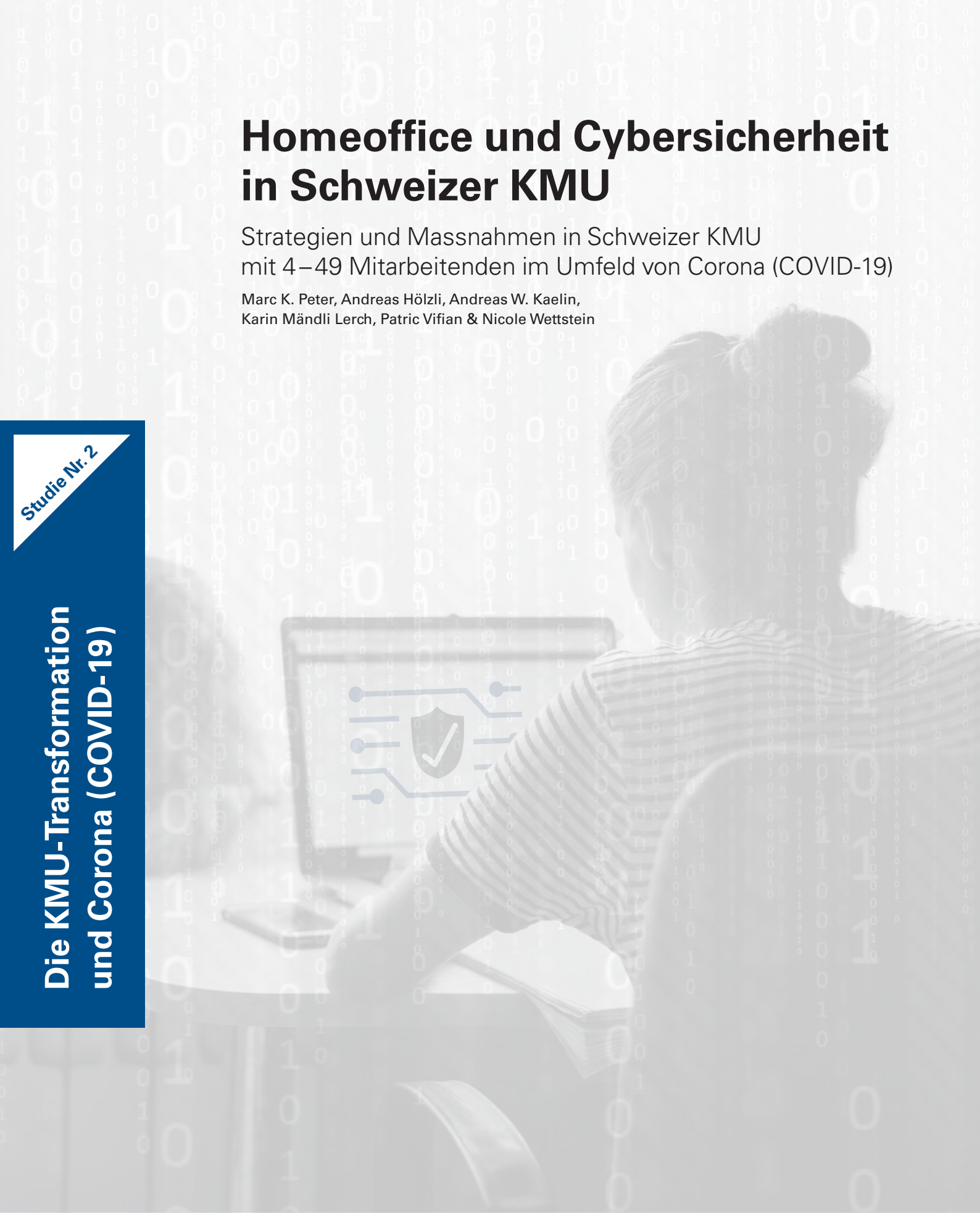
Homeoffice und Cybersicherheit in Schweizer KMU

Strategien und Massnahmen in Schweizer KMU mit 4–49 Mitarbeitenden im Umfeld von Corona (COVID-19)

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

Studie Nr. 2

Die KMU-Transformation und Corona (COVID-19)



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

Impressum

Marc K. Peter, Andreas Hölzli, 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 im Umfeld von Corona (COVID-19)

Die Mobiliar, digitalswitzerland, FHNW Hochschule für Wirtschaft, SATW, gfs-zürich

Bern, November 2021

Koordination dieser Publikation: Prof. Dr. Marc K. Peter, FHNW Hochschule für Wirtschaft (www.fhnw.ch/wirtschaft)

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

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

Forschungsmethodik

Grundgesamtheit: KMU der deutsch-, französisch- und italienisch-sprachigen Schweiz mit 4–49 Mitarbeitenden (= ca. 153'000 KMU gemäss BfS, Statistik der Unternehmensstruktur STATENT 2017, Vers. 22.08.2019).

Stichprobe: 506 Geschäftsführende von Schweizer KMU

Repräsentativität: Das Vertrauensintervall der Gesamtstichprobe liegt bei +/- 4,4 % bei einer Sicherheit von 95 % (50/50-Verteilung). Die Erhebung zeigt ein repräsentatives Abbild der Schweizer KMU-Landschaft; die Ergebnisse sind somit auf die Grundgesamtheit übertragbar.

Methode: CATI-Befragung

Stichprobenmethode: Random-Quota (zufällige Auswahl der KMU, vorgeschichtet nach Region, dann Quotierung nach Firmengrösse)

Gewichtung: keine

Befragungszeitraum: 16. Juni bis 27. Juli 2021

Inhalt

Einleitung und Übersicht

Die Projektgruppe, bestehend aus Mitarbeitenden von digitalswitzerland, der Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz FHNW, der Schweizerischen Akademie der Technischen Wissenschaften SATW, von gfs-zürich und von Die Mobiliar hat sich zum Ziel gesetzt, mittels der Erhebung des Ist-Zustandes und dieser Publikation einen Beitrag zum Verständnis und zur Stärkung von Schweizer KMU mit 4-49 Mitarbeitenden im Umfeld von Corona (COVID-19) zu leisten.

Die zwei durchgeführten repräsentativen Studien geben Einblicke in den Stand der Homeoffice-Nutzung und der Cybersicherheit in KMU, getrieben durch die Ereignisse von Corona/COVID-19 seit anfangs 2020. Die erste Befragung fand zwischen den ersten beiden Corona-Wellen statt, nachdem die erste Homeoffice-Empfehlung des Bundesrats aufgehoben (am 22. Juni 2020) und bevor sie am 19. Oktober 2020 zum zweiten Mal ausgerufen wurde (per 18. Januar 2021 wurde das Homeoffice für alle Unternehmen zur Pflicht). Die vorliegende zweite Befragung fand im Anschluss an die Auflösung der Homeoffice-Pflicht für Betriebe, die regelmässig testen, statt (ab 31. Mai 2021) bzw. begann kurz bevor für alle Unternehmen ab 26. Juni 2021 die Umwandlung in eine Homeoffice-Empfehlung erfolgte: Die zweite Befragung von 506 KMU-Geschäftsleitenden wurde im Zeitraum 16. Juni bis 27. Juli 2021 durchgeführt.

Vor dem ersten Lockdown im März 2020 arbeiteten in denjenigen KMU, in welchen für mindestens eine Mitarbeiterin / einen Mitarbeiter das Homeoffice möglich wäre, 10 % von zu Hause. Dieser Wert hat sich während dem ersten Lockdown fast vervierfacht (auf 38 %) und sank danach auf 16 % (eine Steigerung von 60 % gegenüber der Situation vor dem Lockdown). Dieser Wert hat sich während dem zweiten Lockdown wiederum fast verdreifacht (von 16 % nach dem Lockdown auf 36 % während der Homeoffice-Pflicht) und hat sich nun über alle Industrien hinweg auf einem höheren Niveau (bei 20 %) eingependelt. Der Vergleich der zwei Wellen zeigt, dass sich die Nutzung des Homeoffice als Arbeitsort in Schweizer KMU seit Beginn der Coronakrise verdoppelt hat.

Ähnlich wie in der ersten Studie sehen sich auch in der zweiten Befragung 19 % der KMU mit 4-49 Mitarbeitenden als Pioniere bezüglich des Einsatzes neuer Technologien, 41 % als Early Followers (2020: 44 %) und 37 % als Late Followers (2020: 33 %). Pioniere erreichen einen Wettbewerbsvorteil, indem sie als Vorreiter in neue Technologien sowie Produkt- und Marketinginnovationen investieren. Early Followers folgen zeitnah zu den Pionieren mit Innovationen, während Late Followers erst nach einiger Zeit, wenn die Innovationen getestet sind, diese auch selber nutzen. Beim Einsatz des Homeoffice sind die Pioniere hervorzuheben: In diesen KMU könnten theoretisch 85 % aller oder einiger Mitarbeitenden im Homeoffice arbeiten (und 91 % der Mitarbeitenden sind dort bereits voll oder teilweise dafür ausgerüstet). Aber auch bei den Early Followers und Late Followers gibt es viel Potenzial für das Homeoffice; über alle KMU hinweg, da in rund zwei Drittel der Schweizer KMU theoretisch alle oder einige Mitarbeitenden im Homeoffice arbeiten könnten (und zwei Drittel der KMU bereits alle oder einige Mitarbeitende dafür ausgerüstet haben).

Soziale/emotionale (z. B. der Zusammenhalt im Team), technische (z. B. der externe Datenzugriff) und organisatorische Faktoren (z. B. der Arbeitsplatz) werden als grösste Herausforderungen für die Umsetzung des Homeoffice betrachtet. Zur Umsetzung werden u. a. neue Kommunikationstools (speziell Online-Konferenztools und Online-Beratungen/-Schulungen) eingesetzt. Je grösser das KMU, umso mehr IT-Arbeiten werden von externen Dienstleistern wahrgenommen. Im Durchschnitt nutzen 30 % der KMU externe IT-Dienstleister zur Bereitstellung ihrer IT-Infrastruktur.

Mit Corona/COVID-19 und der Zunahme von Mitarbeitenden im Homeoffice nahmen auch die Angriffe im Cyberraum zu. Geschäftsleitende von Schweizer KMU sagen deshalb, dass die Cyberkriminalität ein ernstzunehmendes Problem ist (bewertet mit 4,6 auf der 5er-Skala) und dass Massnahmen gegen Cyberattacken wichtig sind (4,4).

