Deloitte.

Together makes progress

Unterschätzt, ungeschützt, unterversichert: KMU-Cyberrisiken in der Schweiz

August 2026

Inhalt

Hinweis zur Methodik

Dieser Bericht basiert erstens auf einer Onlineumfrage von 924 Arbeitnehmern, die für Unternehmen mit weniger als 250 Mitarbeitenden tätig sind und die mit Computern arbeiten und daher von Cyberrisiken im beruflichen Umfeld bei KMUs betroffen sein können. Die Umfrage wurde im April 2026 online durchgeführt.

Die Grösseneinteilung der Unternehmen folgt der Klassifizierung des Bundesamts für Statistik. Als KMUs gelten demnach Unternehmen bis 249 Mitarbeitenden, die zusätzlich in drei Kategorien unterteilt werden: Unternehmen mit 1-9 Mitarbeitenden werden als Mikrounternehmen eingestuft, mit 10-49 Mitarbeitenden als kleine Unternehmen und mit 50-249 Mitarbeitenden als mittlere Unternehmen. Unternehmen ab 250 Mitarbeitenden gelten als Grossunternehmen.

Die Studie basiert zweitens auf einer Reihe von Gesprächen mit Cyberexperten von Versicherungen. Die Gespräche fanden im Juni und Juli 2026 statt.
Wir danken allen Experten herzlich für die wertvollen Erkenntnisse.

Wichtigste Ergebnisse

Herausforderungen Cybersicherheit

Bedrohungslage: Angriffe werden schneller und skalierbarer

Die **Bedrohungslage im Bereich der Cybersicherheit** hat sich **grundlegend verändert**. Cyberangriffe nehmen nicht nur in ihrer Anzahl zu, sondern werden durch den **Einsatz von Künstlicher Intelligenz, Automatisierung und immer komplexeren digitalen Ökosystemen** deutlich schneller, gezielter und wirkungsvoller. **Gleichzeitig verkürzt sich das Zeitfenster, in dem Unternehmen ihre technologische Resilienz wirksam stärken können**. Grundsätzlich sind alle Unternehmen unabhängig von ihrer Grösse gefährdet.

Es lassen sich dabei **drei zentrale Sicherheitslücken** identifizieren, die sich gegenseitig verstärken und den grössten Handlungsbedarf aufzeigen:

01 Cyberrisiken werden weiterhin systematisch unterschätzt.

Obwohl ein erheblicher Anteil der Mitarbeitenden bereits konkrete Cybervorfälle erlebt hat, wird das tatsächliche Risiko vielfach zu niedrig eingeschätzt. Unsere Umfrage unter Schweizer Arbeitskräften bei KMUs zeigt: **49%** der Mitarbeitenden haben in den letzten drei Monaten einen ernsten Cybervorfall erlebt, aber nur **22%** schätzen das Cyberrisiko als hoch ein. Diese Diskrepanz ist insbesondere bei kleinen und mittleren Unternehmen ausgeprägt und erschwert eine rechtzeitige Priorisierung wirksamer Schutzmassnahmen.
Phishing ist mit **25%** die am häufigsten wahrgenommene Cyberbedrohung, mit nur kleinen Unterschieden nach Unternehmensgrösse. Gerade skalierbare Angriffe über E-Mail, Zugangsdaten oder manipulierte Zahlungsprozesse machen auch kleinere Unternehmen verwundbar.

02 Die Umsetzung elementarer Sicherheitsmassnahmen bleibt unvollständig.

Moderne Authentifizierungsverfahren, regelmässige Schulungen, Phishing-Tests sowie weitere organisatorische und technische Schutzmechanismen sind zwar zunehmend verbreitet, jedoch noch längst nicht flächendeckend etabliert. Besonders kleinere Unternehmen weisen deutliche Umsetzungsdefizite auf und verfügen dadurch über eine geringere Cybersicherheit.
Der **Deloitte KMU-Cybersicherheitsindex** – ein ungewichteter Durchschnitt der Implementierung von sechs mitarbeiterseitigen elementaren Sicherheitsmassnahmen – liegt bei durchschnittlich 58 von 100 Punkten. Das bedeutet, dass Sicherheitsmassnahmen im Durchschnitt nur zu 58% umgesetzt sind. Die Lücken sind bei modernen Authentifizierungsmethoden besonders gross: Passwortlose Authentifizierung (z.B. biometrisch) ist nur bei 45% der Unternehmen implementiert, Single Sign-On (SSO) ebenfalls nur bei 45%. Multi-Faktor-Authentifizierung (MFA) ist mit 66% zwar verbreiteter, aber immer noch nicht flächendeckend.

03 Der Versicherungsschutz entwickelt sich zwar positiv, erreicht jedoch insbesondere kleine Unternehmen noch unzureichend.

Cyberversicherungen wachsen, aber die Marktdurchdringung bleibt niedrig. Gemäss dem Schweizerischen Versicherungsverband SVV sind mit **72’000 Policen** nur **11.5%** der in der Schweiz domizilierten Unternehmen versichert. Die Lücke zeigt sich vor allem bei der Anzahl der Unternehmen: Grossunternehmen und grössere KMUs sind deutlich häufiger versichert, während viele kleine Unternehmen keine Police haben – obwohl Cyberschäden relativ zum Umsatz bei Letzteren besonders schwer wiegen können.

Wichtigste Ergebnisse

Herausforderungen Cybersicherheit

In Zeiten von KI muss die Cybersicherheit systematisch aktualisiert und die dreifache Sicherheitslücke geschlossen werden. Es bleibt nur ein enges Zeitfenster, um die technologische Resilienz sicherzustellen.

Staat: Verbindliche Leitplanken, aber nicht rein staatliche Regulierung

Die Umfrage zeigt ein klares Mandat für mehr Verbindlichkeit, aber nicht für rein staatliche Regulierung: **87%** unterstützen weitergehende Vorschriften, **81%** sehen aber ausschliesslich staatliche Regulierung nicht als beste Option. Der Staat sollte klare Mindeststandards, Transparenz und Vergleichbarkeit fördern – etwa durch breit anerkannte Standards oder Score-Modelle – und gleichzeitig branchennahe Umsetzung ermöglichen. Ziel ist ein pragmatischer Rahmen: **Mindeststandards ja, starre staatliche Detailvorgaben nein.** Ein Beispiel hierfür könnte sein, Multi-Faktor-Authentifizierung bei kommerziellen Anbietern in den Bereichen Zahlungsverkehr, Kommunikation, IT-Anbietern oder Social Media verpflichtend zu machen. Ein bedeutender Angriffsvektor würde damit erheblich erschwert.

Versicherungen: Deckungslücke durch Einfachheit und Assistance schliessen

Entscheidend sind einfache, verständliche Versicherungsprodukte, bessere Vertriebsanreize, differenzierte technologiegetriebene Risikoprüfung und Assistance-Leistungen im Schadenfall. Cyberversicherung sollte für KMU nicht nur als finanzielle Deckung verstanden werden, sondern als Zugang zu Krisenunterstützung, Unterstützung bei der Bewältigung von Sicherheitsvorfällen, Spezialisten und Präventionsleistungen.

Unternehmen: Cyberresilienz beginnt mit den Grundlagen

Bei KMU (Unternehmen unter 250 Mitarbeitenden) ist die dreifache Sicherheitslücke besonders ausgeprägt: Risiken werden stärker unterschätzt, Sicherheitsmassnahmen weniger stringent umgesetzt und Versicherungen sind seltener vorhanden. Priorität haben deshalb konkrete Grundlagen: Starke Authentifizierung (mindestens MFA, oder besser passwortlose Authentifizierung), eingeschränkte Administratorrechte, regelmässige Schulungen, gesicherte und getestete Backups, Notfallplanung und professionelle IT-Betreuung. Letzteres ist eine Schlüsselmassnahme: KMU sollten sich auf ihre Kernkompetenzen konzentrieren, ihre IT nicht selbst betreiben, sondern einen spezialisierten IT-Dienstleister wählen. Zusätzlich sollten KMU Zahlungs- und Freigabeprozesse gegen Kompromittierung geschäftlicher E-Mail-Konten absichern.

Die zentrale Erkenntnis lautet daher: Cybersicherheit wird im Zeitalter der Künstlichen Intelligenz zu einem entscheidenden Wettbewerbs- und Resilienzfaktor.

Organisationen, die jetzt konsequent in Risikobewusstsein, moderne Sicherheitsarchitekturen, organisatorische Resilienz und partnerschaftliche Zusammenarbeit investieren, schaffen die Voraussetzungen, um auch in einem zunehmend dynamischen Bedrohungsumfeld nachhaltig erfolgreich zu bleiben.

Cyberrisiken

Steigende Bedrohungslage trifft auf drei Sicherheitslücken:

- Risikowahrnehmung: Cyberrisiken werden unterschätzt
- Umsetzung: Elementare Sicherheitsmassnahmen sind nicht flächendeckend implementiert
- Absicherung: Versicherungsschutz fehlt vor allem bei kleineren Unternehmen

Bedrohungslage steigt, und die technologische Resilienz steht an einem kritischen Wendepunkt

Das Risiko von Cybervorfällen wird tendenziell unterschätzt – gleichzeitig nimmt die Bedrohungslage deutlich zu. Entscheidend ist nicht nur, dass mehr Angriffe stattfinden, sondern dass sie schneller, skalierbarer und stärker vernetzt wirken. Drei Entwicklungen verstärken sich gegenseitig:

1. Cyberkriminalität wird wirtschaftlich relevanter und stärker vernetzt.

Die finanziellen Schäden durch Cyberkriminalität wachsen stark: Cybersecurity Ventures erwartet ein jährliches Wachstum der globalen Cybercrime-Kosten von 15%. Gleichzeitig entstehen Cyberrisiken immer häufiger ausserhalb der eigenen Organisation – entlang von Lieferketten, Technologiepartnern und digitalen Abhängigkeiten. SecurityScorecard zeigt, dass 35.5% der untersuchten Datenpannen im Jahr 2024 auf Drittparteien zurückzuführen waren, ein Anstieg um 6.5 Prozentpunkte gegenüber dem Vorjahr. Cyberrisiken sind damit nicht mehr nur eine Frage der eigenen IT-Sicherheit, sondern zunehmend ein Ökosystemrisiko.

