digitalswitzerland
MAKING SWITZERLAND
A LEADING DIGITAL
INNOVATION HUB

Online Pressekonferenz
18. November 2021
Studienergebnisse 2021

Digitalisierung und Cybersecurity in KMU

Agenda

1. **Präsentation der Studienergebnisse**
   Karin Mändli Lerch, Studienverfasserin, gfs-zürich

2. **Digital vernetzt oder verletzt? Warum sich KMU vor Cyberrisiken schützen sollten**
   Andreas Hölzli, Leiter Kompetenzzentrum Cyber Risk, die Mobiliar

3. **CyberSeal «Geprüfter IT-Dienstleister»**
   Andreas W. Kaelin, Stellvertretender Geschäftsführer und Leiter Dossier Cybersecurity, digitalswitzerland

digitalswitzerland

Präsentation der Studienergebnisse

Karin Mändli Lerch
Studienverfasserin, gfs-zürich

digitalswitzerland

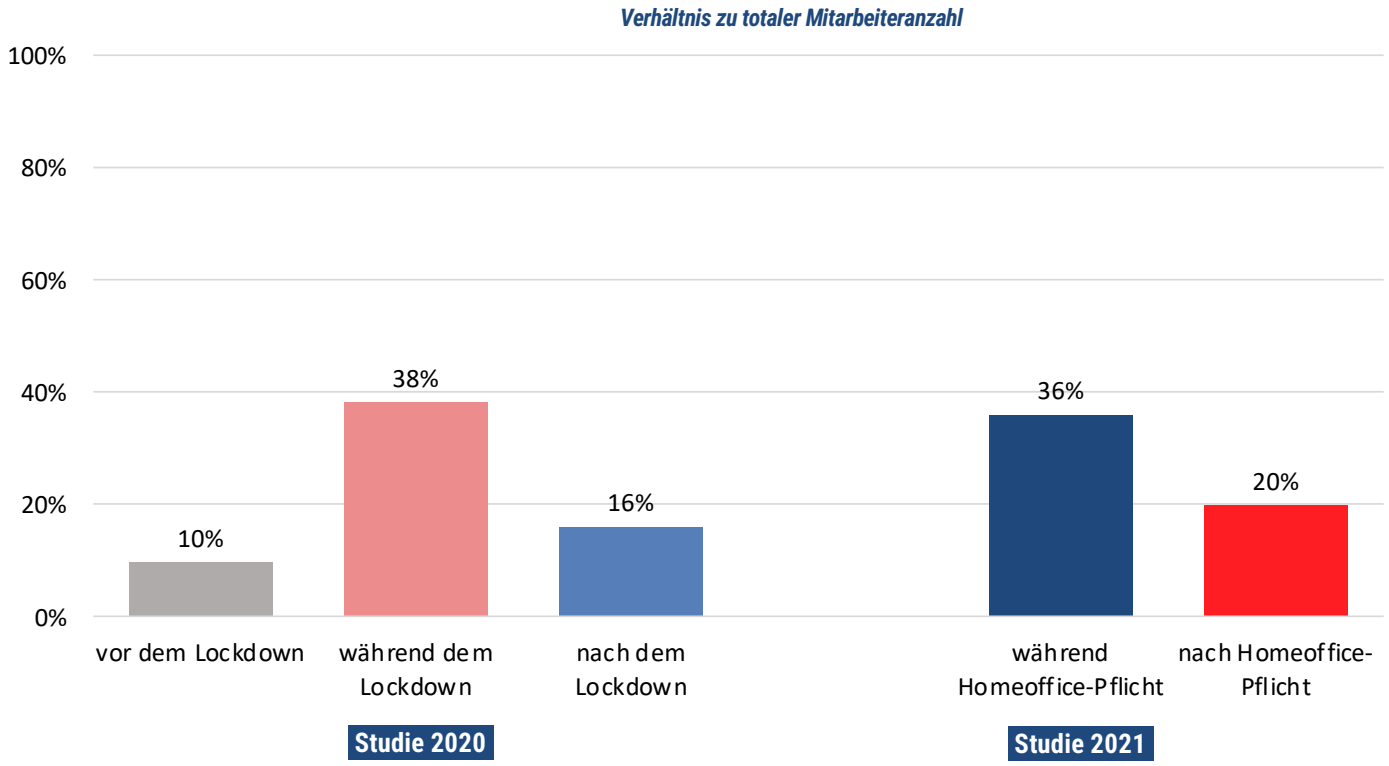
Angaben zur Stichprobe / Repräsentativität

Grundgesamtheit	KMU der deutsch-, französisch- und italienisch-sprachigen Schweiz mit 4-49 MitarbeiterInnen = rund 153’000 KMU (BFS, Statistik der Unternehmensstruktur STATENT 2017, Vers. 22.08.2019)
Stichprobe	506 GeschäftsführerInnen von Schweizer KMU
Repräsentativität	Vertrauensintervall: +/- 4.4% bei einer Sicherheit von 95%. Die Erhebung zeigt ein repräsentatives Abbild der Schweizer KMU-Landschaft, die Ergebnisse sind somit auf die Grundgesamtheit übertragbar.
Methode	CATI-Befragung
Stichprobenmethode	Random-Quota
Gewichtung	Keine
Befragungszeitraum	16. Juni bis 27. Juli 2021

