

## Medienmitteilung

Zürich, 20. August 2026

### Schweizer KMU unterschätzen Cyberrisiken massiv: Grundschutz und Versicherungsschutz bleiben lückenhaft

Cyberangriffe werden durch KI schneller und skalierbarer. Gleichzeitig sind viele Schweizer KMU unzureichend geschützt und unterversichert. [Das zeigt eine repräsentative Befragung von Deloitte bei Mitarbeitenden von Schweizer KMU](#): Demnach unterschätzen viele Firmen die Risiken und setzen grundlegende Schutzmassnahmen nicht konsequent um. Zudem verfügen vor allem kleine Unternehmen noch zu selten über Cyberversicherungen.

Die Cyberbedrohungslage für Schweizer Unternehmen verschärft sich deutlich. Cyberangriffe nehmen stark zu und werden durch künstliche Intelligenz (KI) gezielter und wirkungsvoller. Besonders verwundbar sind kleine und mittlere Unternehmen (KMU): Sie verfügen häufig über weniger Ressourcen, unterschätzen ihr Risiko, setzen weniger Cybersicherheitsmassnahmen um und sind auch beim Versicherungsschutz schlechter aufgestellt. Das zeigt eine Studie des Prüfungs- und Beratungsunternehmens Deloitte zur Cybersicherheit von Schweizer KMU.

Die Ergebnisse zeigen eine deutliche Wahrnehmungslücke zwischen erlebter Bedrohung und Risikowahrnehmung (siehe Abbildung 1): 49 Prozent der befragten KMU-Mitarbeitenden haben in den letzten drei Monaten einen ernstesten Cybervorfall bei ihrem Arbeitgeber erlebt, aber nur 22 Prozent schätzen das Cyberrisiko ihres Unternehmens als hoch ein. Besonders ausgeprägt ist diese Wahrnehmungslücke bei Mikrounternehmen mit ein bis neun Mitarbeitenden: Dort berichten zwar 38 Prozent von ernstesten Cybervorfällen, aber nur 15 Prozent bewerten das Risiko eines Cyberangriffs als hoch.

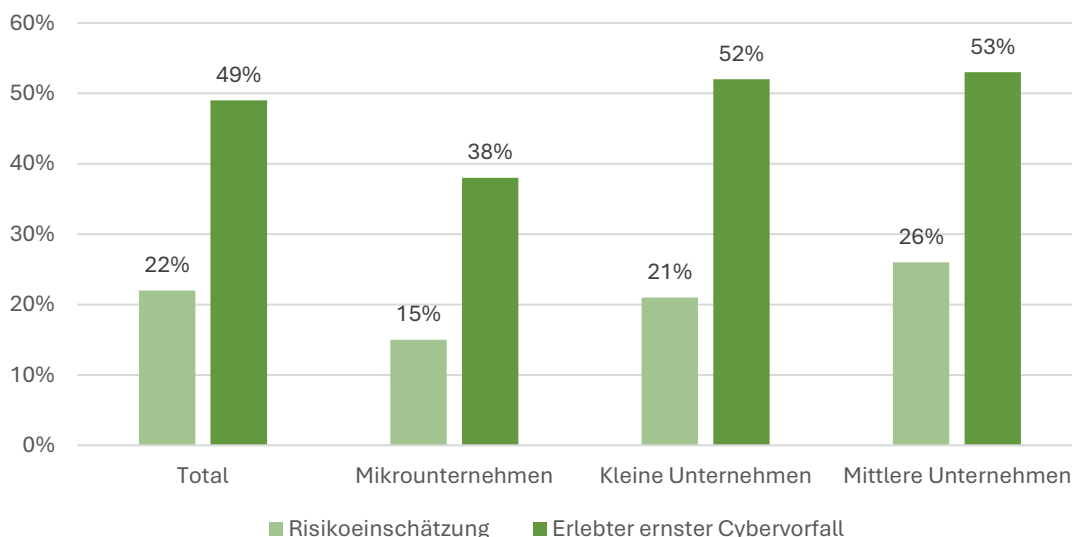


Abbildung 1: Anteil der Befragten mit einer sehr hohen oder hohen Einschätzung des Cyberrisikos sowie Anteil der Befragten, die in den letzten drei Monaten einen ernstesten Cybervorfall bei ihrem Arbeitgeber erlebt haben.

#### Phishing trifft Unternehmen jeder Grösse

Phishing, also der Versuch, über vorgetäuschte Nachrichten Daten zu stehlen oder Zahlungen auszulösen, ist mit 25 Prozent die am häufigsten wahrgenommene Cyberbedrohung. Auffällig ist,

dass Phishing bei Mikrounternehmen fast ebenso häufig vorkommt wie bei KMU allgemein. Das zeigt: Auch sehr kleine Unternehmen sind Cyberrisiken ausgesetzt. Ebenfalls werden Schadsoftware (Malware), CEO-Fraud, Identitätsdiebstahl, Verdacht auf Datenabfluss und Betriebsstörungen von Mitarbeitenden wahrgenommen und betreffen Unternehmen jeder Grösse.

