Raiffeisen Bank International
Member of RBI Group

Group Security

Technische und organisatorische Maßnahmen

Inhalt

Einführung

Sicherheit hat für die Raiffeisen Bank International höchste Priorität. Daten ihrer Kund:innen und Partner:innen werden mit größtmöglicher Sorgfalt behandelt. Um das Vertrauen in die Dienstleistungen der RBI zu gewährleisten, hat sie eine Vielzahl an technischen und organisatorischen Maßnahmen ergriffen. Der rasante Technologiewandel erfordert eine ständige Anpassung und Verbesserung der Sicherheitsmaßnahmen sowohl aus technischer als auch aus organisatorischer Sicht.

Grundlegende Sicherheitsprinzipien
Informationssicherheit zielt darauf ab, Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten. Alle technischen und organisatorischen Maßnahmen in der RBI sind darauf ausgerichtet, diese Grundsätze zu schützen.

- *Vertraulichkeit bedeutet, dass Informationen nicht an unbefugte Personen oder Unternehmen weitergegeben oder in unautorisierte Prozesse eingespeist werden.*
- *Integrität bezieht sich auf die Richtigkeit und Vollständigkeit der Informationen.*
- *Verfügbarkeit bedeutet, dass Informationen bei Bedarf zugänglich und nutzbar sind.*

Sicherheits-Framework
Um die gesetzten Ziele zu erreichen, wurde ein Rahmenwerk etabliert und wird laufend weiterentwickelt, welches als Grundlage für ein effizientes Sicherheitsprogramm dient. Das Sicherheits-Framework der RBI und ihr Informationssicherheitsmanagementsystem bestehen aus den Eckpfeilern Identifizieren, Verhindern, Erkennen, Reagieren und Wiederherstellen.

Die Raiffeisen Bank International AG ist offiziell nach ISO 27001 zertifiziert. Dabei handelt es sich um den de facto Standard für Informationssicherheitsmanagement. Somit hat die RBI alle Prozesse und Verfahren umgesetzt, die notwendig sind um Informationssicherheit angemessen strukturiert zu adressieren und kontinuierlich zu verbessern.

Strategischer Sicherheitsansatz
Die RBI entwickelt und passt ihre Sicherheitsstrategie ständig an, um neue Bedrohungen und Risiken aktiv zu identifizieren, zu bewerten und zu minimieren.

Organisatorische Maßnahmen

Neben technischen Maßnahmen müssen Prozesse sowie die darin involvierten Personen berücksichtigt werden, um das Thema Sicherheit unternehmensweit ganzheitlich angemessen zu adressieren.

Sicherheitsrichtlinien: Es gibt ein umfassendes Rahmenwerk für die Sicherheitsrichtlinien. Dieses spiegelt die Anforderungen eines dezentralen Netzwerks von Bankinstituten wider und setzt moderne Standards um. Die Sicherheitsrichtlinien werden durch den Vorstand freigeben und müssen regelmäßig auf Aktualität überprüft werden.

Sicherheitsrisikomanagement: Sicherheitsrisiken werden identifiziert, bewertet, priorisiert und behandelt. Maßnahmenpläne zur Risikominderung werden definiert, implementiert und getestet.

Kontakt zu Behörden und Interessengruppen: Die RBI steht in regelmäßigem Kontakt und arbeitet eng mit den zuständigen Behörden und Interessengruppen zusammen, um über die neuesten Sicherheitstrends und -vorschriften am Laufenden zu bleiben.

Risikomanagement für die Sicherheit Dritter: Dritte werden vor der Beauftragung risikobasiert überprüft. Vertragliche Sicherheitsanforderungen werden bei Services von Drittanbieter:innen, die ein potentielles Sicherheitsrisiko darstellen, vereinbart.

