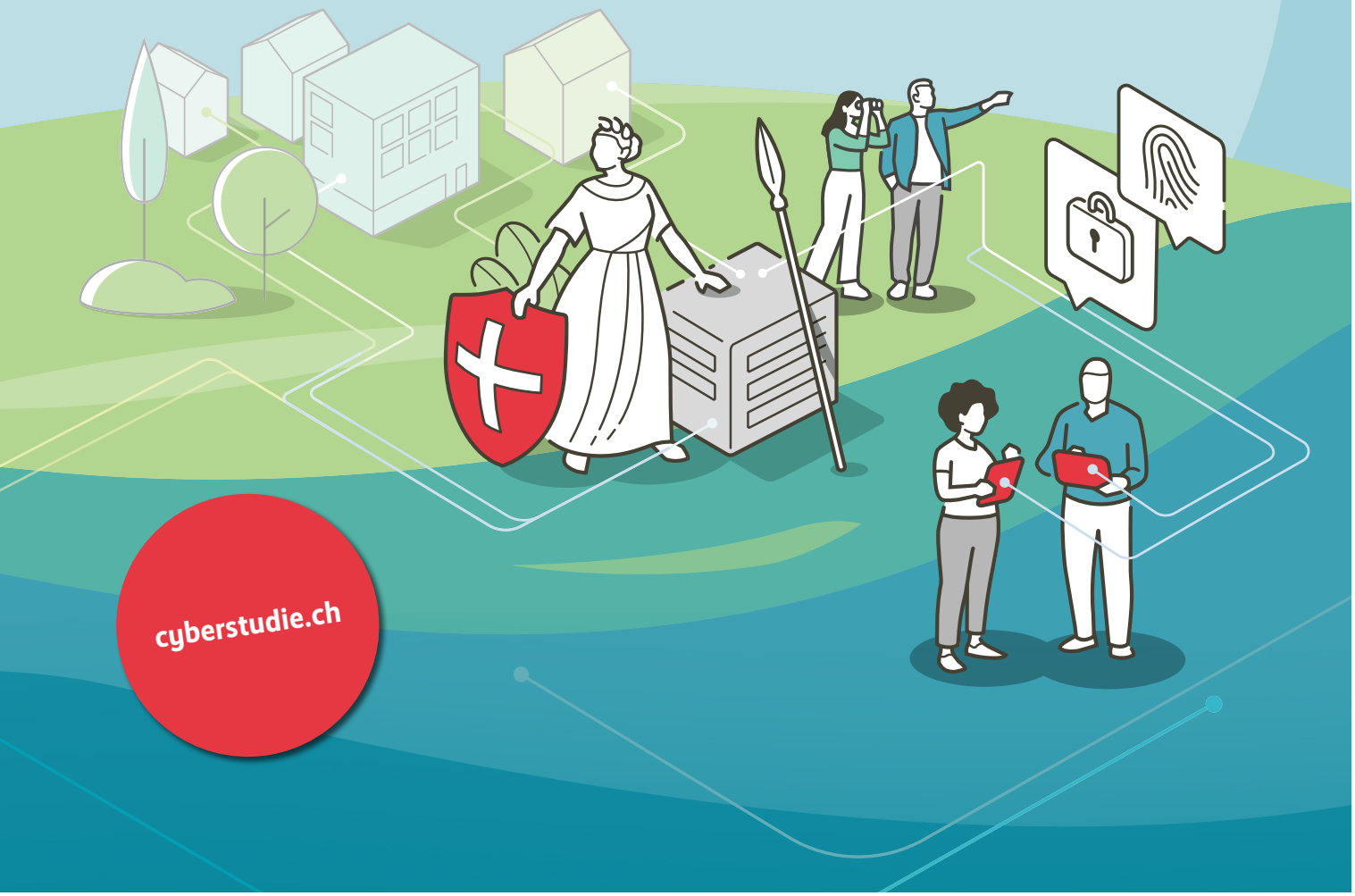
die Mobiliar

KMU Cybersicherheit 2026

Eine Mobiliar Studie in Zusammenarbeit mit BACS, digitalswitzerland, HES-SO, HWZ und SATW

Marc K. Peter, Romain Geiser, Anu Anthamatten, Karin Mändli Lerch, Léonard Marbe, Dr. Anna V. Rozumowski und Tobias Schlegel



cyberstudie.ch

digitalswitzerland

die Mobiliar

satw technology for society

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Hes·so VALAIS WALLIS
School of Management

HWZ Hochschule für Wirtschaft Zürich

YouGov®

Inhalt

Einleitung 3

01 Schweizer KMU – wo stehen sie aktuell im digitalen Zeitalter? 4

02 Digitale Souveränität – ein neues Themenfeld in der aktuellen Weltpolitik 6

03 Cyberkriminalität – ein ernstzunehmendes Problem mit neuen Gefahren durch die KI 8

04 Cyberkriminalität im KMU: Über 35 000 Betroffene und oft mit spürbaren Folgen 10

05 Kenntnis Cyberbedrohungslage und Unterstützung 12

06 Cybersicherheit wird wichtiger und gewinnt wieder an Bedeutung 14

07 Cyberrisk-Verantwortung: Immer mehr KMU regeln Zuständigkeiten 16

08 Umsetzung technischer Cybersicherheitsmassnahmen 18

09 Umsetzung organisatorischer Cybersicherheitsmassnahmen 20

10 Die Zukunft: Cyberresilienz wird wichtiger, aber viele KMU bleiben zurückhaltend 22

Checkliste für Schweizer KMU 24

Praxistools und Forschungsmethodik 26

Kontakt Autorinnen und Autoren 27

Einleitung

Die digitale Transformation hat Schweizer KMU in den letzten Jahren spürbar vorangebracht. Viele Unternehmen investieren in digitale Prozesse, nutzen Cloud-Dienste, setzen zunehmend auf digitale Strategien und beschäftigen sich mit neuen Technologien wie Künstlicher Intelligenz (KI). Gleichzeitig wächst die Abhängigkeit von digitalen Systemen, Daten und externen Dienstleistern. Damit steigen auch die Risiken. Cyberkriminalität gehört heute zu den wichtigsten strategischen Herausforderungen für Schweizer KMU und die grosse Mehrheit der Unternehmen erwartet, dass die Bedrohung durch KI in Zukunft weiter zunehmen wird.

Seit 2020 wir die KMU-Studie jährlich durchgeführt. Die Ergebnisse der aktuellen Studie KMU Cybersicherheit 2026 zeigen ein differenziertes Bild zur KMU-Landschaft in der Schweiz: Viele KMU verfügen über solide technische Grundlagen wie Software-Updates, Firewalls, Datensicherungen und Mehrfaktor-Authentifizierung. Gleichzeitig bestehen bei organisatorischen Massnahmen (wie in den Vorjahren) noch deutliche Lücken. Notfallpläne, Sicherheitsaudits, Lieferantenbewertungen oder systematische Mitarbeiterschulungen sind oft weniger verbreitet, obwohl gerade sie im Ernstfall entscheidend für die Resilienz (Widerstandsfähigkeit) eines Unternehmens sein können.

Erfreulich ist, dass Cybersicherheit wieder stärker in den Fokus rückt. Immer mehr Unternehmen definieren Verantwortlichkeiten und investieren konstant in zusätzliche Schutzmassnahmen. Die wahrgenommene Cyberresilienz hat sich gegenüber 2025 erholt, liegt jedoch weiterhin unter dem Niveau von 2024. Gleichzeitig zeigt die Studie, dass viele KMU das Risiko eines schwerwiegenden Cybervorfalls noch immer eher tief einschätzen.

Die wichtigste Erkenntnis lautet deshalb: Cybersicherheit ist heute keine reine IT-Aufgabe mehr, sondern eine Führungsaufgabe. Erfolgreiche KMU schützen nicht nur ihre Systeme und Daten, sondern bereiten sich auch organisatorisch auf den Ernstfall vor. Wer technische Schutzmassnahmen mit klaren Verantwortlichkeiten, geschulten Mitarbeitenden, getesteten Backups und einem funktionierenden Notfallplan kombiniert, erhöht seine Cyberresilienz nachhaltig und stärkt gleichzeitig die Wettbewerbsfähigkeit seines Unternehmens.

In zehn Kapiteln erläutern wir die zentralen Ergebnisse der neuesten Ausgabe der Studie «KMU Cybersicherheit 2026» und präsentieren Empfehlungen für die Erhöhung der Cybersicherheit und Cyberresilienz im KMU. Die detaillierten Studienergebnisse finden Sie auf cyberstudie.ch.

Bern und Zürich im Oktober 2026

Die Mobiliar, BACS, digitalswitzerland, HES-SO, HWZ und SATW

01 Schweizer KMU – wo stehen sie aktuell im digitalen Zeitalter?

Die aktuelle KMU-Befragung zeigt ein differenziertes Bild der digitalen Transformation in der Schweiz. Viele Unternehmen haben den Weg in die Digitalisierung eingeschlagen, doch die Fortschritte fallen je nach Branche, Unternehmensgrösse und Innovationsbereitschaft unterschiedlich aus.



Positiv ist, dass die Mehrheit der KMU ihre digitale Entwicklung als zumindest mittelmässig fortgeschritten einschätzt. Rund jedes zehnte Unternehmen beurteilt den Fortschritt seiner digitalen Strategie sogar als weit oder sehr weit fortgeschritten. Gleichzeitig gibt es aber noch viel Potenzial: ***Fast jedes fünfte KMU verfügt nach eigener Einschätzung weder über eine digitale Strategie noch über entsprechende Projekte.***

Follower. Bei Letzteren fehlt zudem am häufigsten eine digitale Strategie. Die Studie zeigt: ***Unternehmen, die neue Technologien früh ausprobieren und einsetzen, weisen einen deutlich höheren digitalen Reifegrad aus als Late Follower.***

Bei den laufenden Digitalisierungsprojekten stehen praktische Nutzenaspekte im Vordergrund. ***Am häufigsten investieren KMU in Projekte zur Steigerung der Kundenzufriedenheit, zur besseren Nutzung von Daten sowie zur Digitalisierung und Automatisierung von Prozessen***. Diese Initiativen helfen direkt dabei, effizienter zu arbeiten und die Wettbewerbsfähigkeit zu stärken. Weniger stark verbreitet sind dagegen Projekte zur Entwicklung neuer digitaler Geschäftsmodelle, zur Einführung neuer Technologien oder zur Erhöhung der Arbeitgeberattraktivität.

