digitalswitzerland

die Mobiliar

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

gfs. gfs-zürich

n|w Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

satw it's all about technology

Studienergebnisse: Digitalisierung, Home-Office und Cybersicherheit in Schweizer KMU

Dienstag, 8. Dezember 2020, 9:15-10:15 Uhr
Videokonferenz mit Aufzeichnung

Teilnehmende Personen

Medienkonferenz

Projektleiterin der Studie

Karin Mändli Lerch
gfs-zürich, Markt- und Sozialforschung

Vertreter und Vertreterinnen der Auftraggeber

Florian Schütz
Delegierter des Bunds für Cybersicherheit

Andreas Hölzli
Leiter Kompetenzzentrum Cyber Risk, Die Mobiliar

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

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

Patric Vifian
Marketing Manager KMU
Die Mobiliar

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
SATW

digitalswitzerland die Mobiliar Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Eidgenössisches Finanzdepartement EFD Nationales Zentrum für Cybersicherheit NCSC n|w Fachhochschule Nordwestschweiz Hochschule für Wirtschaft satw it's all about technology gfs. gfs-zürich

Agenda

Medienkonferenz

09:15-09:20	Begrüssung • Andreas W. Kaelin, digitalswitzerland
09:20-10:00	Präsentation der Studienergebnisse • Die Studienergebnisse im Überblick (15') Karin Mändli Lerch, Studienverfasserin, gfs-zürich • Was trägt der Bund zur Cyberresilienz von KMU bei? (10') Florian Schütz, Delegierter des Bundes für Cybersicherheit • Gut informiert – richtig aufgestellt. So schützen sich KMU vor Cyber-Gefahren (15') Andreas Hölzli, Leiter Kompetenzzentrum Cyber Risk, die Mobiliar
10:00-10:15	Q&A

Präsentation der Studienergebnisse I

Die Studienergebnisse im Überblick

Karin Mändli Lerch, Studienverfasserin, gfs-zürich

Studienergebnisse im Überblick

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: 503 GeschäftsführerInnen von Schweizer KMU

Repräsentativität:
- repräsentatives Abbild der Schweizer KMU-Landschaft
- Ergebnisse auf die Grundgesamtheit extrapolierbar
- Vertrauensintervall Gesamtstichprobe: +/- 4.5% bei einer Sicherheit von 95% (50/50 Verteilung)