«Viele KMU unterschätzen, wie stark sich Cyberangriffe verändert haben. Angriffe sind heute skalierbar, automatisiert und treffen Unternehmen jeder Grösse. Gerade Phishing, kompromittierte Zugangsdaten oder manipulierte Zahlungsprozesse können auch kleine Unternehmen empfindlich treffen», sagt Florian Widmer, Partner Cyber bei Deloitte Schweiz. «Die Fähigkeit einer Organisation, Cyberangriffen zu widerstehen, beginnt deshalb mit den Grundlagen: Es braucht unter anderem starke Authentifizierung, restriktive Zugriffsrechte, regelmässige Schulungen, getestete Back-ups sowie einen robusten Notfallplan.»

### Grundlegende Sicherheitsmassnahmen noch nicht Standard

Der erstmals auf Basis der Studie erstellte KMU-Cybersicherheitsindex von Deloitte misst die Verbreitung von sechs grundlegenden mitarbeiterbezogenen Sicherheitsmassnahmen und liegt bei 58 von 100 Punkten (siehe Abbildung 2). Das bedeutet: Im Durchschnitt sind die abgefragten Sicherheitsmassnahmen nur zu 58 Prozent umgesetzt, was eine deutliche Lücke bei elementaren Schutzmassnahmen aufzeigt.

Besonders gross sind die Lücken bei modernen Authentifizierungsmethoden. Die passwortlose Authentifizierung, etwa biometrische Verfahren, haben nur 45 Prozent der Unternehmen eingeführt. Multi-Faktor-Authentifizierung ist mit 66 Prozent zwar häufiger anzutreffen, aber ebenfalls noch lange nicht flächendeckend etabliert. Gleichzeitig werden Massnahmen, wenn sie vorhanden sind, von Mitarbeitenden als wirksam wahrgenommen: 88 Prozent der Befragten, deren Unternehmen E-Mail-Warnhinweise einsetzen, bewerten diese als hilfreich. Die Befragung misst damit die Wahrnehmung der Mitarbeitenden, nicht die tatsächliche Wirksamkeit. Zugleich zeigt sie, dass solche Warnhinweise noch nicht von allen Unternehmen eingesetzt werden.

### Versicherungslücke bleibt gross

Neben der Risikowahrnehmung und der Umsetzung von Schutzmassnahmen zeigt die Studie von Deloitte eine dritte Lücke: den Versicherungsschutz. Die Verbreitung von Cyberversicherungen wächst in der Schweiz zwar, doch die Marktdurchdringung bleibt tief. Gemäss aktuellen Zahlen des Schweizerischen Versicherungsverbandes (SVV) sind 2025 rund 72'000 Firmenkundenpolicen abgeschlossen worden. Damit sind nur 11,5 Prozent der in der Schweiz domizilierten Unternehmen gegen Cyberrisiken versichert.

Die Versicherungslücke ist besonders bei Mikro- und kleinen Unternehmen ausgeprägt. Gerade sie können von Cybervorfällen besonders stark betroffen sein, weil Schäden relativ zum Umsatz schwerer wiegen können. Doch bei vielen KMU fehlen grundlegende Sicherheitsmassnahmen, die für den Abschluss einer Cyberversicherung erforderlich sind. Auch andere Faktoren erschweren den Zugang zu Cyberversicherungen, darunter komplexe Antragsprozesse und geringe Vertriebsanreize, da Provisionen für Cyberversicherungen für kleine Unternehmen oft gering sind.

**Deloitte KMU-Cybersicherheitsindex**

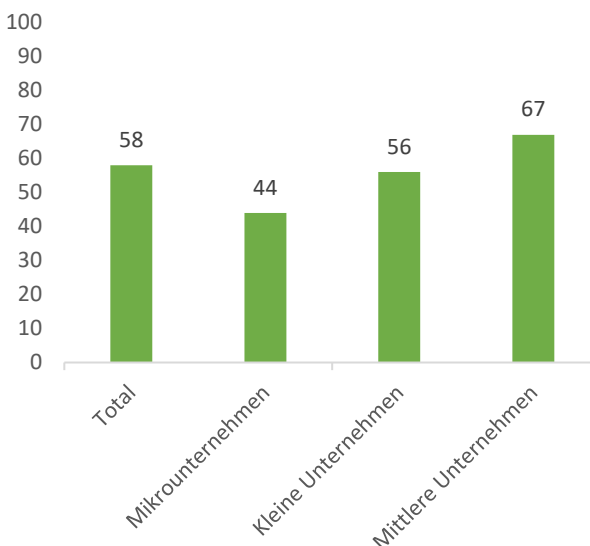


Abbildung 2: Ungewichteter Durchschnitt der Verbreitung von sechs Sicherheitsmassnahmen. Der Cybergrundschutz steigt mit der Unternehmensgrösse.