2. Künstliche Intelligenz und Automatisierung erhöhen die Angriffsgeschwindigkeit.

Angriffe werden nicht nur häufiger, sondern auch schneller und einfacher skalierbar. CrowdStrike berichtet für 2026 von einem Anstieg von 89% bei Angriffen durch KI-gestützte Angreifer. Gleichzeitig sank die durchschnittliche eCrime-Breakout-Time auf 29 Minuten – eine um 65% höhere Geschwindigkeit gegenüber 2024. Auch der Deloitte Cyber Threat Trends Report 2025 zeigt, dass Cyberbedrohungen anspruchsvoller werden und KI zur Automatisierung von Angriffen sowie zur Umgehung von Erkennung eingesetzt wird. Für Unternehmen bedeutet dies: Die verfügbare Reaktionszeit schrumpft deutlich.

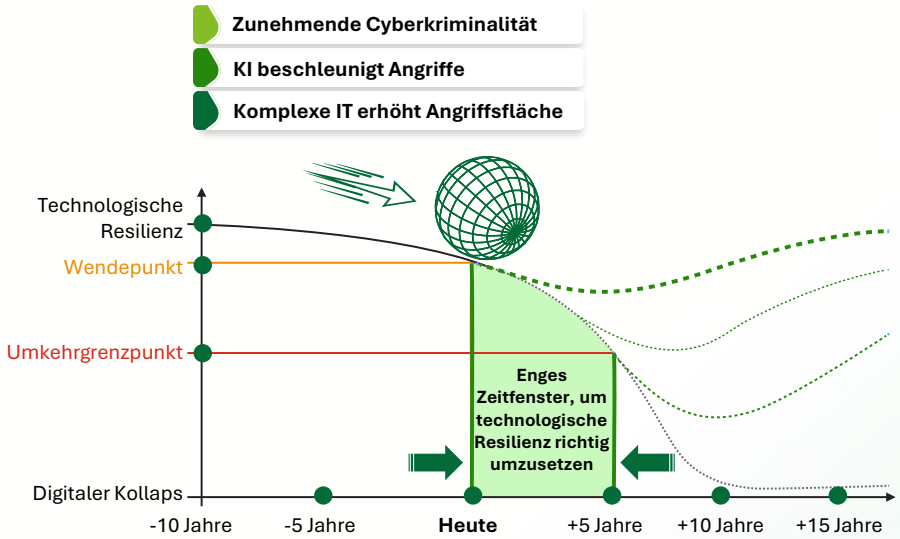
3. Komplexe und veraltete IT-Landschaften erschweren wirksame Verteidigung.

Gerade grosse Unternehmen betreiben häufig sehr komplexe Applikationslandschaften. Laut MuleSoft sind in Unternehmen durchschnittlich über 1’000 Anwendungen im Einsatz; IBM hält fest, dass grössere Unternehmen sogar mehr als 1’000 Applikationen nutzen können. Gleichzeitig laufen in vielen Unternehmen weiterhin kritische Kernprozesse auf jahrzehntealter Software. Diese Komplexität erschwert Transparenz, Priorisierung, Updates, Sicherheitsarchitektur und schnelle Reaktion auf neue Schwachstellen. Je komplexer die IT-Landschaft, desto schwieriger wird es, Angriffe rechtzeitig zu erkennen, einzudämmen und den Betrieb schnell wiederherzustellen.

Neben gezielten Angriffen nehmen auch systemische Risiken zu. Cloud-Ausfälle, Sicherheitsvorfälle bei SaaS-Anbietern oder Fehler bei zentralen Technologieanbietern können viele Unternehmen gleichzeitig betreffen. Der CrowdStrike-Ausfall im Juli 2024 zeigte, wie stark zentrale Technologiedienstleister kritische Branchen wie Luftfahrt, Banken, Börsen, Technologieunternehmen und Gesundheitswesen gleichzeitig beeinträchtigen können. Die Stabilität digitaler Systeme hat damit einen kritischen Punkt erreicht: Die Schweizer Wirtschaft hat nur ein enges Zeitfenster, um technologische Resilienz aufzubauen.

Abbildung 1: Enges Zeitfenster, um technologische Resilienz umzusetzen

Stilisierte eigene Darstellung gemäss Deloitte Einschätzung. Die Weltkugel symbolisiert die technologische Resilienz der Welt, die drei Faktoren zeigen die Bedrohungslage. Die gestrichelten Linien zeigen verschiedene Szenarien, wie sich die technologische Resilienz weiterentwickeln könnte



Lücke 1 – Risikowahrnehmung: Vorfälle werden erlebt, Risiken aber stark unterschätzt

Unsere Umfrage unter Schweizer Arbeitskräften zeigt: Cyberrisiken werden systematisch unterschätzt, insbesondere von Mitarbeitenden kleinerer Unternehmen. Wir konzentrieren uns in der Analyse auf KMUs, kleine und mittlere Unternehmen, nach Definition des Bundesamtes für Statistik. Demzufolge werden KMUs in drei Grössenklassen unterteilt: Mikrounternehmen (1-9 Mitarbeitende), kleine Unternehmen (10-49 Mitarbeitende) und mittlere Unternehmen (50-249 Mitarbeitende).

Die Zahl der erlebten ernsten Cybervorfälle in den letzten drei Monaten liegt durchgehend über dem Risikoempfinden für solche Vorfälle. Während 49% aller Mitarbeitenden in den letzten drei Monaten einen ernsthaften Cybervorfall erlebt haben, schätzen nur 22% das Cyber-Risiko als hoch ein.

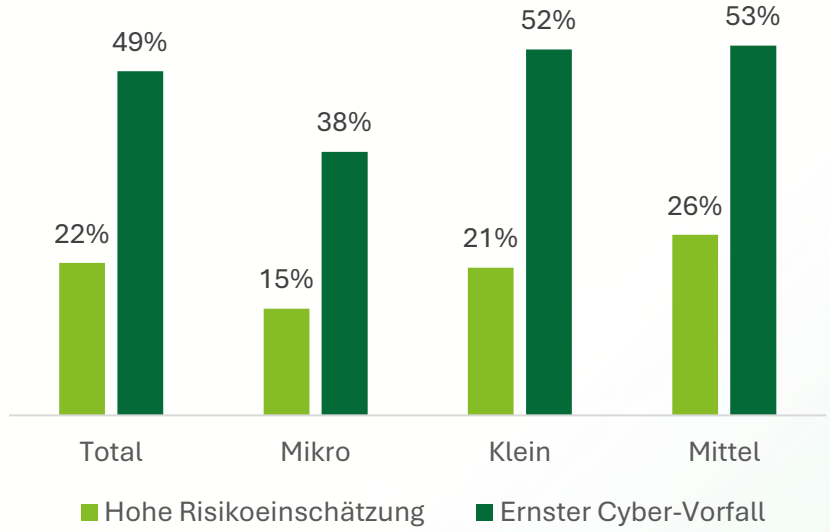
Diese Wahrnehmungslücke ist besonders bei Mikrounternehmen ausgeprägt. Mitarbeitende von Mikrounternehmen (1-9 Mitarbeitende) erleben zwar weniger Vorfälle als ihre Kollegen in mittleren Unternehmen (38% vs. 53%), unterschätzen ihr Risiko aber noch stärker: Nur 15% schätzen das Risiko als hoch ein.

Mitarbeitende von kleinen und mittleren Unternehmen schätzen das Risiko häufiger höher ein, allerdings steigt das Risikobewusstsein leicht weniger stark als die Wahrnehmung von Cybervorfällen: Die Risikoeinschätzung steigt von Mitarbeitenden von Mikrounternehmen bis zu mittleren Unternehmen um 11 Prozentpunkte (von 15% auf 26%), die Wahrnehmung von Vorfällen um 15 Prozentpunkte (von 38% auf 53%).

Diese Risikounterschätzung zeigt sich auch in Erhebungen aus KMU-Unternehmenssicht und aus einer IT-Dienstleister-Perspektive: In der Mobiliar-Studie «KMU Cybersicherheit 2025» halten nur 33% der befragten KMU Cybersicherheit für sehr wichtig oder wichtig. Gleichzeitig fühlen sich nur 42% gut vor Cyberangriffen geschützt, während nur 33% der IT-Dienstleister die Resilienz ihrer KMU-Kunden als hoch bewerten.

Abbildung 2: Grosse Lücke zwischen Risikoeinschätzung und erlebten Cybervorfällen

Antworten auf zwei Fragen, sehr hohe/hohe Cyberrisikoeinschätzung und erlebte ernste Cybervorfälle in den letzten drei Monaten, beides in Bezug auf den eigenen Arbeitgeber. Darstellung nach Unternehmensgrösse (Mikro – Mittlere Unternehmen)



Lücke 1 vertieft: Phishing trifft Unternehmen jeder Grösse

Mitarbeitende von Mikrounternehmen nehmen Cybervorfälle etwas seltener wahr als diejenigen von grösseren Unternehmen. Der Unterschied ist aber klein – deutlich kleiner als ihre niedrigere Risikowahrnehmung vermuten lässt. Das zeigt: Auch sehr kleine Unternehmen sind Cyberrisiken ausgesetzt.

Phishing ist die persistenteste Bedrohung: Mit 25% ist Phishing insgesamt die am häufigsten wahrgenommene Cyberbedrohung. Bemerkenswert ist, dass Phishing bei Mikrounternehmen (24%) fast ebenso häufig auftritt wie bei mittleren Unternehmen (25%). Dies zeigt, dass Phishing-Angriffe unabhängig von Unternehmensgrösse gefährlich sind.

