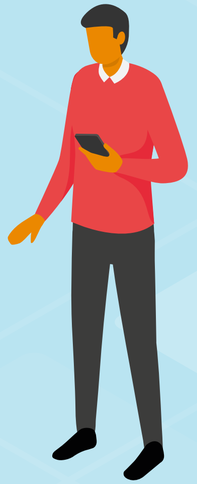
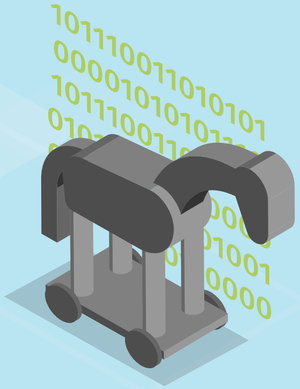
KMU Cybersicherheit 2025

IT-Sicherheit in Schweizer KMU und bei IT-Dienstleistungsunternehmen

Marc K. Peter, Martina Dalla Vecchia, Katja Dörlemann, Kristof A. Hertig, Andreas W. Kaelin, Manuel Kugler, Karin Mändli Lerch & Simon B. Seebeck

www.cyberstudie.ch





Quelle:
Marc K. Peter, Martina Dalla Vecchia, Katja Dörlemann, Kristof A. Hertig, Andreas W. Kaelin, Manuel Kugler, Karin Mändli Lerch & Simon B. Seebeck (2025): KMU Cybersicherheit 2025. IT-Sicherheit in Schweizer KMU und bei IT-Dienstleistungsunternehmen (www.cyberstudie.ch).

digitalswitzerland, Die Mobiliar, Schweizerische Akademie der Technischen Wissenschaften SATW, Information Security Society Switzerland ISSS, Swiss Internet Security Alliance SISA, Allianz Digitale Sicherheit Schweiz ADSS, Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz FHNW, HES-SO Valais-Wallis School of Management, YouGov Schweiz.

Forschungsbericht und Infografik in Deutsch, Englisch, Französisch und Italienisch können auf **www.cyberstudie.ch** bezogen werden.

digitalswitzerland · die Mobiliar · satw · /SSS information security society switzerland · SWISS INTERNET SECURITY ALLIANCE · ALLIANZ DIGITALE SICHERHEIT SCHWEIZ · n|w Fachhochschule Nordwestschweiz Hochschule für Wirtschaft · Hes·so VALAIS WALLIS School of Management · YouGov

KMU Cybersicherheit 2025

IT-Sicherheit in Schweizer KMU und bei IT-Dienstleistungsunternehmen

Cyber-Sicherheitsgefühl zu Cyberkriminalität

	Wir fühlen uns (sehr) sicher	Neutral	Wir fühlen uns (sehr) unsicher
Pioniere	58 %	39 %	–
Early Followers	51 %	37 %	10 %
Late Followers	52 %	37 %	6 %
Alle KMU	52 %	33 %	9 %
IT-Dienstleistungsunternehmen	65 %	22 %	10 %

Cyber-Resilienz: Schutz vor Cyberangriffen

	Wir sind (sehr) gut vorbereitet	Neutral	Wir sind (sehr) schlecht vorbereitet
Pioniere	48 %	50 %	–
Early Followers	55 %	33 %	11 %
Late Followers	32 %	36 %	24 %
Alle KMU	42 %	33 %	17 %
IT-Dienstleistungsunternehmen	68 %	24 %	7 %

Informationsgrad zur Cyber-Thematik

Mittelwert auf der Skala von
1 (sehr schlecht informiert) bis 5 (sehr gut informiert)

Pioniere	3.6
Early Followers	3.5
Late Followers	3.2
Alle KMU	3.3
IT-Dienstleistungsunternehmen	4.1

Erpresst durch Cyberkriminelle

Pioniere	–
Early Followers	3 %
Late Followers	6 %
Alle KMU	5 %
IT-Dienstleistungsunternehmen	4 %

