Raiffeisen Landesbank Vorarlberg

INFORMATIONSSICHERHEIT

Horst Fechtig, CISO
Version: 1.0
Gültig ab: 05.02.2024

INHALTSVERZEICHNIS

1 HOHE STANDARDS ZUR SICHERHEIT IHRER DATEN

Die vertrauensvolle Zusammenarbeit mit unseren Kunden und Partnern für die Raiffeisen Landesbank Vorarlberg an vorderster Stelle. Eine Optimierung und kontinuierliche Weiterentwicklung unserer Prozesse und internen Abläufe ist für uns Selbstverständlich.

Beim Aufbau unseres Informationssicherheitsmanagementsystems (ISMS) orientieren wir uns an den Grundsätzen der Norm ISO/IEC 27001, welche zum Ziel hat Ihre und unsere vertraulichen Daten zu schützen, die Integrität der betrieblichen Daten zu gewahren und die Daten jederzeit verfügbar zu halten. Unser ISMS ist die die notwendige Basis für einen erfolgreichen Unternehmensalltag.

1.1 Organisation der Informationssicherheit

Um ein hohes Level an Informationssicherheit zu gewährleisten sind die Rollen- und Verantwortlichkeiten genau geregelt und die Aufgaben entsprechend getrennt.

Kontakte zu Behörden und Interessensgruppen sind regelmäßig gepflegt, um auf aktuellem Stand zu bleiben und gut vernetzt zu sein.

Die Planung, Umsetzung und Kontrolle von regulatorischen Anforderungen und Projekten läuft genauestens strukturiert ab, wobei auch hier die Aufgaben auf die jeweiligen Instanzen verteilt sind.

Telearbeit (Homeoffice) ist heutzutage nicht mehr wegzudenken, doch auch mit klaren Vorgaben und Regelungen verbunden. Die Arbeitsumgebung, das Ausmaß und die Verwendung bzw. Entsorgung von Daten sind klar geregelt.

1.2 Personalsicherheit

Schon bei der Auswahl des Personals legt die Raiffeisen Landesbank Vorarlberg große Sorgfalt an den Tag, um qualifizierte und motivierte Mitarbeitende zu finden. Jeder Mitarbeiter absolviert einmal jährlich eine IT-Sicherheitsschulung und erhält tourlich einen Security Awareness Letter mit aktuellen Informationen.

1.3 Verwaltung der Werte

Die Verwaltung aller Werte ist klar geregelt. Je nach Klassifizierung der Informationen, sind diese gekennzeichnet und es gibt klare Regelungen für den Umgang mit diesen.

Datenträger werden vom Beginn bis zum Ende ihres Lebenszyklus mit den notwendigen Sicherheitsvorkehrungen behandelt. Eine zeitgemäße Verschlüsselung stellt sicher, dass die Daten jederzeit bestens geschützt sind. Nachdem Ausscheiden von Datenträgern werden diese zertifiziert durch einen externen Dienstleister vernichtet.

1.4 Zugangssteuerung

Der Zugang zu unseren Systemen ist nur im jeweiligen Benutzerkontext möglich. Die Berechtigungen für unsere Mitarbeitenden sind streng nach den Prinzipien von „Need-To-Know" und „Least Privilege" vergeben. Eine Anmeldung an den Arbeitsgeräten ist generell nur über eine Multifaktor-Authentifizierung möglich. Der Zugang zum Netzwerk ist nur mit firmeneigenen Geräten gestattet, welche durch uns betrieben und gewartet werden.

1.5 Kryptographie

Um Daten, Geräte und die Verbindungen unserer Standorte zu schützen, wird eine zeitgemäße Verschlüsselung eingesetzt. So ist sichergestellt, dass die Daten nur von den Berechtigten Personen eingesehen werden können.

1.6 Physische und umgebungsbezogene Sicherheit

Es gibt verschiedene Sicherheitsbereiche im Unternehmen, die bestimmten Mitarbeiter mit den entsprechenden Rechten vorbehalten sind. Besonders wichtige Systeme sind auf mehrere Standorte verteilt, um die Verfügbarkeit zu gewährleisten.

Das Prinzip des aufgeräumten Schreibtisches, auch „Clean Desk Policy" genannt, gewährleistet die Sicherheit von analogen Informationen, die sicher versperrt oder vernichtet werden, wenn sie nicht mehr benötigt werden.

1.7 Betriebssicherheit

Geschäftsprozesse sind modelliert und Verantwortlichkeiten klar geregelt.

Ein mehrstufiger Filter vor Schadsoftware sowie ein definiertes Datensicherungskonzept unterstützen den Informationsschutz.

Ein Sicherheits- und Event Monitoring (SIEM) System überwacht die Zugriffsprotokolle und alarmiert bei verdächtigen Aktivitäten.

Das Schwachstellenmanagement überprüft alle im Netzwerk vorhandene Geräte auf Angriffsvektoren und hilft dabei, die IT-Systeme sicherheitstechnisch auf aktuellem Stand der Technik zu halten.

Softwareinstallationen und Aktualisierungen werden zentral gesteuert, geplant und ausgerollt.

1.8 Kommunikationssicherheit

Vertraulichkeits- und Geheimhaltungsvereinbarungen werden sowohl von Mitarbeitern als auch von Lieferanten eingefordert. Entsprechende Absicherung der Kommunikationswege durch Verschlüsselung und Trennung von Netzwerken sind Standard.

1.9 Anschaffung, Entwicklung und Instandhaltung von Systemen

Von der Anschaffung, über den Lebenszyklus bis zur Entsorgung von Systemen wird ein Augenmerk auf die Sicherheit gelegt und die Spezifikationen detailliert überprüft. Änderungen an bestehenden Systemen durchlaufen einen definierten Change Prozess.

Eigenentwicklungen folgen einem strikten Prozess und durchlaufen eine Reihe von Sicherheitschecks und Tests, bevor sie zum Einsatz freigegeben werden.

1.10 Lieferantenbeziehungen

Lieferantenverträge werden zentralisiert verwaltet und entsprechend den regulatorischen Vorgaben aufbereitet und abgeschlossen, wobei die Informationssicherheit des jeweiligen Lieferanten durch eine entsprechende Zertifizierung gewährleistet wird.

1.11 Handhabung von Sicherheitsvorfällen

Wenn ein Sicherheitsvorfall auftritt, gibt es klare Vorgaben zur Bearbeitung. Angefangen von der Meldung, über die Behebung bis hin zur Retrospektive, um daraus zu lernen und Maßnahmen einzuleiten.

1.12 Business Continuity Management

Im Falle der Beeinträchtigung eines wichtigen Dienstes ist gewährleistet, mundass der Geschäftsbetrieb fortgeführt werden kann bzw. die Beeinträchtigung so klein wie möglich gehalten wird. Umgesetzte Maßnahmen, redundante Standorte und regelmäßige Übungen unterstützen uns dabei, unsere Dienste zuverlässig und integer zur Verfügung zu stellen.

1.13 Compliance

Die Einhaltung gesetzlicher und vertraglicher Vorgaben ist eine Selbstverständlichkeit.

Die Privatsphäre unserer Kunden und Mitarbeitenden und der Schutz ihrer personenbezogenen Informationen hat oberste Priorität.

Die Informationssicherheit ist integraler Bestandteil der Raiffeisen Landesbank Vorarlberg.