YouGov

Cyberstudie 2024

Dreiteilige Befragung unter Schweizer KMU, IT-Dienstleistern und der Bevölkerung

Summary

(detaillierte Ergebnisse siehe Chartbericht)

---

1. Zu der Studie

Vom 4. Juli bis am 5. August 2024 führte YouGov Schweiz im Auftrag einer Projektgruppe, bestehend aus Mitarbeitenden von Die Mobiliar (Patric Vifian), digitalswitzerland (Kristof Hertig), der Allianz digitale Sicherheit Schweiz (Andreas Kaelin), der Fachhochschule Nordwestschweiz FHNW (Marc K. Peter), der Schweizerischen Akademie der Technischen Wissenschaften SATW (Nicole Wettstein) und der Swiss Internet Security Alliance SISA (Katja Dörlemann), eine dreiteilige Befragung durch. Ziel war die Erhebung der Einstellung von Schweizer KMU, IT-Dienstleistungsunternehmen und der Bevölkerung zum Thema Cyberkriminalität.

	KMU	**IT-Dienstleister**	**Bevölkerung**
Befragungszeitraum:	4. Juli bis 5. August 2024		
Sprachregionen:	Alle drei Sprachregionen		
Zielgruppe:	(Mit-)Entscheider bzgl. Geschäftsstrategie von KMU mit 1 – 49 Mitarbeitenden	IT-Dienstleistungsunternehmer mit NOGA-Codes 620200, 620300, 620900, 631100	18- bis 79-jährige sprachassimilierte Bevölkerung
Stichprobe:	n = 526	N = 401	N = 1’247
Methode:	Online-Fragebogen mit Einladung durch Briefversand und YouGov Schweiz Internet Panel	Online-Fragebogen mit Einladung durch Briefversand	YouGov Schweiz Internet Panel
Quoten:	Disproportionale Erhebung mit Quoten auf Firmengrösse und Sprachregion, Gewichtung gemäss effektiver Struktur	Keine Quoten, keine Gewichtung	Quoten auf Alter, Geschlecht und Region, das Tessin überproportional befragt und nachträglich gewichtet

2. Summary

Die Studie mit ihren drei Befragungen zeigt, dass das Risiko von Cyberangriffen und das Gewicht von deren Folgen von KMU und Bevölkerung eher unterschätzt wird, wovor die IT-Dienstleister ihrerseits warnen und empfehlen, das Thema ernster zu nehmen. Erstaunlich viele Befragte sind von Angriffen oder Betrugsfällen mit finanziellen Folgen betroffen, erstaunlich viele bezahlten

Lösegeld bei Erpressungen. Zu einem (zu) hohen Sicherheitsgefühl führt evt. ein zu hohes Vertrauen in technische Schutzmassnahmen, während organisatorische Massnahmen eher vernachlässigt werden. Zudem scheinen sich viele Befragte unter den kleinen KMU und in der Bevölkerung zu uninteressant für Angriffe zu fühlen, was ein durchaus folgenschwerer Trugschluss sein kann.

Massnahmen gegen Cyberkriminalität werden als wichtig betrachtet, deren Umsetzung jedoch als nicht einfach. Möglichst einfache technische Lösungen und Schulungen oder Informationskampagnen müssten somit zu einer besseren Cyberresilienz der Schweizer Bevölkerung und KMU-Landschaft führen, denn die Umfrageresultate zeigen auch: Je besser die Befragten informiert sind, desto sicherer verhalten sie sich.

3. Zielgruppe KMU

3.1 Key Insights KMU-Befragung

Das Angriffsrisiko wird von KMU angesichts der hohen Betroffenheit eher unterschätzt: Die IT-Dienstleister schätzen das Risiko im zweiten Teil der Befragung deutlich höher ein und warnen davor, dass das Thema zu wenig ernst genommen wird. In den letzten drei Jahren waren 4 Prozent der befragten Unternehmen betroffen (bei Unternehmen ab 4 Mitarbeitenden liegt der Anteil bei 7% bis 10%) und in fast drei Viertel der Angriffe entstand ein finanzieller Schaden. Zudem kam es in 6 Prozent der Erpressungsfälle zu Lösegeldzahlungen. Ausgehend von diesen Ergebnissen drängt sich der Schluss auf, dass der finanzielle Verlust und die anfallende Arbeit zur Bereinigung der Schäden unterschätzt wird.

