Checkliste zur Identifizierung und Vermeidung von Schatten-IT

1. Bewusstsein schaffen und schulen

- [x] **Schulung:** Regelmäßige Schulungen der Mitarbeitenden über die Risiken und Konsequenzen von Schatten-IT.

- [x] **Sensibilisierung:** Vermittlung der Notwendigkeit, nur genehmigte IT-Ressourcen zu verwenden.

2. Implementierung strikter Richtlinien

- [x] **Richtlinien:** Einführung klarer Richtlinien und Verfahren zur Nut zung von IT-Ressourcen.

- [x] **Verständnis:** Sicherstellen, dass alle Mitarbeitenden die Richtlinien kennen und verstehen.

3. Regelmäßige IT-Inventarisierung

- [x] **Software-Inventory:** Erstellen einer vollständigen Liste aller offiziell genehmigten Software und Anwendungen.

- [x] **Hardware-Inventory:** Dokumentation aller offiziellen Geräte wie Computer, Mobilgeräte, Server und Netzwerkequipment.

4. **Monitoring und Auditing**

- **Netzwerküberwachung:** Überwachung des Netzwerkverkehrs auf ungewöhnliche Verbindungen und Datenübertragungen.
- **Log-Analyse:** Überprüfung der Logs auf ungewöhnliche Aktivitäten oder Zugriffe.
- **Monitoring-Tools:** Einsatz von Tools zur Überwachung von Software-Installationen und -Nutzung.

5. **Mitarbeiterbefragungen und Schulungen**

- **Befragungen:** Durchführung von Befragungen, um die Nutzung zusätzlicher Software oder Geräte zu ermitteln.
- **Sensibilisierung:** Regelmäßige Schulungen zu Risiken und Richtlinien bezüglich Schatten-IT.

6. **Überprüfung der Anwendung von Sicherheitsrichtlinien**

- **Cloud-Dienste:** Überprüfung der Nutzung nicht genehmigter Cloud-Dienste oder -Speicherlösungen.
- **Zugriffsrechte:** Sicherstellung angemessener Zugriffsrechte auf Anwendungen und Daten.
- **Mobile Geräte:** Registrierung und Sicherung aller mobilen Geräte, die auf Unternehmensdaten zugreifen.

7. Auswahl und Einsatz sicherer Messaging-Lösungen

- **Vermeidung von Risiken:** Einsatz kontrollierter und sicherer Kommunikationslösungen wie Teamwire.

- **Datenschutz und Sicherheit:** Sicherstellen, dass die eingesetzten Lösungen Datenschutzstandards wie der DSGVO und den Sicherheitsanforderungen der Organisation entsprechen.

8. Technische Maßnahmen und Tools

- **Firewalls und Proxy-Server:** Implementierung von Firewalls und Proxy-Servern zur Kontrolle unerlaubter Zugriffe.

- **Endpoint Management:** Einsatz von Endpoint Management-Tools zur Kontrolle von Geräten und Software.

- **Data Loss Prevention (DLP):** Implementierung von DLP-Lösungen zur Überwachung und Kontrolle sensibler Daten.

9. Kontinuierliche Überwachung und Anpassung

- **Regelmäßige Audits:** Durchführung regelmäßiger Audits und Reviews der IT-Infrastruktur.

- **Richtlinien-Updates:** Anpassung der IT-Richtlinien an neue Technologien und Bedrohungen.

- **Feedback-Mechanismen:** Einführung von Mechanismen zur Meldung unsicherer oder ungewöhnlicher IT-Nutzung.

10. Sicherstellung der Einhaltung gesetzlicher Vorgaben

- **Compliance-Überprüfung:** Sicherstellung der Übereinstimmung aller IT-Systeme und -Prozesse mit gesetzlichen Anforderungen.

- **Dokumentation und Berichtswesen:** Gründliche Dokumentation aller Systeme, Prozesse und Audits mit regelmäßiger Berichterstattung an die Geschäftsführung.

11. Zusammenfassung und Maßnahmenplan

- **Identifikation:** Auflistung aller identifizierten Schatten-IT-Systeme

- **Risikobewertung:** Bewertung der potenziellen Risiken durch diese Systeme.

- **Gegenmaßnahmen:** Entwicklung eines Plans zur Integration, Sicherung oder Entfernung von Schatten-IT.