Raiffeisen Bank International

GROUP SECURITY

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Raiffeisen Bank International

Inhalt

EINFÜHRUNG.....2

ORGANISATORISCHE MAßNAHMEN.....3

TECHNISCHE (BETRIEBLICHE) MAßNAHMEN.....4

INFORMATIONS- UND CYBERSICHERHEIT.....4

BUSINESS CONTINUITY MANAGEMENT (BCM).....6

PHYSISCHE SICHERHEIT.....7

Raiffeisen Bank International AG • Am Stadtpark 9, 1030 Wien • Tel.: +43-1-71707-0 • Fax: +43-1-71707-1715 • www.rbinternational.com
Postanschrift: Postfach 50, A-1010 Wien • Sitz der Gesellschaft: Wien • Registriert unter FN 122119m beim Handelsgericht Wien
UID: ATU 57531200 • DVR: 4002771 • Swift Code: RZBAATWW • Bankleitzahl: 31000 • Mitglied der Unico Bankengruppe

Einführung

Sicherheit hat für die Raiffeisen Bank International höchste Priorität. Daten unserer Kunden und Partner 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, ist ein Rahmen erforderlich, der 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.

Seit Mitte Apri 2020 ist die Raiffeisen Bank International AG offiziell nach ISO 27001:2013 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.

Raiffeisen Bank International AG • Am Stadtpark 9, 1030 Wien • Tel.: +43-1-71707-0 • Fax: +43-1-71707-1715 • www.rbinternational.com
Postanschrift: Postfach 50, A-1010 Wien • Sitz der Gesellschaft: Wien • Registriert unter FN 122119m beim Handelsgericht Wien
UID: ATU 57531200 • DVR: 4002771 • S.W.I.F.T.-Code: RZBAATWW • Bankleitzahl: 31000 • Mitglied der Unico Bankengruppe

[1] Die hier gewählte Form bezieht – wie auch in allen weiteren Fällen – immer gleichermaßen weibliche wie männliche Personen ein. Auf eine Doppelbezeichnung wurde aufgrund einfacherer Lesbarkeit verzichtet.

Raiffeisen Bank International

Organisatorische Maßnahmen

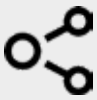
Sicherheit umfasst nicht nur technische Maßnahmen. Zusätzlich müssen Prozesse sowie die darin involvierten Personen berücksichtigt werden, um dem Thema unternehmensweit ganzheitlich angemessen zu begegnen.

	**Sicherheitsrichtlinien:** Es wird ein Rahmen für die Sicherheitsrichtlinien definiert. Dieser spiegelt die Anforderungen eines dezentralen Netzwerks von Bankinstituten wider und setzt moderne Standards um.
	**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.
	**Risiko- und Outsourcing-Management von Drittanbietern:** Jeder externe Partner wird zur Erfüllung der Sorgfaltspflicht vor der Beauftragung überprüft.
	**Sicherheitsbewusstsein:** Alle Mitarbeiter müssen regelmäßig an Schulungen zum Thema Sicherheit teilnehmen bzw. E-Learnings zu dieser Thematik absolvieren.
	**Berufliche Entwicklung:** Regelmäßige Schulungen sind unerlässlich, um mit den neuesten Technologien vertraut zu sein.

Raiffeisen Bank International

Technische (betriebliche) Maßnahmen

Informations- und Cybersicherheit
Um das Vertrauen in ihre Dienstleistungen zu bewahren, schützt die RBI ihre Geschäfts- und Kundendaten 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):** Interne und externe Spezialisten sammeln Informationen über Bedrohungen, analysieren sie und definieren entsprechende Sicherheitsmaßnahmen.
	**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 gewährleisten die Vertraulichkeit und Integrität der Daten.
	**Gerätesicherheit:** Die eingesetzten Endgeräte wie Notebooks und Smartphones werden verschlüsselt und zentral verwaltet. Der Zugriff auf das Firmennetzwerk ist nur mittels autorisierter Geräte möglich.
	**Anti-Malware- und SPAM-Schutz:** Anti-Malware-Dienste und -Systeme sind im Einsatz, um Schadsoftware und verdächtiges Verhalten 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 Benutzern und deren Zugriffsrechte. Die Zugangsrechte werden nach den Grundsätzen „need-to-know", „need-to-do" und „need-to-have" vergeben. Die Zugriffsrechte werden regelmäßig überprüft und angepasst.
	**Passwortsicherheit:** Die Komplexität und Länge der Passwörter wird nach Best Practices festgelegt und bei Bedarf adaptiert. Um den gesteigerten Sicherheitsanforderungen gerecht zu werden, sind zusätzlich Maßnahmen wie Zwei-Faktor-Authentifizierung im Einsatz.
	**Sichere Softwareentwicklung:** Die Softwareentwicklung folgt definierten sicheren Softwareentwicklungs- und Programmierpraktiken, welche auf bewährten Industriestandards basieren.

	**Sicherheitstests:** Sowohl aus dem Internet erreichbare Systeme als auch kritische Systeme werden von externen, akkreditierten, angesehenen Sicherheitsunternehmen getestet.
	**Datenklassifizierung:** Die RBI hat ein Klassifizierungsmodell für Daten definiert, welches von allen RBI-Mitarbeitern 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 über Vertriebskanäle zu vermeiden. Darüber hinaus gibt es mehrere Maßnahmen, um Verbindungen zu bösartigen oder unerwünschten Websites und Inhalten zu erkennen und zu blockieren.
	**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:** Spezielle Systeme erkennen anomale Aktivitäten, die auf Sicherheitsvorfälle hinweisen und alarmieren Experten, welche diese Vorfälle analysieren und darauf entsprechend reagieren.
	**Incident-Management:** Ein Incident-Managementprozess wurde definiert, um Sicherheitsvorfälle zeitnah zu bearbeiten. Das Hauptziel ist es, 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 wie zum Beispiel Naturkatastrophen oder Datenschutzverletzungen zu reagieren und 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 bietet 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-Pläne umgesetzt.
	**Validierung:** Business-Continuity-Tests und Disaster-Recovery-Tests bestätigen, dass das BCM-Programm die in der Richtlinie festgelegten Ziele erfüllt.

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.