D 7465

Zeitschrift für das gesamte
KREDITWESEN

76. Jahrgang · 1. März 2023

5-2023

Pflichtblatt der Frankfurter Wertpapierbörse
Fritz Knapp Verlag · ISSN 0341-4019

Digitaler Sonderdruck

„Wir erwarten nicht, dass der Angriffsdruck in Zukunft nachlassen wird“

Redaktionsgespräch mit Sigrid Kozmiensky

CYBER SECURITY

Foto: Adobe Stock/Thaut Images

Redaktionsgespräch mit Sigrid Kozmiensky

„Wir erwarten nicht, dass der Angriffsdruck in Zukunft nachlassen wird“

Frau Kozmiensky, ist eine Zeit wie die gegenwärtige mit vielen Unsicherheiten und Unwägbarkeiten eigentlich eine gute Zeit für eine Risikovorständin, weil sie sehr gefragt ist, oder wäre Ihnen etwas mehr Berechenbarkeit lieber?

Ich denke, uns allen wäre etwas mehr Berechenbarkeit und Kontinuität lieber. Aber das Managen von Risiken ist wesentlicher Teil des Bankgeschäfts und als Risikovorständin ist es meine Aufgabe, die Bank für möglichst alle Unwägbarkeiten vorzubereiten und dafür Sorge zu tragen, dass wir innerhalb unseres Risikoappetits bleiben.

> „Die Zahl der gemeldeten Cyberangriffe war im Jahr 2021 etwa dreimal so hoch wie noch im Jahr 2015.“

Es wird im Zusammenhang mit Risiken und Risikomanagement sehr viel von der Widerstandskraft, der Operational Resilience der Banken gesprochen. Wie hält man die Widerstandskraft einer Bank angesichts so vieler Variablen, auch unbekannter, hoch beziehungsweise erhöht sie sogar immer noch weiter?

Wir überprüfen natürlich kontinuierlich alle unsere Mechanismen und Prozesse und haben umfassende Instrumente zur Identifizierung und Bewertung von neuen Risiken. Dazu testen wir regelmäßig unser Kontrollumfeld vor dem Hintergrund aktueller Bedrohungen und führen auch Stresstestszenarien durch.

Neben den Risiken aus der Kerngeschäftstätigkeit hat sich der Fokus zuletzt stark auf Business-Continuity-Aspekte verschoben: In der Pandemie gab es mögliche Risiken durch den gleichzeitigen Ausfall von großen Teilen der Belegschaft oder auch von Dienstleistern. Zuletzt gab es durch die Energiekrise infolge des Ukraine-Kriegs Herausforderungen durch eine potenzielle Einschränkung der Energieversorgung und eine potenziell erhöhte Gefährdungslage aufgrund möglicher Cyberattacken.

Welche Rolle spielt hierbei das Thema Cyberkriminalität? Viele Experten halten Cybercrime für die am meisten unterschätzte Gefahr der Zukunft – zu Recht? Wie sehr hat die Bedeutung von solchen Angriffen für das Risikomanagement in den vergangenen Jahren zugenommen?

Dass die Häufigkeit und Schwere von Cyberangriffen zunimmt, ist keine neue Beobachtung und betrifft die gesamte Wirtschaft und besonders auch den öffentlichen Sektor. Cybersecurity ist für uns als Digitalbank schon immer ein zentrales Thema und schon immer ein zentrales Element unserer Risikobetrachtung.

Durch die Pandemie und „Working from Home“ ist ein neuer Aspekt hinzugekommen. Da verstärkt Beschäftigte außerhalb der Office-Standorte arbeiten, haben wir unseren Fokus noch mehr auf die Kontinuität und Sicherheit der Online-Zugänge für unsere Mitarbeiter gelegt.

Der Schwerpunkt unserer Abwehr liegt auf „Cybercrime“. Das heißt, auf nichtstaatlichen Akteuren, die betrügerische Handlungen gegen uns und unsere Kunden unternehmen, um einen persönlichen monetären Gewinn zu erzielen. Wir setzen dabei auf ein etabliertes IT-Sicherheits- und Risikomanagement und überwachen natürlich unsere IT-Systeme und Netzwerkschnittstellen umfassend, um potenzielle Angriffe schnell erkennen und abwehren zu können. Für die Entwicklung und Überprüfung unserer Fähigkeiten spielen regelmäßige Penetrationstests und Übungen auf Basis aktueller Angriffsszenarien eine große Rolle.

Auch Basis-Schutzmaßnahmen, wie ein stringentes Berechtigungsmanagement, die Überwachung privilegierter Benutzerberechtigungen und umfassend Schwachstellen-Scans sowie zeitnahes „patchen“, sind wichtig, um ein resilientes IT-Ökosystem und ein solides Fundament für weiterführende Sicherheitsmaßnahmen zu schaffen.