Unternehmen mit 1 – 3 bzw. 4 – 9 Mitarbeitenden sind grundsätzlich weniger in das Thema Cyberkriminalität involviert: Sie haben seltener eine interne oder externe zuständige Person für Cyberkriminalität, geben Cybersicherheit eine niedrigere Priorität und setzen weniger technische und organisatorische Massnahmen um. Sie schätzen auch das Risiko eines Cyberangriffes signifikant tiefer ein als Unternehmen mit mehr als 10 Mitarbeitenden. Trotzdem waren in den letzten 3 Jahren auch die ganz kleinen Unternehmen von Cyberangriffen mit Folgeschäden betroffen (1 – 3 Mitarbeitende: 3%, 4 – 9 Mitarbeitende: 9%) und sie sollten sich nicht aufgrund ihrer Grösse in falscher Sicherheit wiegen.

Je besser sich die Unternehmen zum Thema Cyberrisk informiert fühlen, desto höhere Priorität geben sie dem Thema und desto höher schätzen sie das Risiko eines Angriffs ein. Zudem liegen sowohl die technische als auch die organisatorische Massnahmenumsetzung bei den eher und sehr gut Informierten signifikant höher. Um die Cybersicherheit zu erhöhen, sollte also über das Risiko und die Schutzmassnahmen informiert werden. Auch die im zweiten Teil befragten IT-Dienstleister raten in erster Linie dazu, das Thema ernster zu nehmen und das Personal zu schulen.

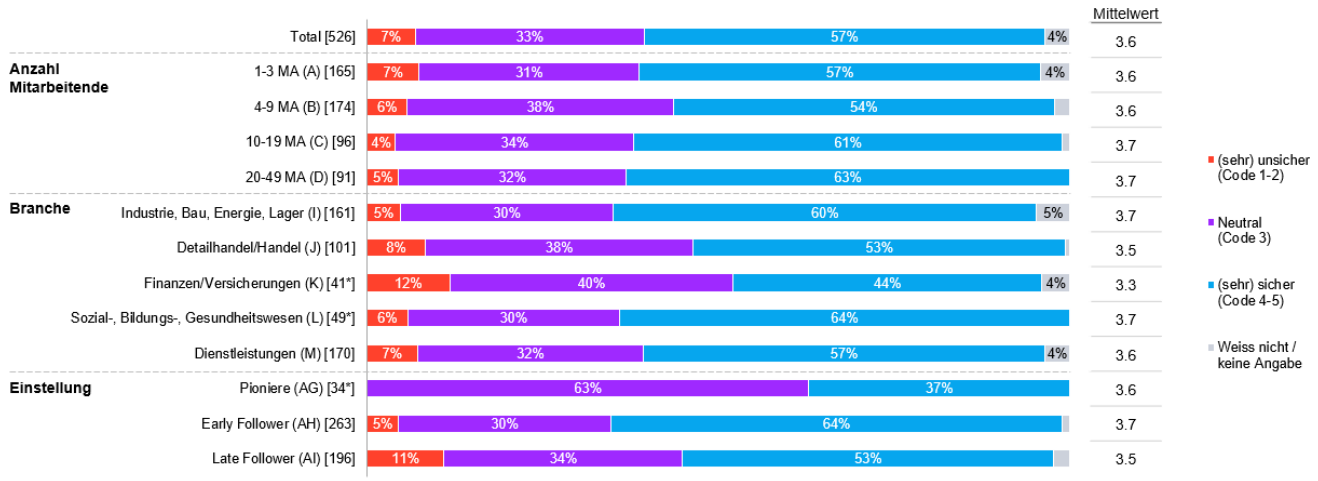
3.2 Zuständigkeiten für IT-Arbeiten und Cybersicherheit

Rund zwei Drittel (67%) der KMU haben einen oder mehrere externe IT-Dienstleister für Informatik, Telefonie, Software- oder Hardware-Arbeiten. Je mehr Mitarbeitende die Unternehmen haben, desto mehr Arbeiten geben sie extern: Die kleinsten befragten Unternehmen mit 1 bis 3 Mitarbeitenden geben rund 16% ihrer IT-Arbeiten extern, die grössten mit 20 bis 49 Mitarbeitenden rund 42%. Ob die IT-Dienstleister über eine IT-Sicherheitszertifizierung verfügen, wie z.B. ISO 27001, ist dabei rund zwei Fünfteln der outsourcenden Unternehmen (43%) nicht bekannt, weitere runde zwei Fünftel (44%) antworten mit «ja,», knapp jede/-r achte mit «nein» (13%). Zertifizierungen werden denn auch nur von 7 Prozent der Befragten als wichtig erachtet, wenn sie einen IT-Dienstleister auswählen.