Veränderung der Homeoffice-Gewohnheiten während des Corona-Lockdowns, Jahresvergleich

Wie viele ihrer Mitarbeitenden haben vor, während und nach dem Lockdown bzw. der Homeoffice-Pflicht *hauptsächlich* von zuhause aus gearbeitet?

n=329 (Filter: Wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann)

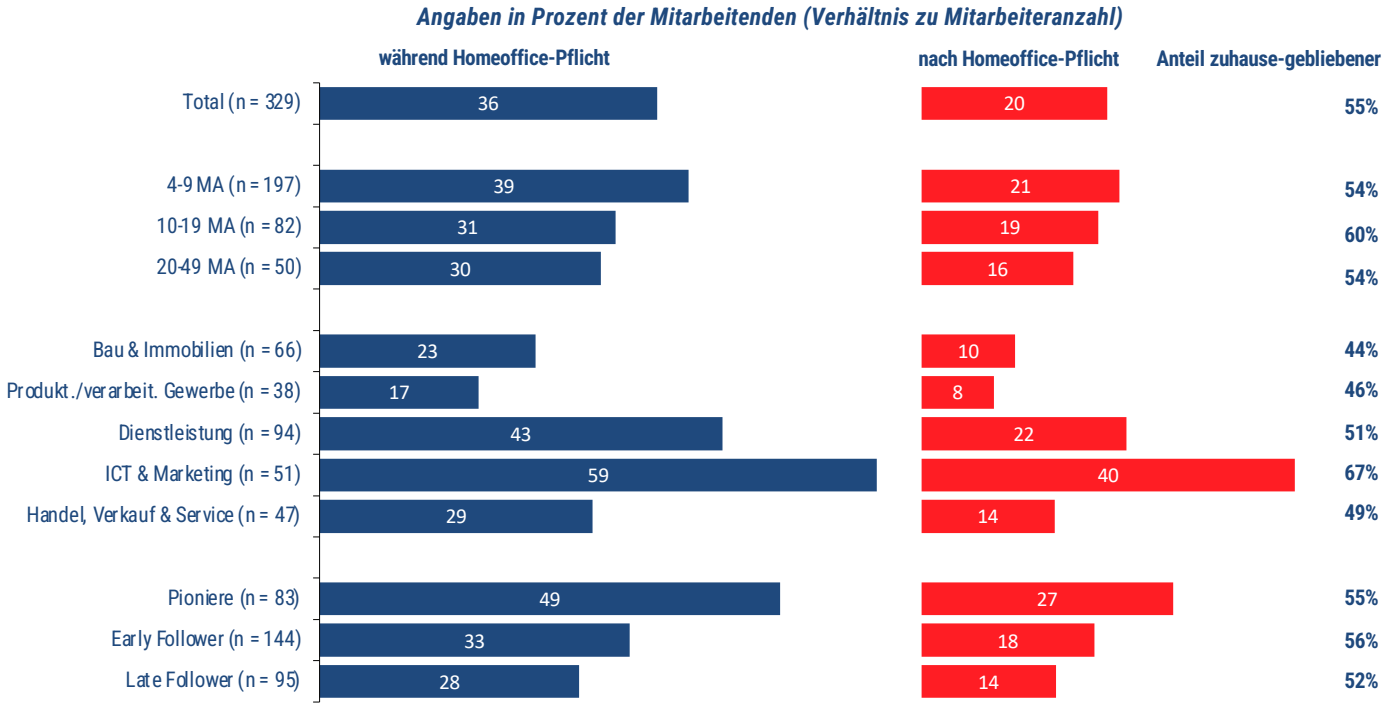


Veränderung der Homeoffice-Gewohnheiten während des Corona-Lockdowns, Subgruppenvergleich

F4a:
Wie viele Ihrer Mitarbeiter haben seit anfangs 2021 hauptsächlich von zuhause aus gearbeitet, also währenddem die Homeoffice Pflicht galt?

F4b:
Und wie viele arbeiten jetzt, nach der Homeoffice Pflicht, hauptsächlich von zuhause aus?

