avolut

Cybersicherheit in der Praxis: Ein Leitfaden für KMU

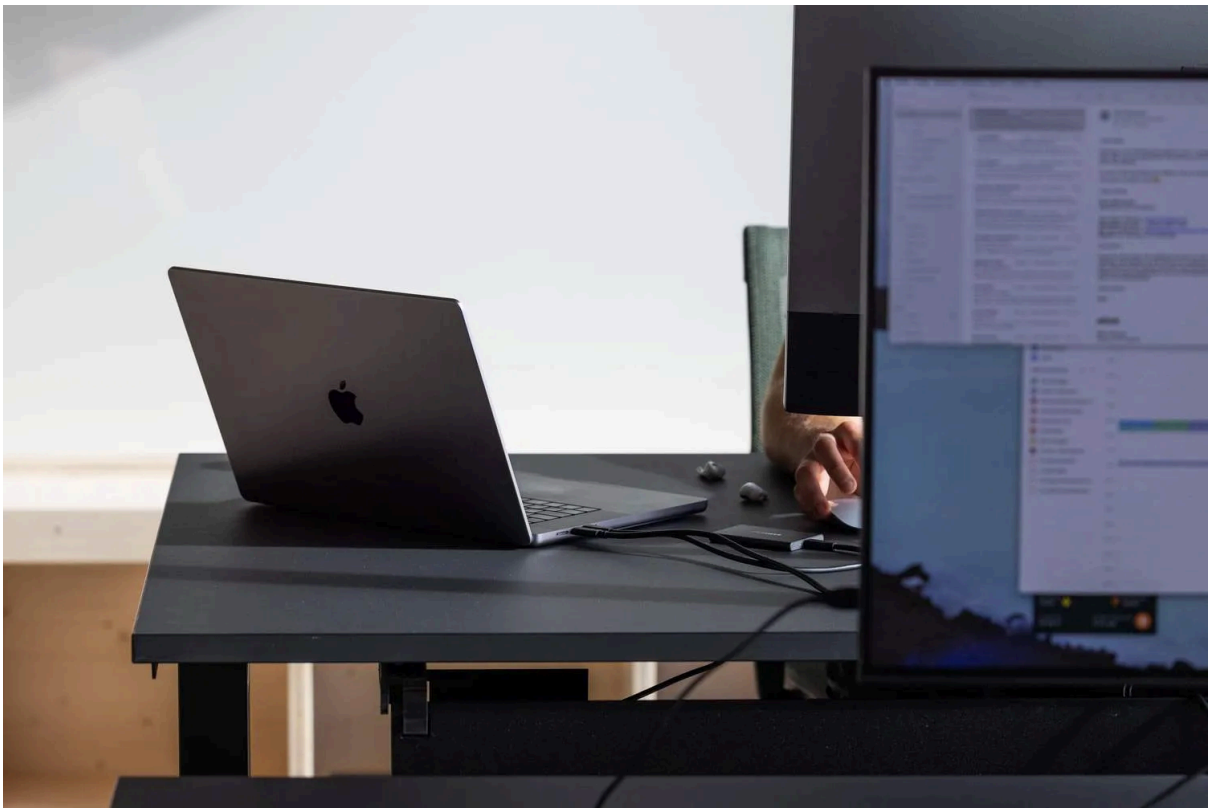
Version 1.0: 15.9.2025

Ansprechpartner

Philippe Regenass
regenass@avolut.ch

avolut solutions AG
Kanalstrasse 8
8953 Dietikon

avolut



Dieser Leitfaden wurde von Avolut Solution AG zusammengestellt, um KMU eine praxisnahe Hilfestellung zu geben, wie sie ein grundlegendes Schutzniveau in der Cybersecurity erreichen und sich damit besser vor den häufigsten Cyberangriffen schützen können.

Gerade kleine und mittlere Unternehmen sind zunehmend Ziel von Cyberattacken, die gravierende Auswirkungen haben können. Bereits wenige, aber gezielte Massnahmen reichen aus, um ein Mindestniveau an Schutz gegenüber den gängigsten Bedrohungen aufzubauen. In diesem Leitfaden werden diese Massnahmen klar, verständlich und konkret erläutert – speziell abgestimmt auf die Bedürfnisse von KMU.

