



|   |   |
|---|---|
| <b>Author</b>   | <b>Dipl.-Ing. Daniel Mrskos, BSc</b>  |
| <b>Funktion</b>   | CEO von Security mit Passion, Penetration Tester, Mentor, FH-Lektor, NIS Prüfer   |
| <b>Datum</b>  | 04. Juli 2024   |
|  |    |
| <b>Zertifizierungen</b>   | CSOM, CRTL, eCPTXv2, eWPTXv2, CCD, eCTHPv2, CRTE, CRTO, eCMAP, PNPT, eCPPTv2, eWPT, eCIR, CRTP, CARTP, PAWSP, eMAPT, eCXD, eCDFP, BTL1 (Gold), CAPEN, eEDA, OSWP, CNSP, Comptia Pentest+, ITIL Foundation V3, ICCA, CCNA, eJPTv2, Developing Security Software (LFD121), CAP, Checkmarx Security Champion |
| <b>LinkedIN</b>   | <a href="https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/">https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/</a>   |
| <b>Website</b>  | <a href="https://security-mit-passion.at">https://security-mit-passion.at</a>   |

## Prozessbeschreibung: Überprüfung der Sicherheit der IT-Systeme

### Prozessname

Überprüfung der Sicherheit der IT-Systeme

### Prozessverantwortliche

- Max Mustermann (IT-Sicherheitsbeauftragter)
- Erika Mustermann (Leiterin IT-Abteilung)

### Ziele des Prozesses

Dieser Prozess hat das Ziel, die Sicherheit der IT-Systeme der Bank regelmäßig zu überprüfen, um Sicherheitslücken zu identifizieren, die Einhaltung der Sicherheitsrichtlinien sicherzustellen und die IT-Infrastruktur gegen Bedrohungen zu schützen.

## **Beteiligte Stellen**

- IT-Abteilung
- Compliance-Abteilung
- Externe Dienstleister (falls erforderlich)

## **Anforderungen an die auslösende Stelle**

Die Überprüfung der IT-Sicherheit wird ausgelöst durch: - Regelmäßige Wartungszyklen (monatlich, quartalsweise, jährlich) - Sicherheitsvorfälle oder -bedrohungen - Änderungen in den regulatorischen Anforderungen - Erkenntnisse aus internen oder externen Audits

## **Anforderungen an die Ressourcen**

- Sicherheitsscanning-Tools und Monitoring-Software
- Fachliche Expertise in IT-Sicherheitsprüfungen und -bewertungen
- Dokumentationssysteme für Prüfberichte und Maßnahmenpläne

## **Kosten und Zeitaufwand**

- Regelmäßige Sicherheitsüberprüfungen: ca. 20 Stunden pro Zyklus
- Ad-hoc-Überprüfungen bei Sicherheitsvorfällen: variiert je nach Vorfall (durchschnittlich 10-30 Stunden)

## **Ablauf / Tätigkeit**

### **1. Initiierung und Planung**

- Verantwortlich: IT-Sicherheitsbeauftragter
- Beschreibung: Planung der regelmäßigen Sicherheitsüberprüfungen, Festlegung von Terminen und Ressourcenbedarf.

### **2. Durchführung der Sicherheitsüberprüfungen**

- Verantwortlich: IT-Abteilung
- Beschreibung: Einsatz von automatisierten Sicherheitsscanning-Tools zur Überprüfung der IT-Systeme auf bekannte Schwachstellen. Durchführung manueller Sicherheitsprüfungen und Penetrationstests.

### **3. Analyse und Bewertung der Ergebnisse**

- Verantwortlich: IT-Sicherheitsbeauftragter
- Beschreibung: Analyse der identifizierten Schwachstellen, Bewertung der Risiken und Priorisierung basierend auf Schweregrad und potenziellen Auswirkungen.

#### **4. Berichterstattung und Kommunikation**

- Verantwortlich: IT-Sicherheitsbeauftragter
- Beschreibung: Erstellung von Berichten über die Ergebnisse der Sicherheitsüberprüfungen und deren Bewertung. Information der relevanten Abteilungen und der Geschäftsführung über kritische Sicherheitslücken.

#### **5. Entwicklung und Umsetzung von Maßnahmenplänen**

- Verantwortlich: IT-Abteilung
- Beschreibung: Entwicklung von Maßnahmenplänen zur Behebung der identifizierten Schwachstellen. Umsetzung der Maßnahmen in Zusammenarbeit mit den betroffenen Abteilungen und externen Dienstleistern.

#### **6. Überprüfung und Validierung**

- Verantwortlich: IT-Sicherheitsbeauftragter
- Beschreibung: Überprüfung der Wirksamkeit der umgesetzten Maßnahmen durch erneute Sicherheitsüberprüfungen und Tests. Validierung, dass die Schwachstellen behoben wurden.

#### **7. Dokumentation und Nachverfolgung**

- Verantwortlich: IT-Sicherheitsbeauftragter
- Beschreibung: Vollständige Dokumentation aller durchgeführten Sicherheitsüberprüfungen, identifizierten Schwachstellen, durchgeführten Maßnahmen und Ergebnisse der Überprüfungen. Regelmäßige Nachverfolgung zur Sicherstellung der langfristigen Wirksamkeit der Maßnahmen.

## Prozessgrafik



## Dokumentation

Alle Schritte und Entscheidungen im Prozess werden dokumentiert und revisionssicher archiviert. Dazu gehören: - Sicherheitsüberprüfungsberichte und Prüfprotokolle - Risikoanalysen und Priorisierungsberichte - Maßnahmenpläne und Umsetzungsprotokolle - Validierungsberichte und Nachverfolgungsprotokolle

## Kommunikationswege

- Regelmäßige Berichte an die Geschäftsführung über den Status der IT-Sicherheit und durchgeführte Maßnahmen
- Information der beteiligten Abteilungen über kritische Schwachstellen und Maßnahmenpläne durch E-Mails und Intranet-Ankündigungen
- Bereitstellung der Dokumentation im internen Dokumentenmanagementsystem

