefahren zu erkennen und abzuwehren. Das führt dazu, dass Unternehmen in Zeiten der Digitalisierung eine deutlich höhere Anzahl Schwachstellen haben als in der Vergangenheit. So zeigen Analysen erfolgter Cyberangriffe – unter anderem vom BSI oder den Security Operations Centers der großen Cloud-Hyperscaler –, dass Angriffe vor allem dann geplant werden, wenn Unternehmen beispielsweise ankündigen, stärker in Cloud-Lösungen oder in Cyber Security zu investieren. Aber auch im Vorfeld bestimmter Events, bei denen eine hohe Performance der IT-Systeme erforderlich ist, werden Angriffe geplant. Um solche Angriffsmuster besser und vor allem frühzeitiger zu erkennen, kann es hilfreich sein, stärker auf Künstliche Intelligenz in der Prevention zu setzen. So haben Machine-Learning-basierte Algorithmen den Vorteil, kontinuierlich und automatisiert Millionen von Ereignissen zu überwachen und Muster (Anomalien) schneller und zuverlässiger zu erkennen. Vor allem um der steigenden Zahl von Bot-Angriffen und immer neuen Schadsoftwareprogrammen etwas entgegenzusetzen, lohnt es sich, sich mit Machine Learning zu befassen und auch KI-betriebene Bots einzuführen, die die Netzwerke nach Gefahren tracken. Ein weiterer Vorteil vom Einsatz KI-basierter Security Services bereits in der Prevention ist, dass KI-Technologien die IT-Netzwerke in einem 24/7-Modus tracken können und damit eine Reihe von Angriffspunkten schließen.

66 %
der Finanzunternehmen fokussieren sich auf die Cloud Security in den kommenden zwei Jahren.

Zum Bereich der Prevention gehören neben dem Security Monitoring auch die Cloud Security und die Data Center Security. Während 70 Prozent der befragten Banken und Vermögensverwaltungen einen Fokus auf die Cloud Security legen, sind es unter den befragten Versicherungen mit 57 Prozent deutlich weniger. Vor allem von denjenigen Finanzdienstleistern mit einer Cloud-first-Strategie werden 83 Prozent ihre Maßnahmen zur Cloud Security erhöhen und 100 % diejenigen zum Security Monitoring.

Dagegen legen 74 Prozent der befragten Versicherer einen ihrer Schwerpunkte auf die Data Center Security – ebenso wie 80 Prozent der Banken und 70 Prozent der Vermögensverwaltungen. Steigende Security-Anforderungen ergeben sich vor allem infolge des zunehmenden Einsatzes von Data Lakes im Finanzdienstleistungssektor – ein Konzept, das unter anderem aufgrund der notwendigen Rechenpower und Skalierung sehr eng mit der Cloud verknüpft ist.

DETECTION: NUR DAS SIEM STEHT WIRKLICH IM FOKUS – DER SCHUTZ VOR REMOTE-ZUGRIFFEN DAGEGEN NICHT

Im Bereich der Detection steht vor allem das SIEM im Fokus der Maßnahmen, nämlich von 83 Prozent der Unternehmen. Von den Unternehmen, die eine Cloud-first-Strategie verfolgen zeigt, werden sich 93 Prozent mehr um ihre SIEM-Prozesse kümmern.

Überraschenderweise unterrepräsentiert bei den Maßnahmen für mehr Cyberresilienz ist die Endpoint Security. Für mehr als jeden zweiten Finanzdienstleister steht die Absicherung der genutzten Endgeräte nicht im Fokus der Security-Maßnahmen für die kommenden zwei Jahre. Durch die zunehmende Nutzung mobiler Endgeräte im Business-Alltag und einen deutlichen Anstieg von Remotezugriffen über mobile Endgeräte auf Unternehmensnetzwerke stehen Mobile Devices mehr und mehr auch im Fokus von Cyberattacken. Darüber hinaus müssen in der Post-Corona-Welt die Security-Konzepte infolge des Trends zu New-Work-Konzepten überarbeitet werden. Denn während der digitale Arbeitsplatz in der Corona-Pandemie zunächst eine ungeplante Notwendigkeit war, zeichnet sich in der Post-Corona-Welt ab, dass sich neue Formen der Arbeit und Remote Working auch langfristig durchsetzen werden. Bei der Interpretation der Maßnahmen zur Endpoint Security ist es allerdings wichtig zu erwähnen, dass nur 18 Prozent der Versicherungen einen Fokus auf Endpoint Security setzen wollen, aber immerhin 28 Prozent der Banken und 30 Prozent der Vermögensverwaltungen.

93 %
der Unternehmen setzen ihren Fokus auf SIEM.

Zur Detektion von Cyberangriffen und Security-Schwachstellen setzen immer mehr Unternehmen auf SOCs. Dabei handelt es sich um eigene Organisationseinheiten, die für die kontinuierliche Überwachung der IT-Systeme und für die Informationssicherheit verantwortlich sind. SOCs können sowohl intern als auch extern oder als hybride Formen – abhängig von der Verfügbarkeit von Inhouse-Security-Expertinnen und Experten – betrieben werden. Sie beschäftigen sich vor allem mit der Prävention, dem aktiven Schutz, der Erkennung und dem Behandeln von Cyberangriffen. Dabei werden Ansätze und Technologien wie Schwachstellenmanagement, Gefährdungsbewertung und Endpoint Detection, Security Monitoring oder SIEM-Systeme in einem zentralen Center of Excellence gebündelt.

Dieser Ansatz verspricht die bestmögliche Umsetzung eigener oder durch Regulatorik vorgegebener Sicherheitskonzepte durch Kombination aller relevanten Aufgaben in einer zentralen Organisation und den Wegfall von Schnittstellen und damit verbundenen Abstimmungsproblemen. 56 Prozent der in der Studie befragten Unternehmen planen im Zeitraum 2022–2023 den Aufbau von SOCs als eine der Schwerpunktmaßnahmen für mehr Cyberresilienz.

SCHWERPUNKTE ZUR ERHÖHUNG DER CYBERRESILIENZ

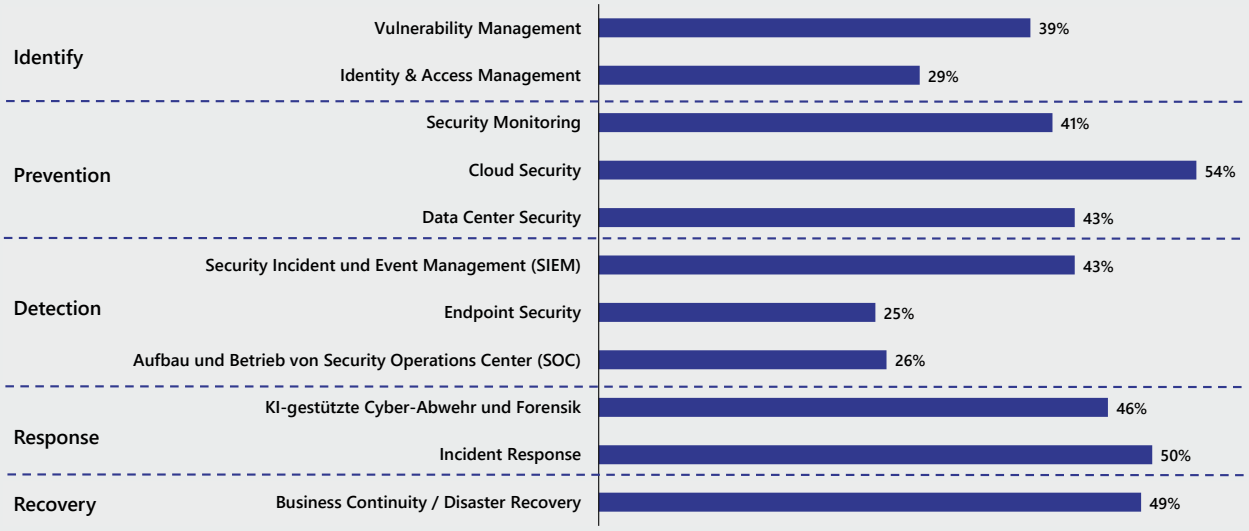


Abb. 20: Frage: Welche der folgenden Security-Aspekte stehen in Ihrem Unternehmen in den kommenden zwei Jahren im Fokus?; Häufigkeitsverteilung; Skala: 1 = kein Fokus" bis 4 = „starker Fokus"; Banken: n = 50; Versicherungen: n = 34; Asset Managements: n = 10