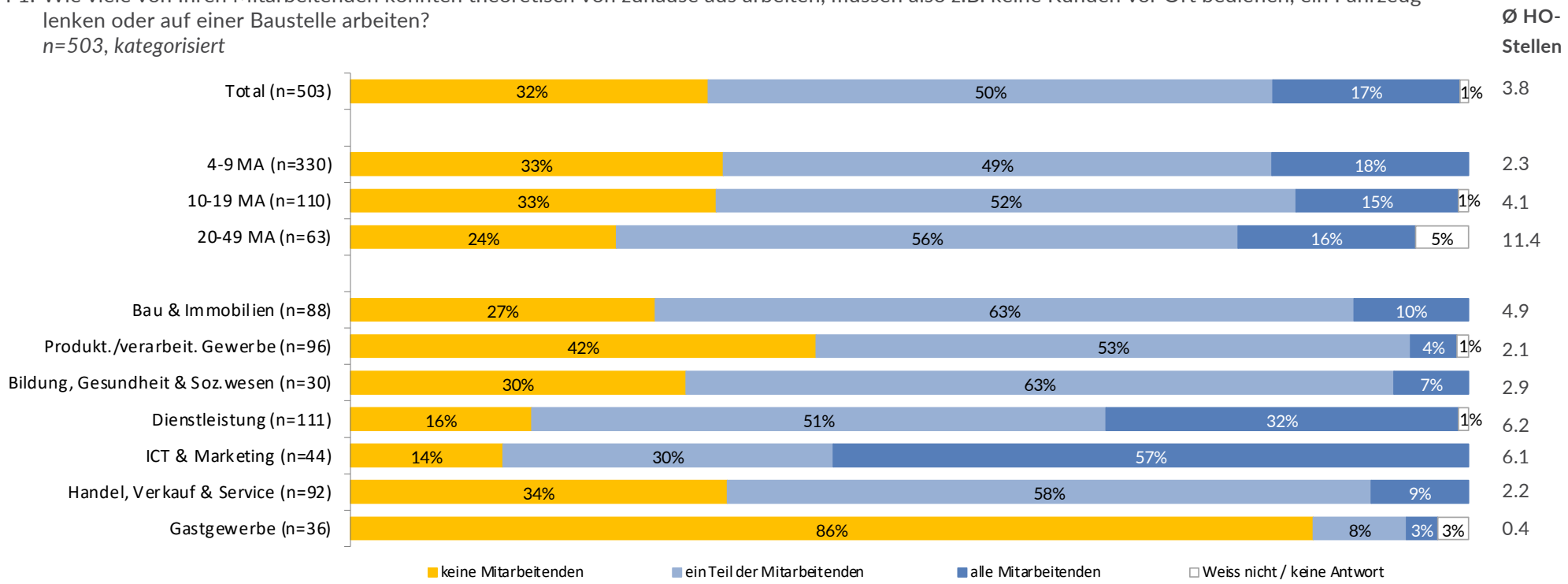
Methode: CATI-Befragung

Befragungszeitraum: 19. August bis 7. Oktober 2020

Studienergebnisse im Überblick

Anzahl Mitarbeitende, die potentiell vom Home Office aus arbeiten könnten

F1: Wie viele von Ihren Mitarbeitenden könnten theoretisch von zuhause aus arbeiten, müssen also z.B. keine Kunden vor Ort bedienen, ein Fahrzeug lenken oder auf einer Baustelle arbeiten?
n=503, kategorisiert

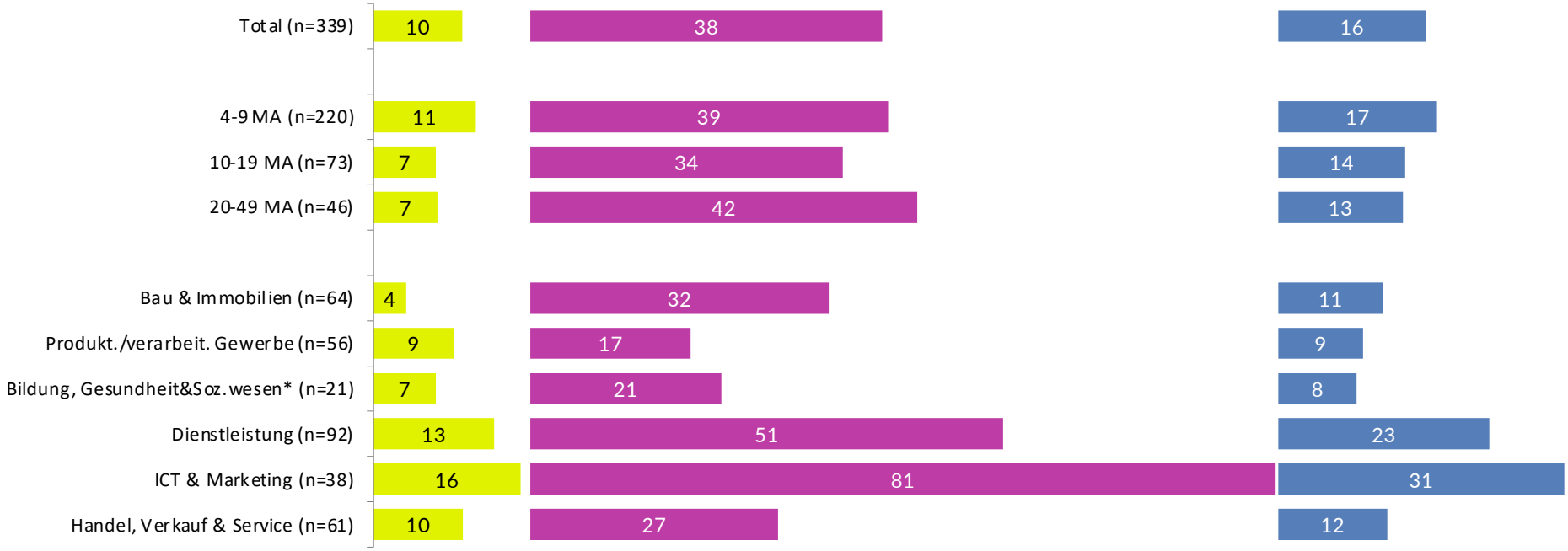


Studienergebnisse im Überblick

Veränderung der Home Office-Gewohnheiten während des Corona-Lockdowns

F4: Wie viele ihrer Mitarbeitenden haben vor, während und nach dem Lockdown **hauptsächlich** von zuhause aus gearbeitet?
n=339 (Filter: Wenn mindestens ein/e Mitarbeiter/in theoretisch im Home Office arbeiten kann)