Besonders auffällig ist die Situation bei der Künstlichen Intelligenz (KI): ***Fast die Hälfte der befragten KMU hat bisher keine entsprechenden Projekte im Umfeld der KI umgesetzt.*** Obwohl KI derzeit in aller Munde ist, befindet sich ihre Nutzung im Schweizer KMU-Sektor somit noch in einer frühen Phase.

Die ***grössten strategischen Chancen*** sehen KMU in der Unternehmens- und Innovationskultur, in

Fast die Hälfte der befragten KMU hat bisher keine entsprechenden Projekte im Umfeld der KI umgesetzt.

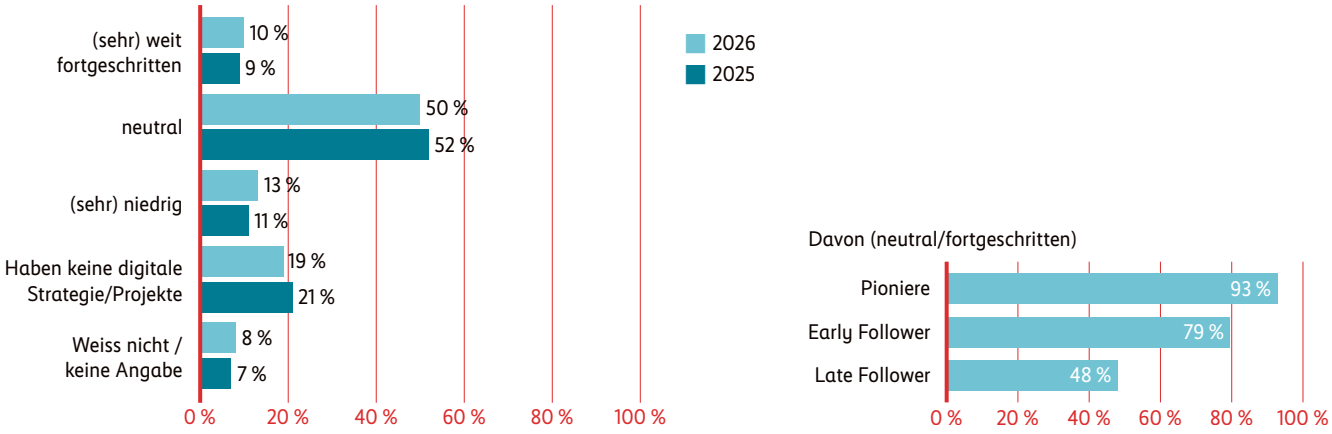
Besonders interessant ist der Zusammenhang zwischen Innovationsverhalten und Digitalisierung. ***Unternehmen, die neue Technologien früh ausprobieren und einsetzen (Pioniere), bewerten ihren digitalen Reifegrad deutlich höher als die Late***

Partnerschaften sowie in der Digitalisierung und Automatisierung. Zudem ist das Homeoffice bei KMU weiter verbreitet als im Vorjahr: ***61% der Unternehmen bieten ihren Mitarbeitenden zumindest teilweise Homeoffice an.***

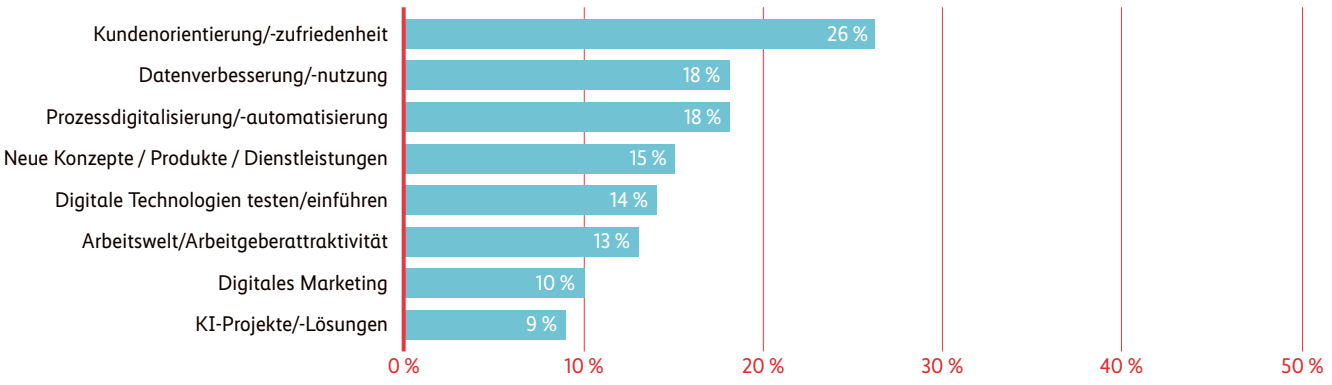
Die Weltpolitik/-wirtschaft ist aus Sicht der KMU das grösste strategische Risiko. Je rund ein Fünftel bis ein Viertel sehen in Inflation, Cyberkriminalität und Fachkräftemangel strategische Risiken. Mit zunehmender Unternehmensgrösse gewinnen insbesondere Fachkräftemangel und Cyberkriminalität an Bedeutung.

Die Ergebnisse zeigen insgesamt: Schweizer KMU digitalisieren sich kontinuierlich, der Fokus liegt jedoch vor allem auf der Optimierung des bestehenden Geschäfts. Die wirklich grossen Chancen der digitalen Transformation, etwa durch neue digitale Angebote, innovative Geschäftsmodelle oder den gezielten Einsatz von KI werden bislang erst von einer Minderheit aktiv genutzt. Für viele Unternehmen könnte genau hier das grösste Potenzial für die kommenden Jahre liegen.

Fortschritt digitale Strategie
Frage: Wie schätzen Sie den Fortschritt Ihrer digitalen Strategie bzw. digitalen Transformation ein?
Skala: 1–2: (sehr) niedrig / 3–5: neutral / 6–7: (sehr) weit fortgeschritten.



Umgesetzte digitale Strategiemassnahmen
Frage: Bitte geben Sie auf einer Skala von 1–7 an, inwiefern Ihr Unternehmen in den vergangenen drei Jahren die folgenden Massnahmen umgesetzt hat.
Skala: 1–2: nein, (überhaupt) nicht umgesetzt / 3–5: neutral / 6–7: (voll und ganz) umgesetzt. Dargestellte Resultate: Skala 6–7 ((voll und ganz) umgesetzt)



02 Digitale Souveränität – ein neues Themenfeld in der aktuellen Weltpolitik

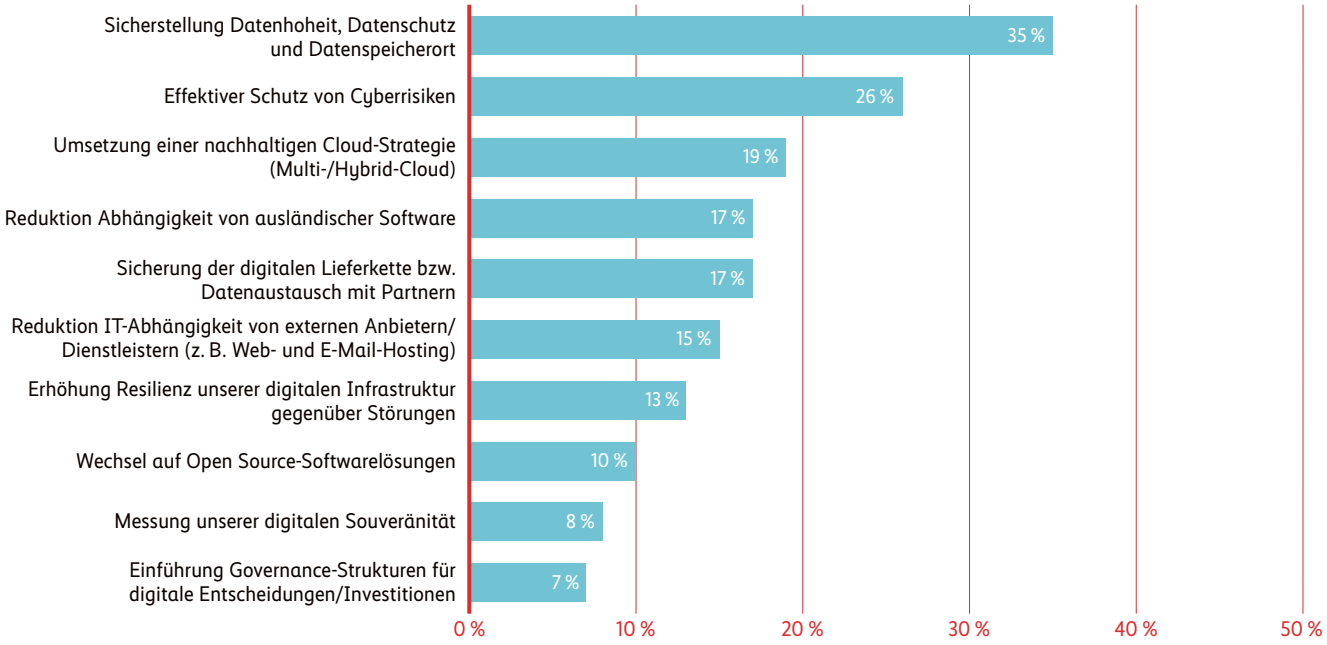
Die geopolitischen Entwicklungen der letzten Jahre haben ein neues Thema in den Fokus gerückt: die digitale Souveränität. Gemeint ist ***die Fähigkeit eines Unternehmens, möglichst selbstbestimmt über Daten, Technologien und digitale Abhängigkeiten entscheiden zu können.*** Die aktuelle Studie zeigt jedoch, dass sich Schweizer KMU erst am Anfang dieser Entwicklung befinden.