Geldeinzahlungen aufgrund betrügerischer Mails

Pioniere	–
Early Followers	3 %
Late Followers	6 %
Alle KMU	4 %
IT-Dienstleistungsunternehmen	2 %

Risikoeinschätzung bezüglich Cyberangriffen

	(Sehr) hohes Risiko	Neutral	(Sehr) kleines Risiko
Pioniere	25 %	13 %	58 %
Early Followers	15 %	31 %	48 %
Late Followers	6 %	30 %	59 %
Alle KMU	10 %	28 %	54 %
IT-Dienstleistungsunternehmen	18 %	28 %	51 %

Cyberrisk-Verantwortung im Unternehmen

	Spezielle Funktion	Teilaufgabe einer Funktion	Externe Partner:in	Niemand/ keine Priorität
Pioniere	39 %	19 %	29 %	14 %
Early Followers	9 %	19 %	31 %	36 %
Late Followers	4 %	11 %	25 %	50 %
Alle KMU	8 %	15 %	26 %	42 %

Priorität der Cybersicherheit

	Ist (sehr) wichtig	Neutral	Ist (überhaupt) nicht wichtig
Pioniere	55 %	37 %	8 %
Early Followers	42 %	39 %	18 %
Late Followers	23 %	36 %	38 %
Alle KMU	33 %	35 %	28 %
IT-Dienstleistungsunternehmen	76 %	16 %	7 %

Planung zusätzlicher Cybersicherheits-Massnahmen

Mittelwert auf der Skala von
1 (stimme überhaupt nicht zu) bis 5 (stimme voll und ganz zu)

Pioniere	3.6
Early Followers	3.4
Late Followers	3.1
Alle KMU	3.2
IT-Dienstleistungsunternehmen	4.0

Technische Cybersicherheits-Massnahmen

Mittelwert auf der Skala von 1 (gar nicht) bis 5 (voll und ganz)

		Pioniere	Early Followers	Late Followers
Backup der Daten	87 %	–	–	–
Sicherung des WLAN-Netzwerks durch Passwörter	81 %	4.9	4.6	4.5
Regelmässiges Update der Software	81 %	4.9	4.6	4.2
Einsatz einer Firewall	68 %	4.7	4.2	4.0
Installieren von zusätzlich eingekaufter Software	62 %	4.4	4.1	3.7
Kontrolle Wiederherstellbarkeit der Datensicherung	61 %	4.6	4.1	3.7
Aktivieren von bereits vorhandener Sicherheitssoftware	55 %	4.0	3.9	3.6
Zweiweg- oder Mehrwegauthentifizierung (2FA/MFA)	53 %	4.2	3.7	3.4
Nutzung eines Passwortmanagers	42 %	4.5	3.4	2.8
Login durch biometrische Daten oder Passkeys	38 %	3.9	3.2	2.5
Nutzung von künstlicher Intelligenz (KI)	8 %	2.1	1.9	1.6

Organisatorische Cybersicherheits-Massnahmen

Mittelwert auf der Skala von 1 (gar nicht) bis 5 (voll und ganz)

		Pioniere	Early Followers	Late Followers
Nutzung von sicheren Passwörtern	74 %	4.5	4.2	4.0
Vorsichtiges Verhalten beim Teilen von persönlichen Informationen	70 %	4.4	4.2	3.9
Mitarbeitende auf Phishing-Mails sensibilisieren	67 %	4.6	4.3	3.7
Herkunft und Inhalt von Dokumenten prüfen	66 %	4.5	4.0	3.9
Bereitstellung von IT-Sicherheitssupport	36 %	4.2	3.4	2.7
Regelmässige Schulung der Mitarbeitenden	31 %	3.9	3.3	2.3
Notfallplan/Konzept für die Geschäftsfortführung	30 %	3.9	3.2	2.4
Implementierung eines Sicherheitskonzepts	30 %	4.0	3.2	2.5
IT-Sicherheit der Partner:innen evaluieren	30 %	3.5	2.9	2.5
Durchführung Sicherheitsaudit	20 %	3.3	2.5	2.0