Sicherheitsbewusstsein: Alle Mitarbeitende müssen regelmäßig an Schulungen zum Thema Sicherheit teilnehmen. Zusätzlich wird eine Vielzahl an Veranstaltungen, E-Learnings, Vorträgen und andere Sicherheitsbewusstseinsbildende Maßnahmen angeboten. Die Effektivität des Programms wird unter anderem mittels „Phishing-Tests“ und „Clean Desk Checks“ überprüft.

Berufliche Entwicklung: Regelmäßige Schulungen sind unerlässlich, um mit den neuesten Technologien, Standards und Best-Practices vertraut zu sein.

Sicherheitskomitees: Sicherheitskomitees, welche Vorstandsmitglieder, die:den Chief Security Officer, die:den Chief Information Security Officer sowie weitere Personen umfassen, treffen sich regelmäßig. Diese Komitees dienen unter anderem zum Berichten und Steuern von Informationssicherheitsrisiken.

Technische (betriebliche) Maßnahmen

Informations- und Cybersicherheit

Um das Vertrauen in ihre Dienstleistungen zu bewahren, schützt die RBI ihre Geschäfts- und Kund:innendaten durch technische Maßnahmen vor unbefugtem Zugriff, Hacking-Versuchen, Malware-Infektionen, DDoS-Angriffen, Geldautomatenbetrug, Datenlecks, Phishing-Versuchen, Offenlegung sensibler Informationen und anderen Bedrohungen. Es werden Maßnahmen ergriffen, um ein angemessenes Risikoniveau in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit aller Systeme zu gewährleisten.

Cyber Threat Intelligence (CTI): Informationen über neue und potenzielle Bedrohungen werden durch Threat-Intelligence-Anbieter gesammelt, analysiert und kommuniziert, um geeignete Sicherheitsmaßnahmen abzuleiten.

Netzwerksicherheit: Systeme in Netzwerken werden durch technische und organisatorische Maßnahmen geschützt: Die Netzwerke sind segmentiert und resilient, der Netzwerkzugang ist abgesichert und der Datenverkehr wird analysiert und gefiltert.

Kryptographie: Kryptografische Maßnahmen wie Verschlüsselung sind umgesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen.

Gerätesicherheit: Die eingesetzten Endgeräte wie Notebooks und Smartphones werden verschlüsselt und zentral verwaltet. Der Zugriff auf das Firmennetzwerk ist ausschließlich mittels autorisierter Geräte möglich.

Anti-Malware- und SPAM-Schutz: Anti-Malware-Lösungen sind im Einsatz, um Schadsoftware, verdächtiges Verhalten und unerwünschte Nachrichten zu erkennen, zu verhindern und zu melden.

Zugriffskontrolle/Authentifizierung und Autorisierung: Im Rahmen des User-Lifecycle- Managements regeln definierte Prozesse das Hinzufügen, Ändern und Entfernen von Benutzer:innen-Accounts und deren Zugriffsrechte. Die Rechtevergabe erfolgt nach den Grundsätzen „need-to-know", „need-to-do" und „need-to-have". Die Zugriffsrechte werden regelmäßig überprüft und angepasst.

Passwortsicherheit: Die Komplexität und Länge der Passwörter entsprechen den aktuellen Best Practices. Um den gesteigerten Sicherheitsanforderungen gerecht zu werden, sind, wo immer es möglich ist, Maßnahmen wie Zwei-Faktor- Authentifizierung im Einsatz.

Sicherheitstests: Sowohl aus dem Internet erreichbare Systeme als auch kritische Systeme werden regelmäßig von externen, akkreditierten und angesehenen Sicherheitsunternehmen getestet.

Sichere Softwareentwicklung: Die Softwareentwicklung folgt definierten sicheren Softwareentwicklungs- und Programmierpraktiken, welche auf bewährten Industriestandards basieren. Sicherheitstests sind verpflichtender Teil des Qualitätssicherungsprozesses. Der Zugriff auf den Quellcode ist streng limitiert.

