Downloaded from PwC Blogs on 19.04.2025 02:43h

Trust and Technology Blog

By PwC Deutschland | 14. Februar 2024

IT-Risiken im Fokus der BaFin 2024

Am 23. Januar 2024 veröffentlichte die BaFin erneut ihren jährlichen Report zu den „Risiken im Fokus der BaFin 2024“.

Downloaded from PwC Blogs on 19.04.2025 02:43h

In ihrem Bericht hat die BaFin sieben Risiken adressiert, die die Finanzstabilität und die Integrität des deutschen Finanzsystems besonders gefährden könnten. Die BaFin teilte zusätzlich eine Pressemitteilung, in der sie die zwei IT-Risiken des Reports nochmal betonen: „Cyber-Attacken oder IT-Pannen sind aus Sicht der Finanzaufsicht BaFin eines der größten Risiken für den Finanzsektor“ (BaFin 2024).

Im Folgenden konkretisieren wir die zwei IT-Risiken.

Zunahme von Risiken durch Cyberangriffe

Weltweit nehmen Angriffe auf IT-Systeme von Unternehmen oder auf Finanzmarktinfrastrukturen durch Cyberangriffe zu. Nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die Bedrohungslage für deutsche Unternehmen im Finanzsektor so hoch wie noch nie. Insbesondere im Jahr 2023 verzeichnete das BSI einen signifikanten Anstieg von Cyberangriffen auf Finanzinstitute und deren Partnerunternehmen. Neben den Finanzunternehmen geraten auch zunehmend deren IT-Dienstleister ins Visier der Angreifer. Auch diese bieten Schwachstellen, über die auf sensible Daten oder Systeme zugegriffen werden könnte.

Cyberangriffe treten in vielfältiger Form auf. Dabei wuchs die Anzahl an Angriffen durch Schadprogramme im Jahr 2023 um täglich durchschnittlich 271.000 neue Varianten. Insbesondere Ransomware-Angriffe sind unter den Angreifern beliebt, bei denen Systeme verschlüsselt und anschließend Lösegeldforderungen gestellt werden. Diese Angriffe haben bereits zu erheblichen finanziellen Schäden und Betriebsunterbrechungen in der Finanzbranche geführt. Ebenfalls weit verbreitet sind DDoS-Attacken, die darauf abzielen, IT-Dienste zu überlasten und unerreichbar zu machen. Die Folgen solcher Angriffe reichen von finanziellen Verlusten über den Verlust des Vertrauens der Kund:innen bis hin zur Beeinträchtigung der Marktstabilität und des Finanzsystems.

Angesichts dieser Bedrohung hat die BaFin betont, bezüglich der sektorübergreifenden EU-Regulierung DORA (Digital Operational Resilience Act) bis Mitte Januar 2025 „ready“ im Sinne von prüffähig zu sein. Des Weiteren fungiert die BaFin als zentraler Melde-Hub für IKT-bezogene Vorfälle im deutschen Finanzsektor gemäß den Vorgaben von DORA. Zusätzlich arbeitet die BaFin eng mit G7-Partnern zusammen, um Orientierungshilfen zu entwickeln, die die Resilienz des Finanzsektors gegenüber Ransomware-Angriffen stärken sollen. Außerdem beabsichtigt die BaFin ein Cyber-Lagebild des Finanzsektors erstellen, das Cyber-Bedrohungen und Verwundbarkeiten von beaufsichtigten Unternehmen aufzeigen soll. Diese Maßnahmen sollen dazu beitragen, die Sicherheit und Stabilität des Finanzsektors langfristig zu gewährleisten und die Auswirkungen von Cyberangriffen zu minimieren.

Risiken durch Drittanbieter und IT-Outsourcing

Ein weiteres IT-Risiko des BaFin Reports sind Risiken durch die Auslagerung von IT-Dienstleistungen an Drittanbieter. Viele Kreditinstitute und Versicherer verlassen sich zunehmend auf externe IT-Dienstleister, um von niedrigeren Kosten und einer Erhöhung der Kapazitäten für ihr Kerngeschäft zu profitieren. Eine weitere Chance von Auslagerungen besteht darin, dass Dienstleister aufgrund ihrer Spezialisierung meist sehr effiziente und sichere Services anbieten können. Dies führt allerdings zu einer hohen Konzentration auf

Downloaded from PwC Blogs on 19.04.2025 02:43h

wenige Dienstleistern, die einen Großteil der Branche bedienen. Die BaFin mahnt, dass von solchen Mehrmandanten-Dienstleistern erhöhte Konzentrationsrisiken ausgehen.

Um diesem Risiko entgegenzuwirken, analysiert die BaFin Auslagerungen im Finanzsektor, die durch sektorweite Anzeigen gemeldet wurden. Die Anzeigepflicht für neue Auslagerungen besteht seit Ende November 2022. Zudem wertet die BaFin die Auslagerungsdatenbank regelmäßig aus, um Beziehungen zu überwachen und Verflechtungen und Konzentrationsrisiken zu identifizieren. Außerdem verstärkt die BaFin die Überwachung von IT-Mehrmandantendienstleistern und plant weitere Prüfungen, um Informationslücken bei bestehenden Auslagerungen zu schließen.

Wie können wir helfen?

Gerne können wir Sie bei den zuvor genannten IT-Risiken in allen genannten Themenfelder unterstützen – vom Assessment über die Implementierung bis zur Prüfung.

Darüber hinaus bieten wir eine umfangreiche Hilfe in der Vorbereitung auf die Einhaltung des Digital Operational Resilience Act (DORA) und anderer regulatorischer Anforderungen. Durch die Bereitstellung von Expertise in regulatorischen Fragen und Compliance helfen wir Unternehmen, sicherzustellen, dass ihre IT-Systeme und -Prozesse den neuesten Standards entsprechen und sie für zukünftige Prüfungen durch die BaFin oder andere Regulierungsbehörden optimal aufgestellt sind.

Durch die Zusammenarbeit mit PwC können Finanzunternehmen ihre Resilienz gegenüber Cyberangriffen stärken, die Risiken durch IT-Outsourcing effektiv managen und regulatorische Compliance sicherstellen, um letztlich die Sicherheit und Stabilität des eigenen Unternehmens und die des Finanzsektors zu fördern.

Mehr zu diesem Thema und allen weiteren Fokusrisiken der BaFin können Sie im BaFin Report nachlesen.

Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie hier mehr über die Möglichkeiten und Angebote.

Zu weiteren PwC Blogs

Schlagwörter

Datenschutz, Datensicherheit, Digitalisierung, IT-Sicherheit, Informationstechnologie (IT), Planung & Unternehmenssteuerung, Prozesse, Risk Management Banking, Risk Management Insurance

Kontakt

Rüdiger Giebichenstein

Köln

ruediger.giebichenstein@pwc.com