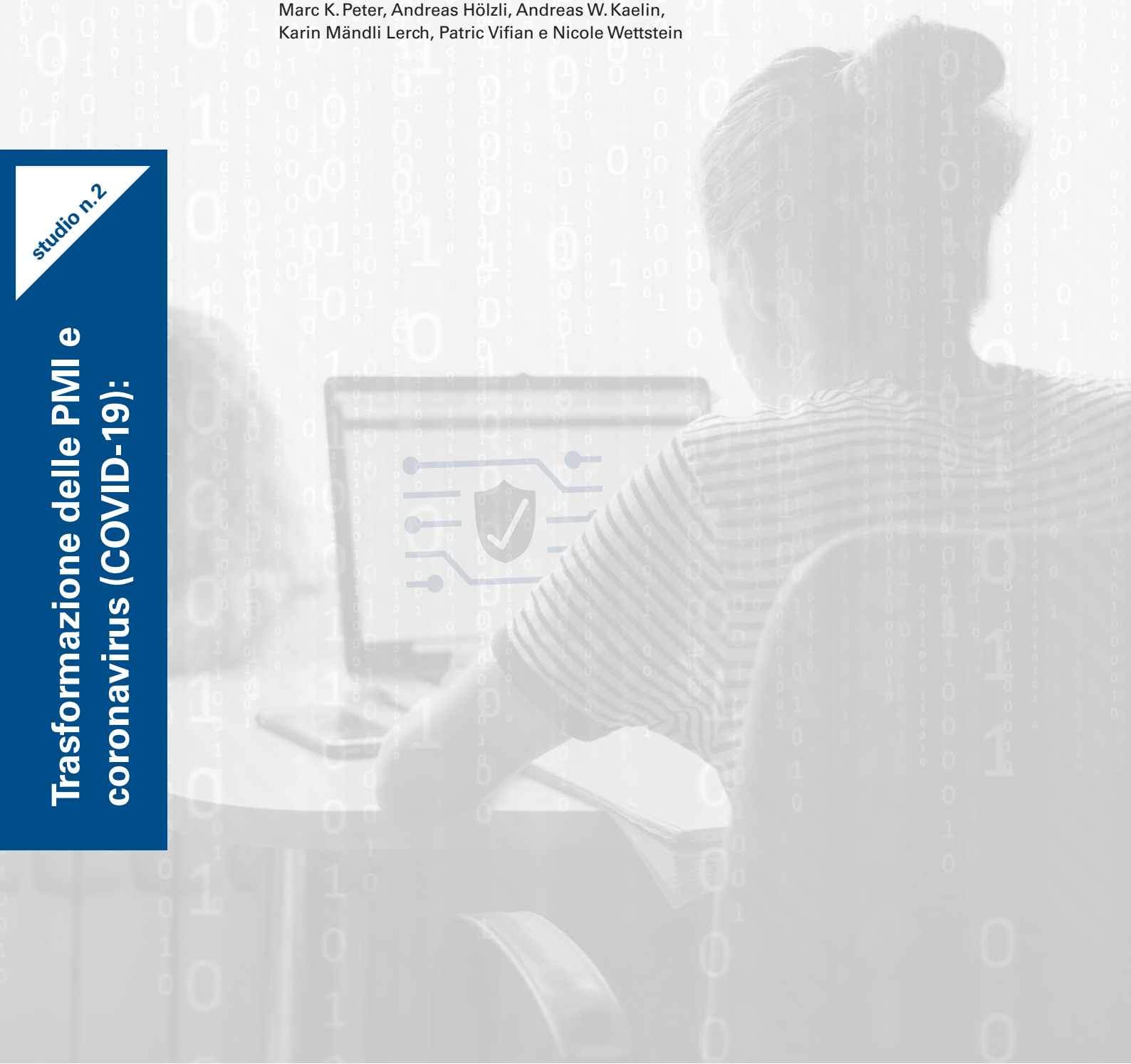
studio n.2

Trasformazione delle PMI e coronavirus (COVID-19):

Home office e cyber sicurezza nelle PMI svizzere

Strategie e misure adottate dalle PMI svizzere con 4–49 collaboratori nel contesto del coronavirus (COVID-19)

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



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

Colophon

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

Home office e cyber sicurezza nelle PMI svizzere: strategie e misure adottate dalle PMI svizzere con 4–49 collaboratori nel contesto del coronavirus (COVID-19)

la Mobiliare, digitalswitzerland, FHNW Hochschule für Wirtschaft, SATW, gfs-zürich

Berna, novembre 2021

Coordinamento della pubblicazione: Prof. Dr. Marc K. Peter, FHNW Hochschule für Wirtschaft (www.fhnw.ch/business)

Layout: Polarstern SA, Soletta e Lucerna (www.polarstern.ch)
Traduzione in francese/italiano: la Mobiliare

La serie di lucidi e il rapporto finale dettagliato sono disponibili sui siti web dei partner dello studio.

Metodologia di ricerca

Popolazione statistica: PMI della Svizzera di lingua tedesca, francese e italiana con 4–49 collaboratori (= circa 153 000 PMI secondo l'UST, Statistica strutturale delle imprese STATENT 2017, vers. 22.8.2019).

Campionamento: 506 dirigenti di PMI svizzere. Rappresentatività: l'intervallo di confidenza del campione totale si colloca al +/- 4,4 % con un livello di fiducia del 95 % (distribuzione 50/50). La rilevazione fornisce un quadro rappresentativo del mondo delle PMI svizzere; i risultati sono pertanto trasferibili alla popolazione statistica. Metodo: sondaggio CATI.