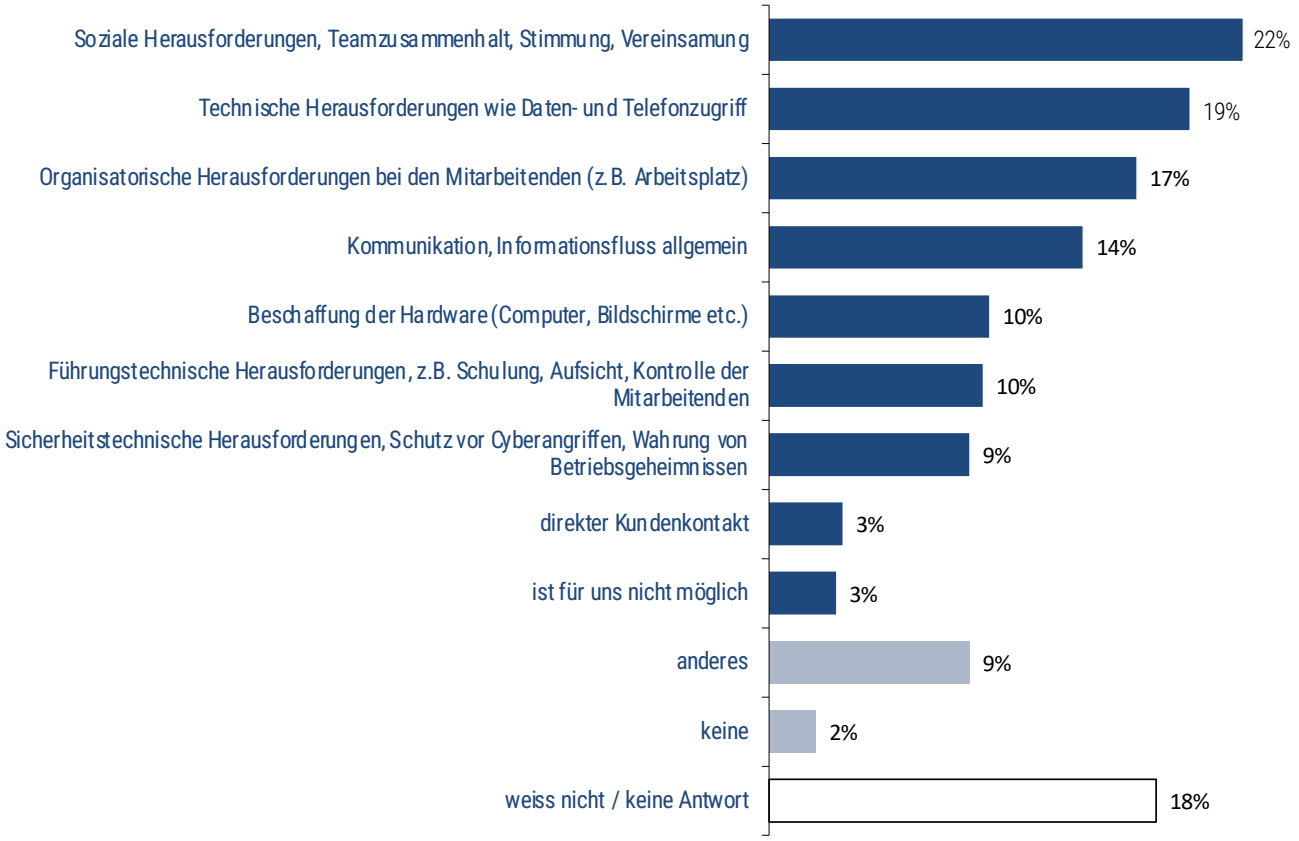
n=329 (Filter: Wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann)



Herausforderungen bei der Umsetzung des Homeoffice

F40:
Was sind aus unternehmerischer Sicht die grössten Herausforderungen bei der Umsetzung des Homeoffice?

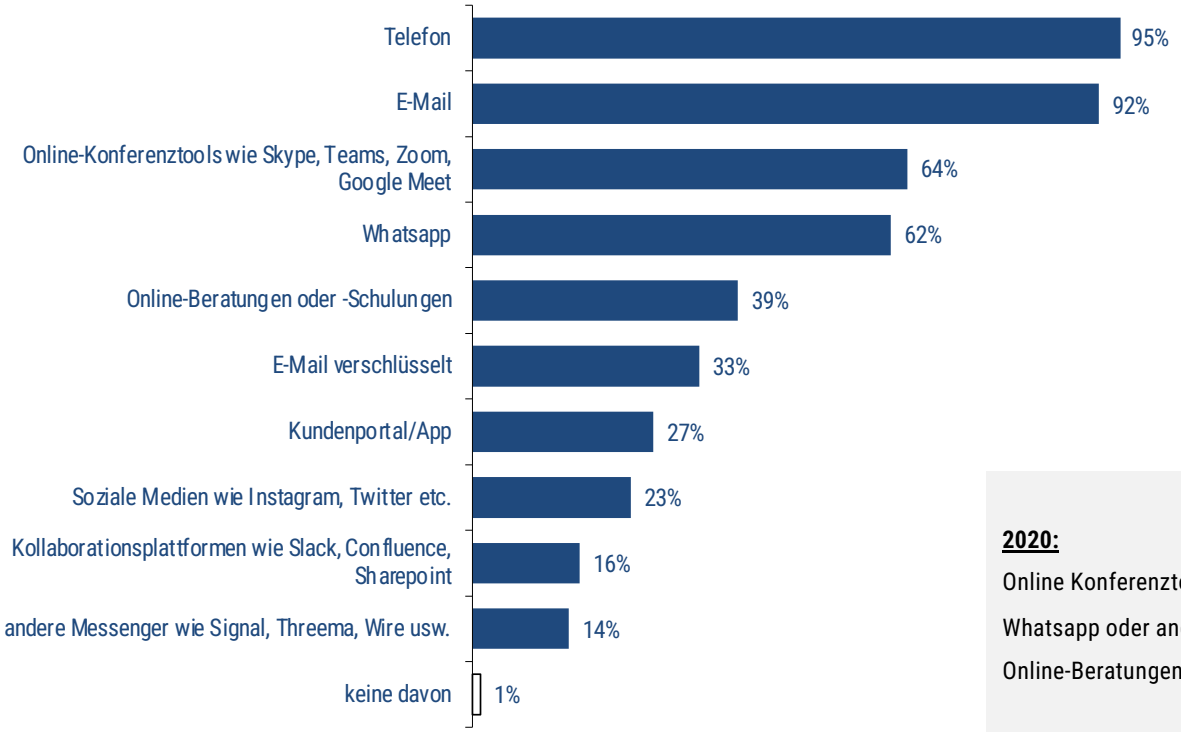
n=329, Mehrfachnennungen möglich, (Filter: Wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann)