Etwas weniger als jedes dritte Unternehmen (29%) wird zum Thema Cyberrisiko von einem externen Partner unterstützt, bei rund einem Fünftel (21%) gibt es eine interne spezielle Funktion oder Teilfunktion dafür. **Bei rund zwei Fünfteln der Befragten (44%) gibt es keine zuständige Person, weil Cyber-Risiken keine Priorität haben.** Dies ist besondere bei den ganz kleinen Unternehmen (1 – 3 Mitarbeitende: 50%, 4 – 9 Mitarbeitende: 36%) der Fall. Bei den grösseren befragten Unternehmen ist es nur noch rund jedes zehnte (10 – 19 Mitarbeitende: 9%, 20 – 49 Mitarbeitende: 8%), welches Cyber-Risiken als zu wenig relevant beurteilt. Beim Branchenvergleich fällt auf, dass selbst bei Unternehmen aus der Finanz- und Versicherungsbranche ein Drittel (33%) dem Thema zu wenig Priorität einräumt, um eine (Teil-)Funktion dafür einzusetzen. **Grundsätzlich gilt: 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 (57%) fühlen sich eher oder sehr sicher vor Cyberkriminalität, nur eine kleine Minderheit (7%) fühlt sich eher oder sehr unsicher. Wenn man konkreter nachfragt, nämlich nach dem Risiko eines Cyberangriffs innerhalb der nächsten 2 bis 3 Jahre, welcher den Betrieb mindestens einen Tag ausser Kraft setzt, so **schätzt nur rund jedes zehnte befragte Unternehmen (12%) dieses Risiko als eher oder sehr hoch ein.** Zum Vergleich: IT-Dienstleister schätzen dieses Risiko für Schweizer KMU sehr viel höher ein. Über zwei Drittel von ihnen (68%) beurteilen es als eher oder sehr hoch.

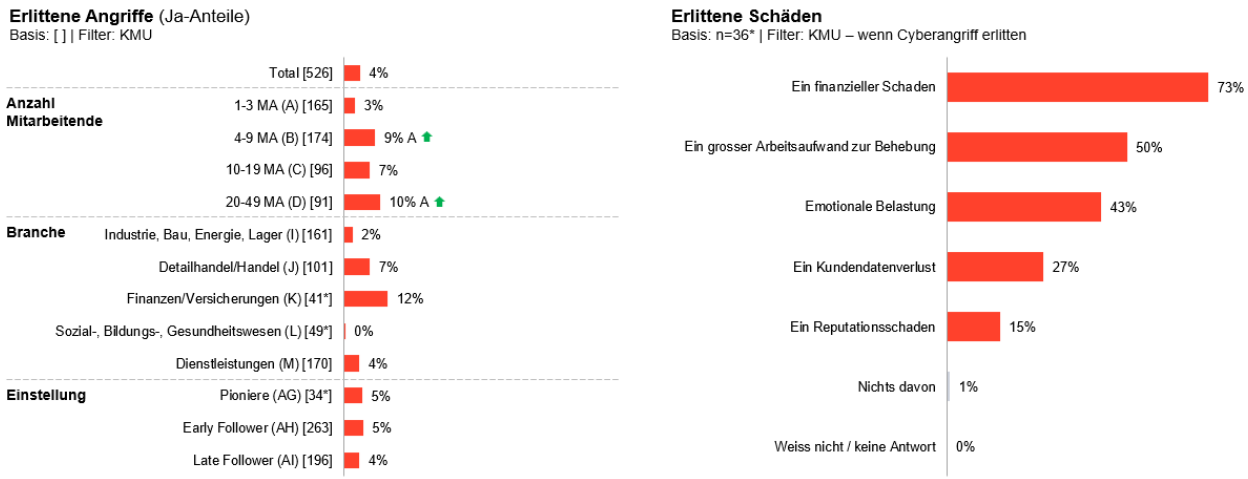


F007: Wie sicher fühlen Sie sich in Ihrem Unternehmen vor Cyberkriminalität?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr unsicher bis 5= sehr sicher | *Kleine Basis <50 | Datenbeschriftung ab 3%

3.4 Betroffenheit von Cyberkriminalität

Jedes 25. Unternehmen (4%) mit 1 – 49 Mitarbeitenden hat in den letzten drei Jahren einen Cyberangriff erlitten, wobei Unternehmen mit 1 – 3 Mitarbeitenden am seltensten betroffen waren (3%) und Unternehmen mit 20 – 49 Mitarbeitenden am häufigsten (10%). **In fast drei Vierteln dieser Fälle entstand ein finanzieller Schaden (73%)**, in der Hälfte der Fälle (50%) ein grosser Arbeitsaufwand zur Behebung und in rund zwei Fünfteln der Fälle (43%) emotionale Belastung. Bei mehr als einem Viertel der erfolgreichen Cyberangriffe (27%) gingen Kundendaten verloren und knapp jede/-r siebte Betroffene (15%) beklagt einen Reputationsschaden.