WAS PASSIERT BEI EINEM ANGRIFF? NOCH GERINGER EINSATZ VON KÜNSTLICHER INTELLIGENZ, ABER DAFÜR FOKUSSIERUNG AUF DIE REAKTIONSGESCHWINDIGKEIT

Ist ein Cyberangriff erfolgt, kommt es darauf an, schnell zu handeln. Denn je effektiver die Reaktion auf einen Security-Vorfall ist, desto höher ist die Chance, einen Datendiebstahl, das Verschlüsseln der Systeme oder den Ausfall produktiver Prozesse zu verhindern. Auch Meldungen an die Aufsichtsbehörden – beispielsweise beim Diebstahl personenbezogener Daten – müssen sehr zeitnah erfolgen. Für eine möglich effektive und effiziente Reaktion auf Cyberangriffe kommt es vor allem auf Kommunikation, Organisation, Prozesse und Ressourcen an. Dass drei Viertel der an der Studie teilnehmenden Institute (74 %) einen Fokus auf Incident Response legen wollen, zeigt, dass bei der Reaktionsfähigkeit noch häufig Handlungsbedarf besteht. Die Aufgaben für den Schutz vor Cyberangriffen werden im Zuge der Digitalisierung immer vielfältiger und komplexer. Die steigende Datenmenge und die Komplexität im Cyber-Security-Tracking stellen viele Security-Abteilungen vor große Herausforderungen, die Flut an Gefahren zu erkennen und abzuwehren.

Um die steigende Datenflut im Security Monitoring besser zu beherrschen, aber auch um die Security-Expertinnen und Experten von aufwendigen Routineaufgaben zu entlasten, denken Unternehmen immer häufiger über den Einsatz Künstlicher Intelligenz beziehungsweise Machine Learning bei der Cyber Security nach. Die kontinuierliche und automatisierte Analyse von Daten und Ereignissen hilft, potenzielle Bedrohungen frühzeitig zu erkennen, zu klassifizieren und gegebenenfalls auf mögliche Angriffe schneller zu reagieren und groß-

flächige Schäden vom Unternehmen abzuwenden. Auf den Einsatz Künstlicher Intelligenz zur Cyberabwehr setzen bereits 44 Prozent der in der Studie untersuchten Unternehmen.

RECOVERY: BUSINESS CONTINUITY STEHT BEI NEUN VON ZEHN UNTERNEHMEN IM FOKUS

Nach einem erfolgten Cyberangriff oder Datendiebstahl ist es essenziell, sehr schnell wieder die Kontrolle über die Prozesse und die Daten zu erlangen. Dabei kommt es im Rahmen von Business-Continuity-Strategien sehr stark darauf an, die Prozesse und Daten wiederherzustellen. Entsprechende Disaster-Recovery-Konzepte werden auch von der Finanzaufsicht zwingend gefordert, weshalb es nur konsequent ist, dass 90 Prozent der befragten Unternehmen in die Optimierung ihrer Recovery-Maßnahmen investieren wollen.

Security Operations Center (SOC)

Das vorangegangene Kapitel hat gezeigt, dass jeder zweite untersuchte Finanzdienstleister (56 %) einen Fokus auf den Aufbau von SOCs legen wird. Diese Maßnahmen sind auch mit Blick auf die bereits im Betrieb befindlichen SOCs notwendig. So haben bisher (Stand: Herbst 2021) nur 14 Prozent der befragten Unternehmen ein SOC etabliert, also bereits in Betrieb genommen. Vor allem Banken sind hier mit 19 Prozent deutlich weiter als Versicherungen (12 %) und die befragen Vermögensverwaltungen (0 %).

45 Prozent der analysierten Finanzdienstleister befanden sich zum Zeitpunkt der Studienerstellung inmitten des Roll-outs, also der Operationalisierung, von SOCs. Hier gaben auch die Vermögensverwaltungen an, SOCs einzuführen. Weitere 28 Prozent der befragten Unternehmen planen in den kommenden Jahren den Aufbau von SOCs.

14 %
der Untenehmen haben ein SOC bereits eingeführt.

SOCs übernehmen für die Umsetzung der Cyber-Security-Strategie eine zentrale Aufgabe: Nicht selten werden Cyberangriffe und Datendiebstahl überhaupt nicht erkannt – unter anderem weil die Monitoring-Systeme bestimmte Schadprogramme gar nicht erst erkennen und entsprechend melden. Ein kontinuierliches Monitoring des gesamten Unternehmensökosystems (Unternehmensinfrastruktur, mobile Endgeräte, Third-Party-Anwendungen) ist daher essenziell, um die steigenden gesetzlichen und regulatorischen Anforderungen zu erfüllen, die bei der Cloud-Nutzung für Finanzdienstleister gelten. Zur effizienten Erfüllung der eigenen oder der externen Compliance-Vorgaben empfiehlt es sich daher, Know-how zur Cyberabwehr zentral in einem SOC zu bündeln. Im SOC sollten Security-Spezialistinnen und Spezialisten organisatorisch angesiedelt sein, um daraus eine eigene Einheit zu schaffen und den ihnen die Möglichkeit zu geben, sich komplett auf die Cyberabwehr zu konzentrieren. SOCs sind oft losgelöst von anderen IT-Teams, um unabhängiger von der IT zu agieren.

REIFEGRAD DER SOCS: NAHEZU ALLE ZENTRALEN AUFGABEN WERDEN ERBRACHT

Die zahlreichen Aufgaben, die in einem SOC gebündelt werden, müssen und werden auch in der Regel nicht komplett innerhalb eines Unternehmens angesiedelt sein. Vielmehr werden einige an Dienstleister für IT-Security im Rahmen von Managed Security Services übertragen, auch Beratungs- und Transformationsaufgaben werden oft ausgelagert. Das hängt damit zusammen, dass in vielen Unternehmen einerseits Security-Expertinnen und Experten und andererseits auch Erfahrungswissen und Best Practices für den Aufbau von SOCs und für die Umstellung der Organisation und Prozesse, die Entwicklung neuer Rollen sowie Weiterbildung und Training fehlen.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

SOCS NEHMEN IMMER HÄUFIGER IHRE ARBEIT AUF

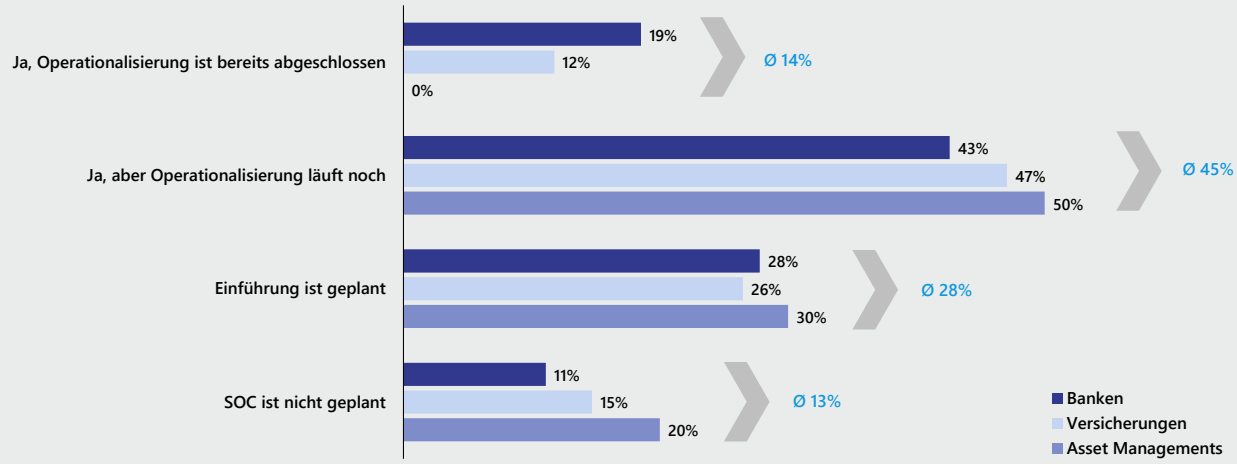


Abb. 21: Frage: Hat Ihr Unternehmen ein Security Operations Center (SOC) etabliert?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 54; Versicherungen: n = 34; Asset Managements: n = 10

Externe Unterstützung und Managed Security Services

IT-Security-Strategien stehen und fallen mit dem Erfolg ihrer Umsetzung – also der tatsächlichen Operationalisierung. Dabei kommt es, neben der passenden Security-Strategie und den technologischen und organisatorischen Voraussetzungen – vor allem auf die Verfügbarkeit von Security-Expertinnen und Experten an, um die Security-Konzepte auch wirksam umzusetzen. Allerdings mangelt es genau hier an Fachkräften. Die Vielzahl an Aufgaben zum Schutz vor der wachsenden Bedrohungslage rund um Cyberkriminalität und Cloud werden die Unternehmen daher nicht aus eigener Kraft bewältigen können.