Die Studie zeigt, dass sich ein Fünftel der KMU-Geschäftsleitenden zum Thema Cybersicherheit nicht oder überhaupt nicht informiert fühlt. Gleich wie in 2020 bewerten 65 % der Geschäftsleitenden die Thematik als wichtig oder sehr wichtig. Dies zeigt sich auch in der Tatsache, dass in 2021 36 % der KMU bereits Cyberangriffe erlitten haben, welche zu einem erheblichen Aufwand zur Beseitigung der Schäden führten (2020: 25 %). Die Auswirkungen dieser Angriffe sind finanzielle Schäden, Kundendatenverluste und Reputationsschäden.

Analog der Umfrage in 2020 sind die Schweizer KMU relativ weit fortgeschritten mit der Umsetzung technischer Massnahmen zur Erhöhung der Cybersicherheit. Viel Potenzial zeigt sich jedoch bei der Planung und Umsetzung organisatorischer IT-Sicherheitsmassnahmen: Nur knapp die Hälfte der Schweizer KMU verfügt über ein IT-Sicherheitskonzept und nur zwei Fünftel schulen ihre Mitarbeitenden regelmässig oder führen IT-Sicherheitsaudits durch. Während der Homeoffice-Pflicht investierten deshalb ein Viertel der KMU in zusätzliche Massnahmen wie Sicherheitssoftware, Firewalls und stärkere Passwörter. Die Ergebnisse der Studie zeigen auch, dass KMU in vielen Fällen die Datenschutzverantwortlichkeit regelten (bei zwei Dritteln der KMU) und Prozesse zum Datenmanagement definierten.

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

www.cyberstudie.ch
www.digitalwitzerland.ch
www.kmu-transformation.ch
www.satw.ch

KMU-Geschäftsleitende, die zum Thema Cybersicherheit informiert sind, haben in der Regel mehr Massnahmen zum Schutz ihrer IT-Infrastruktur und Kundendaten implementiert als nicht informierte. Die Themen der Digitalisierung, des Homeoffice, des Einsatzes von Kommunikationstechnologien und der Cybersicherheit im Umfeld von Corona/COVID-19 haben weiter an Wichtigkeit gewonnen. Gleichzeitig werden diese Themen gesellschaftliche, wirtschaftliche, technologische und verkehrstechnische Diskussionen vorantreiben.

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

Bern, im November 2021

Andreas Hölzli
Leiter Kompetenzzentrum Cyberrisk
Die Mobiliar, Bern

Andreas W. Kaelin
Stellvertretender Geschäftsführer und
Leiter des Dossiers Cybersecurity
digitalswitzerland, Bern

Karin Mändli Lerch
Projektleiterin
gfs-zürich, Zürich

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

Patric Vifian
Marketing Manager KMU
Die Mobiliar, Bern

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

Stellenwert und Nutzung des Homeoffice

Es existiert viel Potenzial für das Homeoffice – und ein Drittel der Mitarbeitenden ist dafür bereits voll ausgerüstet

In rund zwei Dritteln (65 %) der Schweizer KMU könnten theoretisch alle oder zumindest ein Teil der Mitarbeitenden im Homeoffice arbeiten (2020: 67 %). Sie müssen also z. B. keine Kundinnen und Kunden vor Ort bedienen, ein Fahrzeug lenken oder auf einer Baustelle arbeiten (in 14 % alle; in 51 % ein Teil der Mitarbeitenden). Dies ist ein hoher Anteil und zeigt die Potenziale des Homeoffice und die damit verbundenen gesellschaftlichen, wirtschaftlichen, technologischen und verkehrstechnischen Auswirkungen.

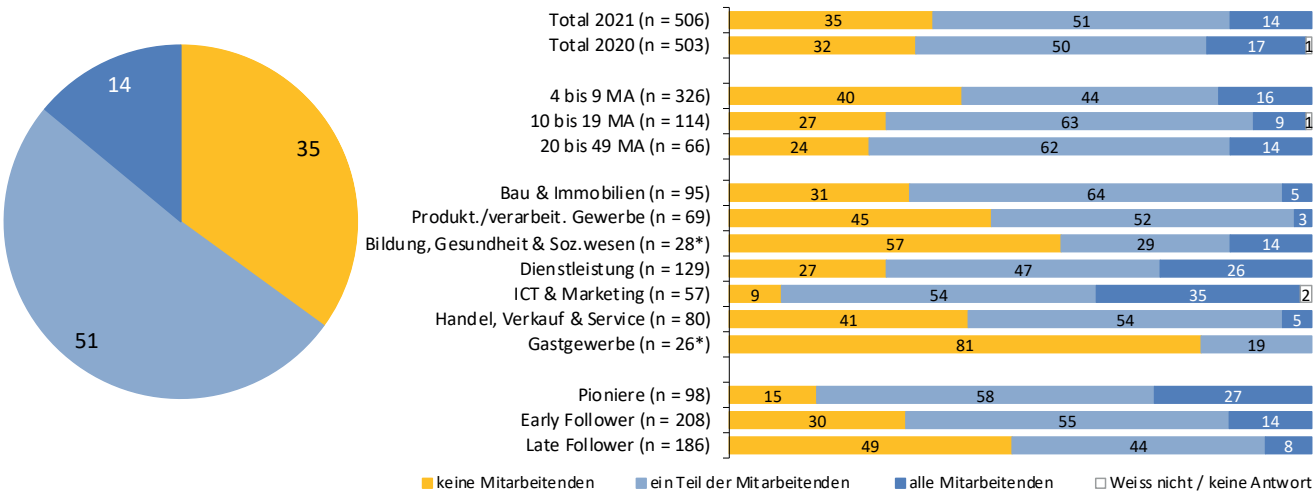
Bereits heute sind 29 % der Mitarbeitenden in KMU (2020: 20 %) vollständig und 39 % teilweise (2020: 46 %) mit Hilfsmitteln für das Arbeiten im Homeoffice ausgerüstet, unabhängig davon, ob es sich um firmeneigene oder private Hilfsmittel handelt. Der Anteil der Mitarbeitenden, welche komplett und teilweise für das Homeoffice ausgerüstet sind, entspricht demjenigen von 2020; jedoch sind nun wesentlich mehr Mitarbeitende komplett fürs Homeoffice ausgerüstet.

Hervorzuheben sind die Pioniere: In diesen KMU könnten theoretisch 85 % aller oder einiger der Mitarbeitenden im Homeoffice arbeiten; und 91 % der Mitarbeitenden sind dort voll oder teilweise bereits dafür ausgerüstet.

Fragen für Schweizer KMU:

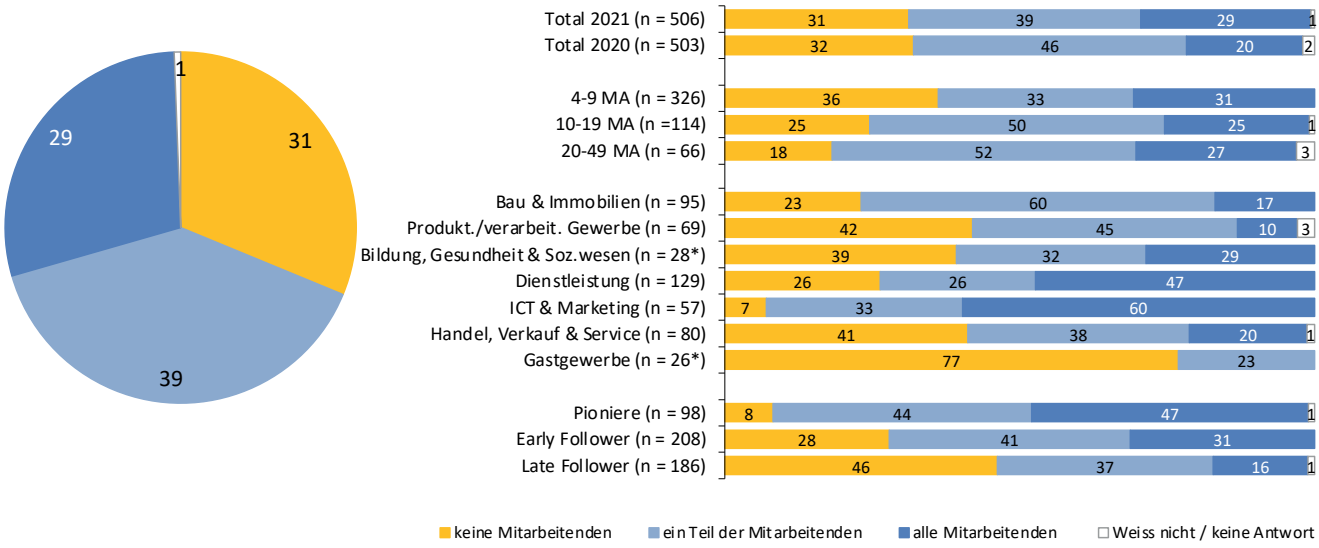
- Wie nutzen Sie das Homeoffice strategisch, um die Flexibilität und Attraktivität für Arbeitnehmende zu erhöhen und Ihre Kostenstruktur zu reduzieren?
- Haben Sie mit Ihren Mitarbeitenden zusammen das Thema Homeoffice bereits diskutiert und so Ideen/Potenziale sowie eine Roadmap entwickelt?
- Gibt es eine Homeoffice-Vereinbarung, z. B. zur Regelung der Kostenübernahme von privater Büroausrüstung?

Anzahl Mitarbeitende, die potenziell vom Homeoffice aus arbeiten könnten



Anzahl Mitarbeitende, die potenziell im Homeoffice arbeiten könnten («Wie viele von Ihren Mitarbeitenden könnten theoretisch von zuhause aus arbeiten, müssen also z. B. keine Kundinnen und Kunden vor Ort bedienen, ein Fahrzeug lenken oder auf einer Baustelle arbeiten?» / n 2021 = 506, n 2020 = 503 / Kategorien mit einer Stichprobengrösse < 30 sind mit einem * gekennzeichnet)

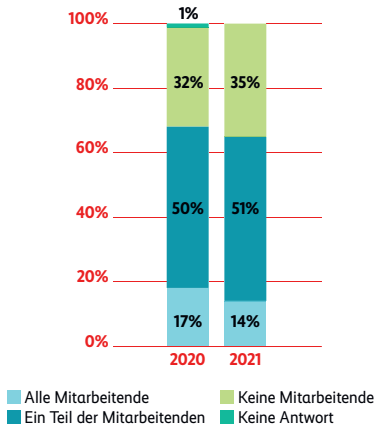
Anzahl Mitarbeitende, die für das Homeoffice ausgerüstet sind



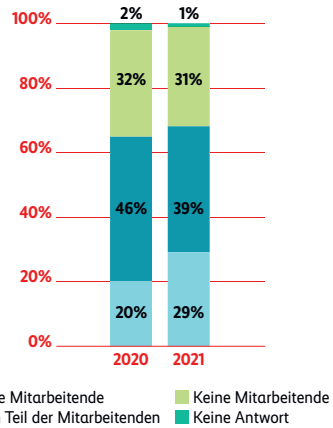
Anzahl Mitarbeitende, die für das Homeoffice ausgerüstet sind («Wie viele von Ihren Mitarbeitenden sind vollständig mit Hilfsmitteln für das Arbeiten von zuhause aus ausgerüstet, unabhängig davon, ob es sich um firmeneigene oder private Hilfsmittel handelt?» / n 2021 = 506, n 2020 = 503 / Kategorien mit einer Stichprobengrösse < 30 sind mit einem * gekennzeichnet)

Infografiken

Anzahl Mitarbeitende, die potenziell im Homeoffice arbeiten könnten



Anzahl Mitarbeitende, die für das Homeoffice ausgerüstet sind



Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Die Hochschule für Wirtschaft FHNW ist international ausgerichtet und praxisorientiert. Sie bildet in Basel, Brugg-Windisch und Olten 3'000 Bachelor- und Masterstudierende aus und ist mit ihrem breiten Business-Weiterbildungsangebot führend unter den Fachhochschulen der Schweiz.

