

# Security Audit

Wir stellen Ihre Sicherheit auf den Prüfstand

## Prozessorientierung im Fokus

Die IT bildet heute unsere gesamten Geschäftsprozesse ab und unterstützt dabei generell den reibungslosen Ablauf des operativen Geschäftes. Bereits ein teilweiser Ausfall der IT gefährdet den Erfolg einzelner Geschäftsprozesse. Daher ist es wichtiger denn je, eine sichere IT-Infrastruktur zu betreiben. Aus diesem Grund entspricht es dem Best Practice, die IT-Infrastruktur in regelmäßigen Abständen einer technischen Sicherheitsüberprüfung zu unterziehen.

Security Audits liefern hier den geeigneten Input: durch maßgeschneiderte Sicherheitsüberprüfungen wird das Sicherheitsniveau bewertet und Sicherheitsschwachstellen werden identifiziert. Die durch Raiffeisen Informatik systematisch durchgeführte Sicherheitsüberprüfung führt sehr rasch zu professionellen Ergebnissen.

## Sicherheit hat viele Gesichter

Die Maßnahmen zum Schutz Ihrer IT und Ihrer Daten sind so vielfältig und individuell wie Ihr Unternehmen selbst. Sie können daher aus einer breiten Palette von Einzelmaßnahmen wählen. Dabei orientieren Sie sich an unterschiedlichen Standards zur Etablierung Ihres Sicherheitsniveaus.

Um das Sicherheitsniveau und die Wirksamkeit unterschiedlicher Sicherheitsmaßnahmen zu messen und zu bewerten, kommen eine Vielzahl an Methoden und Werkzeugen zum Einsatz. Als Ergebnis liefern wir Ihnen eine transparente Aufbereitung der notwendigen Empfehlungen und Maßnahmen.

## Sicherheit erfordert kompetente Partner

Mit unserer langjährigen Erfahrung identifizieren wir umfassend Risiken und Sicherheitschwachstellen. Die Ermittlung des tatsächlichen Risikopotentials erfolgt manuell oder semi-automatisch. Daher können identifizierte Risiken in Live- oder Proof-of-Concept Demonstrationen Entscheidungsträgern und Verantwortlichen veranschaulicht werden. So wird der Grundstein für die Umsetzung zusätzlicher Sicherheitsmaßnahmen gelegt.

Wir bieten unterschiedliche Dienstleistungen beginnend bei einer Basissicherheitsüberprüfung mit allgemeinem Fokus bis hin zum spezialisierten Penetration Test (Security Audit aus der Perspektive und mit den Mitteln realer Angreifer). Dafür stimmen wir vorab die Zielsetzungen für eine detaillierte Überprüfung einzelner Bereiche und Systeme der vorhandenen IT-Landschaft ab. Durch unsere professionelle Aufbereitung der Ergebnisse erhalten Sie sofort einen genauen Überblick.



## Der konkrete Nutzen

Die Durchführung von Security Audits durch die Security Analysten der Raiffeisen Informatik bringt Ihnen vielfältigen Nutzen:

- Identifikation von Sicherheitsschwachstellen und von Maßnahmen
- Unabhängige Security Analyse zur Qualitätssicherung
- Compliance-Nachweis anerkannter Standards z. B. ISO 27001
- Direkte und indirekte Kosteneinsparung durch Vorbeugung von Störfällen
- Einmalige oder regelmäßige Momentaufnahmen der Effektivität und des Reifegrades der Sicherheitsmaßnahmen

## Unsere Erfahrung überzeugt

Sicherheit steht für uns als Rechenzentrumsbetreiber mit einer 40-jährigen Erfahrung an erster Stelle. Dieses Wissen geben wir als Dienstleistung an unsere Kunden weiter. Unsere Spezialisten aus dem Security Competence Center betrachten sämtliche Aspekte im Bereich Sicherheit und sorgen somit dafür, dass Sie sich wieder ausschließlich Ihrer Kernkompetenz widmen können.

Gegen identifizierte Sicherheitsprobleme und -schwachstellen stellen wir Maßnahmenempfehlungen zusammen, die sich nach unserer eigenen Erfahrung oder dem allgemeinen Best Practice bewährt haben. Sind diese Maßnahmen umgesetzt, kann deren Wirksamkeit durch einen abschließenden Re-Check sichergestellt werden.

## Immer einen Schritt voraus

Als erster österreichischer IT Services Provider ist Raiffeisen Informatik offiziell Mitglied beim „Forum of Incident Response and Security Teams“ (FIRST) – dem internationalen Dachverband für IT Security Teams. Dieser Verband unterstützt die Zusammenarbeit des Raiffeisen Informatik Security Competence Centers mit den anderen Security Teams. Ziel ist es, sicherheitsrelevante Informationen (z. B. über neue Malware, Angriffe, Schwachstellen) zeitnah zu erfahren und die Behebung von Sicherheitsproblemen zu beschleunigen.

Die nationale und internationale Vernetzung ermöglicht uns Zugang zu den neuesten Informationen und Best-Practise Verfahren. Dadurch können wir bei Sicherheitsvorfällen frühzeitig Maßnahmen ergreifen.