SELBSTCHECK

Grundlagen der IT-Sicherheit

Für kleine und mittelständische Unternehmen

Ein pragmatischer Überblick über zentrale Schutzmaßnahmen

Dieser Selbstcheck hilft Ihnen, grundlegende Stärken und offene Punkte Ihrer IT-Sicherheit sichtbar zu machen. Er ersetzt keine technische Sicherheitsanalyse, schafft aber eine strukturierte Grundlage für interne Gespräche und die Priorisierung nächster Schritte.

Unternehmen _____

Ansprechperson _____

Datum _____

So verwenden Sie den Check

Bewerten Sie jede Aussage mit Ja, Teilweise, Nein oder Unklar. Beantworten Sie Punkte lieber realistisch als optimistisch. Ein 'Unklar' ist ebenfalls ein wichtiges Ergebnis, weil es auf fehlende Transparenz oder Dokumentation hinweist.

Bewertung und Prioritäten

Ja	Die Maßnahme ist nachvollziehbar umgesetzt und wird gepflegt.	2
Teilweise	Die Maßnahme existiert, ist aber unvollständig, uneinheitlich oder nicht überprüft.	1
Nein	Die Maßnahme ist nicht umgesetzt.	0
Unklar	Der Status ist nicht bekannt oder nicht ausreichend dokumentiert.	0

Sofort prüfen	Konten ehemaliger Mitarbeitender, ungeschützte Fernzugriffe, fehlende Datensicherung, nicht unterstützte Systeme und aktive Sicherheitsvorfälle sollten unabhängig vom Gesamtwert umgehend geklärt werden.
Danach priorisieren	Ordnen Sie offene Maßnahmen nach möglicher Auswirkung, Dringlichkeit, Aufwand und Abhängigkeiten. Nicht jeder offene Punkt hat dasselbe Risiko.

Hinweis

Der Selbstcheck ist eine Orientierungshilfe und keine Zertifizierung, Rechtsberatung oder vollständige Prüfung der technischen Umgebung. Die tatsächliche Priorität hängt von Ihren Systemen, Daten, Geschäftsprozessen und vertraglichen beziehungsweise gesetzlichen Anforderungen ab.

1 Konten und Zugriffsrechte

1.1 Für jede Person existiert ein eigenes Benutzerkonto; gemeinsam genutzte Konten sind auf begründete Ausnahmefälle beschränkt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

1.2 Mehrfaktor-Authentifizierung ist mindestens für E-Mail, Microsoft 365, Cloud-Dienste, Fernzugriffe und administrative Konten aktiviert.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

1.3 Berechtigungen werden nach Aufgabe vergeben und bei Rollenwechseln oder Austritten zeitnah angepasst.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

1.4 Administrative Tätigkeiten erfolgen mit getrennten Administratorkonten; diese werden nicht für E-Mail und normales Arbeiten verwendet.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

Notizen / offene Maßnahmen

2 Arbeitsplätze und mobile Geräte

2.1 Alle betrieblichen Computer und Mobilgeräte werden zentral erfasst und erhalten regelmäßig Sicherheitsupdates.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

2.2 Ein aktueller Endpoint-Schutz ist aktiviert, wird überwacht und kann von Anwendern nicht ohne Weiteres deaktiviert werden.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

2.3 Festplatten mobiler Geräte und Notebooks sind verschlüsselt; Bildschirme sperren sich nach angemessener Inaktivität automatisch.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

2.4 Verlust, Defekt und Austausch von Geräten sind geregelt; betriebliche Daten können bei Bedarf aus der Ferne geschützt oder entfernt werden.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

Notizen / offene Maßnahmen

3 Netzwerk und Fernzugriffe

3.1 Firewall, Router, Switches und WLAN-Komponenten werden noch unterstützt, regelmäßig aktualisiert und sind dokumentiert.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

3.2 Internes WLAN, Gäste-WLAN und besonders schützenswerte Systeme sind sinnvoll voneinander getrennt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

3.3 Fernzugriffe erfolgen ausschließlich über abgesicherte, nachvollziehbare Verbindungen und sind durch Mehrfaktor-Authentifizierung geschützt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

3.4 Standardkennwörter wurden ersetzt; administrative Oberflächen sind nicht unnötig aus dem Internet erreichbar.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

Notizen / offene Maßnahmen

4 E-Mail, Cloud und Zusammenarbeit

4.1 E-Mail-Domäne und Cloud-Dienste sind mit geeigneten Sicherheitsrichtlinien und aktuellen Schutzmechanismen konfiguriert.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

4.2 Externe Freigaben von Dateien und Ordnern werden begrenzt, regelmäßig geprüft und bei Wegfall des Zwecks entfernt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

4.3 Verdächtige Anmeldungen, Weiterleitungsregeln und ungewöhnliche Kontoaktivitäten können erkannt und untersucht werden.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

4.4 Mitarbeitende wissen, wie sie verdächtige Nachrichten, Freigaben oder Anmeldeaufforderungen melden können.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

Notizen / offene Maßnahmen

5 Datensicherung und Wiederherstellung

5.1 Alle geschäftskritischen Daten und Systeme sind in einem dokumentierten Sicherungskonzept berücksichtigt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

5.2 Mindestens eine Sicherung ist vom normalen Netzwerk beziehungsweise von den regulären Benutzerkonten getrennt und gegen Veränderungen geschützt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

