Cybersicherheit 2025

Zweiteilige Befragung unter Schweizer KMU und IT-Dienstleistern

Summary (detaillierte Ergebnisse siehe Chartbericht)

---

1. Zu der Studie

Vom 25. Juni bis am 5. August 2025 führte YouGov Schweiz im Auftrag einer Projektgruppe, bestehend aus Mitarbeitenden von Die Mobiliar (Simon B. Seebeck), digitalswitzerland (Kristof Hertig), der Allianz digitale Sicherheit Schweiz (Andreas W. Kaelin), der Fachhochschule Nordwestschweiz FHNW (Marc K. Peter), der Schweizerischen Akademie der Technischen Wissenschaften SATW (Manuel Kugler), der Swiss Internet Security Alliance SISA (Katja Dörlemann) und in einer Studienpartnerschaft mit der information security society switzerland ISSS, eine zweiteilige Befragung durch. Ziel war die Erhebung der Einstellung von Schweizer KMU und IT-Dienstleistungsunternehmen zum Thema Cybersicherheit.

	KMU	**IT-Dienstleister**
Befragungszeitraum:	25. Juni bis 5. August 2025	
Sprachregionen:	Alle drei Sprachregionen	
Zielgruppe:	(Mit-)Entscheider:innen bzgl. Geschäftsstrategie von KMU mit 1 – 49 Mitarbeitenden	IT-Dienstleistungsunternehmer mit NOGA-Codes 620200, 620300, 620900, 631100
Stichprobe:	n = 515	n = 336
Methode:	YouGov Schweiz Internet Panel	Online-Fragebogen mit Einladung durch Briefversand
Quoten:	Disproportionale Erhebung mit Quoten auf Firmengrösse und Sprachregion, Gewichtung gemäss effektiver Struktur	Keine Quoten, keine Gewichtung

2. Summary

KMU sind sich einig, dass Cyberkriminalität ein ernstzunehmendes Problem ist und Massnahmen dagegen wichtig sind. Die gefühlte Resilienz sinkt – die KMU fühlen sich also weniger gut geschützt und vorbereitet – und trotzdem sinkt auch die Priorität des Themas sowie die Absicht, in naher Zukunft die Massnahmen zu verstärken. Die gefühlte Sicherheit hingegen ist gleichbleibend zur Vorjahresbefragung, so auch die Einschätzung des Risikos, dass das eigene Unternehmen durch einen Cyberangriff mindestens einen Tag lang ausser Kraft gesetzt wird. Tatsächlich war rund jedes 25. KMU in den letzten drei Jahren von Schäden eines Cyberangriffs betroffen. Vielleicht dominieren aktuell andere Themen die Agenda, vielleicht herrscht aber auch die Meinung oder Hoffnung vor, dass es nur «die anderen» trifft.

Download von Infografiken, Medienmitteilung und Präsentation auf: www.cyberstudie.ch

IT-Dienstleister hingegen schätzen das Risiko für Schweizer KMU sehr viel höher ein und warnen vor der unterschätzten Gefahr. Obwohl sie eine ausgeprägtere Meinung zur Cyberkriminalität haben, ihr eine höhere Priorität zuordnen und sich besser informiert fühlen, sinkt ihr Sicherheits- und Resilienzgefühl signifikant gegenüber der Vorjahresstudie. Sie waren in fast genau gleichem Masse von Cyberangriffen betroffen wie die befragten KMU. Treffen kann es also alle gleichermassen; entscheidend ist eine gute Vorbereitung zur Verhinderung oder schnellen Behebung von Schäden.