Knapp jedes 17. Unternehmen (6%) wurde schon einmal durch Cyberkriminelle erpresst, bei Firmen über 10 Mitarbeitenden ist der Anteil etwas höher (10 – 19 Mitarbeitende: 8%, 20 – 49 Mitarbeitende: 11%). **In 6 Prozent dieser Erpressungsfälle wurde Lösegeld bezahlt.**



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=[ ] | ⬆signifikant höher als Total; ⬇signifkant tiefer als Total | *Kleine Basis <50 | Die hinter den Wert gesetzten Buchstaben bedeuten einen sign. Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

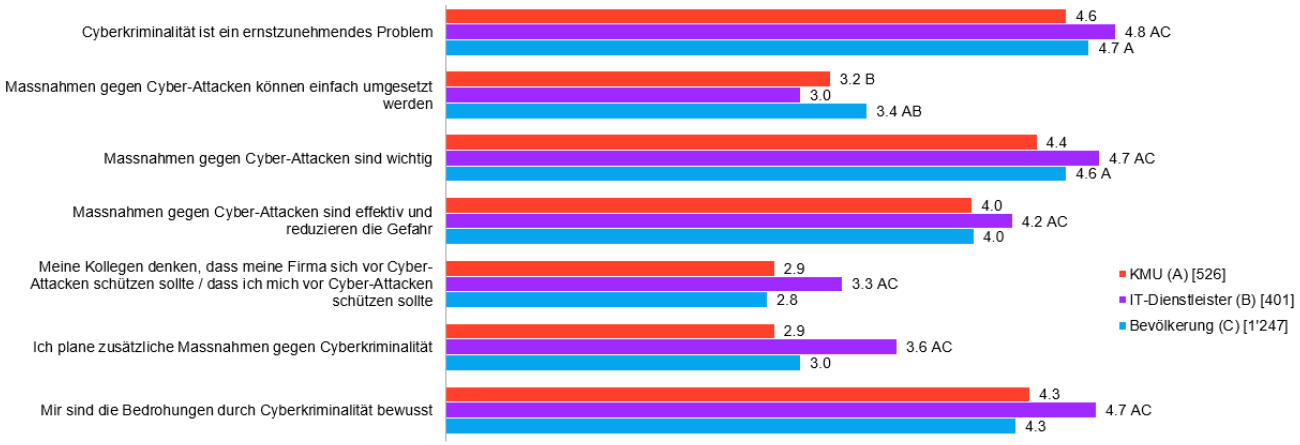
3.5 Massnahmenumsetzung

Technische Massnahmen werden besser umgesetzt als organisatorische, trotzdem gibt es noch deutliches Verbesserungspotential bei der Nutzung von Passwortmanagern (von 37% umgesetzt) und bei der Nutzung von biometrischen Daten oder Passkeys für Logins (von 34% umgesetzt). Nutzung von künstlicher Intelligenz zum Schutz gegen Cyberangriffe ist noch kein Thema bei den befragten KMU (von 6% umgesetzt). Bei den organisatorischen Massnahmen gibt es am meisten Verbesserungspotential bei der Implementierung von Sicherheitskonzepten (von 25% umgesetzt) und der Durchführung von Sicherheitsaudits (von 19% umgesetzt). Aber auch die vergleichsweise einfach umsetzbare und von den IT-Dienstleistern stark empfohlene regelmässige Mitarbeiterschulung birgt noch sehr grosses Potential (von 32% umgesetzt), um sich auf einfache Weise besser vor Cyberangriffen zu schützen.

4. Zielgruppe IT-Dienstleister

4.1 Einstellung Cybersicherheit: Selbst- und Fremdeinschätzung

IT-Dienstleister sind besonders in das Thema Cybersicherheit involviert: Sie schätzen ihren Informationsgrad auf der Fünferskala signifikant höher ein (4.2) als KMU (3.4) und die Bevölkerung (3.3) und sie fühlen sich auch entsprechend sicherer (4.0 vs. KMU 3.6 und die Bevölkerung 3.5). Sie schätzen Cyberkriminalität als ernstzunehmenderes Problem ein (4.8) als KMU (4.6) und die Bevölkerung (4.7) und sie sind am häufigsten der Meinung, dass Massnahmen gegen Cyber-Attacken wichtig sind (4.7).



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.

Die Sicherheit ihrer Kunden (3.4) schätzen die IT-Dienstleister deutlich tiefer ein als die eigene Sicherheit (4.0) und auch tiefer, als sich die KMU im ersten Teil der Befragung selber einschätzen (3.6).