Am weitesten fortgeschritten sind KMU bei den klassischen Themen ***Datenschutz, Datenhoheit und Datenspeicherung.*** Mehr als ein Drittel der befragten Unternehmen hat hierzu bereits konkrete Massnahmen umgesetzt. Auch der ***Schutz vor Cyberrisiken*** wird von vielen Firmen aktiv verfolgt. Diese Bereiche werden von den Unternehmen offenbar als unmittelbar relevant und geschäftskritisch wahrgenommen.

Deutlich weniger ausgeprägt sind dagegen Massnahmen, welche die ***Abhängigkeit von einzelnen Technologien oder Anbietern reduzieren*** sollen. Nur eine Minderheit der KMU hat beispielsweise bereits Schritte unternommen, um die Abhängigkeit von ausländischer Software, externen IT-Dienstleistern oder Cloud-Anbietern zu verringern. Ebenso werden Themen wie die Absicherung der digitalen Lieferkette oder der Wechsel auf Open-Source-Lösungen bislang nur vereinzelt umgesetzt.

Besonders spannend ist, ***dass viele Unternehmen von einigen Aspekten der digitalen Souveränität noch kaum gehört haben.*** So kennen rund ein Viertel der Befragten keine Governance-Strukturen für digitale Entscheidungen (nur 7 % verfügen über eine Governance) und fast ein Drittel hat sich noch nie mit der Messung der eigenen digitalen

Digitale Souveränität
Frage: Haben Sie bereits Massnahmen zum Thema «digitale Souveränität» geplant oder umgesetzt?
Skala: 1 (noch nie gehört) bis 4 (bereits umgesetzt). Dargestellte Resultate: Skala 4 (bereits umgesetzt)





Souveränität beschäftigt. Gerade diese Themen könnten aber in Zukunft an Bedeutung gewinnen, wenn Unternehmen ihre digitalen Risiken systematischer steuern möchten.

Insgesamt zeigt die Studie: Schweizer KMU kümmern sich bereits aktiv um Datenschutz und Cybersicherheit, betrachten digitale Souveränität aber meist noch aus dieser engen Perspektive. ***Die weitergehende Frage, wie sich strategische Abhängigkeiten von Technologien, Plattformen oder einzelnen Anbietern reduzieren lassen, ist für viele Unternehmen noch Neuland.*** Wer sich frühzeitig mit diesen Themen auseinandersetzt, kann seine Resilienz stärken und in einer zunehmend unsicheren digitalen Welt unabhängiger agieren.

Viele Unternehmen haben von einigen Aspekten der digitalen Souveränität noch kaum etwas gehört.

03 Cyberkriminalität – ein ernstzunehmendes Problem mit neuen Gefahren durch die KI

Cyberkriminalität ist bei Schweizer KMU längst auf der Geschäftsleitungsagenda angekommen. Die aktuelle Studie zeigt ein bemerkenswert klares Bild: Fast neun von zehn Unternehmen (88 %) betrachten Cyberkriminalität als ein ernstzunehmendes Problem. Über Unternehmensgrössen, Branchen und Unternehmensarten hinweg herrscht weitgehend Einigkeit: ***Cyberangriffe sind heute eine reale Bedrohung für jedes KMU.***

Aussage. KI wird damit von vielen Unternehmen nicht nur als Chance, sondern auch als neuer Risikofaktor wahrgenommen.

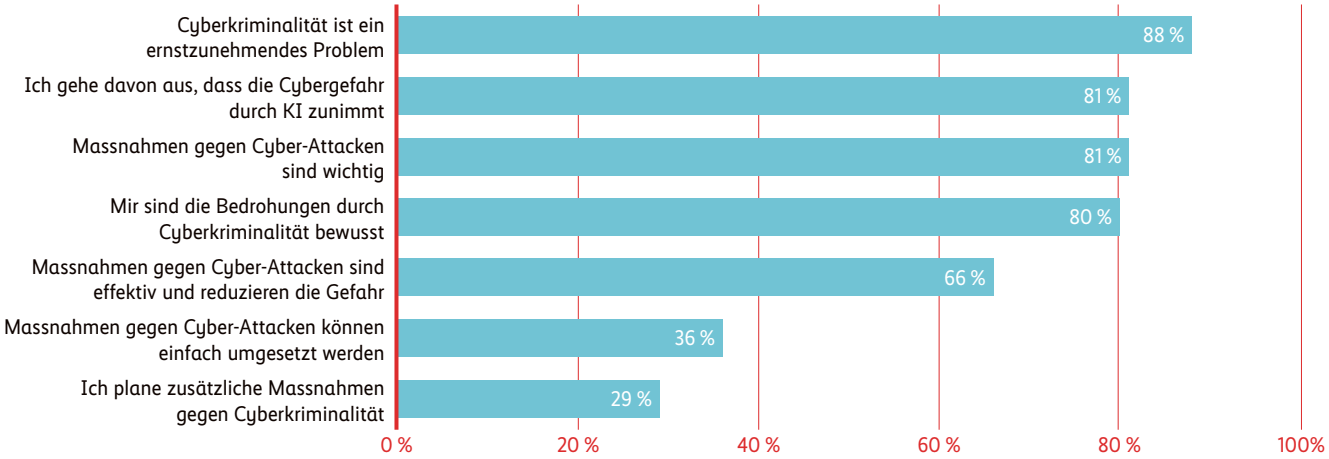
Besonders interessant ist, dass sich die Wahrnehmung der Bedrohung kaum zwischen kleinen und grösseren KMU unterscheidet. Egal ob ein Unternehmen wenige Mitarbeitende beschäftigt oder bereits mehrere Dutzend Personen zählt:

Gut vorbereitete KMU sehen also nicht nur mehr Gefahren, sondern auch mehr Handlungsmöglichkeiten.

Neu zeigt die Studie zudem, dass sich die Sorge nicht nur auf bestehende Cyberrisiken bezieht. ***Vier von fünf KMU (81%) gehen davon aus, dass die Cybergefahr durch KI weiter zunehmen wird.*** Nur eine sehr kleine Minderheit widerspricht dieser

Die Einschätzung der Gefahrenlage ist nahezu identisch. Cyberkriminalität wird heute als Herausforderung für die gesamte Schweizer KMU-Landschaft verstanden.

Einstellung zu Cyberkriminalität
Frage: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Skala: 1 (überhaupt nicht) bis 5 (voll und ganz). Dargestellte Resultate: Skala 4–5 (voll und ganz)



Die Studie zeigt jedoch auch eine wichtige Erkenntnis: Das Problembewusstsein allein reicht nicht aus. Unternehmen, die sich besser über Cybersicherheit informiert fühlen und bereits technische oder organisatorische Schutzmassnahmen umgesetzt haben, beurteilen die Risiken zwar ähnlich hoch wie andere Unternehmen. Sie sind jedoch deutlich überzeugter, dass sich Cyberrisiken wirksam reduzieren lassen. ***Gut vorbereitete KMU sehen also nicht nur mehr Gefahren, sondern auch mehr Handlungsmöglichkeiten.***

Insgesamt lässt sich festhalten: Schweizer KMU erkennen die Bedrohung durch Cyberkriminalität klarer denn je. Gleichzeitig sorgt der rasche Fortschritt bei KI dafür, dass viele Unternehmen von einer weiteren Verschärfung der Risiken ausgehen. Die Herausforderung der kommenden Jahre wird deshalb nicht sein, das Problembewusstsein zu erhöhen. Die Herausforderung besteht vielmehr darin, dieses Bewusstsein in konkrete Schutzmassnahmen und laufende Weiterbildung umzusetzen.



04 Cyberkriminalität im KMU: Über 35 000 Betroffene und oft mit spürbaren Folgen

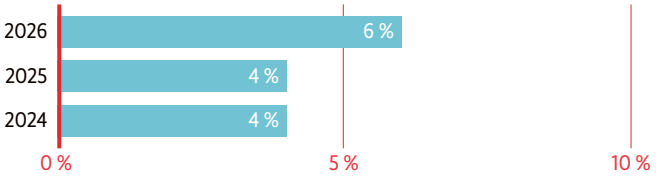


Die gute Nachricht zuerst: Die grosse Mehrheit der Schweizer KMU blieb in den letzten drei Jahren von schwerwiegenden (bekannten) Cyberangriffen verschont. Dennoch zeigt die Studie, dass Cyberkriminalität für betroffene Unternehmen erhebliche Auswirkungen haben kann. Sechs Prozent der befragten KMU (bzw. hochgerechnet über 35 000 KMU in der Schweiz) gaben an, in den vergangenen drei Jahren einen Cyberangriff erlebt zu haben. Viele der Betroffenen gaben an, dass dieser zu finanziellem Schaden, Reputationsproblemen, grossem Aufwand oder einer starken persönlichen Belastung führte. Bei Unternehmen mit mindestens zehn Mitarbeitenden liegt der Anteil an Betroffenen sogar deutlich höher und erreicht bis zu 16 Prozent.

Besonders interessant ist die Art der entstandenen Schäden. Entgegen der öffentlichen Wahrnehmung stehen nicht primär finanzielle Verluste im Vordergrund. ***Am häufigsten berichten betroffene Unternehmen von einem grossen Arbeitsaufwand zur Schadensbehebung, gefolgt von der emotionalen Belastung.*** Erst danach folgen finanzielle Schäden, Reputationsverluste oder der Verlust von Kundendaten. Cyberangriffe kosten also oft vor allem Zeit, Energie und Nerven der Verantwortlichen.

