Cyberrisikomanagement

Mehr als nur Compliance

Die Bedrohung durch Cyber- und Hackerangriffe auf Unternehmen und Banken in Deutschland wächst. Folglich hat sich auch der Umgang mit IT- und Cyberrisiken verändert. Cyberrisikomanagement ist längst nicht mehr nur ein Thema der IT-Abteilung. Stattdessen rückt es immer weiter in den Fokus des Vorstands – aus gutem Grund.

Philipp Diel

Cyberattacken auf Wirtschaftsunternehmen, Behörden, Einrichtungen der kritischen Infrastruktur und auf Banken nehmen stetig zu und verursachen immense finanzielle Schäden. 2022 ist der deutschen Wirtschaft durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage ein Schaden von rund 203 Milliarden Euro entstanden, so der IT-Verband Bitkom.

Auch die BaFin hat das Thema Cyberrisiken in den vergangenen Jahren immer wieder in den Fokus der Aufsichtsschwerpunkte gesetzt. Danach nehmen Cyberattacken mit gravierenden Auswirkungen weltweit zu, so die im Januar veröffentlichten „Risiken im Fokus der BaFin 2023". Durch die voranschreitende Digitalisierung im Laufe der Coronapandemie und weltpolitische Einflüsse wie der Ukrainekrieg hat sich die Angriffsfläche für Cyberattacken stark vergrößert.

Die Bedrohung wächst der BaFin zufolge insbesondere auch für den Finanzsektor – nicht zuletzt, da Banken und Finanzdienstleister mit Geld und sensiblen Daten arbeiten. Fallen durch eine Cyberattacke kritische Funktionen wie der Zahlungsverkehr aus, kann dies die Finanzstabilität gefährden und sogar auf die Realwirtschaft ausstrahlen.

Die entscheidende Frage dabei: Wie geht man mit Cyberangriffen um und wie verhindert man große finanzielle Verluste und Reputationsschäden? Es wird deutlich, dass eine immer stärker digitalisierte Welt Institutionen und Entscheidungsträger erfordert, die aktiv Vorsorge treffen und Lösungen für diese Bedrohungen erarbeiten und bereitstellen.

Cybersicherheit fängt auf Führungsebene an

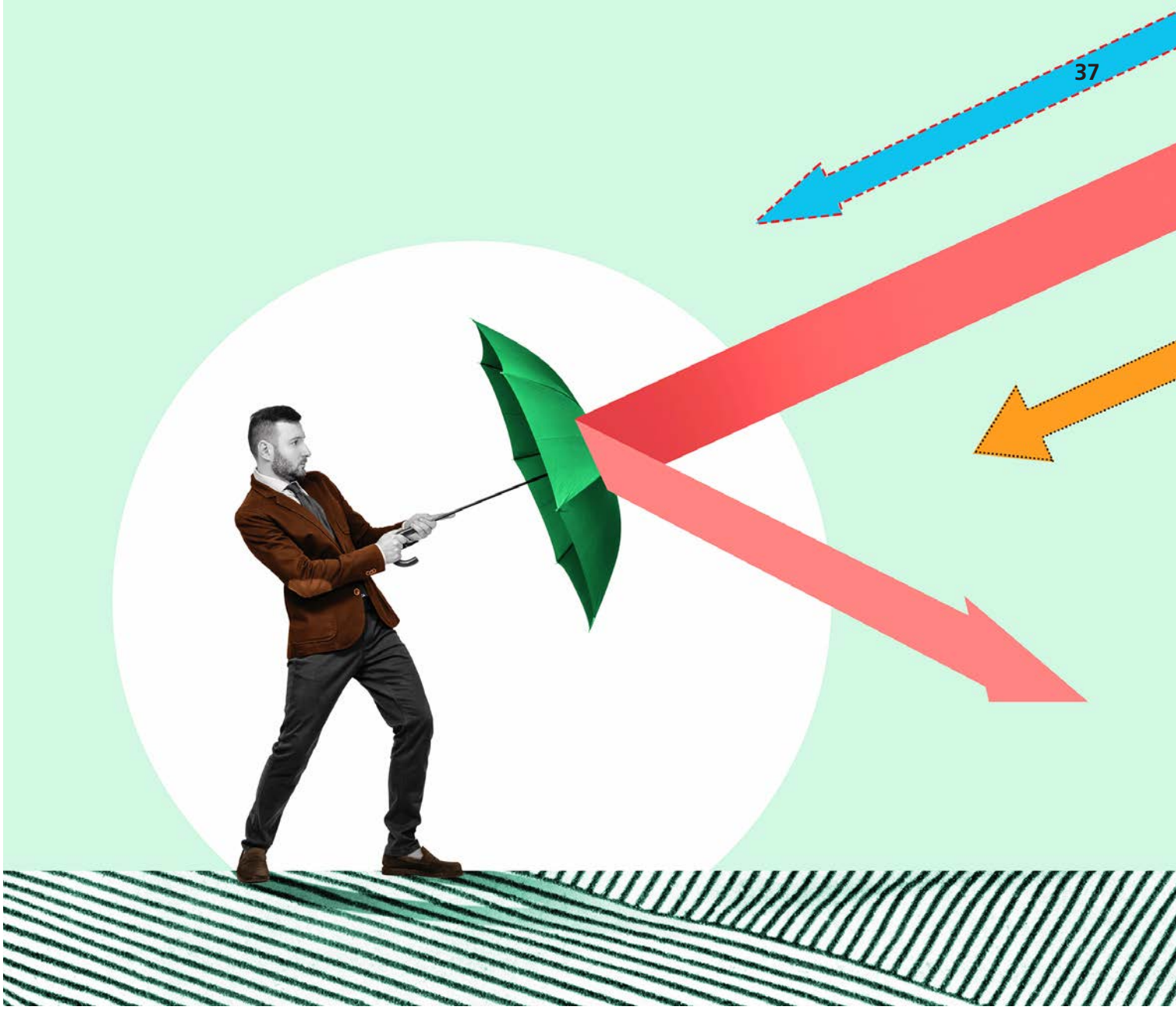
Die Gefährdung der IT-Sicherheit kann unterschiedliche Ursachen haben. Besonders häufig entstehen Sicherheitslücken aufgrund menschlicher Fehlhandlungen, da es bei vielen Mitarbeiterinnen und Mitarbeitern schlichtweg an einem entsprechenden Sicherheitsbewusstsein mangelt. Doch auch organisatorische Mängel oder technisches Versagen wie Systemabstürze und Softwarefehler können Gefahren verursachen.