3. Zielgruppe KMU

3.1 Key Insights KMU-Befragung

Rund jedes 25. KMU (4%) mit 1 bis 49 Mitarbeitenden war innerhalb der letzten drei Jahre von Schäden durch einen Cyberangriff betroffen. Dieser Wert entspricht der Vorjahresstudie, und bedeutet hochgerechnet rund 25'600 bis 26'600 betroffene Schweizer KMU. Als Schäden nennen die Betroffenen am häufigsten die emotionale Belastung, die durch den Angriff entstand, den grossen Arbeitsaufwand und einen finanziellen Schaden. Von einem Verlust von Kundendaten oder Reputationsschäden wird jedoch kaum oder gar nicht berichtet.

Erstmals wurde in dieser Studie auch finanziellen Verlusten gefragt, die durch Betrugsmails entstanden. Vier Prozent der befragten KMU haben schon einmal irrtümlich Geld einbezahlt, weil sie sich durch betrügerische Mails täuschen liessen. Hochgerechnet auf die Grundgesamtheit von rund 614'400 KMU bedeutet dies zwischen 24'000 und 24'900 Fälle in der Schweiz. Bei drei Vierteln davon war das Geld verloren, ein Viertel konnte das Geld wieder zurückgewinnen.

Die Befragten sind sich einig, dass Cyberkriminalität ein ernstzunehmendes Problem ist (9 von 10 stimmen zu) und Massnahmen wichtig sind (8 von 10 stimmen zu). Cyberkriminalität ist aber kein Thema, das unter Kollegen einen gewissen sozialen Druck auslöst: Nur rund ein Viertel der Befragten ist der Meinung, dass die Kollegen denken, die Firma sollte sich besser vor Cyber-Attacken schützen. 2025 zeigt sich sogar, dass die Priorität des Themas stark sinkt: 2024 beurteilte noch knapp die Hälfte das Thema Cybersicherheit als (sehr) wichtig, 2025 ist es nur noch ein Drittel. Dementsprechend planen 2025 auch signifikant weniger Befragte, ihre Sicherheitsmassnahmen zu erhöhen (40%), als noch 2024 (48%).

3.2 Zuständigkeiten für IT-Arbeiten und Cybersicherheit

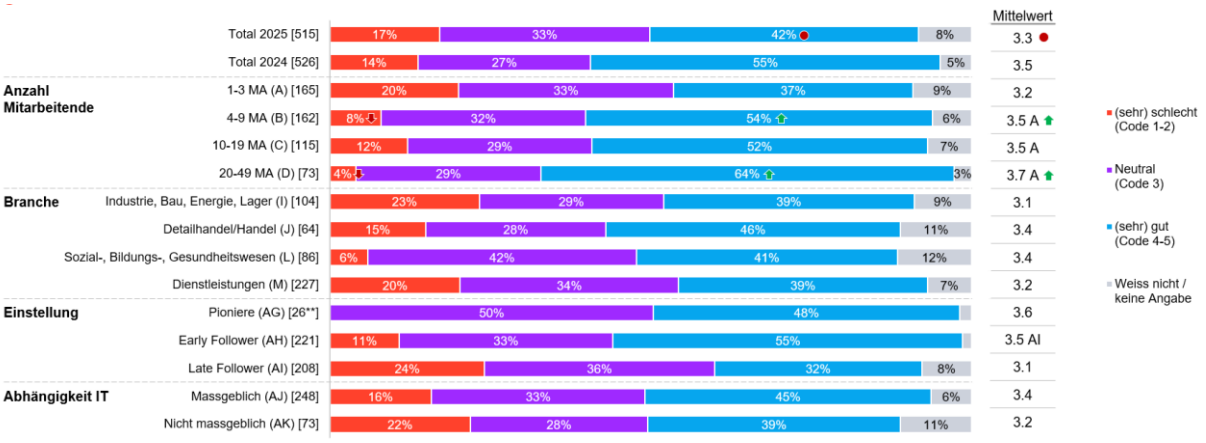
Rund zwei Drittel (63%) der KMU haben einen oder mehrere externe IT-Dienstleister für Informatik, Telefonie, Software- oder Hardware-Arbeiten – dieser Wert ist unverändert zum letzten Jahr. Grössere Unternehmen geben anteilsmässig mehr Arbeiten extern als kleinere: Die kleinsten befragten Unternehmen mit 1 bis 3 Mitarbeitenden geben rund 20 Prozent ihrer IT-Arbeiten extern, die grössten mit 20 bis 49 Mitarbeitenden rund 39 Prozent. Die Frage, ob ihre IT-Dienstleister über eine IT-Sicherheitszertifizierung verfügen, wie z.B. ISO 27001, ist aber für über die Hälfte der Befragten (53%) nicht relevant – sie wissen es nicht. 2024 waren es nur rund zwei Fünftel (43%),