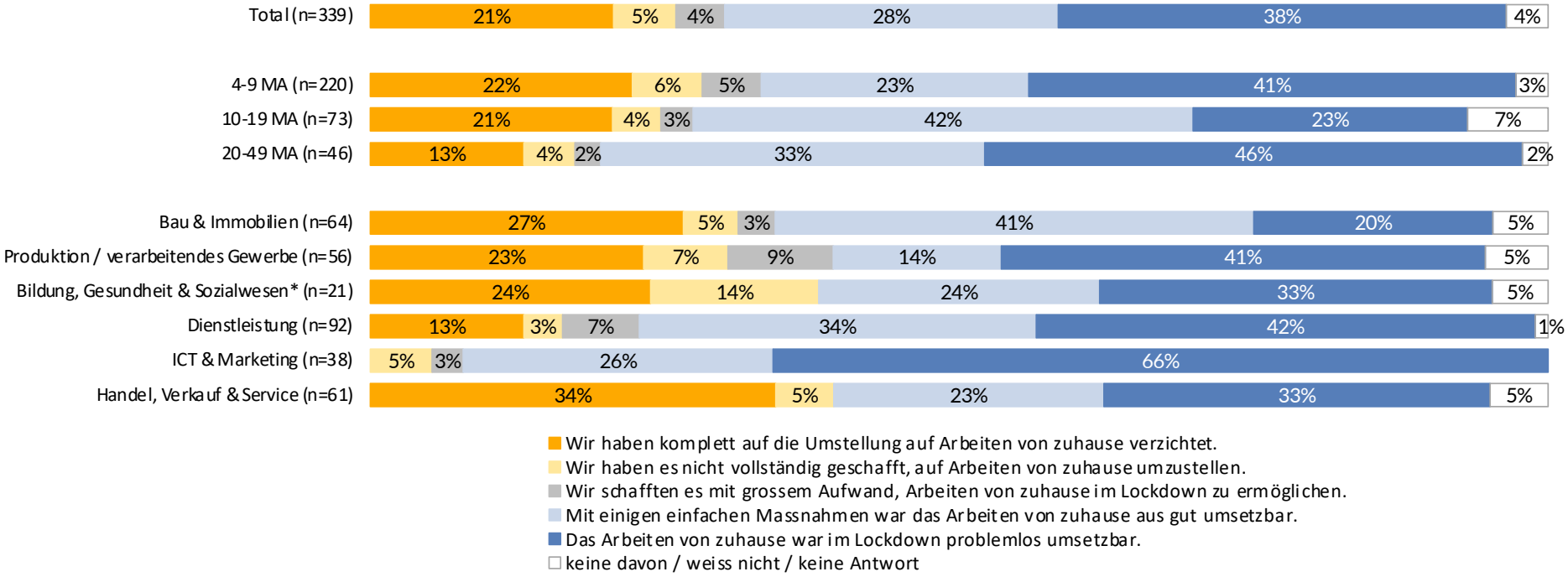
Angaben in Prozent – Verhältnis zu totaler Mitarbeiteranzahl



Studienergebnisse im Überblick

Reaktionsfähigkeit auf das plötzliche Home Office aufgrund des Lockdowns

F7: Wie gut hat Ihre Firma auf das plötzliche Arbeiten von zuhause aufgrund des Lockdowns reagieren können?
n=339 (Filter: Wenn mindestens ein/e Mitarbeiter/in theoretisch im Home Office arbeiten kann)