Diese IT-Sicherheitslücken werden häufig für vorsätzliche und kriminelle Handlungen in Form von Hacking, Spionage oder Sabotage genutzt. In seltenen Fällen stellt auch höhere Gewalt, wie Feuer oder Erdbeben, ein erhöhtes IT-Sicherheitsrisiko dar.

Um diese Sicherheitslücken zu schließen, sind technische Optimierungen in der IT-Infrastruktur wertvoll. Doch vor allem dem Faktor Mensch kommt beim Cyberrisikomanagement eine zentrale Rolle zu. Es bedarf einer Schärfung

Philipp Diel ist Produktmanager der Managementprogramme zu den Themen Digitalisierung, IT, IT-Sicherheit und Cyberrisiken bei der ADG.

E-Mail: philipp.diel@adg-campus.de



Vor allem dem Faktor Mensch kommt beim Cyberrisikomanagement eine zentrale Rolle zu

des Gefahrenbewusstseins für Cybersicherheit auf höchster Unternehmensebene – beginnend beim Vorstand.

Eine koordinierte und umfassende Cyberstrategie transportiert dieses Gefahrenbewusstsein vom Vorstand in das gesamte Unternehmen bis zu jedem einzelnen Mitarbeiter und jeder einzelnen Mitarbeiterin, um so Cyber- und Hackerangriffe rechtzeitig zu identifizieren und ihnen entgegenzuwirken.

Rechtliche IT-Anforderungen

Das Festlegen einer nachhaltigen IT-Strategie ist für Banken und deren Geschäftsleitung nicht nur sinnvoll, sondern wird von der BaFin sogar auf bankaufsichtlicher Ebene gefordert. Die im Jahr 2017 erstmals formulierten und 2021 nochmals verschärften „Bankaufsichtlichen Anforderungen an die IT" (BAIT) konkretisieren die gesetzliche Erwartungshaltung der Aufsicht an deutsche Kreditinstitute.

Darin wird erläutert, was die BaFin unter einer angemessenen „technisch-organisatorischen Ausstattung" der IT-Systeme – insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement – versteht. Zudem werden die Anforderungen an die operative Informationssicherheit und das IT-Notfallmanagement sowie an den externen Bezug von IT-Dienstleistungen, der beispielsweise im Rahmen von Auslagerungen stetig zunimmt, in den BAIT berücksichtigt.