Verwendung von Kommunikationstools

F8:
Ich lese Ihnen jetzt einige digitale Kommunikationsmittel vor. Welche davon nutzen Ihre Mitarbeitenden aktuell für Partner, Kundschaft und anderen Mitarbeitende?

n=506, Mehrfachnennungen möglich



2020:

Online Konferenztools: 46%

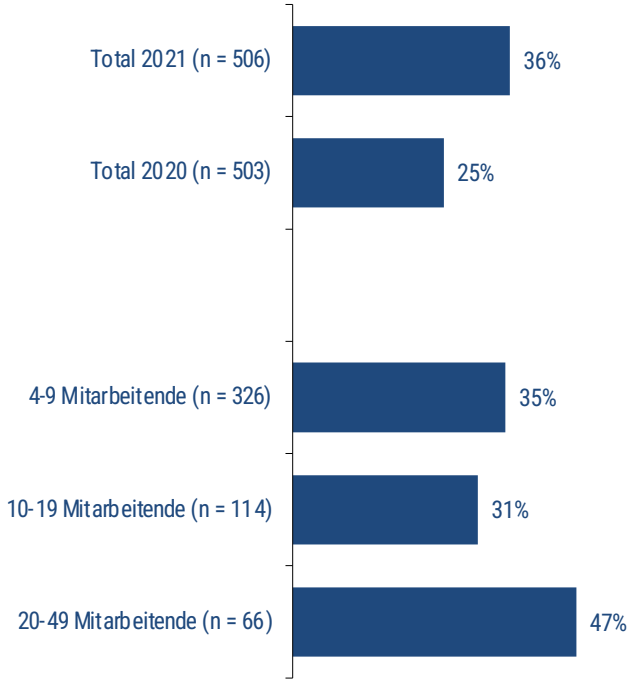
Whatsapp oder andere Messenger: 55%

Online-Beratungen oder -Schulungen: 20%

Cyberangriffe und ihre Schäden

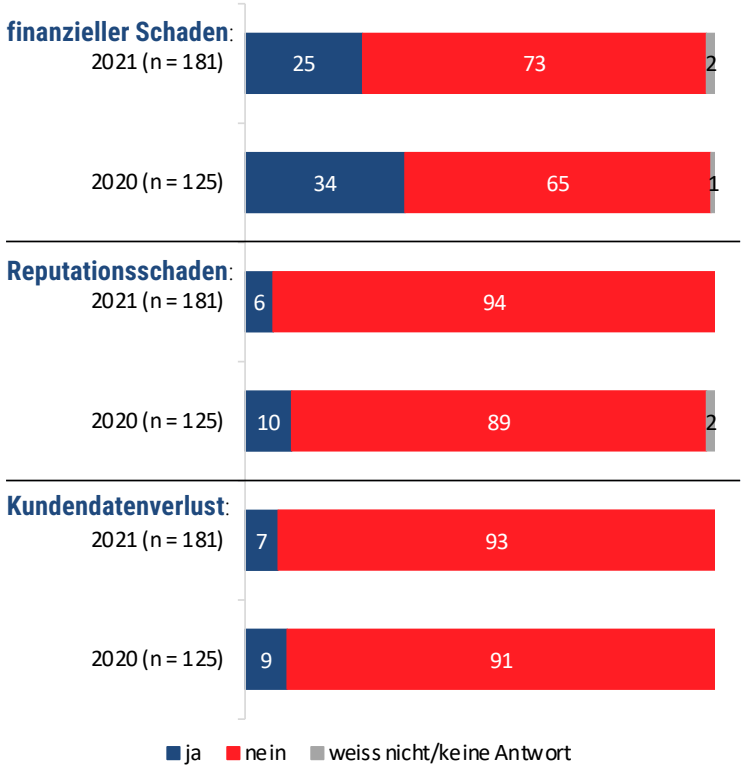
F24:
Wurde Ihre Firma schon einmal erfolgreich angegriffen, so dass ein erheblicher Aufwand nötig war, um Schäden zu beheben?

n2021 = 506, n2020 = 503, Anteil Ja-Antworten:



F25:
Entstand durch diese Angriffe ein …

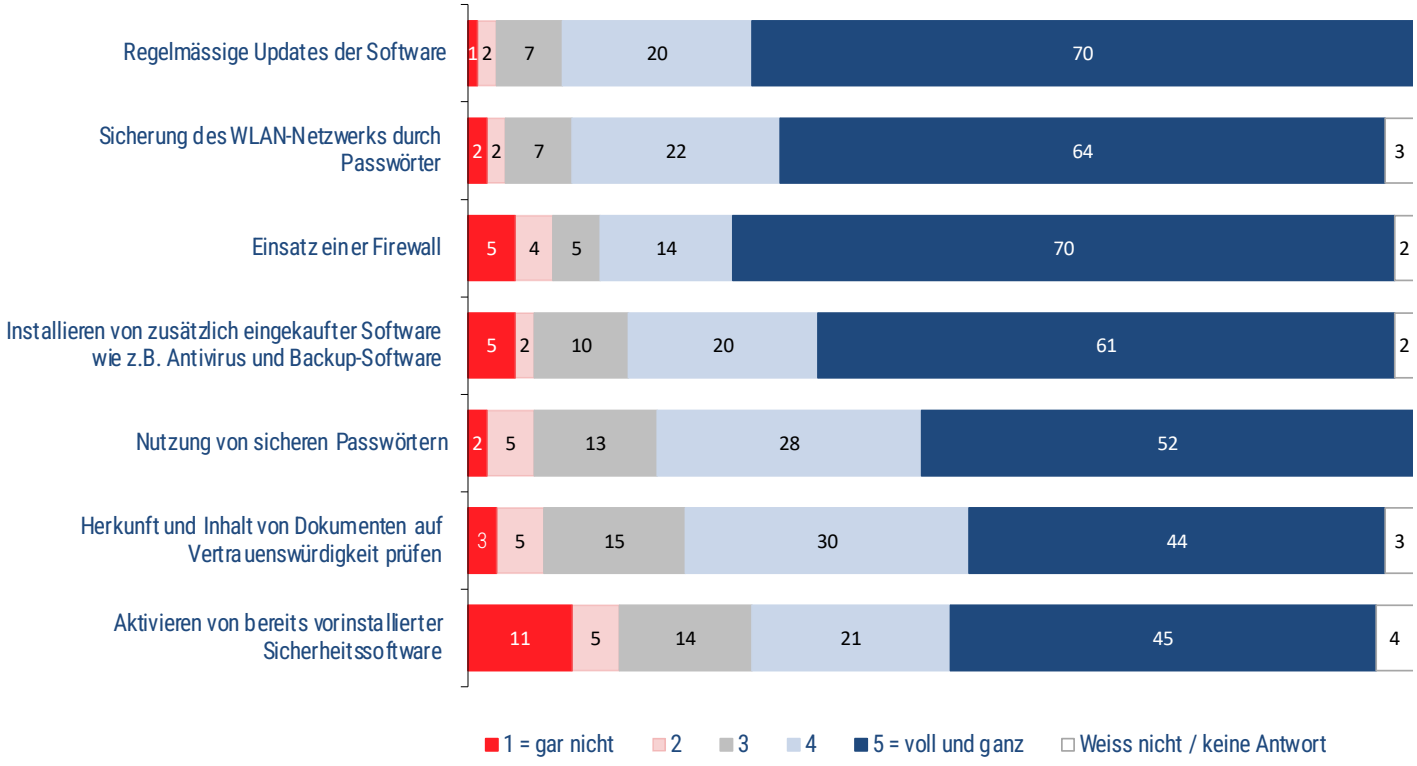
n2021 = 181, n2020 = 125 (Filter: mindestens einmal «ja» in F24)



Technische Massnahmen zur Erhöhung der Cybersicherheit

F19:
Inwieweit sind die folgenden *technischen* Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

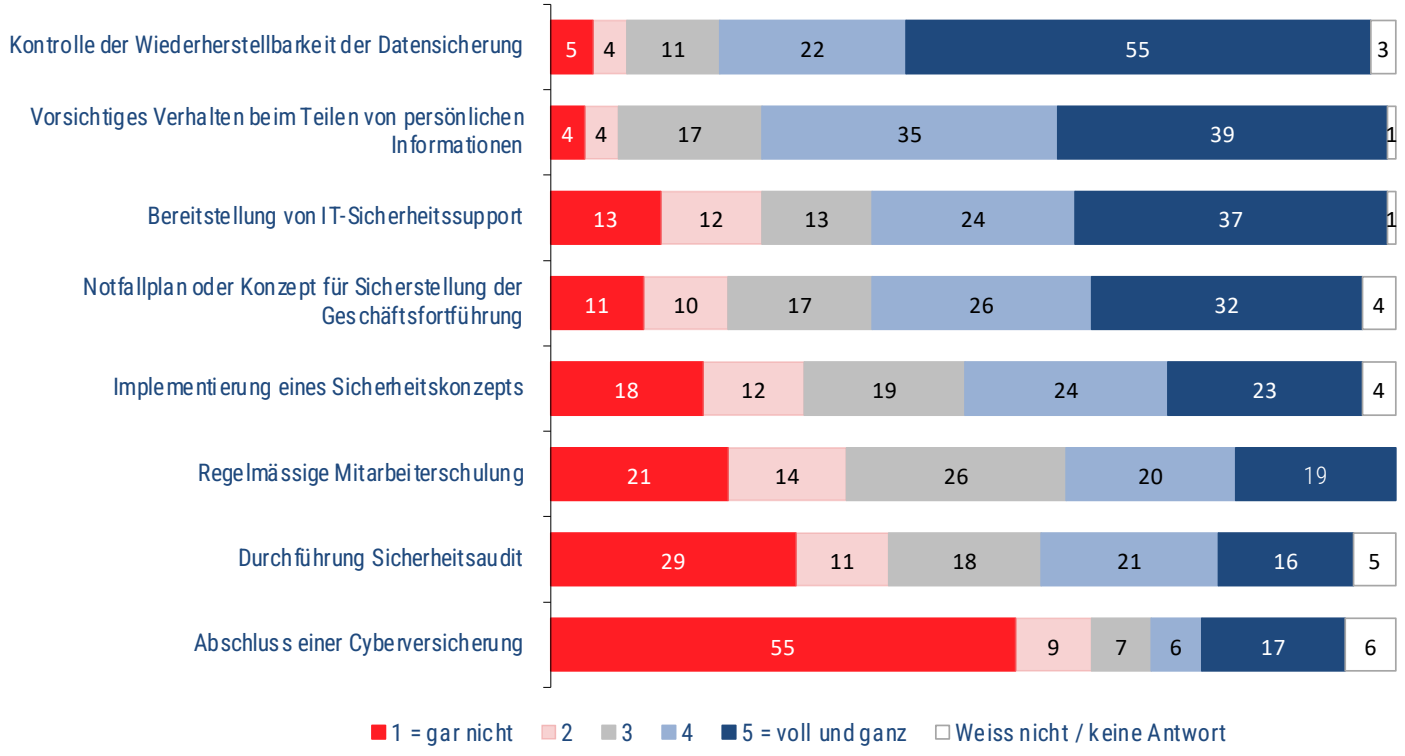
n=506,
Auf einer Skala von
1=gar nicht bis
5=voll und ganz,
Angaben in Prozent