Ein weiteres Element unserer Sicherheitsarchitektur, an der dutzende Experten allein im IT-Security-Management arbeiten, ist der Faktor Awareness. Diesen Faktor stärken wir kontinuierlich durch interne und externe Maßnahmen.

Wie ist die aktuelle Bedrohungssituation für Banken und ihre Kunden Ihrer Meinung nach auf einer Skala von 1 bis 100? War es schon einmal schlimmer?

Dazu hat die EZB in ihrem Stabilitätsbericht von November 2022 eine Entwicklung veröffentlicht. Demnach war die Zahl der gemeldeten Cyberangriffe im Jahr 2021 etwa dreimal so hoch wie noch im Jahr 2015, bevor sie danach wieder etwas zurückging. Der Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) von Oktober 2022 bewertet die „Gefährdungslage im Cyberraum" als so hoch, wie nie zuvor.

Wir erwarten also nicht, dass der Angriffsdruck in Zukunft nachlassen wird. Die Akteure passen ihre Fähigkeiten kontinuierlich an und es ist nicht absehbar, welchen Einfluss der Ukraine-Konflikt und zukünftige geopolitische Entwicklungen auf die Cybersicherheitslage haben werden. Aber auch wir entwickeln unsere Abwehrmechanismen kontinuierlich weiter, um auch für zukünftige Herausforderungen gewappnet zu sein.

Wenn Sie die geläufigen Arten der Bedrohung – Ransomware, Identitätsdiebstahl, Botnetze und Schadprogramme – betrachten, von welcher Art drohen die größten Risiken?

Das lässt sich pauschal nicht beantworten. Jede der genannten Arten stellt eine Bedrohung dar und jede kann zu einem Risiko werden. Wenn sie nicht frühzeitig erkannt und abgewehrt wird, kann dies neben finanziellen Schäden auch einen Reputationsschaden zur Folge haben. Erfreulicherweise sind laut dem Bericht „Risiken im Fokus der BaFin 2023" im deutschen Finanzsektor bislang keine erfolgreichen Cyberangriffe in nennenswerter Zahl festgestellt worden.

Die BaFin hat Gefahren aus der Cyberkriminalität zu einem ihrer Aufsichtsschwerpunkte 2023 erklärt. Spüren Sie davon etwas? Wie geht die Aufsicht mit Blick auf dieses Thema mit einer Bank wie der ING Deutschland um, was sind „key elements" aus Sicht der Aufsicht?

Banken müssen schon auf Basis der MaRisk und BAIT über ein IT-Sicherheits- und Risikomanagement verfügen, das im Rahmen der Jahresabschlussprüfungen auditiert wird. Die Aufsicht hat auch in der Vergangenheit bereits Prüfungen mit Schwerpunkt auf IT-Risiken und Cybersecurity durchgeführt. Auch wir merken in Gesprächen und Nachfragen, dass das Thema „Third Party und Absicherung der Lieferkette" im Fokus steht. Also welche Aktivitäten und Prozesse ausgelagert werden und ob die Dienstleister angemessen gesteuert und kontrolliert werden.

Die ING Deutschland ist nicht nur eine digitale, sondern auch eine agile Bank. Macht das Ihr Haus in besonderer Weise anfällig für kriminelle Aktivitäten aus dem Internet?

Dadurch sind wir nicht mehr im Fokus als andere Banken. Dann schon eher aufgrund unserer Größe mit über neun Millionen Kunden. Die agile Arbeitsweise unterstützt uns dabei, schnell auf neue Herausforderungen zu reagieren. So ermöglicht zum Beispiel die vernetzte Zusammenarbeit zwischen Business, IT- und Risikomanagement eine noch schnellere Kommunikation, Entscheidungsfindung und effektive Umsetzung.

„Die agile Arbeitsweise unterstützt uns dabei, schnell auf neue Herausforderungen zu reagieren."

Wie schützt sich die ING Deutschland dagegen? Welche konkreten Maßnahmen ergreifen Sie beispielsweise, um Angriffspunkten bei den Mitarbeitern im Homeoffice zu minimieren? Und wie sieht es in den Prozessen des normalen Bankalltags aus?

Ich denke, es ist nachvollziehbar, dass wir uns hierzu nicht im Detail äußern, um Kriminellen nicht nützliche Hinweise zu geben. Bei der Risikobetrachtung für das „Work from Home" waren Datenschutzbeauftragte ebenso wie die IT-Sicherheit, Information Risk Management, aber auch die Compliance-Abteilung eingebunden. Es gibt eine Reihe technischer Maßnahmen und klare Vorgaben, die wir „Leitplanken für das mobile Arbeiten" nennen.