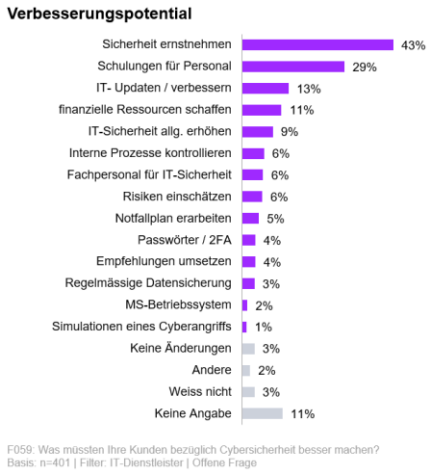
Fast acht von zehn der befragten IT-Dienstleistern geben dem Thema Cybersicherheit in ihrer Firma eine eher bis sehr hohe Priorität (Mittelwert 4.3). Bei ihren Kunden, so schätzen sie, liegt diese Priorität mit einem Mittelwert von 3.5 auf der Fünferskala deutlich tiefer, was auch genau dem Wert entspricht, den die befragten KMU im ersten Teil der Studie angeben.

4.2 Cyberkriminalität: Erfahrung und Risikoeinschätzung

Genau wie bei den KMU wurden 4 Prozent der IT-Dienstleister in den letzten drei Jahren Opfer eines Cyberangriffes, der Schäden nach sich zog. Am häufigsten wird der grosse Arbeitsaufwand zur Behebung des Schadens genannt (15 Fälle); emotionale Belastung und finanzielle Schäden (9 bzw. 8 Fälle) etwas seltener. Bezüglich Erpressungsfälle gleicht das Bild ebenfalls sehr der KMU-Befragung: 5 Prozent der IT-Dienstleister waren schon von Erpressung betroffen, davon haben wiederum 5 Prozent Lösegeld bezahlt (KMU: je 6%). Das Risiko, in den kommenden zwei bis drei Jahren Opfer eines Cyberangriffes zu werden, der das Unternehmen mindestens einen Tag ausser Kraft setzt, schätzen IT-Dienstleister signifikant höher ein (2.5) als die befragten KMU (2.3). Noch viel höher schätzen die IT-Dienstleister dieses Risiko generell für Schweizer KMU ein (3.9).

4.3 Cybersicherheitsnachfrage in Zukunft

Fast 9 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 (69%), 14 Prozent erwarten die Zunahme lediglich bei technischen Massnahmen und 3% lediglich bei organisatorische Massnahmen. Von den befragten KMU hingegen plant nur knapp die Hälfte (48%) eine Erhöhung der Sicherheitsmassnahmen in den nächsten 1 bis 3 Jahren.



Massnahmen bzw. Schutz wird nicht allumfassend umgesetzt bzw. es bestehen meist gute Bestrebungen und auch aktive Massnahmen, aber gleichzeitig an manchen Stellen grosse und bekannte Lücken, welche auch durchaus ignoriert werden. Insbesondere das Risiko Mensch (Mitarbeitende) wird zu wenig adressiert und neue Risiken wie Voice-Phising (Vishing).

Die Abhängigkeit von externen Dienstleistern und die Überführung vieler Applikationen in die Cloud erhöht m.A. das Risiko stark. Durch das fehlende Wissen und die Kompetenz in Sachen Cyberrisiko, Cyberabwehr schwindet die Resilienz stark. Unsere Kunden verlassen sich u.E. zu stark auf die grossen DL wie Microsoft, Amazon, Google und andere Cloudanbieter - das macht anfällig auf "Erpressbarkeit" in Sachen Service, Preis. Die Einflussnahme ist dann eingeschränkt.

Sich besser und genauer informieren und dies nicht aus Unwissenheit oder Angst vor Kosten hinausschieben, bzw. denken, sie wären nie betroffen sein davon.

Sich dafür interessieren und das Thema als geschäftsrelevant erkennen. Diese Einsicht ist an vielen Orten noch nicht vorhanden.

Ganzheitliche Sichtweise, nicht nur technische Lösungen, auch organisatorische Massnahmen

Das Erhalten einer permanenten Cybersicherheitskultur nach deren Einführung wird innerhalb der Firmen oft vernachlässigt. Dabei wird die lange Liste von Schutzmassnahmen und Verhaltensweisen nicht regelmässig kontrolliert und auf dem neusten Stand gehalten.

- Sich weniger auf das Prinzip Hoffnung verlassen.
- Personal schulen (Organisatorische Massnahmen)

