Homeoffice und Cybersicherheit in Schweizer KMU

Strategien und Massnahmen in Schweizer KMU mit 4–49 Mitarbeitenden in 2023

Marc K. Peter, Kristof A. Hertig, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian & Nicole Wettstein

Die KMU-Transformation nach Covid-19

Studie Nr. 4

die Mobiliar
satw
digitalswitzerland
ALLIANZ DIGITALE SICHERHEIT SCHWEIZ
n|w Fachhochschule Nordwestschweiz Hochschule für Wirtschaft
gfs-zürich MARKT- & SOZIALFORSCHUNG

Impressum

Marc K. Peter, Kristof A. Hertig, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian & Nicole Wettstein:
Homeoffice und Cybersicherheit in Schweizer KMU:
Strategien und Massnahmen in Schweizer KMU
mit 4–49 Mitarbeitenden in 2023
Die Mobiliar, digitalswitzerland, Hochschule für Wirtschaft FHNW,
Schweizerische Akademie der Technischen Wissenschaften SATW,
Allianz Digitale Sicherheit Schweiz ADSS, gfs-zürich
Bern, September 2023

Koordination dieser Publikation: Prof. Dr. Marc K. Peter,
Hochschule für Wirtschaft FHNW (www.fhnw.ch/wirtschaft)
Unter Mitarbeit von Mara Huber und Joël Grosjean (gfs-zh)
sowie Johan Lindeque (Hochschule für Wirtschaft FHNW).

Lektorat und Korrektorat: Julia Gremminger und Anja Eicher,
Polarstern AG, Solothurn & Luzern (www.polarstern.ch)
Gestaltung: Polarstern AG, Solothurn & Luzern (www.polarstern.ch)

Der Foliensatz sowie der detaillierte Schlussbericht können auf den Websites der Studienpartner bezogen werden.

Inhalt

Einleitung und wichtige Erkenntnisse

Im Frühling 2022 wurden die letzten Covid-Massnahmen aufgehoben und die Schweiz kehrte langsam zur Normalität zurück. Aber noch während endlich Entspannung eintrat, startete ein Krieg in Europa. Dieser löste eine drohende Energiemangellage aus. Wieder wurde vermehrt über Homeoffice nachgedacht. Dieses Mal jedoch aufgrund ungeheizter Bürogebäude.

Nötig wurde eine weitere Homeoffice-Phase nicht. Stattdessen erhielt das Thema «Cybercrime» durch den Krieg eine neue Dimension: Angriffe von russischen Hackerinnen und Hackern auf westliche Infrastrukturen machten Schlagzeilen. Und nach der Video-Ansprache Selenskis im Bundeshaus am 15. Juni 2023 betrafen diese auch die Schweiz. Zu diesem Zeitpunkt war die Feldforschung dieser Studie allerdings gerade beendet worden. Auch der grosse Data Breach bei einer Berner Softwarefirma, bei dem der Bund sensible Daten verlor, hatte keinen Einfluss mehr auf die hier vorliegenden Resultate.

Vor diesem Hintergrund wurde die vierte Studie zu den Auswirkungen der Covid-19-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU durchgeführt. Es wurden 502 Geschäftsführende von KMU mit 4 bis 49 Mitarbeitenden telefonisch befragt.

In zwölf Kapiteln mit zwölf Grafiken fassen wir die wichtigsten Studienresultate zusammen. Der vollständige Projektbericht kann auf den Websites der Projektpartner bezogen werden (siehe Kasten).

1. **Wie viele Ihrer Mitarbeitenden könnten theoretisch im Homeoffice arbeiten?**
Seit 2020 hat die Anzahl Homeoffice-tauglicher Stellen von Jahr zu Jahr abgenommen. Die Zahl der KMU, in denen ein Teil der Mitarbeitenden oder alle Mitarbeitenden von zu Hause aus arbeiten können, ist von 67 % (in 2020) auf 56 % (in 2023) gesunken.

2. **Wie viele Ihrer Mitarbeitenden arbeiten im Homeoffice?**
In denjenigen Unternehmen, in denen es das Homeoffice gibt, arbeiten rund zwei Fünftel (42 %) der Mitarbeitenden teilweise oder hauptsächlich zu Hause. Genf und Zürich fallen – wie bereits in den Vorstudien – als besonders Homeoffice-freundlich auf.

3. **Wie geht es in Ihrem Unternehmen weiter mit dem Homeoffice?**
In 2023, nach dem Ende sämtlicher Pandemiemassnahmen, erwarten fast drei Viertel der Befragten (73 %), dass der Homeoffice-Anteil langfristig gleichbleiben wird. Es scheint, als hätte sich die Homeoffice-Nutzung im aktuellen Umfang in den meisten KMU etabliert.

4. **Welche digitalen Kommunikationsmittel sind in Ihrem Unternehmen im Einsatz?**
Die Verwendung sämtlicher Kommunikationstechnologien wurde 2023 tiefer eingeschätzt als noch 2022. Onlinekonferenz-Tools werden gemäss den befragten Geschäftsführenden seltener (45 %) verwendet als 2022 (62 %) und 2021 (64 %).

5. **Nutzen Sie einen IT-Dienstleister?**
Die grosse Mehrheit der KMU (79 %) lässt sich von externen IT-Dienstleistern unterstützen. KMU, die über mindestens einen externen IT-Dienstleister verfügen, vergeben rund einen Drittel (36 %) ihrer IT-Arbeiten auswärts. Die Hälfte der IT-Dienstleister verfügt bereits über eine IT-Sicherheitszertifizierung.

6. **Wie zufrieden sind Sie mit Ihrem IT-Dienstleister?**
Rund jedes siebte KMU (14 %) hat in den letzten ein bis zwei Jahren einen bestehenden IT-Dienstleister ersetzt. Neun von zehn KMU (91 %), die ihren Dienstleister nicht gewechselt hatten, gaben an, mit diesem (sehr) zufrieden zu sein. Die besten Noten erhielten die IT-Dienstleister für ihre gute Erreichbarkeit und schnelle Reaktionszeit.

7. **Wurden Sie bereits von Cyberkriminellen angegriffen?**
Jedes zehnte KMU (11 %) wurde bereits erfolgreich von Cyberkriminellen angegriffen, und zwar so, dass ein erheblicher Aufwand nötig war, um die Schäden zu beheben. Über die Hälfte (55 %) der Befragten, die schon einmal attackiert worden waren, beklagte einen finanziellen Schaden. Rund ein Achtel (13 %) gab an, Kundendatenverluste beziehungsweise Reputationsschäden erlitten zu haben.

8. Wie schätzen Sie die Cyberkriminalität ein?
Gemäss den Befragten ist Cyberkriminalität ein ernstzunehmendes Problem (Mittelwert von 4.7 auf der 5er-Skala). Auch anerkennen sie die Massnahmen gegen Cyberattacken als wichtig (4.5). Je aufgeschlossener die KMU gegenüber Technologien eingestellt sind, desto höher werden sowohl die Gefahren als auch die Notwendigkeit von Massnahmen bewertet.

9. Sind Sie über das Thema Cybersicherheit informiert?
Etwas mehr als die Hälfte (56%) der befragten Geschäftsführenden fühlt sich eher oder sehr gut informiert (Skalenwerte 4–5 auf der 5er-Skala). Knapp zwei Drittel (65%) der Befragten schätzen das Thema Cybersicherheit als eher oder sehr wichtig ein. Rund ein Siebtel (14%) empfindet die Cybersicherheit hingegen als eher oder sehr unwichtig.

10. Welche technischen Massnahmen werden in Ihrem Unternehmen umgesetzt?
Die Umsetzungsgrade der verschiedenen abgefragten Massnahmen liegen mit 3.9 und 4.5 (auf der 5er-Skala) verglichen mit den letzten zwei Jahren allesamt auf praktisch unverändert hohem Niveau. Digitale Pioniere haben mehr Massnahmen umgesetzt als Early Followers und diese mehr als Late Followers.

11. Welche organisatorischen Massnahmen werden in Ihrem Unternehmen umgesetzt?
Wie schon in den Vorjahren festgestellt werde konnte, werden organisatorische Massnahmen immer noch deutlich weniger umgesetzt als technische. Die beiden am seltensten umgesetzten organisatorischen Massnahmen sind die regelmässige Mitarbeitendenschulung (2.9 auf der 5er-Skala) und die Durchführung eines Sicherheitsaudits (2.8).

12. Wie sieht die Zukunft zum Thema Cybersicherheit in Ihrem Unternehmen aus?
Rund die Hälfte (52%) der Befragten hält es für eher oder sehr wahrscheinlich, dass sie in den nächsten ein bis drei Jahren ihre Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden. Die besser Informierten zum Thema Cybersicherheit planen mehr Massnahmen gegen die Cyberkriminalität (3.6 auf der 5er-Skala) als die weniger Informierten (3.0).

Mit dieser Studie begleiten wir KMU seit vier Jahren. Homeoffice, Cybersicherheit und die Zusammenarbeit mit IT-Dienstleistern sind Herausforderungen und Erfolgsfaktoren zugleich. KMU, welche diese Themen proaktiv planen und umsetzen, werden ihre digitalen Strategien erfolgreicher umsetzen können und haben gleichzeitig geringere Risiken.

Wir hoffen, mit diesem Bericht und den detaillierten Studienergebnissen zu Ihrer persönlichen Bestandesaufnahme, zu Ihrem Verständnis und zur Stärkung Ihres KMU beizutragen.

Bern, im September 2023

Marc K. Peter
Leiter Kompetenzzentrum Digitale Transformation
Hochschule für Wirtschaft FHNW, Olten

Kristof A. Hertig
Program Lead Infrastructure & Cybersecurity
digitalswitzerland, Zürich

Andreas W. Kaelin
Geschäftsführer Allianz Digitale Sicherheit Schweiz ADSS, Zug
Senior Advisor digitalswitzerland, Zürich

Karin Mändli Lerch
Projektleiterin
gfs-zürich, Zürich

Patric Vifian
Marketing Manager KMU
Die Mobiliar, Bern

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
Schweizerische Akademie der Technischen Wissenschaften SATW, Zürich

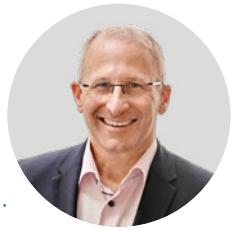
Der komplette Forschungsbericht mit allen Daten und Tabellen kann auf den Websites der Forschungspartner kostenlos als PDF bezogen werden:

www.cyberstudie.ch
www.digitalswitzerland.com
www.kmu-transformation.ch
www.satw.ch
www.mobiliar.ch/kmu-studie

1. «Wie viele Ihrer Mitarbeitenden könnten theoretisch im Homeoffice arbeiten?»

