Cybersecurity-Check für KMU

Version 4.0, 28. November 2025

KMU im Visier von Cyberangriffen

Kleine und mittlere Unternehmen (KMU) geraten zunehmend ins Visier von Cyberkriminellen. Laut *Netzwoche* stieg die Zahl der Cyberangriffe in der Schweiz im ersten Quartal 2025 im Vergleich zum Vorjahr um 113 % – ein alarmierender Anstieg. Besonders besorgniserregend ist der Anstieg an KI-gestützten Angriffen, beispielsweise durch Deepfake-Technologien, die gezielt für CEO-Betrugsversuche eingesetzt werden (Quelle: *KMU-Portal des SECO*).

Die häufigsten Ursachen für erfolgreiche Angriffe sind:

- Unzureichender Schutz der Systeme und Prozesse,
- Nicht aktuell gehaltene IT-Systeme,
- Ausnutzung sozialen Verhaltens (Social Engineering)
- Unzureichende Vorbereitung auf Sicherheitsvorfälle.

Der www.cybersecurity-check.ch wurde für KMU im Rahmen der *Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS)* in der ersten Auflage 2020 entwickelt. Die vorliegende, vollständig überarbeitete Fassung 4.0 (Stand November 2025) entstand gemeinsam mit folgenden Partnern: ADSS, BACS, BDO, digitalswitzerland, EXPERTsuisse, Gobugfree, ISSS, SATW, SISA, SNV, SQS, Suissedigital und SVV.

Ein praxisnahes Werkzeug für den Schutz von KMU

Der Cybersecurity-Check bietet KMU konkrete und umsetzbare Handlungsempfehlungen, um das Sicherheitsniveau wirksam zu erhöhen. Er berücksichtigt die aktuelle Bedrohungslage, neue Technologien sowie gesetzliche Anforderungen. Die modulare Struktur und der Fokus auf Praxistauglichkeit erleichtern die Anwendung – auch für Personen ohne technischen Hintergrund.

Mit dem integrierten Selbstcheck können Unternehmen ihren aktuellen Sicherheitsstand einschätzen und erkennen,

- welche technischen, organisatorischen, prozessualen und mitarbeiterbezogenen Schutzmassnahmen bereits umgesetzt wurden,
- und wo gezielt Handlungsbedarf besteht, um ein Mindestmass an Cybersicherheit sicherzustellen.

Hinweis: Der Cybersecurity-Check ersetzt keine individuelle Sicherheitsberatung, bietet jedoch einen fundierten und praxisorientierten Einstieg für KMU.

Inhaltsverzeichnis

1 Organisation & Prozesse

Wieso ist das wichtig?

Cyber-Vorfälle können Unternehmen jeder Grösse treffen – auch KMU. Entscheidend ist nicht nur die Vorbereitung auf den Ernstfall, sondern auch die kontinuierliche Verbesserung und Prävention durch ein hohes organisatorisches Sicherheitsniveau. Wer klare Prozesse etabliert und regelmässig überprüft, kann im Ernstfall schnell reagieren, Schäden begrenzen und den Geschäftsbetrieb rasch wieder aufnehmen.

Ein gutes organisatorisches Sicherheitsniveau bedeutet:

- Klar geregelte Zuständigkeiten,
- regelmässige Sicherung kritischer Informationen,
- sorgfältige Vergabe und Verwaltung von Zugriffsrechten,
- ein durchdachter und getesteter Notfallplan (inkl. alternative Kommunikationskanäle).

Was kann ich tun?

- ☑ Erfassen Sie die IT-Geräte und Anwendungen der geschäftskritischen Prozesse in einem Inventar vollständig, aktuell und schützen Sie die Assets vor unbefugtem Zugriff.
- ☑ Implementieren Sie regelmässige und automatisierte Backups Ihrer geschäftskritischen Daten.
- ☑ Stärken Sie Ihre Benutzerverwaltung durch rollenbasierte Zugriffsrechte und Zwei-Faktor-Authentifizierung.
- ☑ Erstellen und testen Sie einen umfassenden Notfallplan, der aktuelle Bedrohungen berücksichtigt. (z. B. anhand der Notfallplan-Vorlagen von BACS und BDO).

2 Mitarbeitende & Sensibilisierung

Wieso ist das wichtig?