Ein weiteres wichtiges Ergebnis: Es gibt nicht den einen typischen Angriff. ***Erfolgreiche Angriffe erfolgen über verschiedene Wege. Am häufigsten genannt werden Phishing, Passwort-Hacking, Schadsoftware sowie Netzwerk- und Serverangriffe, die jeweils bei rund einem Drittel der Vorfälle eine Rolle spielen.*** Für KMU bedeutet dies, dass sie sich nicht nur gegen eine einzelne Bedrohung schützen sollten, sondern gegen ein ganzes Spektrum unterschiedlicher Angriffstechniken.

Cyberangriffe mit Schaden
Frage: Hat Ihr Unternehmen innerhalb der letzten 3 Jahre einen Cyberangriff erlitten, der einen finanziellen Schaden oder einen Reputationsschaden verursachte, viel Mühe für die Schadensbereinigung bereitete oder Ihnen emotional sehr zu schaffen gemacht hat? (Antwort: Ja)

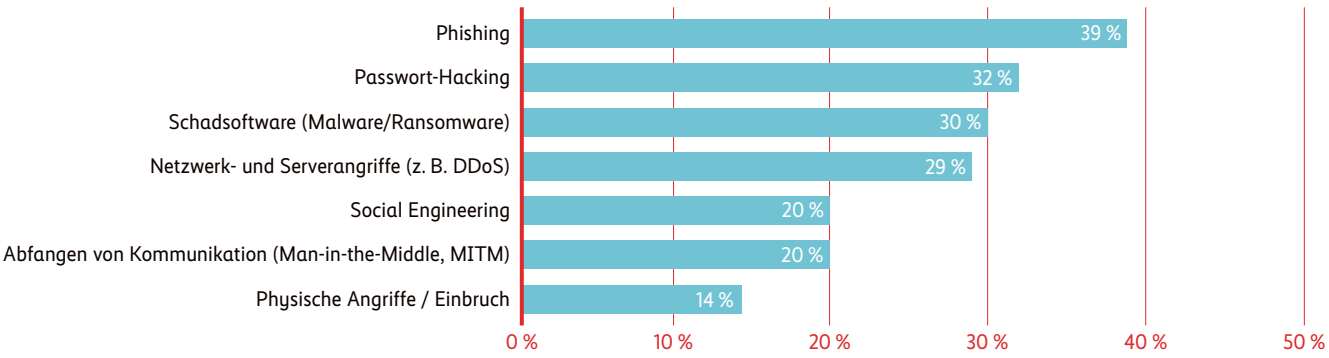


Am häufigsten berichten betroffene Unternehmen von einem grossen Arbeitsaufwand zur Schadensbehebung.

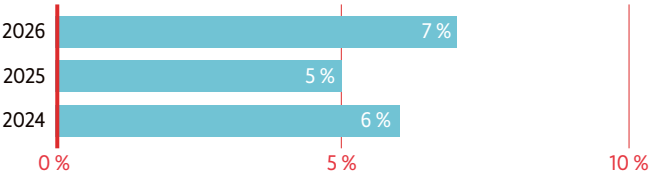
Auch das Thema Erpressung bleibt relevant.
Rund sieben Prozent der befragten Unternehmen (bzw. hochgerechnet ca. 45 000 KMU in der Schweiz) wurden bereits von Cyberkriminellen erpresst. Besonders betroffen sind grössere KMU sowie Unternehmen aus Industrie und Bau.
Von den erpressten Unternehmen haben einzelne sogar Lösegeldzahlungen geleistet. Dies zeigt, dass Cyberkriminalität längst nicht mehr nur ein technisches Problem ist, sondern zunehmend zu einer betriebswirtschaftlichen und strategischen Herausforderung wird.

Die Ergebnisse machen deutlich: Auch wenn nur eine Minderheit der KMU direkt betroffen ist, können die Folgen eines erfolgreichen Angriffs erheblich sein. Entscheidend ist daher nicht die Frage, ob ein Unternehmen gross oder klein ist, sondern wie gut es auf unterschiedliche Angriffsszenarien vorbereitet und gegen finanzielle Schäden abgesichert ist.

Angriffsart
Frage: Welche Art von Angriff haben Sie erlitten? (Filter: Wenn Cyberangriff erlitten)



Erpressung
Frage: Wurde Ihr Unternehmen schon einmal von Cyberkriminellen erpresst? (Antwort: Ja)



05 Kenntnis Cyberbedrohungslage und Unterstützung

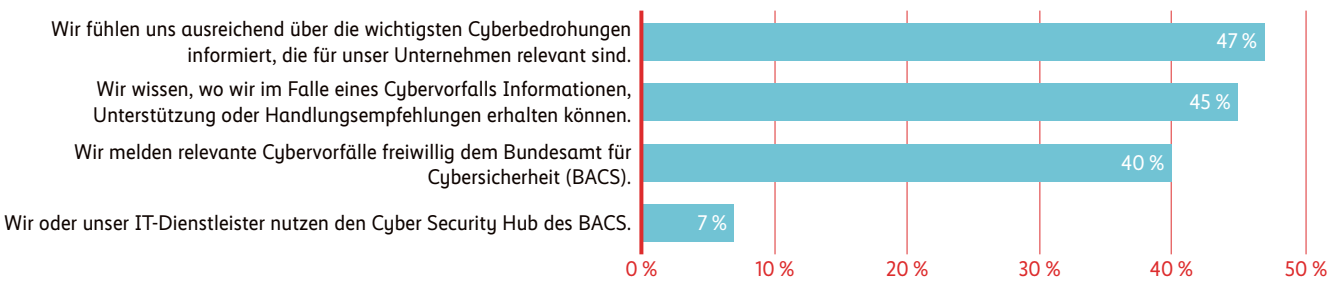
Die aktuelle Befragung zeigt, dass sich viele Schweizer KMU im Umgang mit Cyberrisiken grundsätzlich gut aufgestellt fühlen. ***Fast die Hälfte der Unternehmen gibt an, ausreichend über die wichtigsten Cyberbedrohungen informiert zu sein, die für das eigene Geschäft relevant sind.*** Ebenso wissen viele Befragte nach eigener Einschätzung, wo sie im Ernstfall Informationen, Unterstützung oder konkrete Handlungsempfehlungen erhalten können.

Erfreulich ist auch, dass ***40 % der Unternehmen bereit wären, relevante Cybervorfälle freiwillig dem Bundesamt für Cybersicherheit (BACS) zu melden.*** Das Bewusstsein für die Bedeutung des Informationsaustauschs und der Zusammenarbeit scheint damit grundsätzlich vorhanden zu sein.

Die Studie zeigt, dass bei der Nutzung des Cybersecurity Hub durch KMU noch weiteres Potenzial besteht, insbesondere bei sehr kleinen Unternehmen. So wird der Cybersecurity Hub des BACS erst von rund sieben Prozent der Unternehmen beziehungsweise deren IT-Dienstleistern genutzt. Der Cybersecurity Hub richtet sich in erster Linie an Betreiber kritischer Infrastrukturen sowie an deren Dienstleister. KMU können sich jedoch ebenfalls anschliessen und das Angebot nutzen.



Kenntnis Cyberbedrohungslage und Unterstützung
Frage: Wie sehr stimmen Sie den folgenden Aussagen zu oder nicht zu?
Skala: 1 (trifft gar nicht zu) bis 5 (trifft voll und ganz zu). Dargestellte Resultate: Skala 4–5 (voll und ganz)



Auffällig ist zudem, dass ***grössere KMU ihre Unterstützungsmöglichkeiten besser kennen als kleinere Unternehmen.*** Unternehmen mit 10 bis 49 Mitarbeitenden verfügen signifikant häufiger über konkrete Kenntnisse, an wen sie sich im Cybernotfall wenden können und nutzen auch Angebote wie den Cybersecurity Hub signifikant häufiger. Kleinere Unternehmen verlassen sich vermutlich stärker auf ihr allgemeines Wissen oder auf externe Partner.

Grössere KMU kennen ihre Unterstützungsmöglichkeiten besser als kleinere Unternehmen.

Die Ergebnisse deuten darauf hin, dass viele KMU ihre Cyberresilienz eher aus der Perspektive des persönlichen Wissens beurteilen. Die organisatorische Vorbereitung auf einen Cybervorfall ist jedoch teilweise weniger weit fortgeschritten. ***Gerade hier können Notfallkonzepte, definierte Prozesse und die Nutzung spezialisierter Unterstützungsangebote einen wichtigen Unterschied machen, wenn es tatsächlich zu einem Vorfall kommt.***

Viele KMU fühlen sich informiert und wissen nach eigener Einschätzung, wohin sie sich wenden können. Gleichzeitig fehlen häufig Sicherheitskonzepte, Notfallpläne und Audits. Die Ergebnisse deuten damit auf eine Lücke zwischen wahrgenommener und organisatorisch verankerter Cyberresilienz hin.