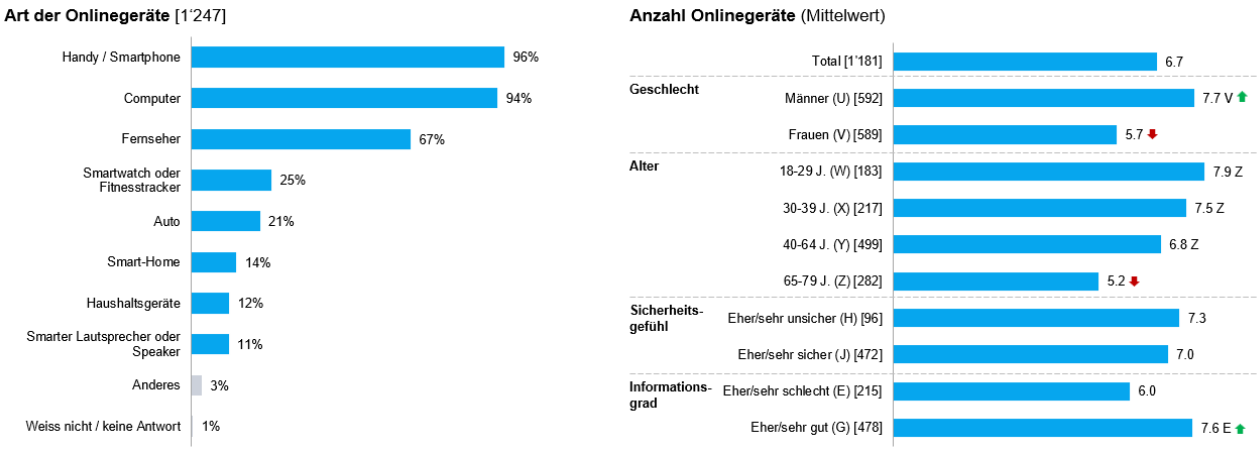
Côté informatique : investir plus dans la cybersécurité et notamment les pentest
Coté organisationnel : Mieux considérer la protection des données et le rôle des DPO. Ce nouveau métier et ses atouts sont délaissés en Suisse en comparaison de nos voisins européens

Um der Nachfrage nachzukommen, sehen die IT-Dienstleiter Herausforderungen in Personalschulungen (25%) bzw. dem Mangel an Fachpersonal (21%). Sie gehen zudem davon aus, dass die Massnahmen vielen zu teuer sein werden (20%). Wenn man sie fragt, was ihre Kunden bezüglich Cybersicherheit besser machen sollten, empfehlen die meisten von ihnen, die Sicherheit ernster zu nehmen (43%) und ihr Personal zu schulen (29%).

5. Zielgruppe Bevölkerung

5.1 Informationsgrad und Sicherheitsgefühl

Je mehr Geräte man hat, die mit dem Internet verbunden sind, desto grösser wird das Risiko von Angriffen über das Internet. Dazu zählen nicht nur Smartphones und Computer, die heutzutage in fast jedem Haushalt anzutreffen sind, sondern auch Fernseher, Autos oder Haushaltgeräte. Durchschnittlich verfügen die Befragten über 6.7 mit dem Internet verbundene Geräte, wobei Männer und jüngere Befragte signifikant mehr Geräte haben als Frauen und ältere Befragte.