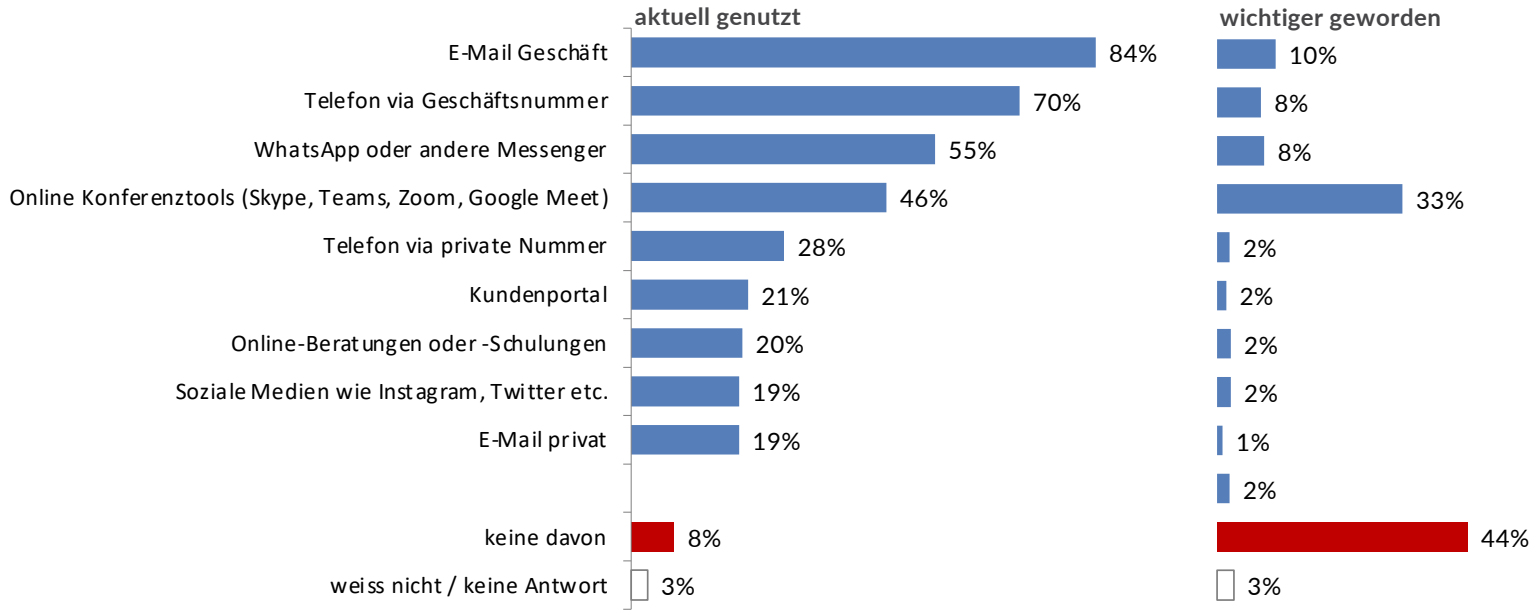


Studienergebnisse im Überblick

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=503, Mehrfachnennungen möglich

F9: Gibt es Kommunikationsmittel, die durch den Lockdown wichtiger geworden sind bzw. häufiger genutzt werden?
n=503, Mehrfachnennungen möglich, offene/vorcodierte Frage