Basis für die Entwicklung einer IT-Strategie ist demnach eine umfangreiche IT-Governance. Die IT-Governance stellt die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen Prozesse im Rahmen der Strategie dar.

Aufbau eines IT-Notfallmanagements

Neben einer IT-Strategie und IT-Governance ist in den BAIT auch der Aufbau eines Notfallmanagements kodifiziert. Das Notfallmanagement soll dabei sicherstellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen – wie beispielsweise bei einem Hackerangriff – nicht oder nur temporär unterbrochen werden, damit die wirtschaftliche Existenz des Unternehmens auch bei einem größeren Schadenereignis gesichert bleibt. Die BaFin stellt dabei hohe Anforderungen an die zeit-

In den BAIT ist auch der Aufbau eines Notfallmanagements kodifiziert

liche Taktung und den Abdeckungsgrad von IT-Notfalltests. Sie müssen mindestens einmal im Jahr durchgeführt werden.

Mithilfe einer Business Impact Analyse (BIA) können Unternehmen überprüfen, wie sich der Ausfall eines Geschäftsprozesses und die Ausfalldauer unter verschiedenen Blickwinkeln auswirken, also wie hoch das Schadenspotenzial ist.

Auch die Bestellung eines oder einer Informationssicherheitsbeauftragten durch die Geschäftsleitung ist Gegenstand der BAIT. Dieser prüft und überwacht die Erfüllung der gesetzlichen und aufsichtsrechtlichen Bestimmungen zur IT-Sicherheit im eigenen Unternehmen. Dazu zählen auch die Erstellung einer Informationssicherheitsleitlinie und die Entwicklung eines Informationssicherheitskonzepts.

Für den Vorstand agiert der oder die Informationssicherheitsbeauftragte als Berater rund um das Thema IT-Sicherheit und schafft als Ansprechpartner für alle Mitarbeiterinnen und Mitarbeiter der Bank ein entsprechendes Gefahrenbewusstsein. Noch effektiver ist aus Sicht der BaFin die Erweiterung des IT-Sicherheitsbeauftragten durch ein ganzes IT-Sicherheitsmanagementteam.

BAIT auch bei Sonderprüfungen im Fokus

In vielen deutschen Kreditinstituten sind die BAIT-Anforderungen heute noch nicht komplett umgesetzt. IT-Sicherheitsprozesse und -systeme sind nicht standardisiert oder das entsprechende Bewusstsein in allen Bereichen eines Unternehmens noch nicht genug ausgeprägt.

Doch bankaufsichtliche Prüfungen können früher oder später jedes Institut treffen. Im Rahmen der in § 44 KWG verankerten Sonderprüfungen – häufig auch „44er-Prüfungen" genannt – müssen Institute der Aufsicht unter anderem Berichte und Auskünfte geben, sämtliche Unterlagen vorlegen und das Betreten und Besichtigen der Geschäftsräume dulden.

Die Prüfungen können sowohl aus besonderem Grund als auch als Routineprüfungen ohne einen besonderen Grund durchgeführt werden. Geprüft wird immer auf Basis von § 25a KWG – möglich auch im Hinblick auf die Umsetzung von IT-Cybersicherheitsmaßnahmen und somit die Erfüllung der BAIT-Anforderungen als Prüfungsschwerpunkt. Die Vorbereitungszeit für die Banken ist in der Regel kurz.

Haftungsrisiken für Vorstände beachten

Wird eine Institution Opfer eines Cyberangriffs, sind die Folgen meist schwerwiegend. Schnell stellt sich die Frage nach der Verantwortung. Mangelhafte Sicherheitsmaßnahmen gegen Hackerangriffe, Datenverlust, die Verletzung von Berichtspflichten – für all dies kann die Führungsebene eines Unternehmens haftbar gemacht werden. Um drohende Haftungsrisiken zu vermeiden, sollten Vorstände rechtliche IT-Sicherheitspflichten beachten.

Bei der so genannten Sorgfaltspflicht droht dem Vorstand persönliche Haftung, wenn IT-Risiken nicht angemessen identifiziert und adressiert werden und dem Unternehmen dadurch Schaden entsteht. Aus der Legalitätspflicht heraus ergeben sich Maßnahmen, um Gesetzesverstöße von Mitarbeiterinnen und Mitarbeitern zu unterbinden.