Dazu schulen wir unsere Mitarbeiter auch kontinuierlich und ausführlich. Ge-


Foto: ING Deutschland

Sigrid Kozmiensky

Mitglied des Vorstands, ING Deutschland, Frankfurt am Main

Die Bedrohungslage für Kreditinstitute durch Cyberangriffe verschärft sich kontinuierlich. Laut aktuellem Stabilitätsbericht der EZB war die Zahl der gemeldeten Cyberangriffe im Jahr 2021 etwa dreimal so hoch wie noch im Jahr 2015. Das liegt natürlich zum einen an einem verstärkten Auftreten krimineller Gruppen, aber auch an neuen Einfallstoren für Cyberkriminelle durch Entwicklungen wie Homeoffice. All das müssen Institute berücksichtigen. Sehr digitale und agile Banken scheinen da besonders im Fokus. Aber nicht mehr als jede andere Bank auch, beruhigt die Risikovorständin im Redaktionsgespräch. Es gelte, kontinuierlich alle Mechanismen und Prozesse zu überprüfen, umfassende Instrumente zur Identifizierung und Bewertung von neuen Risiken vorzuhalten und stetig weiterzuentwickeln sowie die Mitarbeiter zu schulen. Die agile Arbeitsweise unterstütze dabei sogar, da sie es ermögliche, schnell auf neue Herausforderungen zu reagieren. Offensichtlich mit Erfolg: Laut Sigrid Kozmiensky konnten nennenswerte Schäden bislang verhindert werden. Das soll auch in Zukunft so bleiben. (Red.)

nerell lässt sich noch ergänzen, dass wir bei der Gestaltung der „Work from Home"-Rahmenparameter darauf geachtet haben, dass unser Kontrollumfeld vollumfänglich intakt bleibt.

Können Sie dabei auch von Erfahrungen anderer Institute mit Angriffen lernen, tauschen Sie sich mit den Kollegen aus?

Wir sind sehr gut innerhalb des ING-Konzerns und in der deutschen Bankenbranche vernetzt und tauschen uns permanent aus. Generell sind alle Institute und Zahlungsverkehrsdienstleister von Angriffen betroffen und arbeiten daher bei der Erkennung und Bekämpfung zusammen. Als Gründungsmitglied im Verein German Competence Centre against Cyber Crime (G4C e. V.) arbeiten wir mit weiteren Unternehmen an einem sektorübergreifenden verstärkten Erfahrungsaustausch, um Cybercrime-Bedrohungen früh zu erkennen und Lösungen zum Schutz zu etablieren. Dabei gibt es auch eine institutionalisierte Zusammenarbeit mit dem Bundeskriminalamt (BKA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Am 17. Januar 2023 ist die „Verordnung über die digitale operationale Resilienz im Finanzsektor" in Kraft getreten. Mit dem „Digital Operational Resilience Act" will die EU einen Rahmen schaffen, die IT-Sicherheit des Finanzsektors zu erhöhen und Doppelarbeiten durch nationale Vorschriften zu verringern. Wie sehen Sie das neue europäische Regelwerk zur Cybersicherheit im Finanzsektor?

„Wir begrüßen eine Harmonisierung des europäischen Regelwerks."

Als Teil der ING-Gruppe, die in über 40 Ländern aktiv ist, begrüßen wir natürlich eine Harmonisierung des europäischen Regelwerks und die damit beabsichtigte Stärkung des Ökosystems. Von dieser profitieren letztendlich alle.

Der Rahmen steht also, worauf sollte nun bei der Umsetzung in der Praxis geachtet werden?

Generell können solche Regelwerke nur einen übergeordneten Rahmen vorgeben. Die IT-Infrastruktur der einzelnen Finanzdienstleister ist sehr individuell und unterscheidet sich im Aufbau und dem Grad der Komplexität. Daher müssen die Abwehrmaßnahmen und Analysen auch immer auf die jeweiligen Systeme und Applikationen und natürlich die aktuellen Bedrohungsszenarien abgestimmt sein.

Wir finden es sinnvoll, dass auch IKT-Drittdienstleister unter die Regelung fallen und erhoffen uns dadurch, eine noch höhere Markttransparenz und vereinfachte Vertragsgestaltung.

Waren Sie selbst schon einmal Opfer eines Cyberangriffs?

Ja, wie wohl alle Organisationen mit Schnittstellen zum Internet haben wir bereits Cyberattacken feststellen müssen. Allerdings konnten wir aufgrund unserer Vorkehrungen und Maßnahmen immer sehr schnell reagieren und nennenswerte Schäden erfolgreich verhindern. Wir setzen alles daran, dass dies so bleibt.