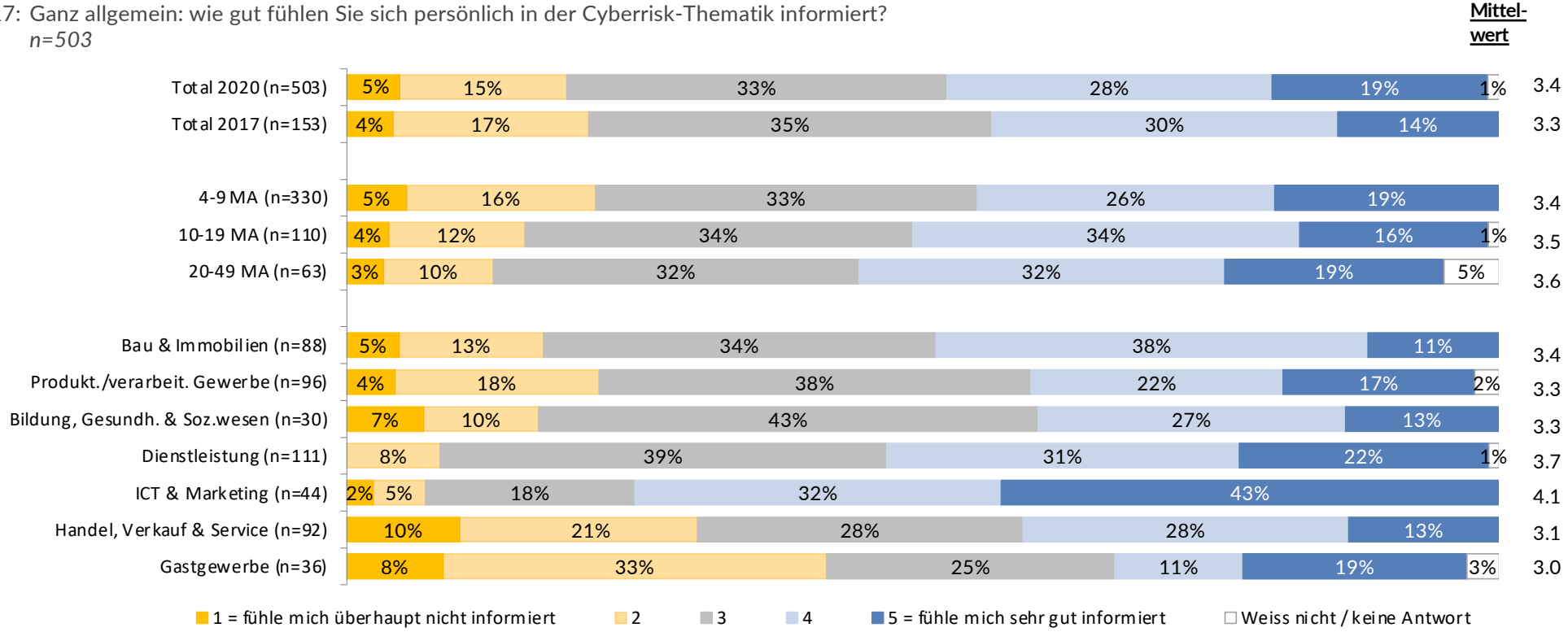


Anteil virtueller Sitzungen
Vor dem Lockdown: 9%
Nach dem Lockdown: 20%

Studienergebnisse im Überblick

Persönlicher Informationsgrad Cyberrisk-Thematik

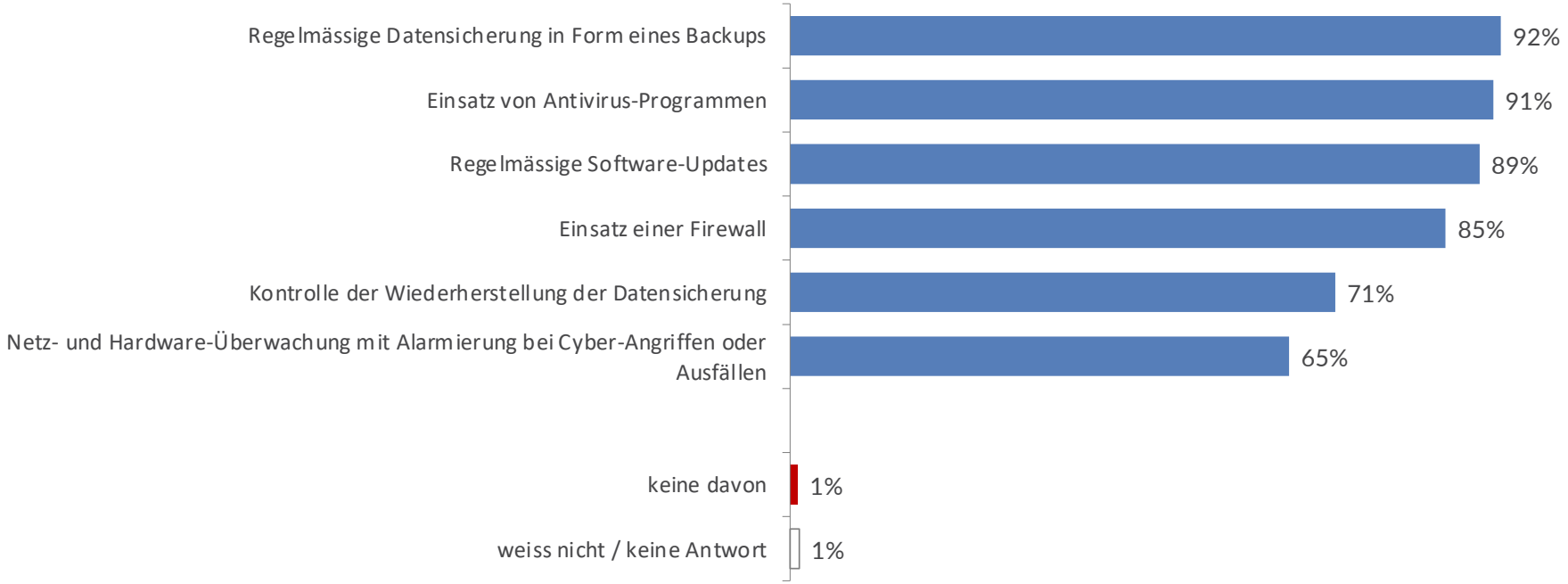
F17: Ganz allgemein: wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert?
n=503



Studienergebnisse im Überblick

Technische Massnahmen zur Erhöhung der Cyber-Sicherheit

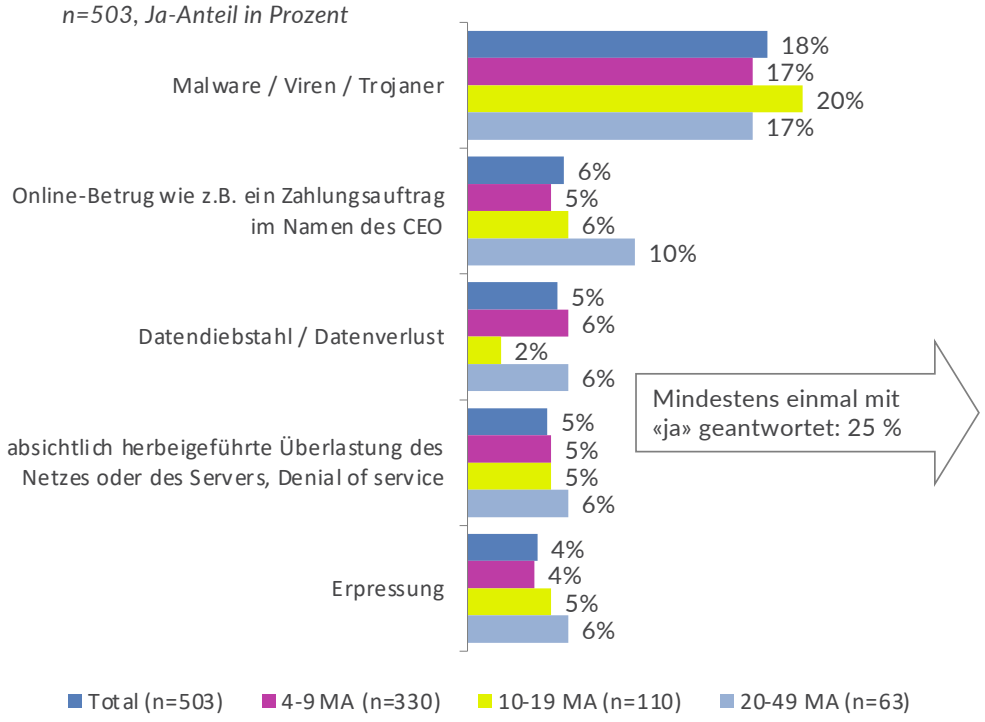
F19: Ich lese Ihnen jetzt einige **technische** Massnahmen zur Erhöhung der Cyber-Sicherheit vor. Welche davon werden in Ihrer Firma eingesetzt?
n=503, mehrere Antworten möglich, Ja-Anteil in Prozent