Backup mit/ohne Cloud

Ja, mit einer Cloud-Lösung	18 %
Ja, lokal	39 %
Ja, lokal und mit einer Cloud-Lösung	30 %
Nein, kein regelmässiger Backup	9 %

Einstellung zu Cyberkriminalität

Cyberkriminalität ist ein ernstzunehmendes Problem	88 %
Massnahmen gegen Cyberattacken sind wichtig	83 %
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	80 %
Massnahmen gegen Cyberattacken sind effektiv und reduzieren die Gefahr	66 %
Massnahmen gegen Cyberattacken können einfach umgesetzt werden	37 %
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	29 %
Meine Kollegen denken, dass sich meine Firma vor Cyberattacken schützen sollte	24 %

Zusammenarbeit mit IT-Dienstleistungsunternehmen

Klarheit zu Sicherheitszertifizierungen

	Ja	Nein	Weiss nicht
Pioniere	67 %	6 %	27 %
Early Followers	37 %	15 %	48 %
Late Followers	37 %	12 %	51 %
Alle KMU	35 %	12 %	53 %

Cybersicherheits-Nachfrage in Zukunft: Herausforderungen für die Branche

(offene Frage, nachträglich codiert)

Schulung der Mitarbeitenden	22 %
Finanzielle Mittel / hohe Investitionen	22 %
Mangel an Fachpersonal	17 %
IT-Infrastruktur verbessern/updaten	12 %
Sensibilisierung IT-Sicherheit beim Kunden	12 %
Informationsbeschaffung generell	7 %
Komplexität der Angriffsmethoden erkennen	6 %
Benutzerfreundliche Anwendungen bereitstellen	5 %

Anzahl der externen IT-Dienstleistungspartner:innen

	Eine	Mehrere	Keine
Pioniere	37 %	27 %	35 %
Early Followers	34 %	24 %	38 %
Late Followers	45 %	23 %	30 %
Alle KMU	39 %	24 %	34 %

Auswahlkriterien für IT-Dienstleistungsunternehmen

	aus Sicht KMU	aus Sicht IT-Dienstleistungs-unternehmen
Gutes Preis-/Leistungsverhältnis	46 %	28 %
Guter (Kunden-)Service	43 %	37 %
Vertrauen ins IT-Dienstleistungsunternehmen	40 %	51 %
Erfahrung und Expertise	30 %	57 %
Flexibilität/Anpassung auf die Kundenbedürfnisse	23 %	24 %
Räumliche Nähe, Regionalität	21 %	12 %
Nachgewiesene Kenntnisse bezüglich Cybersicherheit	19 %	18 %
Empfehlung durch Kolleg:innen etc.	19 %	21 %
Guter Ruf des Dienstleistungsunternehmens	18 %	24 %
Breites/vielfältiges Angebot	7 %	3 %
Zertifizierungen, z. B. ISO 27001	5 %	10 %

Empfehlungen für höhere Cybersicherheit

Sicherheit ernst nehmen	36 %
Schulung der Mitarbeitenden	26 %
In IT investieren / Infrastruktur updaten	15 %
Finanzielle Ressourcen schaffen	13 %
Interne Prozesse kontrollieren	10 %
IT-Sicherheit allgemein erhöhen	7 %
Fachpersonal für IT-Sicherheit bereitstellen	6 %
Optimieren von Passwörtern / 2FA	5 %
Regelmässige Datensicherung	5 %

Quelle:
Marc K. Peter, Martina Dalla Vecchia, Katja Dörlemann, Kristof A. Hertig, Andreas W. Kaelin, Manuel Kugler, Karin Mändli Lerch & Simon B. Seebeck (2025): KMU Cybersicherheit 2025. IT-Sicherheit in Schweizer KMU und bei IT-Dienstleistungsunternehmen (www.cyberstudie.ch).

digitalswitzerland, Die Mobiliar, Schweizerische Akademie der Technischen Wissenschaften SATW, Information Security Society Switzerland ISSS, Swiss Internet Security Alliance SISA, Allianz Digitale Sicherheit Schweiz ADSS, Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz FHNW, HES-SO Valais-Wallis School of Management, YouGov Schweiz.