Dazu zählen Kenntnisse der Regelungen im Bereich IT-Sicherheit, Sicherheitsvorkehrungen zum Umgang mit personenbezogenen Daten sowie Schulungen der Mitarbeiter zur Sensibilisierung für IT-Sicherheit. Hier ist auch der Vorstand durch die in den BAIT formulierten Anforderungen zur Einrichtung eines Überwachungssystems und eines angemessenen IT-Risikomanagements verpflichtet.

Die persönliche Haftung entfällt nur dann, wenn der Vorstand auf Grundlage angemessener Informationen annehmen durfte, zum Wohle der Gesellschaft zu handeln („Business Judgement Rule“) oder die Entscheidung vor dem Hintergrund einer unsicheren Rechtslage getroffen wird, etwa, weil eine höchstrichterliche Rechtsprechung zu einer Streitfrage noch nicht existiert („Legal Judgement Rule“).

Cyberresilienz als Kernkompetenz entwickeln

Cybersicherheit muss auf Vorstandsebene als unternehmensweites Risikomanagement verstanden und behandelt werden, das nicht nur die IT-Abteilung betrifft. Die rechtlichen Auswirkungen von Cyberrisiken sind dabei immer vor dem Hintergrund der individuellen Anforderungen des jeweiligen Unternehmens zu berücksichtigen.

Technologisches Know-how im Cyberrisikomanagement ist Voraussetzung der Vorstandstätigkeit. IT- und Cybersicherheit sollten kontinuierlich in Vorstandssitzungen diskutiert werden. Klar ist auch: Ein unternehmensweites Cyberrisikomanagement erfordert finanzielle und personelle Ressourcen.

Es bedarf einer Risikoabwägung des Vorstands: Welche Risiken wollen wir zwingend vermeiden? Welche Risiken können akzeptiert werden? Welche Bereiche sollten wir über Cyberversicherungen schützen?

Dazu bedarf es auch des Aufbaus einer Cyberresilienz, die die Widerstandsfähigkeit von Unternehmen gegen Angriffe bezeichnet. Ziel ist es, den Regelbetrieb möglichst schnell wieder aufnehmen zu können. Cyberrresilienz zählt damit zu den Kernkompetenzen bei den Sicherheitsmaßnahmen.

Risiken erkennen und managen

„IT-Sicherheit ist so gut, wie der Mensch, der die Systeme bedient“, schreibt das Bundesamt für Informationstechnik (BSI), das den Menschen nicht als Sicherheitslücke, sondern als Abwehrschirm gegen Cyberangriffe sieht (siehe auch Artikel auf Seite 16). Als elementare Sicherheitsmaßnahme muss demnach für alle Mitarbeiterinnen und Mitarbeiter eines Unternehmens im alltäglichen Umgang mit IT-Systemen ein Problembewusstsein – eine Awareness – geschaffen werden (siehe auch Artikel auf Seite 28).

Gezielte Weiterbildungen und Qualifizierungen von Vorständen, Führungskräften und allen Mitarbeitern und Mitarbeiterinnen als Bestandteil der IT-Strategie können dazu beitragen, das Gefahrenbewusstsein für Cybersicherheit zu schärfen und darauf aufbauend eine Verhaltensänderung hin zu einem sicheren, digitalen Umgang zu erreichen.

Fest steht: Einen absoluten Schutz gegen Cyberangriffe gibt es nicht. Durch ein vorausschauendes Risikomanagement kann aber die Gefahr eines erfolgreichen Cyberangriffs erheblich reduziert und die Folgen eines Angriffs begrenzt werden. Voraussetzung hierfür ist, dass Vorstand und Geschäftsleitung dem Thema IT- und Cybersicherheit frühzeitig die erforderliche Aufmerksamkeit widmen.

Dies liegt auch im Interesse der Verantwortlichen selbst, denn im Falle eines Schadens wird schnell hinterfragt, ob die Führungsebene ihren Pflichten ausreichend nachgekommen ist. Falls nicht, drohen womöglich gravierende Haftungsrisiken.

IT- und Cybersicherheit werden häufig als lästige Compliance-Aufgabe wahrgenommen, die personelle und finanzielle Ressourcen kostet. Dabei kann durch hohe Sicherheitsmaßnahmen im digitalen Raum für Kreditinstitute und Unternehmen auch ein Wettbewerbsvorteil entstehen, beispielweise durch die Stärkung des Kundenvertrauens – gerade im Umgang mit Geld und hochsensiblen Daten im Banking. BI