Malware ist die zweithäufigste Bedrohung und folgt einem ähnlichen Muster. Dagegen werden komplexere und seltener beobachtete Angriffe – wie Datendiebstahl, Identitätsdiebstahl oder Betriebsstörungen (Distributed Denial of Service sowie Ransomware) – bei Mikrounternehmen deutlich weniger häufig wahrgenommen. Entweder sind Mikrounternehmen weniger von solchen Angriffen betroffen oder ihre Mitarbeitenden erkennen diese weniger oft.

Abbildung 3: Erlebtes Vorkommen von ernsten Cybervorfällen nach Unternehmensgrösse

Antworten auf Frage zu erlebten ernsten Cybervorfällen in den letzten drei Monaten beim Arbeitgeber. Rot: relativ hohes Vorkommen, Gelb: mittel, Grün: relativ niedriges Vorkommen. Darstellung nach Unternehmensgrösse (Mikro – Mittlere Unternehmen)

	Total	Mikro	Klein	Mittel
Nein, kein Vorfall	51%	62%	48%	47%
Ja, Phishing	25%	24%	27%	25%
Ja, CEO-Fraud	8%	4%	8%	9%
Ja, Malware	13%	10%	12%	15%
Ja, Verdacht auf Datenabfluss	10%	4%	12%	11%
Ja, Identitätsdiebstahl	9%	4%	9%	11%
Ja, Betriebsstörungen	12%	6%	12%	15%

Erklärung der Dimensionen von Cybervorfällen:

Phishing: täuschende Nachrichten zur Preisgabe von Daten oder Auslösung von Zahlungen; CEO-Fraud: Betrug durch vorgetäuschte Führungspersonen; Malware: Schadsoftware auf Geräten oder Systemen; Datenabfluss: möglicher unbefugter Abfluss sensibler Daten; Identitätsdiebstahl: Missbrauch gestohlener Zugangsdaten oder Identitäten; Betriebsstörungen: cyberbedingte Ausfälle oder Einschränkungen des Betriebs

Lücke 1 vertieft: Hoher Vertrauensvorschuss trotz Vorfällen

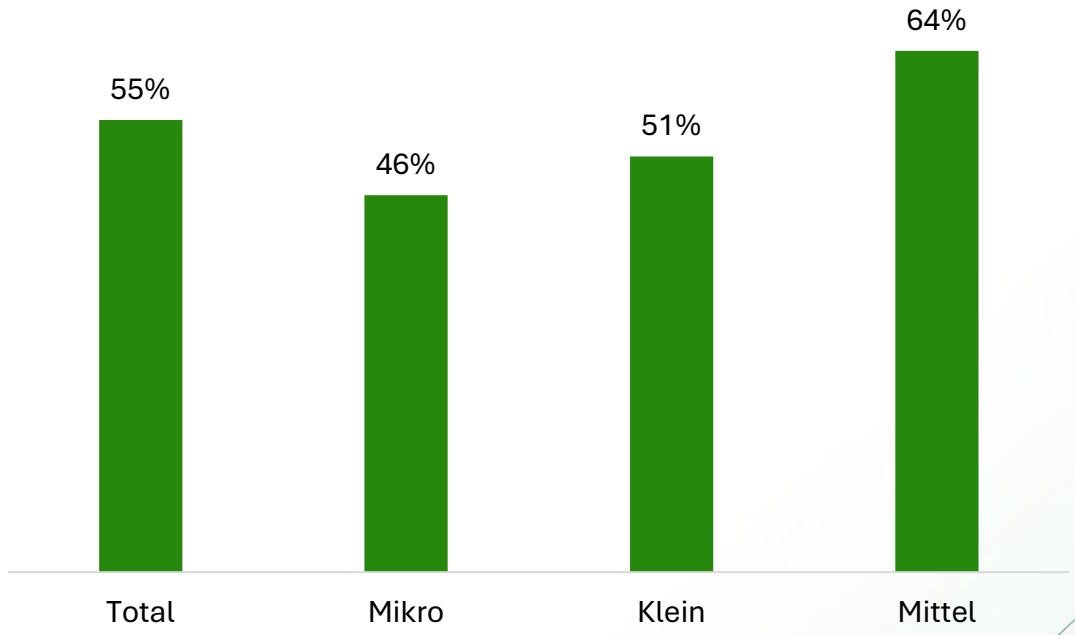
Die Umfrage zeigt einen hohen Vertrauensvorschuss: 55% der Mitarbeitenden haben hohes Vertrauen in die Abwehrkraft ihres Arbeitgebers, obwohl 49% in den letzten drei Monaten Vorfälle erlebt haben, wie zuvor gezeigt. Dieses Paradoxon ist bei mittleren Unternehmen (50-249 Mitarbeitende) am stärksten ausgeprägt (64% hohes Vertrauen), während es bei Mikrounternehmen am schwächsten ist (46% hohes Vertrauen).

Der hohe Vertrauensvorschuss ist ein gutes Zeichen, gleichzeitig muss dieser auch eingelöst werden. Es muss Unternehmen also tatsächlich gelingen, Cyberrisiken zu bekämpfen. Die Bedrohungslage darf nicht unterschätzt werden.

Umgekehrt ist auch klar, dass, obwohl Unternehmen bei der Bekämpfung von Cyberrisiken eine zentrale Rolle einnehmen sollten, einzelne Mitarbeiter dazu beitragen sollten. Es darf seitens der Mitarbeitenden nicht zu einem Abwälzen jeglicher Verantwortung auf ihren Arbeitgeber kommen.

Abbildung 4: Vertrauen dass das eigene Unternehmen sich ausreichend vor Cyberangriffen schützen kann

Antworten «grosses oder sehr grosses» Vertrauen auf die Frage: Wie gross ist Ihr Vertrauen, dass Ihr Unternehmen die Unternehmensdaten ausreichend vor Cyberangriffen schützt? Darstellung nach Unternehmensgrösse (Mikro – Mittlere Unternehmen)



Lücke 2 – Umsetzung: Sicherheitsmassnahmen sind noch nicht flächendeckend implementiert

Obwohl bereits viel getan wird, um der Bedrohungslage zu begegnen, zeigen sich erhebliche Implementierungslücken. Der Deloitte KMU-Cybersicherheitsindex – ein ungewichteter Durchschnitt der Implementierung von sechs elementaren Sicherheitsmassnahmen – liegt bei durchschnittlich 58 von 100 Punkten. Das bedeutet, dass Sicherheitsmassnahmen im Durchschnitt nur zu 58% umgesetzt sind.

Erhebliche Unterschiede nach Unternehmensgrösse: Mikrounternehmen erreichen nur 44 Punkte und liegen damit deutlich unter dem Durchschnitt. Mittlere Unternehmen (50-249 Mitarbeitende) führen mit 67 Punkten.

Kleine Unternehmen (10-49 Mitarbeitende) erleben ähnlich viele Cybervorfälle wie mittlere Unternehmen, setzen aber weniger Sicherheitsmassnahmen um.

Die Lücke betrifft nicht nur mitarbeiterseitige technische Massnahmen, sondern auch die organisatorische Resilienz. Die Studie «KMU Cybersicherheit 2025» zeigt aus Unternehmenssicht, dass nur 30% der KMU über einen Notfallplan oder ein Sicherheitskonzept verfügen. Gerade diese organisatorischen Massnahmen sind entscheidend, damit ein Vorfall nicht zu längeren Betriebsunterbrüchen führt.

«Resilienz ist nicht nur eine technische Frage. Der organisatorische Aspekt trägt genauso zur Gesamtresilienz bei wie technische Lösungen.»

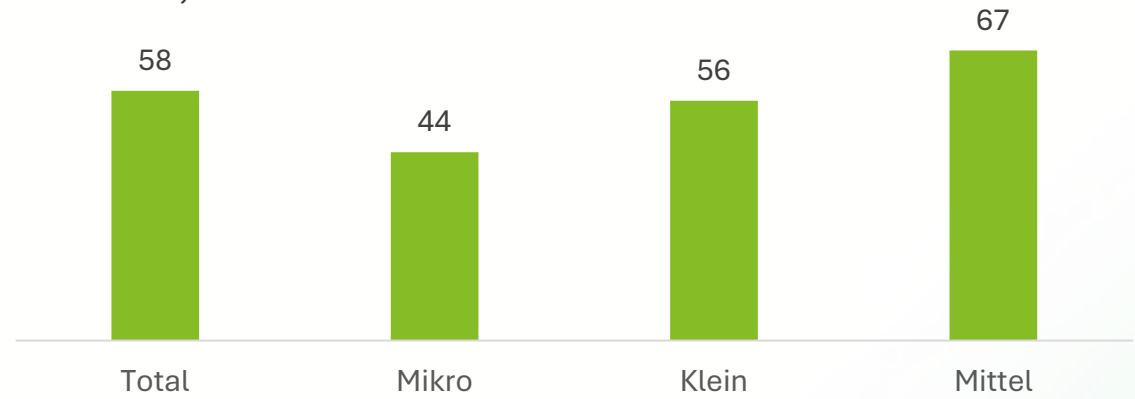
René Buff, Head Center of Excellence Cyber, Helvetia Baloise Group

Abbildung 5: Deloitte KMU-Cybersicherheitsindex

Ungewichteter Durchschnitt der Verbreitung von sechs Sicherheitsmassnahmen, gemäss «ja» Antworten der jeweiligen Fragen. Darstellung nach Unternehmensgrösse (Mikro – Mittlere Unternehmen)

Deloitte KMU-Cybersicherheitsindex: 58

0 minimale, 100 maximale Sicherheitsmassnahmen



Methodologie:
Ungewichteter Durchschnitt der Ja-Antworten der Umfrage, ob folgendes beim eigenen Arbeitgeber vorhanden ist: MFA, Biometrischer Zugang möglich, Single-sign-on (SSO), Warnsignale in E-Mails, Schulungen, Phishing-Tests

Lücke 2 vertieft: Moderne Authentifizierung, Schulungen und Tests nicht ausreichend oft implementiert

Moderne Authentifizierungsmethoden sind unterimplementiert: Passwortlose Authentifizierung (z. B. biometrisch) ist nur bei 45% der Unternehmen implementiert – bei weniger als der Hälfte. Single Sign-On (SSO) ist ebenfalls nur bei 45% verbreitet, wobei Mikrounternehmen besonders zurückliegen (nur 32%). Multi-Faktor-Authentifizierung (MFA) ist mit 66% zwar verbreiteter, aber immer noch nicht flächendeckend.