BEDARF AN EXTERNER UNTERSTÜTZUNG IST IN EINIGEN BEREICHEN SEHR HOCH

Auch in den untersuchten Banken, Versicherungen und Vermögensverwaltungen werden externe Dienstleister zur Reduktion von Cyberrisiken und zur Cyberabwehr eingesetzt. Ein besonders hoher Bedarf an externer Unterstützung besteht im Bereich „Recovery" – ein Aufgabenfeld, das häufig durch Managed-Service-Provider im Rahmen des Rechenzentrumsbetriebs übernommen wird. Da für die Sparkassen und Genossenschaftsbanken jeweils ein zentraler interner IT-Dienstleister tätig ist, ist unter den Banken der Anteil derjenigen, die externe Unterstützung in Anspruch nehmen, geringer als unter den befragten Versicherungen und Vermögensverwaltungen.

Ebenfalls ein hoher Anteil an externen Services findet sich bei den Aufgaben rund um die Response im Falle von Cyber Incidents. Jedes zweite Unternehmen greift in diesem Bereich auf die Dienste externer Fachleute zurück. Auch hier ist der Anteil bei den befragten Versicherungen und Vermögensverwaltungen höher.

Eine häufige Zusammenarbeit mit externen Dienstleistern findet sich auch im SIEM und im gesamten Prevention-Bereich wieder. Mehr als 40 Prozent der untersuchten Unternehmen vergeben die Umsetzungsverantwortung in diesen Themenfeldern an externe Dienstleister.

Die Ergebnisse zeigen ferner, dass diejenigen Unternehmen, die eine Cloud-first-Strategie verfolgen, deutlich häufiger mit externen Dienstleistern zusammenarbeiten – unter anderem weil sie noch mehr als andere Unternehmen die regulatorischen und gesetzlichen Vorgaben zur Cloud-Nutzung einhalten müssen. So arbeiten beispielsweise 72 Prozent der Unternehmen mit einer Cloud-first-Strategie im Bereich der Cloud-Security mit externen Dienstleistern zusammen. Auch im Cloud-Monitoring finden sich mit 62 Prozent deutlich mehr Unternehmen, die auf externe Services setzen, ebenso wie in der KI-gestützten Cyberabwehr (48 %) und im Incident Response (62 %)

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

BEREICHE, IN DENEN FINANZDIENSTLEISTER MIT EXTERNEN DIENSTLEISTERN ZUSAMMENARBEITEN

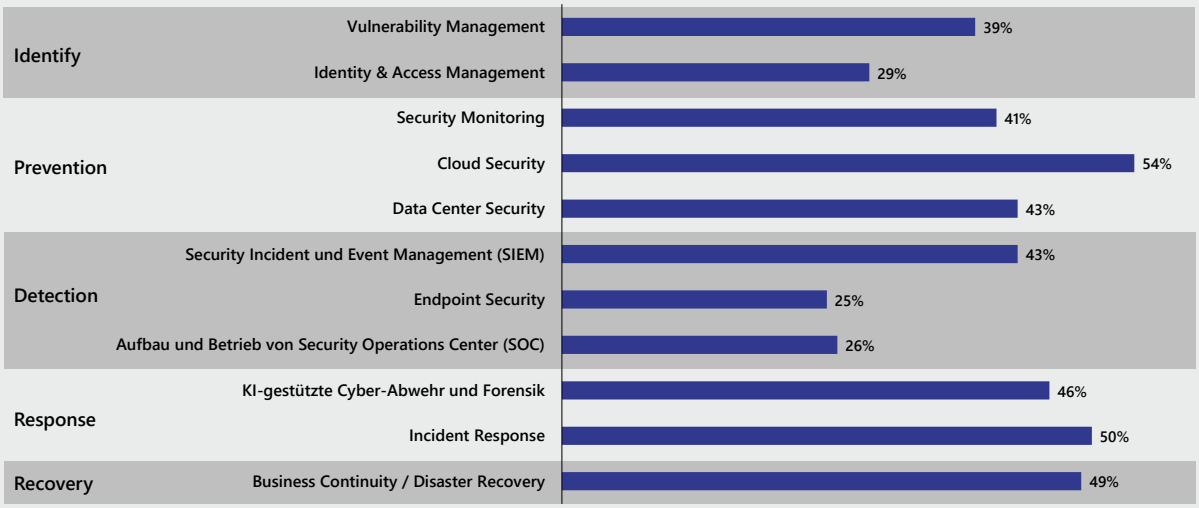


Abb. 22: Frage: Bei welchen der folgenden Themenfelder greift Ihr Unternehmen in Zukunft vermehrt auf externe Dienstleistungen zurück?; Alle Teilnehmer; Häufigkeitsverteilung; Werte beziehen sich auf die Antworten „sehr hoher Bedarf“ und „eher großer Bedarf“; Banken: n = 49; Versicherungen: n = 34; Asset Managements: n = 8

HOHER BEDARF AN MANAGED SECURITY SERVICES

Aufgrund der Vielzahl von Aufgaben und eines gleichzeitigen Mangels an Inhouse-Expertise ist seit Jahren zu beobachten, dass immer mehr Unternehmen auf sogenannte Managed-Security-Service-Provider setzen. Diese übernehmen im Rahmen der Verantwortung für das Management der hybriden und multiplen Cloud-Umgebungen auch Aufgaben rund um die IT-Security. Gerade wenn es um die zunehmende Cloud-Nutzung geht, steigt der Bedarf nach einem professionellen und regulatorikkonformen Management der Cloud-Umgebungen.

Tatsächlich bestätigt das Nachfragebarometer von Lünendonk für den deutschen IT-Dienstleistungsmarkt (siehe Lünendonk®-Studie „Der Markt für IT-Dienstleistungen in Deutschland“) diese Entwicklung: Aufgrund der immer höheren Governance-Anforderungen an die Nutzung der Cloud-Plattformen vor allem der Hyperscaler, des Mangels an Inhouse-Expertinnen und Experten und der häufig notwendigen Aufteilung von Geschäfts- und IT-Prozessen auf mehrere Clouds entscheiden sich auch im Finanzdienstleistungssektor immer mehr Unternehmen für Managed-Cloud-Service-Provider, die die technische Betreuung der IT-Landschaften übernehmen. Diese Entwicklung wird durch die Nachfrage nach IT-Services bestätigt:

Während Cyber Security 2020 noch bei 56 Prozent der durch Lünendonk in der Studie „Der Markt für IT-Beratung und IT-Service in Deutschland“ befragten IT-Dienstleister einen großen Teil der Nachfrage ausmachte, erwarten mit Blick auf 2021 und 2022 nun 72 Prozent

eine hohe Nachfrage nach Dienstleistungen rund um Cyber Security. Tatsächlich berichten viele Kundenunternehmen von massiven Problemen, Security-Expertinnen und -Experten zu rekrutieren. Demnach ist es auch nur konsequent, dass Cyber Security für 85 Prozent der Finanzdienstleister einen Investitionsschwerpunkt für die Jahre 2022–2023 bildet. 23 Prozent der befragten Finanzdienstleister werden ihre Budgets für Cyber Security sogar um mehr als 10 Prozent erhöhen, was auch durch diese Studie (siehe Kapitel 5, Abbildung 17) bestätigt wird.