Metodo: sondaggio CATI.

Metodo di campionamento: campionamento per quote (estrazione casuale delle PMI, prestratificate per regione, quindi selezione delle quote in base alle dimensioni dell'azienda).

Ponderazione: nessuna.

Periodo in cui si è svolta l'indagine: dal 16 giugno al 27 luglio 2021.

Sommario

Introduzione e panoramica

Il gruppo di progetto, composto da collaboratori di digitalswitzerland, della Hochschule für Wirtschaft della Scuola universitaria professionale della Svizzera nordoccidentale (FHNW), della Schweizerische Akademie der Technischen Wissenschaften SATW, di gfs-zürich e della Mobiliare, si è posto l'obiettivo di contribuire, attraverso la rilevazione della situazione attuale e la presente pubblicazione, alla consapevolezza e al rafforzamento delle PMI svizzere con 4–49 collaboratori nel contesto del coronavirus (COVID-19).

I due studi rappresentativi condotti permettono di farsi un'idea in merito al ricorso all'home office e allo stato della cyber sicurezza nelle PMI, sollecitati dagli eventi legati alla pandemia di coronavirus/COVID-19 dal principio del 2020. Il sondaggio iniziale si è svolto tra le prime due ondate di coronavirus, dopo l'abrogazione della prima raccomandazione del Consiglio federale sull'home office (22 giugno 2020) e prima della sua seconda messa in vigore il 19 ottobre 2020 (il 18 gennaio 2021 l'home office è diventato un obbligo per tutte le imprese). Il presente secondo sondaggio ha avuto luogo in seguito all'annullamento dell'obbligo di home office per le aziende che effettuano regolarmente i test (dal 31 maggio 2021) rispettivamente è iniziato poco prima che l'obbligo venisse convertito in una raccomandazione di home office per tutte le imprese a partire dal 26 giugno 2021. La seconda indagine tra i 506 dirigenti di PMI è stata eseguita nel periodo compreso tra il 16 giugno e il 27 luglio 2021.

Prima del primo lockdown di marzo 2020, nelle PMI in cui l'home office era possibile per almeno un collaboratore, il 10 % del personale lavorava da casa. Questo valore è quasi quadruplicato (al 38 %) durante il primo lockdown per poi ridursi al 16 % (un aumento del 60 % rispetto alla situazione prima del lockdown). In seguito, è nuovamente pressoché triplicato (dal 16 % dopo il lockdown al 36 % durante l'obbligo di home office) nel corso del secondo lockdown e si è ora attestato a un livello più alto (20 %) in tutti i settori industriali. Il confronto delle due ondate mostra che il ricorso all'home office come luogo di lavoro nelle PMI svizzere è raddoppiato dall'inizio della crisi legata al coronavirus.

Come per il primo studio, anche dal secondo sondaggio emerge che il 19 % delle PMI con 4–49 collaboratori si considera pioniere, il 41 % Early Follower (2020: 44 %) e il 37 % Late Follower (2020: 33 %) nell'utilizzo di nuove tecnologie. I pionieri ottengono un vantaggio competitivo investendo per primi nelle nuove tecnologie e nelle innovazioni di prodotto e di marketing. Gli Early Follower seguono a ruota i pionieri, mentre i Late Follower utilizzano le innovazioni solo dopo un certo periodo di tempo, quando sono già state testate. Per quanto riguarda il ricorso all'home office spiccano i pionieri: in queste PMI l'85 % di tutti o di alcuni collaboratori potrebbe teoricamente lavorare da casa (e il 91 % dei collaboratori è già equipaggiato totalmente o parzialmente a tal fine). Ma anche gli Early Follower e i Late Follower hanno molto potenziale per l'home office: in circa due terzi delle PMI svizzere, infatti, tutti o alcuni collaboratori potrebbero teoricamente lavorare da casa (e due terzi delle PMI hanno già dotato tutti o alcuni collaboratori dell'equipaggiamento idoneo).

I fattori sociali/emotivi (ad es. la coesione del team), tecnici (ad es. l'accesso esterno ai dati) e organizzativi (ad es. il posto di lavoro) vengono visti come le maggiori sfide per l'attuazione dell'home office. Per lavorare da casa vengono utilizzati, tra l'altro, nuovi tool di comunicazione (in particolare tool di conferenza online e consulenze o formazioni online). Più grande è la PMI, maggiore è il numero di lavori IT che vengono eseguiti da fornitori esterni di servizi. In media, il 30 % delle PMI si avvale di fornitori esterni di servizi IT per approntare la propria infrastruttura informatica.

Con il coronavirus/COVID-19 e l'aumento del numero di collaboratori in modalità home office sono cresciuti anche gli attacchi nel cyber spazio. I dirigenti delle PMI svizzere affermano pertanto che la cyber criminalità è un problema da prendere sul serio (valutato con 4,6 su una scala di 5 punti) e che le misure contro i cyber attacchi sono importanti (4,4).

Lo studio mostra che un quinto dei dirigenti delle PMI non si sente informato o non si sente per niente informato sul tema della cyber sicurezza. Proprio come nel 2020, il 65 % dei dirigenti valuta la tematica come importante o molto importante. Ciò si evince anche dal fatto che nel 2021 il 36 % delle PMI è già stato vittima di cyber attacchi che hanno richiesto un notevole sforzo per rimediare ai danni (2020: 25 %). Gli effetti di questi attacchi sono danni finanziari, perdite dei dati dei clienti e danni alla reputazione.

