// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

KI-Tool Sicherheitsaudit für KMU: Die Checkliste für Österreich

NIS2, DSGVO, Cyberrisiken: So prüfen österreichische KMU ihre IT-Sicherheit selbst — mit KI-Tools, konkreten Checklisten und realistischen Kosten.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
2. Juni 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/ki-tool-sicherheitsaudit-kmu-checkliste-oesterreich/

Ein Tischlereibetrieb in der Steiermark erhält eine E-Mail, scheinbar vom Steuerberater — mit dem Betreff „Dringende Rückforderung Finanzamt". Ein Mitarbeiter klickt, gibt seine Zugangsdaten ein. Drei Tage später sind Kundendaten verschlüsselt, das Kassensystem offline. Erst jetzt fragt sich der Geschäftsführer, wie sicher die IT des Betriebs eigentlich war. Die Antwort: Er hatte keine Ahnung.

Genau für diese Situation ist dieser Artikel geschrieben. Nicht als Anleitung zum perfekten Sicherheitskonzept, sondern als erster, ehrlicher Blick auf den eigenen Status quo — mit Hilfe von KI-gestützten Tools, die das deutlich günstiger machen als ein klassisches IT-Dienstleister-Audit. Am Ende kennen Sie die fünf wichtigsten Prüfbereiche, drei konkrete Tool-Empfehlungen mit realistischen Kostenschätzungen und eine handliche Checkliste, die Sie sofort verwenden können. Und Sie wissen, welche dieser Maßnahmen auch Ihre NIS2- und DSGVO-Pflichten abdeckt.

Was ein Sicherheitsaudit für KMU überhaupt bedeutet

Ein Audit ist kein Zertifizierungsverfahren und kein Behördengang. Es ist eine strukturierte Bestandsaufnahme: Was haben wir? Wer hat Zugriff worauf? Wo liegen unsere Daten? Was passiert, wenn ein Gerät gestohlen wird oder ein Server ausfällt?

Der Unterschied zwischen internem Self-Assessment und externem Audit ist praktisch: Ein Self-Assessment führen Sie selbst durch — mit Checklisten, frei verfügbaren Tools und dem gesunden Menschenverstand. Es reicht für die meisten KMU unter 50 Mitarbeitenden als Ausgangspunkt. Ein externes Audit durch einen IT-Dienstleister geht tiefer, ist aber auch teurer — und sinnvoll, sobald Sie die Ergebnisse des Self-Assessments nicht mehr selbst einordnen können.

Die typische Ausgangslage österreichischer KMU: keine eigene IT-Abteilung, eine Mischung aus Microsoft 365 oder Google Workspace, lokalen Rechnern, einem NAS im Lager und dutzenden SaaS-Diensten, die einzelne Mitarbeitende im Laufe der Jahre eingeführt haben. Genau in dieser Gemengelage entstehen die meisten Sicherheitslücken.

Ein kurzer Hinweis zu NIS2: Das österreichische Umsetzungsgesetz (NISG 2024) schreibt für bestimmte Betriebe regelmäßige Risikoprüfungen vor. Kleinere Betriebe sind in den meisten Fällen nicht direkt betroffen — aber als Zulieferer größerer Unternehmen indirekt schon. Mehr dazu im nächsten Abschnitt.

NIS2 und DSGVO in Österreich – was KMU 2025 konkret prüfen müssen

NIS2-Umsetzung in Österreich – der aktuelle Stand

Das österreichische Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024) setzt die EU-NIS2-Richtlinie in nationales Recht um. Es gilt seit Oktober 2024 und betrifft Betriebe in definierten kritischen Sektoren — darunter Energie, Verkehr, Gesundheit, digitale Infrastruktur und Teile des verarbeitenden Gewerbes.

Die relevanten Schwellenwerte: Als „wichtige Einrichtung" gilt ein Unternehmen ab 50 Mitarbeitenden oder einem Jahresumsatz bzw. einer Jahresbilanzsumme von über 10 Millionen Euro. Betriebe darunter fallen in den meisten Fällen nicht direkt unter das Gesetz. Aufsichtsbehörde ist die RTR (Rundfunk und Telekom Regulierungs-GmbH), technische Unterstützung kommt vom CERT.at.

