

Cybersicherheit und -resilienz in KMU: Pragmatische Sicherheit für den Mittelstand

Armin Baumann

Bei Sicherheit geht es nicht nur um Abwehr, sondern auch um Widerstandsfähigkeit. Cyberresilienz bedeutet, Angriffe nicht nur zu verhindern, sondern im Ernstfall handlungsfähig zu bleiben, Schäden zu begrenzen und den Betrieb rasch wieder aufzunehmen. Für KMU ist das besonders wichtig, weil ein einzelner Vorfall zu Produktionsunterbrüchen, Datenverlust, Reputationsschäden oder finanziellen Verlusten führen kann. Sicherheit ist damit auch eine betriebswirtschaftliche Notwendigkeit.

Warum KMU besonders betroffen sind

Viele KMU gehen davon aus, für Angreifer zu klein oder zu unbedeutend zu sein. In der Realität verfügen gerade kleinere Unternehmen über wertvolle Kundendaten, Zugang zu Lieferketten, Zahlungsinformationen oder Geschäftsgeheimnisse, sind aber oft weniger stark geschützt als Konzerne. Für Cyberkriminelle sind sie deshalb attraktive Ziele. Hinzu kommt die veränderte Bedrohungslage. Phishing, Identitätsdiebstahl, Ransomware, manipulierte E-Mail-Konten und Angriffe über Dienstleister sind weitverbreitet. Die Angriffe sind oft professionell organisiert und automatisiert. Nicht nur Grossunternehmen, sondern auch Handwerksbetriebe, Dienstleister, Handels- und Produktionsunternehmen müssen ihre Sicherheitsstrategie entsprechend anpassen.

Cybersicherheit ist für kleine und mittlere Unternehmen längst kein Randthema mehr. Wer digital arbeitet, vernetzt kommuniziert und Cloud-Services, mobile Geräte oder externe Partner nutzt, ist Teil einer komplexen Angriffsfläche. Gleichzeitig fehlen vielen KMU Zeit, Fachkräfte und Budgets für ein umfassendes Sicherheitsprogramm. Deshalb braucht es einen pragmatischen Ansatz: wirksam, verständlich und im Alltag umsetzbar.

Die häufigsten Schwachstellen

Sicherheitslücken entstehen selten durch einen einzelnen grossen Fehler. Meist ist es eine Kombination technischer, organisatorischer und menschlicher Faktoren. Häufig fehlen klare Zuständigkeiten, aktuelle Softwarestände oder einfache Regeln für den sicheren Umgang mit Daten und Zugängen. Besonders kritisch sind schwache Passwörter, unzureichend geschützte Administratorrechte, fehlende Multifaktorauthentifizierung und unregelmässige Backups. Auch veraltete Systeme oder nicht dokumentierte IT-Installationen erhöhen das Risiko. Dazu kommt der Faktor Mensch:

Eine unbedachte E-Mail, ein falsch angeklickter Link oder ein zu schnell geöffneter Anhang können ausreichen, um Angreifern den Zugang zu ermöglichen. Cybersecurity ist deshalb auch eine Frage der Sensibilisierung und klarer Prozesse.

Vom Schutz zur Resilienz

Ein wirksames Sicherheitskonzept für KMU beginnt mit den Grundlagen: aktuelle Systeme, saubere Zugriffsrechte, starke Authentifizierung, regelmässige Datensicherungen und ein bewusster Umgang mit externen Zugängen. Diese Basis genügt jedoch nicht, denn absolute Sicherheit gibt es nicht. Entscheidend ist auch, wie

KMU Swiss veranstaltet pro Jahr rund 40 Anlässe, in welchen wirtschaftliche Themen abgehandelt werden. Dies sind Symposien, Insidetreffe (Best-Practice-Anlass) und lokale Stammtreffe (After-Work-Session). Rund 2000 Teilnehmer besuchen jährlich diese Anlässe. Die nächsten Symposien sind:

- **15.10.2026 Brugg:** Think greater again! Mit folgenden Referentinnen und Referenten: Martina Hammer (Brandmover), Philip Morger (SGE), KKdt Benedikt Roos (Schweizer Armee), Franz Kainz (Flumroc), Christoph Erni (Juice Technology), Gérald Walti (Innosuisse)
- **14.01.2027 Baden:** Neujahrsapéro mit Einläuten des Jubiläumsjahr
- **18.03.2027 Baden:** The Best of 25 years KMU Swiss Vol. 1
- **21.10.2027 Brugg:** The Best of 25 years KMU Swiss Vol. 2

Ziele von KMU Swiss sind Wissen, zu vermitteln, zu vernetzen und Teilnehmer für Neues zu motivieren. Dies ganz nach dem Motto: «KMU Swiss: Weil Wissen und Kontakte meine Firma und mich weiterbringen!»

www.kmuswiss.ch

das Unternehmen auf einen Vorfall reagiert. Cyberresilienz bedeutet, vorbereitet zu sein. Wer weiss, wer im Ernstfall entscheidet, wie Systeme isoliert, Backups wiederhergestellt und Mitarbeitende informiert werden, verkürzt Ausfallzeiten. Ein einfacher, getesteter Notfallplan ist oft wertvoller als ein komplexes, nie aktualisiertes Sicherheitskonzept. Die beste Lösung ist jene, die verstanden, getragen und im Krisenfall tatsächlich angewendet wird.