Ausnutzung von sozialem Verhalten (Social Engineering) ist einer der Hauptfaktoren für erfolgreiche Cyberangriffe. Sensibilisierte Mitarbeitende erkennen verdächtige Aktivitäten schneller, vermeiden typische Fehler (z. B. Klick auf Phishing-Mails) und handeln im Ernstfall besonnen. Laut dem BACS verursacht die Social Engineering in über 80 % der Cybervorfälle in Schweizer Unternehmen mindestens einen Teil des Schadens. Eine informierte Belegschaft ist daher der wichtigste Schutzfaktor in Ihrer Cyberstrategie.

Ein gutes Sicherheitsverhalten bedeutet:

- Erkennen verdächtiger Nachrichten und Situationen,
- richtiger Umgang mit Passwörtern und sensiblen Informationen,
- klare Benutzerrichtlinien für IT-Systeme und Kommunikationskanäle,
- fortlaufende Schulung und Übung.

Was kann ich tun?

- ☑ Verankern Sie die **Sensibilisierung** der Mitarbeitenden im Unternehmensalltag.
- ☑ Sorgen Sie mit sicheren **Passwörtern** und Zwei-Faktor-Authentifizierung (2FA) für bestmöglichen Schutz Ihrer Anwendungen.
- ☑ Definieren Sie **Benutzerrichtlinien** für einen sicheren Umgang mit Internet und E-Mails.

3 Technische Schutzmassnahmen

Wieso ist das wichtig?

Technische Sicherheitsmassnahmen bilden das Fundament jeder Cyberabwehr. Ohne aktuelle Systeme, Schutzmechanismen und verschlüsselte Kommunikation bleibt Ihr Unternehmen verwundbar – egal wie gut Organisation und Mitarbeitende geschult sind.

Im Jahr 2025 wurde verstärkt Angriffe automatisiert, insbesondere durch KI-gestützte Schwachstellenscans, Cloud-Ausnutzung und Angriffe über veraltete oder ungeschützte Geräte (z. B. Router, IoT, Remote-Zugänge). Software-Schwachstellen und fehlende Updates gehören nach wie vor zu den häufigsten Einfallstoren für Angreifer.

Ein hohes technisches Schutzniveau bedeutet:

- Aktualisierte Systeme und Anwendungen,
- der Einsatz von Sicherheitssoftware,
- verschlüsselte Kommunikation,
- Schutz aller vernetzten Geräte.

Was kann ich tun?

- ☑ Nutzen Sie geeignete Hard- und **Software** (z. B. Firewalls und Antiviren-Software), um Ihre Sicherheit zu erhöhen.
- ☑ Achten Sie auf eine **regelmässige Aktualisierung** Ihrer Software und Geräte.
- ☑ Verbinden Sie keine **veralteten Geräte**, bei denen kein Softwareupdate verfügbar ist und verbinden Sie nur unbedingt notwendige Systeme mit dem Internet.

Hinweis: Technische Schutzmassnahmen sind **kein Einmalprojekt, sondern ein fortlaufender Prozess**. Führen Sie regelmässige Überprüfungen durch – oder ziehen Sie externe IT-Fachpersonen und zertifizierte Anbieter hinzu, um Lücken zu erkennen und zu schliessen.

4 Datenschutz & Rechtliches

Wieso ist das wichtig?

Der Schutz von Personendaten ist nicht nur ein Vertrauensfaktor gegenüber Kunden, sondern auch gesetzlich vorgeschrieben. Verstösse gegen Datenschutzgesetze können zu hohen Geldbussen, rechtlichen Konsequenzen und massiven Reputationsschäden führen – insbesondere, wenn sie auf Cybervorfälle zurückzuführen sind.

Seit Inkrafttreten des revidierten Schweizer Datenschutzgesetzes (DSG) 2023 sowie der laufenden Umsetzung der EU-Datenschutzgrundverordnung (DSGVO) für Schweizer Unternehmen mit EU-Bezug gilt: Wer Personendaten bearbeitet, muss geeignete technische und organisatorische Massnahmen treffen, um deren Sicherheit zu gewährleisten. Leitungskräfte können bei Datenschutzverletzungen unter Umständen persönlich haftbar werden.