die dazu nicht Bescheid wussten. Rund ein Drittel (35%) sagt, ihr IT-Dienstleister sei zertifiziert (2024: 44%).

Fast gleichbleibend ist die Zahl der Unternehmen, bei denen eine Person explizit für die Cybersicherheit zuständig sind: Knapp die Hälfte der Befragten (49%) hat eine interne oder externe zuständige Person (2024: 50%). **Bei rund zwei Fünfteln der Befragten (42%) gibt es keine zuständige Person, weil Cyber-Risiken keine Priorität haben (2024: 44%).** Auch bei knapp zwei Fünfteln (38%) derjenigen Unternehmen, deren Betrieb massgeblich von der IT abhängig ist, gibt es keine für Cyber-Risiken zuständige Person – weder intern noch extern. Grundsätzlich gilt: Je grösser die Firma ist, desto eher gibt es eine entsprechende Zuständigkeit. So haben nur knapp zwei Fünftel (39%) der Unternehmen mit 1 bis 3 Mitarbeitenden eine (interne oder externe) zuständige Person, aber knapp drei Viertel (71%) der Unternehmen mit 4 bis 9 Mitarbeitenden und über vier Fünftel der Unternehmen mit 10 bis 19 Mitarbeitenden (82%) bzw. der Unternehmen mit 20 bis 49 Mitarbeitenden (84%). **Wenn eine interne oder externe Funktion vorhanden ist, wird dem Thema Cybersicherheit eine höhere Priorität gegeben und es werden mehr organisatorische und technische Massnahmen umgesetzt.**

3.3 Sicherheitsgefühl und Risikoeinschätzung

Über die Hälfte der befragten KMU (52%) fühlen sich eher oder sehr sicher vor Cyberkriminalität, nur eine kleine Minderheit (9%) fühlt sich eher oder sehr unsicher. Gegenüber der Vorjahresstudie haben sich diese Werte kaum verändert; der Mittelwert blieb auf einer 3.6 auf der Fünferskala. Stark zurückgegangen ist aber das Gefühl der Resilienz, d.h. wie gut vorbereitet und geschützt man sich einschätzt. So schätzte sich letztes Jahr noch über die Hälfte der Befragten (55%) eher oder sehr gut geschützt ein, dieses Jahr sind es nur noch zwei Fünftel (42%). Der Mittelwert sank von 3.5 auf 3.3 auf der Fünferskala. **Die Befragten fühlen sich also unverändert mehrheitlich sicher, aber signifikant schlechter vorbereitet und geschützt.**



F008: Was schätzen Sie: Wie gut sind Sie vor Cyberangriffen geschützt und auf einen Angriff vorbereitet?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut | **sehr kleine Basis <30 | Datenbeschriftung ab 3% | Die hinter den Wert gesetzten Buchstaben bedeuten einen sign. Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Vielleicht halten viele von ihnen eine gute Vorbereitung bzw. einen guten Schutz für unnötig, denn nur jedes zehnte befragte Unternehmen (10%) schätzt das Risiko, innerhalb der nächsten zwei bis drei Jahre durch einen Cyberangriff mindestens einen Tag lang ausser Kraft gesetzt zu werden, für sehr oder eher hoch, während über die Hälfte (54%) es für eher oder sehr klein hält. Selbst Unternehmen, die massgeblich von einer funktionierenden IT abhängig sind, schätzen das Risiko nicht höher ein (12% eher/sehr grosses Risiko). **Die Risikoeinschätzung hat sich – wie das Sicherheitsgefühl – nicht verändert zum letzten Jahr.** Eine höhere Risikoeinschätzung lässt sich bei den grösseren beiden Unternehmensklassen feststellen: Nur rund zwei Fünftel der Unternehmen mit 10 bis 19 Mitarbeitenden (43%) bzw. mit 20 bis 49 Mitarbeitenden (38%) halten das Risiko für eher oder sehr klein (Total: 54%).