Was bedeutet das für kleinere Betriebe? Direkte Pflichten entstehen kaum. Aber: Wer als Zulieferer oder Dienstleister für eine „wichtige Einrichtung" tätig ist, wird zunehmend mit Sicherheitsanforderungen aus dem Lieferkettenmanagement konfrontiert. Eine freiwillige Orientierung an NIS2-Standards ist deshalb empfehlenswert — und ein Sicherheitsaudit der beste Einstieg. Details zur NIS2-Umsetzung in Österreich finden Sie in unserem Artikel NIS2 / NISG 2026: Auch ohne direkte Pflicht relevant für KMU?.

DSGVO-Sicherheitspflichten – was Art. 32 konkret fordert

Artikel 32 DSGVO verpflichtet alle Unternehmen — ohne Größenschwelle — zu „geeigneten technischen und organisatorischen Maßnahmen" (TOMs), die dem Risiko der Datenverarbeitung entsprechen. Das klingt abstrakt, bedeutet in der Praxis: Passwortrichtlinien, Zugriffskontrollen, Datensicherung, Verschlüsselung, und eine dokumentierte Einschätzung, warum diese Maßnahmen ausreichend sind.

Typische Lücken, die wir bei österreichischen KMU regelmäßig sehen: kein Verzeichnis der Verarbeitungstätigkeiten, keine dokumentierte Risikoeinschätzung, und TOMs, die zwar vorhanden, aber nirgends aufgeschrieben sind. Letzteres ist besonders heikel — bei einer Datenschutzbehörden-Anfrage (nach aktueller Rechtslage) zählt nur, was dokumentiert ist.

Der praktische Vorteil eines kombinierten Audits: Die Ergebnisse eines Sicherheits-Self-Assessments liefern direkt die Grundlage für Ihre TOM-Dokumentation. Zwei Fliegen, eine Klappe.

Die 5 Prüfbereiche eines KMU-Sicherheitsaudits

1. Zugriffsrechte und Benutzerkonten

Was Sie prüfen: Wer hat Zugriff auf welche Systeme — und braucht diese Person diesen Zugriff wirklich? Erfahrungsgemäß haben in vielen KMU mehrere Mitarbeitende Admin-Rechte, weil es „einfacher" war als eine saubere Rechtevergabe.

Checkliste: - [ ] Ist Mehr-Faktor-Authentifizierung (MFA) für alle Konten aktiv — besonders E-Mail und Cloud? - [ ] Gibt es geteilte Passwörter (z. B. ein gemeinsames Admin-Kennwort)? - [ ] Wurden Konten ausgeschiedener Mitarbeitender vollständig deaktiviert? - [ ] Hat jede Person nur die Rechte, die sie für ihre Arbeit braucht? - [ ] Sind Admin-Konten von normalen Arbeitskonten getrennt?

KI-Tool-Tipp: Microsoft Secure Score (für M365-Nutzer) bewertet Ihre Konfiguration automatisch und gibt priorisierte Empfehlungen — inklusive MFA-Status und Benutzerrisiken. Die Entra ID-Audit-Logs zeigen, wer sich wann von wo angemeldet hat. Beides ist im M365-Abo inklusive.

Zeitaufwand: ca. 45 Minuten

---

2. Netzwerk und Endgeräte

Was Sie prüfen: Ihr Netzwerk ist der Einstiegspunkt für die meisten Angriffe von außen. Router mit veralteter Firmware, ungesichertes WLAN und fehlende Firewall-Konfiguration sind die häufigsten Schwachstellen.

Checkliste: - [ ] Wurde die Router-Firmware zuletzt vor weniger als 6 Monaten aktualisiert? - [ ] Ist das Gäste-WLAN vom internen Netzwerk getrennt? - [ ] Ist eine Firewall aktiv — und wurde ihre Konfiguration jemals geprüft? - [ ] Sind automatische Updates auf allen Endgeräten aktiviert? - [ ] Gibt es eine BYOD-Regelung (Bring Your Own Device) für private Smartphones und Laptops? - [ ] Werden VPN-Verbindungen für Remote-Zugriffe genutzt?