Ein rechtskonformer Umgang mit Daten bedeutet:

- Transparenz über die Datenverarbeitung gegenüber den betroffenen Personen,
- Schutz vor unbefugtem Zugriff und Verlust,
- klare Verantwortlichkeiten und Zuständigkeiten,
- Auftragsdatenbearbeitungsvereinbarung mit externen Dienstleistern (Muster)
- Kenntnis und Einhaltung gesetzlicher Meldepflichten bei Datenschutzverletzung (Leitfaden)

Was kann ich tun?

- ☑ Stellen Sie sicher, dass der Umgang mit Personendaten den Vorgaben des DSG und ggf. der DSGVO entspricht.
- ☑ Dokumentieren Sie, welche Daten Sie erheben, verarbeiten und speichern – und zu welchem Zweck.
- ☑ Ergreifen Sie technische und organisatorische Massnahmen zum Schutz dieser Daten.

Hinweis: Der Datenschutz betrifft alle Bereiche Ihres Unternehmens – von der Website über das CRM bis zum Personalwesen. Er ist keine IT-Aufgabe allein, sondern eine unternehmensweite Verantwortung. Weitere Informationen und Hilfsmittel finden Sie z. B. auf www.edoeb.admin.ch/de/datenschutz oder www.kmu.admin.ch.

5 Externe Partner & Dienstleister

Wieso ist das wichtig?

Viele KMU vertrauen heute auf externe IT-Dienstleister, Cloud-Anbieter oder spezialisierte Softwarelösungen. Das ist sinnvoll – denn qualifizierte Partner bringen Fachwissen, Erfahrung und moderne Technologien mit, die intern oft nicht in gleichem Umfang verfügbar sind. Eine erfolgreiche Zusammenarbeit mit externen Anbietern ist damit ein zentraler Baustein für eine starke Cybersicherheitsstrategie.

Gleichzeitig bleibt es wichtig, klare Vereinbarungen zu treffen, Zuständigkeiten zu definieren und die Einhaltung von Sicherheitsstandards regelmässig zu prüfen. Denn: Auch wenn Aufgaben ausgelagert sind – die Verantwortung für die Sicherheit Ihrer Daten und Systeme bleibt beim Unternehmen selbst.

Ein sicherer Umgang mit externen Partnern bedeutet:

- Auswahl qualifizierter Dienstleister mit nachweisbarer Sicherheitskompetenz,
- schriftlich geregelte Sicherheitsanforderungen,
- transparente Kommunikation und gemeinsame Notfallplanung,
- gezielte Vergabe und Verwaltung von Zugriffsrechten.

Was kann ich tun?

- ☑ Arbeiten Sie mit qualifizierten IT-Partnern zusammen, die Sicherheitsstandards (CyberSeal, SN EN ISO/IEC 27001) nachweisen können.
- ☑ Halten Sie technische und organisatorische Anforderungen schriftlich fest.
- ☑ Integrieren Sie Ihre IT-Dienstleister aktiv in die Notfallplanung und Sicherheitsprozesse.

Hinweis: Auch wenn ein Anbieter "alles für Sie übernimmt", bleiben Sie als Unternehmen in der Verantwortung (auch für die Sicherstellung des Backups und Wiederherstellbarkeit der Daten). Prüfen Sie regelmässig, ob Ihre Partner, die für Ihre Branche und Unternehmensgrösse angemessenen Sicherheitsmassnahmen einhalten.

Bei Fragen zur Auswahl geeigneter Anbieter oder zur Vertragsgestaltung helfen nationale Plattformen wie BACS - Informationen für Unternehmen, Allianz Digitale Sicherheit Schweiz - CyberSeal, ITSec4KMU oder Ihre Branchenverbände weiter.

6 Penetration Testing & Schwachstellenanalysen

Wieso ist das wichtig?

Selbst gut gemeinte Sicherheitsmassnahmen helfen nur dann, wenn sie auch tatsächlich funktionieren. Schwachstellen in Systemen, Netzwerken oder Anwendungen bleiben oft unbemerkt – bis sie von Angreifern ausgenutzt werden. Deshalb ist es entscheidend, die eigene IT-Infrastruktur regelmässig zu testen – idealerweise durch qualifizierte unabhängige Dritte.

Gerade im Jahr 2025, wo Angreifer zunehmend automatisierte und KI-gestützte Scans einsetzen, um gezielt Schwachstellen in Unternehmen zu identifizieren, ist ein proaktiver Ansatz zentral. Ein Penetration Test (kurz: Pentest) simuliert reale Angriffe – kontrolliert, nachvollziehbar und mit dem Ziel, Schwachstellen frühzeitig zu erkennen und zu beheben.