Passend zu diesen Resultaten ist denn auch, dass **die Priorität des Themas gegenüber dem Vorjahr massiv gesunken** ist: Von einer 3.5 auf der Fünferskala auf eine 3.1, wobei nur noch ein Drittel (33%) das Thema als (sehr) wichtig bezeichnet (2024: 47%) und über ein Viertel (28%) als (überhaupt) nicht wichtig (2024: 18%).

Je mehr Mitarbeitende das Unternehmen hat, desto höher ist die Priorität des Themas: So liegt der Mittelwert bei Unternehmen…

- mit 1 bis 3 Mitarbeitenden bei 3.0,
- mit 4 bis 9 Mitarbeitenden bei 3.4,
- mit 10 bis 19 Mitarbeitenden bei 3.6 und
- mit 20 bis 49 Mitarbeitenden bei 3.7.

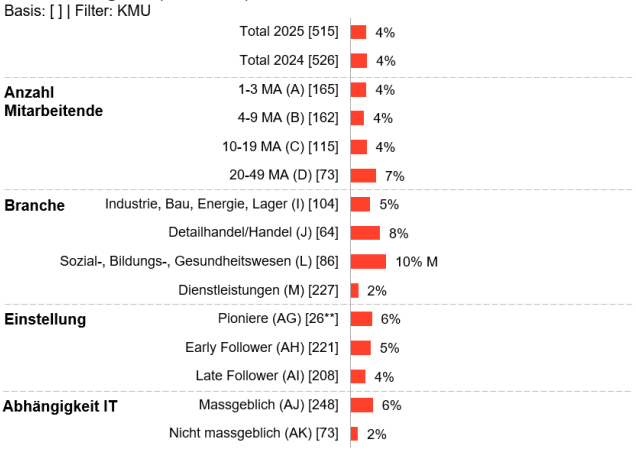
Nicht überraschen dürfte aufgrund dieser Resultate auch, dass **die Absicht, die Sicherheitsmassnahmen in den kommenden 1 bis 3 Jahren zu erhöhen, gegenüber dem letzten Jahr gesunken** ist: War es 2024 noch knapp die Hälfte (48%), die zusätzliche Sicherheitsmassnahmen für (sehr) wahrscheinlich hielten, sind es 2025 noch zwei Fünftel (40%, der Mittelwert sank von 3.5 auf 3.2 auf der Fünferskala. Unternehmen, die massgeblich abhängig sind von einer funktionierenden IT, planen signifikant eher zusätzliche Massnahmen (Mittelwert 3.5). Auch sind grössere Unternehmen eher positiv eingestellt gegenüber neuen Sicherheitsmassnahmen als kleinere Unternehmen.

3.4 Betroffenheit von Cyberkriminalität

Jedes 25. Unternehmen (4%) mit 1 bis 49 Mitarbeitenden hat in den letzten drei Jahren einen Cyberangriff erlitten, wobei Unternehmen mit 20 bis 49 Mitarbeitenden (7%), aus dem Detailhandel/Handel (8%) und dem Sozial-, Bildungs- und Gesundheitswesen (10%) etwas häufiger betroffen waren. In 14 von 23 Fällen entstand dadurch eine hohe emotionale Belastung, 12 Fällen ein finanzieller Schaden und in 10 Fällen ein grosser Arbeitsaufwand. Waren 2024 auch mehrere Kundendatenverluste und Reputationsschäden erwähnt worden, werden diese beiden Schadensarten dieses Jahr kaum bzw. gar nicht erwähnt.