KI-Tool-Tipp: Qualys FreeScan ist cloud-basiert und benötigt keinen installierten Agent — Sie starten einen Scan Ihrer externen IP-Adresse direkt im Browser. Alternativ: Lansweeper Free Tier erstellt ein vollständiges Inventar aller Geräte in Ihrem Netzwerk. Lansweeper speichert Daten lokal oder in der EU.

Hinweis zu Qualys: Der Dienst ist in den USA gehostet. Für einen reinen Netzwerkscan ohne Übertragung personenbezogener Daten ist das nach aktueller Rechtslage in der Regel unproblematisch — prüfen Sie das im Einzelfall.

Zeitaufwand: ca. 30 Minuten (Scan läuft im Hintergrund)

---

3. Datensicherung und Wiederherstellung

Was Sie prüfen: Ob Sie nach einem Angriff oder Hardwareausfall Ihre Daten wiederherstellen können — und wie lange das dauern würde.

Die 3-2-1-Regel in einem Satz: Mindestens 3 Kopien Ihrer Daten, auf 2 verschiedenen Medien, davon 1 außerhalb Ihres Standorts (oder offline).

Checkliste: - [ ] Wie oft werden Backups erstellt — täglich, wöchentlich? - [ ] Wann wurde die Wiederherstellung zuletzt getestet (nicht nur das Erstellen des Backups)? - [ ] Existiert eine Offline-Kopie, die bei einem Ransomware-Angriff nicht verschlüsselt werden kann? - [ ] Wissen mindestens zwei Personen im Betrieb, wie die Wiederherstellung funktioniert? - [ ] Sind Backup-Konten vor Admin-Zugriffen durch normale Benutzerkonten geschützt?

KI-Tool-Tipp: Veeam ONE Community Edition überwacht Ihre Backup-Infrastruktur und schlägt Alarm bei Fehlern. Acronis bietet einen Selbstprüfungsbericht, der den Status Ihrer Backups zusammenfasst.

Zeitaufwand: ca. 30 Minuten (plus Zeit für einen echten Wiederherstellungstest — dringend empfohlen)

---

4. Cloud-Dienste und SaaS-Anwendungen

Was Sie prüfen: Welche Cloud-Dienste nutzen Ihre Mitarbeitenden — auch ohne IT-Freigabe? „Schatten-IT" ist in KMU die Regel, nicht die Ausnahme. Dropbox, WeTransfer, private Gmail-Accounts für Kundenkommunikation: All das existiert, auch wenn niemand darüber spricht.

Checkliste: - [ ] Gibt es eine Liste aller genehmigten Cloud-Dienste? - [ ] Werden Kundendaten über nicht freigegebene Dienste übertragen? - [ ] Wo liegen die Daten der wichtigsten SaaS-Anbieter — EU-Rechenzentrum oder USA? - [ ] Sind für US-Anbieter DSGVO-Standardvertragsklauseln (SCCs) abgeschlossen? - [ ] Wurde der Datenzugriff von KI-basierten Tools geprüft? (Stichwort: Datenzugriff von KI-Agenten absichern)

KI-Tool-Tipp: Obsidian Security bietet einen Free Tier für SaaS-Sichtbarkeit — nützlich, wenn Sie wissen wollen, welche Apps auf Ihre M365- oder Google-Workspace-Umgebung zugreifen. Alternativ: eine manuelle Abfrage bei allen Mitarbeitenden mit einer einfachen Vorlage (Dienst, Zweck, Datenkategorie) reicht als Einstieg.

Wenn Sie nach einer DSGVO-konformen Alternative zu US-Cloud-Diensten suchen: DSGVO-konforme Alternative mit EU-Hosting — Nextcloud ist für viele KMU eine realistische Option.

Zeitaufwand: ca. 20 Minuten für Inventarisierung

---

5. Mitarbeitende und Phishing-Anfälligkeit

Was Sie prüfen: Menschen sind nach wie vor das häufigste Einfallstor. Laut CERT.at-Jahresbericht waren Phishing und Social Engineering 2023 für den Großteil der gemeldeten Sicherheitsvorfälle in österreichischen Unternehmen verantwortlich.