Studienergebnisse im Überblick

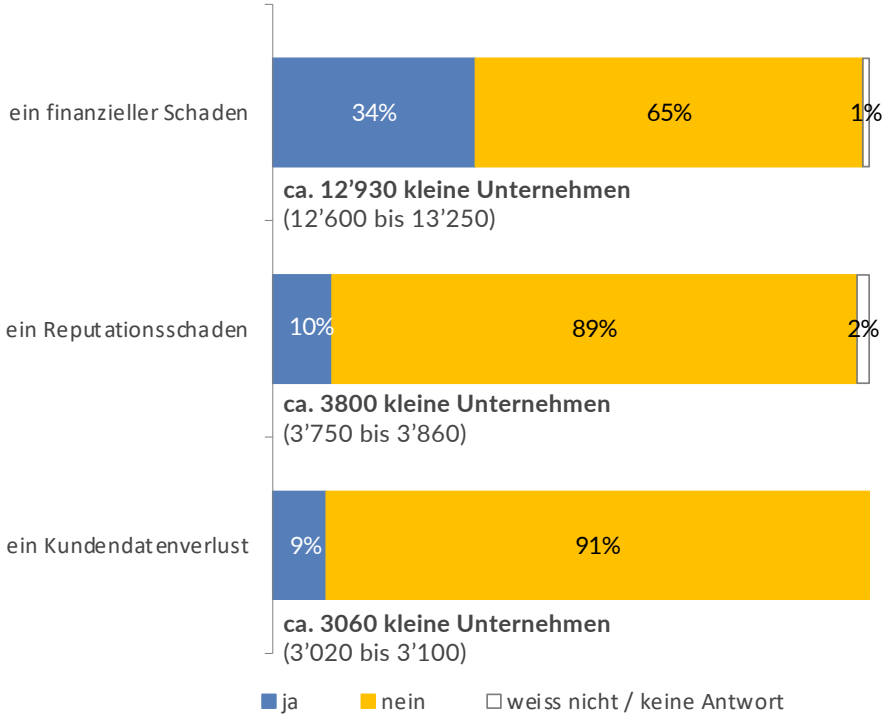
Erfolgreiche Cyber-Angriffe

F24: Wurde Ihre Firma schon einmal erfolgreich durch eine der folgenden Techniken angegriffen, so dass ein erheblicher Aufwand nötig war, um Schäden zu beheben?
n=503, Ja-Anteil in Prozent