Ein professioneller Test bringt:

- Klarheit über tatsächliche Sicherheitslücken,
- realistische Einschätzung des Risikos,
- konkrete Handlungsempfehlungen zur Verbesserung.

Was kann ich tun?

- ☑ Führen Sie regelmässig eine Schwachstellenanalyse Ihrer Systeme durch – intern oder durch externe Fachpersonen.
- ☑ Lassen Sie einmal jährlich oder bei wesentlichen Systemveränderungen bei geschäftskritischen Systemen einen Penetration Test durchführen.
- ☑ Beheben Sie identifizierte Schwachstellen systematisch und dokumentieren Sie die Massnahmen.

Hinweis: Für kleinere KMU können bereits standardisierte Schwachstellenscans ein wichtiger erster Schritt sein. Plattformen wie GoBugFree oder ITSec4KMU bieten praxisnahe Unterstützung. Wer weitergehen möchte, kann mit Partnern aus dem Cybersecurity-Netzwerk (z. B. SCD-DNA, Allianz Digitale Sicherheit Schweiz - CyberSeal) geeignete Anbieter identifizieren.

Info-Box: Penetration Testing vs. Ethical Hacking

Penetration Testing (Pentest)

Ein klar abgegrenzter, strukturierter und zielgerichteter Test, der sich auf einen definierten Bereich (z. B. Webanwendung, Netzwerksegment) konzentriert. Ziel ist die Identifikation technischer Schwachstellen und deren Bewertung.

Ethical Hacking (Friendly Hacking)

Ein breiterer, weniger strikt strukturierter Ansatz, der wie ein echter Angreifer vorgeht – jedoch autorisiert. Dabei werden technische, organisatorische und konzeptionelle Schwachstellen im gesamten Unternehmen geprüft.

Ein Pentest kann ein Teil eines umfassenden Ethical-Hacking-Projekts sein, ist aber deutlich enger gefasst und methodisch standardisiert.

7 Cybersecurity Selbstcheck

Wie gut ist Ihr Unternehmen vor Angriffen aus dem Cyberspace geschützt und darauf vorbereitet? Prüfen Sie jetzt, ob Sie die grundlegenden Anforderungen erfüllen.

1. Organisation & Prozesse	ja	nein	weiss nicht
Sind die Ansprechpersonen bekannt für IT-Sicherheit (intern oder extern)?			
Wird das Thema Cybersicherheit regelmässig in Führungsmeetings behandelt?			
Ist Cybersicherheit Teil Ihres Risikomanagement und in Führungsmeeting thematisiert?			
Haben Sie alle IT-Ressourcen und die geschäftskritischen Prozesse Ihres Unternehmens vollständig erfasst und dokumentiert?			
Sind System- und Anbieterunabhängige Backups vorhanden und wiederherstellbar?			
Bewahren Sie mindestens ein Backup an einem sicheren, offline externen Ort auf?			
Testen Sie regelmässig die Wiederherstellung Ihrer Daten aus den Backups?			
Verwenden Sie getrennte Benutzerkonten für administrative und normale Tätigkeiten?			
Haben alle Benutzerinnen und Benutzer ausschliesslich die für ihre Aufgaben nötigen Zugriffsrechte (Prinzip der minimalen Berechtigung)?			
Werden die Zugriffsrechte konsequent rollenbasiert (z. B. Buchhaltung, Personal, IT) vergeben?			
Nutzen Sie ausschliesslich persönliche Benutzerkonten und keine geteilten Accounts?			
Wird sichergestellt, dass Passwörter von Firmen- und Gruppenaccounts umgehend bei Mitarbeiteraustritten geändert werden.			
Deaktivieren Sie Benutzerkonten umgehend bei Austritten oder Rollenwechseln?			
Haben Sie geschäftskritische Systeme, Daten und Informationen identifiziert und dokumentiert?			
Gibt es definierte Rückfallebenen wie Ersatzgeräte oder Notvereinbarungen mit Lieferanten?			
Ist dokumentiert, wer mit welchen Systemen arbeitet, inklusive Kontaktdaten?			
Haben Sie Sofortmassnahmen im Notfall definiert und ist der Notfallplan offline verfügbar, z. B. Trennung betroffener Systeme vom Netzwerk?			
Haben Sie Massnahmen geplant, um die Arbeitsfähigkeit rasch wiederherzustellen (z. B. Ausdruck wichtiger Kontaktdaten)?			
Sind Rollen und Zuständigkeiten im Notfallplan klar definiert (z. B. IT-Reaktion, rechtliche Abklärung, Kommunikation, Behördenmeldung)?			
Üben Sie regelmässig mit Ihrem Team den Notfallplan?			