Checkliste: - [ ] Gibt es eine schriftliche Sicherheitsrichtlinie, die alle Mitarbeitenden kennen? - [ ] Wurde jemals eine Phishing-Simulation durchgeführt? - [ ] Wissen alle Mitarbeitenden, an wen sie einen verdächtigen Vorfall melden? - [ ] Gibt es eine Regelung für den Umgang mit externen USB-Geräten? - [ ] Sind Sicherheitsschulungen Teil des Onboardings neuer Mitarbeitender?

KI-Tool-Tipp: KnowBe4 bietet kostenlose Phishing-Tests und Sicherheitsbewertungen — hosting in den USA, aber für anonymisierte Simulations-Tests akzeptabel. GoPhish ist eine selbst gehostete Open-Source-Alternative, bei der alle Daten lokal bleiben. Mehr dazu, wie KI-generierte Phishing-Mails erkannt werden, lesen Sie in unserem Artikel dazu — das Thema KI-Phishing behandeln wir separat.

Zeitaufwand: ca. 15 Minuten für Checkliste; Phishing-Simulation läuft über 1–2 Wochen

---

KI-Tools im Vergleich – welche für österreichische KMU taugen

TOOL	EINSATZBEREICH	PREIS (EINSTIEG)	DATENSPEICHERORT	NIS2-RELEVANT
Microsoft Secure Score	M365-Umgebungen	Inklusive M365	EU möglich	Ja
Qualys FreeScan	Netzwerk-Scan (extern)	Kostenlos	USA (SaaS)	Eingeschränkt
Lansweeper Free	Asset-Inventar	Kostenlos	Lokal/EU	Ja
KnowBe4 Free Tools	Phishing-Test	Kostenlos	USA	Bedingt
Tenable.io Essentials	Vulnerability Scan	Kostenlos (bis 32 IPs)	EU-Option	Ja

Ehrliche Einschätzung: Kein einzelnes Tool ersetzt ein vollständiges Audit. Was diese Tools leisten, ist die Einstiegshürde erheblich zu senken — von „ich habe keine Ahnung“ zu „ich weiß, wo die größten Lücken sind“. Das ist für die meisten KMU der entscheidende erste Schritt.

Besonderer Hinweis für Tools mit US-Hosting: Prüfen Sie, ob der Anbieter DSGVO-Standardvertragsklauseln (SCCs) anbietet und ob ein Auftragsverarbeitungsvertrag (AVV) abgeschlossen werden kann. Bei reinen Scan-Ergebnissen ohne personenbezogene Daten ist das Risiko überschaubar — aber prüfen Sie es nach aktueller Rechtslage im Einzelfall.

Schritt-für-Schritt – So führen Sie das Audit in einem Nachmittag durch

Der realistische Gesamtaufwand: 3–4 Stunden, wenn Sie vorbereitet starten. Kein IT-Hintergrund nötig.

Schritt 1: Asset-Inventar erstellen (30 Min.) Schreiben Sie auf — oder fragen Sie rum — welche Geräte, Cloud-Dienste und Software im Betrieb genutzt werden. Laptops, Tablets, Smartphones, NAS-Geräte, Drucker mit Netzwerkanschluss. Das klingt trivial, aber die meisten KMU haben noch nie eine vollständige Liste gehabt.

Schritt 2: Zugriffsrechte-Check (45 Min.) M365-Nutzer starten den Secure Score im Admin-Center. Ohne M365: Gehen Sie manuell durch — wer hat Admin-Rechte, welche Konten ausgeschiedener Mitarbeitender sind noch aktiv, wo gibt es geteilte Passwörter?

Schritt 3: Netzwerk-Scan mit Qualys FreeScan (läuft im Hintergrund) Scan starten, weitermachen. Das Ergebnis zeigt offene Ports und bekannte Schwachstellen an Ihrer externen IP-Adresse. Lansweeper parallel für das interne Inventar.

Schritt 4: Cloud-Dienste-Inventar (20 Min.) Kurze Runde bei den Mitarbeitenden: Welche Online-Tools nutzt ihr für die Arbeit? Welche Apps habt ihr auf dem Firmen-Smartphone? Keine Wertung, nur Sammeln. Erfahrungsgemäß kommen dabei 5–15 ungekannte Dienste ans Licht.