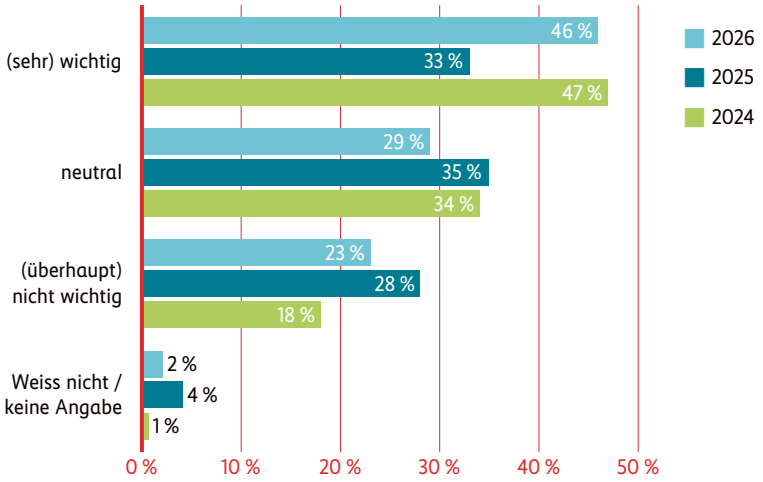
06 Cybersicherheit wird wichtiger und gewinnt wieder an Bedeutung

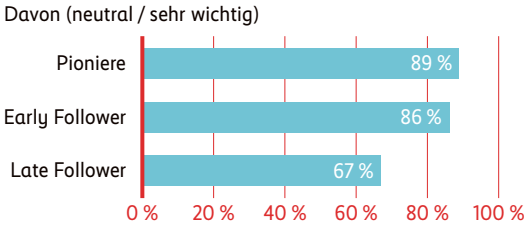
Nach einem Rückgang im Vorjahr erlebt das Thema Cybersicherheit bei Schweizer KMU wieder eine viel höhere Priorität. 2026 stufen 46 Prozent der befragten Unternehmen Cybersicherheit als wichtig oder sehr wichtig ein. Im Vorjahr waren es noch 33 Prozent. ***Damit kehrt das Thema wieder auf das Niveau früherer Jahre zurück.***

Besonders stark ausgeprägt ist diese Entwicklung bei Unternehmen ab 10 Mitarbeitenden. ***In dieser Gruppe messen rund sechs von zehn Unternehmen der Cybersicherheit eine hohe Priorität bei.*** Auch technologisch fortschrittliche Unternehmen, die als Pioniere oder Early Follower gelten, gewichten das Thema Cybersicherheit deutlich stärker als weniger technologieinnovative Betriebe (Late Follower).

Die Wahrnehmung der Cyberrisiken nimmt mit der Unternehmensgrösse zu.

Priorität Cybersicherheit
Frage: Welche Priorität hat in Ihrer Firma das Thema Cybersicherheit?
Skala: 1–2: (überhaupt) nicht wichtig / 3: neutral / 4–5: (sehr) wichtig





Die steigende Aufmerksamkeit kommt nicht von ungefähr. Die aktuelle Studie zeigt, dass Cyberkriminalität heute zu den wichtigsten strategischen Risiken für Schweizer KMU zählt. Mit 23 Prozent der Nennungen liegt sie praktisch gleichauf mit Inflation und Kostensteigerungen sowie Fachkräftemangel. Nur die weltpolitischen und weltwirtschaftlichen Unsicherheiten werden noch etwas häufiger als langfristiges Risiko genannt.

Besonders bemerkenswert ist, dass die Wahrnehmung der Cyberrisiken mit der Unternehmensgrösse zunimmt. Bei Unternehmen mit 20 bis 49 Mitarbeitenden zählt bereits mehr als ein Drittel Cyberkriminalität zu den grössten strategischen Risiken. Damit rangiert das Thema in dieser Unternehmensgruppe noch deutlich weiter oben auf der Risikoliste.

Die Ergebnisse zeigen insgesamt ein klares Bild: Schweizer KMU erkennen zunehmend, dass Cybersicherheit nicht nur eine technische Frage für die IT ist, sondern ein strategisches Geschäftsthema. Angesichts wachsender digitaler Abhängigkeiten, neuer Bedrohungen und professioneller Cyberkrimineller rückt der Schutz von Daten, Prozessen und Geschäftsbeziehungen wieder stärker in den Mittelpunkt der Unternehmensführung.



07 Cyberrisk-Verantwortung: Immer mehr KMU regeln Zuständigkeiten

Die aktuelle Studie zeigt einen positiven Trend: ***Schweizer KMU weisen dem Thema Cybersicherheit zunehmend klare Verantwortlichkeiten zu***. Während Cyberrisiken früher oft nebenbei behandelt wurden, wird heute häufiger festgelegt, wer sich im Unternehmen mit diesem Thema beschäftigt.

Besonders stark gewachsen ist der Anteil der Unternehmen, die die Verantwortung für Cybersicherheit einer Person ***als Teilaufgabe*** übertragen. Dieser Wert stieg innerhalb eines Jahres signifikant von 15 auf 21 Prozent. ***Gleichzeitig verfügt mittlerweile fast jedes zehnte KMU sogar über eine spezielle Funktion mit klar definierten Zuständigkeiten für Cybersicherheit.***

Viele Unternehmen setzen zudem auf externe Unterstützung. Mehr als ein Viertel der befragten KMU arbeitet beim Thema Cyberrisiken mit einem externen Partner zusammen. Gerade für kleinere Unternehmen kann dies eine effiziente Möglichkeit sein, fehlende interne Ressourcen oder Fachkenntnisse zu ergänzen.

Die grösste Veränderung zeigt sich jedoch bei den Unternehmen, die dem Thema bisher kaum Aufmerksamkeit geschenkt haben. Der Anteil der KMU, für die Cyberrisiken keine Priorität darstellen, ist von 42 Prozent im Vorjahr auf 36 Prozent gesunken. Auch bei Kleinstunternehmen mit nur ein bis drei Mitarbeitenden ist dieser Rückgang sichtbar. ***Dies deutet darauf hin, dass das Bewusstsein für Cyberrisiken zunehmend auch die kleinsten Unternehmen erreicht.***

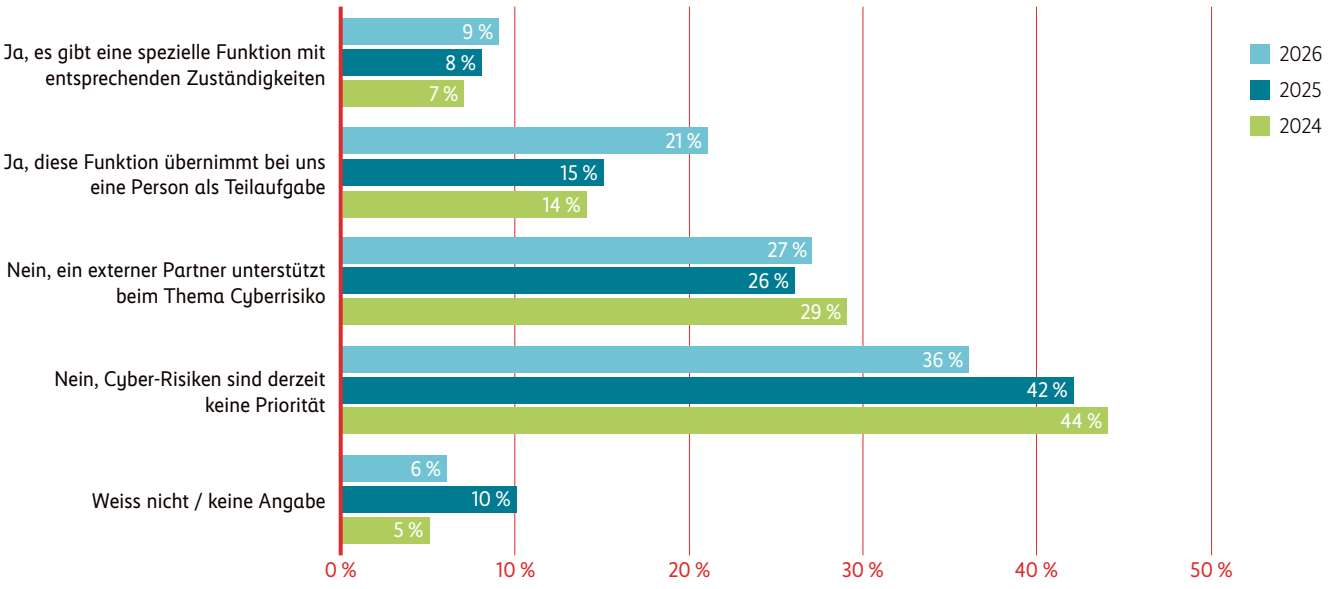
Viele Unternehmen setzen auf externe Unterstützung.



Auffällig sind die Unterschiede nach Unternehmensgrösse: Bei Unternehmen mit 10 oder mehr Mitarbeitenden sind Zuständigkeiten deutlich häufiger geregelt, sei es intern oder mit Unterstützung externer Spezialisten. Gleichzeitig betrachten diese Unternehmen Cyberrisiken wesentlich seltener als «kein prioritäres Thema».

Die Ergebnisse zeigen insgesamt, dass Cybersicherheit in Schweizer KMU zunehmend von einer technischen Einzelaufgabe zu einer Managementaufgabe wird. Die wichtigste Erkenntnis lautet dabei: Nicht jedes KMU benötigt eine speziell für Cybersecurity verantwortliche Person. Entscheidend ist vielmehr, dass klar geregelt ist, wer im Unternehmen Verantwortung übernimmt und wer im Ernstfall handelt.

Cyberrisk-Verantwortung
Frage: Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für Cybersicherheit zuständig ist?