Mit diesem Leitfaden möchte die Avolut Solution AG dazu beitragen, dass Schweizer KMU ihre Widerstandsfähigkeit gegen Cyberrisiken nachhaltig stärken können.

avolut

Sicherheit in Organisation und Prozessen

Warum ist das wichtig?

Im Falle eines Cybervorfalls entscheidet die richtige Vorbereitung und eine schnelle Reaktion darüber, ob und wie rasch Ihr Unternehmen den Betrieb fortsetzen kann. Eine strukturierte Vorgehensweise kann Schäden deutlich reduzieren oder im besten Fall sogar verhindern. Dafür ist es entscheidend, die eigene Organisation klar auf Cyber-Bedrohungen auszurichten und passende Prozesse zu etablieren – etwa regelmässige Datensicherungen, eine sorgfältige Vergabe von Zugriffsrechten sowie einen klar definierten Notfallplan.

Was können Sie tun?

- ☐ Führen Sie regelmässige Backups Ihrer geschäftskritischen Daten durch.
- ☐ Richten Sie eine strukturierte Benutzer- und Rechteverwaltung ein.
- ☐ Erarbeiten Sie einen Notfallplan für den Ernstfall.

Wie gehen Sie vor?

Daten sichern: Backup als Routine

- Erstellen Sie regelmässig – idealerweise automatisiert – Backups auf ein geeignetes Speichermedium (z. B. externe Festplatte, Cloud-Lösung, je nach Geschäftsmodell und regulatorischen Vorgaben)
- Lagern Sie diese Backups geschützt und getrennt vom Unternehmensnetzwerk (Offline-Backup)
- Testen Sie in regelmässigen Abständen, ob sich die Daten im Ernstfall zuverlässig wiederherstellen lassen

Angriffsfläche minimieren: Benutzeradministration optimieren

Eine saubere Benutzer- und Rechteverwaltung erschwert Angreifern den Zugang zu sensiblen Informationen.

- Trennen Sie administrative Konten strikt von regulären Benutzerkonten
- Vergeben Sie nur so viele Zugriffsrechte wie unbedingt nötig (Prinzip der minimalen Rechte)
- Verwenden Sie möglichst ausschliesslich persönliche Konten und vermeiden Sie gemeinsame Logins
- Richten Sie rollenbasierte Zugriffsrechte ein (z. B. Buchhaltung, Personal, IT-Administration, Verkauf)
- Stellen Sie sicher, dass Benutzerkonten und Zugangsdaten bei Austritten umgehend deaktiviert werden

avolut

Vorsorge für den Ernstfall: Notfallplans

Ein Cybervorfall trifft Unternehmen oft unvorbereitet. Mit einem Notfallplan stellen Sie sicher, dass im Ernstfall klar ist, wie vorzugehen ist. So gewinnen Sie Zeit, vermeiden Chaos und können Schäden deutlich verringern.

Was können Sie tun?

- ☐ Identifizieren Sie kritische Systeme und Daten
- ☐ Legen Sie Rückfallebenen und Alternativen fest
- ☐ Definieren Sie klare Abläufe, Zuständigkeiten und Kommunikationswege
- ☐ Üben Sie den Ernstfall regelmässig mit Ihrem Team

Wie gehen Sie vor?

- ☐ Kritische Systeme bestimmen
  - ☐ Erfassen Sie, welche Systeme und Daten im Notfall unverzichtbar sind (z. B. Mail, Adressdatenbank, Terminkalender, Kundendaten)
- ☐ Rückfallebenen definieren
  - ☐ Planen Sie Ersatzmöglichkeiten wie Reserve-PCs, mehrere Browser pro Arbeitsplatz oder klare Vereinbarungen mit Lieferanten zu Reaktionszeiten
- ☐ Verantwortlichkeiten und Abläufe festlegen
  - ☐ Dokumentieren Sie, wer für welches System zuständig ist, inkl. Name und Telefonnummer
  - ☐ Definieren Sie die ersten Schritte im Ernstfall: Betroffene Systeme sofort vom Netz trennen (Kabel und WLAN)
  - ☐ Legen Sie fest, wie eine schnelle Wiederherstellung erfolgen soll (z. B. Ausdruck wichtiger Kontaktdaten als Offline-Kopie)
- ☐ Kommunikations- und Eskalationswege klären
  - ☐ Bestimmen Sie Ansprechpersonen für:
    - ☐ Technische Unterstützung bei IT-Vorfällen
    - ☐ Rechtliche Sofortmassnahmen (z. B. bei Datenabfluss Rechtsberatung kontaktieren)
    - ☐ Kommunikationsmassnahmen (intern und extern)
  - ☐ Offizielle Meldungen: Vorfälle an Polizei und das Nationale Zentrum für Cybersicherheit (NCSC) melden
  - ☐ Bei finanziellen Schäden sofort Bank und Polizei kontaktieren, um Zahlungen zu stoppen
- ☐ Notfallplan trainieren
  - ☐ Üben Sie regelmässig die Abläufe, damit alle Beteiligten im Ernstfall sicher handeln

