specialis IT
Für anspruchsvolle Dienstleister

Kundendaten

Firma: Mautner GmbH
Ansprechpartner: Daniel Mautner
Datum: 16.03.2026

---

1. Allgemeines & Wartungssituation

Ob Sicherheit im Alltag wirklich umgesetzt wird, hängt stark davon ab, ob Zuständigkeiten klar sind und Hilfe rasch erreichbar ist. Wir erkennen das daran, ob es einen externen IT-Dienstleister gibt, wie schnell Support verfügbar ist, ob regelmäßig gewartet wird und ob intern eine zuständige Person benannt ist.

1.1 Gibt es derzeit einen externen IT-Dienstleister?
☒ Ja ☐ Nein (weiter zu 1.4) ☐ Weiß ich nicht

1.2 Wie schnell ist Unterstützung bei Problemen verfügbar?
☐ Sofort ☒ 1–2 Tage ☐ Länger ☐ Weiß ich nicht

1.3 Wird die IT regelmäßig gewartet oder überprüft (z. B. Updates, Fehlerkontrolle)?
☒ Ja ☐ Nein ☐ Weiß ich nicht

1.4 Gibt es im Betrieb eine Person, die sich um IT-Themen kümmert?
☒ Ja ☐ Nein ☐ Weiß ich nicht

---

2. Hardware (PCs, Notebooks, Geräte)

Die Geräte sind die Basis – wenn sie nicht sauber geschützt sind, können Unbefugte leichter zugreifen oder es kommt schneller zu Ausfällen. Wir prüfen die eingesetzten Geräte, die verwendeten Betriebssysteme, den Status von Passwort oder PIN sowie die Einhaltung der Sperr- und Abmeldeprozesse.

2.1 Welche Geräte sind im Einsatz?
☐ __ Stk. Registrierkassa (Kassen-PC) ☒ 2 Stk. PCs ☒ Notebook ☒ Tablet
☒ Smartphone ☒ Drucker ☐ Videoüberwachung ☐ Alarmanlage
☒ Sonstiges: Zebra Scanner

2.2 Betriebssystem(e):
☐ Windows 10 ☒ Windows 11 ☐ Apple ☐ Andere: _____

2.3 Haben die Geräte ein Passwort oder eine PIN beim Einschalten?
☒ Ja ☐ Nein ☐ Weiß ich nicht

2.4 Werden Geräte beim Verlassen des Arbeitsplatzes gesperrt oder abgemeldet?
☒ Ja ☐ Nein ☐ Weiß ich nicht

---

3. Passwortsicherheit

Schwache oder wiederverwendete Passwörter sind ein häufiger Grund für gehackte Konten und Datenprobleme. Wir bewerten, ob Passwörter ausreichend sicher gewählt werden und ob sie so verwaltet werden, dass niemand sie einfach finden oder mitlesen kann.

3.1 Werden sichere Passwörter verwendet (für jeden Zugang ein eigenes Passwort, bestehend aus mind. 8 Zeichen, Buchstaben, Zahlen und Sonderzeichen)?
☒ Ja ☐ Nein ☐ Weiß ich nicht

3.2 Werden Passwörter sicher verwaltet (z. B. Passwortmanagerprogramm, kein Zettel)?
☒ Ja ☐ Nein ☐ Weiß ich nicht

---

4. Software & Programme

Aktuelle Software schließt bekannte Lücken – fehlende Updates lassen Probleme oft unnötig lange offen. Wir schauen, welche Programme genutzt werden, ob sie aktuell und offiziell eingesetzt werden, ob Updates regelmäßig installiert werden und ob auf allen Geräten ein aktueller Schutz aktiv ist.

4.1 Welche Hauptprogramme werden verwendet (Nennen Sie die wichtigsten und täglich benutzten Programme, z. B. Kassensystem, Buchhaltung)?
Office 365, Tarra, Chrome, 3CX

4.2 Ist die verwendete Software lizenziert?
☒ Ja ☐ Nein ☐ Weiß ich nicht ☐ Sonstiges: _____

4.3 Werden regelmäßig Sicherheits- und Systemupdates durchgeführt (Windows Updates)?
☒ Ja ☐ Nein ☐ Weiß ich nicht

4.4 Ist auf allen Geräten ein aktueller Virenschutz installiert?
☐ Ja, folgender:_____ ☒ Nein ☐ Weiß ich nicht

---

5. E-Mail & Kommunikation

E-Mail ist ein zentraler Kommunikationsweg und daher ein häufiger Ansatzpunkt für Betrugsversuche oder fremde Logins. Wir erkennen den Schutz daran, wie das E-Mail-Konto abgesichert ist (z. B. zusätzlicher Anmeldeschutz), ob unerwünschte Nachrichten gefiltert werden und ob bei Nutzung am Smartphone der Zugriff auf die Mails angemessen geschützt ist.