2. Mitarbeitende & Sensibilisierung	ja	nein	weiss nicht
Führen Sie eine Basisschulung zur Cybersicherheit für alle Mitarbeitenden durch?			
Beinhaltet die Schulung Themen wie den Nutzen von IT-Sicherheit, den Umgang mit Logins, sicheren Umgang mit Informationen, sowie sicheren Umgang mit Internet und E-Mail?			
Wiederholen Sie diese Schulung regelmässig (z. B. jährlich)?			
Verwenden Sie reale Beispiele wie Phishing, CEO-Fraud oder Deepfakes in der Schulung?			
Verhindern Sie das unkontrollierte Anstecken von Geräten wie Handys an USB-Anschlüsse von Arbeitsgeräten?			
Fördern Sie eine Kultur, in der Mitarbeitende bei Unsicherheiten offen kommunizieren und Unterstützung suchen können – ganz ohne Schuldzuweisung?			
Machen Sie Cybersicherheit intern sichtbar – z. B. durch Poster, Newsletter oder Kurzvideos?			
Nutzen Ihre Passwörter mindestens 12 Zeichen sowie Gross-/Kleinbuchstaben, Zahlen und Sonderzeichen?			
Empfehlen oder verwenden Sie Passwortmanager im Unternehmen?			
Setzen Sie überall dort, wo möglich, Zwei-Faktor-Authentifizierung (2FA) ein?			
Vermeiden Sie die Mehrfachnutzung von Passwörtern? Überprüfen Sie regelmässig, ob Passwörter von Ihren Mitarbeiter-/innen kompromittiert wurden (Have I Been Pwned?)			
Haben Sie klare, verständliche Benutzerrichtlinien für E-Mail, Internet, Social Media und mobile Geräte definiert?			
Ist die Weitergabe von Login-Daten ausdrücklich untersagt?			
Sensibilisieren Sie Ihre Mitarbeitenden für verdächtige E-Mails (z. B. von unbekannten Absendern oder mit ungewöhnlichem Stil)?			
Wird vor der Nutzung öffentlicher, ungesicherter WLANs gewarnt?			
Ist die Installation unbekannter Apps oder Software geregelt (Desktop und Mobil)?			
Ist auch die Geschäftsleitung aktiv sensibilisiert und handelt als Vorbild in Sachen Cybersicherheit?			

3. Technische Schutzmassnahmen	ja	nein	weiss nicht
Sind automatische Updates für Betriebssysteme, Anwendungen und Cloud-Dienste aktiviert?			
Überprüfen Sie regelmässig den Update-Stand aller Geräte, inkl. Drucker, Router, Kameras oder Smartphones?			
Nutzen Sie zentrale Verwaltungstools für das Patch-Management (wenn technisch und betrieblich sinnvoll)?			
Werden Geräte ohne Update-Möglichkeit konsequent vom Internet getrennt oder ersetzt?			
Verwenden Sie eine Endpoint-Protection Lösung (inklusive Anti-Viren-Software) zur Erkennung und Verhinderung verdächtigen Verhaltens?			
Ist eine Firewall aktiv, die unautorisierte Zugriffe blockiert?			
Setzen Sie bei mobilen Geräten Mobile-Device-Management-Lösungen ein oder prüfen deren Einsatz?			
Verwenden Sie verschlüsselte Verbindungen (z. B. VPN) für E-Mail, Dateiübertragungen und Fernzugriffe?			
Erzwingen für externe Systemzugriffe konsequent starke Authentisierung (Zwei-Faktor-Authentifizierung (2FA), Passkeys) ein?			
Haben Sie Ihr Netzwerk segmentiert, um sensible Systeme (z. B. Buchhaltung) von allgemeiner Nutzung (z. B. Gäste-WLAN) zu trennen?			
Sind ungenutzte Schnittstellen wie offene USB-Ports oder Bluetooth deaktiviert?			
Sind Serverräume physisch gesichert, und gibt es keine frei zugänglichen Netzwerkanschlüsse in öffentlichen Bereichen?			