Analogamente al sondaggio condotto nel 2020, le PMI svizzere sono in una fase relativamente molto avanzata per quanto riguarda l'attuazione delle misure tecniche per aumentare la cyber sicurezza. Tuttavia, la pianificazione e l'adozione di misure di sicurezza informatica a livello organizzativo presentano tanto potenziale: solo circa la metà delle PMI svizzere dispone di una strategia in materia di sicurezza informatica e soltanto due quinti di esse formano i loro collaboratori regolarmente oppure eseguono audit sulla sicurezza informatica. Durante l'obbligo di home office un quarto delle PMI ha pertanto investito in misure supplementari quali software di sicurezza, firewall e password più sicure. I risultati dello studio mostrano anche che le PMI hanno in molti casi regolamentato la responsabilità in materia di protezione dei dati (due terzi delle PMI) e definito i processi per la gestione dei dati.

Il rapporto completo con tutti i dati e le tabelle può essere scaricato gratuitamente in formato PDF dai siti web dei partner di ricerca:

www.cyberstudie.ch
www.digitalswitzerland.ch
www.kmu-transformation.ch/news
www.satw.ch

Di norma, i dirigenti delle PMI che sono informati sul tema della cyber sicurezza hanno implementato più misure per la tutela della propria infrastruttura informatica e dei dati dei clienti rispetto a quelli non informati. I temi della digitalizzazione, dell'home office, dell'impiego di tecnologie di comunicazione e della cyber sicurezza nel contesto del coronavirus/COVID-19 hanno ulteriormente acquisito importanza. Allo stesso tempo, daranno luogo a dibattiti sociali, economici, tecnologici e legati ai trasporti.

Con questo rapporto e i risultati dettagliati dello studio (vedi riquadro) speriamo di fornire un contributo per analizzare la situazione attuale, comprendere i fenomeni e rafforzare la vostra PMI.

Berna, novembre 2021

Andreas Hölzli
Responsabile del centro di competenza Cyber Risk
la Mobiliare, Berna

Andreas W. Kaelin
Amministratore delegato supplente e
responsabile del dossier Cybersecurity
digitalswitzerland, Berna

Karin Mändli Lerch
Responsabile di progetto
gfs-zürich, Zurigo

Marc K. Peter
Responsabile del centro di competenza
Trasformazione digitale
FHNW Hochschule für Wirtschaft, Olten

Patric Vifian
Marketing Manager PMI
la Mobiliare, Berna

Nicole Wettstein
Responsabile del programma Cybersecurity
Schweizerische Akademie der Technischen
Wissenschaften SATW, Zurigo

Importanza e utilizzo dell'home office

Sussiste un grande potenziale per l'home office e un terzo dei collaboratori è già totalmente equipaggiato a tal fine

In circa due terzi (65 %) delle PMI svizzere tutti o almeno una parte dei collaboratori potrebbero teoricamente lavorare da casa (2020: 67 %). Non devono dunque avere mansioni quali ad es. seguire clienti in loco, guidare un veicolo o lavorare in un cantiere (nel 14 % tutti; nel 51 % una parte dei collaboratori). Si tratta di una percentuale elevata che mostra i potenziali dell'home office e i relativi effetti sociali, economici, tecnologici e legati ai trasporti.

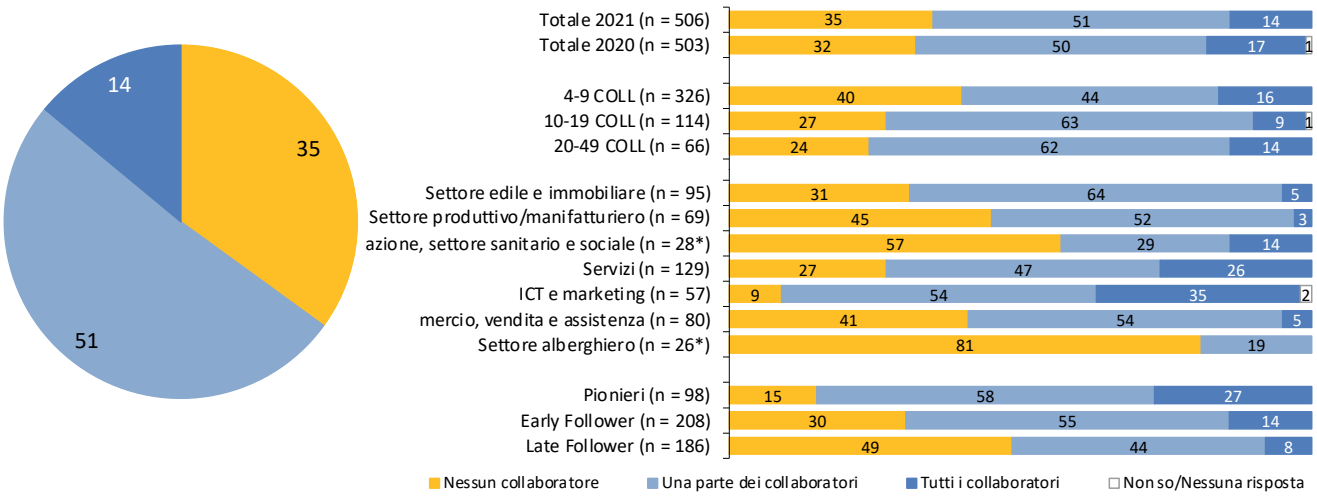
Già oggi il 29 % dei collaboratori delle PMI (2020: 20 %) è equipaggiato totalmente e il 39 % parzialmente (2020: 46 %) con gli strumenti adatti per lavorare da casa, a prescindere dal fatto che siano essi aziendali o privati. La quota di collaboratori che sono totalmente o parzialmente equipaggiati per l'home office corrisponde a quella del 2020; tuttavia, ora un numero significativamente maggiore di collaboratori è equipaggiato al 100 % per lavorare da casa.

