

IT-Sicherheit im kleinen Unternehmen: der 15-Punkte-Selbstcheck

Fünfzehn Fragen, keine davon technisch. Etwa zwanzig Minuten, kein IT-Wissen nötig – nur Ehrlichkeit beim Ankreuzen.

Kreuzen Sie je Punkt **Ja**, **Nein** oder **Weiß ich nicht** an. „Weiß ich nicht“ ist dabei kein Ausweichfeld, sondern die aufschlussreichste Antwort von allen.

	Ja	Nein	Weiß ich nicht
Backup: Können Sie morgen weiterarbeiten?			
1 Es gibt ein Backup, das nicht am selben Ort liegt wie die Daten. Eine externe Festplatte im Serverschrank zählt nicht, ein Sync in die Cloud auch nicht.	☐	☐	☐
2 Jemand hat in den letzten drei Monaten eine Wiederherstellung ausprobiert. Tatsächlich eine Datei zurückgeholt und geöffnet – nicht nur „Backup erfolgreich“ gelesen.	☐	☐	☐
3 Sie wissen, wie lange eine komplette Wiederherstellung dauern würde. Einen Tag, eine Woche? Die Antwort bestimmt, wie lange Ihr Betrieb stillsteht.	☐	☐	☐
Zugänge: Wer kommt an was heran?			
4 Jeder Mitarbeiter hat ein eigenes Konto. Kein „Büro-Login“, den alle kennen.	☐	☐	☐
5 Bei E-Mail und Cloud ist eine zweite Bestätigung eingeschaltet. Zwei-Faktor-Anmeldung per App oder Code – bei allen Konten, nicht bei der Hälfte.	☐	☐	☐
6 Wenn jemand das Unternehmen verlässt, werden alle Zugänge am selben Tag gesperrt. E-Mail, Cloud, VPN, Buchhaltungssoftware, Online-Banking-Freigaben.	☐	☐	☐
7 Es gibt einen Passwort-Manager, und er wird benutzt. Damit tatsächlich jeder Dienst ein eigenes Passwort bekommt.	☐	☐	☐
Geräte und Updates			
8 Alle Rechner laufen mit einem Betriebssystem, das noch Updates bekommt. Windows 10 ist seit Oktober 2025 ohne Sicherheitsupdates – auch im Lager und an der Zeiterfassung.	☐	☐	☐
9 Updates werden innerhalb weniger Tage eingespielt, nicht irgendwann. Windows, Browser, Office und die Firmware der Firewall gleichermaßen.	☐	☐	☐
10 Auf jedem Gerät läuft ein aktueller Virenschutz, den jemand auch überwacht. Entscheidend ist weniger das Produkt als die Frage, wer die Meldungen liest.	☐	☐	☐
11 Firmenlaptops sind verschlüsselt. Sonst sind die Daten eines verlorenen Laptops für den Finder lesbar – im Zweifel eine meldepflichtige Datenpanne.	☐	☐	☐
Netz und E-Mail			
12 Gäste-WLAN und Firmennetz sind getrennt. Das Handy des Besuchers sollte den Server nicht sehen können.	☐	☐	☐
13 Ihre Mitarbeiter wissen, wie eine Phishing-Mail aussieht, und trauen sich nachzufragen. Der zweite Teil ist der wichtigere.	☐	☐	☐

	Ja	Nein	Weiß ich nicht
Verantwortung und Dokumentation			
14 Sie wissen, wen Sie anrufen, wenn heute Nacht alles verschlüsselt ist. Mit Telefonnummer – und derjenige weiß, dass Sie ihn anrufen würden.	☐	☐	☐
15 Es gibt eine Liste, welche Systeme, Zugänge und Verträge Ihr Unternehmen hat. Für den Fall, dass Sie ausfallen oder den Dienstleister wechseln wollen.	☐	☐	☐

Und jetzt?

Anzahl **Nein**: _____ Anzahl **Weiß ich nicht**: _____ Zusammen: _____

Bis 3

Sie stehen besser da als die meisten. Kümmern Sie sich um genau diese Punkte.

4 bis 7

Typisch für Unternehmen, die IT „nebenbei“ betreuen lassen. Das lässt sich in einigen Wochen aufräumen.

Ab 8

Mit dem Backup anfangen, heute, und den Rest danach sortieren.

Zweimal Nein bei den Punkten 1 bis 3? Dann zuerst das Backup in Ordnung bringen, der Rest kann warten.

Genauer als mit einer Liste geht es mit dem **IT-Sicherheitscheck** entlang der Prüfbereiche der DIN SPEC 27076: dieselben Fragen, mit Blick in die Systeme statt aufs Bauchgefühl, und mit einem Bericht, den Sie auch Ihrer Versicherung zeigen können.

Erläuterungen zu jedem Punkt: ingenius-heimdall.de/it-sicherheit-selbstcheck-kmu

Erstgespräch vereinbaren: ingenius-heimdall.de/erstgespraech

Ingenius Heimdall · IT-Sicherheit in Essen und im Ruhrgebiet
015678 580073 · kontakt@ingenius-heimdall.de

Stand: September 2026