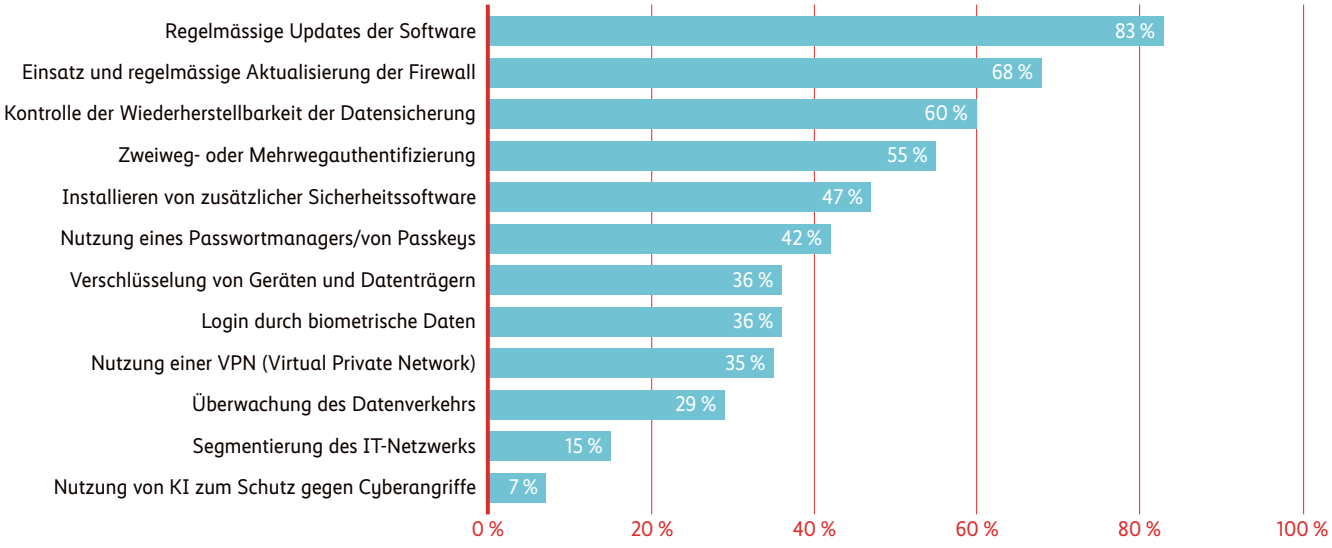
08 Umsetzung technischer Cybersicherheitsmassnahmen

Die Schweizer KMU investieren weiterhin vor allem in bewährte technische Schutzmassnahmen. Am weitesten verbreitet sind regelmässige Software-Updates: Über 80 Prozent der Unternehmen setzen diese konsequent um. Ebenfalls weit verbreitet sind Firewalls, Datensicherungen und die Zweiweg- beziehungsweise Mehrfaktorauthentifizierung (MFA). Diese Massnahmen bilden heute das Fundament der Cybersicherheit in den meisten KMU.

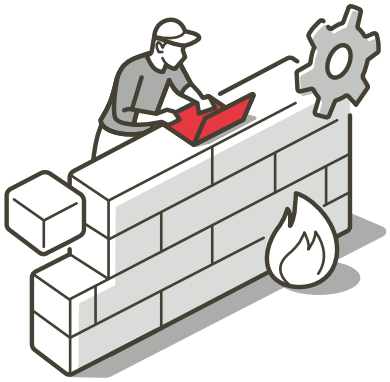
Deutlich seltener kommen dagegen fortgeschrittene Schutzmechanismen zum Einsatz. Dazu gehören etwa die Überwachung des Datenverkehrs, die Segmentierung von Netzwerken oder der Einsatz von KI zum Schutz gegen Cyberangriffe. Gerade bei diesen Themen zeigt sich eine grosse Kluft zwischen technologischen Vorreitern und Nachzüglern. Während innovative Unternehmen solche Massnahmen zunehmend einsetzen, verlassen sich viele andere KMU weiterhin auf die klassischen Basismassnahmen.

Ein besonders erfreuliches Ergebnis betrifft das Thema Backup: ***Neun von zehn Schweizer KMU führen heute regelmässige Datensicherungen durch.*** Der Anteil der Unternehmen ohne regelmässiges Backup ist auf lediglich vier Prozent gesunken. Zudem setzen immer mehr Unternehmen auf eine Kombination aus lokaler Datensicherung und Cloud-Backup. Diese Kombination erhöht die Ausfallsicherheit und reduziert das Risiko eines vollständigen Datenverlusts.

Technische Cybersicherheitsmassnahmen
Frage: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Skala: 1–2: (gar) nicht / 3–5: neutral / 6–7: (voll und) ganz. Dargestellte Resultate: Skala 6–7 (voll und ganz umgesetzt)



Interessant ist auch der Speicherort der Sicherungen. ***Rund drei Viertel der Unternehmen mit Backup speichern ihre Daten in der Schweiz.*** Nur wenige lagern ihre Backups ausserhalb Europas. Das zeigt, dass Datensouveränität und die Kontrolle über sensible Unternehmensdaten für viele KMU eine wichtige Rolle spielen.



Die grösste Schwachstelle zeigt sich jedoch an einem anderen Punkt: Ein Backup ist nur dann wertvoll, wenn es im Ernstfall auch tatsächlich funktioniert. Obwohl regelmässige Datensicherungen heute Standard sind, ***testen lediglich ein Viertel der KMU regelmässig das Zurückspielen ihrer Backups.*** Damit bleibt für viele Unternehmen unklar, ob ihre Daten nach einem Cyberangriff, einem technischen Defekt oder einer Fehlbedienung tatsächlich wiederhergestellt werden könnten.

Neun von zehn Schweizer KMU führen heute regelmässige Datensicherungen durch.

Die Ergebnisse zeigen insgesamt: Viele KMU verfügen über technische Basismassnahmen. Bei Zugriffsschutz, Überwachung, Segmentierung und getesteter Wiederherstellung bestehen jedoch weiterhin Lücken. Besonders beim Thema Backup wurden in den vergangenen Jahren wichtige Fortschritte erzielt. Die nächste Herausforderung besteht jedoch darin, nicht nur Daten zu sichern, sondern die Wiederherstellung regelmässig zu testen. Denn im Ernstfall zählt nicht nur, ob ein Backup vorhanden ist, sondern ob es auch funktioniert.

09 Umsetzung organisatorischer Cybersicherheitsmassnahmen



Die aktuelle Studie zeigt, dass Schweizer KMU bei der Cybersicherheit vor allem auf technische Schutzmassnahmen setzen. ***Organisatorische Massnahmen sind dagegen deutlich weniger verbreitet.*** Am häufigsten umgesetzt werden grundlegende Verhaltensregeln wie der sorgfältige Umgang mit persönlichen Informationen, die Nutzung sicherer Passwörter und die Prüfung von verdächtigen Dokumenten oder E-Mails. Diese Massnahmen sind heute bei einer grossen Mehrheit der Unternehmen etabliert.

Sobald es jedoch um übergeordnete Prozesse und Strukturen geht, sinken die Umsetzungsgrade deutlich. ***Nur rund ein Drittel der KMU inventarisiert systematisch seine IT-Systeme und Cloud-Dienste oder führt regelmässige Mitarbeiterschulungen durch.*** Noch weniger verbreitet sind Notfallpläne für die Geschäftsfortführung, die Bewertung der IT-Sicherheit von Lieferanten, formelle Sicherheitskonzepte oder die Klassifizierung von Daten nach ihrem Schutzbedarf. ***Am seltensten werden Sicherheitsaudits durchgeführt.***

Besonders auffällig ist der Einfluss der Unternehmensgrösse. Während die grundlegenden Verhaltensregeln in kleinen und grossen KMU ähnlich gut verankert sind, steigt die Professionalisierung mit zunehmender Mitarbeiterzahl deutlich an. Unternehmen mit 10 bis 49 Mitarbeitenden verfügen wesentlich häufiger über Notfallkonzepte, IT-Sicherheitssupport, Sicherheitsrichtlinien und regelmässige Audits als Kleinstunternehmen.

Ein weiterer spannender Zusammenhang betrifft das Wissen über Cybersicherheit. Unternehmen, die sich gut über Cyberrisiken informiert fühlen, setzen organisatorische Schutzmassnahmen

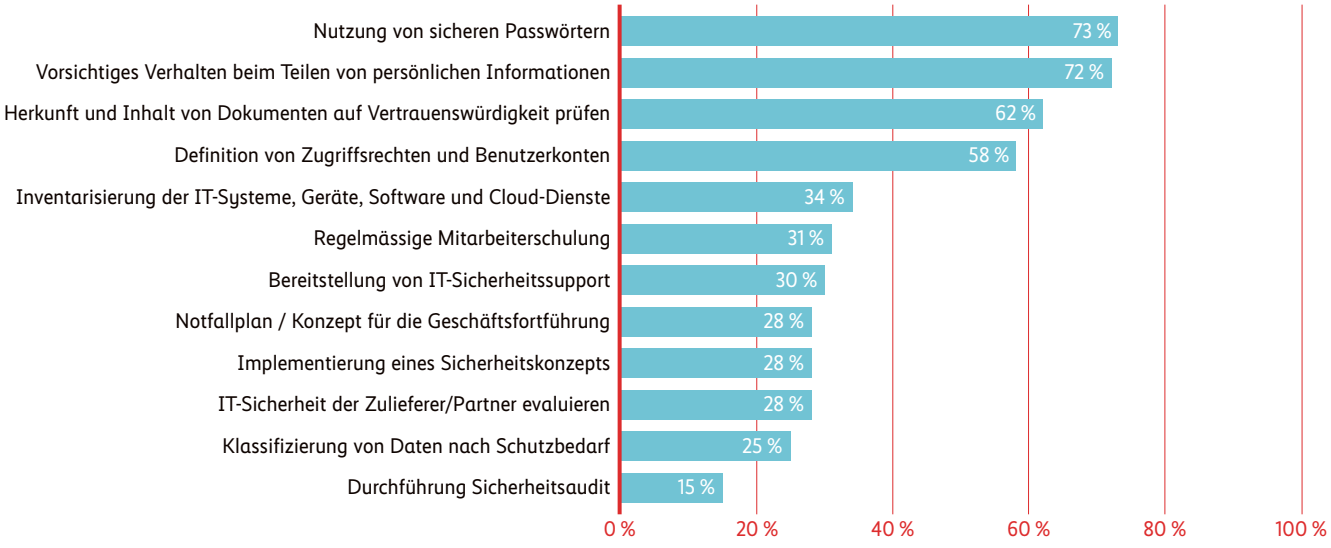
Nur rund ein Drittel der KMU inventarisiert systematisch seine IT-Systeme und Cloud-Dienste oder führt regelmässige Mitarbeiterschulungen durch.

signifikant deutlich häufiger um als weniger gut informierte Betriebe. Das gilt nahezu für alle untersuchten Bereiche, von Mitarbeiterschulungen über Notfallpläne bis hin zu Sicherheitskonzepten. Einzige Ausnahme bilden die Sicherheitsaudits und die Klassifizierung der schützenswerten Daten. Mit höherem Informationsgrad gehen folglich höhere Umsetzungsgrade organisatorischer Schutzmassnahmen einher.