E-Mail-Warnungen sind weit verbreitet, das heisst, das Mailsystem liefert Warnsignale bei potenziell schädlichen E-Mails, wie etwa den Zusatz «EXT» für externe E-Mails oder einen Hinweis, dass von diesem Absender selten E-Mails empfangen werden: Mit 70% sind solche E-Mail-Warnungen grundsätzlich weit verbreitet, mit einem Sprung in der Verbreitung bei Unternehmen mit mehr als 50 Mitarbeitenden (81%).

Schulungen zeigen grosse Unterschiede: Schulungen sind bei Mikrounternehmen weniger verbreitet (32%), während sie in 82% von mittleren Unternehmen vorhanden sind.

Phishing-Tests sind unterimplementiert: Nur 48% der Unternehmen führen regelmässig Phishing-Tests durch. Hier zeigen sich die grössten Unterschiede: Während 63% der mittleren Unternehmen Tests durchführen, sind es bei Mikrounternehmen nur 24%.

Abbildung 6: Cybersicherheitsindex: Verbreitung Massnahmen aus Mitarbeitersicht nach Unternehmensgrösse

Ungewichteter Durchschnitt der Verbreitung von acht Sicherheitsmassnahmen, gemäss «ja» Antworten der jeweiligen Fragen. Grün: hohe Verbreitung, gelb: mittel, rot: niedrige Verbreitung. Darstellung nach Unternehmensgrösse (Mikro – Mittlere Unternehmen)

	Total	Mikro	Klein	Mittel
Passwortlos	45	44	42	47
Multi-Faktor	66	51	67	73
SSO	45	32	47	49
E-Mail-Warnungen	70	62	63	81
Schulungen	65	32	65	82
Phishing Tests	48	24	44	63
Index	**58**	**44**	**56**	**67**

Methodologie:
Ungewichteter Durchschnitt der Ja-Antworten der Umfrage, ob folgendes beim eigenen Arbeitgeber vorhanden ist: MFA, Biometrischer Zugang möglich, Single-sign-on (SSO), Warnsignale in E-Mails, Schulungen, Phishing-Tests

Massnahmen im Detail: E-Mail-Warnungen helfen, reichen aber nicht aus

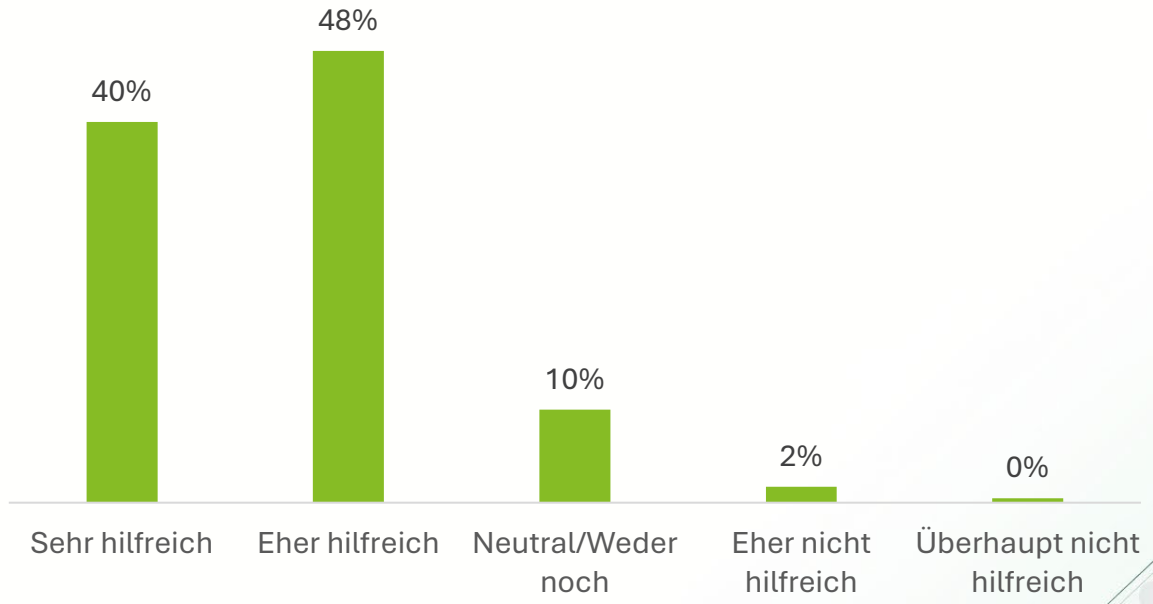
E-Mail-Warnhinweise sind bereits weit verbreitet und werden als überwiegend hilfreich wahrgenommen. Wie Abbildung 7 zeigt, finden 88% der Befragten E-Mail-Warnungen hilfreich – ein Signal, dass diese Massnahme funktioniert.

Phishing ist allerdings mit 25% (Abbildung 3) die am häufigsten wahrgenommene Cyberbedrohung und kann über verschiedene Kanäle erfolgen, neben E-Mail beispielsweise auch per SMS. Trotz der hohen Wirksamkeit von E-Mail-Warnungen bleibt Phishing die persistenteste Bedrohung. Dies deutet auf Folgendes hin:

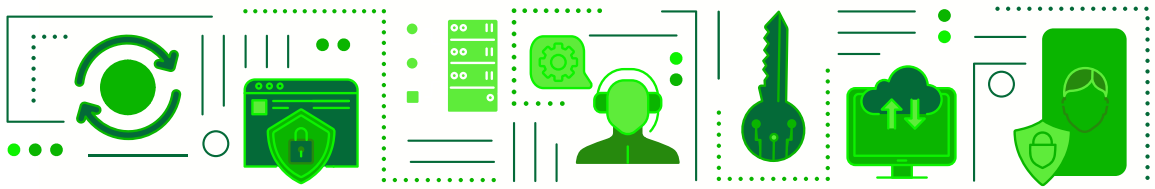
- **Technische Massnahmen allein reichen nicht aus:** E-Mail-Warnungen sind wirksam, aber Phishing-Angriffe sind vielfältig und ausgefeilt.
- **Kontinuierliche Aufmerksamkeit ist notwendig:** Mitarbeitende müssen ständig wachsam bleiben, da ständig neue Phishing-Varianten entstehen.
- **Eine ganzheitliche Strategie ist erforderlich:** E-Mail-Warnungen müssen mit Schulungen, Phishing-Tests (siehe nächste Seite), einer Kultur der Cybersicherheit sowie mit technischen Hintergrundmassnahmen (z.B. Multifaktor- bzw. passwortlose Authentifizierung) kombiniert werden, so dass Phishing Nachrichten möglichst selten zugestellt werden, möglichst selten auf Ebene Mitarbeitende erfolgreich sind und möglichst selten allfälliges Fehlverhalten seitens der Mitarbeitende zu einem Schadenseintritt führt.

Abbildung 7: Wie hilfreich sind E-Mail-Warnhinweise?

Antworten in Prozent auf Frage (nur an diejenigen, in deren Unternehmen es Warnhinweise gibt): Wie hilfreich sind diese Warnsignale für Sie bei der Vermeidung von schädlichen E-Mails?



Massnahmen im Detail: Phishing-Tests sind wichtig, aber unterimplementiert

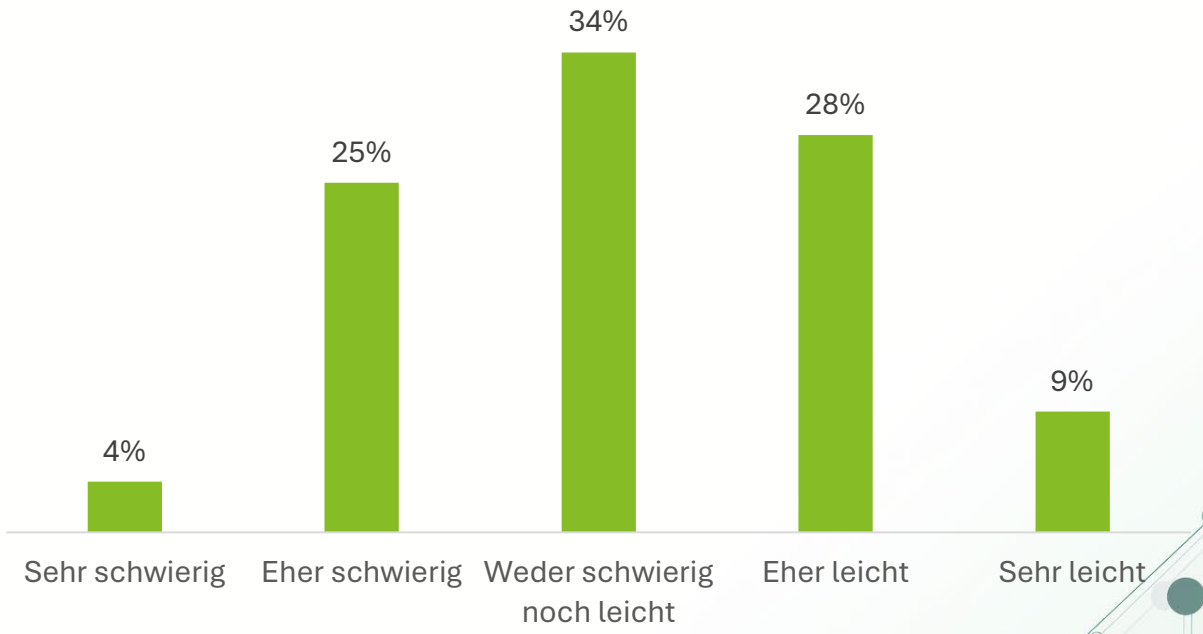


Phishing-Tests sind ein wichtiges Instrument zur Messung der Mitarbeitenden-Resilienz gegen die häufigste Cyberbedrohung. Insgesamt führen 48% der Schweizer Unternehmen regelmässig Phishing-Tests durch – allerdings mit erheblichen Unterschieden nach Unternehmensgrösse. Während Mikrounternehmen (24%) und kleine Unternehmen (44%) deutlich unter dem Durchschnitt liegen, erreichen mittlere Unternehmen (50-249 Mitarbeitende) mit 63% eine deutlich höhere Implementierungsquote.