Praxisfrage an KMU:

Wird das Homeoffice von Ihren Mitarbeitenden gewünscht und wenn ja, haben Sie ein Arbeitswelt-Konzept entwickelt, welches die Spielregeln definiert?



Marc K. Peter, FHNW-HSW

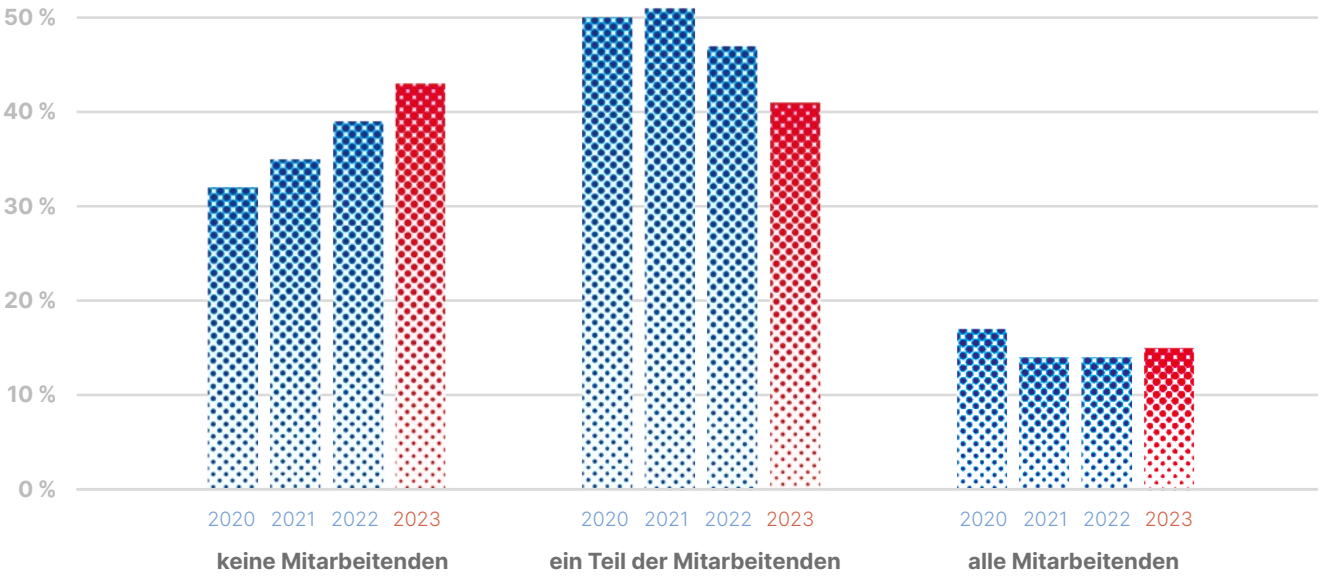
Als diese Studie 2020 erstmals durchgeführt wurde, war gerade die erste Phase der Homeoffice-Pflicht (Covid-19) vorüber. Damals sagte rund ein Drittel (32 %) der befragten KMU-Geschäftsführenden, dass keine ihrer Mitarbeitenden theoretisch im Homeoffice arbeiten könnten.

Seit 2020 hat die Anzahl Homeoffice-tauglicher Stellen von Jahr zu Jahr abgenommen.

Die Hälfte (50 %) gab an, ein Teil der Mitarbeitenden könne im Homeoffice arbeiten. Rund ein Sechstel (17 %) erklärte, dass alle Mitarbeitenden theoretisch im Homeoffice arbeiten könnten.

In 2023 sagten mehr als zwei Fünftel (43%) der Befragten, dass es bei ihnen keine einzige Homeoffice-taugliche Stelle gäbe. Weitere rund zwei Fünftel (41%) bezeichneten einen Teil ihrer Arbeitsstellen als Homeoffice-tauglich. Rund ein Siebtel (15%) der Befragten gab an, alle Mitarbeitenden könnten theoretisch im Homeoffice arbeiten.

Der Rückgang von 2020 bis 2023 ist signifikant. Die Autorenschaft geht davon aus, dass die Arbeitgebenden ihre positive Einstellung gegenüber dem Homeoffice über die letzten Jahre immer wie mehr verloren und deshalb immer weniger ihrer Arbeitsstellen heute als «theoretisch Homeoffice-tauglich» bezeichnen. Das bedeutet aber nicht, dass die effektive Menge an Homeoffice-Tätigkeit in der Schweiz gesunken ist.



Anzahl Mitarbeitende von 2020 bis 2023, die theoretisch von zu Hause aus arbeiten könnten, da sie zum Beispiel keine Kundinnen und Kunden vor Ort bedienen, kein Fahrzeug lenken oder nicht auf einer Baustelle arbeiten.

2. «Wie viele Ihrer Mitarbeitenden arbeiten im Homeoffice?»

Praxisfrage an KMU:

Möchten Sie, dass Ihre Mitarbeitenden wieder vermehrt im Büro sind? Wenn ja, was bieten Sie ihnen an, damit das Arbeiten im Büro attraktiv ist?

Karin Mändli Lerch, gfs-zh

Wie schon in den letzten Jahren gilt noch immer: Bei den kleinsten KMU ist der Anteil an Mitarbeitenden im Homeoffice am grössten: Bei KMU mit vier bis neun Mitarbeitenden arbeiten je rund ein Viertel (24% beziehungsweise 25%) der Mitarbeitenden teilweise beziehungsweise hauptsächlich im Homeoffice. Insgesamt ist also fast die Hälfte (49%) der Mitarbeitenden in dieser Grössenkategorie zumindest teilweise im Homeoffice tätig.

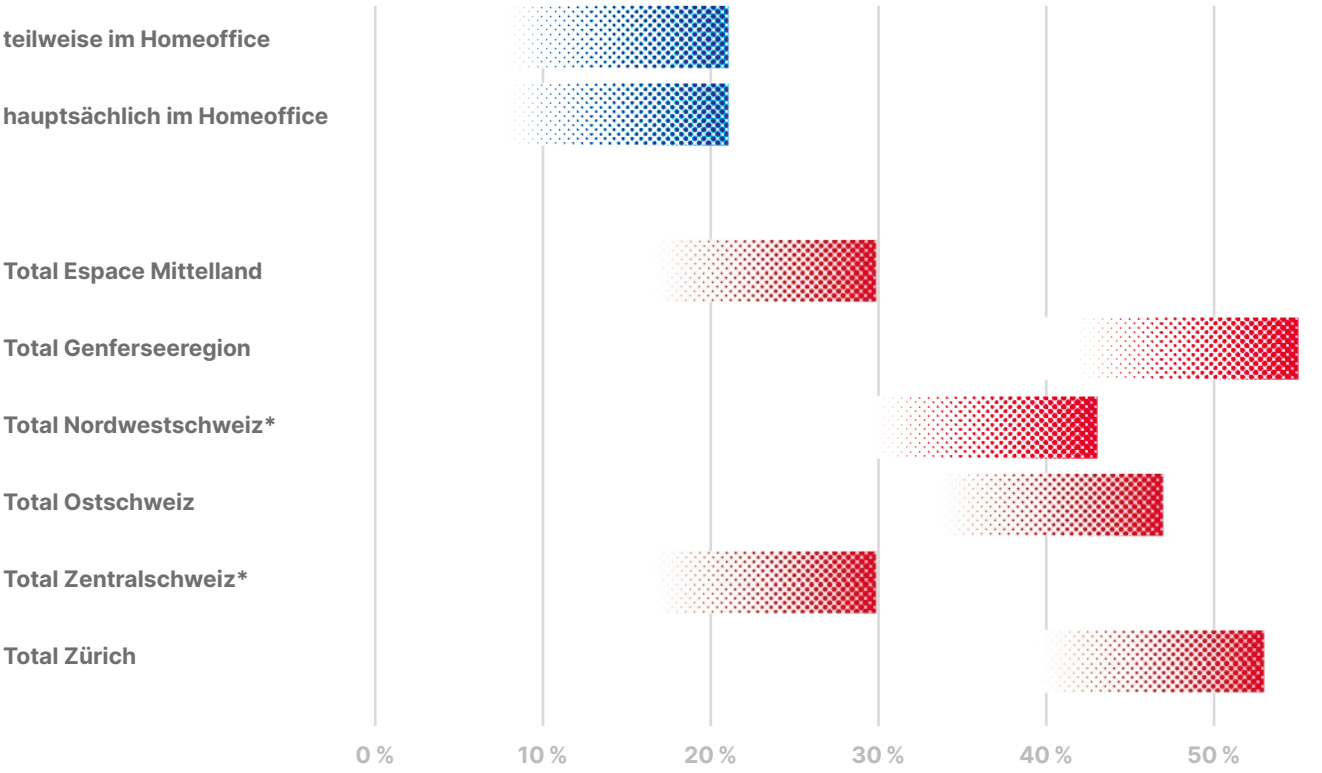
Rund zwei Fünftel (42 %) der Mitarbeitenden arbeiten teilweise oder hauptsächlich im Homeoffice (in denjenigen Firmen, in denen mindestens eine Person von zu Hause arbeiten kann).

In KMU mit 10 bis 19 Mitarbeitenden arbeitet je rund ein Siebtel (14%) teilweise oder hauptsächlich im Homeoffice. Bei KMU mit 20 bis 49 Mitarbeitenden sind es je rund ein Sechstel (18% beziehungsweise 17%) der Mitarbeitenden, die teilweise beziehungsweise hauptsächlich im Homeoffice arbeiten.

In der neusten Umfrage wurden die Antwortmöglichkeiten unterteilt in «teilweise» und «hauptsächlich», was eine andere Einschätzung und somit ein anderes Antwortverhalten der Befragten zur Folge gehabt haben könnte.

Nach dem Lockdown 2020 arbeiteten noch 16% der Mitarbeitenden der befragten Geschäftsführenden hauptsächlich im Homeoffice. Nach der Homeoffice-Pflicht 2021 waren es noch 20% und nach der Homeoffice-Pflicht 2022 nur noch 12%. 2023 sind es wieder 21% und somit fast doppelt so viele wie nach dem «Taucher» 2022 beziehungsweise fast gleich viele wie 2021. Die Autorenschaft vermutet, dass sich über die letzten drei Jahre eine neue Interpretation des Begriffs «hauptsächlich» entwickelt hat.

Genf und Zürich fallen – wie bereits in den Vorstudien – als besonders Homeoffice-freundlich auf.

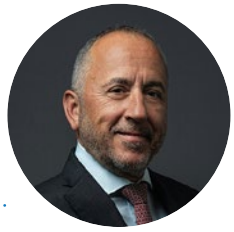


Anzahl Mitarbeitende (in Prozent des Totals der Mitarbeitenden), die teilweise und hauptsächlich im Homeoffice arbeiten (in KMU, in welchen mindestens eine Person von zu Hause aus arbeiten kann) (das Tessin hat als Subgruppe < 20 Studienteilnehmende und ist deshalb nicht ausgewiesen).