Auch die Innovationskultur spielt eine wichtige Rolle. Technologieoffene Unternehmen und sogenannte Early Follower weisen deutlich höhere Umsetzungsgrade auf als Late Follower. Letztere verfügen wesentlich seltener über strukturierte Sicherheitsprozesse und erreichen überdurchschnittlich oft tiefe Werte bei den organisatorischen Schutzmassnahmen.

Die Ergebnisse zeigen insgesamt ein klares Bild: Die meisten KMU wissen, wie man sich im Alltag vorsichtig verhält. ***Die eigentliche Herausforderung liegt jedoch darin, Cybersicherheit organisatorisch zu verankern.*** Notfallpläne, Schulungen, Lieferantenprüfungen und regelmässige Sicherheitsaudits sind oft weniger sichtbar als bspw. Firewalls, können im Ernstfall aber entscheidend dafür sein, wie schnell ein Unternehmen auf einen Cybervorfall reagieren und den Geschäftsbetrieb aufrechterhalten kann.

Organisatorische Cybersicherheitsmassnahmen
Frage: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Skala: 1–2: (gar) nicht / 3–5: neutral / 6–7: (voll und) ganz. Dargestellte Resultate: Skala 6–7 (voll und ganz umgesetzt)



10 Die Zukunft: Cyberresilienz wird wichtiger, aber viele KMU bleiben zurückhaltend

Die aktuelle Studie zeigt ein grundsätzlich positives Bild der Cyberresilienz in Schweizer KMU. Jedes zweite Unternehmen ist der Meinung, gut oder sehr gut gegen Cyberangriffe geschützt und auf einen Vorfall vorbereitet zu sein. Gegenüber dem Vorjahr ist diese Einschätzung sogar leicht gestiegen. Besonders selbstbewusst zeigen sich grössere Unternehmen sowie technologisch fortschrittliche Betriebe. ***Pioniere der Digitalisierung schätzen ihre Resilienz deutlich höher ein als Late Follower, die ihre Cyberresilienz wesentlich kritischer beurteilen.***

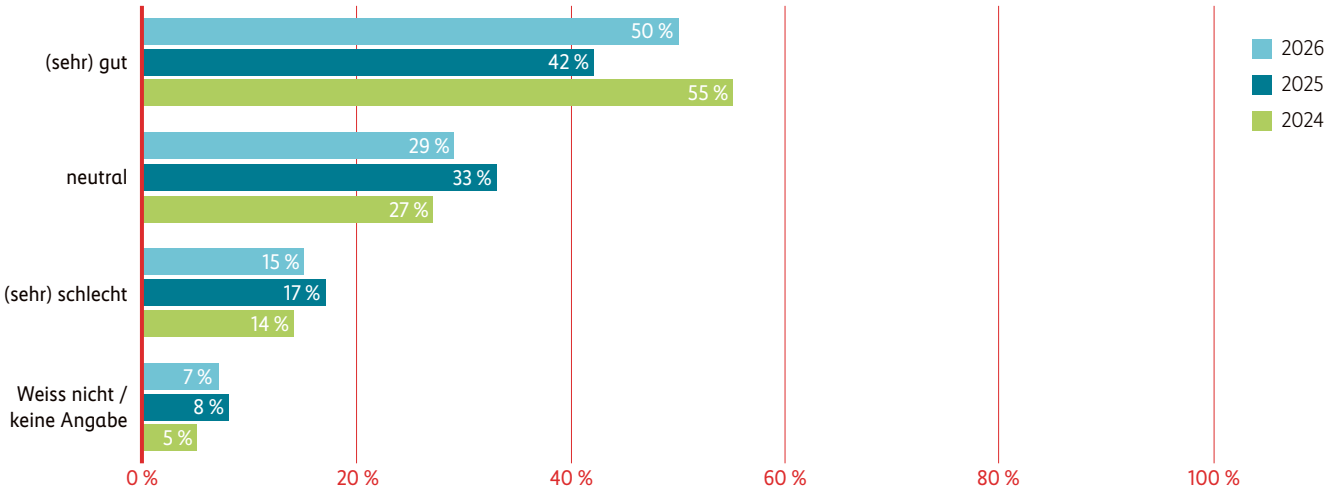
Gleichzeitig gewinnt das Thema Cybersicherheit wieder an strategischer Bedeutung. Nachdem die Priorität im Vorjahr gesunken war, betrachtet inzwischen fast jedes zweite KMU Cybersicherheit als wichtig oder sehr wichtig. Besonders Unternehmen mit mehr als zehn Mitarbeitenden haben das Thema wieder stärker auf die Agenda gesetzt.



Auch innovative Unternehmen messen der Cybersicherheit überdurchschnittlich hohe Bedeutung bei.

Spannend ist der Blick in die Zukunft: ***Rund zwei von fünf KMU halten zusätzliche Sicherheitsmassnahmen in den kommenden ein bis drei Jahren für (sehr) wahrscheinlich.*** Die Bereitschaft steigt mit der Unternehmensgrösse und dem Informationsgrad. Unternehmen, die sich gut über

Cyberresilienz
Frage: Was schätzen Sie: Wie gut sind Sie vor Cyberangriffen geschützt und auf einen Angriff vorbereitet?
Skala: 1–2: (sehr) schlecht / 3: neutral / 4–5: (sehr) gut



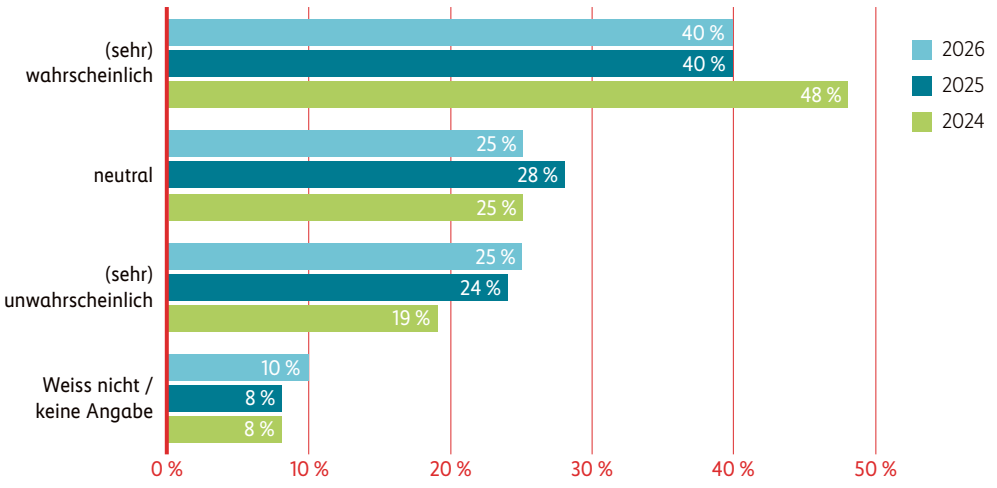
Cyberresilienz bedeutet nicht nur, Angriffe zu verhindern, sondern auch nach einem Vorfall rasch handlungsfähig zu bleiben.

Cybersicherheit informiert fühlen, planen deutlich häufiger weitere Investitionen als weniger gut informierte Betriebe.

Trotz des hohen Problembewusstseins zeigt sich jedoch ein gewisser Widerspruch. Zwar wird Cyberkriminalität in anderen Befragungsteilen klar als ernstzunehmende Bedrohung wahrgenommen, gleichzeitig schätzt eine Mehrheit der KMU das Risiko eines Cyberangriffs mit mindestens eintägigem Betriebsausfall in den nächsten zwei bis drei Jahren als eher klein ein. Nur rund jedes zehnte Unternehmen erwartet ein hohes Risiko. Erst bei grösseren KMU steigt diese Risikoeinschätzung deutlich an.

Die Ergebnisse deuten darauf hin, dass viele Unternehmen heute zwar mehr Vertrauen in ihre eigene Resilienz haben, gleichzeitig aber die Auswirkungen eines möglichen Vorfalls teilweise unterschätzen könnten. ***Cyberresilienz bedeutet nicht nur, Angriffe zu verhindern, sondern auch nach einem Vorfall rasch handlungsfähig zu bleiben.*** Gerade deshalb werden die kontinuierliche Verbesserung von Schutzmassnahmen, Notfallvorbereitungen und regelmässige Überprüfungen der eigenen Sicherheitslage in den kommenden Jahren weiter an Bedeutung gewinnen.

Erhöhung Cybersicherheitsmassnahmen
Frage: Wie wahrscheinlich ist es, dass Sie in den kommenden 1 bis 3 Jahren die Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden?
Skala: 1–2: (sehr) unwahrscheinlich / 3: neutral / 4–5: (sehr) wahrscheinlich



Umsetzung

Checkliste Cybersicherheit und Cyberresilienz für Schweizer KMU

Die Studienergebnisse zeigen: Viele KMU haben die technischen Grundlagen im Griff. Die grössten Verbesserungspotenziale liegen heute oft bei organisatorischen Massnahmen, Notfallvorbereitungen und der regelmässigen Überprüfung der Wirksamkeit bestehender Schutzmassnahmen. Diese Checkliste hilft Ihnen bei der Stärkung Ihrer Cyberresilienz.