4. Datenschutz & Rechtliches	ja	nein	weiss nicht
Führen Sie ein vollständiges Verzeichnis aller Personendaten, die im Unternehmen verarbeitet werden (z. B. Kundendaten, Mitarbeiterdaten, Logindaten)?			
Haben Sie zu jeder Datenart den Zweck der Erhebung dokumentiert (z. B. Vertragsabwicklung, Marketing, HR)?			
Haben Sie geprüft, ob für jede Datenverarbeitung eine gültige Rechtsgrundlage vorliegt (z. B. Einwilligung, Vertrag, gesetzliche Pflicht)?			
Wenden Sie auf Personendaten dieselben technischen Schutzmassnahmen an wie auf Ihre übrigen Unternehmensdaten (z. B. Zugriffskontrolle, Verschlüsselung, Backup)?			
Ist sichergestellt, dass nur autorisierte Personen auf personenbezogene Daten zugreifen können?			
Ist eine Datenschutzerklärung auf Ihrer Website vorhanden?			
Geben Sie betroffenen Personen die Möglichkeit, Auskunft über ihre Daten zu verlangen sowie deren Berichtigung oder Löschung zu beantragen?			
Gibt es in Ihrem Unternehmen einen definierten Ablauf für den Umgang mit Datenschutzvorfällen (z. B. gestohlene Kundendaten)?			
Können Sie sicherstellen, dass meldepflichtige Datenschutzverletzungen innerhalb von 72 Stunden dem EDÖB gemeldet werden?			
Werden betroffene Personen informiert, wenn durch eine Datenschutzverletzung ihre Rechte verletzt sein könnten?			
Haben Sie mit allen Auftragsbearbeitern (das sind Partner, welche für ihre Organisation Personendaten bearbeiten) eine schriftliche Auftragsverarbeitungsvereinbarung abgeschlossen?			
Überprüfen Sie, ob Ihre IT-Dienstleister angemessene Sicherheitsstandards erfüllen (z. B. CyberSeal)?			

5. Externe Partner & Dienstleister	ja	nein	weiss nicht
Achten Sie bei der Auswahl von IT- und Cloud-Anbietern auf anerkannte Sicherheitszertifikate (z. B. CyberSeal)?			
Lassen Sie sich regelmässig Nachweise über aktuelle Schutzmassnahmen wie Patch-Management, Backups und Notfallprozesse geben?			
Verwenden Sie Hilfsmittel wie den Cybersecurity-Schnelltest für KMU zur Anforderungsklärung mit potenziellen Anbietern?			
Gibt es schriftliche Vereinbarungen inkl. Service Level Agreements (SLA) zur Zusammenarbeit mit externen Partnern, insbesondere bei Datenverarbeitung oder Systemzugriffen?			
Haben Sie darin Zugriffsrechte, Meldepflichten bei Sicherheitsvorfällen und den Datenverarbeitungsort (z. B. Schweiz, EU, Drittstaat) definiert?			
Sind externe Partner in Ihre Notfallplanung eingebunden (z. B. wer, wann, wie informiert wird)?			
Planen und führen Sie gemeinsame Sicherheitsübungen oder Tests durch (z. B. Reaktion auf Phishing oder Ausfälle)?			
Erhalten Sie regelmässige, proaktive Status-Updates zur Sicherheitslage von Ihren Dienstleistern?			
Erhalten externe Personen nur minimal notwendige Zugriffsrechte (Prinzip der geringsten Berechtigung)?			
Dokumentieren Sie klar, wer Zugriff auf welche Systeme hat – inklusive Dauer und Zweck?			
Werden Zugänge von Externen unmittelbar entfernt, wenn sie nicht mehr benötigt werden (z. B. nach Projektabschluss)?			