3. «Wie geht es in Ihrem Unternehmen weiter mit dem Homeoffice?»

Praxisfrage an KMU:

In welchem Umfang planen Sie die Homeoffice-Nutzung in Ihrem KMU? Gehen Sie davon aus, dass sich die Situation nach Covid-19 wieder eingependelt hat?

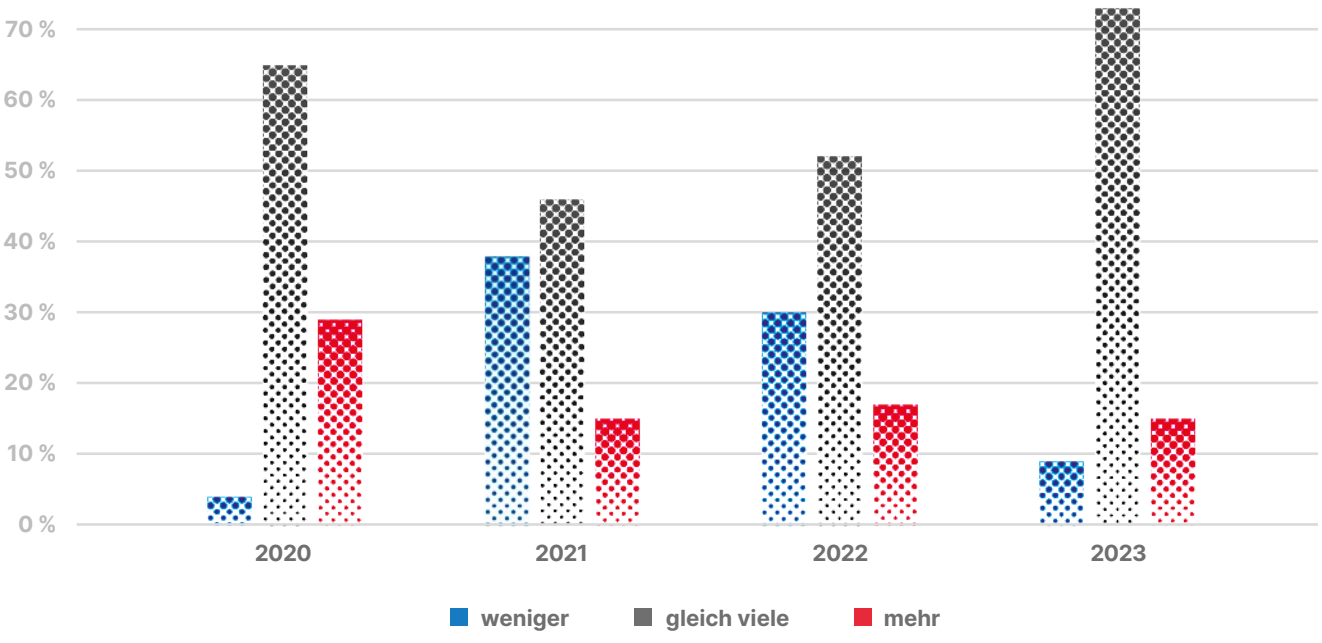


Andreas W. Kaelin, ADSS

Die Einschätzung, wie sich der Anteil an Mitarbeitenden im Homeoffice langfristig verändern wird, hat sich seit 2020 stetig verändert. Kurz nach der ersten Homeoffice-Pflichtphase, welche mit dem generellen Lockdown einherging, erwartete fast ein Drittel (29%) der befragten Geschäftsführenden eine langfristige Steigerung des Homeoffice-Anteils. Nach der zweiten Homeoffice-Pflichtphase 2021 ging hingegen mehr als ein Drittel (38%) der Befragten davon aus, dass es langfristig weniger Mitarbeitende im Homeoffice geben würde und nur noch rund jede beziehungsweise jeder siebte Befragte (15%) erwartete eine Steigerung. In 2022 rechnete knapp ein Drittel (30%) mit einer Reduktion des Homeoffice-Anteils, während knapp ein Sechstel (17%) eine Steigerung erwartete.

Nur noch rund jede beziehungsweise jeder Zehnte (9%) erwartet eine Reduktion und weiterhin rund jede beziehungsweise jeder Siebte eine Steigerung. Es scheint somit, als habe sich die Situation etwas eingependelt, und dies in sämtlichen Subgruppen in ähnlichem Mass.

In 2023, nach dem Ende sämtlicher Pandemiemassnahmen, erwarten fast drei Viertel der Befragten (73 %), dass der Homeoffice-Anteil nun langfristig gleichbleiben wird.



Einschätzung, ob im KMU in Zukunft mehr, gleich viele oder weniger Mitarbeitende von zu Hause aus arbeiten werden (in KMU, in welchen mindestens eine Person von zu Hause aus arbeiten kann).

4. «Welche digitalen Kommunikationsmittel sind in Ihrem Unternehmen im Einsatz?»

Praxisfrage an KMU:

Wie setzen Sie Kommunikationstechnologien ein? Gibt es ein Konzept für eine effizientere Kommunikation? Und: Berücksichtigen Sie dabei das Thema Cybersicherheit?

Nicole Wettstein, SATW

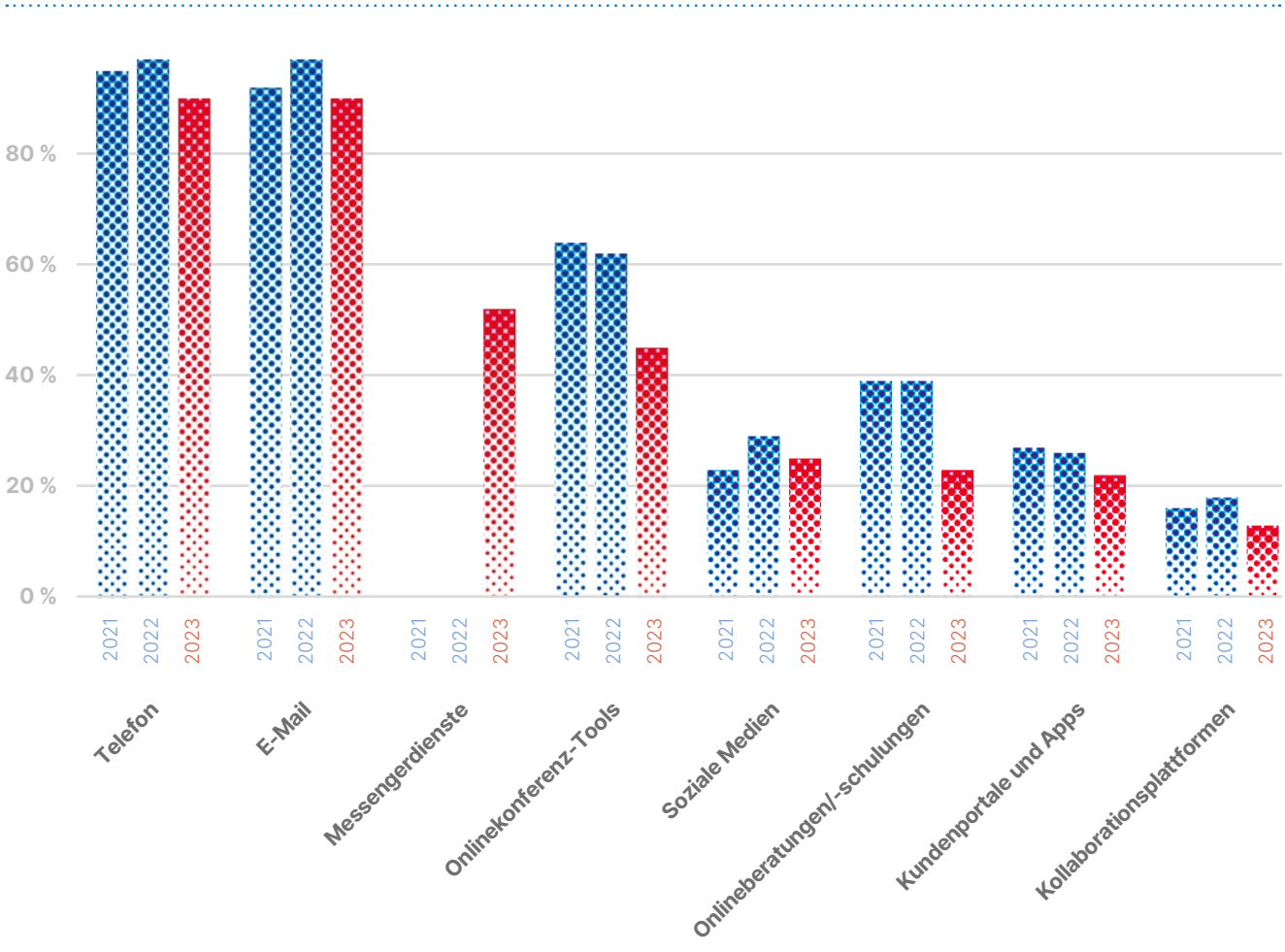
Telefon und E-Mail (je 90 %) sind – wie schon in den Vorgängerstudien – auch 2023 die am häufigsten verwendeten Kommunikationsmittel der befragten KMU. Gegenüber den Vorgängerstudien gibt es nur marginale Veränderungen.

Die Verwendung sämtlicher Kommunikationstechnologien wurde 2023 tiefer eingeschätzt als noch 2022. Auffallend wird dies insbesondere bei den Messengerdiensten wie WhatsApp, Signal, Threema, Wire und so weiter, welche in den Vorjahren noch separat abgefragt wurden: WhatsApp alleine wurde in den Vorgängerstudien von fast zwei Dritteln (60 % in 2022 und 62 % in 2021) genannt. In der vorliegenden Befragung wurde sie, zusammen mit Signal, Threema, Wire et cetera, nur von rund der Hälfte (52 %) der Befragten erwähnt.

Ebenfalls stark zurückgegangen ist die Anwendung von Onlineberatungen oder -schulungen (2021: 39 %, 2022: 39 %, 2023: 23 %) sowie die Nutzung von Kollaborationsplattformen wie Slack, Confluence oder SharePoint. Im Durchschnitt wurden 3.6 verschiedene Kommunikationsmittel angegeben.

Auch Onlinekonferenz-Tools wie Skype, Teams, Zoom oder Google Meet werden gemäss den befragten Geschäftsführenden seltener (45 %) verwendet als 2022 (62 %) und 2021 (64 %).

Je mehr Mitarbeitende theoretisch im Homeoffice arbeiten könnten, desto mehr Kommunikationsmittel werden in den befragten KMU verwendet.

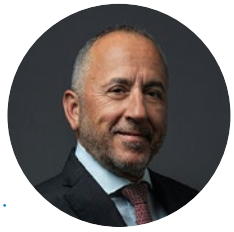


Einsatz digitaler Kommunikationsmittel in Schweizer KMU von 2021 bis 2023.