Die wahrgenommene Schwierigkeit der Tests zeigt ein ausgewogenes Bild (Abbildung 9): 37% der Befragten bewerten die Tests als eher leicht bis sehr leicht, während 29% sie als eher schwierig bis sehr schwierig einstufen. Diese Verteilung deutet darauf hin, dass Phishing-Tests wirksam sind – sie sind weder trivial noch überwältigend. Trotzdem bleibt Phishing die persistenteste Bedrohung (25% aller Vorfälle, Abbildung 3). Dies legt nahe, dass Tests allein nicht ausreichen; sie müssen mit kontinuierlicher Schulung, technischen Massnahmen und einer Kultur der Cybersicherheit kombiniert werden.

Abbildung 8: Schwierigkeitsgrad von Phishing Tests

Antworten in Prozent auf die Frage (nur an diejenigen, in deren Unternehmen es Phishing Tests gibt): Wie schwierig ist es für Sie in diesen Tests, Phishing-E-Mails als solche zu erkennen?



Massnahmen im Detail: Schulungen wirken, erreichen aber Mikrounternehmen zu selten

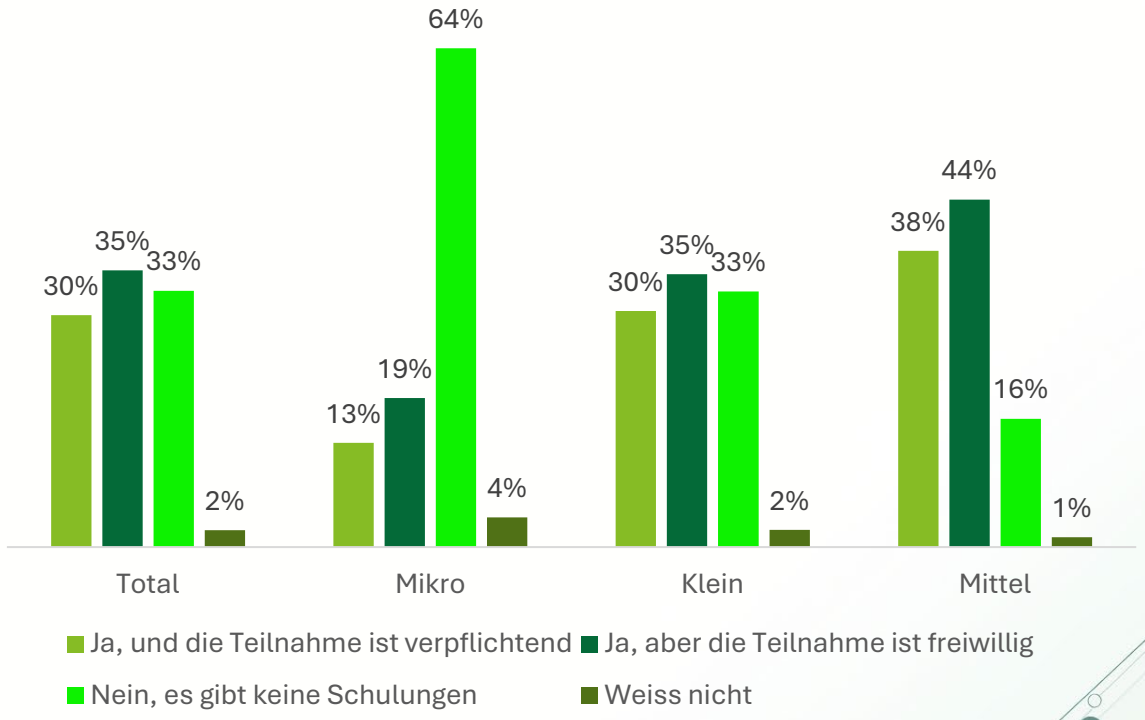
Cyber-Security-Schulungen sind, mit Ausnahme von Mikrounternehmen, weit verbreitet. Je grösser das Unternehmen, desto eher sind die Schulungen verpflichtend, wie die Abbildung zeigt.

Wie Antworten auf eine separate Frage zeigen, werden Schulungen grossmehrheitlich als wirksam wahrgenommen: Unabhängig davon, ob freiwillig oder verpflichtend, werden Schulungen fast durchgehend als hilfreich bewertet. Insgesamt 86% der Befragten stufen Schulungen als hilfreich ein, um Cyberrisiken zu erkennen und zu vermeiden – nur 1% bewertet sie als nicht hilfreich.

Eine weitere Frage zeigt die bevorzugten Schulungsformate: Bei der Art der Schulung werden Workshops von 48% der Befragten bevorzugt, gefolgt von interaktiven Online-Modulen und Kurzvideos (40% und 43%). Dies zeigt, dass Mitarbeitende interaktive und praktische Formate bevorzugen.

Abbildung 9: Verbreitung von Cyber-Security-Schulungen

Antworten in Prozent auf die Frage: Mein Arbeitgeber organisiert regelmässig Cyber-Security-Schulungen



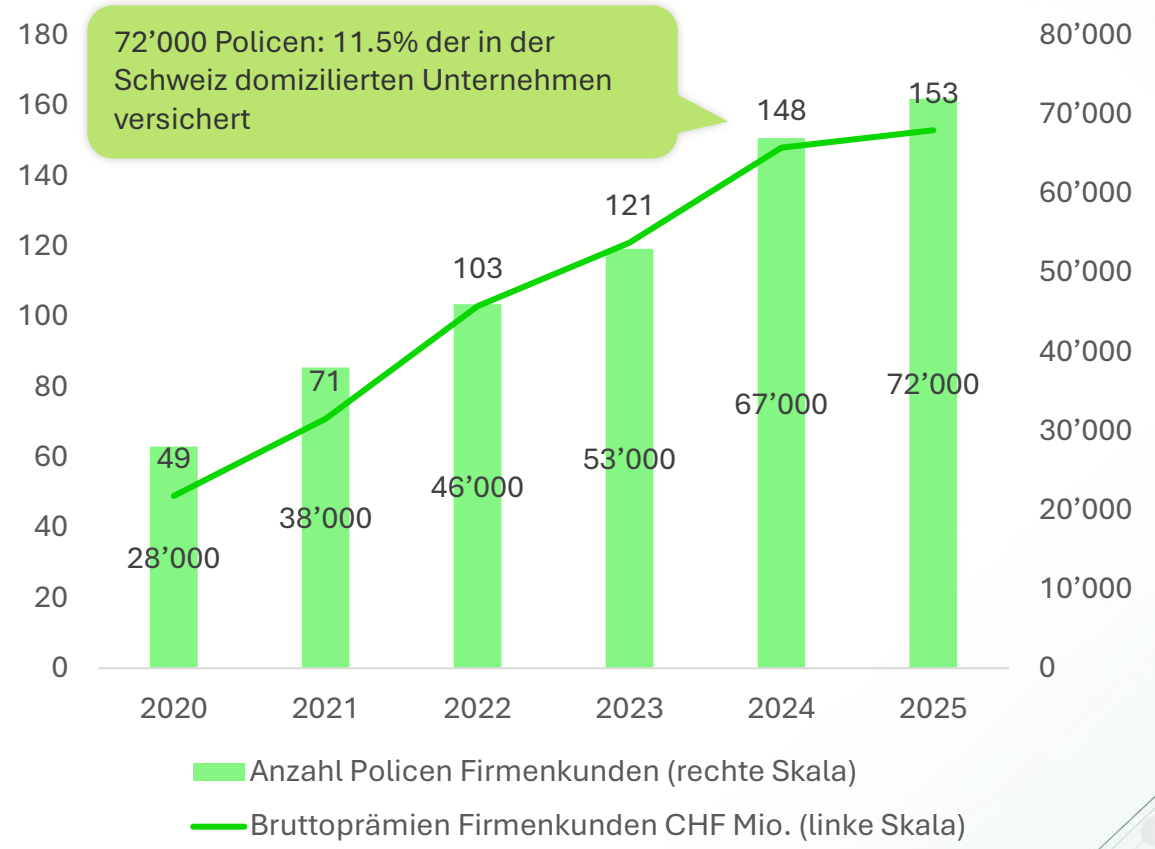
Lücke 3 – Absicherung: Versicherungsschutz fehlt vor allem bei kleinen Unternehmen

Cyberversicherungen sind ein Wachstumsmarkt in der Schweiz, auch wenn sich das Wachstum jüngst stark abgeschwächt hat. Gemäss SVV hat sich seit dem Jahr 2020 die Zahl der Policen mehr als verdoppelt; die Bruttoprämien mehr als verdreifacht. Mit 72’000 Policen sind insgesamt aber nur 11.5% aller in der Schweiz domizilierten Unternehmen abgedeckt. Die Versicherungslücke ist besonders ausgeprägt bei Mikrounternehmen und kleinen Unternehmen. Bei Grossunternehmen (mit mehr als 250 Mitarbeitenden) sind Cyberversicherungen weit verbreitet, und auch mittlere Unternehmen sind deutlich häufiger versichert. Die insgesamt tiefe Marktdurchdringung zeigt sich vor allem bei der Anzahl der Unternehmen: Viele sehr kleine Unternehmen haben keine Cyberversicherung, obwohl Cybervorfälle sie relativ zum Umsatz besonders stark treffen können.