avolut

Sicherheit dank dem Faktor Mensch

Warum ist das wichtig?

Technische Schutzmassnahmen allein reichen nicht aus – der Mensch bleibt der entscheidende Faktor. Mitarbeitende, die Gefahren kennen, sichere Passwörter verwenden und die wichtigsten Regeln im Alltag beachten, erhöhen das Sicherheitsniveau Ihres Unternehmens erheblich.

Was können Sie tun?

- ☐ Fördern Sie das Bewusstsein für Cybergefahren im Arbeitsalltag
- ☐ Setzen Sie auf sichere Passwörter und Multi-Faktor-Authentisierung
- ☐ Etablieren Sie klare Benutzerrichtlinien für den Umgang mit Internet und E-Mails

Wie gehe ich vor?

Sicherheit zum Thema machen: Sensibilisierung

- ☐ Behandeln Sie IT-Sicherheit regelmässig im Unternehmen und machen Sie sicheres Verhalten im Internet zu einem festen Bestandteil des Arbeitsalltags.
- ☐ Führen Sie eine Grundschulung für Ihre Mitarbeitenden durch – mit Themen wie:
  - ☐ Warum ist IT-Sicherheit wichtig?
  - ☐ Was sind starke Passwörter und wie erstellt man sie?
  - ☐ Wie gehe ich sicher mit Internet und E-Mail um?

Anwendungen schützen: Starke Passwörter

- ☐ Verwenden Sie lange, komplexe Passwörter mit mindestens 12 Zeichen – bestehend aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- ☐ Nutzen Sie einen Passwortmanager und lassen Sie Passwörter automatisch generieren.
- ☐ Alternativ können Sie einen Passsatz verwenden: Wählen Sie einen persönlichen Satz, den niemand erraten kann, und bilden Sie daraus ein

Passwort (z. B. durch die ersten Buchstaben jedes Wortes). Vermeiden Sie bekannte Redewendungen oder Zitate.

- ☐ Verwenden Sie niemals dasselbe Passwort für mehrere Dienste (z. B. E-Mail, Online-Banking, Buchhaltung, CRM).
- ☐ Aktivieren Sie wenn möglich die Zwei-Faktor-Authentifizierung (z. B. Einmalpasswort-App, SMS-Code, Token).
- ☐ Geben Sie Ihr Passwort nie auf Webseiten ein, die Sie über Links erreicht haben – tippen Sie die Adresse immer manuell in die Browserzeile ein.
- ☐ Ändern Sie Standard- oder gemeinsam genutzte Passwörter sofort und deaktivieren Sie Zugangsdaten, wenn Mitarbeitende das Unternehmen verlassen.

Sicherer Umgang mit Internet und E-Mail: Benutzerrichtlinien

Erstellen Sie klare Regeln für den Umgang mit Online-Diensten. Diese sollten mindestens beinhalten:

- ☐ Login-Daten (Benutzername und Passwort) niemals weitergeben.
- ☐ Kreditkartendaten nur auf vertrauenswürdigen Webseiten eingeben – achten Sie auf https:// in der Browserzeile
- ☐ Keine unbekannten Programme aus dem Internet herunterladen.
- ☐ Öffentliche, ungeschützte WLANs meiden – insbesondere beim Online-Banking. Verwenden Sie stattdessen Ihr Smartphone als persönlichen Hotspot. Vorsicht beim Umgang mit E-Mails
- ☐ Seien Sie grundsätzlich misstrauisch bei eingehenden E-Mails und achten Sie auf folgende Punkte:
    - ☐ Öffnen Sie keine Anhänge und klicken Sie keine Links an, wenn Ihnen eine E-Mail verdächtig vorkommt (z. B. ungewohnte Absenderadresse, Schreibfehler, untypische Formulierungen oder falsche Logos)
    - ☐ Geben Sie niemals vertrauliche Informationen preis, wenn Sie Zweifel haben. Versuchen Sie stattdessen, den Absender über einen anderen Weg (z. B. telefonisch) zu erreichen, um die Echtheit zu überprüfen
    - ☐ Prüfen Sie auch E-Mails kritisch, die scheinbar von bekannten Personen oder leitenden Mitarbeitenden stammen. Angreifer können kompromittierte Postfächer nutzen und täuschend echte Nachrichten versenden

avolut

Sicherheit durch technische Massnahmen

Warum ist das wichtig?

Ungepatchte Sicherheitslücken sind ein Einfallstor für Cyberangriffe. Kriminelle können Daten löschen, manipulieren oder Ihre Systeme für ihre Zwecke missbrauchen. Updates schliessen solche Lücken.
Eine aktuelle Firewall schützt vor unbefugten Zugriffen, Antiviren-Software vor Schadprogrammen. Ohne Verschlüsselung können Angreifer zudem Ihren Datenverkehr abfangen und verändern.

Was können Sie tun?

- ☐ Setzen Sie geeignete Sicherheitssoftware ein (z. B. Firewall, Antiviren-Software)
- ☐ Halten Sie alle Systeme und Programme regelmässig aktuell.
- ☐ Entfernen oder trennen Sie Geräte, für die es keine Updates mehr gibt, vom Internet

Wie gehen Sie vor?

Mit Soft- und Hardware die Sicherheit erhöhen

- ☐ Aktualisieren Sie Betriebssystem, Firewall und Anwendungen regelmässig
- ☐ Prüfen Sie regelmässig, ob Updates verfügbar sind, und installieren Sie diese sofort
- ☐ Nutzen Sie, wo immer möglich, automatische Updates – auch bei Geräten wie Druckern, IoT-Systemen, Smartphones oder Steuerungsanlagen
- ☐ Trennen Sie Geräte, für die keine Updates mehr bereitgestellt werden, vom Netz oder ersetzen Sie diese
- ☐ Installieren Sie eine aktuelle Antiviren-Software und halten Sie diese stets auf dem neuesten Stand. Für zusätzlichen Schutz können Sie zwei verschiedene Virenscanner parallel einsetzen
- ☐ Verschlüsseln Sie Ihre Kommunikation, z. B. durch den Einsatz eines Virtual Private Networks (VPN)

avolut

Cybersicherheit als Teil des Datenschutzes

Warum ist das wichtig?

Ihr Unternehmen trägt die Verantwortung für den sicheren Umgang mit Personendaten und geistigem Eigentum. Kommt es zu Datenverlust oder Datenschutzverletzungen, drohen hohe Geldstrafen, strafrechtliche Folgen und ein schwerer Reputationsschaden – im schlimmsten Fall sogar eine existenzielle Bedrohung für das Unternehmen.

Seit 2018 gilt die Datenschutz-Grundverordnung (DSGVO / GDPR) der EU, die auch Schweizer Unternehmen betreffen kann. Dies ist der Fall, wenn Sie Daten von EU-Bürgerinnen und -Bürgern verarbeiten oder Ihre Dienstleistungen gezielt im EU-Raum anbieten. Dazu zählen beispielsweise auch Webseiten, die über Cookies das Verhalten von Besuchern aus der EU nachverfolgen.

Cybersicherheit und Datenschutz sind eng miteinander verknüpft: Ein Cyberangriff kann den Verlust oder Missbrauch sensibler Daten verursachen – mit gravierenden rechtlichen und finanziellen Konsequenzen.

Was können Sie tun?

- ☐ Stärken Sie Ihre Cybersicherheit, um zugleich die Einhaltung der Datenschutzgesetze zu unterstützen
- ☐ Stellen Sie sicher, dass Personendaten jederzeit angemessen geschützt sind

Wie gehen Sie vor?