5. «Nutzen Sie einen IT-Dienstleister?»

Praxisfrage an KMU:

Verfügt Ihr IT-Dienstleister über eine Sicherheits-zertifizierung? Wenn nicht, wie überprüfen Sie seine Kompetenzen in Bezug auf Cybersicherheit?



Andreas W. Kaelin, ADSS

Dieses Jahr fragten wir die KMU zum ersten Mal, ob sie mit einem IT-Dienstleister zusammenarbeiten. Die meisten arbeiten mit einem einzelnen IT-Dienstleister (44%) zusammen. Rund ein Drittel wird von mehreren IT-Dienstleistern (35%) unterstützt. Rund jede beziehungsweise jeder fünfte Geschäftsführende gab an, über keinen IT-Dienstleister (21%) zu verfügen.

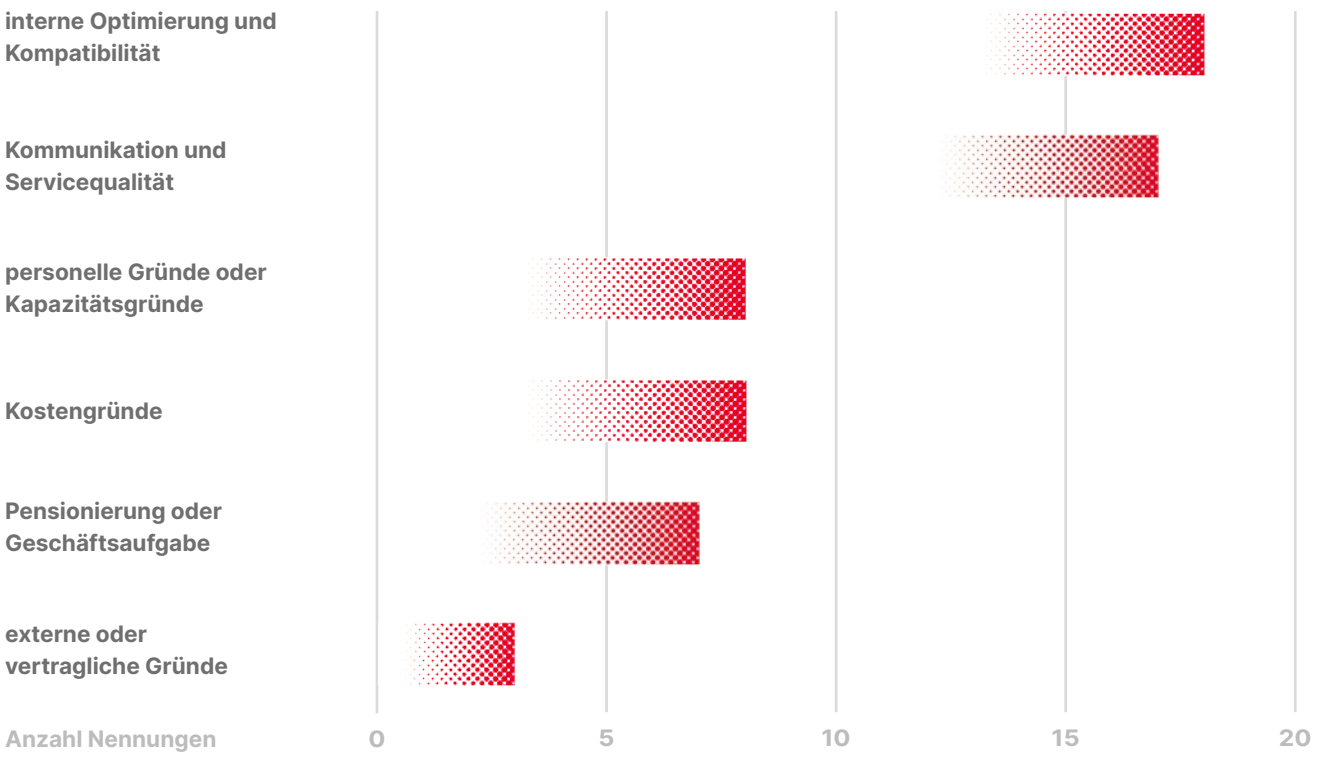
KMU, die über mindestens einen externen IT-Dienstleister verfügen, vergeben rund einen Drittel (36%) der IT-Arbeiten auswärts. Bei der Mehrheit (84%) der KMU, die angaben, mit mindestens einem externen IT-Dienstleister zusammenzuarbeiten, berät und unterstützt dieser das KMU auch bezüglich Cybersicherheit.

Damit hat sich dieser Anteil an sicherheitszertifizierten IT-Dienstleistern gegenüber 2022 kaum verändert. Auffallend diesbezüglich ist der hohe Anteil an Befragten (34%), welche die Frage nicht beantworten wollten oder konnten.

KMU, die in den letzten ein bis zwei Jahren einen bestehenden IT-Dienstleister durch einen neuen ersetzt haben, nahmen den Wechsel vor allem aus internen Optimierungs- und Kompatibilitätsgründen (zum Beispiel wegen des Kaufs einer neuen Software oder eines neuen Servers) sowie aufgrund von Unzufriedenheit bezüglich Kommunikation und Service-Qualität vor. Auch genannt wurden personelle, Kapazitäts- oder Kostengründe. Für die meisten KMU (64%) scheint dieser Wechsel (sehr) einfach gewesen zu sein.

Die Hälfte (53 %) der IT-Dienstleister verfügt über eine IT-Sicherheitszertifizierung wie zum Beispiel ISO 27001 oder CyberSeal.

Rund jedes siebte KMU (14 %) hat in den letzten ein bis zwei Jahren einen bestehenden IT-Dienstleister ersetzt.

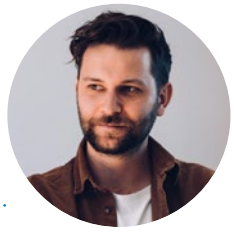


Gründe in 2023 (Anzahl Nennungen), weshalb Geschäftsführende in den letzten ein bis zwei Jahren einen bestehenden IT-Dienstleister ersetzten (in KMU, welche in den letzten ein bis zwei Jahren einen IT-Dienstleister ausgetauscht haben; mehrere Antworten möglich).

6. «Wie zufrieden sind Sie mit Ihrem IT-Dienstleister?»

Praxisfrage an KMU:

IT-Dienstleister können als strategische Partner viel Mehrwert liefern. Haben Sie sich bereits überlegt, wie Sie durch Ihren IT-Dienstleister effizienter werden könnten?



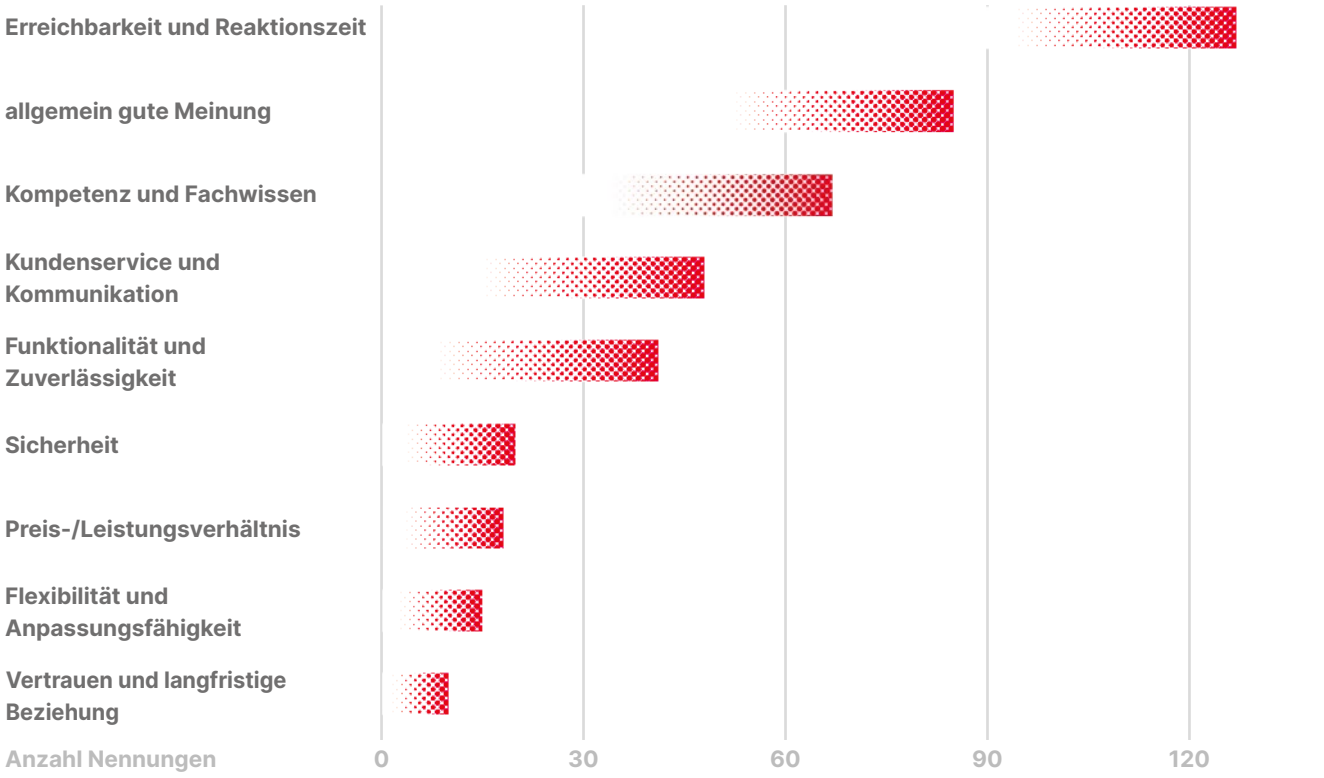
Kristof A. Hertig, digitalswitzerland

Bei KMU, welche ihren IT-Dienstleister nicht ersetzt haben, ist die Zufriedenheit mit diesem sehr hoch:

Neun von zehn KMU (91 %) gaben an, mit ihrem IT-Dienstleister (sehr) zufrieden zu sein.

Der Mittelwert liegt somit bei 4.5 auf einer Skala von 1 (sehr unzufrieden) bis 5 (sehr zufrieden). Spannendes Detail: KMU mit einem hohen Umsetzungsgrad an technischen und organisatorischen Massnahmen zur Steigerung der Cybersicherheit sind signifikant häufiger zufrieden mit ihrem IT-Dienstleister als KMU mit einem tieferen Umsetzungsgrad.

Die häufigsten Gründe, weshalb KMU mit ihrem IT-Dienstleister zufrieden sind, sind die Erreichbarkeit und Reaktionszeit, die gute Reputation («allgemein gute Meinung») sowie die Kompetenz und das Fachwissen des IT-Dienstleisters.