NEUN VON ZEHN FINANZDIENSTLEISTERN SETZEN MITTELFRISTIG AUF MANAGED SECURITY SERVICES

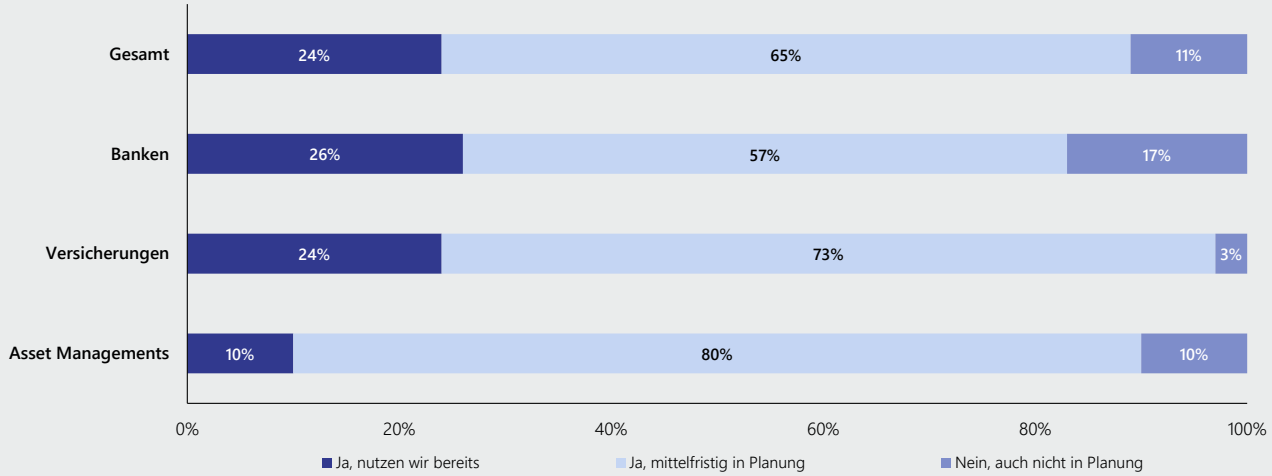


Abb. 23: Frage: Beziehen Sie bestimmte Security-Aufgaben als Managed Security Services und/oder als Security-as-a-Service?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 53; Versicherungen: n = 34; Asset Managements: n = 10

AUFGABENFELDER, IN DENEN MANAGED SECURITY SERVICES GENUTZT WERDEN

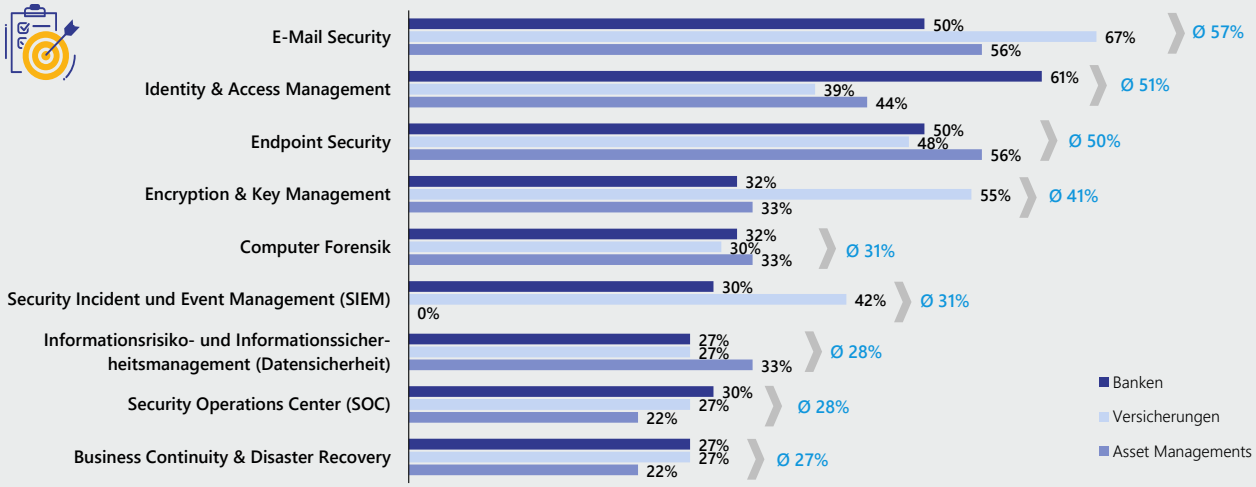


Abb. 24: Frage: Für welche Aufgabenfelder nutzen Sie als Managed Security Services oder Security-as-a-Service-Leistungen?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 44; Versicherungen: n = 33; Asset Managements; n = 9

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Den steigenden Bedarf an Managed Security Services bestätigen auch die Teilnehmer dieser Lünendonk®-Studie: 89 Prozent nutzen bereits solche Dienstleistungen oder planen mittelfristig auf sie zurückzugreifen. Besonders die befragten Versicherungen setzen nahezu vollständig auf Managed Security Services. Vor allem bei Aufgaben wie E-Mail-Security, Identity & Access Management und Endpoint Security arbeitet mehr als jeder zweite Finanzdienstleister mit Managed-Security-Service-Providern oder plant, dies zu tun.

ABRECHNUNG NACH AUFWAND IST DERZEIT DIE PRÄFERIERTE VERTRAGSFORM BEI MANAGED SECURITY SERVICES

Das gängige Vertragsmodell für Managed Security Services oder Security as a Service ist derzeit die Abrechnung nach Aufwand. 49 Prozent der befragten Finanzdienstleister setzen auf die aufwandsbasierte Abrechnung, wogegen ein Drittel (33 %) Festpreise und weitere 18 Prozent KPI-basierte Vergütungsmodelle bevorzugen. Auffällig ist, dass Versicherungen deutlich häufiger auf Festpreise und Banken sowie Vermögensverwaltungen eher auf KPI-basierte Modelle setzen.

END-TO-END-SECURITY-SERVICES VOR ALLEM BEI VERSICHERUNGEN BELIEBT

Eine Erkenntnis aus den vergangenen Cyberangriffen lautet: Mit isolierten Security-Ansätzen ist es aufgrund der komplexen Bedrohungslage und der vielschichtigen Herausforderungen rund um die Nutzung von Cloud-Services nicht getan. Auch das BSI empfiehlt, Cyber Security mehr ganzheitlich zu sehen und IT-Security-Strategien zum einen stärker mit den Business-Strategien zu verzahnen und zum anderen die Schnittkanten zwischen den einzelnen Security-Services deutlich zu reduzieren.

Gerade wenn von mehreren Providern Cloud-Dienste bezogen werden und immer mehr Workloads auf mehreren Cloud-Services aufsetzen (Multi-Cloud), kommt es darauf an, diese komplexeren Umgebungen möglichst effizient und regelkonform zu managen. Integrierte End-to-End-Lösungen, die alle Bereich der Security-Strategie abdecken, gewinnen daher an Relevanz. Jeder zweite befragte Finanzdienstleister bevorzugt einen solchen ganzheitlichen und integrierten Ansatz im Rahmen seiner Cyber-Security-Strategie. Allerdings zeigen sich Branchenunterschiede: Während 59 Prozent der Versicherungen den integrierten Ansatz präferieren, setzen nur 45 Prozent der Banken auf End-to-End-Security-Konzepte. Unter den ebenfalls befragten Vermögensverwaltungen bevorzugt immerhin jede zweite einen End-to-End-Ansatz.

TIME & MATERIAL IST BEI SECURITY-AS-A-SERVICE DAS BEVORZUGTE ABRECHNUNGSMODELL

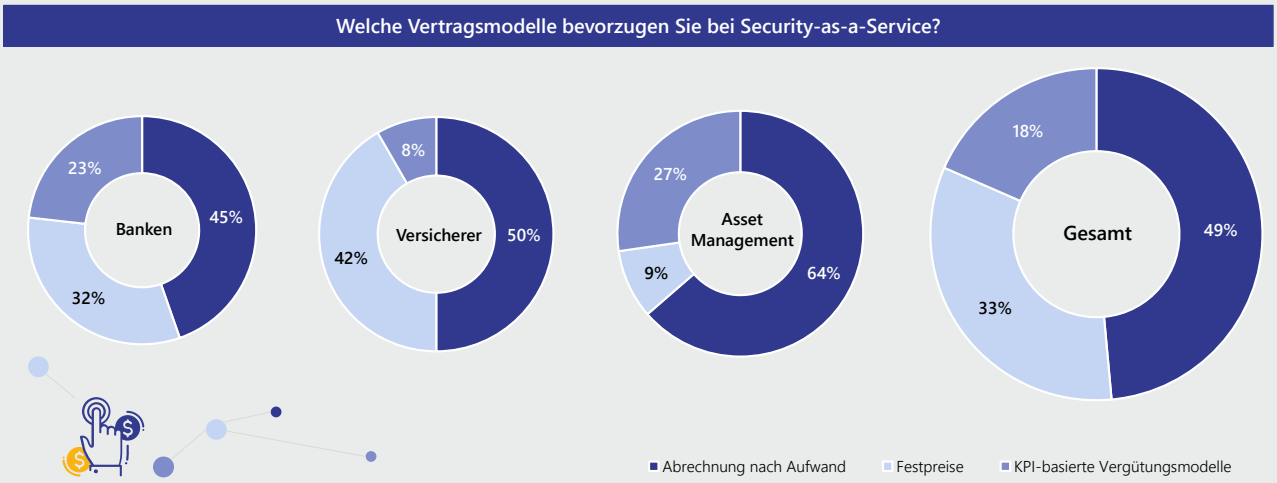


Abb. 25: Frage: Welche Vertragsmodelle bevorzugen Sie bei Security-as-a-Service?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n =41; Versicherungen: n = 32; Asset Managements: n = 8