Das Kompetenzzentrum Digitale Transformation von Prof. Dr. Marc K. Peter an der Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz FHNW bietet Forschungs-, Beratungs- und Bildungsleistungen rund um die Digitale Transformation an, um Organisationen und Mitarbeitenden zu helfen, digitale Wachstumsstrategien zu entwickeln und erfolgreich umzusetzen.

Wichtige Hilfsmittel für KMU in der digitalen Transformation:

Workshop-Canvas Digitale Transformation
Mit dem Workshop-Canvas zur digitalen Transformation erhalten Sie ein kostenloses Hilfsmittel, um mit Ihren Mitarbeitenden zusammen Ideen und Potenziale für Ihre Unternehmenstransformation zu identifizieren.
www.digital-transformation-canvas.net

Workshop-Canvas Strategieentwicklung im digitalen Zeitalter
Mit dem Workshop-Canvas zur Strategieentwicklung erhalten Sie ein kostenloses Hilfsmittel, um mit Ihren Mitarbeitenden zusammen Ihre Strategie für die digitale Transformation des Unternehmens zu entwickeln.
www.act-strategy-canvas.ch

Workshop-Canvas Arbeitswelt 4.0
Mit dem Workshop-Canvas zur Arbeitswelt 4.0 erhalten Sie ein kostenloses Hilfsmittel, um mit Ihren Mitarbeitenden zusammen Ideen und Potenziale für Ihre Arbeitswelt-Strategie zu identifizieren.
www.arbeitswelt-zukunft.ch/workshop-canvas

Bestimmung der digitalen Maturität
Mit der kostenlosen Maturitätsanalyse können Sie sich und Ihr Unternehmen selber evaluieren: Wie weit sind Sie mit Ihrer Transformation fortgeschritten? Haben Sie in allen Handlungsfeldern Projekte initialisiert oder bereits realisiert? Wo liegt das (grösste) Potenzial?
www.digitale-reife.net

Bestimmung der strategischen Themen
Mit dem kostenlosen Online-Strategiecheck definieren Sie diejenigen Themen und Fragen, welche im Rahmen der Strategieentwicklung für das digitale Zeitalter diskutiert werden sollten.
www.digital-strategy-check.ch

Praxisleitfaden Strategieentwicklung im digitalen Zeitalter
Forschungsresultate, Praxistipps, Fallstudien, Strategievorlagen und Checklisten für die Planung und Umsetzung der digitalen Transformation:
www.strategische-transformation.ch

Praxisleitfaden Digitale Transformation für KMU
Forschungsresultate, Praxistipps, Fallstudien und Checklisten für Ihre KMU-Transformation:
www.kmu-transformation.ch

Praxisleitfaden Arbeitswelt 4.0
Forschungsresultate, Praxistipps, Fallstudien und Checklisten für Ihre neue Arbeitswelt:
www.arbeitswelt-zukunft.ch

Weitere Informationen:
FHNW Hochschule für Wirtschaft
Institute for Competitiveness & Communication
Prof. Dr. Marc K. Peter
Kompetenzzentrum Digitale Transformation
Riggenbachstrasse 16
4600 Olten

marc.peter@fhnw.ch
www.digitale-transformation-artikel.ch

Veränderung der Homeoffice-Gewohnheiten während und nach dem Corona-Lockdown

Verdoppelung der Homeoffice-Nutzung in Schweizer KMU innert zwei Jahren

Vor dem ersten Lockdown in 2020 arbeiteten in denjenigen KMU, in welchen für mindestens eine Mitarbeiterin / einen Mitarbeiter das Homeoffice möglich wäre, 10 % von zu Hause. Dieser Wert hat sich während dem ersten Lockdown fast vervierfacht (auf 38 %) und sank danach auf 16 % (eine Steigerung von 60 %).

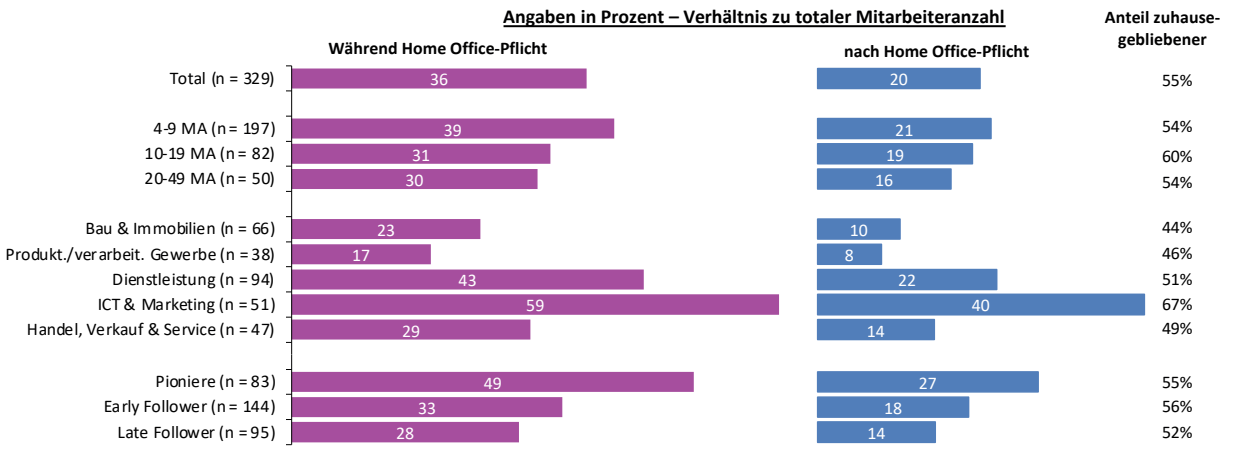
Während dem zweiten Lockdown hat sich dieser Wert wiederum fast verdreifacht (von 16 % nach dem Lockdown auf 36 % während der Homeoffice-Pflicht) und hat sich nun über alle Industrien hinweg auf einem höheren Niveau (bei 20 %) eingependelt. Bei den Pionieren liegt dieser Wert bei 27 %; bei den Late Followers bei nur 14 %.

Der Vergleich der zwei Wellen zeigt, dass sich die Nutzung des Homeoffice als Arbeitsort in Schweizer KMU seit Beginn der Coronakrise verdoppelt hat. Dieser Wert wird mittelfristig unter Umständen ein wenig sinken, da 15 % der KMU zwar von einer Steigerung, aber 38 % von einer Reduktion ausgehen. Interessanterweise ist dieser Wert gerade bei den Pionieren relativ hoch (45 % gehen von einer Reduktion aus). Gesamthaft betrachtet sind mehr Geschäftsleitende als in 2020 nicht erfreut über eine langfristige Entwicklung mit mehr Mitarbeitenden im Homeoffice. In 2020 waren dies 8 % der Geschäftsleitenden, welche persönlich an dieser Entwicklung nicht erfreut waren (Werte 1 und 2 auf einer 5er-Skala); in 2021 waren dies bereits 15 %.

Fragen für Schweizer KMU:

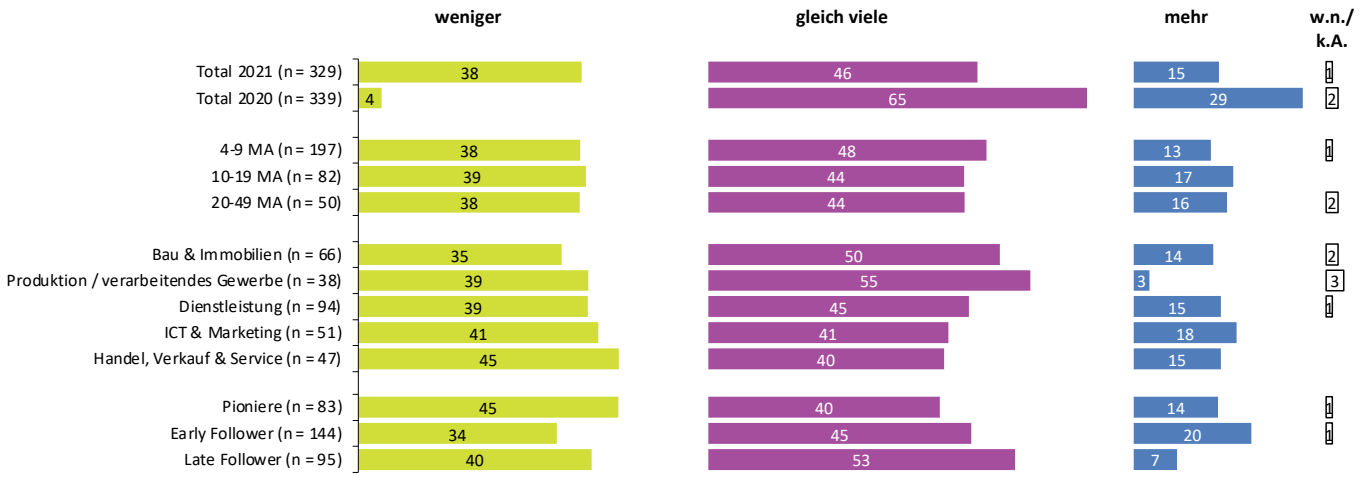
- Wird sich das Homeoffice bei Ihnen langfristig etablieren – haben Sie die Potenziale identifiziert und diskutiert?
- Haben Sie die Anforderungen an New Work (an die Arbeitswelt 4.0) zu den Themen Kultur, Führung und Kommunikation identifiziert und definiert?
- Haben Sie eine Strategie mit einer Roadmap für die Arbeitswelt 4.0 entwickelt?