Schritt 5: Ergebnisse dokumentieren und Prioritäten setzen (30 Min.) Tragen Sie die Ergebnisse in eine einfache Tabelle ein: Prüfbereich, Status (ok / Lücke / unklar), Priorität (hoch / mittel / niedrig). Diese Tabelle ist bereits eine erste TOM-Dokumentation für Ihre DSGVO-Rechenschaftspflicht.

Dokumentations-Tipp: Speichern Sie das Ergebnis mit Datum. Bei einer Datenschutzbehörden-Anfrage oder einem Sicherheitsvorfall können Sie nachweisen, dass Sie den Status Ihrer IT-Sicherheit aktiv geprüft haben.

Kostenrahmen – Was ein KMU-Sicherheitsaudit realistisch kostet

Eigenaufwand: 4–8 Stunden intern, je nach Betriebsgröße und Vorbereitung. Bei einem Stundensatz von 60–80 € (Opportunitätskosten eines Geschäftsführers) sind das 240–640 € in Arbeitszeit.

Tool-Kosten: 0 € bis ca. 200 €/Jahr für Einstiegslösungen. Die meisten der oben genannten Tools haben kostenlose Versionen, die für ein KMU-Erst-Audit ausreichen.

Externer IT-Dienstleister: Ein strukturiertes Erst-Audit durch einen österreichischen IT-Dienstleister kostet realistisch 800–2.500 €, abhängig von Betriebsgröße und Umfang. Das ist kein Routinebudget — aber einmalig als Investition sinnvoll, sobald das Self-Assessment Fragen aufwirft, die Sie nicht selbst beantworten können.

Gegenrechnung: Laut WKO-Wirtschaftsbericht und KPMG Österreich Cybersicherheitsstudie liegen die durchschnittlichen Kosten eines erfolgreichen Cyberangriffs auf ein österreichisches KMU bei 20.000–80.000 € — Systemausfall, Datenverlust, Reputationsschaden und Wiederherstellungskosten zusammengerechnet. Ein Self-Assessment für 300 € Eigenaufwand ist die günstigste Versicherungsprämie, die es gibt.

Fördermöglichkeiten: Das KMU Digital-Programm der Austria Wirtschaftsservice (aws) fördert Digitalisierungsmaßnahmen — darunter auch IT-Sicherheitsberatung. Details und aktuelle Förderbedingungen finden Sie direkt auf aws.at. Zusätzlich gibt es Förderungen im Rahmen der KI Förderung Österreich 2026 für KMU, die KI-gestützte Sicherheitslösungen einsetzen wollen.

Branchenspezifische Hinweise für Österreich

Gastronomie und Hotellerie: Kassensysteme sind oft veraltet und schlecht gewartet — ein beliebtes Angriffsziel. Buchungsplattformen (Booking.com, eigene Systeme) speichern Kreditkartendaten. Und das Gäste-WLAN ist in vielen Betrieben mit dem internen Netzwerk verbunden. Diese drei Punkte verdienen Priorität.

Handwerk: Mobile Geräte auf Baustellen, geteilte Tablets in der Werkstatt, Angebots- und Abrechnungssoftware mit Kundendaten — und oft kein Passwortschutz, weil es im Arbeitsalltag zu umständlich ist. Hier sind einfache technische Lösungen (automatische Displaysperre, MFA für Cloud-Dienste) schnell wirksam.

Gesundheitswesen (Arztpraxen, Therapeuten, Physiotherapie): Besonderer Schutzbedarf nach Art. 9 DSGVO für Gesundheitsdaten. ELGA-Anbindung bringt zusätzliche Anforderungen. Ein reines Self-Assessment reicht hier in der Regel nicht — ein begleitetes Audit ist empfehlenswert.

Für branchenspezifische Tiefenanalysen lohnt sich ein persönliches Gespräch. Die Ausgangslage eines Tischlereibetriebs mit 12 Mitarbeitenden unterscheidet sich erheblich von der einer Zahnarztpraxis mit 8.

Was tun mit den Audit-Ergebnissen?

Teilen Sie die Ergebnisse in drei Kategorien ein:

Sofortmaßnahmen (diese Woche, Kosten: 0 €): MFA aktivieren, Konten ausgeschiedener Mitarbeitender deaktivieren, geteilte Passwörter ersetzen, Gäste-WLAN trennen. Diese Maßnahmen kosten nichts außer einer Stunde Zeit.