Spiccano i pionieri: in queste PMI l'85 % di tutti o di alcuni collaboratori potrebbe teoricamente lavorare da casa; e il 91 % dei collaboratori è già equipaggiato totalmente o parzialmente a tal fine.

Domande per le PMI svizzere

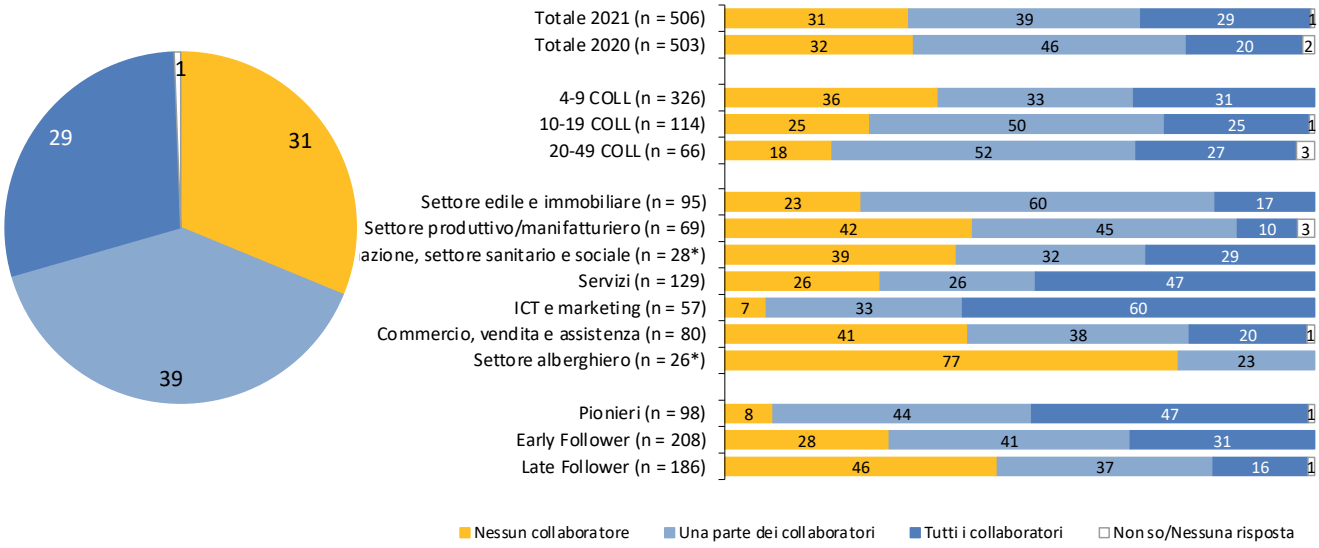
- Come utilizzate strategicamente l'home office per aumentare la flessibilità e l'attrattiva per i collaboratori e ridurre la struttura dei costi?
- Avete già discusso del tema home office con i vostri collaboratori e avete individuato idee/potenziali sviluppi nonché realizzato una tabella di marcia?
- È disponibile un accordo di home office, ad es. per regolamentare l'assunzione dei costi dell'equipaggiamento privato per l'ufficio?

Numero di collaboratori che potenzialmente potrebbero lavorare dall'home office



Numero di collaboratori che potenzialmente potrebbero lavorare dall'home office («Quanti dei suoi collaboratori potrebbero teoricamente lavorare da casa, ossia non devono ad es. seguire i clienti in loco, guidare un veicolo o lavorare in un cantiere?» / n 2021 = 506, n 2020 = 503 / le categorie con un campionamento inferiore a 30 sono contrassegnate con un *)

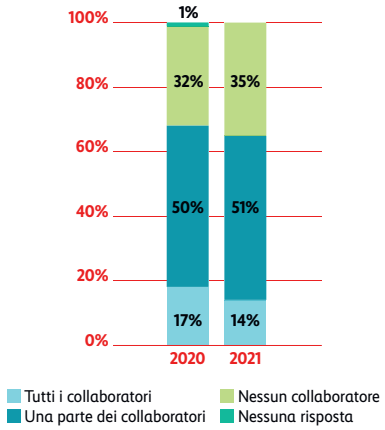
Numero di collaboratori che sono equipaggiati per l'home office



Numero di collaboratori che sono equipaggiati per l'home office («Quanti dei suoi collaboratori sono totalmente equipaggiati con gli strumenti adatti per lavorare da casa, a prescindere dal fatto che siano essi aziendali o privati?» / n 2021 = 506, n 2020 = 503 / le categorie con un campionamento inferiore a 30 sono contrassegnate con un *)

Infografica

Numero di collaboratori che potenzialmente potrebbero lavorare in homeoffice



Numero di collaboratori che sono equipaggiati per l'homeoffice

Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

La Scuola universitaria professionale della Svizzera nordoccidentale (FHNW) ha un profilo internazionale e un forte orientamento alla pratica. Forma 3000 studenti di bachelor e master a Basilea, Brugg-Windisch e Olten e, con la sua vasta gamma di corsi di formazione aziendale, è leader tra le scuole universitarie professionali svizzere.

Il centro di competenza Trasformazione Digitale del Prof. Dr. Marc K. Peter presso la FHNW offre servizi di ricerca, consulenza e formazione in materia di trasformazione digitale per aiutare le organizzazioni e il personale a sviluppare e attuare con successo strategie di crescita digitale.