Vorbemerkung: Dies trifft vor allem für KMU zu, die eigene Lösungen entwickeln und betreiben bzw. die mit dem Internet direkt verbunden sind

6. Penetration Testing & Schwachstellenanalysen	ja	nein	weiss nicht
Klären Sie vorab den Testumfang (z. B. Netzwerk, Webanwendungen, Remote-Zugänge, WLAN)?			
Setzen Sie identifizierte Massnahmen aus Schwachstellenanalysen und Penetration Tests priorisiert um – insbesondere bei hohem Risiko?			
Dokumentieren Sie die ergriffenen Massnahmen (z. B. durchgeführte Updates, Konfigurationsänderungen)?			
Führen Sie Nachtests durch, um zu prüfen, ob erkannte Schwachstellen vollständig behoben wurden?			
Gibt es klare Kriterien, wann Schwachstellenanalysen oder Penetration Tests durchgeführt werden (z. B. nach Updates, jährlich)?			
Sind diese Tests als fester Bestandteil Ihrer IT-Sicherheitsstrategie verankert?			

8 Anhang

Nützliche Links

Behörden & Offizielle Stellen

- **Bundesamt für Cybersicherheit (BACS) – „Schützen Sie Ihr KMU“**
  Offizielle Leitfäden, Checklisten, Empfehlungen für KMU.
  Bundesamt für Cybersicherheit BACS – Schützen Sie Ihr KMU
  Bundesamt für Cybersicherheit BACS – Informationen für Unternehmen
- **Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)**
  Leitfäden, Muster, FAQ, rechtliche Vorgaben zum Schweizer Datenschutzgesetz (DSG).
  Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) – Datenschutz
- **Meldeformular Cyberangriffe (BACS)**
  Online-Meldung von Vorfällen für Unternehmen.
  Bundesamt für Cybersicherheit BACS – Meldeformular

Branchenspezifische Unterstützungsangebote

- **CyberSeal – Gütesiegel der Allianz Digitale Sicherheit Schweiz**
  Zeichnet IT-Dienstleister aus, die ein angemessenes Schutzniveau gewährleisten – hilft KMU bei der Auswahl vertrauenswürdiger IT-Partner.
  Allianz Digitale Sicherheit Schweiz – CyberSeal
- **GObugfree – Ehtical Hacking & Schwachstellenplattform**
  Lösung für KMU zur Identifikation und Meldung von Schwachstellen.
  GObugfree
- **ITsec4KMU – Prävention und Abwehr von Cyberangriffen für Schweizer KMU**
  Kostenlose, praxisorientierte Selbstevaluation und Leitfäden für KMU.
  ITSec4KMU
- **Suissedigital – KMU Security Check**
  Niederschwelliger Sicherheitscheck für KMU der digitalen Kommunikationsbranche.
  Suissedigital – KMU Security Check
- **Swiss Cyber Defence DNA (SCD-DNA)**
  Modell zur systematischen Erfassung und Verbesserung der Cybersicherheit für KMU.
  SWISS CYBER DEFENCE DNA

Sensibilisierung & Schulungsmaterial

- **SUPERR Kampagne**
  Nationale Kampagne für Cybersicherheits-Basisschutz – einfach verständliche Tipps für Mitarbeitende.
  Machen - Cybersicherheit ist S-U-P-E-R.ch
- **Cybernavi**
  Interaktive Aufklärungs- und Schulungsplattform zu Cyberrisiken, speziell für KMU und Mitarbeitende.
  Cybernavi

Normen & Standards (für Anbieterbewertungen sinnvoll)

- **SNV – Schweizerische Normen-Vereinigung**
  Information zu ISO/IEC-Normen, u. a. 27001, 27002 und 27701.
  Schweizerische Normen-Vereinigung - SNV
- **SQS – Zertifizierungsstelle für Informationssicherheit**
  Zertifizierungen, Auditmodelle und Branchenstandards (z. B. ISO 27001, Datenschutzstandards).
  Schweizerische Vereinigung für Qualitäts- und Managementsysteme | SQS Schweiz

Kontaktadressen für Notfälle

Polizei (Cyberkriminalität):
Notrufnummer: 117
Kantonale Polizeistellen bieten spezialisierte Cybercrime-Dienste.
www.fedpol.admin.ch

Bundesamt für Cybersicherheit (BACS):
Meldeformular für Cybervorfälle in der Schweiz
Online-Meldung: BACS - Meldeformular

Rechtsberatung bei Cybervorfällen:
Viele Kantone und Branchenverbände bieten spezialisierte Rechtsdienste an. Alternativ:

- BDO Cybersecurity & Recht: www.bdo.ch
- Datenschutzexperten: www.edoeb.admin.ch

Glossar

2FA (Zwei-Faktor-Authentifizierung)
Zusätzliche Sicherheitsschicht, die beim Login zwei unabhängige Faktoren benötigt (z. B. Passwort + SMS-Code oder App-Bestätigung).