Veränderung der Homeoffice-Gewohnheiten während des Corona-Lockdowns



Veränderung der Homeoffice-Gewohnheiten während des Corona-Lockdowns / während der Homeoffice-Pflicht («Wie viele Ihrer Mitarbeitenden haben seit anfangs 2021 hauptsächlich von zuhause aus gearbeitet, also während die Homeoffice-Pflicht galt?», «Und wie viele arbeiten jetzt, nach der Homeoffice-Pflicht, hauptsächlich von zuhause aus?» / n = 329 (Filter: wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann))

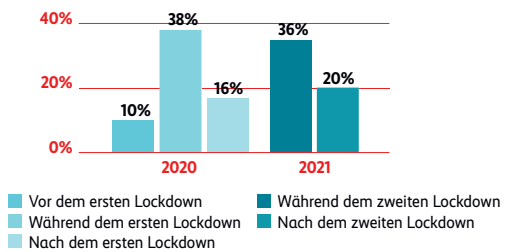
Einschätzung der Veränderung der Homeoffice-Arbeitsplätze



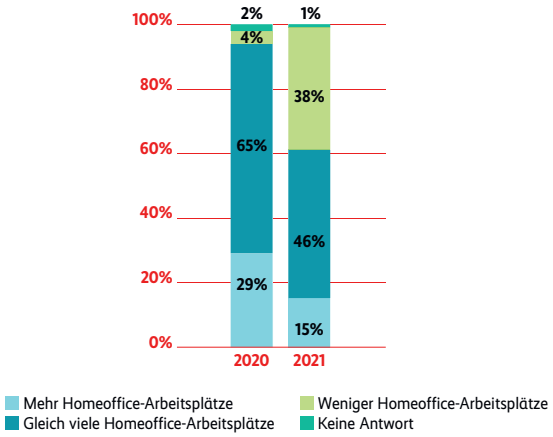
Einschätzung der Veränderung der Homeoffice-Arbeitsplätze («Wie schätzen Sie die langfristige Entwicklung ein: Werden in Ihrer Firma in Zukunft mehr, gleich viele oder weniger Mitarbeitende von zuhause aus arbeiten als während der Pandemie?» / n 2021 = 329, n 2020 = 339 (Filter: wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann))

Infografiken

Veränderung der Homeoffice-Gewohnheiten während des Corona-Lockdowns



Einschätzung der Veränderung der Homeoffice-Arbeitsplätze



Herausforderungen bei der Umsetzung des Homeoffice

Zusammenarbeit, Führung und Organisation als wichtige Erfolgsfaktoren

Der soziale/emotionale Faktor (soziale Herausforderungen, Teamzusammenhalt, Stimmung, Vereinsamung), der technische Faktor (technische Herausforderungen wie Daten- und Telefonzugriff) sowie der organisatorische Faktor (Herausforderungen bei den Mitarbeitenden wie z. B. der Arbeitsplatz) werden als grösste Herausforderungen zur Umsetzung des Homeoffice bei knapp einem Fünftel der KMU betrachtet. Dazu gehören sowohl führungstechnische als auch sicherheitstechnische Herausforderungen bei knapp einem Zehntel der Schweizer KMU.

Dies bestätigt eine Studie der FHNW Hochschule für Wirtschaft aus dem Jahr 2019, welche die Dimensionen People (Mitarbeitende), Place (Arbeitsumfeld) und Technology (Technologien) als Erfolgsfaktoren für die Gestaltung der Arbeitswelt 4.0 beschrieb (vgl. Infobox mit Buchtipp).

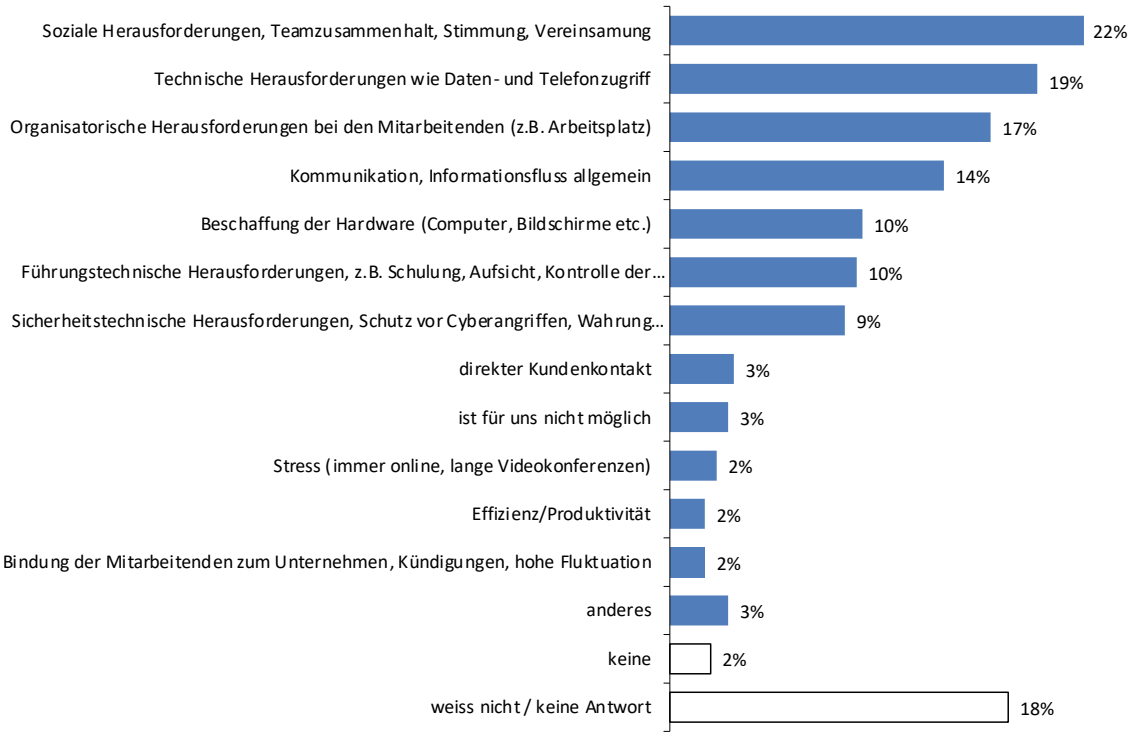
Fragen für Schweizer KMU:

- Welche positiven und negativen Erfahrungen haben Sie mit dem Homeoffice während den Lockdowns gemacht – was können Sie daraus lernen und verbessern?
- Weshalb nutzen Sie das Homeoffice nicht intensiver und strategisch zur Erneuerung Ihres Unternehmens; z. B. zur Stärkung der Arbeitgebendenreputation?

Buchempfehlung

Nicole Krättli & Marc K. Peter
Arbeitswelt 4.0

Führung, Arbeitsplatzgestaltung und Technologieeinsatz im digitalen Zeitalter
1. Auflage 2021, 240 Seiten
ISBN 978-3-03875-379-7
www.kmu-arbeitswelt.ch



Herausforderungen bei der Umsetzung des Homeoffice («Was sind aus unternehmerischer Sicht die grössten Herausforderungen bei der Umsetzung des Homeoffice?» / n = 329, Mehrfachnennungen möglich (Filter: wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann))

Verwendung von Kommunikationstools

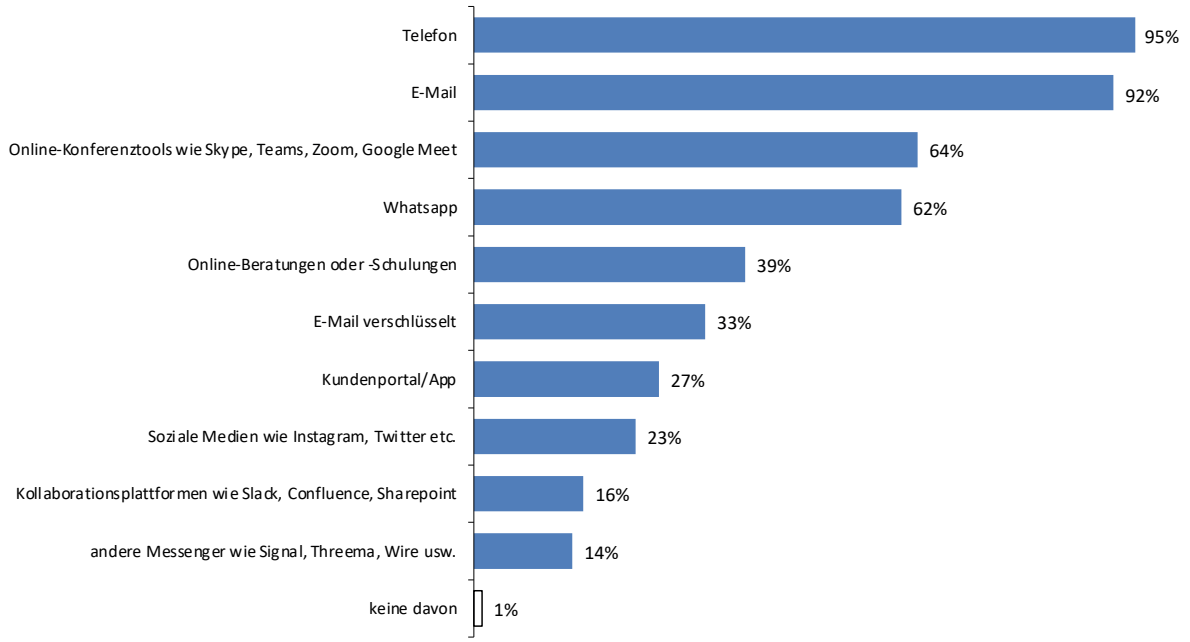
Online-Konferenztools und Online-Beratungen/-Schulungen als wichtige neue Plattformen

Wichtigste Kommunikationstools sind weiterhin das Telefon und E-Mails. In der zweiten Befragung in 2021 wurde erstmals nach der Anzahl verschlüsselter E-Mails gefragt: Ein Drittel der Schweizer KMU nutzt diese nun bereits. In Anbetracht der notwendigen technischen und organisatorischen Vor- bzw. Mehrarbeit ist dies ein hoher Anteil. Der Einsatz von Online-Konferenztools (2020: 46 %, 2021: 64 %) sowie von Online-Beratungen/-Schulungen (2020: 20 %, 2021: 39 %) ist stark gestiegen.

Fragen für Schweizer KMU:

- Wurde ein Konzept zum Einsatz von Kommunikationstools erarbeitet (und wurden anschliessend die zweckmässigsten Plattformen implementiert)?
- Gibt es ein Konzept und Vorgaben zur Datensicherheit für die geschäftliche Nutzung dieser Kommunikationsplattformen?
- Sind die Plattformen sicher; welche Informationen/Daten werden bzw. dürfen über welche Plattformen ausgetauscht werden?

Verwendung von Kommunikationstools



Verwendung von Kommunikationstools («Ich lese Ihnen jetzt einige digitale Kommunikationsmittel vor. Welche davon nutzen Ihre Mitarbeitenden aktuell für Partner, Kundschaft und anderen Mitarbeitende?» / n = 506, Mehrfachnennungen möglich)

Persönliche Informiertheit zur Cyberrisk-Thematik

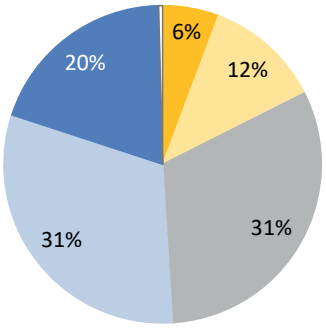
Ein Fünftel der KMU-Geschäftsleitenden fühlt sich nicht / überhaupt nicht informiert

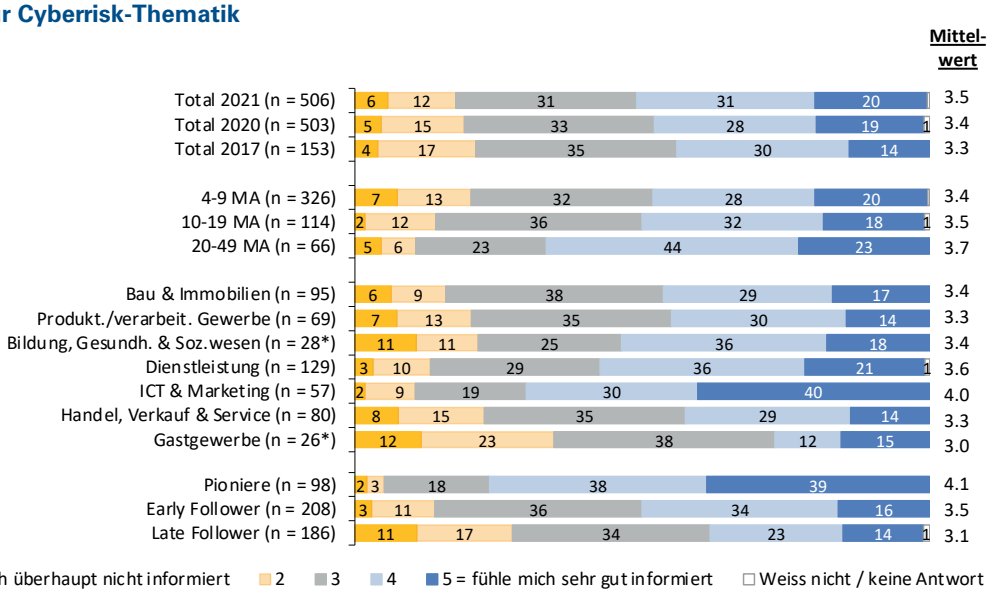
Geschäftsleitende von Schweizer KMU fühlen sich etwas besser informiert als vor einem Jahr; der Wert ist jedoch immer noch gering: Nur 51 % fühlen sich gut / sehr gut informiert (2020: 47 %). Je grösser das KMU, desto besser sind die Geschäftsleitenden zur Thematik informiert. Speziell die Pioniere fühlen sich gut / sehr gut informiert (77 %). Die Cybersicherheit ist auch weiterhin wichtig: Gleich wie in 2020 bewerten 65 % der Geschäftsleitenden von Schweizer KMU die Thematik als wichtig oder sehr wichtig.

Fragen für Schweizer KMU:

- Identifizieren Sie regelmässig die Potenziale für den Einsatz neuer Technologien und existiert eine Strategie/Roadmap für die Einführung neuer IT-Infrastruktur?
- Welche neuen Produkte und Leistungen könnten Sie durch Investitionen in die IT und Cybersicherheit erfolgreich(er) im Markt einführen?
- Erfüllen Sie Ihre eigenen Anforderungen (oder diejenigen des Marktes) an die Cybersicherheit?
- Wie informieren Sie sich regelmässig über Gefahren sowie Konzepte und Lösungsansätze zur Erhöhung der Cybersicherheit?

Persönliche Informiertheit zur Cyberrisk-Thematik





Persönliche Informiertheit zur Cyberrisk-Thematik («Ganz allgemein: Wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert?» / n 2021 = 506, n 2020 = 503 / Kategorien mit einer Stichprobengrösse < 30 sind mit einem * gekennzeichnet)

digitalswitzerland

Über digitalswitzerland

digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 230 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartner in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.

Wichtige Hilfsmittel für KMU:

Cybersecurity-Schnelltest für KMU
cybersecurity-check.ch

Schweizer KMU sind vor den akuten Bedrohungen aus dem Cyberspace oft nicht gut genug geschützt und sind sich dessen nicht bewusst. Eine von ICTswitzerland initiierte Arbeitsgruppe mit Vertretern der Wirtschaft, Verbänden und des Bundes hat sich zusammengeschlossen, um KMU für die Bedrohungen aus dem Cyber Space zu sensibilisieren. Das Resultat ist der Cybersecurity-Schnelltest für KMU, mit dem jeder unkompliziert herausfinden kann, ob das eigene Unternehmen ausreichend vor Cyberrisiken geschützt ist.

Eine gemeinsame Initiative vom Bundesamt für wirtschaftliche Landesversorgung (BWL), der Expertenkommission Bund zur Datenbearbeitung und Datensicherheit, ICTswitzerland, dem Informatiksteuerungsorgan des Bundes (ISB) – Melde- und Analysestelle Informationssicherung (MELANI), der Information Security Society Switzerland (ISSS), der Schweizerische Akademie der Technischen Wissenschaften (SATW), Schweizerische Normen-Vereinigung (SNV), der Schweizer Organisation für kompetente Zertifizierungs- und Bewertungsdienstleistungen (SQS) und dem Schweizerischen Versicherungsverband (SVV).

Mit kompetenten IT-Dienstleistern zu mehr Cybersicherheit
digitalsecurityswitzerland.ch

Die Allianz Digitale Sicherheit Schweiz entwickelt das Gütesiegel CyberSeal «Geprüfter IT-Dienstleister». Das CyberSeal macht die Vertrauenswürdigkeit von IT-Dienstleistern auf den ersten Blick sichtbar und hilft KMU bei der Wahl ihres IT-Partners. Es zeichnet IT-Dienstleister aus, die ihren Kunden mit den nötigen technischen und organisatorischen Massnahmen ein angemessenes Schutzniveau gewährleisten. So steigert das CyberSeal die digitale Sicherheit der KMU und verankert die Digitalisierung auf einem höheren Qualitätsniveau.

Erfolgreiche Cyberangriffe und entstandener Schaden

Über ein Drittel der Schweizer KMU wurde bereits erfolgreich angegriffen

36 % der Schweizer KMU erlitten bereits einmal Cyberangriffe, welche zu einem erheblichen Aufwand zur Beseitigung der Schäden führten (2020: 25 %). Dies entspricht einer Zunahme von 44 % innerhalb eines Jahres. Eine starke Zunahme erfährt die Angriffstechnik des Online-Betrugs. In vielen Fällen geschieht dies mittels CEO-Betrugs: Hier werden den Mitarbeitenden gefälschte E-Mails zugestellt, als deren Sender die/der CEO der eigenen Firma aufgeführt ist. In den E-Mails bittet die/der CEO mit einer erfundenen Geschichte darum, eine Zahlung an eine Drittperson/-firma auszulösen.

Eingesetzte Techniken 2021 von erfolgreichen Cyberangriffen in Schweizer KMU
(in Klammern die Werte von 2020)

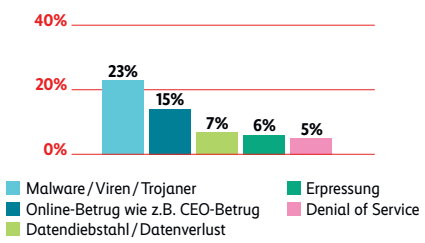
- Malware/Viren/Trojaner: 23 % (18 %)
- Online-Betrug wie z. B. CEO-Betrug: 15 % (6 %)
- Datendiebstahl/Datenverlust: 7 % (5 %)
- Erpressung: 6 % (4 %)
- Denial of Service: 5 % (5 %)

Die Auswirkungen von Cyberangriffen sind finanzielle Schäden (in 25 % der KMU, in welchen ein Angriff zu erheblichen Schäden geführt hat), Kundendatenverlust (7 %) und Reputationsschäden (6 %).

Fragen für Schweizer KMU:

- Kennen die Mitarbeitenden die diversen Angriffstechniken; wie sensibilisieren Sie und wie erfolgt die Aufklärung?
- Welche technischen und organisatorischen Massnahmen treffen Sie, um die Cybersicherheit in Ihrem Unternehmen zu erhöhen?
- Wie überprüfen Sie regelmässig Ihre Konzepte und Massnahmen zur Cybersicherheit

Infografiken



Erfolgreiche Cyberangriffe («Wurde Ihre Firma schon einmal erfolgreich durch eine der folgenden Techniken angegriffen, sodass ein erheblicher Aufwand nötig war, um Schäden zu beheben?» / n = 506, Ja-Anteil in Prozent)

Die Schweizerische Akademie der Technischen Wissenschaften SATW ist das bedeutendste Expertennetzwerk im Bereich Technikwissenschaften in der Schweiz. Sie identifiziert im Auftrag des Bundes industriell relevante technologische Entwicklungen und informiert Politik und Gesellschaft über deren Bedeutung und Konsequenzen. Als politisch unabhängige Fachorganisation setzt sie Impulse für ein sicheres Verhalten aller Akteure im Cyberraum.

Cybersecurity Herausforderungen für die Schweiz
Basierend auf kurzen Textbeiträgen geben die Mitglieder des Advisory Boards Cybersecurity der SATW Einblick in aktuelle, aus Cybersecurity-Perspektive relevante, technologische Entwicklungen. Für jede Entwicklung wird der Handlungsbedarf für die kurz- und mittelfristige Zukunft erläutert.
www.satw.ch/cybersecurity-herausforderungen

Technology Outlook
Die SATW identifiziert wirtschaftlich relevante technologische Entwicklungen und informiert Politik und Gesellschaft über deren Bedeutung und Konsequenzen. Dazu erstellt sie unter anderem den alle zwei Jahre erscheinenden Technology Outlook.
https://www.satw.ch/to2021

Netzwerk Digitale Selbstbestimmung
Das Netzwerk Digitale Selbstbestimmung setzt sich für eine innovative und selbstbestimmte Nutzung von Daten in der Schweiz ein. Ziel ist es, Potenziale der Datenwirtschaft und-gesellschaft vollständig zu ergreifen und zu fördern. Gemeinsam mit der Direktion für Völkerrecht des EDA, dem Bundesamt für Kommunikation und der Swiss Data Alliance ist die SATW Gründungsorganisation des Netzwerks.
https://www.satw.ch/digitale-selbstbestimmung

Nachwuchsförderung
Die Nachwuchsförderung der SATW fördert das Technikinteresse und-verständnis bei Jugendlichen. Sie setzt sich für eine umfassende Technik-Bildung ein und wirkt dem Fachkräftemangel aktiv entgegen. Ein besonderes Anliegen ist ihr die Förderung von Mädchen in technischen Berufen.
https://www.satw.ch/de/technik-bildung

Weitere Informationen:

SATW
Schweizerische Akademie
der Technischen Wissenschaften
St. Annagasse 18
8001 Zürich
www.satw.ch

Risiken von kleinen und existenzgefährdenden Cyberangriffen

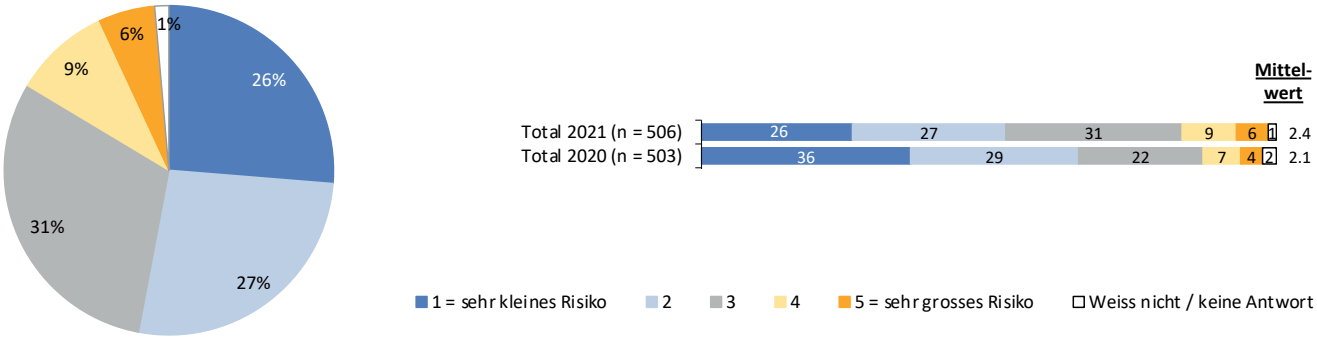
Die Risikoeinschätzung von Cyberangriffen wächst auf niedrigem Niveau

Die Digitalisierung, das Homeoffice und das lukrative Geschäft der Cyberkriminalität steigern die Risikoeinschätzung von Schweizer KMU: In 2021 schätzen 15 % der Geschäftsleitenden das Risiko als hoch / sehr hoch ein, dass ihre Firma innerhalb der nächsten zwei bis drei Jahre von einem Cyberangriff betroffen sein wird, der ihr Geschäft für mindestens einen Tag lang ausser Kraft setzen wird (2020: 11 %). Der Wert für die Einschätzung von existenzgefährdenden Cyberangriffen steigt im Vorjahresvergleich, liegt aber mit 4 % deutlicher tiefer als die Eintrittswahrscheinlichkeit eines eintägigen Ausfalls (2020: 2 %).

Fragen für Schweizer KMU:

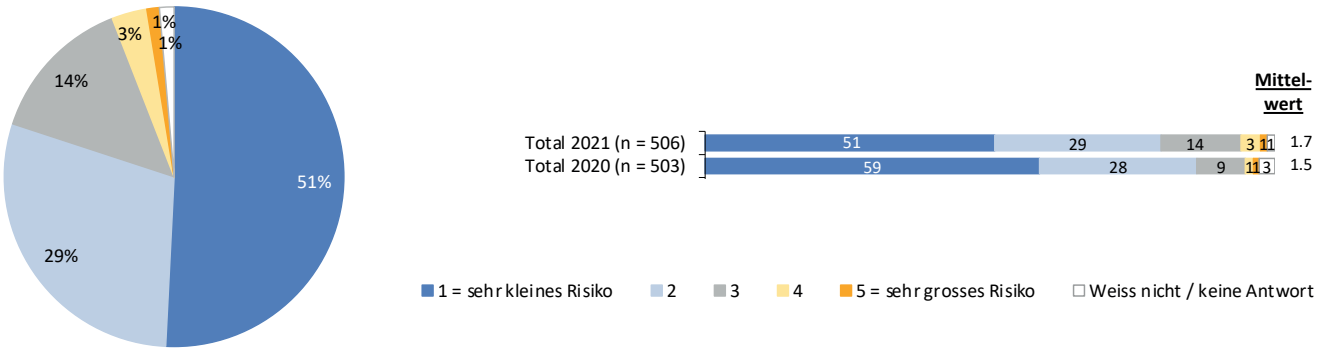
- Welche IT-Infrastruktur ist kritisch für die Leistungserbringung in Ihrem Unternehmen bzw. wie wichtig ist für Sie die Cybersicherheit?
- Welche Leistungen können Sie nicht erbringen, wenn die IT nicht läuft?
- Wie schützen Sie diese IT-Infrastruktur?
- Welche Alternativen (sogenannte Recovery-Konzepte) haben Sie vorbereitet?
- Welche Notfallkonzepte/-pläne bestehen bzw. welche Komponenten fehlen Ihnen?

Risikoeinschätzung «kleiner» Cyberangriff



Risikoeinschätzung «kleiner» Cyberangriff («Als wie hoch schätzen Sie das Risiko ein, dass Ihr KMU innerhalb der nächsten zwei bis drei Jahre von einem Cyberangriff betroffen sein wird, der Ihr Geschäft für mindestens einen Tag lang ausser Kraft setzt?» / n 2021 = 506, n 2020 = 503)

Risikoeinschätzung existenzgefährdender Cyberangriff



Risikoeinschätzung existenzgefährdender Cyberangriff («Als wie hoch schätzen Sie das Risiko ein, dass Ihr KMU innerhalb der nächsten zwei bis drei Jahre von einem Cyberangriff betroffen sein wird, der für Ihr Geschäft existenzgefährdend ist?» / n 2021 = 506, n 2020 = 503)

Technische und organisatorische Massnahmen zur Erhöhung der Cybersicherheit

Viel Potenzial zeigt sich bei der Planung und Umsetzung organisatorischer IT-Sicherheitsmassnahmen

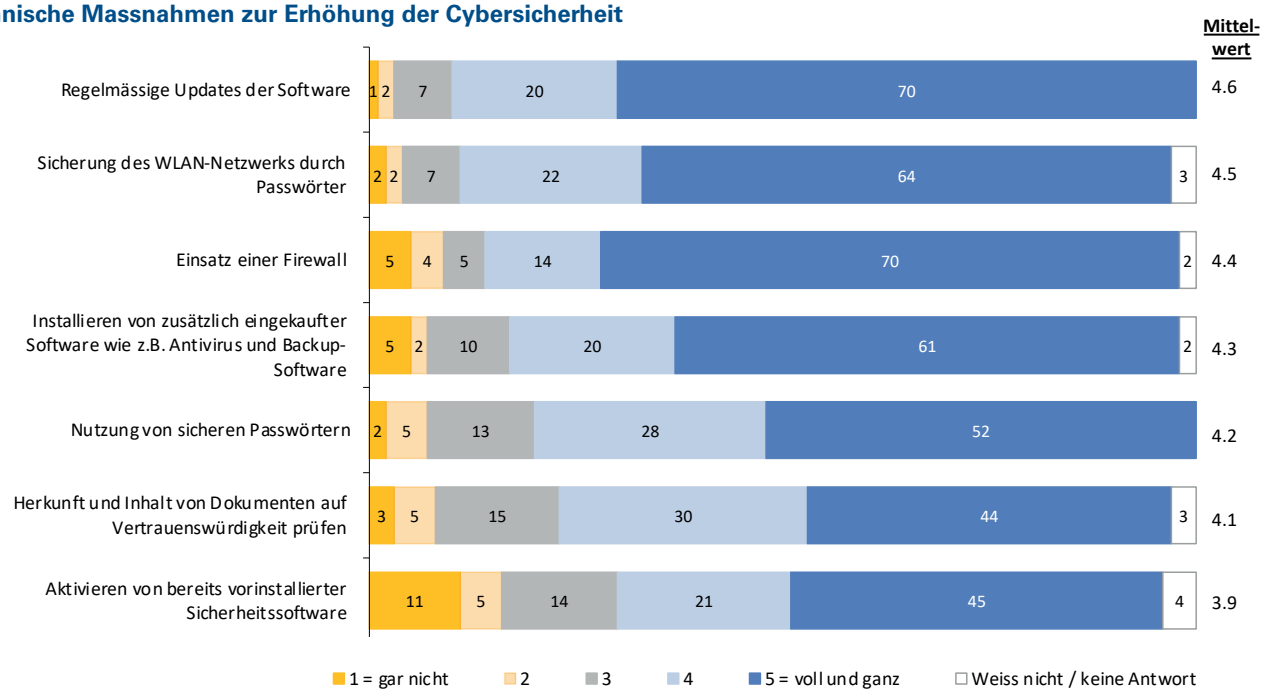
Analog der Umfrage in 2020 sind die Schweizer KMU relativ weit fortgeschritten mit der Umsetzung technischer Massnahmen zur Erhöhung der Cybersicherheit. Bei den organisatorischen Massnahmen besteht auch in 2021 (analog 2020) viel Potenzial. Nur knapp die Hälfte der Schweizer KMU verfügt über ein IT-Sicherheitskonzept (47 % ganz/voll und ganz) und nur zwei Fünftel schulen ihre Mitarbeitenden regelmässig (39 %) oder führen IT-Sicherheitsaudits (37 %) durch.

In einem Drittel der KMU (30 %) stellen die Geschäftsleitenden ein separates Budget für die IT-Sicherheit zur Verfügung. Dieser Wert ist höher bei denjenigen KMU, welche bereits angegriffen wurden (31 %) und bei denen sich die Geschäftsleitenden zum Thema Cybersicherheit eher informiert fühlen (37 %).