Datenschutz im Alltag umsetzen

- ☐ Sobald Sie Personendaten (z. B. von Kunden oder Mitarbeitenden) erfassen oder bearbeiten, müssen diese geschützt werden
- ☐ Als Datenbearbeitung gilt jeder Umgang mit Daten – z. B. Beschaffen, Speichern, Verwenden, Verändern, Weitergeben, Archivieren oder Löschen
- ☐ Prüfen Sie, ob Ihr Unternehmen von der DSGVO betroffen ist (z. B. mit Online-Checks wie Economiesuisse oder offiziellen Faktenblättern)

avolut

Sicherheit durch ein geeignetes Umfeld

Warum ist das wichtig?

Die Sicherheit Ihres Unternehmens hängt auch von Ihren Partnern ab. Wird einer Ihrer Lieferanten oder IT-Dienstleister Opfer eines Angriffs, kann dies auch Ihr Unternehmen betreffen – etwa durch den Verlust von Kundendaten. Gerade beim Outsourcing von IT- oder Security-Leistungen ist es daher entscheidend, dass auch Drittparteien grundlegende Cybersecurity-Massnahmen konsequent umsetzen.

Was können Sie tun?

- ☐ Verlangen Sie von Lieferanten und Outsourcing-Partnern die Einhaltung grundlegender Sicherheitsstandards
- ☐ Achten Sie bei der Auswahl externer IT- und Security-Dienstleister auf Zertifikate und den Nachweis angemessener Schutzmassnahmen

Wie gehe ich vor?

Sicherheit bei Lieferanten und Outsourcing-Partnern einfordern

Cyberrisiken enden nicht an der Unternehmensgrenze. Auch Partner und Dienstleister müssen grundlegende Sicherheitsmassnahmen umsetzen. Gehen Sie mit Ihren Lieferanten den Cybersecurity-Schnelltest durch und stellen Sie sicher, dass die gleichen Anforderungen gelten wie für Ihr eigenes Unternehmen.

Fragen Sie insbesondere nach:

- ☐ Werden regelmässig Backups erstellt und extern gespeichert?
- ☐ Gibt es einen Notfallplan für Cybervorfälle?
- ☐ Existieren Benutzerrichtlinien und werden diese aktiv umgesetzt?
- ☐ Sind klare Vorgaben für die Benutzer- und Rechteverwaltung vorhanden?
- ☐ Werden Mitarbeitende regelmässig zu Cybersecurity sensibilisiert (z. B. Umgang mit Phishing-E-Mails, Passwortsicherheit)?
- ☐ Werden Betriebssysteme, Firewalls und Anwendungen regelmässig aktualisiert?
- ☐ Erfolgt die Kommunikation verschlüsselt?
- ☐ Wird eine aktuelle Antivirensoftware eingesetzt und gepflegt?

avolut

Sicherheit bei ausgelagerten IT-Security-Dienstleistungen

Wenn Sie IT- oder Security-Aufgaben auslagern, müssen auch Ihre Provider die wichtigsten Sicherheitsanforderungen zuverlässig erfüllen.

- ☐ Gehen Sie mit dem IT- oder Security-Provider den Cybersecurity-Schnelltest durch.
- ☐ Lassen Sie sich geeignete Zertifikate vorlegen, die ein hohes Sicherheitsniveau bestätigen – z. B.:
  - ☐ für IT-Dienstleister
    - ☐ CyberSeal
  - ☐ für IT-Security-Provider
    - ☐ ISO 27001
    - ☐ OSCP oder Practical Network Penetration Tester (PNPT)
    - ☐ Cyber Security Spezialisten mit eidg. Fachausweis

avolut

Referenzen

Dieser Leitfaden stützt sich auf anerkannte Quellen und bewährte Standards im Bereich Cybersicherheit und Datenschutz. Dazu gehören:

- Allianz Digitale Sicherheit Schweiz: Cybersecurity Leidfaden für KMU
- NCSC: Merkblatt Informationssicherheit für KMU
- NCSC: Informationen für Unternehmen
- EDÖB: Datenschutz (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter)
- IT-Sicherheit für KMU
- Tagblatt: Datenschutzgesetz
- UBS: Informationen und Hinweise zu Phishing