5.1 Welcher Anbieter wird genutzt bzw. über welche Dienst laufen E-Mails?
(A1 / Gmail / Office 365 / Sonstige) A1

5.2 Ist Zwei-Faktor-Authentifizierung (MFA wie Code per App oder SMS) aktiviert?
☒ Ja ☐ Nein ☐ Weiß ich nicht

5.3 Sind Spam- und Virenfilter aktiv? (E-Mails werden automatisch auf unerwünschte Nachrichten und mögliche Schadinhalte geprüft und aussortiert in Spam-Ordner)
☒ Ja ☐ Nein ☐ Weiß ich nicht

5.4 Wird E-Mail auch am Smartphone verwendet? ☒ Ja ☐ Nein ☐ Weiß ich nicht
Wenn ja: Ist das Gerät mit PIN (FaceID/Fingerprint) oder 2-Faktor-Authentifizierung gesichert? ☒ Ja ☐ Nein ☐ Weiß ich nicht

---

6. Datensicherung (Backup)

Werden diverse Daten nach einem Fehler, Defekt oder Vorfall wieder verfügbar sein? Wir beurteilen, ob es überhaupt Sicherungen gibt, wie regelmäßig sie gemacht werden und ob klar ist, wo diese Sicherungen liegen (damit sie im Notfall auch nutzbar sind).

specialis IT
Für anspruchsvolle Dienstleister

Nr.	Datenkategorie	Gesichert?	Speicherort / Methode
6.1	Kundendaten	☒ Ja ☐ Nein ☐ Weiß ich nicht	Cloud (meos)
6.2	Buchhaltung / Kassensystem	☒ Ja ☐ Nein ☐ Weiß ich nicht	Cloud (meos)
6.3	E-Mails	☒ Ja ☐ Nein ☐ Weiß ich nicht	Cloud (meos)
6.4	Dokumente / Rechnungen	☐ Ja ☐ Nein ☒ Weiß ich nicht	—
6.5	Sonstige wichtige Daten	☒ Ja ☐ Nein ☐ Weiß ich nicht	Cloud (meos)
6.6	Häufigkeit Backups	(Täglich, Wöchentlich…)	Täglich

7. Netzwerk & Internetverbindung

Ein ungeschütztes oder „zu offenes" Netzwerk kann ungewollten Zugriff ermöglichen. Wir schauen darauf, ob das WLAN sinnvoll abgesichert ist und ob kritische Geräte (z. B. Kassa/PC) eher geschützt eingebunden sind oder „einfach mit allem zusammen" laufen.

7.1 Gibt es ein aktives WLAN im Betrieb?
☒ Ja ☐ Nein ☐ Weiß ich nicht

7.2 Ist das WLAN mit Passwort/WPA2/WPA3 gesichert?
☒ Ja ☐ Nein ☐ Weiß ich nicht

7.3 Sind Kassensysteme, PCs und Handys über dasselbe WLAN verbunden?
☒ Ja ☐ Nein ☐ Weiß ich nicht

7.4 Wird die Internetverbindung nur für betriebliche Zwecke genutzt?
☒ Ja ☐ Nein ☐ Weiß ich nicht

---

8. Schulung & Bewusstsein

Technik hilft nur begrenzt, wenn im Alltag riskante Nachrichten oder Anhänge unbemerkt geöffnet werden. Wir erkennen den Stand daran, ob Risiken grundsätzlich bekannt sind, ob verdächtige E-Mails eher erkannt werden und ob es bereits Vorfälle gab (als Hinweis, wo man besonders aufpassen sollte).

8.1 Sind Sie und Ihre Mitarbeiter über Risiken wie Cyberangriffe und Phishing (Betrugs-/Täuschungsversuche per Mail) informiert?
☒ Ja ☐ Nein ☐ Weiß ich nicht

8.2 Erkennen Sie und Ihre Mitarbeiter verdächtige E-Mails?
☒ Ja ☐ Nein ☐ Weiß ich nicht

8.3 Hatten Sie schon mal ein Sicherheitsproblem, oder einen Datenverlust?
☐ Ja ☒ Nein ☐ Weiß ich nicht

---

9. Zusammenfassung / Bewertung

Wir nutzen die Selbsteinschätzung und den genannten größten Bedarf als Orientierung, welche Themen aus Sicht des Betriebs am dringendsten wirken oder am meisten Unsicherheit auslösen.

9.1 Wie sicher schätzen Sie Ihre IT aktuell ein?

☐ Sehr sicher ☒ Eher sicher ☐ Unsicher ☐ Keine Einschätzung

9.2 Wo sehen Sie den größten Handlungsbedarf?

☐ Datensicherung ☐ E-Mail ☐ Virenschutz ☐ Netzwerk ☒ Physische Sicherheit

☐ Sonstiges: _____