Jedes 20. Unternehmen (5%) wurde schon einmal durch Cyberkriminelle erpresst, bei Firmen über 10 Mitarbeitenden ist der Anteil etwas höher (10 – 19 Mitarbeitende: 6%, 20 – 49 Mitarbeitende: 7%). **In einem von 23 Erpressungfällen wurde Lösegeld bezahlt.**

Erlittene Angriffe (Ja-Anteile)
Basis: [ ] | Filter: KMU



Erlittene Schäden
Basis: n=23** | Filter: KMU – wenn Cyberangriff erlitten

Schäden	Anzahl Fälle
Emotionale Belastung	14
Ein finanzieller Schaden	12
Ein grosser Arbeitsaufwand zur Behebung	10
Ein Kundendatenverlust	1
Ein Reputationsschaden	0
Nichts davon	1
Weiss nicht / keine Antwort	0

F016: 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? | F017: Entstand durch diesen Angriff… | Basis: n=[ ] | ** Sehr kleine Basis <30 | Die hinter den Wert gesetzten Buchstaben bedeuten einen sign. Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Von einem betrügerischen E-Mail getäuscht und zu einer Einzahlung verleitet wurden 4 Prozent der Befragten, wobei das Geld in einem Viertel der Fälle (25%) wieder zurückgewonnen werden konnte.

3.5 Massnahmenumsetzung

Grundsätzlich schätzen die Befragten die Umsetzung von technischen Massnahmen höher ein als diejenige von organisatorischen Massnahmen. Trotzdem erstaunt die **noch wenig verbreitete Umsetzung einer Zweiweg- oder Mehrwegauthentifizierung (53%) oder die eher seltene Verwendung eines Passwortmanagers (42%).**

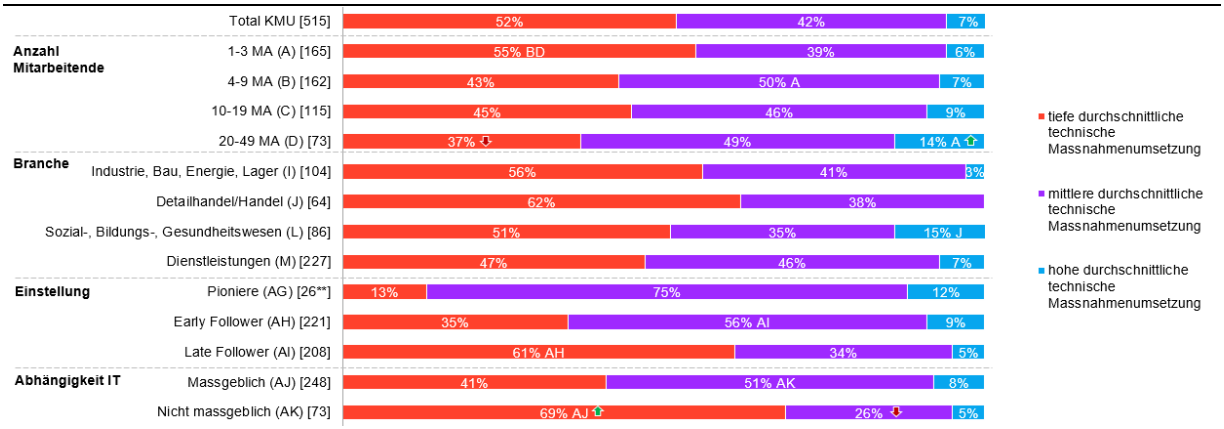
Fünf von zehn organisatorischen Massnahmen wurden von weniger als einem Drittel der Befragten umgesetzt: Nur rund 30 Prozent…

- … haben einen Notfallplan für die Geschäftsfortführung,
- … haben ein Sicherheitskonzept,
- … schulen ihre Mitarbeitenden regelmässig oder
- … evaluieren die IT-Sicherheit ihrer Zulieferer/Partner.