Technische Cybersicherheitsmassnahmen

1. Grundlagen absichern

- ☐ Regelmässige Updates aller Betriebssysteme, Anwendungen und Geräte durchführen.
- ☐ Firewall einsetzen und laufend aktualisieren.
- ☐ Mehrfaktor-Authentifizierung (MFA) für E-Mail, Cloud-Dienste und kritische Systeme aktivieren.
- ☐ Zusätzliche Sicherheitssoftware (ERD / Endpoint Protection, Antivirus) einsetzen.
- ☐ Passwortmanager oder Passkeys verwenden.

2. Daten schützen

- ☐ Regelmässige Datensicherungen (Backups) erstellen.
- ☐ Backups lokal und in der Cloud speichern.
- ☐ Sicherstellen, dass Backups möglichst auch in der Schweiz gespeichert werden.
- ☐ Die Wiederherstellung von Backups regelmässig testen. Nur ein zurückspielbares Backup schützt im Ernstfall.
- ☐ Geräte, Datenträger und sensible Daten verschlüsseln.

3. Infrastruktur absichern

- ☐ VPN-Lösungen für externe Zugriffe einsetzen.
- ☐ Biometrische Login-Verfahren dort einsetzen, wo sie sinnvoll sind.
- ☐ Datenverkehr und verdächtige Aktivitäten überwachen.
- ☐ Kritische Systeme durch Netzwerksegmentierung voneinander trennen.
- ☐ Potenzial von KI-basierten Schutzlösungen prüfen.

Organisatorische Cybersicherheitsmassnahmen

1. Mitarbeitende sensibilisieren

- ☐ Klare Regeln zum Umgang mit persönlichen und vertraulichen Informationen festlegen.
- ☐ Sichere Passwortregeln verbindlich einführen.
- ☐ E-Mails, Links und Dokumente auf Vertrauenswürdigkeit prüfen.
- ☐ Mitarbeitende regelmässig zu Cyberrisiken schulen.

2. Strukturen und Verantwortlichkeiten schaffen

- ☐ Verantwortlichkeiten für Cybersicherheit eindeutig festlegen.
- ☐ Zugriffsrechte und Benutzerkonten systematisch verwalten.
- ☐ Alle IT-Systeme, Geräte, Softwarepakete und Cloud-Dienste inventarisieren.
- ☐ Internen oder externen IT-Sicherheitssupport organisieren.
- ☐ Sicherheitskonzept für das Unternehmen dokumentieren.

3. Resilienz erhöhen

- ☐ Notfallplan und Konzept für die Geschäftsfortführung erstellen.
- ☐ Zuständigkeiten für den Krisenfall definieren.
- ☐ Wissen, wo im Ernstfall Unterstützung verfügbar ist (IT-Dienstleister, Versicherer, Bundesamt für Cybersicherheit (BACS)).
- ☐ Relevante Cybervorfälle an das Bundesamt für Cybersicherheit (BACS) melden.

4. Risiken regelmässig überprüfen

- ☐ IT-Sicherheit von Lieferanten und Geschäftspartnern bewerten.
- ☐ Daten nach Schutzbedarf klassifizieren.
- ☐ Regelmässige Sicherheitsaudits durchführen.
- ☐ Digitale Abhängigkeiten von einzelnen Anbietern, Plattformen oder Cloud-Diensten überprüfen.

Cyberresilienz bedeutet nicht nur, Angriffe zu verhindern. Erfolgreiche Unternehmen wissen, wie sie einen Angriff erkennen, den Schaden begrenzen, den Betrieb rasch wiederherstellen und daraus lernen.

Praxistools zur Stärkung Ihrer Cybersicherheit

Cybertest für KMU

- Mit diesem Selbsteinschätzungstest finden Sie heraus, was Hacker an Ihnen mögen und erhalten auf Sie zugeschnittene Cybertipps.
  https://www.mobiliar.ch/kampagne/cybertest
- Ermitteln Sie mit IT Sec 4 KMU Ihren Cyberscore und erhalten konkrete Massnahmen zur Verbesserung Ihrer Cybersicherheit.
  https://itsec4kmu.ch/

Bundesamt für Cybersicherheit BACS

- Informationen für Unternehmen und Behörden zum Schutz und dem Vorgehen bei Cybervorfällen sowie zur Meldepflicht.
  https://www.bacs.admin.ch/de/infos-unternehmen-behoerden
- Informationen zum Cybersecurity Hub (CSH)
  https://www.bacs.admin.ch/de/informationen-zum-csh

Cybersecurity Map

- Die Cybersecurity Map bietet Entscheidungsträger:innen einen prägnanten Überblick über wichtige technologischen Entwicklungen
  https://www.satw.ch/de/cybersecurity/cybersecurity-map

Forschungsmethodik

Das Studienziel war die Erhebung der Einstellung von Schweizer KMU zu den Themen Cyberkriminalität, Cybersicherheit und Digitalisierung.

Im Zeitraum vom 24. Juni bis 10. Juli 2026 wurden 507 Interviews via Online-Fragebogen mit Geschäftsleitenden von KMU mit 1–49 Mitarbeitenden durchgeführt. Das Einladungsverfahren basiert auf dem YouGov Internet-Panel mit ca. 115 000 Mitgliedern.

Die Stichprobe wurde mittels Quoten nach Firmengrösse und Sprachregion disproportional erhoben und anschliessend proportional gewichtet.

Die durch die Stichprobe abgebildete Grundgesamtheit umfasst rund 614 400 Firmen mit 1 bis 49 Mitarbeitenden (BfS STATENT, 2025) in allen Landesteilen. Das Vertrauensintervall der Gesamtstichprobe liegt bei +/– 4.4 Prozentpunkten bei einer Sicherheit von 95 Prozent (50/50 Verteilung).

Die gewichtete Stichprobe bildet die Grundgesamtheit hinsichtlich Firmengrösse und Sprachregion strukturgleich ab.
Die Ergebnisse sind somit unter Berücksichtigung des Vertrauensintervalls auf die Grundgesamtheit extrapolierbar.

Kontakt YouGov:
Karin Mändli Lerch,
karin.maendlilerch@yougov.ch

Kontakt Autorinnen und Autoren



Marc K. Peter
Professor für Digital Business
HES-SO Valais-Wallis School of Management
marckurt.peter@hes-so.ch



Romain Geiser
Program Manager NCS
Bundesamt für Cybersicherheit
ncs@ncsc.admin.ch



Anu Anthamatten
Senior Project Manager
digitalswitzerland, Zürich
anu@digitalswitzerland.com



Léonard Marbe
Senior Marketing Manager
Die Mobiliar
leonard.marbe@mobiliar.ch



Dr. Anna V. Rozumowski
Dozentin und Studiengangleiterin
HWZ Hochschule für Wirtschaft Zürich
anna.rozumowski@fh-hwz.ch



Tobias Schlegel
Leiter Tech Intelligence
SATW Schweizerische Akademie
der Technischen Wissenschaften
tobias.schlegel@satw.ch



Karin Mändli Lerch
Senior Research Consultant
YouGov
karin.maendlilerch@yougov.ch

Marc K. Peter, Romain Geiser, Anu Anthamatten,
Karin Mändli Lerch, Léonard Marbe,
Dr. Anna V. Rozumowski und Tobias Schlegel:

KMU Cybersicherheit 2026
Eine Mobiliar Studie in Zusammenarbeit
mit BACS, digitalswitzerland, HES-SO,
HWZ und SATW

- Bundesamt für Cybersicherheit BACS
- Die Mobiliar
- digitalswitzerland
- HES-SO Valais-Wallis School of Management
- HWZ Hochschule für Wirtschaft Zürich
- SATW Schweizerische Akademie
  der Technischen Wissenschaften
- YouGov

cyberstudie.ch
Bern und Zürich, Oktober 2026

Impressum

Marc K. Peter, Romain Geiser, Anu Anthamatten, Karin Mändli Lerch, Léonard Marbe,
Dr. Anna V. Rozumowski und Tobias Schlegel:

KMU Cybersicherheit 2026:
Eine Mobiliar Studie in Zusammenarbeit mit BACS, digitalswitzerland, HES-SO, HWZ und SATW

Bundesamt für Cybersicherheit BACS, Die Mobiliar, digitalswitzerland, HES-SO Valais-Wallis School of Management, HWZ Hochschule für Wirtschaft Zürich, SATW Schweizerische Akademie der Technischen Wissenschaften, YouGov
Bern und Zürich, Oktober 2026

Dieses Werk wurde sorgfältig erarbeitet. Dennoch übernehmen Autor:innen und die beteiligten Forschungspartner:innen in keinem Fall, einschliesslich des vorliegenden Werkes, irgendeine Haftung für die Richtigkeit von Angaben, Hinweisen und Ratschlägen sowie für eventuelle Druckfehler.

Alle Rechte, auch die Übersetzung in andere Sprachen, vorbehalten.
Die Rechte der genannten Marken liegen bei ihren entsprechenden Eigentümern.

Kein Teil dieses Werkes darf ohne schriftliche Genehmigung der Autor:innen in irgendeiner Form reproduziert oder in eine von Maschinen, insbesondere von Datenverarbeitungsmaschinen, verwendbare Sprache übertragen und/oder übersetzt werden.

Koordination dieser Publikation: Prof. Dr. Marc K. Peter,
HES-SO Valais-Wallis School of Management

Unter Mitarbeit von Thomas Burkhardt (YouGov), Michèle C. Kaufmann (YouGov), Kenza Leclere (BACS), Bettina Mavrommatis (BACS) und David Torcasso (digitalswitzerland).

Gestaltung: Team Mediengestaltung, die Mobiliar
Illustration: Livia Lüthi

Der Foliensatz mit allen Umfrageresultaten kann auf den Websites der Studienpartner:innen oder auf cyberstudie.ch bezogen werden.

2270609 09.26