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?