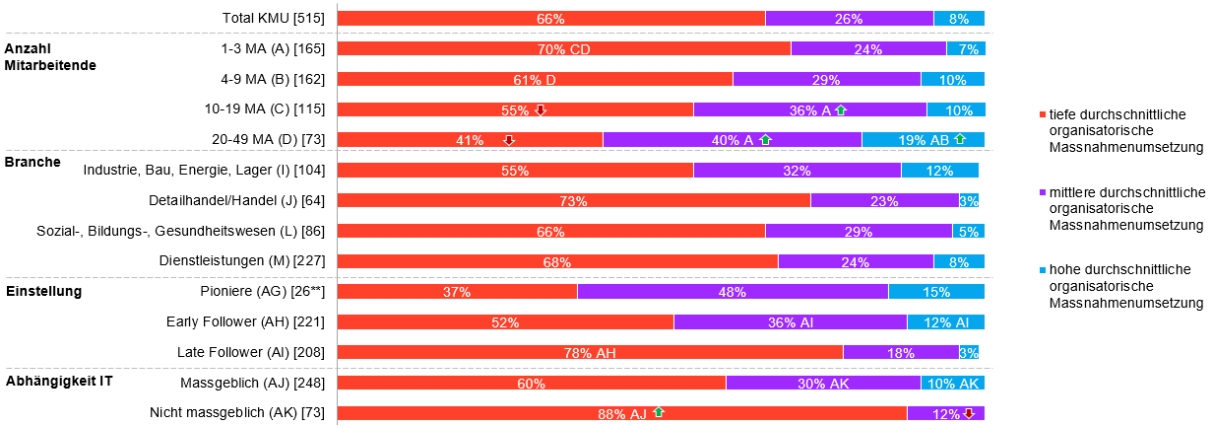
Gar nur ein Fünftel der Befragten Sicherheitsaudits durch.

Mit einem Mittelwert über den Umsetzungsgrad aller abgefragten Massnahmen wurde eine Unterteilung in «tiefe», «mittlere» und «hohe» Massnahmenumsetzung erstellt («tief“ = Mittelwert

<=3.49, «mittel» = Mittelwert >=3.5 und <=4.49, «hoch» = Mittelwert >= 4.5). Dabei zeigt sich, dass rund die Hälfte (52%) einen tiefen, zwei Fünftel (42%) einen mittleren und 7 Prozent einen hohen Umsetzungsgrad technischer Massnahmen erreichen:



Bei den organisatorischen Massnahmen erreichen zwei Drittel (66%) aller befragten Unternehmen einen tiefen, rund ein Viertel (26%) einen mittleren und knapp jedes zehnte Unternehmen (8%) einen hohen Umsetzungsgrad organisatorischer Massnahmen:



Sowohl bei den technischen als auch bei den organisatorischen Massnahmen sind es **ausschliesslich Unternehmen mit 20 bis 49 Mitarbeitenden, die signifikant häufiger einen hohen Umsetzungsgrad (14% bzw. 19%) erreichen.** Selbst von den Unternehmen, deren Betrieb massgeblich abhängig von einer funktionierenden IT ist, erreichen lediglich 8 Prozent einen hohen technischen bzw. 10 Prozent einen hohen organisatorischen Umsetzungsgrad.

Weder bei den technischen noch bei den organisatorischen Massnahmen gibt es Verbesserungen gegenüber 2024.