Importanti strumenti per la trasformazione digitale delle PMI (in tedesco):

Workshop Canvas Trasformazione digitale
Il workshop Canvas sulla trasformazione digitale è uno strumento gratuito grazie al quale le aziende assieme ai propri collaboratori possono sviluppare idee e individuare opportunità per avviare una trasformazione digitale.
www.digital-transformation-canvas.net

Workshop Canvas Sviluppo strategico nell'era digitale
Il workshop Canvas sullo sviluppo strategico nell'era digitale è uno strumento gratuito, grazie al quale le aziende assieme ai propri collaboratori possono sviluppare la loro strategia per la trasformazione digitale dell'azienda.
www.act-strategy-canvas.ch

Workshop Canvas Mondo del lavoro 4.0
Il workshop Canvas sul mondo del lavoro 4.0 è uno strumento gratuito grazie al quale le aziende assieme ai propri collaboratori possono sviluppare idee e individuare opportunità per definire una strategia legata all'ambiente di lavoro.
www.arbeitswelt-zukunft.ch/workshop-canvas

Valutazione della maturità digitale
Con l'analisi gratuita della maturità digitale si può valutare se stessi e la propria azienda per monitorare i progressi dalla trasformazione e i progetti avviati o realizzati in tutti i campi d'azione. Dove risiede il (maggior) potenziale?
www.digitale-reife.net

Valutazione dei temi strategici
Il check online gratuito della strategia permette di definire i temi e le questioni da discutere nell'ambito dello sviluppo della strategia per l'era digitale.
www.digital-strategy-check.ch

Guida pratica Sviluppo strategico nell'era digitale
Risultati delle ricerche, consigli pratici, studi di casi, modelli di strategia e liste di controllo per pianificare e attuare la trasformazione digitale:
www.strategische-transformation.ch

Guida pratica Trasformazione digitale per PMI
Risultati delle ricerche, consigli pratici, studi di casi e liste di controllo per la trasformazione della propria PMI:
www.kmu-transformation.ch

Guida pratica Mondo del lavoro 4.0
Risultati delle ricerche, consigli pratici, studi di casi e liste di controllo per il nuovo mondo del lavoro:
www.arbeitswelt-zukunft.ch

Ulteriori informazioni:
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

Cambiamento delle abitudini relative all'home office durante e dopo il lockdown dovuto al coronavirus

Raddoppiamento del ricorso all'home office nelle PMI svizzere entro due anni

Prima del primo lockdown del 2020, nelle PMI in cui l'home office era possibile per almeno un collaboratore, il 10% del personale lavorava da casa. Questo valore è quasi quadruplicato (al 38%) durante il primo lockdown per poi ridursi al 16% (un aumento del 60%).

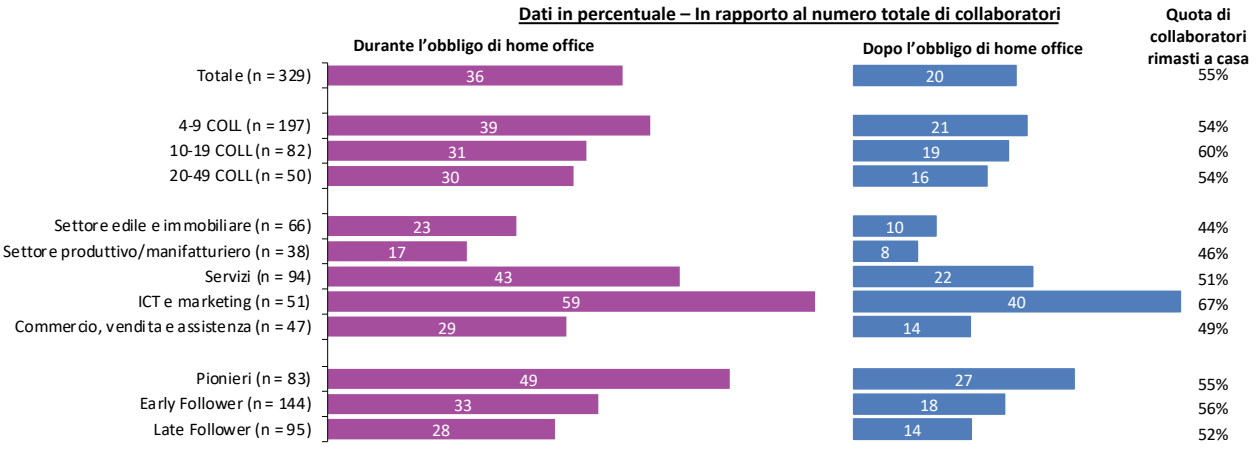
In seguito, è nuovamente pressoché triplicato (dal 16% dopo il lockdown al 36% durante l'obbligo di home office) nel corso del secondo lockdown e si è ora attestato a un livello più alto (20%) in tutti i settori industriali. Per i pionieri questo valore si attesta al 27%, per i Late Follower solo al 14%.

Il confronto delle due ondate mostra che il ricorso all'home office come luogo di lavoro nelle PMI svizzere è raddoppiato dall'inizio della crisi legata al coronavirus. In talune circostanze, questo valore diminuirà leggermente a medio termine, poiché il 15% delle PMI parte sì dal presupposto di un aumento, ma il 38% presuppone una riduzione. È interessante notare che tale valore è relativamente alto proprio per i pionieri (il 45% parte dal presupposto di una riduzione). Nel complesso, un numero maggiore di dirigenti rispetto al 2020 non è contento di uno sviluppo a lungo termine che prevede più collaboratori in modalità home office. Nel 2020 la quota di dirigenti che personalmente non si rallegravano di tale evoluzione era pari all'8% (valori 1 e 2 su una scala di 5 punti); nel 2021 questa percentuale è salita già al 15%.