Forschungsbericht und Infografik in Deutsch, Englisch, Französisch und Italienisch können auf www.cyberstudie.ch bezogen werden.

KMU Cybersicherheit 2025

IT-Sicherheit in Schweizer KMU und bei IT-Dienstleistungsunternehmen

Cyberangriffe und die Einstellung der KMU-Geschäftsleitenden
Wie bereits 2024 gaben auch in diesem Jahr 4 % der befragten Unternehmen an, in den letzten drei Jahren Opfer eines Cyberangriffs geworden zu sein. 5 % der Firmen wurden bereits von Cyberkriminellen erpresst und 4 % haben aufgrund betrügerischer E-Mails versehentlich Geld überwiesen. Entsprechend sehen 88 % der Befragten (9/10 der befragten KMU) Cyberkriminalität als ernstzunehmendes Problem an. Dennoch verspüren nur 24 % einen sozialen Druck von Kolleg:innen, zusätzliche IT-Schutzmassnahmen zu ergreifen.

IT-Sicherheitsgefühl und Cyberresilienz nehmen ab
Das IT-Sicherheitsgefühl im Cyberraum nimmt ab: Während sich 2024 noch 57 % der Unternehmen sicher fühlten, sind es 2025 nur noch 52 %. Gleichzeitig steigt der Anteil derjenigen, die sich unsicher fühlen, von 7 % auf 9 %. Auch die Einschätzung der eigenen Cyberresilienz sinkt: Nur noch 42 % (2024: 55 %) halten ihren Schutz im Falle eines Angriffs für ausreichend, während 17 % (2024: 14 %) sich als schlecht geschützt einstufen.

Die Priorität von Cybersicherheit sinkt
Cybersicherheit verliert bei kleinen Schweizer Unternehmen an Bedeutung: Bei 28 % hat das Thema 2025 keine Priorität mehr (2024: 18 %). Bei grösseren Unternehmen mit 10–49 Mitarbeitenden sowie bei Technologiepionieren bleibt Cybersicherheit jedoch weiterhin bei vielen Firmen ein zentrales Anliegen.

Verantwortlichkeit für Cyberrisiken wird verstärkt wahrgenommen
Die Verantwortung für Cyberrisiken wird in kleinen Unternehmen zunehmend wahrgenommen. Inzwischen gibt es in 23 % der kleinen KMU eine Person oder Funktion, die sich zumindest teilweise um dieses Thema kümmert (2024: 21 %).

Organisatorische Schutzmassnahmen werden vernachlässigt
Technische Massnahmen wie Software-Updates, Firewalls und Datenwiederherstellungstests werden von ca. zwei Dritteln der Unternehmen umgesetzt. Bei organisatorischen Massnahmen besteht jedoch Nachholbedarf: Nur 20 % führen IT-Sicherheitsaudits durch und lediglich 30 % verfügen über ein IT-Sicherheitskonzept, schulen regelmässig ihre Mitarbeitenden oder haben einen Notfallplan.

Investitionsbereitschaft in Cybersicherheit sinkt
Nur noch 40 % der Unternehmen planen, ihre Cybersicherheitsmassnahmen in den nächsten 1–3 Jahren zu erhöhen – 2024 waren es noch 48 %.

IT-Dienstleistungsunternehmen sehen Nachholbedarf bei KMU
Auch die IT-Dienstleister sehen Nachholbedarf: Nur 39 % stufen ihre KMU-Kunden als sicher ein, während 14 % die Sicherheit ihrer Kunden als unzureichend bewerten (2024: 12 %). Zudem nimmt die Bedeutung von Cybersicherheit aus Sicht der IT-Unternehmen bei ihren Kunden etwas ab (2024: 46 %, 2025: 43 %). Positiv an der Situation ist: 84 % der IT-Dienstleister erwarten eine steigende Nachfrage nach Sicherheitsmassnahmen von ihren KMU-Kunden.