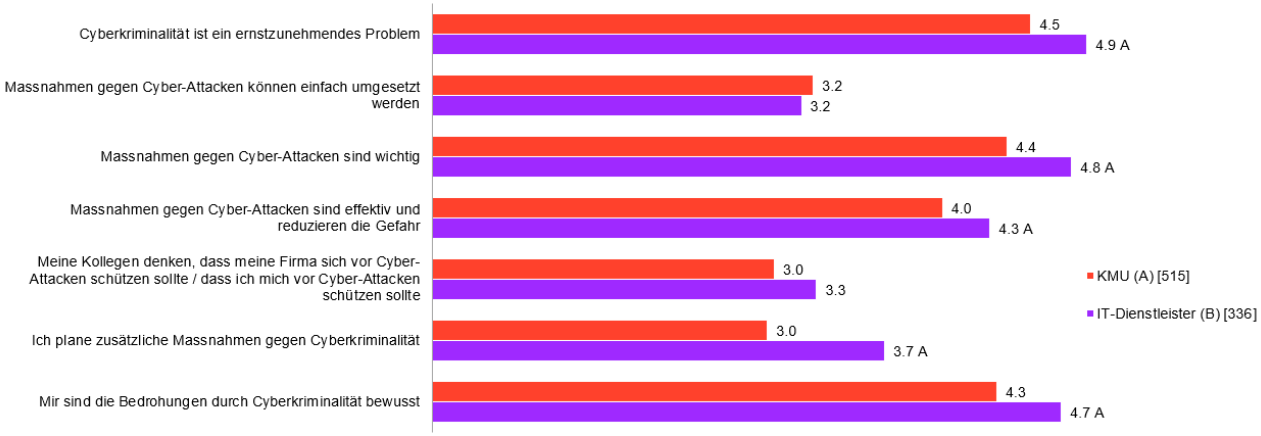
Download von Infografiken, Medienmitteilung und Präsentation auf: www.cyberstudie.ch

4. Zielgruppe IT-Dienstleister

4.1 Einstellung Cybersicherheit: Selbst- und Fremdeinschätzung

Das Sicherheits- und Resilienzgefühl der IT-Dienstleister ist gegenüber 2024 signifikant gesunken – **nur noch rund zwei Drittel fühlen sich (sehr) sicher (65%) und gut geschützt bzw. vorbereitet (68%).** 2024 waren es noch rund drei Viertel (77% bzw. 75%). Die Sicherheit ihrer Kunden schätzen sie noch tiefer ein: Nur rund zwei Fünftel (39%) der IT-Dienstleister halten ihre Kunden für (sehr) sicher und nur ein Drittel von ihnen (33%) hält sie für (sehr) gut geschützt und vorbereitet.

Die Einstellung der IT-Dienstleister unterscheidet sich in mehreren Aspekten signifikant von der Einstellung der KMU: Sie halten Cyberkriminalität für ein ernsteres Problem (4.9 vs. 4.5), Massnahmen für wichtiger (4.8 vs. 4.4) und für effizienter (4.3 vs. 4.0), sind sich der Bedrohungen eher bewusst (4.7 vs. 4.3) und planen selber eher zusätzliche Massnahmen (3.7 vs. 3.0).



F15: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: Alle Befragten | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Mittelwerte ausgewiesen
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Fast zwei Drittel der IT-Dienstleister (61%) schätzen das Risiko für Schweizer KMU, innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff für mindestens einen Tag ausser Kraft gesetzt zu werden, (sehr) hoch ein. Das ist zwar ein hoher Wert, aber signifikant tiefer als noch 2024 (68%). Zur Erinnerung aus dem vorherigen Kapitel: Nur 10 Prozent der KMU schätzen dieses Risiko (sehr) hoch ein. Sie empfehlen bezüglich Cybersicherheit, das Thema ernst zu nehmen (36%), das Personal zu schulen (26%) und die IT upzudaten und zu verbessern (15%).