Organisatorische Massnahmen zur Erhöhung der Cybersicherheit

F21:
Inwieweit sind die folgenden *organisatorischen* Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

n=506,
Auf einer Skala von
1=gar nicht bis
5=voll und ganz,
Angaben in Prozent



digitalswitzerland

Zusammenfassung als Whitepaper
in Deutsch, Französisch und Italienisch

Download auf
cyberstudie.ch

digitalswitzerland

- Mehr Menschen im Homeoffice
- Nutzung von neuen digitalen Kommunikationskanälen
- Mehr erfolgreiche Cyberangriffe
- Organisatorische Massnahmen noch zu wenig umgesetzt

gfs-zürich
Karin Mändli Lerch
Projektleiterin

Digital vernetzt oder verletzt? Warum sich KMU vor Cyberrisiken schützen sollten

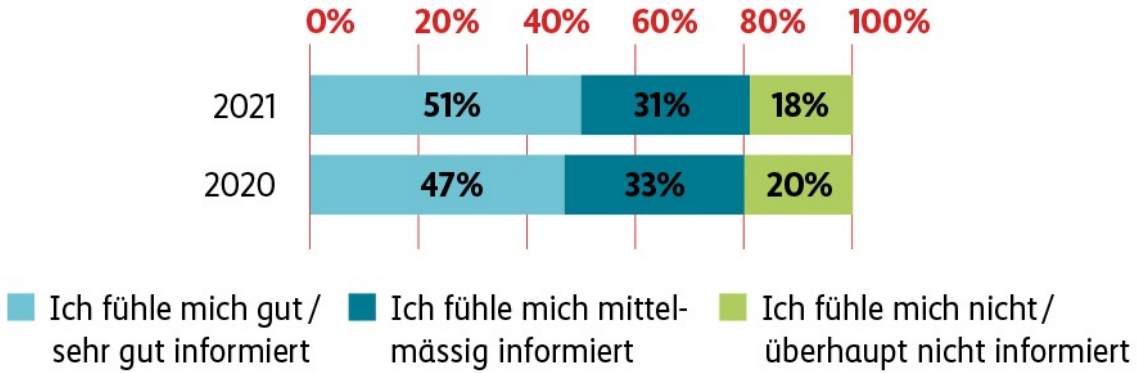
Andreas Hölzli
Leiter Kompetenzzentrum Cyber Risk, die Mobiliar

digitalswitzerland

die Mobiliar

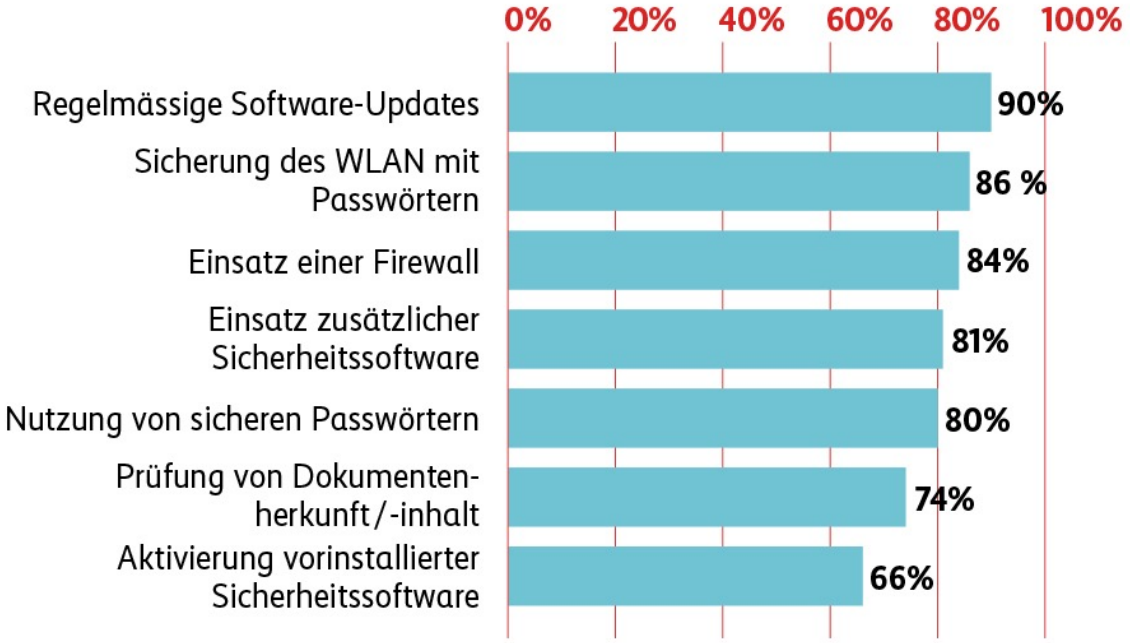
Homeoffice und Cybersicherheit in Schweizer KMU

Persönliche Informiertheit



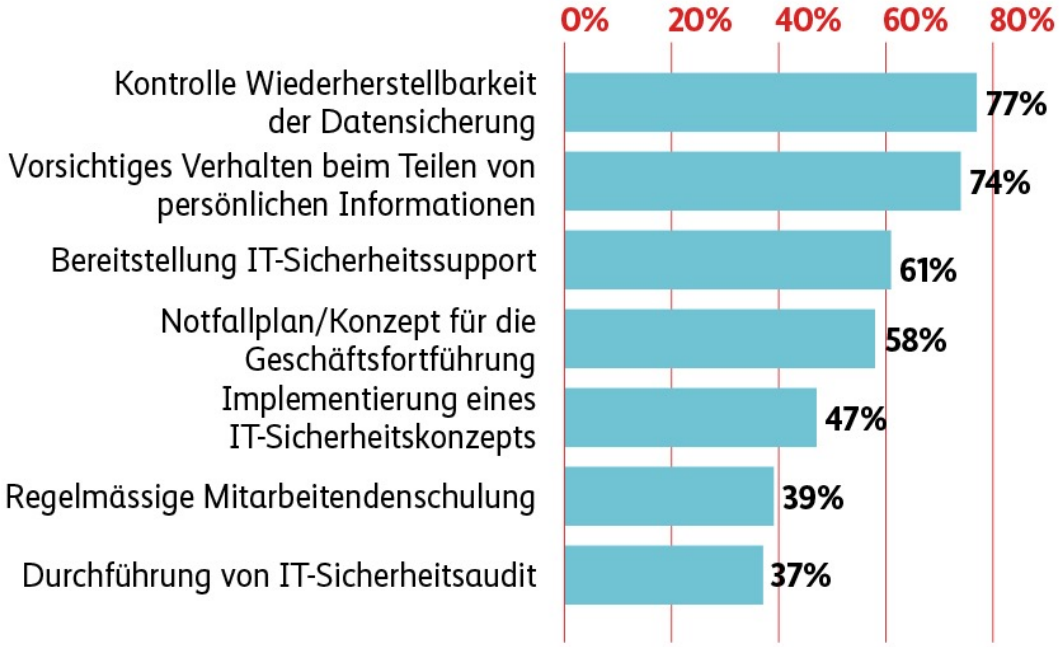
die Mobiliar

Technische Massnahmen zur Erhöhung der Cybersicherheit



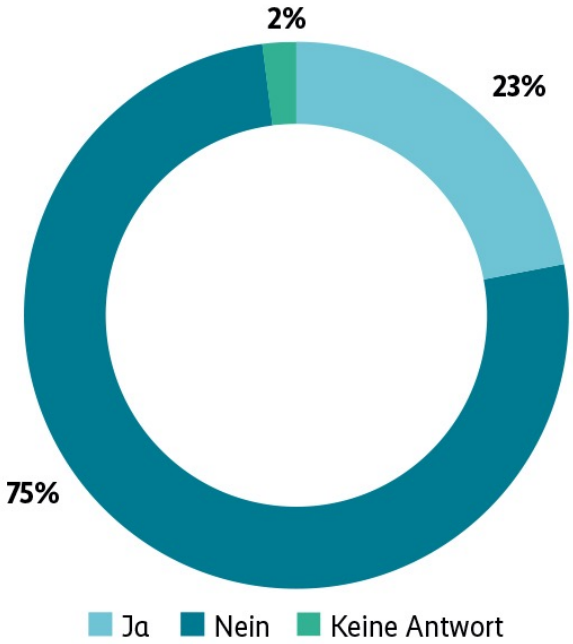
die Mobiliar

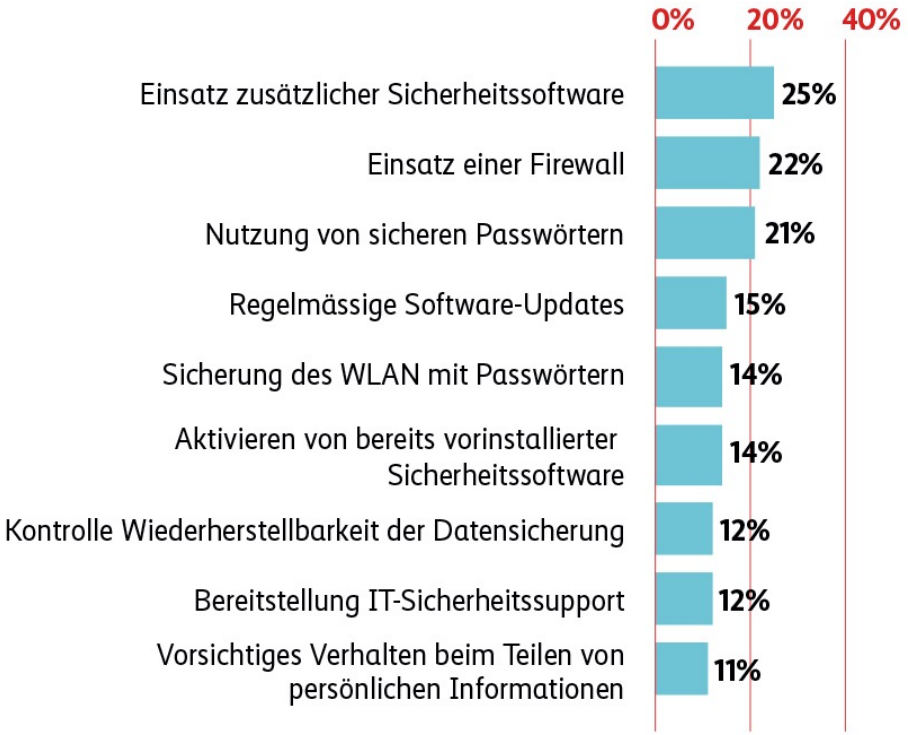
Organisatorische Massnahmen zur Erhöhung der Cybersicherheit



die Mobiliar

Cybersicherheitsmassnahmen aufgrund der Homeoffice-Pflicht





KMU, die cyberfit sind:

- halten die IT-Infrastruktur à jour
- bleiben gut informiert und sensibilisiert
- ergreifen Sicherheitsmassnahmen

die Mobiliar

Andreas Hölzli,
Leiter Kompetenzzentrum
Cyber Risk, die Mobiliar

CyberSeal «Geprüfter IT-Dienstleister»

Andreas W. Kaelin
Stellvertretender Geschäftsführer und
Leiter Dossier Cybersecurity, digitalswitzerland

digitalswitzerland

CyberSeal
mit IT-Dienstleistern zu mehr Sicherheit

ALLIANZ DIGITALE SICHERHEIT SCHWEIZ

- Gemäss letztjähriger Studie lassen sich rund zwei Drittel der kleinen Unternehmen von externen IT-Dienstleistern unterstützen.
- Wir lancieren heute das CyberSeal «geprüfter IT-Dienstleister»

digitalswitzerland

CyberSeal
mit IT-Dienstleistern zu mehr Sicherheit

ALLIANZ DIGITALE SICHERHEIT SCHWEIZ

- Ein **IT-Dienstleister** trägt eine wesentliche **Verantwortung** hinsichtlich der digitalen Sicherheit der KMU
- Der klassische „**PC-Supporter**“ hat **ausgedient**. Sie benötigen einen IT-Partner / IT-Dienstleister mit zusätzlicher **Spezialisierung** im Thema **IT-Sicherheit – Digitale Sicherheit**
- Ein guter IT-Dienstleister erkennt man heute an seiner **Zertifizierung**.
- In der Schweiz sind CyberSeal und ISO27001 geeignete **Qualitätslabel** für den IT-Dienstleister