Asset
Wertgegenstand eines Unternehmens im IT-Kontext, z. B. Server, Software, Daten oder Endgeräte.

Backup
Kopie wichtiger Daten, die getrennt vom Produktivsystem gespeichert wird, um sie nach einem Vorfall wiederherstellen zu können.

Bluetooth
Drahtlose Nahfunktechnologie. Offene oder ungeschützte Bluetooth-Verbindungen können ein Sicherheitsrisiko darstellen.

Cloud-Dienst
Externe IT-Ressource, die über das Internet bereitgestellt wird (z. B. Microsoft 365, Google Workspace). Erfordert klare Sicherheits- und Zugriffsregeln.

Cyberangriff
Versuch, IT-Systeme zu kompromittieren, Daten zu stehlen, zu manipulieren oder den Betrieb zu stören.

CyberSeal
Schweizer Gütesiegel, das IT-Dienstleister auszeichnet, die mit geeigneten technischen und organisatorischen Massnahmen ihren Kunden ein angemessenes Schutzniveau vor Cyberrisiken garantieren.

Datenschutzverletzung
Unbefugter Zugriff, Verlust oder Offenlegung von Personendaten. Gesetzlich meldepflichtig, wenn ein Risiko für betroffene Personen besteht.

DLP (Data Loss Prevention)
Werkzeuge oder Policies, die verhindern, dass vertrauliche Informationen verloren gehen oder unerlaubt weitergegeben werden.

Endpoint Protection
Sicherheitssoftware für Endgeräte wie Notebooks, Smartphones oder Server. Erkennung von Malware, verdächtigem Verhalten und Angriffen.

Ethical Hacking (Friendly Hacking)
Autorisiertes Angriffsszenario, bei dem alle erdenklichen Schwachstellen (technisch, organisatorisch, prozessual) geprüft werden.
→ Pentesting ist ein Teil davon, aber enger und klar definiert.

Firewall
Sicherheitskomponente, die den Datenverkehr überwacht und unerlaubte Zugriffe blockiert.

IoT (Internet of Things)
Mit dem Internet verbundene Geräte wie Kameras, Sensoren oder Router. Oft ein Einfallstor bei fehlenden Updates.

MDM (Mobile Device Management)
Software zur zentralen Verwaltung und Absicherung mobiler Geräte wie Smartphones oder Tablets.

Malware
Schädliche Software wie Viren, Trojaner oder Ransomware.

Netzwerksegmentierung
Aufteilung eines Netzwerks in getrennte Bereiche, um Angriffe zu begrenzen (z. B. Gäste-WLAN getrennt von Buchhaltung).

Notfallplan (Incident Response Plan)
Dokument, das beschreibt, wie ein Unternehmen bei einem Cybervorfall reagieren soll.

Passkeys
Passwortlose Authentisierungsmethode, die kryptografische Schlüssel nutzt. Deutlich sicherer als klassische Passwörter.

Patch / Patch-Management
Software-Update zur Schliessung von Sicherheitslücken.
Patch-Management = systematisches Aktualisieren aller Geräte und Anwendungen.

Pentest (Penetration Test)
Gezielter, definierter Test, der Schwachstellen in einem festgelegten Bereich identifiziert. Strukturierter, methodischer Ansatz.

Phishing
Manipulative Nachricht (meist E-Mail), um Logins, Daten oder Geld zu erbeuten.

Ransomware
Schadsoftware, die Daten verschlüsselt und Lösegeld verlangt.

Rolling Backup / Offline-Backup
Backup, das getrennt vom Netzwerk aufbewahrt wird (z. B. externes Laufwerk, Tape). Schutz vor Ransomware.

Social Engineering
Manipulation von Menschen, um vertrauliche Informationen oder Zugänge zu erhalten.

VPN (Virtual Private Network)
Verschlüsselte Verbindung, die sichere Kommunikation über das Internet ermöglicht.

WLAN (Wireless Local Area Network)
Kabelloses Netzwerk. Öffentliche oder schlecht gesicherte WLANs können Angriffe erleichtern.

Zero Trust
Sicherheitsprinzip: „Traue niemandem – überprüfe alles." Keine automatische Vertrauensstellung innerhalb oder ausserhalb des Unternehmens.