Mindestens einmal mit «ja» geantwortet: 25 %

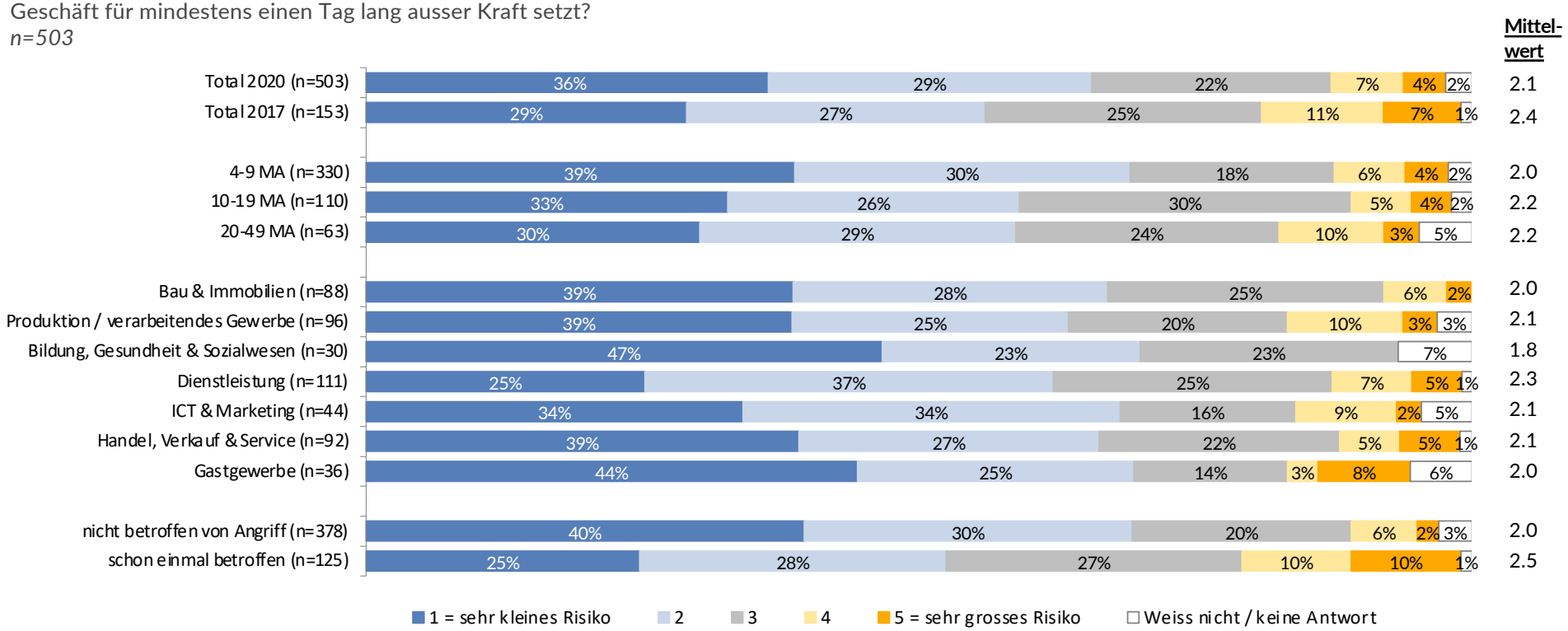
F25: Entstand durch diesen Angriff / Entstanden durch diese Angriffe …
n=125 (Filter: mindestens einmal «ja» in F24)



Studienergebnisse im Überblick

Risikoeinschätzung Cyberangriff

F26: Als wie hoch schätzen Sie das Risiko ein, dass Ihre KMU innerhalb der nächsten 2-3 Jahre von einem Cyberangriff betroffen sein wird, der Ihr Geschäft für mindestens einen Tag lang ausser Kraft setzt?
n=503



Präsentation der Studienergebnisse II

Was trägt der Bund zur Cyberresilienz von KMU bei?

Florian Schütz, Delegierter des Bundes für Cybersicherheit

Präsentation der Studienergebnisse III

Gut informiert – richtig aufgestellt. So schützen sich KMU vor Cyber-Gefahren

Andreas Hölzli, Leiter Kompetenzzentrum Cyber Risk
die Mobiliar

die Mobiliar

Gut informiert – richtig aufgestellt. So schützen sich KMU vor Cyber-Gefahren.

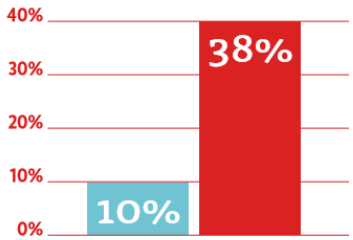
8. Dezember 2020 / Andreas Hölzli

Während des Lockdowns schöpfen Schweizer KMU das Potenzial von Homeoffice aus – der Trend hält an

Vor Lockdown

2/3 der Schweizer KMU haben die Möglichkeit für Homeoffice

Während Lockdown



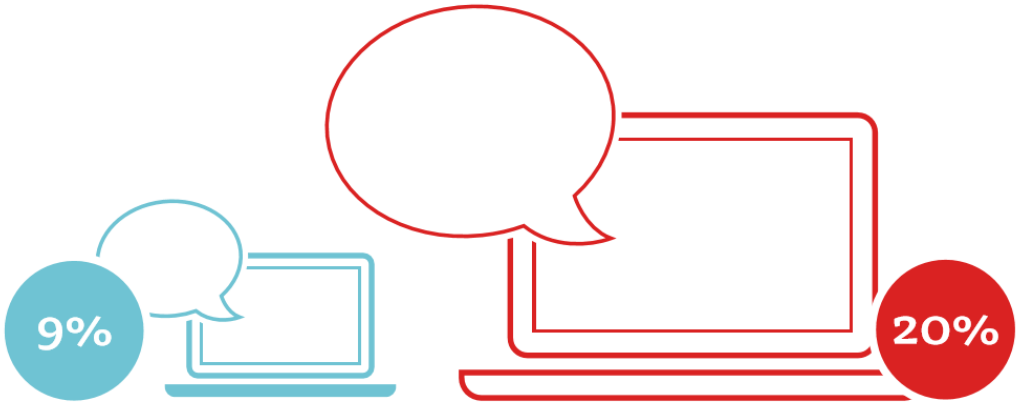
18

4x mehr Mitarbeitende im Homeoffice

Nach Lockdown

60% Steigerung an Homeoffice-Stellen nach dem Lockdown

Online-Konferenztools auf dem Vormarsch



Die Zahl von virtuellen Sitzungen hat sich seit dem Lockdown verdoppelt

Cyberkriminalität in Bezug auf COVID-19 in den Nachrichten

Neue Betrugsmaschen

Cyberkriminelle machen sich Corona-Krise zunutze

Cyber-Kriminelle profitieren von Corona

In nur einem Monat schnellte die Zahl von entdeckten Cyber-Angriffen um 30 Prozent in die Höhe. Das kriminelle Geschäft im Netz rund um Corona reicht von Nepp bis zu Lösegeldforderungen.