50:50-VERTEILUNG: KEINE TENDENZ ZU INTEGRIERTEN ODER EINZELNEN SERVICES

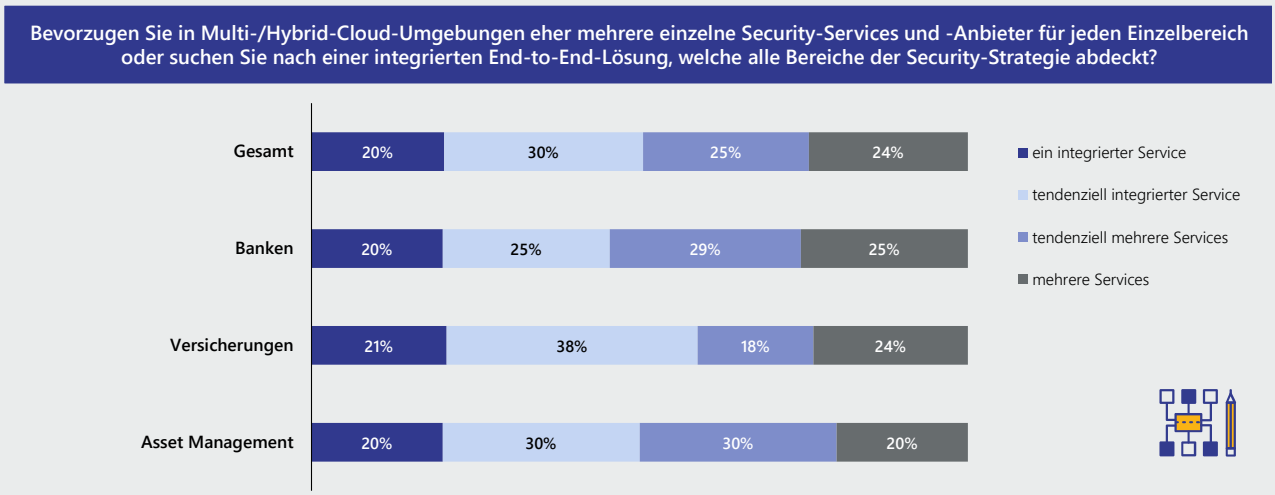


Abb. 26: Frage: Bevorzugen Sie in Multi-/Hybrid-Cloud-Umgebungen eher mehrere einzelne Security-Services und -Anbieter für jeden Einzelbereich oder suchen nach einer integrierten End-to-End-Lösung, welche alle Bereiche der Security-Strategie abdeckt?; Alle Teilnehmer; Häufigkeitsverteilung; Banken: n = 55; Versicherungen: n = 34; Asset Managements: n = 10

Fazit und Ausblick

Für die Lünendonk®-Studie „Von Cyber Security zur Cyber Resilience – wie Finanzdienstleister auf die neue Bedrohungslage reagieren" wurde auf der Basis von 100 Gesprächen – überwiegend mit IT- und Security-Verantwortlichen – analysiert, wie Banken, Vermögensverwalter und Versicherungen hinsichtlich der steigenden Bedrohungslage rund um Cyberkriminalität und Datendiebstahl aufgestellt sind.

Auffällig an den Studienergebnissen ist zunächst, dass 92 Prozent der befragten C-Level-Verantwortlichen ihre Unternehmen gut gegen Cyberangriffe geschützt sehen. Gleichzeitig rechnet aber ein ebenso hoher Anteil damit, dass ihre Unternehmen Opfer von schwerwiegenden Cyberangriffen werden können. Eine besonders große Gefahr geht laut den Befragten von Ransomware/Phishing-E-Mails (68 %) und der Nutzung unautorisierter Devices (66 %) aus. DDoS-Attacken werden von 55 Prozent der befragten Business- und IT-Entscheidenden befürchtet. Solche Angriffe, die schwerwiegende Schäden nach sich ziehen können, können aus Sicht der Mehrheit der Befragten jedoch passieren, obwohl die Unternehmensnetzwerke ausreichend geschützt sind. Nur 28 Prozent glauben, dass schwerwiegende Cyberangriffe passieren, weil die Unternehmensnetzwerke unzureichend geschützt sind.

FINANZDIENSTLEISTER KENNEN NICHT IMMER IHREN SECURITY-STATUS

Mit zunehmender Digitalisierung ihrer Geschäftsprozesse und -modelle sind Finanzdienstleister – als Betreiber von kritischen Infrastrukturen – aber einer immer größeren Bedrohung durch Internetkriminalität ausgesetzt. So entfielen im Jahr 2020 65 von 419 Meldungen von Cyberangriffen im Bereich der kritischen Infrastrukturen auf Finanzdienstleister. Vor allem DDoS-Angriffe auf IT-Infrastrukturen und Online-Dienste von Banken, Versicherungen und Vermögensverwaltungen waren zu beobachten. Besonders große Schwächen haben Finanzdienstleister laut dem BSI in der regelmäßigen Überprüfung der IT-Systeme und der technischen Informationssicherheit, aber auch hinsichtlich des organisatorischen und personellen Reifegrades. Tatsächlich überprüfen drei von zehn der untersuchten Finanzdienstleister ihre IT-Systeme nicht hinsichtlich ihres Cyber-Security-Status. Einen Ansatz mit regelmäßigen Penetrationstests der IT-Systeme verfolgen sogar nur sechs von zehn Unternehmen. Daraus folgt die Erkenntnis, dass sich ein Teil der untersuchten Finanzdienstleister bisher in trügerischer Sicherheit wähnt. Allerdings plant ein Großteil derjenigen Unternehmen, die bisher noch keine regelmäßigen Security-Tests durchführen, mit Blick auf die Zukunft nachzubessern.

DIE CLOUD VERÄNDERT DIE SICHERHEITSLAGE

Große Veränderungen kommen auf IT-Security-Verantwortliche durch die zunehmende Nutzung von Cloud-Services zu. So wirkt sich laut 83 Prozent der Befragten die intensivere Cloud-Nutzung im Finanzdienstleistungssektor auf die IT-Sicherheit aus. 84 Prozent sehen ferner durch die aufkommende Plattformökonomie eine größere Bedrohungslage auf ihre Unternehmen zukommen und für 90 Prozent verändert die Entwicklung digitaler Produkte mit einer Cloud-Architektur (Cloud-native) die IT-Risikomanagementstrategien. 95 Prozent der untersuchten Finanzdienstleister werden bis zum Jahr 2023 eine Cloud-Strategie ausgerollt haben, was bedeutet, dass sie ihre Compliance- und Risikomanagementprozesse auf die Vorgaben der Finanzaufsicht an die Cloud-Nutzung anpassen müssen. So sehen 56 Prozent der Befragten bereits heute die Notwendigkeit, aufgrund von mehr Cloud-Nutzung auch mehr in die IT-Sicherheit zu investieren. 49 Prozent der Unternehmen werden darüber hinaus ihre Security-Architektur an die höhere Komplexität durch die stärkere Nutzung von Cloud-Services anpassen.

Trotz des bereits hohen Grades an Cloud-Nutzung und der Notwendigkeit, schärfere regulatorische und gesetzliche Vorgaben zu erfüllen, enden IT-Security-Strategien in 46 Prozent der analysierten Finanzunternehmen noch an den eigenen Unternehmensgrenzen. Im Umkehrschluss bezieht aber jedes zweite Unternehmen bereits sein gesamtes Ökosystem in das IT-Security-Monitoring mit ein. Auch an dieser Stelle zeigt die Studie noch großen Handlungsbedarf in vielen Unternehmen auf, da mit Blick auf die Zukunft immer mehr digitale Geschäftsmodelle entstehen, die auch Drittanbieter mit einbeziehen. So sind beispielsweise Banken durch die PSD2 verpflichtet, ihre Schnittstellen (APIs) gegenüber Drittanbietern zu öffnen (Open Banking), um ihren Kundinnen und Kunden Zugang zu innovativen Lösungen von FinTechs oder InsurTechs zu bieten. Ebenso investieren Banken, Versicherer und Vermögensverwaltungen immer stärker in digitale Produkte wie Kunden-Apps, Online-Portale oder in plattformbasierte Ökosysteme – kurzum in die Digitalisierung der Kundenschnittstellen und der Customer Journey. Immer mehr solcher digitaler Anwendungen werden auf der Grundlage einer Cloud-native-Architektur entwickelt, woraus sich wiederum hohe Anforderungen an den Schutz der gesammelten personenbezogenen Daten ergeben. Insbesondere die Finanzaufsichtsbehörden fordern die Erfüllung bestimmter Sicherheitsstandards bei der Entwicklung digitaler Produkte.

SECURITY BY DESIGN WIRD NOCH ZU SELTEN IN DER PRODUKTENTWICKLUNG BERÜCKSICHTIGT

Security by Design, also die Berücksichtigung von Security-Elementen bereits während der Produktentwicklung, ist im Zuge von immer mehr digitalen Produkten und Services eine wichtige Kernanforderung, die Finanzdienstleister zu erfüllen haben. Aber nur 44 Prozent der befragten Unternehmen beziehen Security-Anforderungen bisher beim Design digitaler

Produkte mit ein. Allerdings planen nahezu alle anderen befragten Unternehmen, in Zukunft Security by Design in der Softwareentwicklung als integralen Bestandteil zu berücksichtigen.

UNTERNEHMEN INVESTIEREN AUFGRUND DER MASSIVEN HERAUSFORDERUNGEN IN IHRE CYBER RESILIENCE

Aus den steigenden Compliance- und Risk-Anforderungen im Zuge der digitalen Transformation ergeben sich auch steigende Ausgaben für die IT-Sicherheit. Gleichzeitig reift im Top-Management von immer mehr Unternehmen die Erkenntnis, dass die Bedrohung durch Cyberangriffe enorm hoch ist, der reine Basisschutz der IT-Infrastruktur nicht mehr ausreicht und entsprechend mehr in den Schutz der IT-Systeme investiert werden muss. Demnach wird auch bei keinem der untersuchten Finanzdienstleister im Jahr 2022 weniger Geld für die IT-Sicherheit ausgegeben. Die größten Zuwächse in den Budgets finden sich erwartungsgemäß im Identifizieren von Schwachstellen: 74 Prozent der befragten Unternehmen werden ihre Budgets für die Früherkennung potenzieller Cyberrisiken und -angriffe um bis zu 10 Prozent erhöhen. Ebenso erhöhen mehr als drei Viertel der Unternehmen ihre Budgets im Bereich der Prävention, also der Antizipation von Cyberangriffen – 17 Prozent sogar um mehr als 10 Prozent. Aber auch in den anderen Security-Bereichen (Detection, Response und Recovery) werden die Budgets in mehr als jedem zweiten befragten Unternehmen steigen.

IT-SECURITY MUSS JENSEITS DER TECHNOLOGISCHEN PERSPEKTIVE GESTEUERT WERDEN

Für einen wirksamen Schutz vor Cyberbedrohungen genügt es schon heute nicht mehr, den Fokus nur auf die Absicherung der eigenen IT-Infrastruktur zu legen. Auch die Verantwortung für IT-Security nur in der IT und bei den externen IT-Dienstleistern zu sehen wird der Bedrohungslage im digitalen Zeitalter nicht mehr gerecht. Aus den Gesprächen im Rahmen dieser Studie wird deutlich, dass eine ganze Reihe neuer interner Kompetenzen und Rollen notwendig ist, um die digitalen Geschäftsmodelle der Zukunft, aber auch den digitalen Arbeitsplatz der Zukunft abzusichern. Die Wettbewerbsstärke wird sich künftig auch im Finanzdienstleistungssektor viel stärker danach bemessen, wie sicher die Kundinnen und Kunden ihre Daten bei einem Finanzdienstleister aufgehoben sehen. Security dabei als Teil der Unternehmensstrategie und als integralen Bestandteil der Produktentwicklung im Sinne von Security by Design zu begreifen wird hier die entscheidende Rolle spielen.

Lünendonk im Interview mit KPMG zu den Studienergebnissen

CHRISTIAN NERN IST PARTNER IM BEREICH IT SECURITY FÜR FINANCIAL-SERVICES-UNTERNEHMEN UND ENTWICKELT MIT SEINEM TEAM SICHERE IT-ARCHITEKTUREN UND TECHNOLOGIEKONZEPTE IM FINANZSEKTOR. IM GESPRÄCH MIT LÜNENDONK INTERPRETIERT ER DIE STUDIENERGEBNISSE, ZEIGT INSIGHTS AUS DER PRAXIS AUF UND GIBT EMPFEHLUNGEN FÜR DEN UMGANG MIT DEN STEIGENDEN CYBER-SECURITY-BEDROHUNGEN.

CHRISTIAN NERN
Partner, Financial Services / IT Security
KPMG AG Wirtschaftsprüfungsgesellschaft

LÜNENDONK: Die Studie zeigt, dass Cyber Security ein wichtiges Thema für Ihre Mandanten ist. Was sind aus Ihrer Sicht die wichtigsten Treiber für eine steigende Relevanz von Cyber Security im Finanzdienstleistungssektor?

CHRISTIAN NERN: Remote Work wurde schon durch Covid-19 zur Regel – und ein Trend zur Digitalisierung. Diese neue Form der Zusammenarbeit und gerade auch die Ukraine-Krise führen zu vermehrten Cyberattacken, vor allem in der Form von Phishing. Dies wurde auch Anfang März durch das BSI bestätigt. Das vermehrte Remote Working bedingt auch neue Angriffsmuster, Financial-Services-Institute sind mit mehr Malware konfrontiert und werden stärker ausspioniert, um Kundendaten zu gewinnen oder in Unternehmensnetzwerke einzudringen. Unternehmen im Finanzdienstleistungsbereich besitzen ein großes Schadenspotenzial und sind dadurch ein beliebtes Angriffsziel. Deswegen muss zukünftig das Augenmerk auf der gesamten Absicherung von Finanzinstituten hinsichtlich Cyber-Attacken liegen – nicht zuletzt weil sie auch eine kritische Infrastruktur für uns in Deutschland darstellen.

"Unternehmen im Finanzdienstleistungsbereich besitzen ein großes Schadenspotenzial und sind dadurch ein beliebtes Angriffsziel."

Christian Nern
KPMG

LÜNENDONK: Wo sehen Sie die größten Bedrohungen für Finanzdienstleister in den kommenden Jahren?

CHRISTIAN NERN: Finanzdienstleister kommen aus einer Welt, in der Security als reines IT-Problem gesehen wurde, das heißt, das Thema wurde hier nur reaktiv, zum Beispiel mit Firewalls und anderen Schutzfunktionen, behandelt.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Das Thema Sicherheit wurde lange Zeit nicht proaktiv bearbeitet, obwohl es in der DNA der Finanzdienstleister liegen sollte, die Sicherheit der Kundendaten als oberste Priorität einzustufen. Das bedeutet, dass die IT-Security bei Financial-Services-Unternehmen noch kaum modernisiert und automatisiert ist. Security war in der Vergangenheit stark Compliance-getrieben, gerade weil die BaFin durch Prüfungen der BAIT/VAIT in den letzten Jahren große Anforderungen an die Unternehmen stellte.

Dennoch ist eine End-to-End Umsetzung und Vernetzung der Sicherheitslösungen nur in geringem Maße erfolgt. Gerade bei den aktuellen Digitalisierungsprojekten, die Banken und vor allem Versicherungen auf dem Tisch liegen haben, stellen wir fest, dass Digitalisierungs- und Wachstumsinitiativen nicht mit Security by Design hinterlegt sind. An Security wird erst im Nachgang gedacht. Somit stellen wir fest, dass IT-Security bis heute kein Vorstandsthema ist und weiterhin eher als reines Kosten- bzw. IT-Thema betrachtet wird.

"Security war in der Vergangenheit stark Compliance-getrieben, gerade weil die BaFin durch Prüfungen der BAIT/VAIT in den letzten Jahren große Anforderungen an die Unternehmen stellte."

Christian Nern
KPMG

Da im Bereich Financial Services in Deutschland auch oft Fachkräfte zu IT-Security fehlen, ist es noch schwerwiegender, Security als reines IT-Thema darzustellen, da alternative Ansätze wie Managed Services beziehungsweise End-to-End-Szenarien erforderlich sind.

LÜNENDONK: Immer mehr Geschäftsaktivitäten laufen online ab. Wie wirkt sich die Entwicklung von Cyber Security im Financial-Services-Sektor für den Endkunden respektive die Endkundin aus?

CHRISTIAN NERN: Die Endkundinnen und Endkunden fordern heute von Financial-Services-Instituten Apps und Services wie Online-Banking bzw. digitale Kundenerlebnisse, wobei sie von absoluter Sicherheit ihrer Daten und Transaktionen ausgehen. Neben dem Hinterlegen sensibler Kundendaten wie Adressen oder Kreditkartennummern soll die Sicherheit auch nach der Transaktion bei den Instituten gewährleistet und die Daten beispielsweise vor Diebstahl sicher sein. Das Thema Fraud bei Online-Transaktionen wird also immer wichtiger und zwingt Unternehmen im Financial-Services-Bereich sicherzustellen, dass ihre Kundinnen und Kunden keiner Gefahr ausgesetzt sind.

LÜNENDONK: Die Kunden und Kundinnen fühlen sich laut Studie grundsätzlich gut abgesichert gegenüber Cyber-Attacken (92 % fühlen sich sicher). Können Sie diesen Eindruck bestätigen?

CHRISTIAN NERN: Nach meiner Ansicht handelt es sich hier eher um einen Wunsch als um Wissen. Wenn wir in die Welt der Financial-Services-Institute blicken, stellen wir fest, dass heute kein beziehungsweise keine CIO oder CISO weiß, wie sicher er oder sie wirklich ist. Es fehlen relevante, automatisierte Security-KPIs, die tagesaktuell das Sicherheitsniveau zeigen.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

LÜNENDONK: Überrascht Sie dieses Ergebnis?

CHRISTIAN NERN: Nein, aus regulatorischer Sicht wurde prozessseitig in den letzten Jahren viel geleistet und damit eine gute Basis gelegt, nicht zuletzt weil die BaFin in diesem Bereich auch stark Vor-Ort-Prüfungen durchführt. Aus der IT-/Cyber-Security-Sicht ist das Ergebnis schon eher überraschend, da eine unternehmensweite Security-Architektur oder die Investition in moderne IT-Security-Systeme wie SOC oder IAM Incident Response, die automatisiert zusammenarbeiten, nicht im Fokus der Geschäftsführung von Financial-Services-Instituten stehen.

Eine vernetze End-to-End-Architektur rückt also immer mehr in den Fokus, die selektive Betrachtung einzelner Disziplinen schöpft nicht das Gesamtpotenzial aus. Je mehr Kontextinformationen für Sicherheitslösungen bereitgestellt werden, desto mehr Visibilität und Transparenz können die Unternehmen hinsichtlich ihrer Bedrohungslage gewinnen.

"Eine vernetze End-to-End-Architektur rückt also immer mehr in den Fokus, die selektive Betrachtung einzelner Disziplinen schöpft nicht das Gesamtpotenzial aus."

Christian Nern
KPMG

LÜNENDONK: Wie können Kundenunternehmen den Stand ihrer Security erkennen und feststellen, wie sicher sie vor Cyber-Angriffen sind?

CHRISTIAN NERN: Wenn Unternehmen von Cyber-Angriffen betroffen sind, ist es zu spät. Unternehmen müssen regelmäßig im Vorfeld ihre Bedrohungslage überprüfen und ihre Security-Systeme danach ausrichten, um mögliche Cyber-Angriffe abwehren zu können. Um dies sicherzustellen, gibt es mehrere Ansätze, angefangen bei begleitenden Reifegradanalysen zur Schwachstellenermittlung über die Anpassung der Security-Strategie und die Festlegung von Roadmaps bis hin zur gezielten Nutzung von Frameworks wie MITRE ATT&CK als Basis zur Bedrohungsmodellierung.

Grundsätzlich zum Start der Security-Planungen gilt es von der Geschäftsführung den Risikoappetit auf Basis der wichtigsten Gefahren für das jeweilige Finanzinstitut und der bereits implementierten Security Maßnahmen (Prozesse, Technologien) festzulegen.
Ein regelmäßiges und zielgerichtetes Testen auf wichtige Anwendungen und kritische Infrastrukturen – ausgehend von einer Bedrohungsmodellierung des Unternehmens – ist ebenfalls entscheidend.

Dazu kann auch das Tiber-EU Framework zur Simulation von Cyber-Angriffen genutzt werden, unter „Moderation" der BaFin. Auch spielerische „Red Team – Blue Team"-Trainings (was Security-Mitarbeitende wie bei einem Teamsport oft sehr motiviert) oder „C-Level Cyber Range"-Trainings können als weitere Security-Maßnahmen helfen.

Von Cyber Security zur Cyber Resilience - wie Finanzdienstleister auf die neue Bedrohungslage reagieren

Grundsätzlich kann ein automatisiertes Security Dashboard auf der Basis der Daten-Security-Systeme wie SOC (Security Operations Center), IAM (Identity- and Access Management), IDR (Incident Detection & Response), Firewalls, Datenbanken und weiterer die Visibilität herstellen. Basis dafür sind Top-10-KPIs, die anhand von Schwellwerten den Sicherheitsstatus eines Finanzinstituts spiegeln.

LÜNENDONK: In der Studie werden einige Möglichkeiten zur Verbesserung der Security genannt, von Technologien bis hin zu Schulungen der Mitarbeiter. Wie entscheiden Sie, was für den Kunden die beste Lösung ist?

CHRISTIAN NERN: Es gibt zwei Aspekte: Erstens stellt sich die Frage, was der moderne Marktstandard ist. Dazu gibt es gute Security Guidelines (beispielsweise vom BSI) und dementsprechend auch geeignete Berater wie etwa die KPMG AG Wirtschaftsprüfungsgesellschaft (KPMG), die das nötige Know-how von der Planung bis hin zur Provider-Auswahl zur Verfügung stellen.

"Nach heutigem Stand geschehen 50 Prozent der Security Breaches über Mitarbeitende."

Christian Nern
KPMG

Das zweite Thema ist die Mitarbeiter-Awareness. Diese ist wichtig und sollte gefördert werden, mit modernen Security-Trainings wie etwa mehrstufigen Phishing-Kampagnen auf KI-Basis. Nach heutigem Stand geschehen 50 Prozent der Security Breaches über Mitarbeitende.

LÜNENDONK: Welche Empfehlung würden Sie Unternehmen aussprechen, die sich unsicher sind, wie sie Cyber Security holistisch in ihre Unternehmensstrategie integrieren sollen?

CHRISTIAN NERN: Der Start ist hier auf jeden Fall ein ganzheitlicher Ansatz mit einem Security Assessment und einem Benchmarking auf NIST-Basis (National Institute of Standards and Technology). Als Zweites sollte man als Unternehmen der Finanzbranche definieren, welches die wichtigsten und größten Risikotreiber sind und welche Risiken akzeptiert werden können. Minimumstandards im Markt bzw. ein Benchmarking zu anderen, vergleichbaren Häusern im Markt können dabei als erste Orientierung zur Definition der Security-Risiko-Strategie und daraus abgeleiteten Prioritäten dienen.

LÜNENDONK: Wie haben Sie in der Vergangenheit erfolgreich Projekte rund um Cyber Security bei Ihren Kunden durchgeführt? Wie unterstützt KPMG Kunden konkret beim Thema Security? Und wie hebt sich KPMG dabei von Wettbewerbern ab?

CHRISTIAN NERN: Gerade die Themen, welche die Kunden in der Studie als Fokus darstellen, zum Beispiel Detection & Response oder Aufbau/Optimierung eines SOC sowie Design und fachliche, technische Implementierung eines IAM-Systems inkl. PAM (Privileged

Access Management) und auch das Design und die Umsetzung von Security-Architekturen auf Cloud-Basis sind und waren in den letzten drei Jahren Schwerpunkte unserer Arbeit. Im konzeptionellen und prozessualen Fachdesign, in der Architektur und Provider-Auswahl wie auch in der technischen Implementierung mit unseren Herstellerallianzen können wir unseren Financial-Services-Kunden bei den in der Studie aufgezeigten Security-Schwerpunkten helfen. Damit können unsere Kunden eine End-to-End Beratung im Sinne einer technischen wie auch fachlichen Umsetzung inklusive der notwendigen IT-Compliance von uns erhalten. Gerade für Financial-Services-Kunden können wir damit auf der Basis unserer Prüfungserkenntnisse im Hinblick auf Prüfungen und steigende Anforderungen der BaFin eine End-to-End-Lösung implementieren, die automatisiert dem Stand der Technik entspricht.