Die Versicherungslücke vor allem bei KMUs (Firmen unter 250 Mitarbeitern) ist das Resultat mehrerer sich gegenseitig verstärkender Faktoren:

1) Vor allem KMUs unterschätzen systematisch ihr Cyber-Risiko. Häufig steht dahinter die Annahme, dass kleinere Unternehmen für Cyberkriminelle weniger attraktiv seien als Grossunternehmen. Diese Annahme wird zunehmend gefährlich: Angriffe sind skalierbarer geworden und setzen auf schwache Zugangsdaten, Phishing oder manipulierte Zahlungsprozesse. Die Mobiliar-Studie «KMU Cybersicherheit 2025» zeigt diese Wahrnehmungslücke deutlich: Nur 10% der KMU schätzen das Risiko hoch ein, durch einen Cyberangriff mindestens einen Tag ausser Kraft gesetzt zu werden, während 61% der IT-Dienstleister dasselbe Risiko für KMU als hoch einschätzen. Unsere Umfrage zeigt, dass die Wahrnehmungslücke bei Mitarbeitenden ähnlich gross ausfällt: 49% der Mitarbeitenden haben in den letzten drei Monaten einen ernsten Cybervorfall erlebt, aber nur 27% schätzen das Cyberrisiko als hoch ein.

Abbildung 10: Trotz Wachstum weiter geringe Cyberversicherungsdurchdringung bei KMUs



Quelle: SVV 2025

Lücke 3: Versicherung

2) Wie gezeigt fehlen vielen KMUs die notwendigen Sicherheitsmassnahmen, die eine Versicherbarkeit unterstützen oder gar ermöglichen: Multi-Faktor-Authentifizierung, Mitarbeitersensibilisierung und Backup-Konzepte. Der Deloitte KMU-Cybersicherheitsindex zeigt, dass Kleinunternehmen mit 41 von 100 Punkten deutlich unter dem Durchschnitt liegen. Dies betrifft nicht nur mitarbeiterseitige Massnahmen, wie vom Cybersicherheitsindex gemessen, sondern wie die Mobiliar-Studie «KMU Cybersicherheit 2025» zeigt, auch Massnahmen wie einen Notfallplan oder ein Sicherheitskonzept, die nur bei unter einem Drittel der KMUs vorhanden sind.

3) Der Antragsprozess selbst kann für eine Cyberversicherung ein Hindernis sein. Dies wurde häufig in den Expertengesprächen angesprochen. Übermässig komplexe Fragebögen können sowohl Versicherungsberater, Broker als auch Kunden überfordern.

4) Der Vertrieb bei Kleinstunternehmen ist eine strukturelle Hürde. Cyberversicherungen für kleine Unternehmen sind oft günstig, entsprechend gering sind die Provisionen im Agenturvertrieb. Für Versicherungsberater ist der Verkaufsaufwand im Verhältnis zum Ertrag häufig wenig attraktiv. Eine Cyberversicherung wird daher nicht einfach gekauft, sondern muss aktiv verkauft werden – genau hier besteht eine Lücke.

Die Vertriebslücke ist dabei nicht gleichbedeutend mit fehlendem Vertrauen. Die Deloitte-Studie «Die Zukunft der KMU-Versicherung» zeigt etwa, dass Schweizer KMU Versicherern und Vermittlern weiterhin stark vertrauen und gleichzeitig offen für digitale Informations- und Abschlusskanäle sind. Die Herausforderung liegt daher darin, Cyberversicherungen einfach, verständlich und effizient über passende Kanäle zugänglich zu machen.

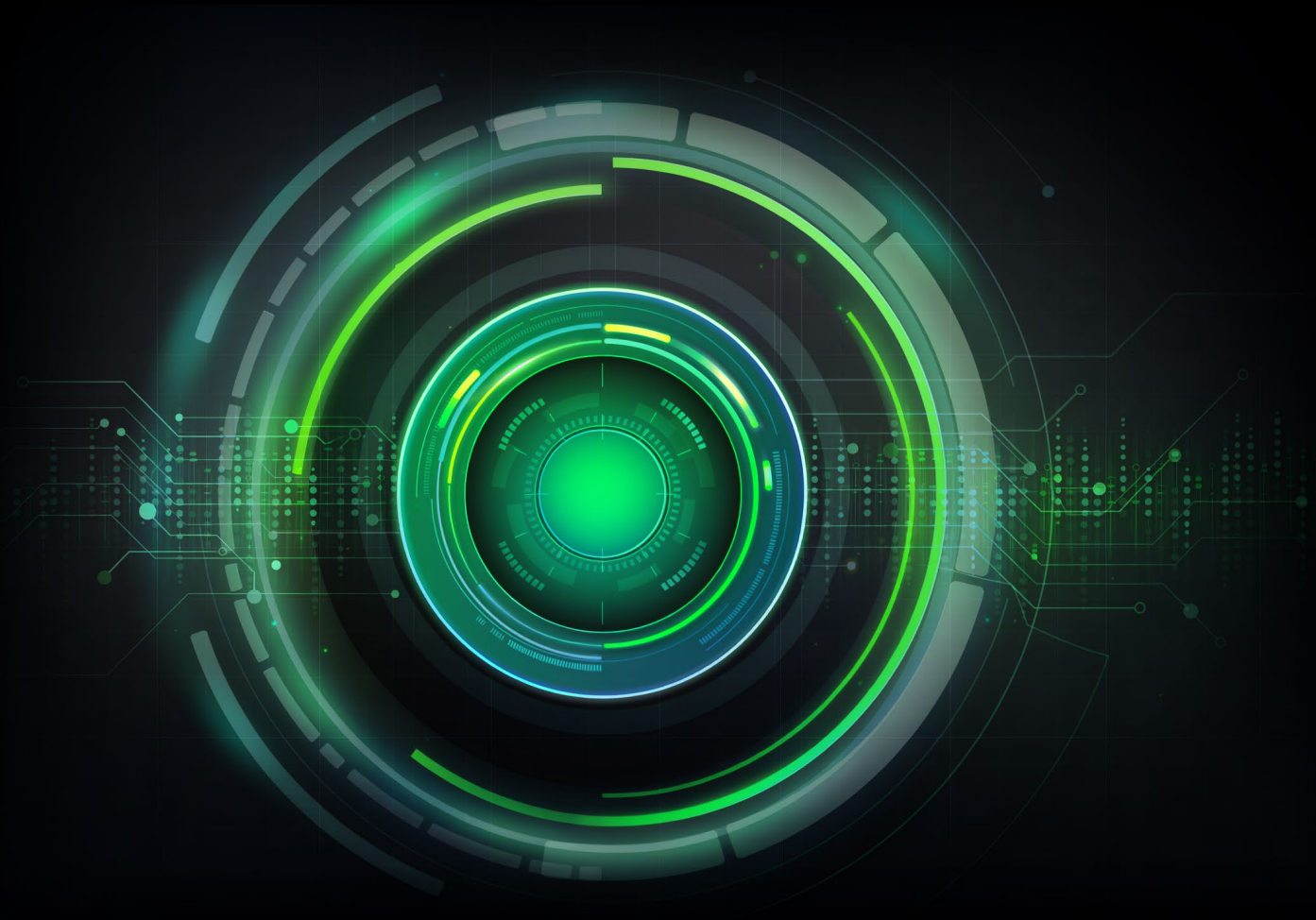
5) KMU-Risiken werden häufig zu technisch gedacht. Ein grosser Teil der Schäden entsteht nicht durch hochkomplexe Angriffe, sondern durch Business-Email-Compromise, CEO-Fraud oder manipulierte Zahlungsanweisungen. Diese Low-Tech-Angriffe basieren oft auf kompromittierten Zugangsdaten, fehlender Sensibilisierung oder unzureichenden Freigabeprozessen.

«Schadenssummen bei kleineren Unternehmen sind absolut in Schweizer Franken zwar kleiner als bei Grossunternehmen, aber in Prozent des Umsatzes durchschnittlich grösser. Ein Cybervorfall kann kleineren Unternehmen wirklich wehtun – oder sogar existenzbedrohend werden.»
Dr. Stephan von Watzdorf, Head Cyber Centre, Swiss Re

Cybersicherheit im KI-Zeitalter

Welche Massnahmen braucht es jetzt, um mit der wachsenden Bedrohungslage Schritt zu halten?

Handlungsoptionen für den Bund, Unternehmen und Versicherer



Bund: Rahmen schaffen, Unternehmen befähigen

Die Befragten sehen Unternehmen als zentrale Akteure bei der Bekämpfung von Cyberrisiken. 46% schreiben Unternehmen eine mehrheitliche oder alleinige Verantwortung zu, während nur 5% die Verantwortung primär bei Mitarbeitenden sehen. Weitere 49% verteilen die Verantwortung gleichmässig.

Gleichzeitig zeigen die Regulierungspräferenzen in einer separaten Frage (Abbildung 11): Der Staat soll unterstützen, mehr Verbindlichkeit wird gefordert, eine reine staatliche Lösung präferieren aber nur wenige: 87% wünschen sich weitergehende Regulierung, bzw. nur 13% sind gegen Regulierung. Aber nur 19% wollen strengere staatliche Regulierung, 81% sehen dies nicht als beste Option. Stattdessen bevorzugen 62% flexible, branchengeführte Standards oder Hybrid-Modelle – 34% eine Kombination aus staatlichen Vorgaben und Branchenstandards, 28% reine Branchenselbstregulierung. Die gewünschte Richtung ist damit eine pragmatische Regulierung: Mindeststandards ja, starre staatliche Detailvorgaben nein.

