Author	Dipl.-Ing. Daniel Mrskos, BSc
Funktion	CEO von Security mit Passion, Penetration Tester, Mentor, FH-Lektor, NIS Prüfer
Datum	04. Juli 2024
	
Zertifizierungen	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
LinkedIN	https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/
Website	https://security-mit-passion.at

Prozessbeschreibung: Sicherstellung der Sicherheit im Home-Office

Prozessname

Sicherstellung der Sicherheit im Home-Office

Prozessverantwortliche

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

Ziele des Prozesses

Dieser Prozess hat das Ziel, die Sicherheit der IT-Infrastruktur und der sensiblen Daten der

Bank zu gewährleisten, während Mitarbeitende von zu Hause arbeiten.

Beteiligte Stellen

- IT-Abteilung
- Compliance-Abteilung
- Fachabteilungen
- Personalabteilung

Anforderungen an die auslösende Stelle

Die Sicherstellung der Sicherheit im Home-Office wird ausgelöst durch: - Einführung oder Ausweitung von Home-Office-Regelungen - Änderungen in der Bedrohungslage - Sicherheitsvorfälle im Zusammenhang mit Home-Office - Regelmäßige Überprüfungen und Audits

Anforderungen an die Ressourcen

- VPN-Software und -Hardware
- Endpoint Security Software
- Multifaktor-Authentifizierung (MFA)
- Schulungs- und Informationsmaterialien
- Dokumentationssysteme für Sicherheitsrichtlinien und -protokolle

Kosten und Zeitaufwand

- Einmalige Implementierung von Home-Office-Sicherheitsmaßnahmen: ca. 20-40 Stunden
- Regelmäßige Überprüfungen und Schulungen: ca. 5-10 Stunden pro Monat

Ablauf / Tätigkeit

1. **Planung und Vorbereitung**
    - Verantwortlich: IT-Sicherheitsbeauftragter
    - Beschreibung: Erstellung eines Sicherheitsplans für das Home-Office, der alle relevanten Systeme und Anwendungen abdeckt. Festlegung der Verantwortlichkeiten und Zeitpläne für die Implementierung der Sicherheitsmaßnahmen.
2. **Bereitstellung sicherer Zugangsmöglichkeiten**
    - Verantwortlich: IT-Abteilung
    - Beschreibung: Implementierung von VPN-Lösungen für den sicheren Remote-

Zugriff auf das Unternehmensnetzwerk. Sicherstellung, dass alle Remote-Verbindungen verschlüsselt sind.

3. **Implementierung von Endpoint Security**
    - Verantwortlich: IT-Abteilung
    - Beschreibung: Installation und Konfiguration von Endpoint Security Software auf den Geräten der Mitarbeitenden, einschließlich Antivirus, Antimalware und Firewalls.

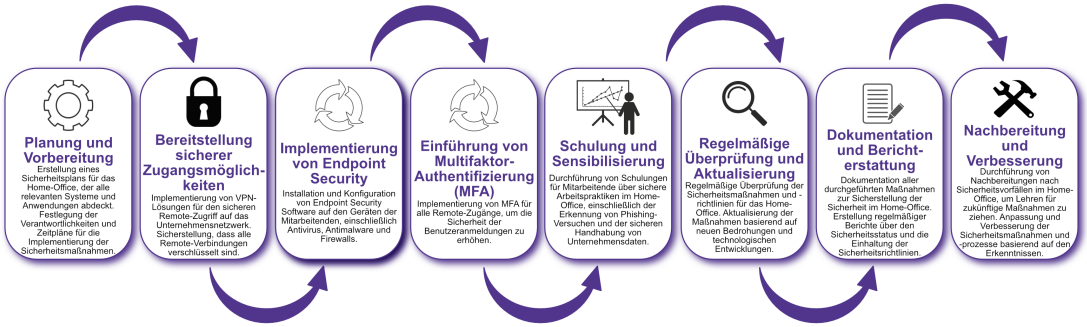
4. **Einführung von Multifaktor-Authentifizierung (MFA)**
    - Verantwortlich: IT-Abteilung
    - Beschreibung: Implementierung von MFA für alle Remote-Zugänge, um die Sicherheit der Benutzeranmeldungen zu erhöhen.

5. **Schulung und Sensibilisierung**
    - Verantwortlich: Personalabteilung, IT-Abteilung
    - Beschreibung: Durchführung von Schulungen für Mitarbeitende über sichere Arbeitspraktiken im Home-Office, einschließlich der Erkennung von Phishing-Versuchen und der sicheren Handhabung von Unternehmensdaten.

6. **Regelmäßige Überprüfung und Aktualisierung**
    - Verantwortlich: IT-Sicherheitsbeauftragter
    - Beschreibung: Regelmäßige Überprüfung der Sicherheitsmaßnahmen und -richtlinien für das Home-Office. Aktualisierung der Maßnahmen basierend auf neuen Bedrohungen und technologischen Entwicklungen.

7. **Dokumentation und Berichterstattung**
    - Verantwortlich: IT-Sicherheitsbeauftragter
    - Beschreibung: Dokumentation aller durchgeführten Maßnahmen zur Sicherstellung der Sicherheit im Home-Office. Erstellung regelmäßiger Berichte über den Sicherheitsstatus und die Einhaltung der Sicherheitsrichtlinien.

8. **Nachbereitung und Verbesserung**
    - Verantwortlich: IT-Sicherheitsbeauftragter
    - Beschreibung: Durchführung von Nachbereitungen nach Sicherheitsvorfällen im Home-Office, um Lehren für zukünftige Maßnahmen zu ziehen. Anpassung und Verbesserung der Sicherheitsmaßnahmen und -prozesse basierend auf den Erkenntnissen.



Dokumentation

Alle Schritte und Entscheidungen im Prozess werden dokumentiert und revisionssicher archiviert. Dazu gehören: - Sicherheitspläne und Zeitpläne - Protokolle zur Bereitstellung sicherer Zugangsmöglichkeiten - Endpoint Security Konfigurationsprotokolle - MFA-Implementierungsprotokolle - Schulungsunterlagen und Teilnehmerlisten - Berichte und Kommunikationsergebnisse

Kommunikationswege

- Regelmäßige Berichte an die Geschäftsführung über den Status der Sicherheit im Home-Office und durchgeführte Maßnahmen
- Information der beteiligten Abteilungen über Sicherheitsrichtlinien und Änderungen durch E-Mails und Intranet-Ankündigungen
- Bereitstellung der Dokumentation im internen Dokumentenmanagementsystem