5.3 Sicherungen werden automatisch überwacht; Fehler führen zu einer Benachrichtigung und werden zeitnah bearbeitet.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

5.4 Wiederherstellungen werden regelmäßig getestet und die benötigte Zeit sowie die Verantwortlichkeiten sind bekannt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

Notizen / offene Maßnahmen

6 Updates, Monitoring und Dokumentation

6.1 Betriebssysteme, Anwendungen, Server und Netzwerkkomponenten erhalten innerhalb definierter Fristen Sicherheitsupdates.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

6.2 Nicht mehr unterstützte Systeme sind bekannt und werden ersetzt, isoliert oder durch geeignete Übergangsmaßnahmen abgesichert.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

6.3 Wichtige Systeme und Sicherheitsereignisse werden überwacht; Warnmeldungen haben einen klaren Empfänger und Bearbeitungsweg.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

6.4 Netzplan, Systemübersicht, Zuständigkeiten, Dienstleisterzugänge und wichtige Konfigurationen sind aktuell dokumentiert.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

Notizen / offene Maßnahmen

7 Mitarbeitende und organisatorische Abläufe

7.1 Neue Mitarbeitende erhalten eine verständliche Sicherheitseinweisung und werden regelmäßig für aktuelle Risiken sensibilisiert.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

7.2 Ein- und Austritte sowie Rollenwechsel lösen einen dokumentierten Prozess für Konten, Berechtigungen, Geräte und Schlüssel aus.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

7.3 Regeln für Passwörter, private Geräte, Softwareinstallationen, Datenfreigaben und mobiles Arbeiten sind verständlich festgelegt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

7.4 Sicherheitsrelevante Auffälligkeiten können ohne Umwege gemeldet werden; Ansprechpartner und Kommunikationswege sind bekannt.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

Notizen / offene Maßnahmen

8 Vorbereitung auf Sicherheitsvorfälle

8.1 Für einen Sicherheitsvorfall existiert ein kurzer, erreichbarer Notfallplan mit Ansprechpartnern und ersten Maßnahmen.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

8.2 Es ist festgelegt, wer im Ernstfall technische Dienstleister, Geschäftsführung, Datenschutz, Versicherung und gegebenenfalls Behörden einbindet.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

8.3 Kritische Geschäftsprozesse, Systeme und akzeptable Ausfallzeiten sind bekannt und priorisiert.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

8.4 Notfallkontakte und Wiederanlaufverfahren sind auch verfügbar, wenn zentrale IT-Systeme oder E-Mail nicht funktionieren.

☐ Ja ☐ Teilweise ☐ Nein ☐ Unklar

Notizen / offene Maßnahmen

Ihre Auswertung

Tragen Sie für jedes Kapitel die erreichten Punkte ein. Pro Kapitel sind maximal 8 Punkte möglich; insgesamt maximal 64 Punkte.

1. Konten und Zugriffsrechte	/ 8	
2. Arbeitsplätze und mobile Geräte	/ 8	
3. Netzwerk und Fernzugriffe	/ 8	
4. E-Mail, Cloud und Zusammenarbeit	/ 8	
5. Datensicherung und Wiederherstellung	/ 8	
6. Updates, Monitoring und Dokumentation	/ 8	
7. Mitarbeitende und organisatorische Abläufe	/ 8	
8. Vorbereitung auf Sicherheitsvorfälle	/ 8	
Gesamtergebnis	/ 64	

49-64 Punkte	**Gute Grundlage**	Viele Grundlagen sind vorhanden. Prüfen Sie besonders alle Antworten mit 'Teilweise', 'Nein' oder 'Unklar' und stellen Sie sicher, dass Maßnahmen regelmäßig kontrolliert werden.
33-48 Punkte	**Gezielt verbessern**	Wichtige Grundlagen sind vorhanden, es bestehen jedoch relevante Lücken. Priorisieren Sie zuerst Konten, Fernzugriffe, Updates, Backups und Notfallvorsorge.
17-32 Punkte	**Strukturiert handeln**	Mehrere grundlegende Maßnahmen fehlen oder sind nicht transparent. Eine strukturierte Bestandsaufnahme und ein priorisierter Maßnahmenplan sind empfehlenswert.
0-16 Punkte	**Kurzfristig prüfen**	Wesentliche Grundlagen sind nicht umgesetzt oder ihr Status ist unklar. Beginnen Sie zeitnah mit einer fachlichen Bestandsaufnahme und sichern Sie zuerst besonders kritische Zugänge, Systeme und Daten.

Ihr Maßnahmenplan

Wählen Sie zunächst höchstens fünf Maßnahmen. Halten Sie Verantwortung und Zieltermin fest. Ein kurzer, konsequent bearbeiteter Plan ist hilfreicher als eine lange, ungeordnete Aufgabenliste.

1			
2			
3			
4			
5			

Sie möchten die Ergebnisse einordnen?

Ich unterstütze Sie bei einer strukturierten Bestandsaufnahme, der Priorisierung offener Punkte und der nachvollziehbaren Umsetzung geeigneter Schutzmaßnahmen.

Marc Zingsheim · IT Zingsheim
Edelweißstraße 8c · 32457 Porta Westfalica
marc@it-zingsheim.de · +49 (0) 571 78469510
www.it-zingsheim.de