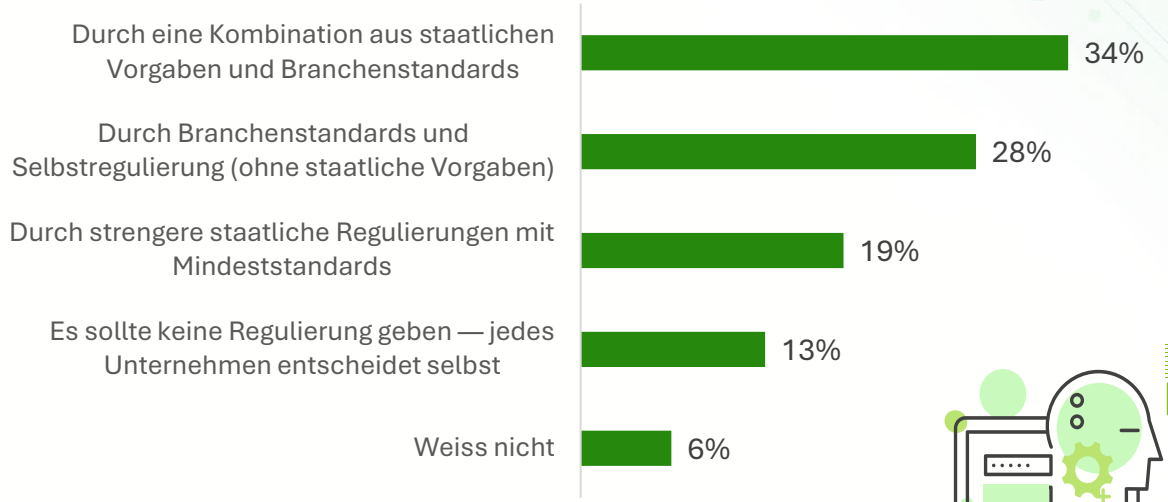
Für den Bund ergeben sich daraus drei Aufträge: Der Bund sollte…

1. leicht verständliche und umsetzbare **Mindeststandards und Orientierungspunkte** schaffen, insbesondere für KMUs und kritische Infrastrukturen. Ein Beispiel hierfür könnte sein, Multi-Faktor-Authentifizierung bei kommerziellen Anbietern für Zahlungsverkehr, Kommunikation, IT-Anbieter oder Social Media verpflichtend zu machen. Ein bedeutender Angriffsvektor würde damit erheblich erschwert.
2. Transparenz und Vergleichbarkeit fördern, etwa durch breit **anerkannte Standards oder Score-Modelle** – ohne den Eindruck zu erwecken, Cyberrisiko sei vollständig messbar.
3. **Koordination und Sensibilisierung** stärken, damit Unternehmen, Branchenverbände, Versicherer und IT-Dienstleister entlang gemeinsamer Leitplanken handeln können.

So kann die Schweiz Cybersicherheit als Standortvorteil positionieren: flexibel genug für Innovation, verbindlich genug für Resilienz.

Abbildung 11: Regulierungspräferenzen für Cybersicherheit

Antworten in Prozent auf die Frage: Wie sollte Cybersicherheit in Unternehmen reguliert werden?



«Die Schweiz ist für ihre Stabilität und ihre hohen Sicherheitsstandards bekannt. Diesen Ruf muss sie nun auf den Bereich der digitalen Sicherheit übertragen, um die Interessen ihres Wirtschaftsstandorts nachhaltig zu sichern. In diesem letzten Punkt müssen wir entschlossen vorankommen, um den Kompetenzaufbau auf individueller und kollektiver Ebene zu beschleunigen und so das zu bewahren, was seit jeher unsere Stärke ausmacht.

Zudem sollen Staat und Privatwirtschaft die Zusammenarbeit bei der Absicherung grosser systemischer Risiken weiter ausbauen. Dafür braucht es einen klaren Rahmen und gemeinsame Regulierungsmechanismen (ÖPP). Mehr Transparenz könnte auch ein Cyber-Score schaffen. Er würde Unternehmen sowie ihren Kundinnen und Kunden einen besseren Einblick in die Verarbeitung ihrer Daten ermöglichen.»
Jesús Pampín, Leiter Kompetenzzentrum Cyber Risk, Schweizerische Mobiliar Versicherungsgesellschaft

Unternehmen: Cyberresilienz beginnt mit den Grundlagen

Optionen für Unternehmen

Entgegen der immer noch häufigen Meinung, dass KMUs aufgrund ihrer Grösse weniger gefährdet seien, sind Cyberrisiken für alle Unternehmen relevant, wie etwa Microsoft schreibt. Zudem ist die dreifache Sicherheitslücke – Risikounterschätzung, unzureichende Sicherheitsmassnahmen und Versicherungsabdeckung - gerade bei KMUs besonders ausgeprägt. Das Risiko wird durchschnittlich stärker unterschätzt, Sicherheitsmassnahmen weniger stringent umgesetzt, Versicherungen sind seltener vorhanden. Schadensfälle können stärker auf die Unternehmensergebnisse durchschlagen. Basierend auf unserer Umfrage, Expertengesprächen und den Empfehlungen des SVV ergeben sich die folgenden Massnahmen:

Erstens: Mitarbeiterseitige Mindeststandards konsequent einhalten. Dazu gehören beispielsweise geregelte Zugriffsrechte, starke Passwortregeln, Multi-Faktor-Authentifizierung (wenn möglich Passwortlose Authentifizierung), eingeschränkte Administratorenrechte, oder regelmässige Sensibilisierung der Mitarbeitenden. Die Investition in diese elementaren Massnahmen ist deutlich günstiger als die Kosten eines Cybervorfalls.

Zweitens: In weitergehende Sicherheitsmassnahmen investieren. Weitere Schutzmassnahmen wie regelmässige Backups mit Wiederherstellungsfähigkeit, Notfallplanung oder Schwachstellenscans reduzieren das tatsächliche Risiko zusätzlich und können zu besseren Versicherungskonditionen führen. Backups sollten automatisiert, verschlüsselt und vom Netzwerk getrennt gespeichert werden; die Wiederherstellung sollte mindestens zweimal jährlich getestet werden. Zusätzlich sollten Netzwerke geschützt und segmentiert, Fernzugriffe über Zwei-Faktor-Authentifizierung (wenn möglich Passwortlose Authentifizierung) abgesichert sowie veraltete Software und Hardware systematisch ersetzt oder isoliert werden. Die Dringlichkeit dieser Massnahmen wird durch die Studie «KMU Cybersicherheit 2025» unterstrichen, die die niedrige Durchdringung solcher Massnahmen bei KMUs aufzeigt.

Drittens: Versicherungsschutz nicht unterschätzen. Cyberversicherungen bieten finanzielle Deckung und darüber hinaus Zusatzdienstleistungen wie die Assistance-Komponente – Krisenmanagement, Notfallplanung, Zugang zu Spezialisten im Notfall. KMUs, die vorbereitet sind und einen Notfallplan haben, bewältigen Vorfälle besser. Grundlegende Sicherheitsmassnahmen sind zudem für den Abschluss und die Konditionen einer Cyberversicherung relevant. Versicherungsschutz ist daher auch eine Investition in Geschäftskontinuität, nicht nur in Schadensersatz.

Viertens: IT nicht selber betreiben, sondern professionell betreiben lassen. Sehr kleine, kleine und mittlere Unternehmen sollten sich verstärkt auf ihre eigenen Kernkompetenzen ausrichten und ihre IT auslagern, statt sie selbst zu betreiben – auch wenn dies knappes Investitionskapital benötigen kann. Entscheidend ist jedoch nicht bloss die Nutzung von Cloud-Diensten, sondern deren professionelle Konfiguration und laufende Verwaltung. Gerade bei E-Mail, Identitäten, Zugriffsrechten, Backups und Cloud-Umgebungen entstehen viele Risiken durch Fehlkonfiguration oder fehlende Multi-Faktor-Authentifizierung. Professionell gemanagte IT ist deshalb häufig günstiger und sicherer als interne Ad-hoc-Lösungen.

Fünftens: Zahlungs- und Freigabeprozesse gegen Kompromittierung geschäftlicher E-Mail-Konten absichern. Viele KMU-Schäden entstehen durch manipulierte Rechnungen, gefälschte Zahlungsanweisungen oder kompromittierte E-Mail-Konten. Deshalb sollten KMUs klare Vier-Augen-Prozesse, Rückrufpflichten bei geänderten Bankverbindungen, MFA für E-Mail-Konten und regelmässige Sensibilisierung etablieren. Ergänzend sollten potenziell gefährliche E-Mail-Anhänge blockiert, Makros eingeschränkt sowie Spam- und Internetfilter eingesetzt werden.

Versicherungen: Schliessen der Versicherungslücke

Optionen für Versicherer

Entscheidend sind vereinfachte Produkte, bessere Vertriebsanreize, verständliche Kundensprache, verstärkter, aber differenzierter, Einsatz von technologiegetriebener Risikoprüfung und Assistance-Leistungen im Schadenfall.

Vereinfachung und Kundenfreundlichkeit:

Statt komplexer Fragebögen sollten Versicherer technologiegetriebene Risikoprüfung einsetzen und den Antragsprozess radikal vereinfachen. Vereinfachung bedeutet nicht nur weniger Fragen, sondern auch bessere Vertriebslogik. Gerade bei Kleinstunternehmen sind geringe Prämien und niedrige Provisionen ein Hindernis. Versicherer sollten deshalb einfache, bündelbare Produkte entwickeln, die über bestehende Kanäle effizient verkauft werden können. Zusätzlich könnte geprüft werden, inwieweit bestehende durch neue, digitale Verkaufskanäle ergänzt werden könnten. Schweizer KMU schätzen weiterhin persönliche Beratung durch Versicherer, Makler und Agenten, sind aber zugleich offen für digitale Kanäle. Laut Deloitte sind 36% der Schweizer KMU bereit, Versicherungen online zu kaufen, deutlich mehr als der internationale Durchschnitt von 23%. Gleichzeitig kann die Kundenansprache weiter optimiert werden: weniger technische Details, mehr Fokus auf Risiken und Risikotransfer sowie Krisenmanagement und Unterstützung in der Krise. Berater und Broker können noch besser geschult und mit datengestützten Beratungshilfen ausgestattet werden.

