CHECKLISTE DATENSICHERHEIT

CHECKLISTE DATENSICHERHEIT

Einführung

Die nachfolgende Checkliste hilft Ihnen dabei, die wichtigsten Aspekte der Datensicherheit in Ihrem Unternehmen systematisch zu überprüfen. Die Fragen sind nach Priorität geordnet:

- 🔴 **= Kritisch (sofortiger Handlungsbedarf)**
- 🟠 **= Wichtig (mittelfristig umsetzen)**
- 🟢 **= Wünschenswert (langfristige Optimierung)**

Inhalt

Teil 1: Backup und Notfallvorsorge

Frage	Ja	Nein	Priorität
Wird regelmäßig ein Backup der wichtigsten Unternehmensdaten erstellt?	☐	☐	🔴
Wird das Backup an unterschiedlichen Orten gespeichert (Unternehmen, extern, Cloud)?	☐	☐	🔴
Ist das Backup gegen Diebstahl oder Zerstörung (Brand, Wasserschaden) geschützt?	☐	☐	🔴
Ist sichergestellt, dass eine Rücksicherung jederzeit möglich ist?	☐	☐	🔴
Wird die Rücksicherung regelmäßig getestet?	☐	☐	🔴
Gibt es einen Notfallplan für den Fall eines Cyberangriffs?	☐	☐	🔴
Gibt es einen Verantwortlichen im Fall eines Notfalls?	☐	☐	🔴

Teil 2: Firmeneigene Endgeräte (PCs, Notebooks, Smartphones)

Frage	Ja	Nein	Priorität
Läuft auf allen Endgeräten ein aktuelles Betriebssystem?	☐	☐	🔴
Werden automatisch alle Patches und Updates installiert?	☐	☐	🔴
Ist auf den Endgeräten stets ein aktueller Virenscanner aktiv?	☐	☐	🔴
Melden sich alle Beschäftigten über die Benutzerverwaltung an den Geräten an?	☐	☐	🔴
Werden die Benutzer zur Verwendung sicherer Passwörter angehalten?	☐	☐	🔴
Wird der Anwender bei Inaktivität automatisch abgemeldet?	☐	☐	🟠
Können externe Medien (USB-Stick) angeschlossen werden?	☐	☐	🟠
Müssen Passwörter regelmäßig geändert werden?	☐	☐	🟢

Teil 3: Mitarbeiterschulungen

Frage	Ja	Nein	Priorität
Gibt es Verhaltensregeln für das Öffnen von E-Mail-Anhängen?	☐	☐	🔴
Werden Beschäftigte regelmäßig über Datensicherheitsrisiken informiert?	☐	☐	🔴
Gibt es eine Datensicherheitsschulung für Beschäftigte?	☐	☐	🔴
Findet diese Schulung regelmäßig statt?	☐	☐	🔴
Wird die Teilnahme an Schulungen dokumentiert?	☐	☐	🟠
Gibt es Verhaltensregeln für das Surfen im Internet?	☐	☐	🟠

Teil 4: Server/Rechenzentrum

Frage	Ja	Nein	Priorität
Läuft auf den Servern ein aktuelles Betriebssystem?	☐	☐	🔴
Werden automatisch alle Patches und Updates installiert?	☐	☐	🔴
Ist eine Benutzerverwaltung eingerichtet?	☐	☐	🔴
Werden Benutzerkonten ehemaliger Beschäftigter umgehend deaktiviert?	☐	☐	🔴
Wird unbenutzte Software umgehend deinstalliert?	☐	☐	🟠
Wird die Funktionalität der Server überwacht?	☐	☐	🟠
Werden Altgeräte fachgerecht gelöscht/entsorgt?	☐	☐	🟠

Teil 5: Netzwerk

Frage	Ja	Nein	Priorität
Ist das Firmen-WLAN verschlüsselt oder deaktiviert?	☐	☐	🔴
Ist eine Firewall im Einsatz?	☐	☐	🔴
Ist für Besucher ein eigenes Gast-WLAN eingerichtet?	☐	☐	🟠
Nutzen Beschäftigte im Homeoffice einen VPN-Zugang?	☐	☐	🟠
Ist ein externer Dienstleister für die Netzwerksicherheit zuständig?	☐	☐	🟢

Teil 6: Physikalische Sicherheit

Frage	Ja	Nein	Priorität
Ist die Stromversorgung der IT-Infrastruktur gesichert (USV)?	☐	☐	🔴
Verfügen wir über einen stabilen Internetzugang?	☐	☐	🔴
Gibt es bei Ausfall einen alternativen Internetzugang?	☐	☐	🟠
Gibt es eine Brandmeldeanlage?	☐	☐	🟠
Gibt es kontrollierten Zugang zum Firmengelände?	☐	☐	🟢

Auswertung und nächste Schritte

Sofortiger Handlungsbedarf 🔴

Bei mehr als 3 "Nein"-Antworten bei kritischen Fragen:

Ihr Unternehmen hat erhebliche Sicherheitslücken. Handeln Sie sofort:

1. Backup-Strategie implementieren - ohne funktionsfähiges Backup sind Sie Ransomware schutzlos ausgeliefert
2. Grundlegende Endpoint-Security - veraltete Systeme sind das Einfallstor Nr. 1
3. Sofortige Mitarbeiterschulung - 95% aller Angriffe nutzen menschliche Schwächen

Empfohlene Reihenfolge:

1. Backup testen/einrichten (diese Woche)
2. Updates und Virenscanner prüfen (diese Woche)
3. Mitarbeiter-Awareness-Schulung (diesen Monat)

Mittelfristiger Handlungsbedarf 🟠

Bei mehr als 2 "Nein"-Antworten:

Grundlagen sind vorhanden, aber wichtige Sicherheitslücken bestehen. Planen Sie:

- Netzwerksicherheit optimieren
- Passwort-Richtlinien verschärfen
- Regelmäßige Schulungszyklen etablieren

Gute Ausgangslage 🟢

Bei weniger als 2 "Nein"-Antworten insgesamt:

Ihr Sicherheitsniveau ist überdurchschnittlich. Fokus auf:

- Kontinuierliche Verbesserung
- Neue Bedrohungen im Blick behalten
- Mitarbeiter-Awareness aufrechterhalten

Dokumentation

Wichtig: Dokumentieren Sie alle getroffenen Maßnahmen für:

- Versicherungen (Cyber-Police)
- Aufsichtsbehörden (DSGVO-Compliance)
- Zertifizierungen (ISO 27001)

Nächste Schritte

Basierend auf Ihrer Auswertung empfehlen wir:

1. **Security Awareness Quick Check** durchführen (kostenlos): Bewerten Sie das Bewusstsein Ihrer Mitarbeiter
2. **Professionelle Risikoanalyse:** Bei kritischen Lücken sollten Sie externe Expertise hinzuziehen
3. **Systematisches Security-Programm:** Für nachhaltige Verbesserung der Unternehmenssicherheit

---

Security Awareness Toolbox - Verwandeln Sie Ihre Mitarbeiter von der größten Schwachstelle zur ersten Verteidigungslinie

Weitere Informationen: www.security-awareness-toolbox.de