Domande per le PMI svizzere

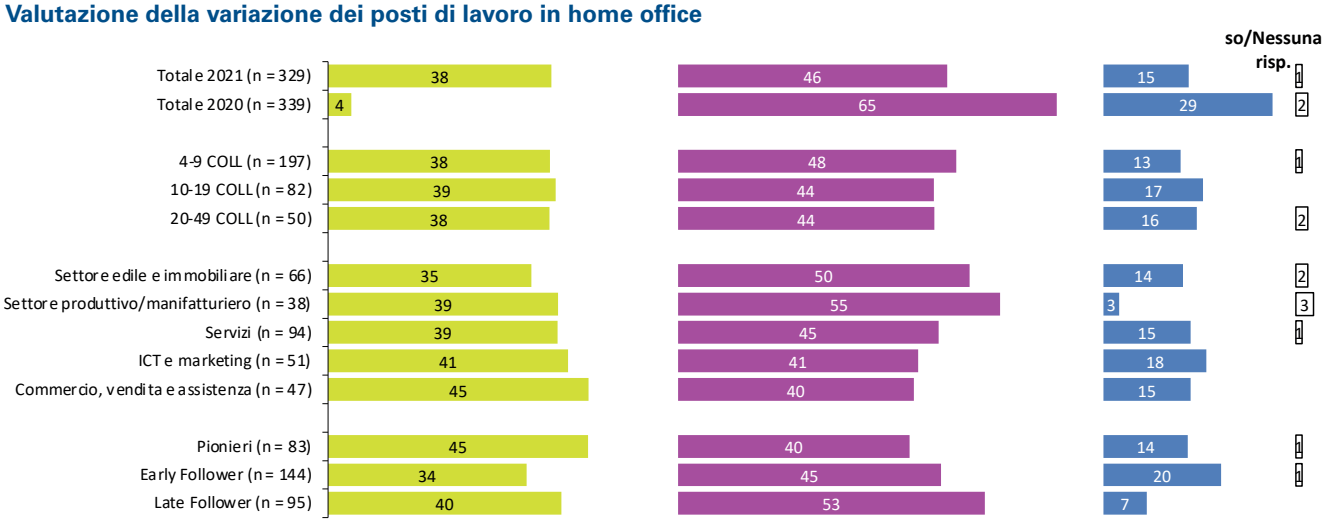
- A lungo termine l'home office si affermerà nella vostra azienda? Ne avete individuato e discusso il potenziale?
- Avete identificato e definito i requisiti per il «new work» (mondo del lavoro 4.0) in relazione ai temi della cultura, della conduzione e della comunicazione?
- Avete sviluppato una strategia accompagnata da una tabella di marcia per il mondo del lavoro 4.0?

Cambiamento delle abitudini relative all'home office durante il lockdown dovuto al coronavirus/durante l'obbligo di home office



Cambiamento delle abitudini relative all'home office durante il lockdown dovuto al coronavirus/durante l'obbligo di home office («Quanti dei suoi collaboratori hanno lavorato principalmente da casa dall'inizio del 2021, ovvero durante l'obbligo di home office?», «E quanti lavorano ora, dopo l'obbligo di home office, principalmente da casa?» / n = 329 (filtro: se almeno un collaboratore può lavorare teoricamente dall'home office))

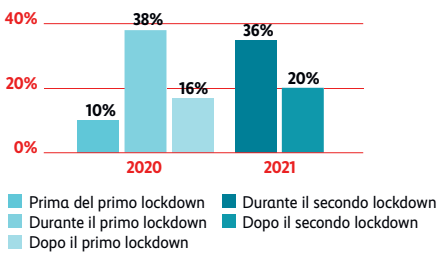
Valutazione della variazione dei posti di lavoro in home office



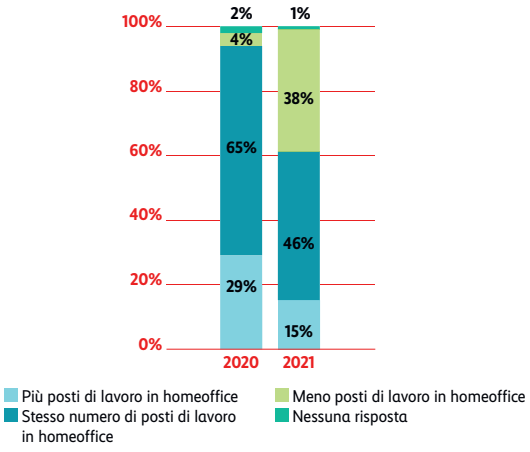
Valutazione della variazione dei posti di lavoro in home office («Come valuta l'evoluzione a lungo termine? Rispetto al periodo della pandemia, in futuro nella sua azienda lavorerà da casa un numero maggiore, uguale o minore di collaboratori?» / n 2021 = 329, n 2020 = 339 (filtro: se almeno un collaboratore può lavorare teoricamente dall'home office))

Infografica

Cambiamento delle abitudini rispetto all'homeoffice durante il lockdown dovuto al coronavirus