Gründe in 2023, weshalb Geschäftsführende mit ihrem IT-Dienstleister zufrieden sind (in KMU, welche in den letzten ein bis zwei Jahren ihren IT-Dienstleister nicht ersetzt haben).

7. «Wurden Sie bereits von Cyberkriminellen angegriffen?»

Praxisfrage an KMU:

Jedes zehnte KMU wurde bereits erfolgreich angegriffen. Verfügen Sie über ein Notfallkonzept für den Fall eines Cyberangriffs?

Karin Mändli Lerch, gfs-zh

Rund jede beziehungsweise jeder zehnte Befragte (11 %) sagte, dass das eigene KMU schon einmal erfolgreich von Cyberkriminellen angegriffen worden sei, und zwar so, dass ein erheblicher Aufwand nötig war, um die Schäden zu beheben.

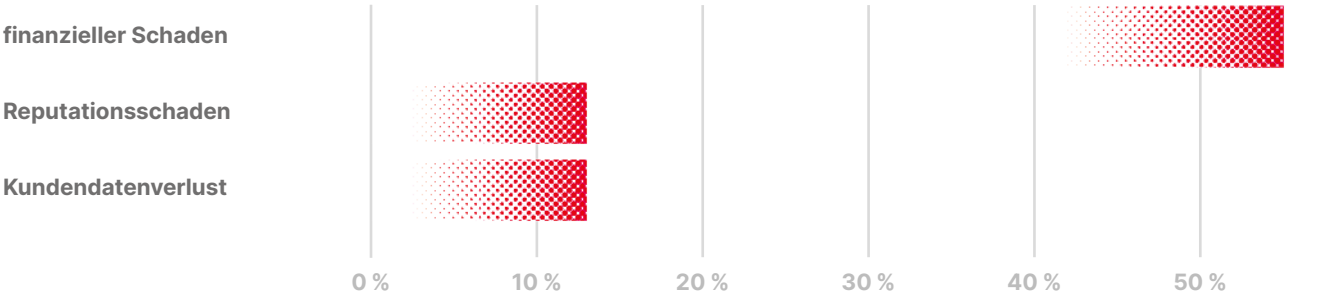
Es gibt keine Unterschiede in den Branchen: Cyberangfriffe können jedes KMU treffen.

Über die Hälfte (55 %) der Befragten, die schon einmal attackiert worden waren, beklagte einen finanziellen Schaden. Dies entspricht rund 6 % der Gesamtstichprobe und würde bedeuten, dass 6 % der Schweizer KMU mit 4 bis 49 Mitarbeitenden schon einmal einen finanziellen Schaden durch einen Cyberangriff erlitten haben.

Einen Kundendatenverlust beziehungsweise einen Reputationsschaden erlitt je rund ein Achtel (13 %) der Befragten, die schon einmal angegriffen worden sind.

Jede beziehungsweise jeder Siebte (14 %) schätzt das Risiko als eher oder sehr hoch ein, durch einen Cyberangriff für mindestens einen Tag lang ausser Kraft gesetzt zu werden.

Jede beziehungsweise jeder zehnte Befragte (10 %) sagte, dass das eigene KMU schon einmal von Cyberkriminellen erpresst worden sei.

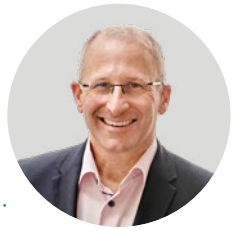


Schäden, welche durch einen erfolgreichen Cyberangriff entstanden sind
(nur bei KMU, die bereits einmal von Cyberkriminellen angegriffen worden sind).

8. «Wie schätzen Sie die Cyberkriminalität ein?»

Praxisfrage an KMU:

Die Gefahren von Cyberkriminellen sind bekannt, die Massnahmenumsetzung dennoch zu tief. Wie könnten Sie motiviert werden, weitere Massnahmen umzusetzen?



Marc K. Peter, FHNW-HSW

Die sieben abgefragten Einstellungsmerkmale zu Cyberkriminalität wurden 2023 fast gleich beantwortet wie in den Vorjahren. Hohe Zustimmung erhalten die Aussagen «Cyberkriminalität ist ein ernstzunehmendes Problem» (4.7), «Massnahmen gegen Cyberattacken sind wichtig» (4.5) und «Mir sind die Bedrohungen durch Cyberkriminalität bewusst» (4.5).

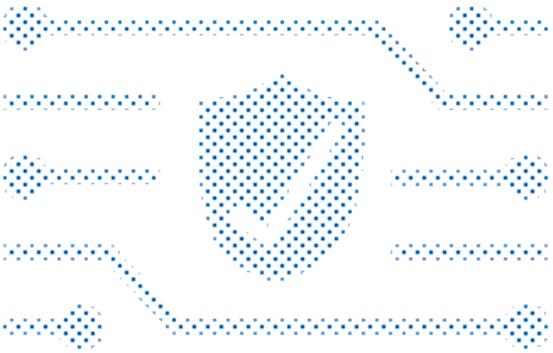
Weniger einverstanden sind die Befragten mit der Aussage «Massnahmen gegen Cyberattacken können einfach umgesetzt werden» (3.4) und «Meine Kolleginnen und Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte» (3.2). Unverändert gegenüber den beiden Vorjahren kann deshalb gesagt werden:

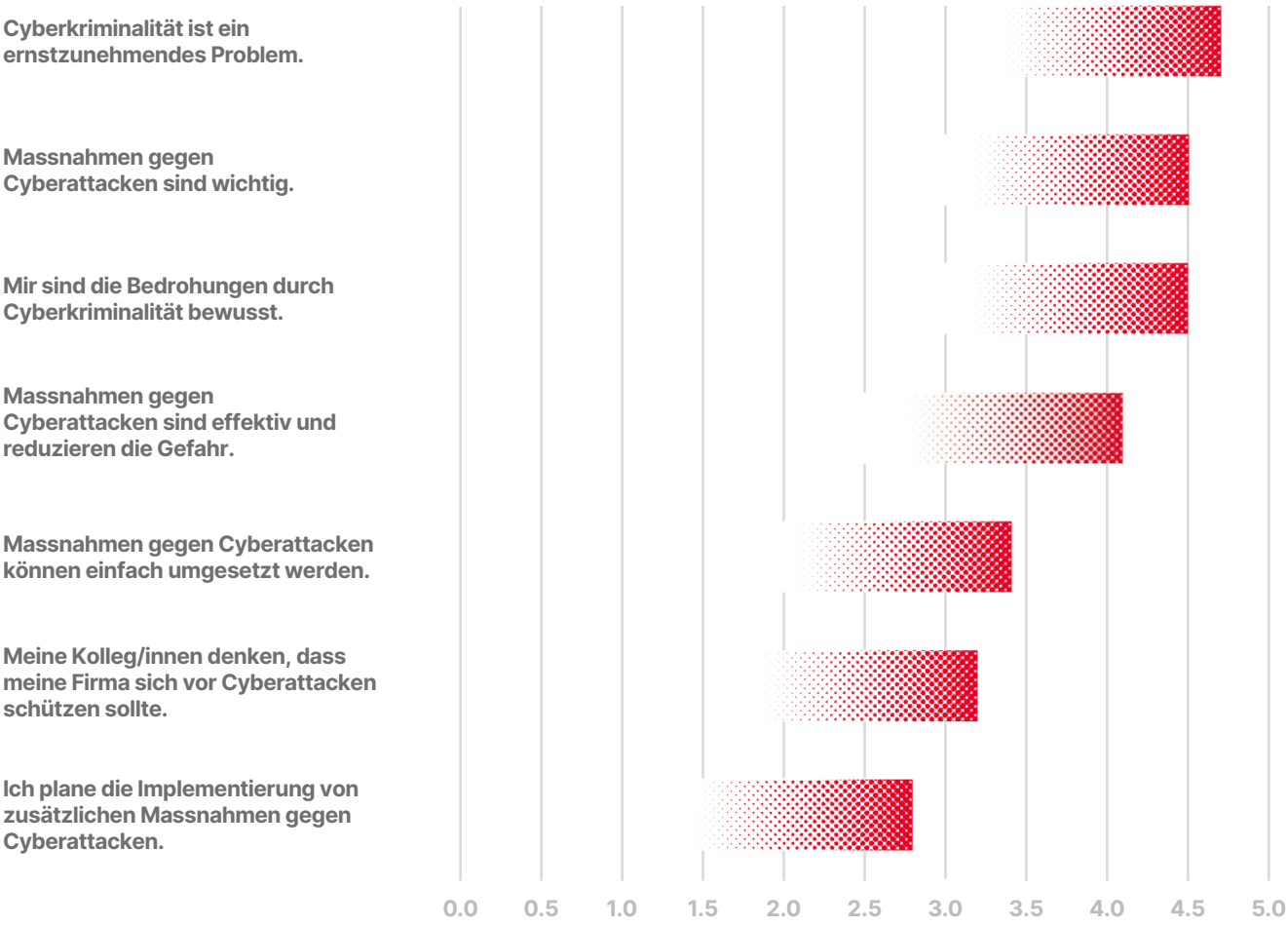
Die Gefahr der Cyberkriminialität wird zwar erkannt, doch Massnahmen dagegen werden nur von einer Minderheit der Befragten geplant.

Gründe gegen die Massnahmen können in deren Umsetzungsschwierigkeit liegen oder darin, dass die Befragten keinen sozialen Druck verspüren innerhalb des KMU (zum Beispiel von Kolleginnen und Kollegen aus der Geschäftsleitung).

Ausserdem gilt bei sämtlichen Aussagen: Je höher die technische oder organisatorische Umsetzung der Sicherheitsmassnahmen, desto höher ist auch die Zustimmung zu den Aussagen.

Zudem gilt: Je aufgeschlossener die KMU gegenüber Technologien eingestellt sind, desto höher ist ihre Zustimmung zu den verschiedenen Aussagen.



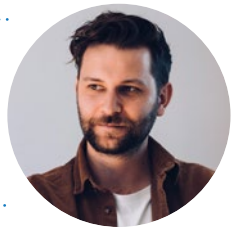


Zustimmung zu diesen Aussagen aus der Perspektive von Schweizer KMU-Geschäftsleitenden (auf der Skala von 1 (überhaupt nicht) bis 5 (voll und ganz)).

9. «Sind Sie über das Thema Cybersicherheit informiert?»

Praxisfrage an KMU:

Cybersicherheit ist allgegenwärtig. Wie gut fühlen Sie sich über das Thema informiert und wie informieren Sie sich? Konferenzen, Weiterbildungen und Gespräch mit Ihrem IT-Dienstleister können Sie unterstützen.



Kristof A. Hertig, digitalswitzerland

Etwas mehr als die Hälfte (56 %) der befragten Geschäftsführenden fühlt sich bezüglich der Cyberrisk-Thematik eher oder sehr gut informiert (Skalenwerte 4–5 auf der 5er-Skala). Dieser Wert hat sich gegenüben der letzten Jahre minimal, aber stetig verbessert (2020: 47 %).

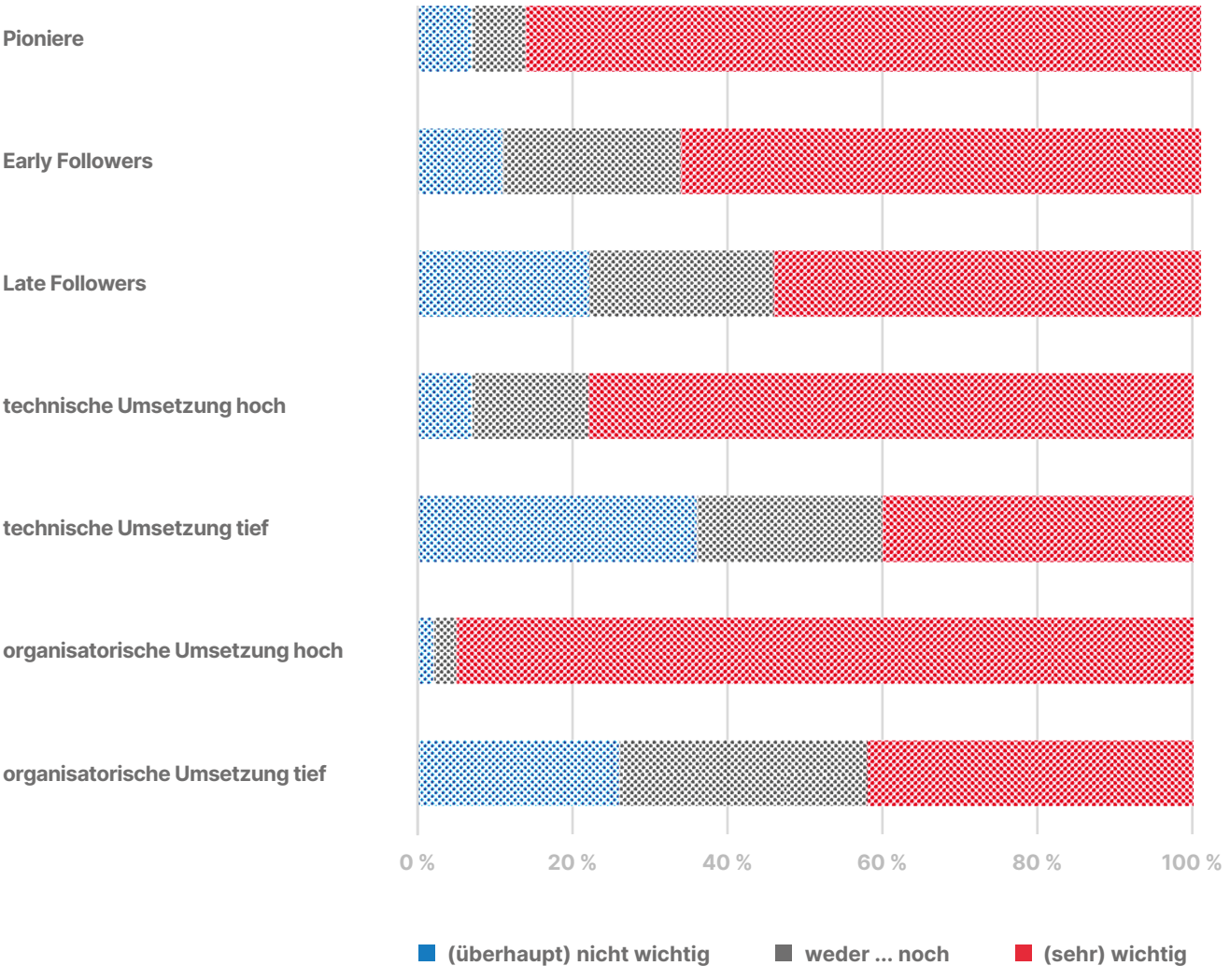
Die Pioniere, welche digitale Technologien früh einsetzen, fühlen sich besser informiert.

Pioniere (4.2) fühlen sich signifikant besser informiert als Early Followers (3.6) und diese wiederum fühlen sich signifikant besser informiert als Late Followers (3.3).

Besonders hoch und ebenfalls signifikant sind die Unterschiede zwischen den KMU, die erst wenige beziehungsweise schon viele technische und organisatorische Sicherheitsmassnahmen umgesetzt haben. Mehr als zwei Drittel (69 %) der Befragten aus Unternehmen mit einer hohen technischen Massnahmenumsetzung fühlen sich gut informiert, jedoch nur rund ein Viertel (26 %) der Befragten aus KMU mit einer geringen technischen Massnahmenumsetzung.

Knapp zwei Drittel (65 %) der Befragten schätzen das Thema Cybersicherheit als eher oder sehr wichtig und rund ein Siebtel (14 %) schätzt es als eher oder sehr unwichtig ein.

Die Wichtigkeit der Cybersicherheit wird seit 2020 praktisch unverändert hoch eingeschätzt.



Einschätzung des Themas Cybersicherheit in 2023 in den Kategorien
(auf der Skala von 1+2 ((überhaupt) nicht wichtig), 3 (weder/noch) bis 4+5 ((sehr) wahrscheinlich)).

10. «Welche technischen Massnahmen werden in Ihrem Unternehmen umgesetzt?»

Praxisfrage an KMU:

Die Pioniere, welche digitale Technologien früh einsetzen, sind besser geschützt. Haben Sie in Ihrem KMU ebenfalls technische Massnahmen umgesetzt?

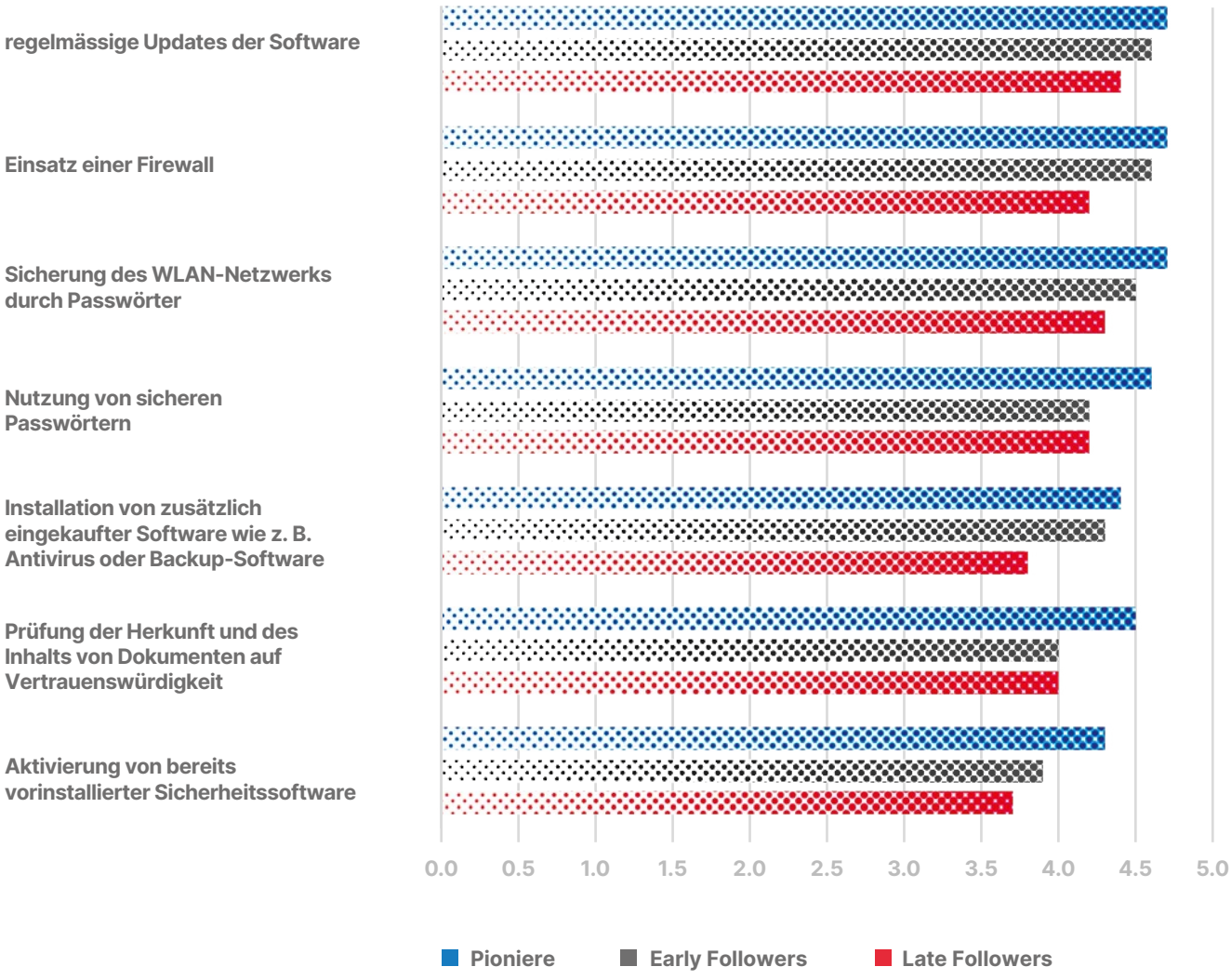
Patric Vifian, Die Mobilar

Die Umsetzungsgrade der verschiedenen abgefragten Massnahmen liegen zwischen 3.9 und 4.5 (auf der 5er-Skala) und allesamt auf praktisch unverändertem Niveau zu 2022 und 2021. Den höchsten Umsetzungsgrad erzielen die beiden Massnahmen «regelmässige Softwareupdates» und «Einsatz einer Firewall» (beide 4.5).

Bei allen Massnahmen gilt in signifikanter Weise (wie schon in den Vorjahren): Je höher der selbst eingeschätzte Informationsgrad zur Cybersicherheit, desto höher ist auch die Massnahmenumsetzung.

Sämtliche Massnahmen wurden von den Firmen mit 20 bis 49 Mitarbeitenden häufiger umgesetzt als von Firmen mit 4 bis 9 beziehungsweise mit 10 bis 19 Mitarbeitenden.

Pioniere haben mehr Massnahmen umgesetzt als Early Followers und diese mehr als Late Followers.



Umsetzung technischer Cybersicherheits-Massnahmen in Schweizer KMU 2023
(auf der Skala von 1 (gar nicht) bis 5 (voll und ganz)).

11. «Welche organisatorischen Massnahmen werden in Ihrem Unternehmen umgesetzt?»