4.2 Cyberkriminalität: Erfahrung und Risikoeinschätzung

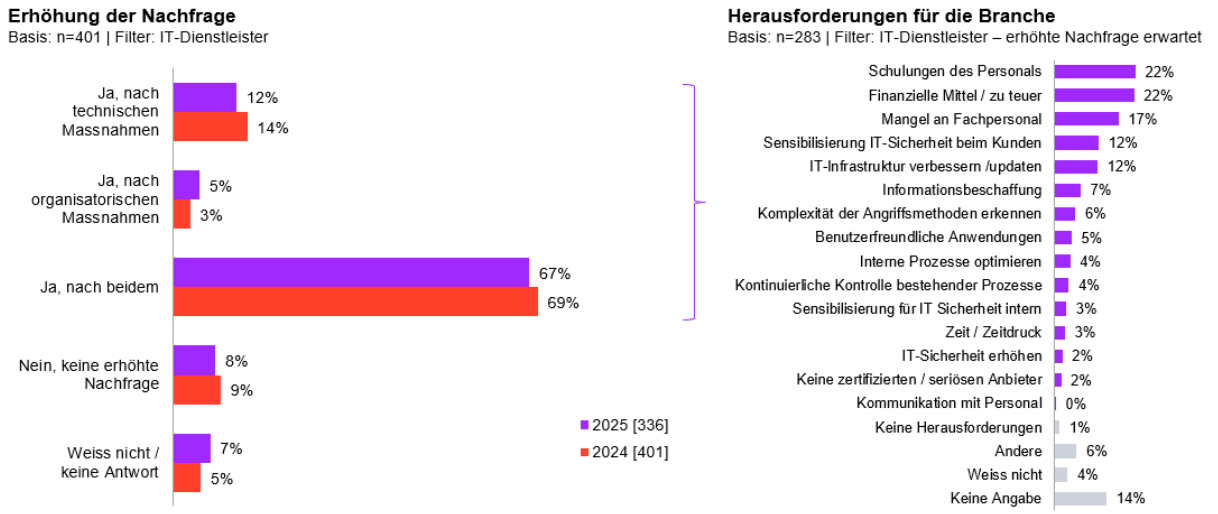
Trotz der ausgeprägteren Einstellung sind prozentual genau gleich viele IT-Dienstleister (4%) wie KMU in den letzten drei Jahren Opfer eines Cyberangriffes geworden, der Schäden nach sich

zog. Am häufigsten wird von den Betroffenen der grosse Arbeitsaufwand zur Behebung des Schadens genannt (10 von 15 Fällen), sowie die emotionale Belastung (9 Fälle). Reputationsschäden (5 Fälle) und finanzielle Schäden (4 Fälle) nennen sie seltener.

Cyberangriffe betreffen somit beide Zielgruppen gleichermassen; entscheidend für das Ausmass der Folgen ist die Vorbereitung darauf – und somit besonders die organisatorischen Massnahmen.

4.3 Cybersicherheitsnachfrage in Zukunft

Mehr als 8 von 10 befragten IT-Dienstleistern erwarten in naher Zukunft eine höhere Nachfrage nach Cybersicherheit. Die meisten IT-Dienstleister erwarten sowohl bei technischen als auch bei organisatorischen Massnahmen eine Zunahme (67%), 12 Prozent erwarten die Zunahme lediglich bei technischen Massnahmen und 5 Prozent lediglich bei organisatorische Massnahmen. Von den befragten KMU hingegen planen nur knapp zwei Fünftel (40%) eine Erhöhung der Sicherheitsmassnahmen in den nächsten 1 bis 3 Jahren.



F060: Erwarten Sie in naher Zukunft eine erhöhte Nachfrage durch KMU nach Cybersicherheit? | F061: Was sind die Herausforderungen für Ihre Branche, um dieser erhöhten Nachfrage nachzukommen?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Frage (F060) & offene Frage (F061)

Um der Nachfrage nachzukommen, sehen die IT-Dienstleister Herausforderungen in Personalschulungen (22%) bzw. dem Mangel an Fachpersonal (17%). Sie gehen zudem davon aus, dass die Massnahmen vielen zu teuer sein werden (22%).