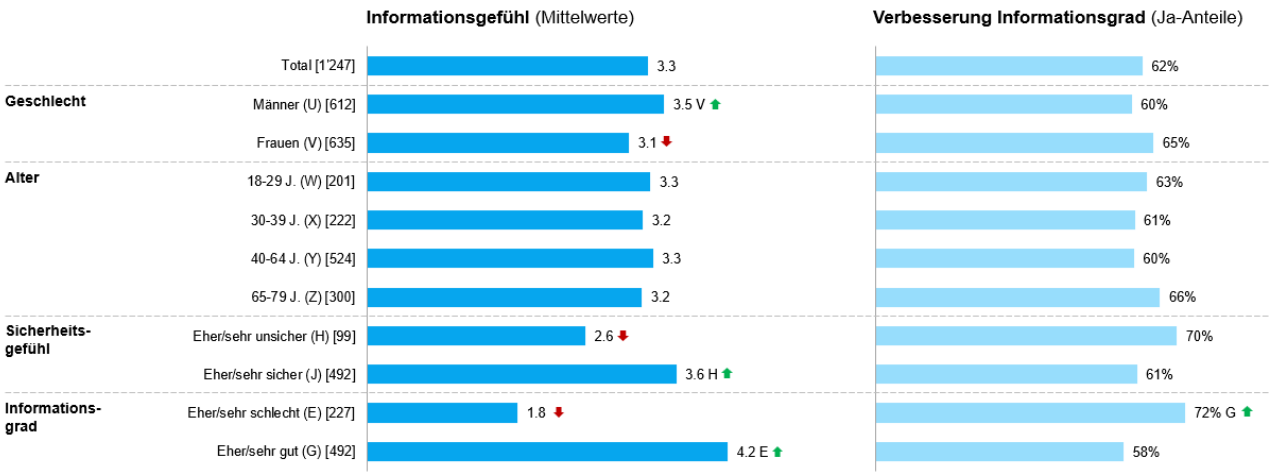


F101: Welche Geräte besitzen Sie, die mit dem Internet verbunden sind? | F102: Was schätzen Sie: Wie viele Geräte besitzen Sie zuhause, die mit dem Internet verbunden sind?
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Frage | ▲ signifikant höher als Total; ▼ signifkant tiefer als Total | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Die Befragten sind mehrheitlich der Meinung, eher bis sehr gut Bescheid zu wissen, wie sie sich vor Cyberangriffen schützen können. Auf der Fünferskala schätzen sie ihren Informationsgrad durchschnittlich auf 3.3. **Fast zwei Drittel (62%) wären gerne besser informiert, besonders diejenigen, die ihren Informationsgrad tief einschätzen.** Genau wie bei den in Teil 1 befragten KMU gilt: **Wer sich gut informiert fühlt, fühlt sich sicherer und verhält sich auch sicherer:** Gut Informierte führen die Updates auf ihren Geräten schneller durch, verwenden mehr verschiedene Passwörter, führen eher regelmässige Backups durch und setzen mehr technische Massnahmen um.

Fast die Hälfte der Befragten beurteilt die Cybersicherheit des eigenen Haushalts als sicher, der Mittelwert liegt bei 3.5 auf der Fünferskala. Auffallend ist eine hohe Unsicherheit bei den 30- bis 39-Jährigen (3.3), insbesondere im Vergleich zu den besonders sicheren über 65-jährigen (3.6). Da die über 65-jährigen am wenigsten Online-Geräte zu Hause haben, könnten sie ihr Sicherheitsgefühl daraus schöpfen.

Etwas mehr als ein Viertel (28%) der Befragten hat schon einmal eine Schulung zum Thema Cybersicherheit besucht. Dabei handelt es sich eher um Männer (35%) und 40- bis 64-jährige (35%). In rund drei Vierteln der Fälle (76%) wurden diese Schulungen vom Arbeitgeber initiiert. Die Wirkung solcher Schulungen sollte nicht unterschätzt werden: Befragte, die eine Schulung besuchten, fühlen sich sehr viel besser informiert (3.8) als ungeschulte Befragte (3.1); und wie oben beschrieben, hängt ein höherer Informationsgrad auch mit sichererem Verhalten zusammen. Arbeitgebende schützen mit Schulungen (wie sie auch von IT-Dienstleistern empfohlen werden) also nicht nur ihr Unternehmen vor Cyberangriffen, sondern haben damit höchstwahrscheinlich auch einen positiven Einfluss auf die Cybersicherheit der Bevölkerung.



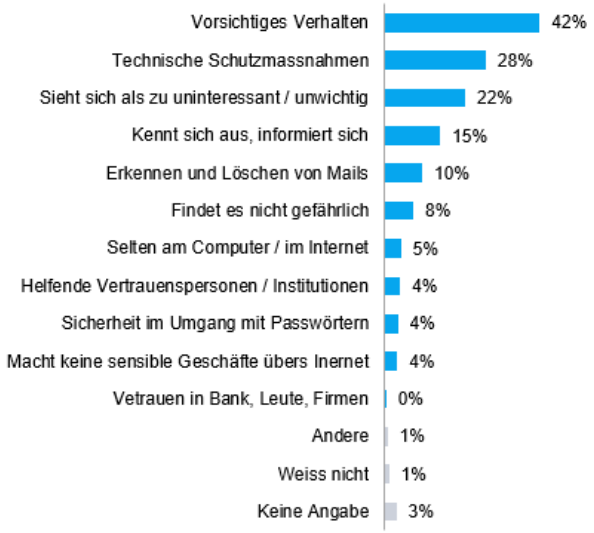
F009: Wie gut wissen Sie im Vergleich zu ihren Kolleginnen und Kollegen Bescheid, wie Sie sich vor Cyberangriffen schützen können? | F010: Wären Sie gerne besser informiert über das Thema Cybersicherheit?
Basis: n=[ ] | Filter: Bevölkerung | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut (F009) & geschlossene Frage (F010) | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

5.2 Cyberkriminalität: Erfahrung und Risikoeinschätzung

Jede/-r zwanzigste Befragte (5%) hat in den letzten drei Jahren einen Cyberangriff erlebt; der Anteil an Betroffenen liegt bei Privatpersonen also ähnlich hoch wie bei IT-Dienstleistern (4%) und KMU (4%). Rund in der Hälfte der Fälle entstand durch den Angriff ein finanzieller Schaden (53%) und/oder emotionale Belastung (49%). Erstaunlich hoch ist die Betroffenheit bei den 18- bis 29-jährigen: Jede/-r zehnte von ihnen erlebte in den letzten 3 Jahren einen Cyberangriff mit Folgen. Trotzdem fühlt sich diese Altersgruppe durchaus sicher: Ihr Sicherheitsgefühl liegt bei 3.5 auf der Fünferskala und sie schätzen das Risiko eines Angriffs in den nächsten zwei bis drei Jahren als eher tief ein (49% eher/sehr tiefes Risiko). Die jüngste Altersgruppe hat zudem schon am häufigsten Lösegeld bezahlt: Zwei von hundert 18- bis 29-Jährigen haben schon einmal Lösegeld

an Cyberkriminelle bezahlt, bei allen Altersgruppen zusammen liegt der Anteil bei einem Prozent. Fast jede/-r zehnte Befragte (9%), der/die in den letzten 1 – 3 Jahren von einem Cyberangriff betroffen war, bezahlte Lösegeld.