«Eine Cyberversicherung entfaltet ihren Nutzen für KMU nicht erst nach einem Angriff», sagt Marcel Thom, Partner und Leiter Versicherungen bei Deloitte Schweiz. «Ihr Mehrwert liegt in der Verbindung von Prävention, rascher Krisenhilfe und finanzieller Absicherung. Gerade kleinere Betriebe brauchen verständliche Produkte, transparente Anforderungen und einfache, digital unterstützte Abschlussprozesse. So kann die Cyberversicherung zu einem zentralen Baustein unternehmerischer Widerstandsfähigkeit werden.»

### **Mehr Verbindlichkeit, aber keine starre Regulierung**

Die Studie zeigt auch klare Erwartungen an die Rolle des Staates. 87 Prozent der Befragten unterstützen weitergehende Vorschriften zur Cybersicherheit. Gleichzeitig bevorzugen nur 19 Prozent strengere, rein staatliche Vorgaben mit Mindeststandards. Für die Schweiz ergibt sich daraus ein pragmatischer Handlungsauftrag: Der Bund sollte verständliche Mindeststandards setzen und die Zusammenarbeit zwischen Unternehmen, Branchenverbänden, Versicherern und IT-Dienstleistern erleichtern.

### **Über die Studie**

[Die von Deloitte durchgeführte Studie «Unterschätzt, ungeschützt, unterversichert: KMU-Cyberisiken in der Schweiz»](#) basiert auf einer repräsentativen Onlineumfrage von 924 Arbeitnehmenden, die für Schweizer Unternehmen mit bis zu 249 Mitarbeitenden tätig sind und beruflich am Computer arbeiten. Die Umfrage wurde im April 2026 durchgeführt. Ergänzend wurden im Juni und Juli 2026 Gespräche mit Cyberexpertinnen und Cyberexperten von Versicherungen geführt. Als KMU gelten gemäss Klassifizierung des Bundesamts für Statistik Unternehmen mit bis zu 249 Mitarbeitenden.

---

Kontakt: Michael Wiget  
Leiter Externe Kommunikation  
Tel.: +41 58 279 70 50  
E-Mail: [mwiget@deloitte.ch](mailto:mwiget@deloitte.ch)

Kontakt: Kevin Capellini  
Externe Kommunikation  
Tel.: +41 58 279 59 74  
E-Mail: [kcapellini@deloitte.ch](mailto:kcapellini@deloitte.ch)

---

### **[Deloitte Schweiz](#)**

Deloitte bietet integrierte Dienstleistungen in den Bereichen Audit & Assurance, Tax & Legal, Strategy, Risk & Transactions Advisory und Technology & Transformation. Mit rund 2'500 Mitarbeitenden an sechs Standorten in Basel, Bern, Genf, Lausanne, Lugano und Zürich (Hauptsitz) betreut Deloitte Unternehmen und Organisationen aller Rechtsformen und Grössen aus allen Branchen in der Schweiz.

Unsere Mitarbeitenden erzielen messbare und nachhaltige Ergebnisse, die dazu beitragen, das Vertrauen der Öffentlichkeit in die Kapitalmärkte zu stärken, und es unserer Kundschaft ermöglichen, sich weiterzuentwickeln und erfolgreich zu sein. Aufbauend auf ihrer über 180-jährigen Geschichte ist Deloitte in mehr als 150 Ländern und Gebieten vertreten und beschäftigt weltweit rund 470'000 Fachkräfte.

### **Hinweis für Redakteure**

«Deloitte» bezieht sich auf Deloitte Touche Tohmatsu Limited («DTTL»), ihr globales Netzwerk aus Mitgliedsunternehmen und verbundenen Unternehmen (zusammen die «Deloitte Organisation»). DTTL, ihre Mitglieds- und verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, ihre Mitglieds- und verbundenen Unternehmen haften ausschliesslich für ihre eigenen Handlungen und Unterlassungen. DTTL erbringt selbst keine Dienstleistungen gegenüber Kundinnen und Kunden. Weitere Informationen finden Sie unter [www.deloitte.com/about](http://www.deloitte.com/about).

Deloitte AG ist eine von der Eidgenössischen Revisionsaufsichtsbehörde (RAB) und der Eidgenössischen Finanzmarktaufsicht (FINMA) zugelassene und beaufsichtigte Revisionsgesellschaft.

Die Informationen in dieser Pressemitteilung waren zum Zeitpunkt der Veröffentlichung korrekt.



© 2026 Deloitte AG