Studienmethodik
Die Cyberstudie hat zum Ziel, die Einstellung von Schweizer KMU und IT-Dienstleistungsunternehmen zum Thema Cyberkriminalität zu erheben. Im Zeitraum vom 25. Juni bis 5. August 2025 wurden 515 KMU-Interviews und 336 Interviews mit IT-Dienstleistern (jeweils via Online-Fragebogen) geführt. Bei den KMU mit 1 bis 49 Mitarbeitenden wurden Personen befragt, die in ihrem Unternehmen alleine oder gemeinsam mit anderen Personen Entscheidungen in Bezug auf die Unternehmensstrategie treffen. Davon bezeichnen sich 26 als digitale Pioniere, welche digitale Technologien früh einsetzen, 221 als Early Followers, welche digitale Technologien kurz nach der Markteinführung einsetzen und 208 als Late Followers, welche digitale Technologien erst einführen, wenn sie von anderen erfolgreich genutzt werden (nicht alle Teilnehmende haben diese Frage beantwortet). Die IT-Dienstleister wurden schriftlich zur Teilnahme eingeladen. Sie wurden durch die NOGA-Codes 620200, 620300, 620900 und 631100 identifiziert.

Download von Studienpräsentation und Infografik auf www.cyberstudie.ch

Tipps für eine sichere private Internetnutzung

1. Prüfen Sie Links in E-Mails, deren Absender/Absenderin Sie nicht kennen, bevor Sie klicken.
2. Teilen Sie keine persönlichen oder sensiblen Informationen mit unbekannten Personen.
3. Kaufen Sie auf Shopping-Sites ein, die Sie kennen bzw. wo Sie die Firma verifizieren können.
4. Erstellen Sie automatisiert/regelmässig ein Backup Ihrer Daten.
5. Aktualisieren Sie automatisiert/regelmässig die Software auf Ihrem Mobiltelefon, Tablet und Laptop/Computer.
6. Nutzen Sie starke Passwörter – nutzen Sie einen Passwort-Manager.
7. Wo angeboten, aktivieren Sie die Zwei- oder Multi-Faktoren-Authentifizierung (2FA/MFA).
8. Nutzen Sie öffentliches Wi-Fi nur wenn notwendig und mit einer VPN.
9. Achten Sie darauf, Ihre Informationen aus vertrauenswürdigen Quellen zu beziehen.
10. Melden Sie Betrugsfälle bei der Polizei.

Weitere Informationen:
iBarry – Tipps und Checklisten von der Plattform für Internetsicherheit, www.ibarry.ch

iBarry
Plattform für Internetsicherheit

Quelle:
Marc K. Peter, Martina Dalla Vecchia, Katja Dörlemann, Kristof A. Hertig, Andreas W. Kaelin, Manuel Kugler, Karin Mändli Lerch & Simon B. Seebeck (2025): KMU Cybersicherheit 2025. IT-Sicherheit in Schweizer KMU und bei IT-Dienstleistungsunternehmen (www.cyberstudie.ch).

digitalswitzerland, Die Mobiliar, Schweizerische Akademie der Technischen Wissenschaften SATW, Information Security Society Switzerland ISSS, Swiss Internet Security Alliance SISA, Allianz Digitale Sicherheit Schweiz ADSS, Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz FHNW, HES-SO Valais-Wallis School of Management, YouGov Schweiz.

Forschungsbericht und Infografik in Deutsch, Englisch, Französisch und Italienisch können auf www.cyberstudie.ch bezogen werden.

digitalswitzerland · die Mobiliar · satw · /SSS information security society switzerland · SWISS INTERNET SECURITY ALLIANCE · ALLIANZ DIGITALE SICHERHEIT SCHWEIZ · n|w Fachhochschule Nordwestschweiz Hochschule für Wirtschaft · Hes·so VALAIS WALLIS School of Management · YouGov