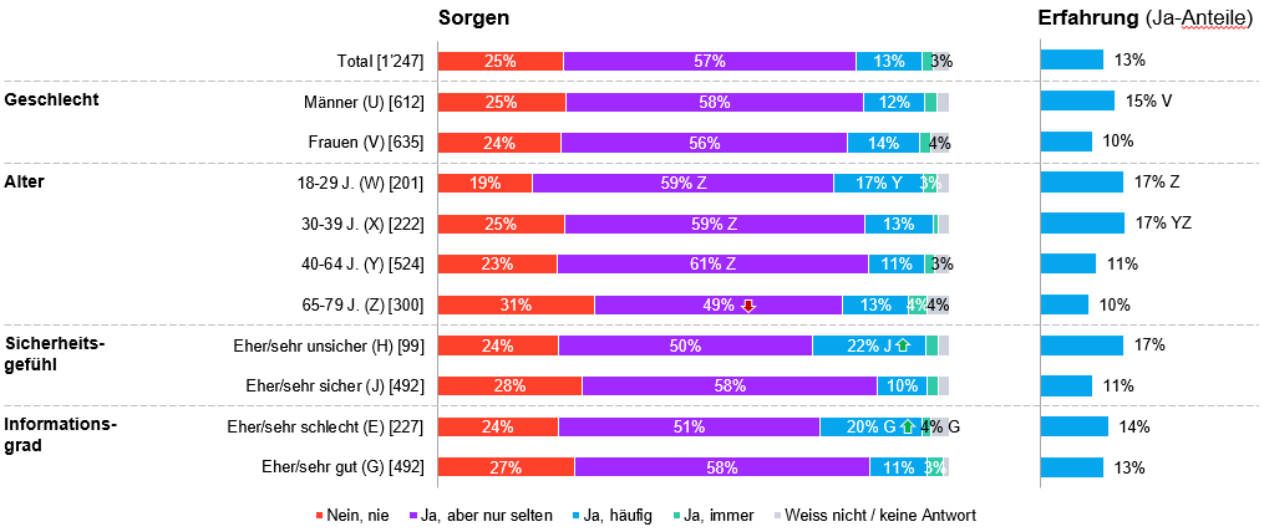
Rund jede/-r sechste Befragte (16%) schätzt das Risiko, innerhalb 2-3 Jahren durch einen Cyberangriff Geld oder Daten zu verlieren, als hoch ein, knapp zwei Fünftel (38%) als klein. Fragt man nach, warum Befragte das Risiko eines Cyberangriffs eher tief einschätzen, antworten sie am häufigsten, dass sie sich vorsichtig verhalten (42%). Die zweithäufigste Antwort bezieht sich auf technische Schutzmassnahmen (28%), rund jede/-r fünfte (22%) sieht sich selbst als zu uninteressant für Cyberangriffe.



F113: Was sind die Gründe dafür, dass Sie dieses Risiko eher tief einschätzen?
Basis: n=[ ] | Filter: siehe oben | offene Frage (F113)

5.3 Onlineshopping

Fast die Hälfte der Befragten (49%) kauft mindestens zwei- bis dreimal pro Monat online ein, weitere 20% monatlich und gut ein Viertel (27%) seltener. Die Bezahlung gegen Rechnung wird dabei als die sicherste Zahlungsmethode betrachtet (43%), gefolgt von der Kredit- oder Debitkarte (18%) und Twint (17%). Knapp drei Viertel (72%) der Befragten machen sich (zumindest selten) Sorgen, auf Onlineshops oder Buchungsplattformen betrogen zu werden, wobei 13 Prozent der Befragten tatsächlich in den letzten fünf Jahren schon einem betrogen wurden in dem Sinne, dass sie für etwas bezahlten, dies dann aber nicht erhielten.



F122: Haben Sie sich schon Sorgen gemacht, dass Sie auf Onlineshops oder Buchungsplattformen betrogen werden, dass also die Webseite oder das Angebot nicht echt ist?
F123: Wurden Sie in den letzten fünf Jahren in einem Onlineshop oder auf einer Buchungsplattform betrogen in dem Sinne, dass Sie für etwas bezahlten, dies dann aber nicht bekamen?
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Fragen | ⇧signifikant höher als Total; ⇩ signifkant tiefer als Total | Datenbeschriftung ab 3% | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.