Technologiegetriebene Risikoprüfung:

Kontinuierliche, automatisierte Scans (Internet-Footprint, Dark-Web-Monitoring, Schwachstellen) können einmalige Befragungen ergänzen und in bestimmten Segmenten teilweise ersetzen. Ihre Aussagekraft ist jedoch je nach Unternehmensgrösse unterschiedlich: Bei mittelgrossen Unternehmen können Outside-in-Scans wertvolle Signale liefern. Bei Kleinstunternehmen zeigen sie oft primär die IT-Dienstleister oder Cloud-Anbieter, nicht das tatsächliche Verhalten des Unternehmens.

Mindeststandards und ein möglichst universeller, transparenter Cyber Score:

Ein solcher schafft Klarheit und Vergleichbarkeit und setzt Anreize für die Umsetzung von Sicherheitsmassnahmen. Um eine Verbesserung zu heutigen Standards, Scans oder Scores zu sein, muss ein Cyber Score breit anerkannt und Transparenz schaffen, ohne Scheingenauigkeit zu erzeugen. Die Einführung muss entsprechend breit getragen sein und ist nicht Aufgabe einzelner Versicherer, sondern kann nur branchenübergreifend sinnvoll eingeführt werden. Zugleich sollten Cyber Scores nicht überschätzt werden. Zwar sind sehr schlechte Scores ein Warnsignal; durchschnittliche oder gute Scores beweisen aber nicht automatisch ein gutes Risiko. Zudem können Unternehmen ihre externe Sichtbarkeit und damit Scores aktiv managen. Entscheidend bleibt die Kombination aus Daten, Mindeststandards, Präventionsmassnahmen und Schadenhistorie.

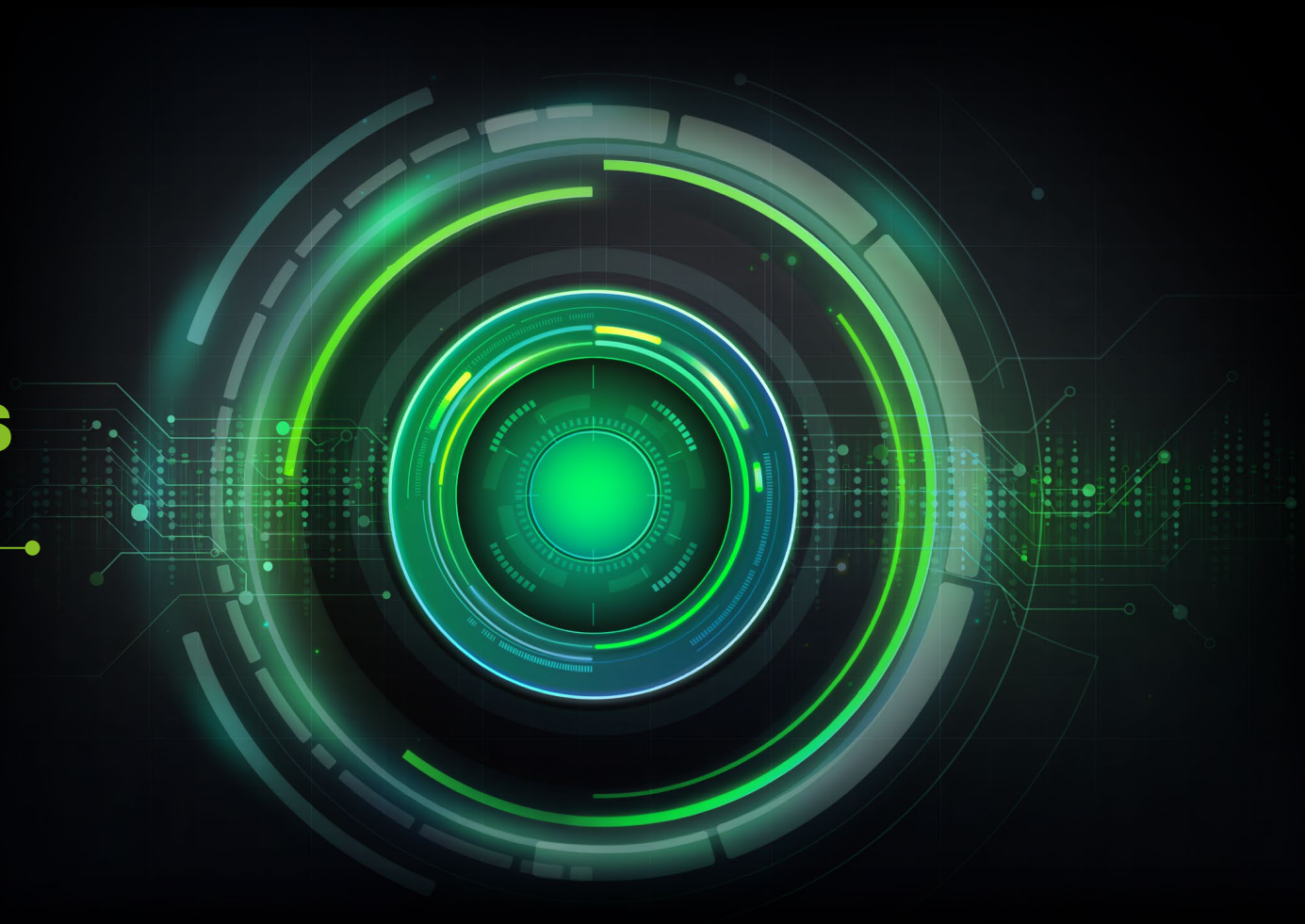
Prävention und Zusatzdienstleistungen:

Notfallplanung, technische Beratung und Spezialistenunterstützung im Notfall differenzieren Versicherer und schaffen echten Mehrwert. Präventionsleistungen sollten besonders auf häufige KMU-Schäden ausgerichtet werden: Kompromittierung geschäftlicher E-Mail-Konten, CEO-Fraud und manipulierte Zahlungsprozesse. Zu den potentiellen Angeboten gehören MFA, Zahlungsfreigabeprozesse, Sensibilisierung, Empfehlungen zur Bewältigung von Sicherheitsvorfällen und schneller Zugang zu Spezialisten im Schadenfall. Gerade die Assistance-Komponente kann für KMUs wertvoller sein als die reine Deckung.

«Cyber-Versicherungen sind nicht Luxus, sondern eine Notwendigkeit – aber das Produkt muss einfacher verständlich und leichter zugänglich werden. Cyber ist seit Jahren das Nummer-1-Risiko, das unsere Kunden beunruhigt. Zusammen mit Betriebsunterbrechungen, Datenschutzregulierungen und künstlicher Intelligenz ist es zentral.»

Ivo Heeb, Expert Underwriter Cyber & Technology, Allianz Commercial

Kontakte und Quellenverzeichnis



Autoren und Kontakte

Florian Widmer
Partner, Cyber
+41 58 279 69 10
fwwidmer@deloitte.ch

Marcel Thom
Partner, Leiter Versicherungen
+41 58 279 51 79
mthom@deloitte.ch

Dennis Brandes
Senior Research Manager
+41 58 279 65 37
dbrandes@deloitte.ch

Martin Gertsch
Director
+41 58 279 62 44
mgertsch@deloitte.ch

Quellenverzeichnis

BMC (o. J.), Software modernization: solutions, strategies, and examples, Internetseite: https://www.bmc.com/blogs/application-software-modernization/

Cybersecurity Ventures (2025), 2025 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics, https://cybersecurityventures.com/cybersecurity-almanac-2025/

CrowdStrike (2026), Global Threat Report 2026, https://www.crowdstrike.com/en-us/global-threat-report/

Deloitte (2022), Die Zukunft der Versicherungen für Kleinunternehmen, https://www.deloitte.com/ch/de/Industries/insurance/analysis/the-future-of-small-business-insurance.html

Deloitte (2025), Cyber Threat Trends Report 2025, https://www.deloitte.com/us/en/services/consulting/articles/cybersecurity-report-2025.html

Die Mobiliar et al. (2025), KMU Cybersicherheit 2025, repräsentative Online-Befragung von 515 KMU mit 1-49 Mitarbeitenden und 336 IT-Dienstleistungsunternehmen in der Deutsch-, französischen und italienischen Schweiz, Befragungszeitraum 25. Juni bis 5. August 2025, https://www.mobiliar.ch/studie/cybersicherheit-schweiz

IBM (o. J.), 5 best practices for managing application growth, https://www.ibm.com/think/insights/5-best-practices-managing-application-growth

Microsoft (2024), 7 cybersecurity trends and tips for small and medium businesses to stay protected, https://www.microsoft.com/en-us/security/blog/2024/10/31/7-cybersecurity-trends-and-tips-for-small-and-medium-businesses-to-stay-protected/

MuleSoft (o. J.), Legacy applications can be revitalized with APIs, https://www.mulesoft.com/legacy-system-modernization/legacy-application

Munich Re (2025), Cyber Insurance: Risks and Trends 2025, https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html

SecurityScorecard (2025), Global Third-Party Breach Report, Analyse von 1’000 Datenpannen über Branchen und Regionen hinweg, https://securityscorecard.com/resources/resources/global-third-party-breach-report/

Schweizerischer Versicherungsverband SVV (2025): KMU: In sechs Schritten zu mehr Cybersicherheit, https://svv.ch/de/hintergruende/listicle/kmu-sechs-schritten-zu-mehr-cybersicherheit

Schweizerischer Versicherungsverband SVV (2025): Prämienvolumen für Cyberversicherungen wächst – Schutzlücke bei KMU noch immer gross, https://svv.ch/de/news/medienmitteilung/praemienvolumen-fuer-cyberversicherungen-waechst-schutzluecke-bei-kmu-noch

Deloitte.