Datenklassifizierung: Die RBI hat ein Klassifizierungsmodell für Daten definiert, welches von allen RBI-Mitarbeitenden eingehalten werden muss. Darin werden das Schutzniveau und die Anforderungen an die Datenverarbeitung für jede Datenklasse genau festgelegt.

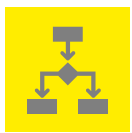
Prävention von Datenverlust: Alle Geräte sind verschlüsselt und die Verwendung externer Medien ist eingeschränkt, um Datenverlust oder Preisgabe vertraulicher Informationen zu vermeiden. Kommunikation über öffentliche Netze erfolgt verschlüsselt. Darüber hinaus gibt es mehrere Maßnahmen, um Verbindungen zu bösartigen oder unerwünschten Websites und Inhalten zu erkennen und zu blockieren.

Zero Trust: Die RBI verfolgt eine Zero-Trust-Strategie. Standardmäßig wird Systemen, Applikationen und Nutzer:innen technisch nicht vertraut. Stattdessen werden Privilegien und Zugriffsberechtigungen abhängig vom Risiko vergeben und dem Kontext entsprechend angepasst. Durch die so implementierte Mikrosegmentierung werden Netzwerke gegen Bedrohungen wie z.B. "Lateral movement" abgesichert.

Datenmaskierung (Anonymisierung): Daten in so genannten nicht-produktiven Umgebungen wie Test- und Entwicklungsumgebungen werden maskiert, um Missbrauch zu verhindern.

Schwachstellen- und Patch-Management: Sowohl interne als auch externe Schwachstellen-Scans werden regelmäßig durchgeführt, um sicherzustellen, dass Schwachstellen rechtzeitig erkannt und gemäß ihrer Kritikalität behoben werden.

Security-Monitoring: Sicherheitsrelevante Ereignisse aus unterschiedlichen internen und externen Quellen (wie z.B.: Server-, Firewall-, IDS-/IPS-, Anwendungs-Logs sowie „Indicators of Compromise") werden gesammelt und in einem Security Information and Event Management (SIEM) System korreliert und analysiert.
Das RBI-interne Cyber Defense Center ist ein wichtiger Bestandteil bei der Erkennung von Vorfällen und der Reaktion darauf. Es bietet zentralisierte Funktionen zur Prävention, Erkennung und Reaktion auf Cybersicherheitsvorfälle. Rund um die Uhr werden Aktivitäten auf den Systemen und Anwendungen auf anomale Aktivitäten, die auf einen Sicherheitsvorfall hinweisen könnten, analysiert.



Incident-Management: Ein definierter Incident-Managementprozess ermöglicht es Sicherheitsvorfälle zeitnah zu bearbeiten. Der Prozess wird regelmäßig geübt und die gewonnen Erkenntnisse fließen in die Verbesserung des Prozesses ein. Es gilt, so schnell wie möglich zum normalen Geschäft zurückzukehren sowie die Auswirkungen so gering wie möglich zu halten.

Business Continuity Management (BCM)

BCM ist ein Rahmenwerk zur Identifizierung des Gefährdungspotentials eines Unternehmens, welches internen und externen Bedrohungen ausgesetzt ist.

In der RBI ist das Ziel von BCM, die Fähigkeit zu schaffen, effektiv auf Bedrohungen zu reagieren und sicherzustellen, dass kritische Geschäftstätigkeiten trotz schwerwiegender Zwischenfälle oder Katastrophen weitergeführt werden, um die Geschäftsinteressen der Bank zu schützen. Der BCM-Lifecycle ist ein kontinuierlicher Zyklus, der die Aktivitäten des Business Continuity Programms steuert und mit dessen Umsetzung sich die organisatorische Resilienz erhöht.

Policy- und Programm-Management: Die Business Continuity Richtlinie bildet den Rahmen, auf dem das BCM-Programm konzipiert und aufgebaut ist. Es ist das wichtigste Dokument hinsichtlich Umfang und Governance.