Corona-Soforthilfe

Betrüger verschicken gefälschte Mails

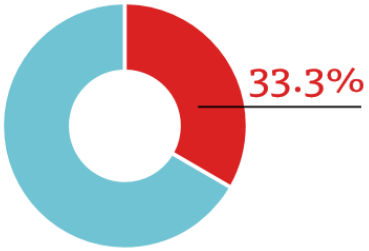
Der perfekte Köder: Cyberkriminelle nutzen die Corona-Panik

Die Coronavirus-Krise ist für die Angreifer besonders geeignet. Experten rechnen mit einem starken Anstieg der kriminellen Aktivitäten.

Erhöhte Gefahr von Cyber-Attacken in der Corona-Krise

Ein Viertel der Schweizer KMU war schon Opfer eines folgenschweren Cyberangriffs

1/4 der Schweizer KMU war schon Opfer eines Cyberangriffs



1/3 der angegriffenen KMU trugen einen finanziellen Schaden davon

Versicherer hilft den KMU, ihr Risiko aktiv zu managen

Risiko / Gefahr verstehen

Vermeiden

Vermindern

Überwälzen

Präventive Massnahmen

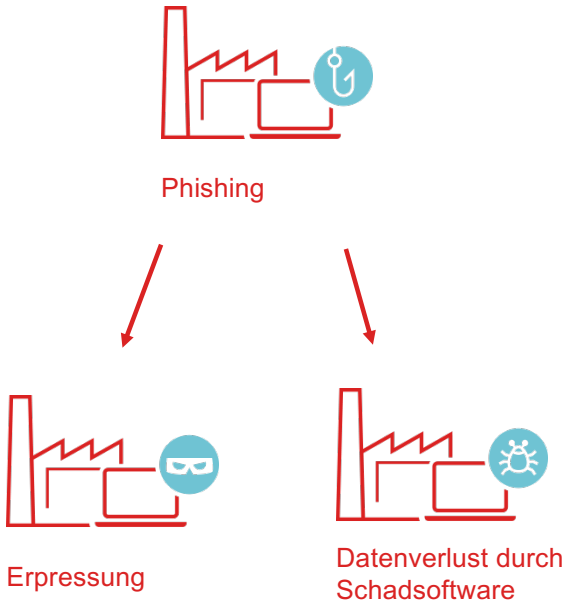
Versicherung

Häufigste Cyber Schadenereignisse bei KMU

Social Engineering verknüpft mit Ransomware

Offene Ports verknüpft mit Ransomware

Betrug mit manipulierten Rechnungen



Ein Cyberereignis kostet ein KMU Zeit und Nerven ...

- **Säuberung IT-Systeme bis hin zur Neuinstallation von Applikationen**
- **Datenrettung und meistens -wiederherstellung**
- **oft aufwändiges Einspielen des Backups der verlorenen Daten**
- **oft fehlende oder mangelhafte Notfallorganisation**

… und kommt ein KMU oft auch teuer zu stehen.

- **finanzielle Verluste durch Betriebsunterbruch**
- **Wiederherstellungskosten der Infrastruktur**
- **Vermögensschäden infolge eBanking Betrug**
- **Reputationsschaden infolge mangelhaftem Krisenmanagements**

Präventive Massnahmen werden zu selten ergriffen

Nur die Hälfte der KMU hat einen Notfallplan für die Sicherstellung der Geschäftsfortführung

2/3 führen weder regelmässige Mitarbeiterschulungen durch noch haben sie ein Sicherheitskonzept

Der Mensch als Risikofaktor – Cyberrisiken werden häufig unterschätzt

47% der CEO geben an, über sicherheits-relevante Themen gut informiert zu sein

Nur gerade 11% schätzen das Risiko gross ein, durch einen Cyberangriff einen Tag ausser Gefecht gesetzt zu werden

Praxistipps mit hoher, präventiver Wirkung

Sensibilisierungs-training

Technische und prozessuale Schutzmechanismen

Funktionierendes Backup

Notfallplanung und Krisenmanagement

Sicherstellung der Geschäftsfortführung im Cyber Ereignis

die Mobiliar

Vielen Dank für Ihre Aufmerksamkeit

HERZLICHEN DANK!

digitalswitzerland

die Mobiliar

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

n|w Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

satw it's all about technology

gfs. gfs-zürich