LÜNENDONK: Welche konkreten Bedrohungen beziehungsweise Herausforderungen sehen Sie für Ihre Kunden bei einer Cloud-Migration und wie unterstützen Sie Ihre Kunden dabei?

CHRISTIAN NERN: Gerade während der Transition zu einem oder mehreren Cloud-Providern gilt es, die Bedrohungen, die durch die Cloud-Infrastruktur und deren Spezifika entstehen oder relevanter sind, zu kennen und ihnen zu begegnen, unter anderem durch die Absicherung der Management Plane, also kontrollierter Zugang zur Verwaltungsoberfläche und deren APIs, beispielsweise durch Einsatz von Multi-Factor-Authentifizierung, die Härtung von Systemen, die Vermeidung von Fehlkonfigurationen und die Absicherung gegen Datenverlust.

KPMG nutzt dazu anerkannte Standards wie beispielsweise die Cloud Control Matrix der Cloud Security Alliance, um die Maßnahmen sowohl der Cloud-Provider als auch der Cloud-Nutzer unter Anwendung des Shared-Responsibility-Modells zu evaluieren und gegebenenfalls zu entwickeln. Darauf basierend entwickeln wir eine angepasste End-to-End-Sicherheitsarchitektur, die die Vorteile der Cloud nutzt, die Anforderungen der Kunden berücksichtigt und die Anbindung der klassischen Rechenzentren sicherstellt. Abschließend muss auch das Target Operating Model beispielsweise für das Security Incident Management aktualisiert werden, da Methoden und Vorgehensweisen zur Erkennung und Behebung von Sicherheitsvorfällen angepasst werden müssen.

LÜNENDONK: Welche Verantwortung tragen die Unternehmen selbst für die Absicherung ihrer Daten in der Cloud?

CHRISTIAN NERN: Sobald die Unternehmen in Erwägung ziehen, Cloud-Infrastruktur bzw. Cloud-Services zu nutzen, müssen sie sich ihrer Verantwortung bewusst werden und auf eine klare Aufteilung achten. Die alleinige Verantwortung liegt nicht bei den Cloud-

"Gerade während der Transition zu einem oder mehreren Cloud-Providern gilt es, die Bedrohungen, die durch die Cloud-Infrastruktur und deren Spezifika entstehen oder relevanter sind, zu kennen und ihnen zu begegnen."

Christian Nern
KPMG

Providern, wie teilweise noch fälschlicherweise vermutet wird. Beispielsweise beim Einsatz von IaaS (Infrastructure as a Service) müssen die Kunden nach wie vor für die weitere Härtung der Systeme und das Beheben von Schwachstellen sorgen.

Auch die Absicherung des Zugangs zu Systemen und Anwendungen über ein etabliertes Identity- und Access-Management-System bleibt weiterhin in der Verantwortung des Kunden, genau wie die Entwicklung sicherer Anwendungen und der Schutz der Daten.

KPMG AG Wirtschaftsprüfungsgesellschaft

KPMG ist ein weltweites Netzwerk rechtlich selbstständiger Firmen mit rund 236.000 Mitarbeitern in 145 Ländern. Auch in Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen und ist hier mit rund 12.200 Mitarbeitern an 26 Standorten präsent. Die Leistungen gliedern sich in die Geschäftsbereiche Audit, Tax, Consulting und Deal Advisory.

KPMG berät Unternehmen zu allen Fragestellungen entlang der gesamten Wertschöpfungskette, beispielsweise bei der Entwicklung neuer Geschäftsmodelle, der Optimierung der Supply Chain ebenso wie zu Steuerungskonzepten und zu Fragen rund um Digital Labour und Cyber Security. Für wesentliche Wirtschaftsbranchen hat KPMG eine bereichsübergreifende Spezialisierung vorgenommen, mit der insbesondere Familienunternehmen und Mittelstand, Staat und öffentliche Hand sowie das Finanzwesen praxisnah beraten werden.

Die Begleitung von Transformationsprojekten ist ein Kernthema der Beratung. Dabei setzt die Beratungsgesellschaft auf eine multidisziplinäre Ausrichtung der Geschäftsbereiche Audit, Tax, Transactions & Restructuring sowie Consulting. Dadurch werden Kunden in betriebswirtschaftlichen, prozessualen, steuerlichen und rechtlichen Einzelfragen beraten.

KPMG betreut Mandanten jeder Größe und aus allen Branchen – vom mittelständischen Autozulieferer über die Regionalbank bis hin zu internationalen Pharma- und Medienunternehmen.

KONTAKT

KPMG AG
Wirtschaftsprüfungsgesellschaft
Christian Nern
Partner Financial Services / IT-Security
Ganghoferstraße 29
80339 München
Telefon: +49 (089) 9282-6639
E-Mail: cnern@kpmg.com
Website: www.kpmg.de

Lünendonk & Hossenfelder GmbH

LÜNENDONK

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Management- und IT-Beratung, Wirtschaftsprüfung, Steuer- und Rechtsberatung, Facility Management und Instandhaltung sowie Personaldienstleistung (Zeitarbeit, Staffing).

Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden „Lünendonk®-Listen und -Studien" heraus.

Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalisten. Jährlich zeichnet Lünendonk zusammen mit einer Medienjury verdiente Unternehmen und Unternehmer mit den Lünendonk-Service-Awards aus.

KONTAKT

Lünendonk & Hossenfelder GmbH

Mario Zillmann
Partner
Maximilianstraße 40, 87719 Mindelheim
Telefon: +49 82 61 7 31 40 - 0
E-Mail: zillmann@luenendonk.de
Website: www.luenendonk.de

Studieninformation

www.luenendonk.de/agbs

Die hier dargestellte Studie wurde exklusiv für die KPMG Wirtschaftsprüfungsgesellschaft AG erstellt. Eine Zweitverwertung der Studienergebnisse ist nur unter Quellenangabe erlaubt. Eine Nutzung der Studie zu eigenen Marketing- oder Vertriebszwecken ist nicht gestattet.

Die Marke Lünendonk® ist geschützt und ist Eigentum des Unternehmens Lünendonk & Hossenfelder GmbH. Bei Fragen zur Studienlizenz steht Ihnen das Team von Lünendonk & Hossenfelder gerne zur Verfügung (Sekretariat@luenendonk.de).

Alle Informationen dieses Dokuments entsprechen dem Stand zum Veröffentlichungsdatum. Alle Berichte, Auskünfte und Informationen dieses Dokuments entstammen aus Quellen, die aus Sicht der Lünendonk & Hossenfelder GmbH verlässlich erscheinen. Die Richtigkeit dieser Quellen wird vom Herausgeber jedoch nicht garantiert. Enthaltene Meinungen reflektieren eine angemessene Beurteilung zum Zeitpunkt der Veröffentlichung, die ohne Vermerk verändert werden können.

Um weitere Vorteile eines Dokuments im PDF Format kennenzulernen, klicken Sie bitte auf den Hilfe-Leitfaden des Acrobat Reader, den Sie im aktuellen Dokument finden.

LÜNENDONK

ÜBER LÜNENDONK & HOSSENFELDER

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Management- und IT-Beratung, Wirtschaftsprüfung, Steuer- und Rechtsberatung, Facility Management und Instandhaltung sowie Personaldienstleistung (Zeitarbeit, Staffing). Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden „Lünendonk®-Listen und -Studien" heraus. Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalisten.

Wirtschaftsprüfung & Steuerberatung

Managementberatung

Engineering Services

Informationstechnologie

Facility Management & Instandhaltung

Zeitarbeit & Personaldienstleistung

IMPRESSUM

Herausgeber:
Lünendonk & Hossenfelder GmbH
Maximilianstraße 40
87719 Mindelheim

Telefon: +49 8261 73140-0
Telefax: +49 8261 73140-66
E-Mail: info@luenendonk.de

Erfahren Sie mehr unter www.luenendonk.de

Autor:
Mario Zillmann, Partner

Bilderquellen:
Titel, © Adobe Stock / NicoElNino