- Die KMU sollen darauf achten, dass ihr **IT Dienstleister zertifiziert** ist. Es ist der einzige Weg zur Überprüfung, dass der IT-Dienstleister über das richtige Personal verfügt und ein sicheres Produkt und Dienstleistungsangebot für die KMU bereit hat

CyberSeal versus ISO27001

	IT-Dienstleister für KMU bis 250 Mitarbeitende	**IT-Dienstleister für grosse Unternehmen oder zusätzlich umfangreichen Anforderungen** (Betreiber kritischer Infrastrukturen, Unternehmen in stark regulierten Umfeld wie z. B. Banken)
CyberSeal	✓	
ISO27001		✓

CyberSeal USP

ALLIANZ DIGITALE SICHERHEIT SCHWEIZ

- Das CyberSeal wurde in der **Schweiz** entwickelt und berücksichtigt die **lokalen Eigenheiten**
- Die **Rückmeldungen** vom Nationalen Zentrum für Cybersicherheit des Bundes **NCSC** und der **Mobiliar** Versicherung über real eingetretene Schadensereignisse bzw. Veränderungen der Gefahrensituation werden jährlich in der **CyberSeal Prüfliste** verarbeitet
- Die Allianz Digitale Sicherheit Schweiz bietet den IT-Dienstleister **Schulung** und **Vorbereitungsworkshop** an
- CyberSeal ist auch für ein kleiner IT-Dienstleister **bezahlbar**
- CyberSeal unterstützt die IT-Dienstleister mit **Beratung**, **Tools** und **Musterchecklisten**, etc.
- Mit dem CyberSeal **Audits** wird sich die Qualität des IT-Dienstleister laufend weiterentwickeln.
- CyberSeal arbeitet **partnerschaftlich** mit den **IT-Dienstleister** zusammen – nicht nur kontrollierend
- CyberSeal ist **praxisnah** und **realitätsnaher** als andere Zertifizierungen.

ALLIANZ
DIGITALE SICHERHEIT
SCHWEIZ

CyberSeal

Allianz Digitale Sicherheit Schweiz

digitalsecurityswitzerland.ch

digitalswitzerland

Alle Dokumente:

- Studie Cybersicherheit in KMU 2021 (DE)
- Cyberseal
- Whitepaper in DE/FR/IT