Die Rolle der Geschäftsleitung

Cybersicherheit ist keine reine IT-Aufgabe. Die Verantwortung liegt bei der Unternehmensleitung, weil Sicherheitsvorfälle direkte Auswirkungen auf Geschäft, Kunden, Recht und Reputation haben. Die Geschäftsleitung muss nicht jedes technische Detail kennen, aber Prioritäten setzen, Risiken verstehen und Ressourcen bereitstellen.

Wichtig ist ein klarer Blick auf die eigene Risikolage: Welche Daten sind besonders kritisch? Welche Prozesse müssen auch bei einem Ausfall weiterlaufen? Welche Abhängigkeiten bestehen zu Cloud-Anbietern, Softwarepartnern oder externen Dienstleistern? Solche Fragen helfen, Investitionen sinnvoll zu steuern. Nicht jedes Unternehmen braucht dieselben Massnahmen, aber jedes braucht ein Mindestmass an Transparenz, Verantwortung und Übung.

Mitarbeitende als Schutzfaktor

Die Mitarbeitenden sind oft die erste Verteidigungslinie, können aber auch ein Einfallstor sein. Deshalb braucht es keine trockenen Pflichtschulungen, sondern verständliche, regelmässige und praxisnahe Awareness-Massnahmen. Wer Phishing erkennt, verdächtige Nachrichten meldet und sichere Gewohnheiten entwickelt, reduziert das Risiko. Sinnvoll sind kurze Lerneinheiten, konkrete Verhaltensregeln und wiederkehrende Übungen. Wichtig ist eine Kultur, in der Fehler früh gemeldet werden können, ohne Schuldzuweisungen. Wenn ein verdächtiger Vorfall sofort gemeldet wird, kann Schaden verhindert oder begrenzt werden. Cyberresilienz ist deshalb Teamarbeit.

Technische und organisatorische Basis

Für KMU braucht es keine überdimensionierte Sicherheitsarchitektur, sondern eine solide, gut gepflegte Basis. Dazu gehören aktuelles Patch- und Update-Management, Backup-Konzepte mit Wiederherstellungstests, Multifaktor-Authentifizierung, Rechtekonzepte und eine klare Geräteverwaltung. Ebenso wichtig sind Regeln für Zugänge, externe Dienstleister und sensible Informationen. Organisatorisch muss klar sein: Wer darf was freigeben? Wer prüft ungewöhnliche Rechnungen oder Zah-

lungsanweisungen? Wer übernimmt im Notfall die Kommunikation? Solche Fragen wirken banal, sind aber im Ernstfall entscheidend. Je klarer die Abläufe, desto schneller kann ein Unternehmen reagieren. Sicherheit entsteht nicht durch Komplexität, sondern durch Verlässlichkeit.

Der Nutzen für das Geschäft

Cybersecurity wird häufig als Kostenfaktor gesehen. Tatsächlich schützt sie Wertschöpfung, Vertrauen und Kontinuität. Ein Unternehmen, das Ausfälle vermeidet oder schnell übersteht, schützt nicht nur seine Daten, sondern auch Kundenbeziehungen und Marktposition. Gerade im KMU-Umfeld ist Vertrauen ein zentraler Wettbewerbsvorteil. Viele Kunden, Partner und öffentliche Auftraggeber erwarten heute zudem einen nachvollziehbaren Umgang mit Informationssicherheit. Wer glaubhaft zeigt, dass Risiken ernst genommen und Prozesse beherrscht werden, stärkt seine Position im Markt. Cyberresilienz ist damit nicht nur Defensive, sondern auch ein Signal von Professionalität und Zukunftsfähigkeit.

Ein pragmatischer Weg für KMU

Der Einstieg muss nicht gross sein. Eine kurze Standortbestimmung genügt: Welche Systeme sind kritisch? Wo liegen die grössten Risiken? Welche drei Massnahmen bringen den grössten Nutzen? Daraus lässt sich ein realistischer Fahrplan ableiten. Wichtig ist, Schritt für Schritt vorzugehen und nicht auf den perfekten Plan zu warten.

Ein guter Anfang kann sein, Zugänge zu überprüfen, Backups zu testen, ein Meldeverfahren für Vorfälle einzuführen und Mitarbeitende gezielt zu sensibilisieren. Danach lassen sich weitere Massnahmen ergänzen, etwa ein Krisenhandbuch, externe Unterstützung oder regelmässige Sicherheitsreviews. So wird Cybersecurity zu einem machbaren Führungs- und Betriebsinstrument statt zu einem abstrakten Spezialthema.

Cybersicherheit und Cyberresilienz sind für KMU kein Luxus, sondern eine Voraussetzung für Stabilität im digitalen Alltag. Wer das Thema pragmatisch angeht, schafft nicht nur Schutz vor Angriffen, sondern auch mehr Sicherheit für Wachstum, Zusammenarbeit und unternehmerische Entscheidungsfreiheit. ■