Kurzfristig (bis 3 Monate, geringes Budget): Backup-Strategie überarbeiten, Sicherheitsrichtlinie schriftlich festhalten, Passwort-Manager für das gesamte Team einführen. Budget: 0–500 €.

Mittelfristig (Investitionsentscheidung): Endpoint-Security-Lösung evaluieren, NIS2-konforme Dokumentation aufbauen, externe Überprüfung kritischer Systeme beauftragen. Budget: 500–3.000 €.

Eine einfache 2×2-Risikomatrix hilft bei der Priorisierung: Tragen Sie jede identifizierte Lücke nach Wahrscheinlichkeit (gering/hoch) und Auswirkung (gering/hoch) ein. Was oben rechts landet — hohe Wahrscheinlichkeit, hohe Auswirkung — ist Ihre Priorität, unabhängig vom Budget.

Viele KMU kommen an einen Punkt, wo die Audit-Ergebnisse Fragen aufwerfen, die ein Self-Assessment nicht beantworten kann: Welche Maßnahmen sind nach aktueller Rechtslage verpflichtend, welche nur empfehlenswert? Wie baut man NIS2-Dokumentation konkret auf? Welches Tool passt zu meiner konkreten Infrastruktur? An genau diesem Punkt ist ein begleitetes Gespräch deutlich effizienter als weitere Stunden mit Selbstrecherche.

FAQ

Bin ich als kleines österreichisches Unternehmen unter 10 Mitarbeitern von NIS2 betroffen? In den meisten Fällen nicht direkt. Das NISG 2024 richtet sich an Betriebe ab 50 Mitarbeitenden oder 10 Millionen Euro Umsatz in definierten Sektoren. Aber: Als Zulieferer oder Dienstleister für größere Unternehmen werden Sie zunehmend mit Sicherheitsanforderungen aus dem Lieferkettenmanagement konfrontiert. Eine Orientierung an NIS2-Standards ist deshalb auch für kleinere Betriebe empfehlenswert.

Wie oft sollte ein KMU ein Sicherheitsaudit durchführen? Mindestens einmal jährlich als Routine. Zusätzlich anlassbezogen: bei Einführung eines neuen Cloud-Dienstes, bei Personalwechsel in Schlüsselrollen (IT-Zuständige, Geschäftsführung), nach einem Sicherheitsvorfall — und nach wesentlichen Änderungen in der IT-Infrastruktur.

Kann ich mit einem Self-Assessment meine DSGVO-Pflichten erfüllen? Teilweise. Ein dokumentiertes Self-Assessment liefert die Grundlage für Ihre TOM-Dokumentation nach Art. 32 DSGVO und zeigt, dass Sie Ihre Sicherheitslage aktiv einschätzen. Es ersetzt jedoch nicht die vollständige Datenschutzdokumentation (Verarbeitungsverzeichnis, Datenschutzrichtlinie, AVVs mit Dienstleistern). Für die Gesamtbeurteilung empfiehlt sich nach aktueller Rechtslage eine ergänzende Beratung.

Nächste Schritte – Ihr persönlicher Fahrplan

Drei Dinge, die Sie heute noch tun können: Prüfen Sie, ob MFA für alle E-Mail-Konten im Betrieb aktiv ist. Schauen Sie nach, welche Konten ausgeschiedener Mitarbeitender noch existieren. Und starten Sie einen Qualys FreeScan Ihrer externen IP-Adresse — das dauert 10 Minuten und liefert sofortige Ergebnisse.

Wenn Sie das Audit durchgeführt haben und nun konkrete Folgefragen entstehen — zu NIS2-Pflichten in Ihrer Branche, zur richtigen Tool-Auswahl für Ihre Infrastruktur oder zum Aufbau einer DSGVO-konformen Dokumentation — ist ein strukturiertes Gespräch der effizienteste nächste Schritt. Bei Strukturaflow bieten wir ein unverbindliches 30-Minuten-Beratungsgespräch an, in dem wir gemeinsam auf Ihre konkrete Situation schauen: ohne Verkaufsdruck, ohne vorgefertigte Lösungen. Das Ziel ist Orientierung — damit Sie wissen, was Sie als nächstes tun müssen und was warten kann.