Stima della variazione del numero di posti di lavoro in homeoffice



Sfide nell'attuazione dell'home office

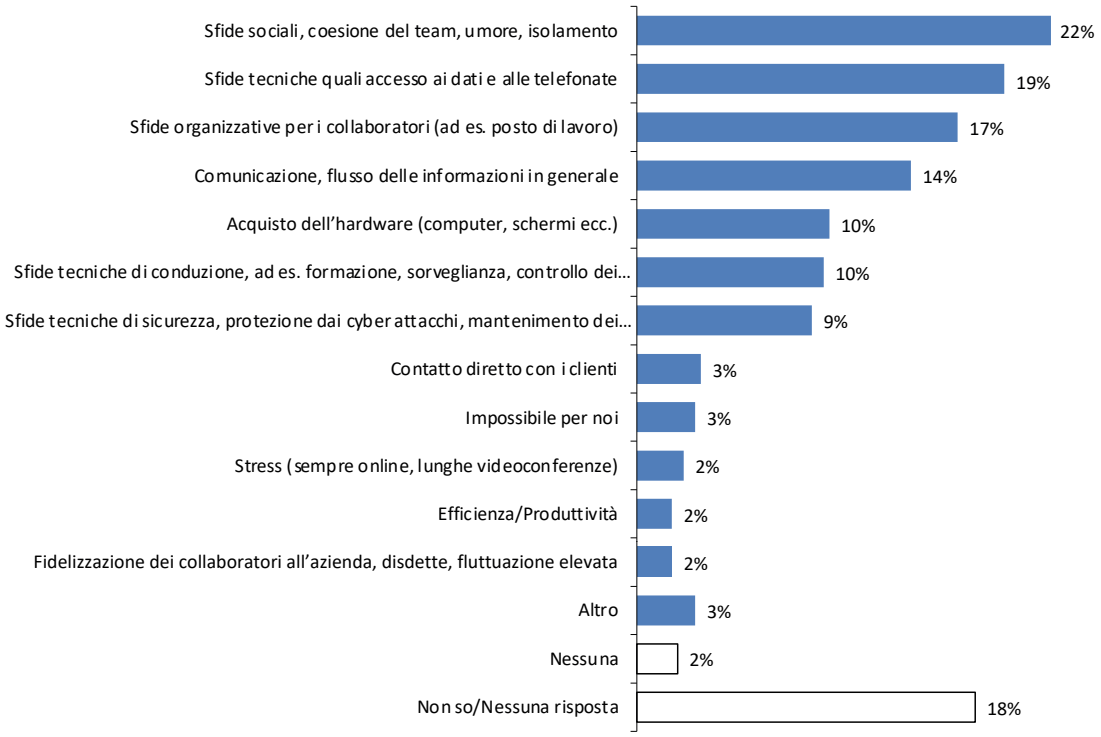
Collaborazione, conduzione e organizzazione come importanti fattori di successo

Il fattore sociale/emotivo (sfide sociali, coesione del team, umore, isolamento), quello tecnico (sfide tecniche quali accesso ai dati e alle telefonate) nonché quello organizzativo (sfide per i collaboratori quali ad es. il posto di lavoro) vengono visti come le maggiori sfide per l'attuazione dell'home office da quasi un quinto delle PMI. Per circa un decimo delle PMI svizzere a ciò si aggiungono sia le sfide tecniche di conduzione sia quelle di sicurezza.

Questo quadro viene confermato da uno studio della FHNW Hochschule für Wirtschaft condotto nel 2019 che descriveva le dimensioni People (collaboratori), Place (ambiente di lavoro) e Technology (tecnologie) come i fattori di successo per la creazione del mondo del lavoro 4.0 (vedi riquadro informativo con libro consigliato).

Domande per le PMI svizzere

- Quali esperienze positive e negative avete raccolto con l'home office durante il lockdown? Cosa vi ha consentito di imparare e migliorare?
- Perché non utilizzate maggiormente e in modo strategico l'home office per rinnovare la vostra azienda, ad es. per rafforzare la vostra reputazione come datore di lavoro?



Sfide nell'attuazione dell'home office («Quali sono dal punto di vista aziendale le maggiori sfide nell'attuazione dell'home office?») / n = 329, sono possibili più risposte (filtro: se almeno un collaboratore può lavorare teoricamente dall'home office))

Utilizzo dei tool di comunicazione

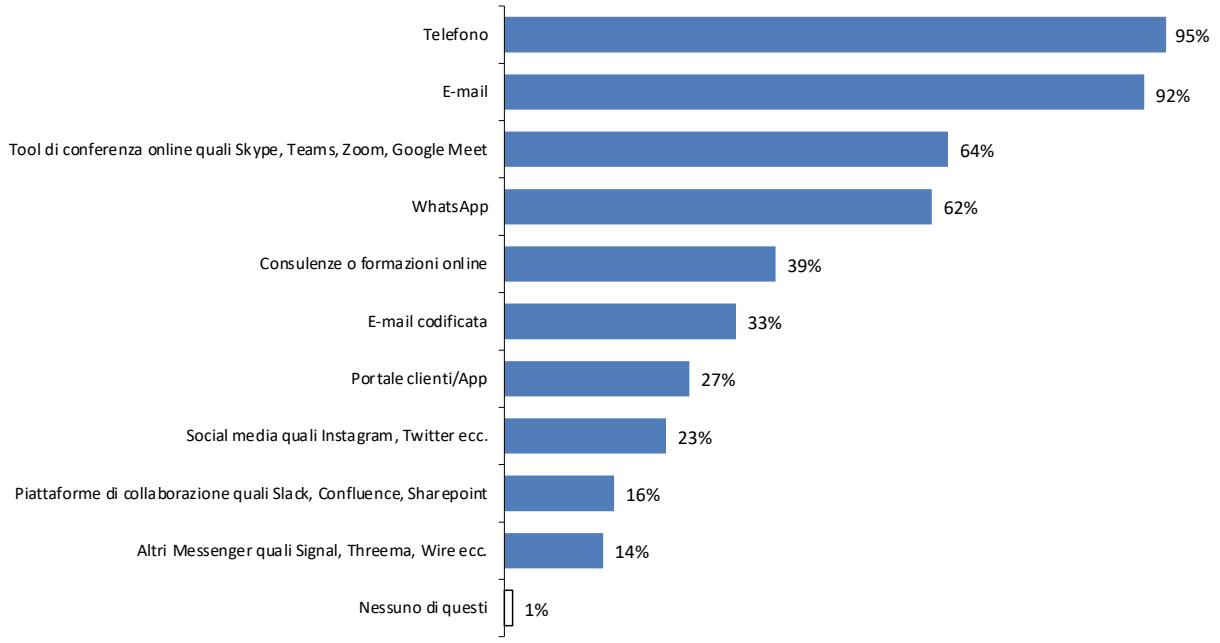
Tool di conferenza online e consulenze o formazioni online come importanti nuove piattaforme