Praxisfrage an KMU:

Die Cybersicherheit ist heute erfolgskritisch. Führen Sie regelmässige Mitarbeitendenschulung und IT-Sicherheits-audits durch?

Nicole Wettstein, SATW

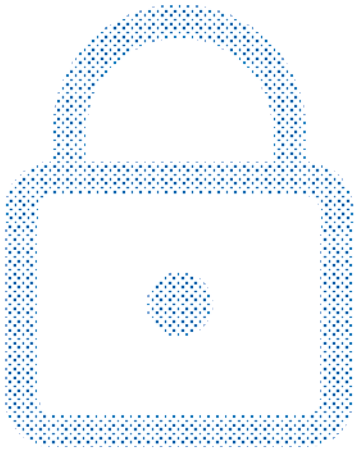
Wie schon in den Vorjahren festgestellt wurde, werden organisatorische Massnahmen immer noch deutlich weniger umgesetzt als technische. Die am häufigsten umgesetzte organisatorische Massnahme ist die Kontrolle der Wiederherstellbarkeit der Datensicherung (4.2), gefolgt vom vorsichtigen Verhalten beim Teilen von persönlichen Informationen (4.2) sowie der Sensibilisierung von Mitarbeitenden auf Phishing-E-Mails (4.0). Die beiden am seltensten umgesetzten organisatorischen Massnahmen sind die regelmässige Mitarbeitendenschulung (2.9) und die Durchführung eines Sicherheitsaudits (2.8).

Die Unterschiede sind alle signifikant (siehe Grafik auf Seite 23).

Je besser sich die Befragten bezüglich dem Thema Cyberrisk informiert fühlen, desto höher ist ihre organisatorische Massnahmenumsetzung. Besonders tief ist der Umsetzungsgrad der regelmässigen Mitarbeitendenschulung bei den (eher) Uninformierten (1.9).

Bei der grossen Mehrheit der organisatorischen Massnahmen verhält es sich so, dass die grösseren KMU sie eher umgesetzt haben als die kleineren.

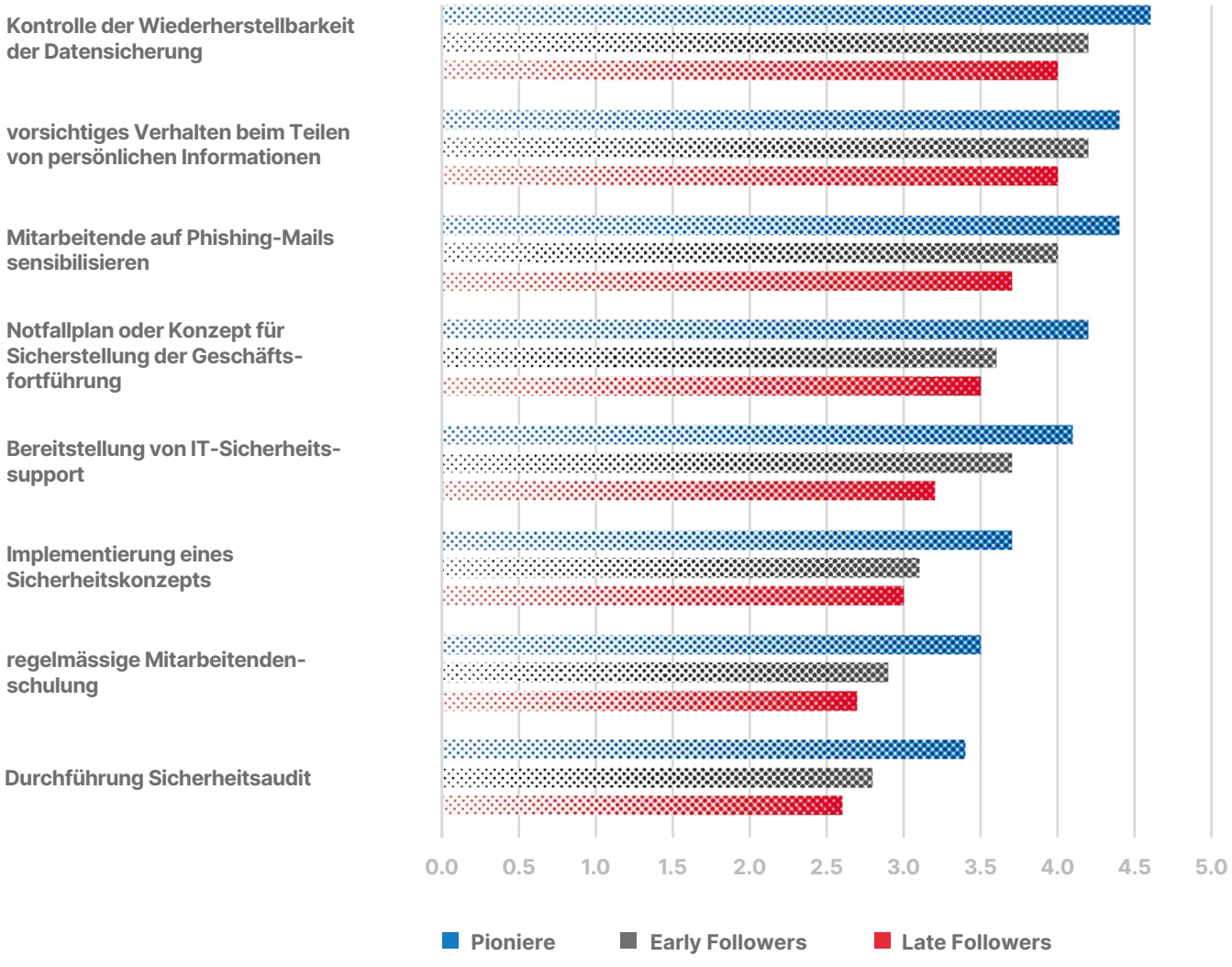
Pioniere haben die meisten organisatorischen Massnahmen umgesetzt, Late Followers die wenigsten.



Gut zu wissen: Passwörter

Fast neun von zehn Befragten (89 %) haben mindestens eine Passwort-Sicherheitsvorkehrung getroffen.
Das heisst aber auch, dass rund jede beziehungsweise jeder Zehnte (11 %) gar keine entsprechenden Vorkehrungen unternommen hat. So werden Passwort-Sicherheitsmassnahmen umgesetzt:

- Regelmässige Erneuerung der Passwörter (60 %)
- Zwei-Faktor-Authentifizierung (60 %)
- Passwort-Mindestlänge von zwölf Zeichen (59 %)
- Unterschiedliche Passwörter pro Service (58 %)
- Passwort-Management-Programm (32 %)



Umsetzung organisatorischer Cybersicherheits-Massnahmen in Schweizer KMU 2023
(auf der Skala von 1 (gar nicht) bis 5 (voll und ganz)).

12. «Wie sieht die Zukunft zum Thema Cybersicherheit in Ihrem Unternehmen aus?»

Praxisfrage an KMU:

Und wie sieht Ihre Zukunft zum Thema Cybersicherheit aus? Sind Sie für die Zukunft gewappnet oder bräuchte es noch mehr Massnahmen zur Erhöhung der IT-Sicherheit?

Patric Vifian, Die Mobilar

Rund die Hälfte (52%) der Befragten hält es für eher oder sehr wahrscheinlich, dass sie in den nächsten ein bis drei Jahren ihre Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen. Das sind fast genau gleich viele wie im Vorjahr (55%) und deutlich mehr als noch 2021 (40%).

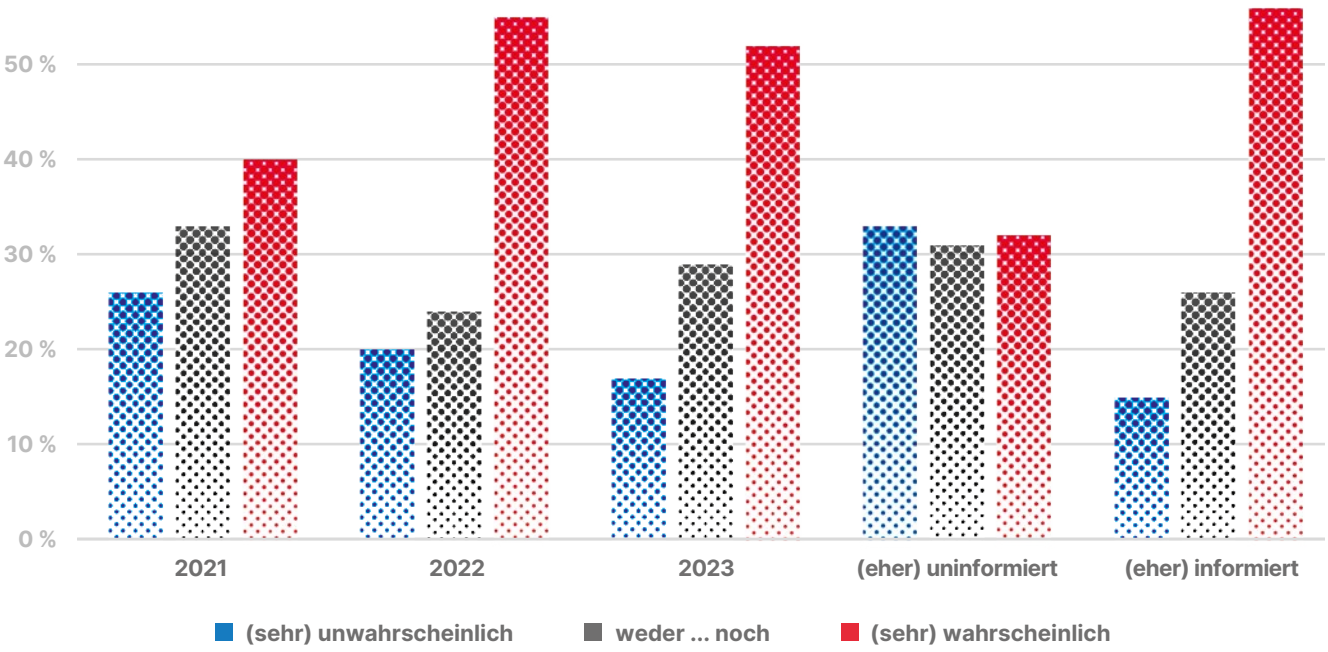
Je grösser das KMU ist, desto eher sind zukünftige Massnahmen geplant.

Der Mittelwert der kleinsten befragten Unternehmen (4–9 Mitarbeitende) liegt bei 3.5 (auf der 5er-Skala), bei den mittleren Unternehmen (10–19 Mitarbeitende) bei 3.6 und bei den grössten Unternehmen (20–49 Mitarbeitende) bei 3.7.

Zwischen den Grossregionen und Branchen gibt es keine signifikanten Unterschiede, wenn auch die Wahrscheinlichkeit, Sicherheitsmassnahmen zu erhöhen, bei den Branchen Finanz-Dienstleistungen sowie Information und Kommunikation tendenziell etwas höher liegt (3.9) als bei den anderen (3.4 bis 3.6).

Signifikant ist der Unterschied zwischen den (eher) uninformierten Befragten (3.0) und den (eher) informierten (3.6) Befragten. Auch die Pioniere (4.0) und Early Followers (3.7) planen signifikant häufiger eine Erhöhung der Sicherheitsmassnahmen als Late Followers (3.2).

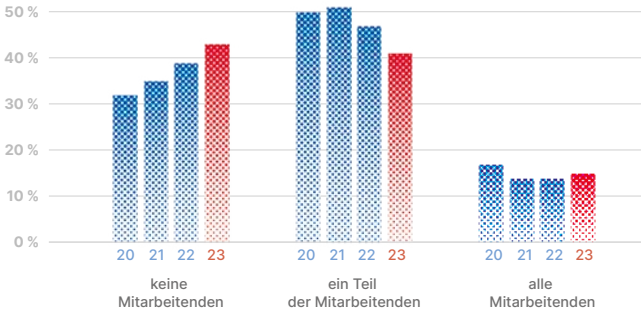
Die besser Informierten zum Thema Cybersicherheit planen mehr Massnahmen.



Wahrscheinlichkeit, dass die KMU in den kommenden ein bis drei Jahren die IT-Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen (auf der Skala von 1+2 ((sehr) unwahrscheinlich), 3 (weder/noch) bis 4+5 ((sehr) wahrscheinlich)).

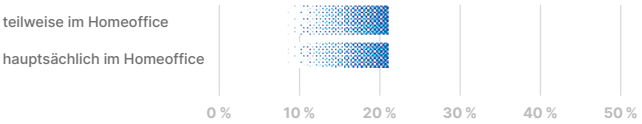
Die wichtigsten Infografiken auf einer Seite:

Mitarbeitende, die theoretisch im Homeoffice arbeiten könnten



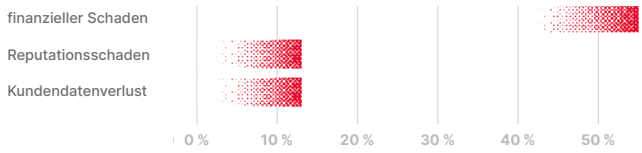
Anzahl Mitarbeitende von 2020 bis 2023, die theoretisch von zu Hause aus arbeiten könnten, da sie zum Beispiel keine Kundinnen und Kunden vor Ort bedienen, kein Fahrzeug lenken oder nicht auf einer Baustelle arbeiten.

Mitarbeitende, die aktuell im Homeoffice arbeiten



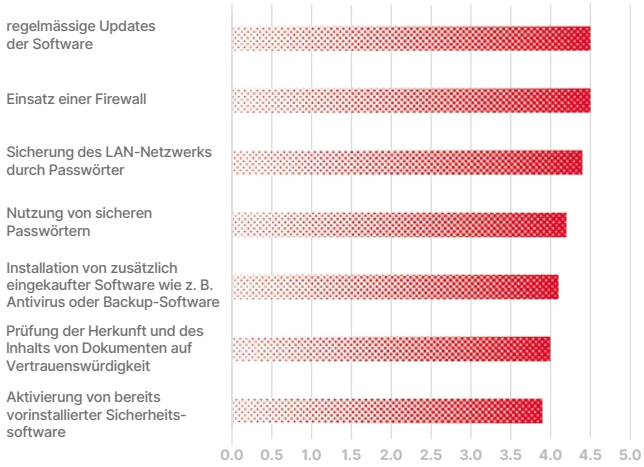
Anzahl Mitarbeitende (in Prozent des Totals der Mitarbeitenden), die teilweise und hauptsächlich im Homeoffice arbeiten (in KMU, in welchen mindestens eine Person von zu Hause aus arbeiten kann).

Durch Cyberangriff entstandener Schaden



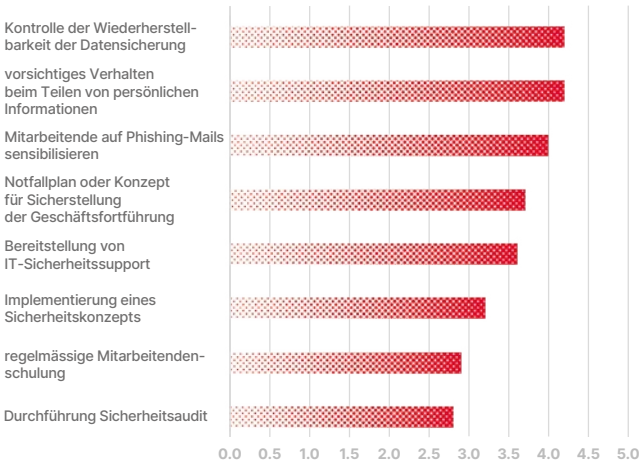
Schäden, welche durch einen erfolgreichen Cyberangriff entstanden sind (bei KMU, die bereits einmal von Cyberkriminellen angegriffen worden sind).

Umgesetzte technische Cybersicherheits-Massnahmen



Umsetzung technischer Cybersicherheits-Massnahmen in Schweizer KMU 2023 (auf der Skala von 1 (gar nicht) bis 5 (voll und ganz)).

Umgesetzte organisatorische Cybersicherheits-Massnahmen



Umsetzung organisatorischer Cybersicherheits-Massnahmen in Schweizer KMU 2023 (auf der Skala von 1 (gar nicht) bis 5 (voll und ganz)).

Forschungsmethodik

Die telefonische Befragung mittels CATI (Computer Assisted Telephone Interviewing) wurde vom 18. April bis 13. Juni 2023 mit Geschäftsführenden von kleinen Unternehmen (4 bis 49 Mitarbeitende) in der deutsch-, französisch- und italienischsprachigen Schweiz durchgeführt.

Die durch die Stichprobe abgebildete Grundgesamtheit umfasst rund 153 000 Firmen mit 4 bis 49 Mitarbeitenden in allen Landesteilen (BFS / STATENT 2017). Das Vertrauensintervall der Gesamtstichprobe liegt bei +/– 4.4% bei einer Sicherheit von 95% (50/50-Verteilung). Die Erhebung zeigt ein bezüglich den Firmengrössen und Sprachregionen strukturgleiches Abbild der Grundgesamtheit. Die Ergebnisse sind somit unter Berücksichtigung des Vertrauensintervalls auf die Grundgesamtheit extrapolierbar.

Die Stichprobe wurde proportional zu den Firmengrössen erhoben. Dabei wurde die Verteilung der drei Grössenkategorien (nach Anzahl Mitarbeitenden) mittels Quotensteuerung sichergestellt. Die Verteilung nach Grossregion wurde mittels Adress-Vorschichtung erzielt.

Die Stichprobe beinhaltet 326 KMU mit 4 bis 9 Mitarbeitenden (Stichprobe: 65% / BFS STATENT: 66%), 110 KMU mit 10 bis 19 Mitarbeitenden (22% / 22%) und 66 KMU mit 20 bis 49 Mitarbeitenden (13% / 12%). Die Adressen stammen von einem Schweizer Adressbroker aus einem Potenzial von über 100 000 Adressen (entspricht 2/3 der Grundgesamtheit).

Die Subgruppen zu technischer Innovation (Pioniere, Early Followers und Late Followers) wurden aufgrund der Fragen zur Adaption neuer Technologien gebildet:
- Pioniere gehören immer zu den ersten, die neue Technologien und Geräte kaufen respektive einsetzen.
- Early Followers fangen erst dann an, neue Technologien und Geräte zu verwenden, wenn sie wissen, welche Erfahrungen andere mit ihnen gemacht haben.
- Late Followers übernehmen neue Technologien und Geräte erst dann, wenn es für sie unerlässlich ist.

Für die Subgruppen zu den technischen und organisatorischen Umsetzungen von Cybersicherheits-Massnahmen wurde der Durchschnitt aller technischen beziehungsweise organisatorischen Massnahmen berechnet (Durchschnittswerte von 1 bis 3 gelten als tiefe Massnahmenumsetzung, der Durchschnittswert 4 als mittlere Massnahmenumsetzung und der Durchschnittswert 5 als hohe Massnahmenumsetzung).

Kontaktiert wurden 37 376 KMU, wovon 21 636 nicht erreichbar waren (zum Beispiel Verweigerung, keine Antwort, besetzt oder Anrufbeantworter). Die Ausschöpfung beträgt (bei 502 realisierten Interviews) 3.2%.

Allgemeiner Lesehinweis zu den Grafiken: Subgruppen, die weniger als 30 Interviews enthalten, werden als Warnhinweis mit * gekennzeichnet, um einer Überinterpretation vorzubeugen. Subgruppen mit $n \geq 20$ werden abgebildet, Subgruppen mit $n < 20$ nicht mehr. Die Prozentzahlen sind auf ganze Zahlen gerundet, es können deshalb kleine Rundungsdifferenzen entstehen. Die Antwortoption «weiss nicht / keine Antwort» wurde für die Lesbarkeit der Grafiken nicht angegeben, weshalb die Summe aller Antworten teilweise nicht 100% ergibt.

Kontakt Autorinnen und Autoren

Prof. Dr. Marc K. Peter
Leiter Kompetenzzentrum
Digitale Transformation
Hochschule für Wirtschaft
FHNW, Olten
marc.peter@fhnw.ch

Kristof A. Hertig
Program Lead Infrastructure &
Cybersecurity
digitalswitzerland, Zürich
kristof@digitalswitzerland.com

Andreas W. Kaelin
Geschäftsführer Allianz Digitale
Sicherheit Schweiz ADSS, Zug
Senior Advisor digitalswitzerland,
Zürich
andreas@digitalswitzerland.com

Karin Mändli Lerch
Projektleiterin
gfs-zürich, Zürich
karin.maendlilerch@gfs-zh.ch

Patric Vifian
Marketing Manager KMU
Die Mobiliar, Bern
patric.vifian@mobi.ch

Nicole Wettstein
Leiterin Schwerpunktprogramm
Cybersecurity
Schweizerische Akademie
der Technischen
Wissenschaften SATW, Zürich
nicole.wettstein@satw.ch

Marc K. Peter, Kristof A. Hertig, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian & Nicole Wettstein:

Homeoffice und Cybersicherheit in Schweizer KMU:
Strategien und Massnahmen in Schweizer KMU
mit 4–49 Mitarbeitenden in 2023

– Die Mobiliar
– digitalswitzerland
– Hochschule für Wirtschaft FHNW
– Schweizerische Akademie der Technischen
Wissenschaften SATW
– Allianz Digitale Sicherheit Schweiz ADSS
– gfs-zürich

www.cyberstudie.ch
Bern, September 2023