Verankerung von Business Continuity: Business Continuity wird durch Aus- und Weiterbildung kontinuierlich in den Geschäftsalltag und die Unternehmenskultur der RBI integriert.

Analyse: Ziele, Prozesse und Einschränkungen der Betriebsumgebung, in dem die RBI tätig ist, werden überprüft und bewertet. Dazu wird als wesentliche Methode die Business Impact Analysis angewendet.

Design: Geeignete Strategien und Taktiken werden identifiziert und ausgewählt, um zu bestimmen, wie im Falle eines Ereignisses Kontinuität erreicht werden kann.

Implementierung: Die vereinbarten Strategien und Taktiken werden im Rahmen der Entwicklung der Business Continuity und Response Pläne umgesetzt.

Validierung: Business Continuity Tests bestätigen, dass das BCM-Programm die in der Richtlinie festgelegten Ziele erfüllt.

IT-Resilienz: Informations- und Kommunikationstechnologie ist für alle Aspekte des Betriebs der RBI sowohl im Bankgeschäft als auch im Nichtbankgeschäft von entscheidender Bedeutung. Desaster Recovery Pläne stellen sicher, dass IT-Systeme und deren Daten im Notfall rasch wiederhergestellt werden können. Zusätzlich wird die Widerstandsfähigkeit der IT im Rahmen Szenario basierter Tests regelmäßig auf die Probe gestellt.

Krisenmanagement: Die RBI hat einen einheitlichen Krisenmanagement Standard in der gesamten Gruppe etabliert. Die Definierung klarer Kommunikations- und Eskalationslinien ermöglicht es auf Krisen, egal welcher Art, effektiv zu reagieren und entsprechend gegenzusteuern.

Blackout: Automatische Erkennung und Alarmierung im Blackout-Fall. Implementierung von Maßnahmen auf technischer, organisatorischer und personeller Ebene, die in einem Scenario Response Plan abgebildet wurden (z.B. Notstromversorgung, Satelliten-Geräte, Dienstanweisungen, Handlungsleitfäden, etc.) sowie ein entsprechendes Awareness-Programm für relevante Zielgruppen kritischer und in weiterer Folge auch nicht-kritischer Unternehmensbereiche.

Physische Sicherheit

Physisches Sicherheitsmanagement beschränkt den physischen Zugang zu den Räumlichkeiten der RBI, um Daten und Datensysteme mit einer Mischung aus organisatorischen, baulichen und technischen Maßnahmen in einem mehrschichtigen Schutzkonzept zu schützen.

Sicherheitszonen: Die Räumlichkeiten sind in verschiedene Schutzzonen eingeteilt. Die Sicherheitsstufe einer Zone hängt von der Kritikalität der darin zu schützenden Werte ab.

Zutrittskontrollmanagement und -system: Über ein Zutrittskontrollsystem wird der Zutritt zu den Schutzzonen gewährt und verfolgt, außerdem werden die Zutrittsberechtigungen gepflegt.

Sicherheitspersonal: Sicherheitspersonal wird eingesetzt, um Probleme frühzeitig zu erkennen oder abzuwehren und fungiert gleichzeitig als Einsatzteam in der Sicherheitszentrale.

Einbruchmeldeanlage: Eine Einbruchmeldeanlage wird eingesetzt, um unbefugtes Betreten von Schutzzonen zu erkennen.

Videoüberwachung: Die Videoüberwachung unterstützt das Sicherheitsmanagement bei der Abschreckung, Erkennung und Dokumentation unberechtigter Zugriffe und jeglicher Art von unangemessenen oder rechtswidrigen Aktivitäten.

Sichere Entsorgung: Die RBI setzt ein sicheres Abfallmanagement ein, damit sensible Daten sicher zerstört werden. Geeignete Mittel werden von externen Dienstleistern bereitgestellt.