Il telefono e la posta elettronica continuano a essere importanti tool di comunicazione. Nel corso del secondo sondaggio condotto nel 2021 è stata per la prima volta posta una domanda sul numero di e-mail codificate: un terzo delle PMI svizzere le utilizza già. In considerazione del lavoro preparatorio risp. straordinario necessario a livello tecnico e organizzativo si tratta di una quota elevata. L'utilizzo dei tool di conferenza online (2020: 46 %, 2021: 64 %) nonché delle consulenze o formazioni online (2020: 20 %, 2021: 39 %) è decisamente aumentato.

Domande per le PMI svizzere

- È stata elaborata una strategia per l'utilizzo dei tool di comunicazione (e sono state in seguito implementate le piattaforme più opportune)?
- Esistono un piano di sicurezza dei dati e le relative direttive per l'uso professionale di queste piattaforme di comunicazione?
- Le piattaforme sono sicure? Quali informazioni/dati vengono risp. possono essere scambiati e attraverso quali piattaforme?

Utilizzo dei tool di comunicazione



Utilizzo dei tool di comunicazione («Le menziono ora alcuni strumenti di comunicazione digitali. Quali di questi utilizzano attualmente i suoi collaboratori per comunicare con partner aziendali, clienti e altri collaboratori?» / n = 506, sono possibili più risposte)

Informazione personale sulla tematica dei cyber rischi

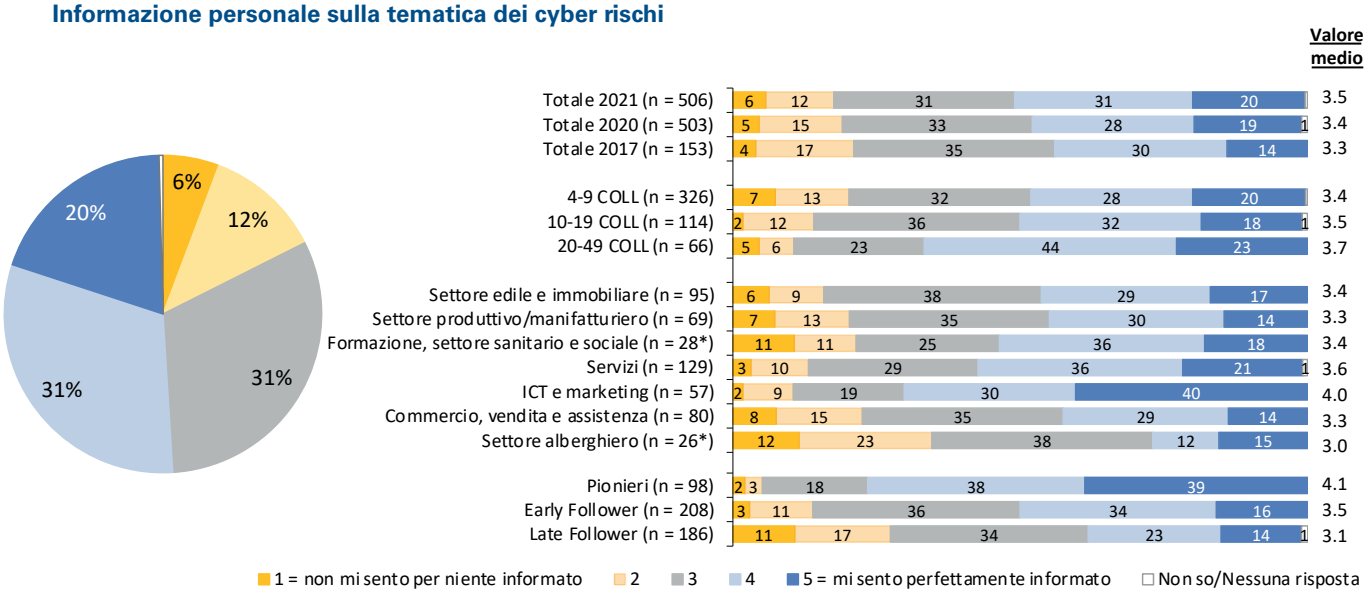
Un quinto dei dirigenti delle PMI non si sente informato o non si sente per niente informato

I dirigenti delle PMI svizzere si sentono leggermente meglio informati rispetto a un anno fa. