Homeoffice und Cybersicherheit in Schweizer KMU

Strategien und Massnahmen in Schweizer KMU mit 4–49 Mitarbeitenden nach zwei Jahren mit COVID-19

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

Studie Nr. 3

Die KMU-Transformation und Corona (COVID-19)

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

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 nach zwei Jahren mit COVID-19

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

Bern, Juni 2022

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

Lektorat: Nadine Kammermann, 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

Die telefonische Stichprobe wurde vom 28. Februar bis 30. März 2022 mit 504 Geschäftsführenden von kleinen Unternehmen (4 bis 49 Mitarbeitende) in der deutsch-, französisch- und italienisch-sprachigen Schweiz erhoben.

Die durch die Stichprobe abgebildete Grundgesamtheit umfasst rund 153 000 Firmen mit 4 bis 49 Mitarbeitenden in allen Landesteilen (BfS, Statistik der Unternehmensstruktur STATENT 2017, Vers. 22.08.2019).

Das Vertrauensintervall der Gesamtstichprobe liegt bei +/- 4.4 Prozent bei einer Sicherheit von 95 Prozent (50/50 Verteilung). Die Erhebung zeigt ein 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 Ausschöpfungsquote liegt bei 3.6 Prozent, was einem üblichen Wert bei der vorliegenden Methode und Zielgruppe entspricht (22 909 Anrufe abzüglich 8851 nicht erreichbare Kontakte = 14 058 Kontakte für 504 realisierte Interviews (bzw. 2.2 % im Verhältnis zu gesamthaft durchgeführten Anrufen).

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, der Allianz Digitale Sicherheit Schweiz ADSS, von gfs-zürich und von Die Mobiliar, hat sich zum Ziel gesetzt, mittels eines Forschungsprojekts und dieser Publikation einen Beitrag zum Verständnis und zur Stärkung von Schweizer KMU mit 4 bis 49 Mitarbeitenden im Umfeld von Digitalisierung, modernen Arbeitswelten, Risiken der Cyberkriminalität sowie Massnahmen zur Erhöhung der Cybersicherheit zu leisten.

Die drei durchgeführten Studien von 2020 bis 2022 geben Einblicke in den Stand der Homeoffice-Nutzung und der Cybersicherheit in KMU, getrieben durch die Ereignisse von COVID-19 seit Anfang 2020. Die erste Befragung fand zwischen den ersten beiden Pandemiewellen 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. Ab dem 18. Januar 2021 wurde Homeoffice für alle Unternehmen verpflichtend. Die zweite Befragung fand im Anschluss an die Aufhebung der Homeoffice-Pflicht für Betriebe, die regelmässig testen, statt (ab 31. März 2021), bzw. begann kurz bevor für alle Unternehmen am 26. Juni 2021 die Überführung in eine Homeoffice-Empfehlung erfolgte. (Die zweite Befragung wurde im Zeitraum vom 16. Juni bis zum 27. Juli 2021 durchgeführt.) Im Winter 2021/2022 wurden die Schweizer Arbeitgebenden ein drittes Mal durch einen bundesrätlichen Beschluss verpflichtet, ihre Mitarbeitenden ins Homeoffice zu senden, «[…] wo dies aufgrund der Art der Aktivität möglich und mit verhältnismässigem Aufwand umsetzbar ist» (Verordnung über Massnahmen in der besonderen Lage zur Bekämpfung der Covid-19-Epidemie, 17.12.2021, Art. 25, Abs. 5). Diese letzte Homeoffice-Pflicht galt vom 20. Dezember 2021 bis am 3. Februar 2022 und wurde dann ebenfalls in eine Empfehlung überführt, wobei der Schutz vor einer Ansteckung immer noch gewährleistet werden musste, beispielsweise mit einer Maskenpflicht am Arbeitsplatz. Die nun vorliegende dritte Studie fusst auf einer telefonischen Stichprobe vom 28. Februar bis zum 30. März 2022 mit 504 Geschäftsführenden von kleinen Unternehmen (4 bis 49 Mitarbeitende) in der deutsch-, französisch- und italienischsprachigen Schweiz. Wichtig anzumerken ist, dass Teilzeit-Homeoffice-Angebote und -nutzung aufgrund der Fragestellung in dieser Studie nicht erfasst wurden.

Diese Studie zeigt: Anfang 2022 herrscht eine gewisse Homeoffice-Müdigkeit bei den Arbeitgebenden. Sie können oder wollen Homeoffice im Mix ihrer Arbeitswelt-Konzepte nicht (mehr) aktiv anbieten. Während Mitte 2020 bei 67 % und Mitte 2021 bei 65% der befragten KMU alle oder ein Teil der Mitarbeitenden theoretisch von zuhause aus hätten arbeiten können, waren es Anfang 2022 nur noch 61 %. Die Anzahl an homeoffice-tauglichen Stellen sinkt in diesen KMU von durchschnittlich 3.8 in 2020 auf 3.4 in 2021 und 2.9 im Jahr 2022. Es könnte sein, dass sich die Einschätzung der Eignung der Arbeitsstellen für Homeoffice geändert hat oder die Erfahrungen zeigen, dass die Arbeitsausführung vor Ort optimaler ist – oder dass zumindest davon ausgegangen wird.

Bereits 2021 zeichnete sich ab, dass die KMU-Geschäftsleitenden von einem Rückgang der Anzahl Homeoffice-Arbeitsplätze ausgehen. Dies hat sich nun bestätigt: Vor dem ersten Lockdown im März 2020 arbeiteten in KMU, in denen für mindestens eine Mitarbeiterin bzw. einen Mitarbeiter Homeoffice möglich wäre, 10 % zuhause. Dieser Wert vervierfachte sich während des ersten Lockdowns fast (auf 38 %) und sank danach auf 16 % (eine Steigerung von 60 % gegenüber dem Wert vor der Pandemie). Während der Homeoffice-Pflicht des zweiten Lockdowns stieg der Wert wieder auf 36 % , pendelte sich anschliessend, ab Ende 2021, über alle Industrien hinweg auf einem höheren Niveau (20 %) ein und ist nun wieder auf 12 % gesunken und somit fast auf dem Niveau vor Beginn der Pandemie, als er bei 10 % lag. Es besteht allerdings nicht nur ein Zusammenhang zwischen COVID-19 und Homeoffice: Je aufgeschlossener die befragten Geschäftsführenden ihr Unternehmen bezüglich technischer Innovationen beurteilten (die sogenannten Pioniere), desto eher haben die Mitarbeitenden hauptsächlich im Homeoffice gearbeitet.

Die Wichtigkeit der Cybersicherheit wird 2022 ähnlich wie 2021 und 2020 beurteilt: Rund zwei Drittel der Befragten (64 %) beurteilen das Thema Cybersicherheit als eher wichtig bis sehr wichtig (Skalenwerte 4–5), rund ein Siebtel (14 %) beurteilt es als eher bis sehr unwichtig (Skalenwerte 1–2). Der Mittelwert liegt somit im Jahr 2022 mit 3.8 minimal tiefer als 2021 und 2020 (je 3.9). Erwähnenswert ist jedoch, dass der Anteil der KMU-Geschäftsleitenden, die das Thema als sehr wichtig empfinden, kontinuierlich abnimmt (von 42 % in 2020 über 41 % in 2021 auf 35 % in 2022). Zum Thema selbst fühlen sich die KMU-Geschäftsleitenden weiterhin recht gut informiert

(die Hälfte eher gut oder sehr gut informiert). Der Mittelwert liegt wie 2021 bei 3.5. Je aufgeschlossener die Unternehmen gegenüber technischen Innovationen sind, desto besser sind sie informiert und desto besser werden die Sicherheitsmassnahmen umgesetzt.

Nachdem der Anteil an Unternehmen, die von einem Cyberangriff betroffen waren, der zu einem erheblichen Aufwand zur Beseitigung der Schäden führte, von 25 % in 2020 auf 36 % in 2021 stieg, sinkt er 2022 um wenige Prozentpunkte auf 31 %. Die Einschätzung des Risikos, durch einen Cyberangriff einen Tag lang ausser Kraft gesetzt zu werden, steigt 2022 jedoch zum zweiten Mal leicht an: 2020 lag der Mittelwert bei 2.1 (von 5), stieg 2021 auf 2.4 und liegt nun im Jahr 2022 bei 2.5. Der Anteil an Befragten der das Risiko als eher hoch oder sehr hoch einschätzt, aufgrund eines Cyberangriffs einen Tag lang ausser Kraft gesetzt zu werden, liegt mittlerweile bei knapp einem Fünftel (18 %). Ausserdem gilt: Wer schon einmal von einem Cyberangriff betroffen war, schätzt das Risiko ebenfalls höher ein (2.6) als (noch) nicht Betroffene (2.4). Ein Cyberangriff als existenzgefährdendes Vorkommnis ist nur für wenige Geschäftsführende ein realistisches Szenario, aber auch diese Einschätzung steigt seit 2020 kontinuierlich. 2020 lag der Mittelwert bei 1.5 (von 5), im Jahr 2021 bei 1.7 und 2022 bei 1.9.

Zur Steigerung der Cybersicherheit werden weiterhin häufiger technische Massnahmen (wie regelmässige Software-Updates (86 %) und die Sicherung von WLAN-Netzwerken mit Passwörtern (82 %)) als organisatorische umgesetzt. Je höher der selbst eingeschätzte Informationsgrad der oder des KMU-Geschäftsleitenden ist, desto höher ist auch die Massnahmenumsetzung. Bei den organisatorischen Massnahmen gibt es noch immer viel Verbesserungspotenzial. Die Implementierung eines Sicherheitskonzepts (44 %), regelmässige Mitarbeiterschulungen (34 %) und die Durchführung von IT-Sicherheitsaudits (32 %) werden am seltensten umgesetzt. Auch hier gilt: Je besser sich die Befragten über die Cyberrisk-Thematik informiert fühlen, desto mehr organisatorische Massnahmen treffen sie zur Verbesserung der Cybersicherheit. Die Studie zeigt, dass es fast ein Drittel (29 %) der Befragten für sehr wahrscheinlich hält, in den nächsten ein bis drei Jahren ihre Sicherheitsmassnahmen gegen Cyberkriminalität zu erhöhen. Und zudem: Wer schon einmal von einem Angriff betroffen war, will die Massnahmen eher erhöhen als jemand, der noch nie betroffen war.

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 Juni 2022

Andreas Hölzli
Leiter Kompetenzzentrum Cyberrisk
Die Mobiliar, Bern

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

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

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

Stellenwert und Nutzung des Homeoffice

Wie viele von Ihren Mitarbeitenden könnten theoretisch von zuhause aus arbeiten, müssen also z. B. keine Kundschaft vor Ort bedienen, ein Fahrzeug lenken oder auf einer Baustelle arbeiten?

Anfang 2022 konnten in 61 % der befragten KMU alle oder ein Teil der Mitarbeitenden theoretisch zuhause arbeiten (2021: 65 %, 2020: 67 %). Die Homeoffice-Pflicht galt für Arbeitsstellen, bei denen das Homeoffice aufgrund der Art der Aktivität möglich und mit verhältnismässigem Aufwand umsetzbar war.

Seit 2020 gibt es stetig weniger homeoffice-taugliche Stellen: 2020 waren es durchschnittlich 3.8, 2021 3.4 und 2022 2.9 Arbeitsstellen. Der Rückgang von 2020 auf 2022 ist signifikant und könnte wie folgt erklärt werden:

- Es herrscht eine gewisse Homeoffice-Müdigkeit bei den Arbeitgebenden: Sie können oder wollen das Homeoffice im Mix ihrer Arbeitswelt-Konzepte nicht (mehr) aktiv anbieten.
- Die Einschätzung der Homeoffice-Tauglichkeit einer Arbeitsstellen hat sich verändert, bzw. die Erfahrungen haben gezeigt, dass die Arbeitsausführung vor Ort (im Büro) optimaler ist – oder es wird zumindest davon ausgegangen.

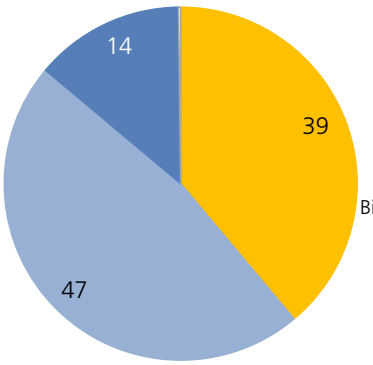
Hervorzuheben sind in diesem Kontext die Pioniere, die im Vergleich zu Early und Late Followern gegenüber dem Homeoffice aufgeschlossener sind: Selbst in diesen KMU könnten 2022 nur noch 69 % aller oder einiger der Mitarbeitenden im Homeoffice arbeiten (2021: 85%).

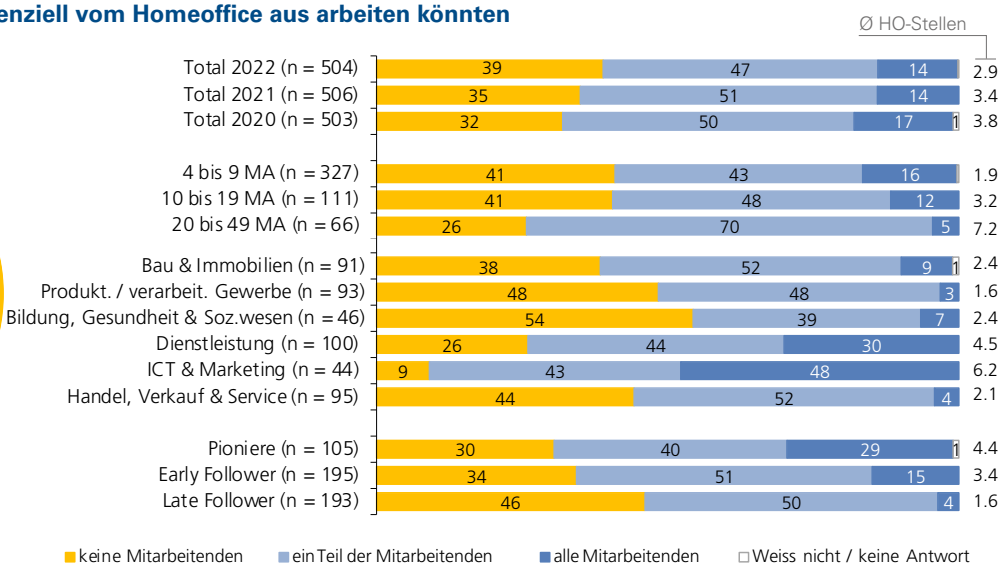
Die Branchen Dienstleistung (4.5) und ICT & Marketing (6.2) verfügen über überdurchschnittlich viele Arbeitsstellen, die im Homeoffice erledigt werden können, während die Branchen Produktion und verarbeitendes Gewerbe (1.6) sowie Handel, Verkauf und Service (2.1) nur wenige solche Arbeitsstellen anbieten.

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 (n 2022=504, n 2021=506, n 2020=503, kategorisiert, Angaben in Prozent, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet)

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 den ersten zwei COVID-19-Jahren

Wie viele Ihrer Mitarbeitenden haben zwischen dem 20. Dezember 2021 und dem 2. Februar 2022 hauptsächlich zuhause gearbeitet, also während der Homeoffice-Pflicht? Und wie viele arbeiten jetzt, nach der Aufhebung der Homeoffice-Pflicht, hauptsächlich zuhause?

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?

Die Anzahl Mitarbeitende im Homeoffice hat sich während und nach den Homeoffice-Pflichten im Laufe der drei Studien von 2020 bis 2022 den jeweiligen Gegebenheiten angepasst. Vor dem ersten Lockdown in 2020 arbeiteten in KMU, in denen für mindestens eine Mitarbeiterin bzw. einen Mitarbeiter Homeoffice möglich wäre, 10 % hauptsächlich zuhause. Dieser Wert hat sich während des ersten Lockdowns fast vervierfacht (auf 38 %) und sank danach auf 16 % (eine Steigerung von 60 % gegenüber dem Wert vor der Pandemie). Während des zweiten Lockdowns hat sich dieser Wert wiederum fast verdreifacht (auf 36 %). Anschliessend hat er sich, Ende 2021, über alle Industrien hinweg auf einem hohen Niveau (bei 20 %) eingependelt. Wie in 2021 angenommen, ist dieser Wert Anfang 2022 ein wenig gesunken. Zudem ist auch während den jeweiligen Phasen mit Homeoffice-Pflicht der Anteil an Mitarbeitenden im Homeoffice ebenfalls leicht (nicht-signifikant) zurückgegangen, nämlich von 38 % (2020) auf 36 % (2021) und nun auf 32 % (2022).

Rund ein Drittel (32 %) der Mitarbeitenden der befragten KMU, die über mindestens eine homeoffice-taugliche Stelle verfügen, sind während der Homeoffice-Pflicht 2021/2022 vornehmlich zuhause geblieben. Besonders hoch war der Anteil an Mitarbeitenden im Homeoffice während der Homeoffice-Pflicht in der Branche ICT & Marketing (60 %), in der auch danach noch ein Viertel der Mitarbeitenden (25 %) zuhause arbeitete. Auch die Branche Dienstleistungen verzeichnet einen hohen Homeoffice-Anteil: Rund zwei Fünftel (43 %) der Mitarbeitenden blieben während der Homeoffice-Pflicht daheim und auch danach blieb gut ein Achtel (13 %) hauptsächlich im Homeoffice.

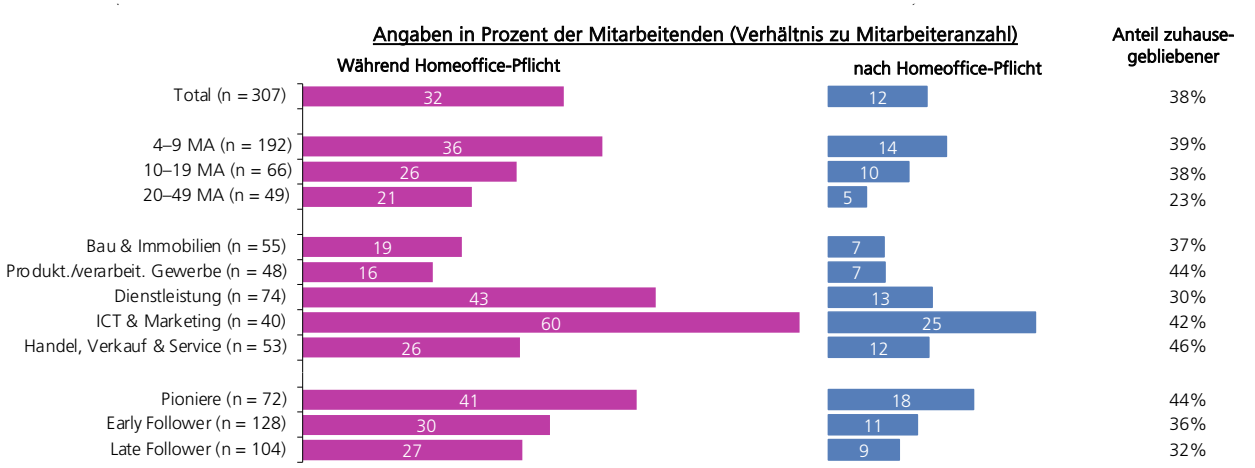
Je aufgeschlossener die befragten Geschäftsführenden ihr Unternehmen bezüglich technischer Innovationen bezeichnen, desto eher arbeiteten die Mitarbeitenden im Homeoffice. Bei den Pionieren waren es während der Homeoffice-Pflicht rund zwei Fünftel (41 %), bei den Early-Followern rund ein Drittel (30 %) und bei den Late Followern rund ein Viertel (27 %). Nach der Aufhebung verblieb bei den Pionieren rund ein Fünftel (18 %), bei den Early und Late Followern rund ein Zehntel (11 bzw. 9 %) der Mitarbeitenden im Homeoffice.

Während nach der ersten Homeoffice-Pflicht noch fast jede/r dritte Geschäftsführende (29 %) der Meinung war, dass zukünftig mehr Mitarbeitende im Homeoffice arbeiten würden, waren es 2021 nur noch halb so viele (15 %). 2022 verbleibt dieser Anteil auf gleichem Niveau (17 %). Rund jede/r dritte Geschäftsführende (30 %) erwartet zukünftig weniger Mitarbeitende im Homeoffice. Etwas mehr als die Hälfte (52 %) der Befragten geht davon aus, dass sich der Anteil an Homeoffice-Mitarbeitenden eingependelt hat, es also zukünftig gleich viele bleiben werden.

Fragen für Schweizer KMU:

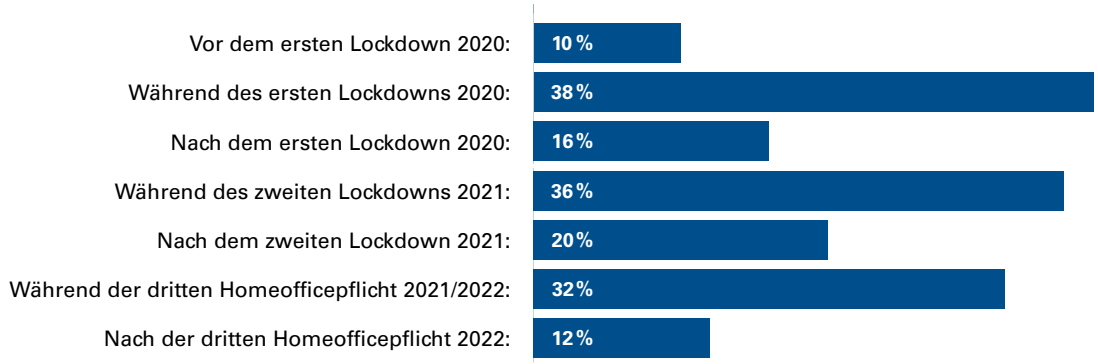
- Gibt es Bereiche in Ihrem Unternehmen, in welchen die Homeoffice-Nutzung von den Mitarbeitenden positiv beurteilt wurde?
- Gäbe es Potenziale, in diesem Bereich das Homeoffice auch nach der Pandemie weiterhin anzubieten?
- Haben Sie für die Mitarbeitenden spezielle Anlässe (z. B. ein Willkommens-Apéro) geplant, um die Rückkehr ins Büro kulturell und kommunikativ zu begleiten?

Veränderung der Homeoffice-Gewohnheiten während der Covid-19-Pandemie 2022



Veränderung der Homeoffice-Gewohnheiten während der Covid-19-Pandemie 2022 (n 2022 = 307, n 2021 = 329, n 2020 = 339, kategorisiert, Angaben in Prozent, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet, Filter: wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann)

Veränderung der Homeoffice-Gewohnheiten während der Covid-19-Pandemie 2020–2022



Veränderung der Homeoffice-Gewohnheiten während der Covid-19-Pandemie 2020–2022 (n 2022 = 307, n 2021 = 329, n 2020 = 339, kategorisiert, Angaben in Prozent, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet, Filter: wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann)

Einschätzung der Veränderung der Homeoffice-Arbeitsplätze

Einschätzung der Veränderung der Homeoffice-Arbeitsplätze (n 2022 = 307, n 2021 = 329, n 2020 = 339, kategorisiert, Angaben in Prozent, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet, Filter: wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann)

Interview zu Homeoffice:

«Die Schattenseiten wurden sichtbar»

Immer weniger Mitarbeitende arbeiten hauptsächlich im Homeoffice. Warum?
Erika Meins, Leiterin des Mobiliar Labs für Analytik an der ETH Zürich, erforscht verantwortungsvolle digitale Interaktionen. Der Trend zu weniger Homeoffice überrascht sie nicht.

Erika Meins ist Leiterin des Mobiliar Labs für Analytik

Erika Meins, Sie erforschen mit Ihrem Team seit fünf Jahren Interaktionen zwischen Mensch und Maschine. Die aktuelle Studie zeigt einen deutlichen Trend vom Homeoffice zurück ins Büro. Wir sind jetzt bei 12 %, die hauptsächlich im Homeoffice arbeiten, gegenüber 38 % beim ersten Lockdown. Wie interpretieren Sie dieses Resultat?
Vor der Pandemie war Homeoffice ein Nischenthema. Etwa 10 % der Mitarbeitenden arbeiteten von daheim und wenn, dann häufig nur einen Tag. Mit dem Lockdown kam der Riesensprung. Die Unternehmen haben stark davon profitiert. Ohne Homeoffice wäre der wirtschaftliche Einbruch während der Pandemie viel grösser gewesen. Dass der Anteil der Mitarbeitenden im Homeoffice nach jeder Homeoffice-Pflicht gesunken ist, erstaunt mich aber nicht. Der Grund liegt darin, dass neben den vielen Vorteilen auch die Schattenseiten von Homeoffice immer deutlicher zutage getreten sind.

Welche Schattenseiten sind das?
Als Dauerzustand hat Homeoffice seine Grenzen. Physische Erschöpfung, emotionale Leere, bis hin zum Verlust vom Raum- und Zeitgefühl – all dies kann bei Mitarbeitenden auftreten, die plötzlich statt im Büro sehr viel oder permanent im Homeoffice sind.

Warum ist das so?
Aus wissenschaftlicher Sicht gibt es dafür verschiedene Erklärungsansätze: Da ist als erstes die «Zoom-Fatigue», die Erschöpfung nach Videokonferenzen. Sie ist mittlerweile gut erforscht. Unser Gehirn benötigt bei Video-Meetings schlicht mehr Energie, um Informationen aufzunehmen. Denn es gibt kleinste Verzögerungen bei der Übertragung, die zwischenmenschliche Kommunikation ist erschwert und auch das ewige Starren auf den Bildschirm strengt an.
Dann das Multitasking: Man bearbeitet parallel zum Meeting noch schnell ein Mail oder liest Handy-Nachrichten – machen wir wohl alle. Aber das reduziert paradoxerweise unsere Fähigkeit, zwischen Aufgaben zu wechseln, und schwächt unsere Merk- und Leistungsfähigkeit.
Auch fehlen im Homeoffice visuelle Eindrücke, Gerüche und Geräusche, die wir sonst automatisch auf dem Arbeitsweg oder am Arbeitsort haben. Ohne wechselnde sensorische Reize verkommen die Tage zum gefühlten Einheitsbrei, alles gleicht sich und man verliert die Orientierung im Alltag. Auch das senkt die Leistung.
Und als Letztes fehlen die physischen persönlichen Interaktionen bei der Arbeit. Das lässt sich virtuell nur bedingt kompensieren. Soziale Kontakte sind jedoch für unsere mentale und körperliche Gesundheit essenziell. Physische soziale Kontakte haben einen beruhigenden und regulierenden Effekt auf das Nervensystem und helfen, Stress zu reduzieren. Bei Face-to-Face ist auch das Gefühl von sozialer Verbundenheit unter Arbeitskollegen am grössten. Erst danach kommen Videocalls, Telefon und – am untersten Ende – Textnachrichten.

Also sollten alle zurück ins Büro?
Zumindest teilweise. Aber wenn keine physischen Treffen stattfinden können, dann lieber einmal einen virtuellen Videoaustausch initiieren oder zum Telefon greifen, als noch eine Mail oder eine Chatnachricht senden. Die vielen digitalen Interaktionsmöglichkeiten sind eine grosse Chance. Aber erst wenn wir sie als Arbeitgebende und -nehmende bewusst und gezielt einsetzen, entsteht ein verantwortungsvoller Einsatz in einer hybriden Arbeitswelt.

Was können Unternehmen tun, um den Nachteilen im Homeoffice entgegenzuwirken?
Allen Unternehmen, speziell auch den KMU, rate ich: Führen Sie mit Ihren Mitarbeitenden einen offenen Dialog. Sie sollten ihre Bedürfnisse kennen. Genauso wichtig ist, dass das Unternehmen seine Erwartungen klar formuliert, zum Beispiel im Hinblick auf Präsenztage und -zeiten und was im Homeoffice gilt bezüglich Erreichbarkeit und Freiräumen. Es braucht klare Abmachungen.

Was können Mitarbeitende tun, damit es ihnen im Homeoffice gut geht?
Am wichtigsten ist es, Pausen einzulegen, damit die Leistungsfähigkeit erhalten bleibt. Insbesondere bei langer Bildschirmtätigkeit sollte man in den Pausen andere physische Erlebnisse ermöglichen: rausgehen in die Natur, ein Buch lesen, soziale Kontakte pflegen. Und Schluss mit Multitasking. Es hilft, Mail- und andere Benachrichtigungen abzuschalten und nicht benutzte Arbeitsprogramme zu schliessen.

Ein Blick in die Kristallkugel: Wohin geht die Entwicklung?
Homeoffice bleibt, aber ersetzt die Präsenzarbeit nicht. Die beiden Arbeitsformen sollten sich sinnvoll und flexibel ergänzen. So vereinen wir das Beste aus beiden Welten.

Mobiliar Lab
für Analytik an der ETH Zürich
Das Mobiliar Lab für Analytik wurde 2013 von der ETH und der Mobiliar ins Leben gerufen und ist Teil des Gesellschaftsengagements der Mobiliar. Seit der Gründung wurden verschiedene interdisziplinäre Forschungsprojekte an der Schnittstelle von Mensch und Maschine durchgeführt. Das Lab hat sich unter anderem zum Ziel gesetzt, digitale Interaktionen für den Menschen weiter zu verbessern und das Vertrauen in sie zu stärken.

Weitere Informationen (in Englisch):
mobiliarlab.ethz.ch

Herausforderungen bei der Umsetzung des Homeoffice

Was sind aus unternehmerischer Sicht die grössten Herausforderungen bei der Umsetzung von Homeoffice?

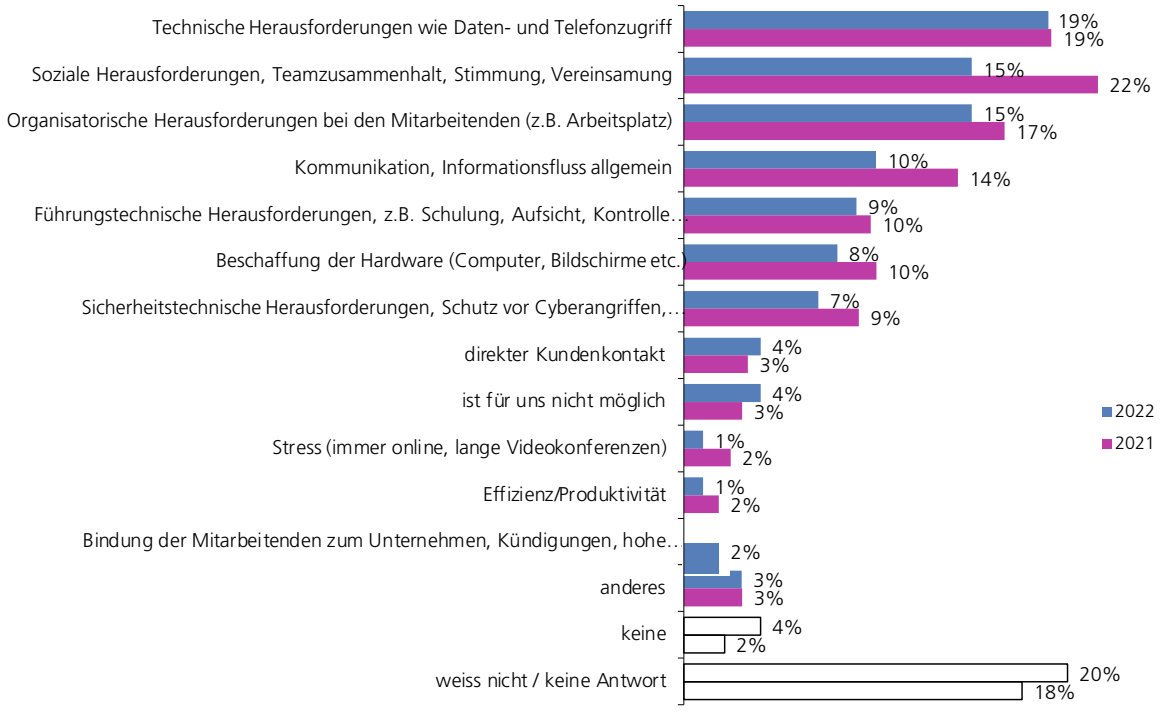
Der soziale/emotionale Faktor (Soziale Herausforderungen, Teamzusammenhalt, Stimmung, Vereinsamung), der technische Faktor (Technische Herausforderungen wie Daten- und Telefonzugriff) sowie der organisatorische Faktor (Organisatorische Herausforderungen bei den Mitarbeitenden wie z. B. der Arbeitsplatz) werden als grösste Herausforderungen bei der Umsetzung des Homeoffices bei etwas über einem Fünftel der KMU betrachtet. Zudem nennt knapp ein Zehntel der Schweizer KMU führungs- und sicherheitstechnische Herausforderungen.

Gegenüber 2021 ist die Beurteilung fast aller Herausforderungen gesunken, was ein Zeichen für die mittlerweile entschärfte Situation bzw. für die implementierten Massnahmen und die bessere IT-Infrastruktur sein dürfte. Wurden 2021 durchschnittlich noch 1.4 Herausforderungen genannt, waren es 2022 derer noch 1.2. Am deutlichsten ging die Beurteilung von soziale Herausforderungen, Teamzusammenhalt, Stimmung und Vereinsamung zurück (2021: 22 %, 2022: 15 %). Dieser Aspekt fällt damit von Rang 1 auf Rang 2 zurück, den er sich mit organisatorischen Herausforderungen (ebenfalls 15 %) teilt. Technische Herausforderungen wie Daten- und Telefonzugriff rücken damit neu auf Rang 1 vor mit einem gegenüber 2021 unveränderten Wert (2021 und 2022: 19 %).

Fragen für Schweizer KMU:

- Welche positiven und negativen Erfahrungen haben Sie mit dem Homeoffice während Covid-19 gemacht – was können Sie daraus lernen und verbessern?
- Weshalb nutzen Sie das Homeoffice nicht intensiver und strategisch zur Erneuerung Ihres Unternehmens; z. B. für die Talent-Suche für Ihre Firma?

Herausforderungen bei der Umsetzung des Homeoffice



Herausforderungen bei der Umsetzung des Homeoffice (n 2022 = 307, n 2021 = 329, n 2020 = 339, Mehrfachnennungen möglich, kategorisiert, Angaben in Prozent, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet, Filter: wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann)

Verwendung von Kommunikationstools

Ich lese Ihnen jetzt einige digitale Kommunikationsmittel vor. Welche davon nutzen Ihre Mitarbeitenden aktuell für Partner, Kundschaft und andere Mitarbeitende?

Telefon (97 %) und E-Mail (97 %) sind auch 2022 die am häufigsten verwendeten Kommunikationsmittel der befragten Unternehmen. Gegenüber dem Jahr 2021 gibt es nur geringe Veränderungen. Ein Vergleich mit 2020 ist nur unter Vorbehalt möglich, da damals teilweise andere Antwortkategorien definiert wurden. Der Einsatz von Online-Konferenztools stieg zwischen 2020 und 2021 von knapp der Hälfte (46 %) auf knapp zwei Drittel (64 %) und stagniert 2022 auf hohem Niveau (62 %). Auch Online-Beratungen/-schulungen stiegen von 2020 auf 2021 auf knapp zwei Fünftel (2020: 20 %, 2021: 39 %) und bleiben nun auf diesem Wert (2022: 39 %).

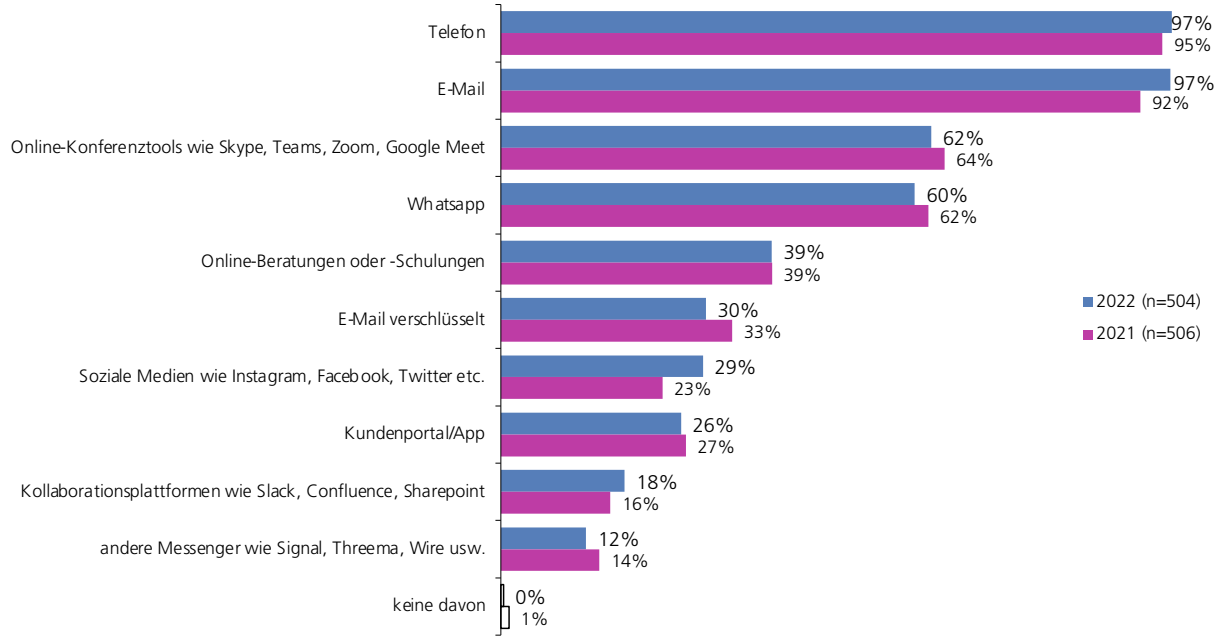
Online-Konferenztools (91 %), Online-Beratungen/-Schulungen (64 %) und Kollaborationsplattformen (64 %) werden in der ICT- & Marketingbranche deutlich häufiger verwendet als in allen anderen Branchen. Diese Branche nutzt generell mehr Kommunikationsmittel als die anderen; durchschnittlich sind es 6.0, während es bei den anderen Branchen 4.3 bis 4.9 sind. Erwähnenswert ist auch der Anstieg der Nutzung sozialer Medien von 23 % (2021) auf 29 % (2022).

Grundsätzlich gilt: Je mehr Mitarbeitende ein Unternehmen hat und je mehr Mitarbeitende im Homeoffice arbeiten können, desto mehr Kommunikationsmittel werden verwendet. So verwenden Unternehmen mit 4 bis 9 Mitarbeitenden durchschnittlich 4.5 Kommunikationsmittel, Unternehmen mit 10 bis 19 Mitarbeitenden 4.8 und Unternehmen mit 20 bis 49 Mitarbeitenden 5.2. Unternehmen ohne homeoffice-taugliche Arbeitsstellen nutzen durchschnittlich 4 verschiedene Kommunikationsmittel, Unternehmen mit einem Teil homeoffice-tauglichen Arbeitsplätzen 4.9 und Unternehmen mit ausschliesslich homeoffice-tauglichen Stellen 5.7. Auch die Einstellung zu technischen Innovationen wirkt sich auf Anzahl genutzter Kommunikationsmittel aus: Pioniere nutzen durchschnittlich 5.7 verschiedene Kommunikationsmittel, Early Follower 5.0 und Late Follower 3.9.

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 (n 2022=504, n 2021=506, Mehrfachnennungen möglich, kategorisiert, Angaben in Prozent, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet)

Persönliche Informiertheit zur Cyberrisk-Thematik

Ganz allgemein: Wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert?

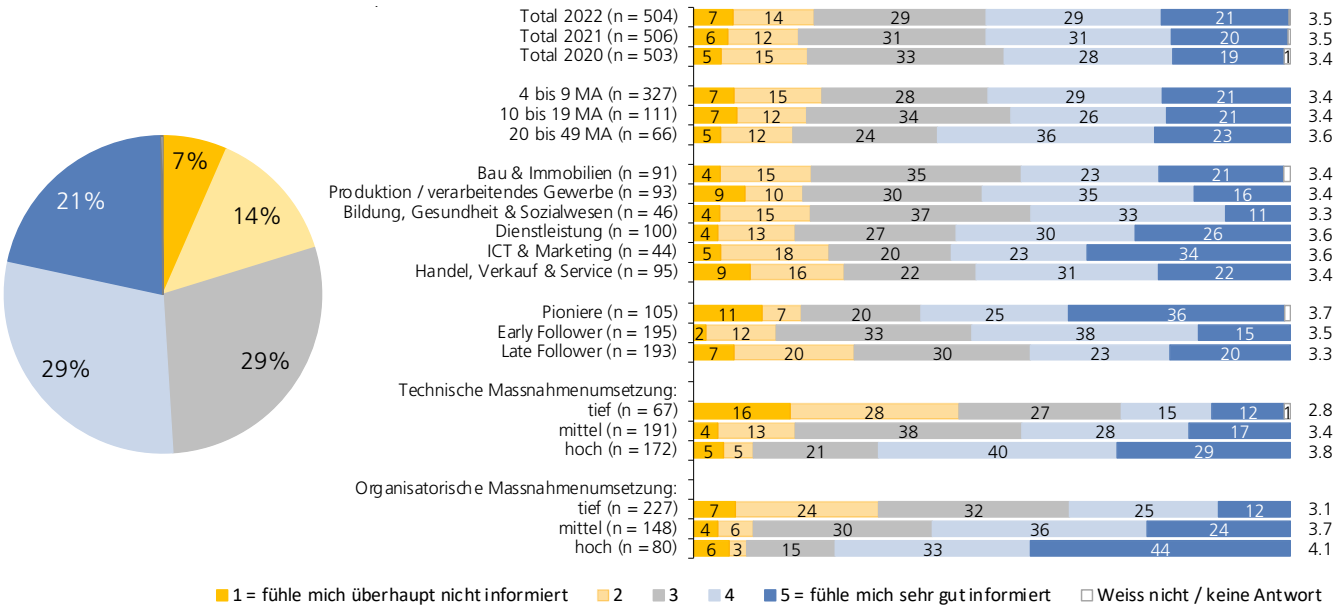
Die Hälfte (50 %) der befragten Geschäftsführenden fühlt sich eher gut oder sehr gut informiert (Skalenwerte 4–5) bezüglich der Cyberrisk-Thematik, rund ein Fünftel (21 %) eher schlecht oder sehr schlecht (Skalenwerte 1–2). Der Mittelwert liegt somit bei 3.5 und ist unverändert gegenüber dem Vorjahr und nur minimal verändert gegenüber 2020 (3.4). Die grössten Unternehmen (20–49 Mitarbeitende) fühlen sich am besten informiert (Mittelwert 3.6), die beiden anderen KMU-Kategorien (4–9 bzw. 10–19 Mitarbeitende) liegen mit einem Mittelwert von 3.4 leicht tiefer (Unterschied nicht signifikant). Je aufgeschlossener die Unternehmen gegenüber technischen Innovationen sind und je stärker die technischen und organisatorischen Sicherheitsmassnahmen umgesetzt sind, desto besser fühlen sich die Geschäftsführenden auch über Cyberrisiken informiert.

Die Branchen ICT & Marketing sowie Dienstleistungen schätzen ihren Informationsgrad am höchsten (je 3.6), aber nicht signifikant höher als die anderen Branchen (3.3 bis 3.4) ein. In den Vorjahren 2020 und 2021 lag die ICT- & Marketingbranche noch signifikant höher als andere Branchen (2020: 4.1, 2021: 4.0). Sie hat also ihre Selbsteinschätzung als einzige Branche stark nach unten korrigiert, während die anderen auf ähnlichem Niveau blieben.

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 Cyberrisk-Thematik (n 2022=504, 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. Der Cybersecurity-Schnelltest von Cybero ermöglicht dem Unternehmen zu beurteilen, ob es ausreichend gegen Cyberrisiken geschützt ist. Mögliche Risiken können identifiziert und besser eingeschätzt werden. Der Schnelltest gibt Anhaltspunkte, wie das Unternehmen sich angesichts der Risiken verhalten kann:

– Verhindern: z. B. Schulungen, Antivirus-Software
– Reduzieren: z. B. Notfallplan, Backup
– Übertragen: z. B. mittels einer Cybersecurity-Versicherung

Der Cybersecurity-Schnelltest wird von folgenden Partnern unterstützt:
digitalswitzerland, Nationales Zentrum für Cybersicherheit (NCSC), Allianz Digitale Sicherheit Schweiz ADSS, Information Security Society Switzerland (ISSS), Schweizerische Akademie der Technischen Wissenschaften (SATW), Schweizerische Normen-Vereinigung (SNV), der Schweizer Organisation für kompetente Zertifizierungs- und Bewertungsdienstleistungen (SQS), 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

Wurde Ihre Firma schon einmal erfolgreich durch eine der folgenden Techniken angegriffen, so dass ein erheblicher Aufwand nötig war, um Schäden zu beheben?

Nachdem der Anteil angegriffener Unternehmen von 2020 auf 2021 signifikant von 25 auf 36 % stieg, sank er 2022 um wenige Prozentpunkte auf 31 %. Wie schon 2021 gibt es keine signifikanten Unterschiede zwischen den Subgruppen; selbst nicht zwischen denjenigen, die sich ansonsten in dieser Studie konsequent unterscheiden, wie zum Beispiel der Informationsgrad oder die Einstellung zu technischen Innovationen. Interessanterweise gilt aber: Je stärker die technischen Sicherheitsmassnahmen umgesetzt werden, desto eher sind die Unternehmen schon einmal angegriffen worden. Dieses Verhältnis bestand schon 2021. Eine mögliche Erklärung ist, dass die betroffenen Unternehmen die entsprechenden Massnahmen nach dem Angriff umgesetzt haben und nun deshalb auf gutem Stand sind.

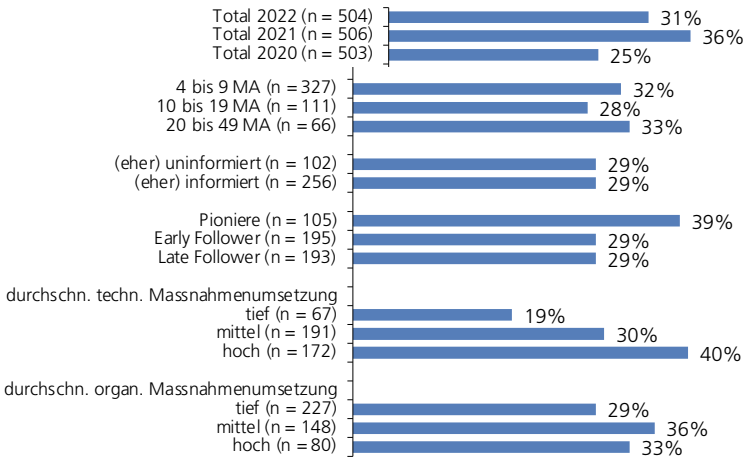
Bei den organisatorischen Massnahmen ergibt sich ein ähnliches, wenn auch nicht ganz so deutliches Bild: Unternehmen mit mittlerer und hoher Massnahmenumsetzung verzeichneten in der Vergangenheit tendenziell häufiger einen erfolgreichen Cyberangriff als Unternehmen mit tiefer Massnahmenumsetzung. Auch dieses Verhältnis bestand schon 2021. Falls die Annahme stimmt, dass Unternehmen die Umsetzung von Massnahmen nach einem erfolgreichen Angriff verstärken, werden mehr (bzw. zuerst) technische als organisatorische Massnahmen umgesetzt.

Die am häufigsten genannten Angriffe erfolgten, wie schon 2021 mit Malware, Viren und Trojanern: Ein Fünftel der Befragten (20 %) wurde so angegriffen. Dieser Wert liegt zwischen dem Ergebnis von 2020 (18 %) und 2021 (23 %). Die zweithäufigste genannte Angriffsform ist Onlinebetrug (11 %). Auch dieser Wert stieg 2021 stark an (von 6 auf 15 %) und sinkt jetzt wieder leicht. Erpressungsfälle steigen seit 2020 stetig an. Die Unterschiede sind aber sehr klein und könnten auch durch Zufall entstanden sein. Datendiebstahl und absichtlich herbeigeführte Überlastungen des Netzes oder des Servers (DoS) liegen konstant bei einem zwanzigstel der Unternehmen vor (5 %).

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

Anteile erfolgreich angegriffener KMU



Anteile erfolgreich angegriffener KMU (n 2022=504, n 2021=506, n 2020=503, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet)

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.
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.
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.
www.satw.ch/de/technik-bildung

Weitere Informationen:

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

Risiken von erfolgreichen Cyberangriffen

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 ausser Kraft setzt?

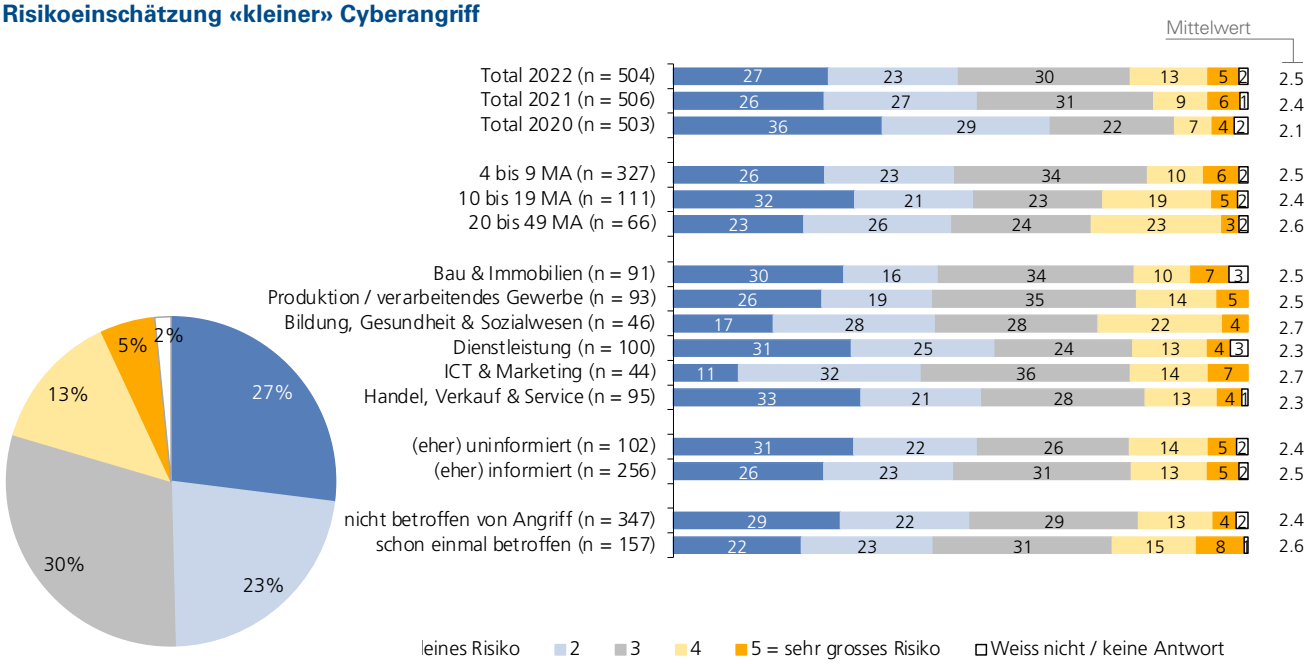
Die Einschätzung des Risikos, durch einen Cyberangriff einen Tag ausser Kraft gesetzt zu werden, steigt 2022 zum zweiten Mal leicht an: 2020 lag der Mittelwert noch bei 2.1, stieg dann 2021 auf 2.4 und liegt nun im Jahr 2022 bei 2.5. Der Anteil an Befragten, die das Risiko als sehr hoch oder eher hoch einschätzen, wegen eines Cyberangriffs einen Tag ausser Kraft gesetzt zu werden, liegt mittlerweile bei knapp einem Fünftel (18 %). Die Hälfte der Befragten (50 %) hält dieses Risiko für eher tief oder sehr tief.

Dieses Sicherheitsgefühl ist zwischen den Subgruppen gleichmässig bzw. innerhalb des Vertrauensbereichs verteilt; es ergeben sich nur wenige signifikante Unterschiede: Late Follower (Mittelwert 2.2) schätzen das Risiko signifikant tiefer ein als Pioniere (2.8) und Early Follower (2.6). Die Einschätzung der Late Follower hat sich gegenüber dem Vorjahr nicht verändert, während die Early Follower und Pioniere das Risiko 2022 etwas höher einschätzen als 2021 (Pioniere: 2.7, Early Follower: 2.5). Ausserdem gilt: Wer schon einmal von einem Cyberangriff betroffen war, schätzt das Risiko ebenfalls höher ein (2.6) als (noch) nicht Betroffene (2.4).

Frage für Schweizer KMU:

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

Risikoeinschätzung «kleiner» Cyberangriff



Risikoeinschätzung existenzgefährdender Cyberangriff (n 2022=504, n 2021=506, n 2020=503, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet)

Risiken von existenzgefährdenden Cyberangriffen

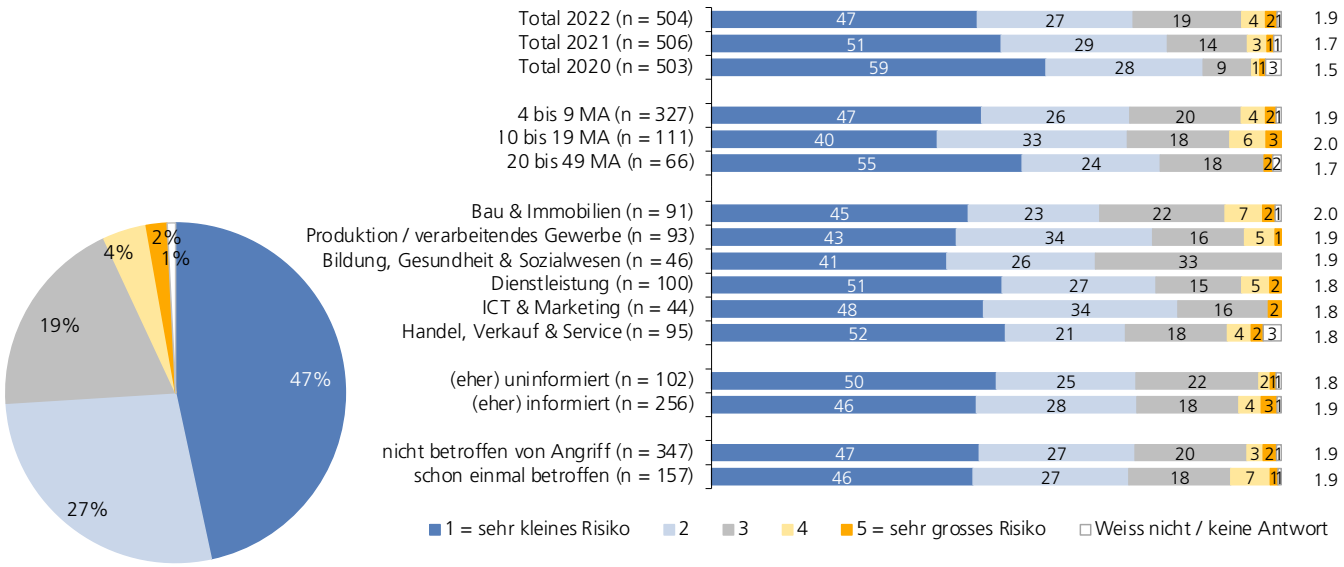
Als wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen innerhalb der nächsten zwei bis drei Jahre von einem Cyberangriff betroffen sein wird, der für Ihr Geschäft existenzgefährdend ist?

Ein existenzgefährdender Cyberangriff ist nur für wenige Geschäftsführende ein realistisches Szenario, aber auch diese Einschätzung steigt seit 2020 kontinuierlich. Damals lag der Mittelwert noch bei 1.5, 2021 bei 1.7 und 2022 bei 1.9. Der Anteil an Befragten, die das Risiko eines existenzgefährdenden Cyberangriffs als eher hoch oder sehr hoch einschätzen, liegt bei rund einem Zwanzigstel (6 %). Als eher tiefes oder sehr tiefes Risiko beurteilen es knapp drei Viertel der Befragten (74 %). Nur bei einer einzigen Subgruppe gibt es einen signifikanten Unterschied: Deutsch- und Westschweizer Unternehmen (2.0 bzw. 1.8) schätzen das Risiko signifikant höher ein als Tessiner Unternehmen (1.4). Anders als bei der vorangegangenen Frage besteht hingegen kein Unterschied zwischen von Cyberangriffen betroffenen und nicht betroffenen Unternehmen (je 1.9); Betroffene nennen also ein höheres Risiko für Cyberangriffe, die ein Unternehmen einen Tag ausser Kraft setzen können, nicht aber ein solches für existenzgefährdende Cyberangriffe.

Frage für Schweizer KMU:

- Welche Alternativen (sogenannte Recovery-Konzepte) haben Sie vorbereitet?
- Wäre es, sofern eine grosse Abhängigkeit von der IT Ihrer Firma besteht, ggf. sinnvoll, in eine parallele IT-Infrastruktur (eine sogenannte «hot site») zu investieren?
- Welche Notfallkonzepte/-pläne bestehen bzw. welche Komponenten fehlen Ihnen?

Risikoeinschätzung existenzgefährdender Cyberangriff



Risikoeinschätzung existenzgefährdender Cyberangriff (n 2022=504, n 2021=506, n 2020=503, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet)

Technische Massnahmen zur Erhöhung der Cybersicherheit

Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

Die Umsetzungsgrade der verschiedenen erhobenen Massnahmen liegen zwischen 3.8 und 4.5 und somit minimal tiefer als 2021. Den höchsten Umsetzungsgrad erzielen regelmässige Softwareupdates» (86 % fast/voll umgesetzt, Mittelwert 4.5), gefolgt von der Sicherung des WLAN-Netzwerks durch Passwörter (82 % fast/voll umgesetzt, Mittelwert 4.5). Den tiefsten Umsetzungsgrad und einen Mittelwert unter 4.0 erreicht das Aktivieren von bereits vorinstallierter Sicherheitssoftware (60 % fast/voll umgesetzt, Mittelwert 3.8). Bei allen Massnahmen gilt: Je höher der selbst eingeschätzte Informationsgrad ist, desto höher ist auch die Massnahmenumsetzung.

Nicht oder nur minimal umgesetzte Massnahmen können unter Umständen ein massgebliches Sicherheitsrisiko bedeuten: einerseits für die Unternehmen selbst, andererseits für die Besitzerinnen bzw. Besitzer der Daten, die dort entwendet werden können (z. B. Kundendaten, Passwörter). Diesen Gedanken berücksichtigend, sollte auch auf tiefe Skalenwerte geachtet werden: So haben zum Beispiel 8 von 100 befragten Unternehmen keine Firewall, 7 von 100 Unternehmen keine zusätzlich eingekaufte Sicherheitssoftware und mehr als jedes zehnte Unternehmen aktiviert die bereits vorinstallierte Sicherheitssoftware nicht. Eine gewisse Ungenauigkeit aufgrund des zu tiefen Wissensstands der Befragten ist dabei aber mitzuberücksichtigen.

Frage für Schweizer KMU:

- Haben Sie Ihre IT-Infrastruktur inventarisiert; gibt es eine Liste der Hardware und Software (mit Seriennummern, Einkaufsdatum/-preis, Softwareversionen etc.)?
- Welche IT-Infrastruktur wird durch wen und wie oft aktualisiert?
- Wie schützen Sie Ihre IT-Infrastruktur, um die Weiterführung des Geschäfts bei Angriffen und anderen Problemen sicherzustellen?

Buchempfehlung

Nicolas Mayencourt & Marc K. Peter

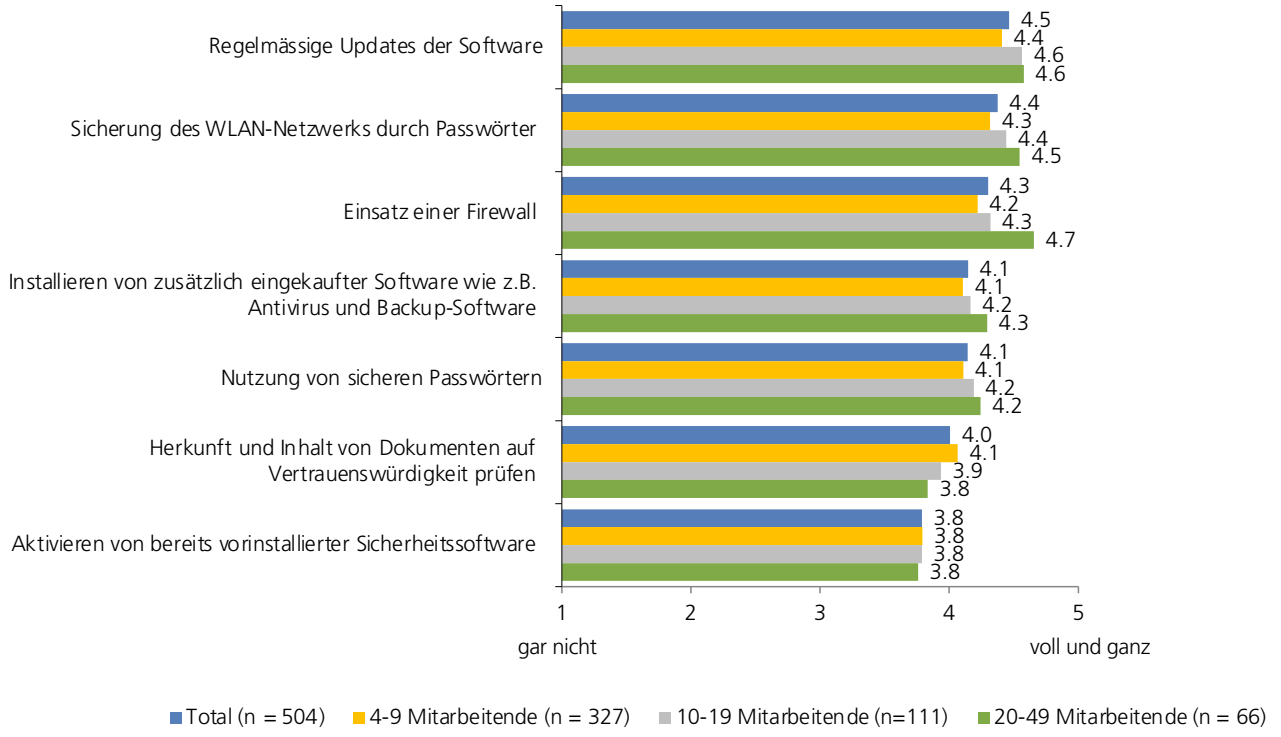
IT-Sicherheit für KMU

So navigieren Sie Ihr Unternehmen sicher durch Cyber-Turbulenzen

1. Auflage 2021, 176 Seiten
ISBN 978-3-03875-343-8

www.it-sicherheit-kmu.ch

Technische Massnahmen zur Erhöhung der Cybersicherheit



Technische Massnahmen zur Erhöhung der Cybersicherheit nach Anzahl Mitarbeitende (n 2022=504)

Organisatorische Massnahmen zur Erhöhung der Cybersicherheit

Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

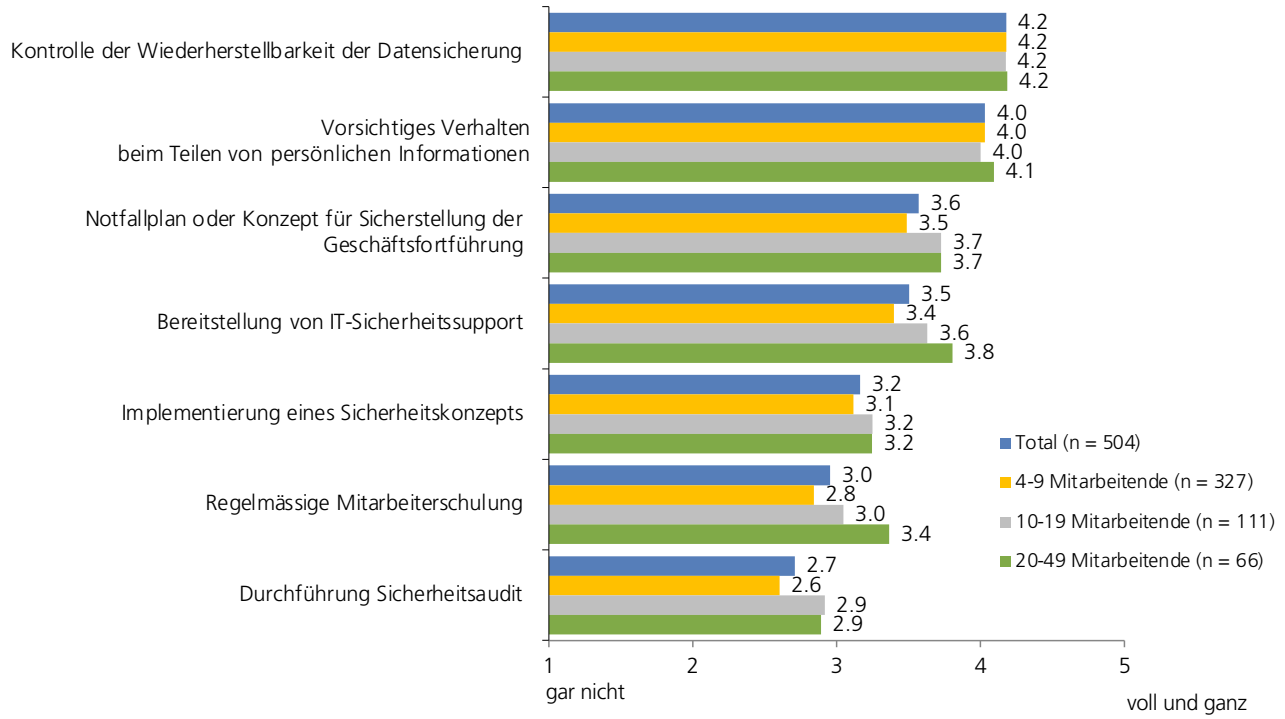
Wie schon in der Vorjahresstudie festgestellt wurde, werden organisatorische Massnahmen immer noch deutlich weniger umgesetzt als technische. Die am häufigsten umgesetzte organisatorische Massnahme ist die Kontrolle der Wiederherstellbarkeit der Datensicherung (4.2). Rund drei Viertel (76 %) der Befragten haben sie fast oder voll und ganz umgesetzt (2021: 77 %). Zum Vergleich: Die am häufigsten vollständig umgesetzte technische Massnahme, regelmässige Softwareupdates, wurde von über vier Fünfteln (86 %) fast oder voll und ganz umgesetzt. An zweiter Stelle der umgesetzten organisatorischen Massnahmen steht das vorsichtige Verhalten beim Teilen von persönlichen Informationen: Fast drei Viertel der Befragten (73 %) haben sie fast oder voll und ganz umgesetzt (2021: 74 %). An dritter Stelle und damit neu einen Platz weiter vorne liegt der Notfallplan oder das Konzept für die Sicherstellung der Geschäftsfortführung mit etwas mehr als der Hälfte (57 %) der Befragten, die diese Massnahme fast oder voll umgesetzt haben (2021: 58 %). Es folgt die Bereitstellung von IT-Sicherheitssupport mit rund der Hälfte (53 %) der Befragten, die sie fast oder voll und ganz umgesetzt haben (2021: 61 %). Die Implementierung eines Sicherheitskonzepts (von 44 % fast oder voll umgesetzt), regelmässige Mitarbeiterschulungen (von 34 % fast oder voll umgesetzt) und die Durchführung von Sicherheitsaudits (von 32 % fast oder voll umgesetzt) werden am wenigsten umgesetzt. Die Unterschiede gegenüber dem Vorjahr sind minimal bzw. nicht signifikant.

Bei der grossen Mehrheit der organisatorischen Massnahmen verhält es sich so, dass Deutschschweizer Unternehmen sie eher als Westschweizer Unternehmen umgesetzt haben, Pioniere eher als Early und Late Follower und bereits von Cyberangriffen betroffene eher als nicht betroffene Unternehmen. Je besser sich die Befragten über die Cyberrisk-Thematik informiert fühlen, desto mehr organisatorische Massnahmen treffen sie zur Verbesserung der Cybersicherheit (bei allen Massnahmen signifikant). Diese Erkenntnis wurde auch schon aus der 2020er- und 2021er-Studie gewonnen.

Frage für Schweizer KMU:

- Welche konkreten organisatorischen Massnahmen sollten geplant und umgesetzt werden?
- Ist Ihr IT-Dienstleister zertifiziert bzw. kompetent genug, um Sie zu unterstützen?
- Sollten Sie ggf. ein IT-Sicherheitsaudit durchführen und eine Cyberversicherung abschliessen?

Organisatorische Massnahmen zur Erhöhung der Cybersicherheit



Organisatorische Massnahmen zur Erhöhung der Cybersicherheit nach Anzahl Mitarbeitende (n 2022=504)

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.

Das Cyberschutz Angebot für KMU Kunden im Überblick

Cyber RedBox-Schwachstellen-Scan
Durch Sicherheitslücken in der IT-Infrastruktur können Internetkriminelle in die Systeme Ihres Betriebs eindringen. Die RedBox identifiziert solche Schwachstellen – damit Sie sie schliessen können, bevor etwas passiert. Der RedBox-Schwachstellen-Scan ist ein innovativer, digitaler Service der Mobiliar, der speziell für KMU ntwickelt wurde. Er hilft Ihnen, Ihr Unternehmen besser vor Cyberattacken zu schützen. Die RedBox scannt permanent Ihre IT-Infrastruktur und warnt Sie, wenn sie neue Schwachstellen findet.

Weitere Informationen unter
www.mobiliar.ch/redbox

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.
- Die IT Assistance hilft Ihnen in IT-Belangen schnell und unkompliziert. Via Remote-Zugriff analysiert und behebt ein Experte Ihre IT-Probleme.

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

Wie cyberfit ist Ihr KMU?
Erfahren Sie in einem kurzen Fitness-Check, wo Sie heute stehen und wo Sie Verbesserungspotenzial haben.
www.mobiliar.ch/cyberfit

Erhöhung der Sicherheitsmassnahmen gegen Cyberkriminalität

Wie wahrscheinlich ist es, dass Sie in den kommenden ein bis drei Jahren die Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden?

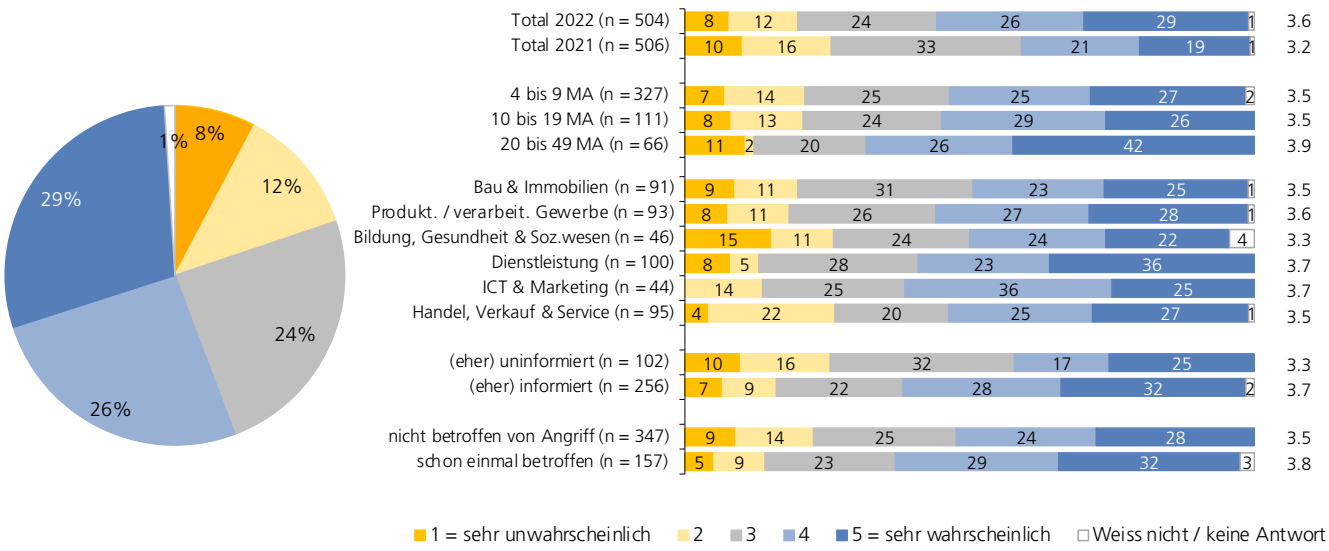
Fast ein Drittel (29 %) der Befragten hält es für sehr wahrscheinlich (Skalenwert 5), dass sie in den nächsten ein bis drei Jahren ihre Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen. Seit dem letzten Jahr (19 %) hat sich dieser Anteil somit um rund die Hälfte erhöht. Rund ein weiteres Viertel (26 %) hält eine Sicherheitserhöhung für eher wahrscheinlich (Skalenwert 4). Der Mittelwert steigt im Vergleich zum Vorjahr von 3.2 auf 3.6.

Pioniere (3.9) und Early Follower (3.7) gehen signifikant häufiger von einer Erhöhung der Sicherheitsmassnahmen aus als Late Follower (3.3), und auch die bezüglich Cyberrisiken eher gut bis sehr gut informierten Befragten wollen ihre Sicherheitsmassnahmen eher erhöhen (3.7) als die eher uninformierten bis sehr uninformierten (3.3). Zudem will jemand, der schon einmal von einem Angriff betroffen war, die Massnahmen eher erhöhen (3.8) als jemand, der noch nie betroffen war (3.5).

Fragen für Schweizer KMU:

- Hat sich die IT-Angriffsfläche mit der Zunahme des Homeoffice erhöht?
- Welche Cybersicherheitsmassnahmen sollten Sie in Vorbereitung auf die nächsten Monate (und in Hinblick auf neue Projekte) baldmöglichst 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?

Erhöhung der Sicherheitsmassnahmen gegen Cyberkriminalität



Erhöhung der Sicherheitsmassnahmen gegen Cyberkriminalität (n 2022=504, n 2021=506, Kategorien mit einer Stichprobengrösse <30 sind mit einem * gekennzeichnet)

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?
- ☐ Gibt es Bereiche in Ihrem Unternehmen, wo die Homeoffice-Nutzung von den Mitarbeitenden positiv kommentiert wurde?
- ☐ 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 COVID-19 gemacht – was können Sie daraus lernen und verbessern?
- ☐ Gäbe es Potenziale, in diesem Bereich das Homeoffice auch nach der Pandemie weiterhin anzubieten?
- ☐ Haben Sie für die Mitarbeitenden spezielle Anlässe (z. B. ein Willkommens-Apéro) geplant, um die Rückkehr ins Büro auch kulturell und kommunikativ zu begleiten?
- ☐ 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

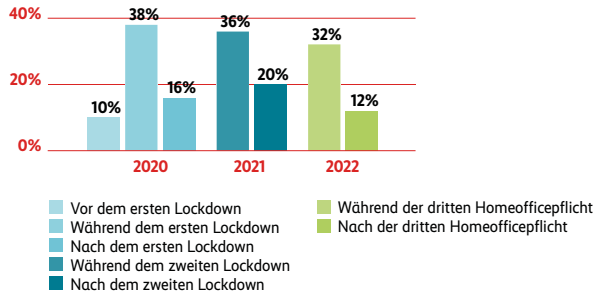
- ☐ Identifizieren Sie regelmässig die Potenziale für den Einsatz neuer Technologien und existiert eine Strategie/Roadmap für die Einführung neuer IT-Infrastruktur?
- ☐ Welche neuen Produkte und Leistungen könnten Sie durch Investitionen in die IT und Cybersicherheit erfolgreich(er) im Markt einführen?
- ☐ 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?
- ☐ Ist ihr IT-Dienstleister zertifiziert bzw. kompetent genug, um Sie zu unterstützen?

Konzepte und Massnahmen

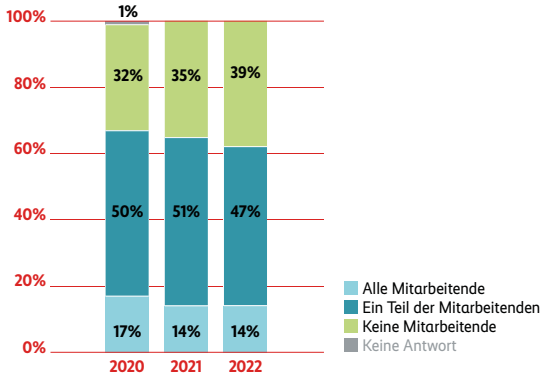
- ☐ Welche IT-Infrastruktur ist kritisch für die Leistungserbringung in Ihrem Unternehmen bzw. wie wichtig ist für Sie die Cybersicherheit?
- ☐ Welche Leistungen können Sie nicht erbringen, wenn die IT nicht läuft?
- ☐ Wie schützen Sie diese IT-Infrastruktur?
- ☐ Welche Alternativen (sogenannte Recovery-Konzepte) 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?
- ☐ Welche Alternativen (sogenannte Recovery-Konzepte) haben Sie vorbereitet?
- ☐ Würde es, bei einer grossen Abhängigkeit von der IT in Ihrer Firma, ggf. Sinn machen, in eine parallele IT-Infrastruktur (eine sog. «hot site») zu investieren?
- ☐ 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 2022»

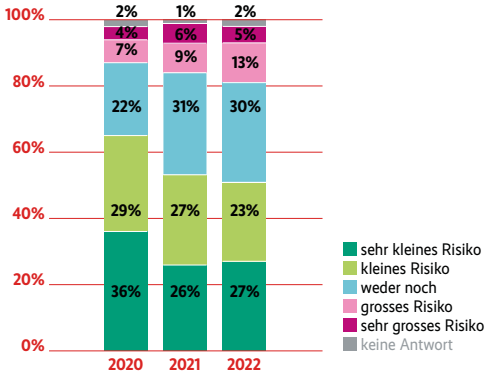
Entwicklung Homeoffice von vor der Pandemie bis heute



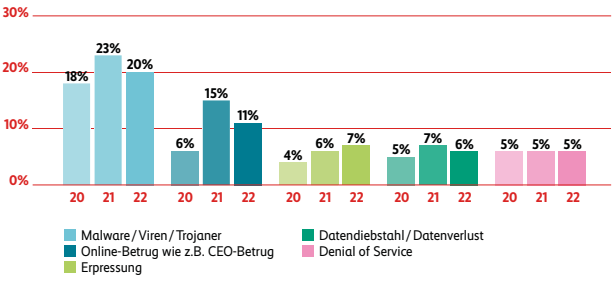
Anzahl Mitarbeitende, die potenziell im Homeoffice arbeiten können



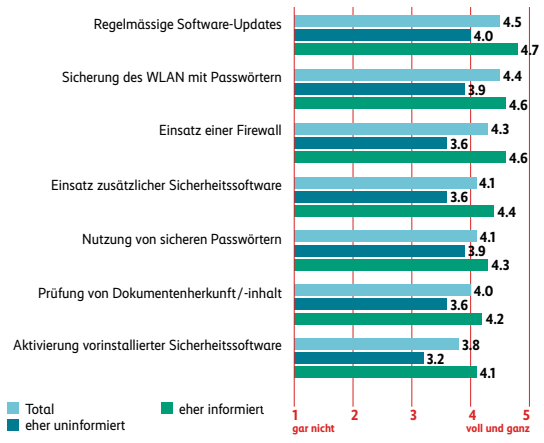
Einschätzung des Risikos, durch einen Cyberangriff einen Tag lang ausser Kraft gesetzt zu werden



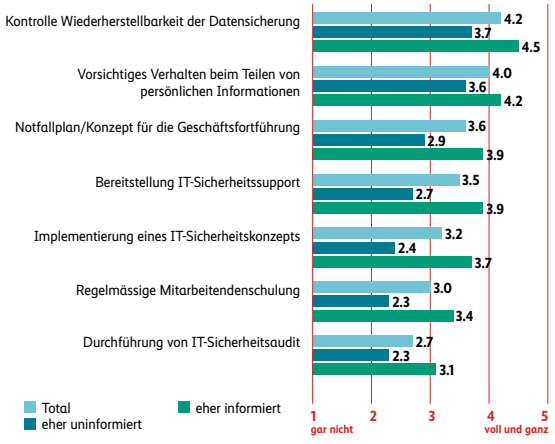
Arten von Cyberattacken



Umsetzung von technischen Massnahmen



Umsetzung von organisatorischen Massnahmen



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
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, 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 nach zwei Jahren mit COVID-19

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

www.cyberstudie.ch
Bern, Juni 2022