Fragen für Schweizer KMU:

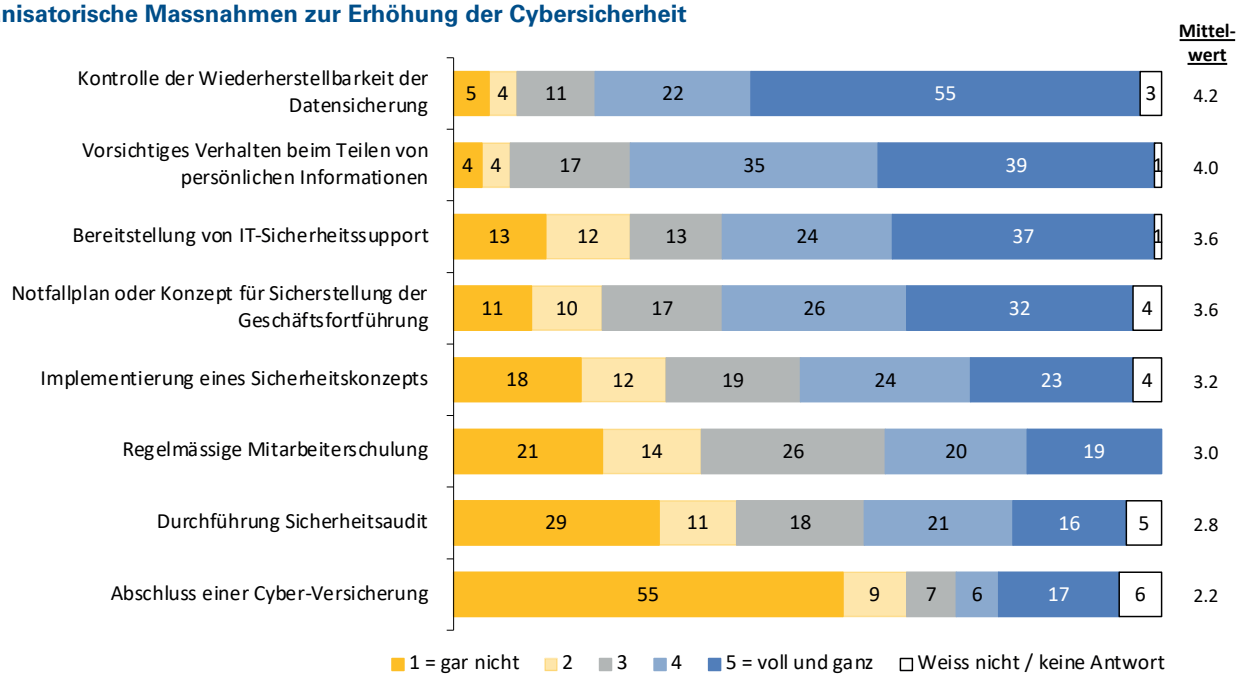
- Haben Sie Ihre IT-Infrastruktur inventarisiert; gibt es eine Liste der Hardware und Software (mit Seriennummern, Einkaufsdatum/-preis und Softwareversionen etc.)?
- Welche IT-Infrastruktur wird durch wen und wie oft aktualisiert?
- Wie schützen Sie Ihre IT-Infrastruktur, um die Weiterführung des Geschäftes bei Angriffen und anderen Problemen sicherzustellen?
- Welche konkreten organisatorischen Massnahmen sollten geplant und umgesetzt werden?
- Sollten Sie ggf. ein IT-Sicherheitsaudit durchführen und eine Cyberversicherung abschliessen?

Technische Massnahmen zur Erhöhung der Cybersicherheit



Technische Massnahmen zur Erhöhung der Cybersicherheit («Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?» / n = 506 / Skala von 1 = gar nicht bis 5 = voll und ganz, Angaben in Mittelwerten).
Die gezeichnete Illustration beinhaltet die Werte 4 und 5 der 5er-Skala.

Organisatorische Massnahmen zur Erhöhung der Cybersicherheit



Organisatorische Massnahmen zur Erhöhung der Cybersicherheit («Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cyber-Sicherheit bei Ihnen umgesetzt?» / n = 506 / Skala von 1 = gar nicht bis 5 = voll und ganz, Angaben in Mittelwerten)
Die gezeichnete Illustration beinhaltet die Werte 4 und 5 der 5er-Skala.

die Mobiliar

Die Gruppe Mobiliar («Mobiliar») ist die führende Schweizer Retail-Versicherung und die Nummer eins für Haushalt-, KMU- und Risikolebensversicherungen. 1826 gegründet, ist sie die älteste private Versicherungsgesellschaft der Schweiz und bis heute genossenschaftlich verankert.
Ihre 80 unternehmerisch geführten Generalagenturen mit eigenem Schadendienst garantieren an 160 Standorten persönliche Nähe zu den über 2,2 Millionen Kundinnen und Kunden. So ist jeder dritte Haushalt und jedes dritte Unternehmen in der Schweiz bei der Mobiliar versichert. Als Allbranchenversicherer beschäftigt die Mobiliar 5856 Mitarbeitende und bietet 338 Ausbildungsplätze an.

Das Cyberschutz Angebot für KMU Kunden im Überblick

Kurzbeurteilung der Cybersicherheit
Die Kurzbeurteilung ist eine kostenlose Überprüfung der Cybersicherheit von Unternehmen mit konkreten Handlungsempfehlungen zur Verbesserung der Sicherheit und bietet dem KMU folgende Mehrwerte:

- Neutrale, standardbasierte Einschätzung der aktuellen Cybersicherheit
- Vergleich der Risikosituation des KMU mit anderen Unternehmen
- Konkrete, individuelle Handlungsempfehlungen mit Verweis auf zusätzliche Informationsquellen

Weitere Informationen unter
www.mobiliar.ch/kurzbeurteilung-cybersicherheit

Cybertraining für Unternehmen
Es ist schnell passiert: Ein Mitarbeiter öffnet unbedacht ein E-Mail und plötzlich steht das ganze Unternehmen still. Das Cybertraining sensibilisiert Mitarbeitende im Umgang mit Internet und E-Mail.
Nach diesem Cyber-Sensibilisierungstraining kennen die Mitarbeitenden des Betriebs die unterschiedlichen Methoden der Hacker und wissen, wie sie richtig darauf reagieren.
Das Cyber-Sensibilisierungstraining besteht aus verschiedenen Bausteinen:

- Online-Trainingssequenzen zum Umgang mit Bedrohungen aus dem Internet
- Simulierte Phishing-Attacken mit Auswertung der Mitarbeiterreaktion
- Bericht mit den wichtigsten Erkenntnissen aus der Trainingseinheit

Weitere Informationen unter
www.mobiliar.ch/cyber-training

Cyberversicherung
Die Cyberversicherung ist ein umfangreiches Massnahmenpaket, mit dem der Betrieb der KMU nach einer Cyberattacke abgesichert wird. Die Versicherung deckt die folgenden Punkte ab:

- Kostenübernahme für Spezialisten, die Schadprogramme entfernen, Daten wieder verfügbar machen und gegen eine angedrohte Veröffentlichung angehen.
- Entschädigung eines Betriebsausfalls, falls das KMU mehr als zwölf Stunden nicht arbeiten kann.
- Finanzielle und rechtliche Hilfe, wenn ein Kunde dem KMU vorwirft, dass das E-Mail des KMU mit Viren infiziert war und Schaden angerichtet hat.

Weitere Informationen unter
www.mobiliar.ch/cyberschutz-unternehmen

Eine Zusammenstellung nützlicher Informationen für KMU, auch zum Thema Cyber, finden Sie unter
www.mobiliar.ch/kmu

Cybersicherheitsmassnahmen aufgrund der Homeoffice-Pflicht

Zusätzliche Investitionen in Software, Firewall und Passwörter

Mit der Zunahme von Cyberangriffen und dem Homeoffice als Arbeitsort für viele Mitarbeitende haben die Schweizer KMU auch mit zusätzlichen Cybersicherheitsmassnahmen reagiert. 23 % der KMU (2020: 9 %) haben aufgrund der Homeoffice-Pflicht/-Empfehlung zusätzliche Massnahmen umgesetzt. Dies wiederum speziell in KMU, in welchen sich die Geschäftsleitenden als (eher) informiert zur Cyberthematik einschätzen (30 %).

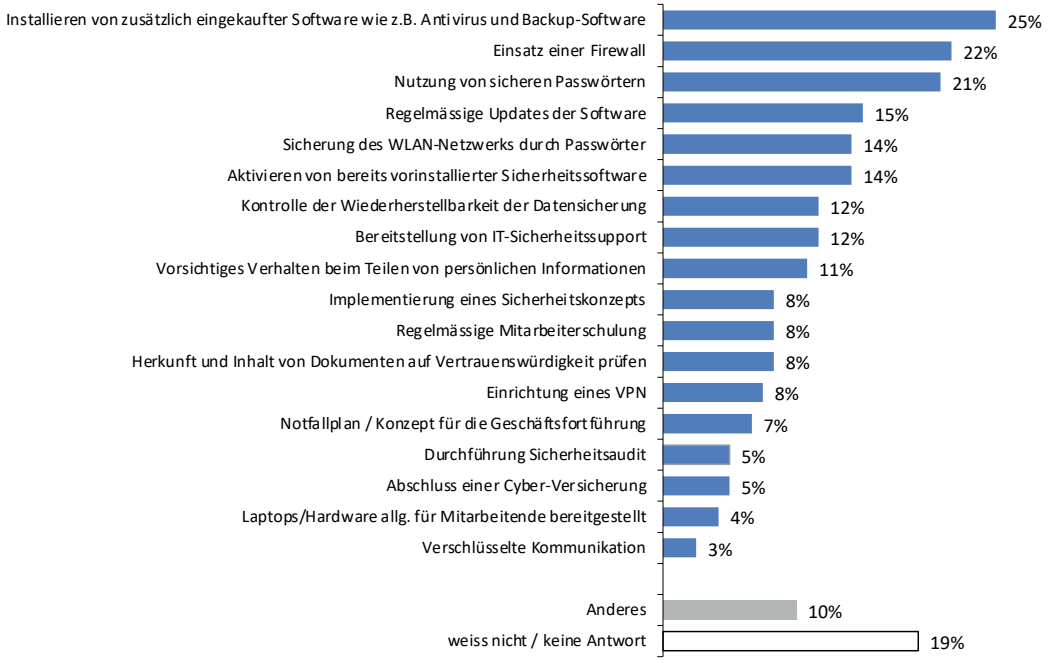
Zu den wichtigsten Massnahmen gehören die Installation zusätzlich eingekaufter Software (25 %), der Einsatz einer Firewall (22 %), die Nutzung sicherer Passwörter (21 %) und regelmässige Software-Updates (15 %).

Zu den Massnahmen gehören ebenfalls die Bestimmung von Datenschutzverantwortlichen in Unternehmen (in 64 % der Schweizer KMU), definierte Prozesse zur Herausgabe/Löschung von Daten (28 %) und Führung eines Datenbearbeitungsinventars (20 %).

Fragen für Schweizer KMU:

- Hat sich die IT-Angriffsfläche mit der Zunahme des Homeoffice weiter erhöht?
- Welche Cybersicherheitsmassnahmen sollten Sie in Vorbereitung auf die nächsten Monate zwingend bzw. sofort implementieren?
- Welche weiteren Massnahmen sollten geplant werden, um langfristig die Cybersicherheit zu erhöhen?
- Wurde ein/e Mitarbeiter/in mit der Verantwortung für den Datenschutz bestimmt und wurden entsprechende Reglemente/Prozesse eingeführt?

Cybersicherheitsmassnahmen aufgrund der Homeoffice-Pflicht



Cybersicherheitsmassnahmen aufgrund der Homeoffice-Pflicht («Welche Sicherheitsmassnahmen haben Sie während dem Lockdown umgesetzt? / n = 118 (Filter: wenn im Zuge des Corona-Lockdowns zusätzliche Sicherheitsmassnahmen gegen Cyberangriffe umgesetzt wurden) / vorcodierte, halboffene Frage)

Praxisumsetzung für Schweizer KMU

Themen und Fragen für die Umsetzung in Ihrem Unternehmen

Auf Grundlage dieser Studie und den identifizierten Themen und Herausforderungen in KMU haben die Autorinnen und Autoren diese Checkliste für Diskussionen und die Projektarbeit zusammengestellt.

Bei der Umsetzung dieser wichtigen Themen wünschen wir Ihnen viel Erfolg.

Arbeitsweltstrategie und Umsetzung des Homeoffice

- ☐ Wie nutzen Sie das Homeoffice strategisch, um die Flexibilität und Attraktivität für Arbeitnehmende zu erhöhen und Ihre Kostenstruktur zu reduzieren?
- ☐ Haben Sie mit Ihren Mitarbeitenden zusammen das Thema Homeoffice bereits diskutiert und so Ideen/Potenziale sowie eine Roadmap entwickelt?
- ☐ Wird sich das Homeoffice bei Ihnen langfristig etablieren – haben Sie die Potenziale identifiziert und diskutiert?
- ☐ Gibt es eine Homeoffice-Vereinbarung, z. B. zur Regelung der Kostenübernahme von privater Büroausrüstung?
- ☐ Haben Sie die Anforderungen an New Work (an die Arbeitswelt 4.0) zu den Themen Kultur, Führung und Kommunikation identifiziert und definiert?
- ☐ Haben Sie eine Strategie mit einer Roadmap für die Arbeitswelt 4.0 entwickelt?
- ☐ Welche positiven und negativen Erfahrungen haben Sie mit dem Homeoffice während den Lockdowns gemacht – was können Sie daraus lernen und verbessern?
- ☐ Weshalb nutzen Sie das Homeoffice nicht intensiver und strategisch zur Erneuerung Ihres Unternehmens; z. B. zur Stärkung der Arbeitgebendenreputation?
- ☐ Wurde ein Konzept zum Einsatz von Kommunikationstools erarbeitet (und wurden anschliessend die zweckmässigsten Plattformen implementiert)?
- ☐ Gibt es ein Konzept und Vorgaben zur Datensicherheit für die geschäftliche Nutzung dieser Kommunikationsplattformen?
- ☐ Sind die Plattformen sicher; welche Informationen/Daten werden bzw. dürfen über welche Plattformen ausgetauscht werden?

Strategien und Massnahmen zur Cybersicherheit

Wissensaufbau und Sensibilisierung

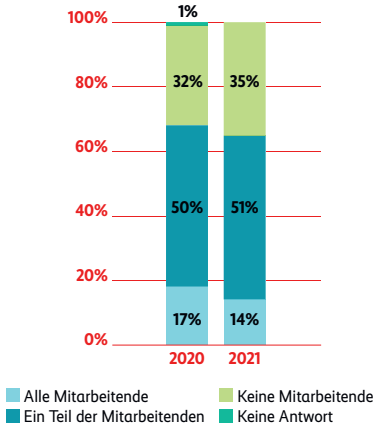
- ☐ Identifizieren Sie regelmässig die Potenziale für den Einsatz neuer Technologien und existiert eine Strategie/Roadmap für die Einführung neuer IT-Infrastruktur?
- ☐ Welche neuen Produkte und Leistungen könnten Sie durch Investitionen in die IT und Cybersicherheit erfolgreich(er) im Markt einführen?
- ☐ Erfüllen Sie Ihre eigenen Anforderungen (oder diejenigen des Marktes) an die Cybersicherheit?
- ☐ Wie informieren Sie sich regelmässig über Gefahren sowie Konzepte und Lösungsansätze zur Erhöhung der Cybersicherheit?
- ☐ Kennen die Mitarbeitenden die diversen Angriffstechniken; wie sensibilisieren Sie und wie erfolgt die Aufklärung?
- ☐ Welche technischen und organisatorischen Massnahmen treffen Sie, um die Cybersicherheit in Ihrem Unternehmen zu erhöhen?
- ☐ Wie überprüfen Sie regelmässig Ihre Konzepte und Massnahmen zur Cybersicherheit?

Konzepte und Massnahmen

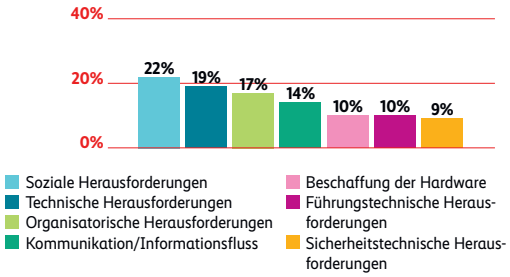
- ☐ Welche IT-Infrastruktur ist kritisch für die Leistungserbringung in Ihrem Unternehmen bzw. wie wichtig ist für Sie die Cybersicherheit?
- ☐ Welche Leistungen können Sie nicht erbringen, wenn die IT nicht läuft?
- ☐ Wie schützen Sie diese IT-Infrastruktur?
- ☐ Welche Alternativen (sogenannte Recovery-Konzepte) haben Sie vorbereitet?
- ☐ Welche Notfallkonzepte/-pläne bestehen bzw. welche Komponenten fehlen Ihnen?
- ☐ Haben Sie Ihre IT-Infrastruktur inventarisiert; gibt es eine Liste der Hardware und Software (mit Seriennummern, Einkaufsdatum/-preis und Softwareversionen etc.)?
- ☐ Welche IT-Infrastruktur wird durch wen und wie oft aktualisiert?
- ☐ Wie schützen Sie Ihre IT-Infrastruktur, um die Weiterführung des Geschäftes bei Angriffen und anderen Problemen sicherzustellen?
- ☐ Welche konkreten organisatorischen Massnahmen sollten geplant und umgesetzt werden?
- ☐ Sollten Sie ggf. ein IT-Sicherheitsaudit durchführen und eine Cyberversicherung abschliessen?
- ☐ Hat sich die IT-Angriffsfläche mit der Zunahme des Homeoffice weiter erhöht?
- ☐ Welche Cybersicherheitsmassnahmen sollten Sie in Vorbereitung auf die nächsten Monate zwingend bzw. sofort implementieren?
- ☐ Welche weiteren Massnahmen sollten geplant werden, um langfristig die Cybersicherheit zu erhöhen?
- ☐ Wurde ein/e Mitarbeiter/in mit der Verantwortung für den Datenschutz bestimmt und wurden entsprechende Reglemente/Prozesse eingeführt?

Infografiken «Homeoffice und Cybersicherheit in Schweizer KMU 2021»

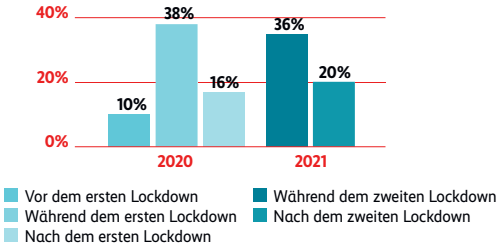
Anzahl Mitarbeitende, die potenziell im Homeoffice arbeiten könnten



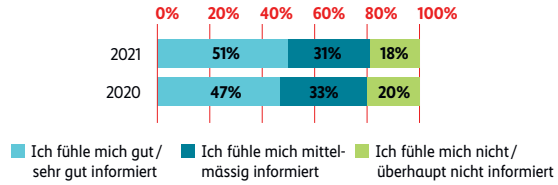
Die sieben grössten Herausforderungen bei der Umsetzung des Homeoffice



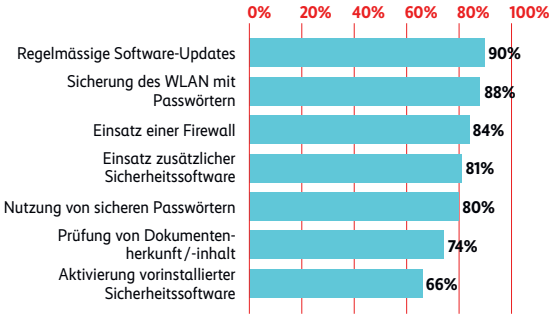
Veränderung der Homeoffice-Gewohnheiten während des Corona-Lockdowns



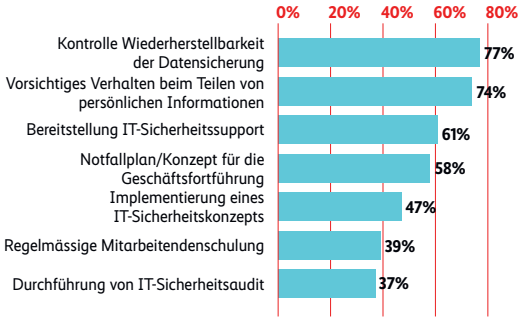
Persönliche Informiertheit



Technische Massnahmen zur Erhöhung der Cybersicherheit



Organisatorische Massnahmen zur Erhöhung der Cybersicherheit



Kontakt / Autorinnen und Autoren

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

Andreas Hölzli
Leiter Kompetenzzentrum
Cyber Risk
Die Mobiliar, Bern
andreas.hoelzli@mobi.ch

Andreas W. Kaelin
Stellvertretender Geschäftsführer
und Leiter des Dossiers
Cybersecurity
digitalswitzerland, Bern
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, Andreas Hölzli, 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 im Umfeld von Corona (COVID-19)

— Die Mobiliar
— digitalswitzerland
— Hochschule für Wirtschaft FHNW
— SATW
— gfs-zürich

www.cyberstudie.ch
Bern, November 2021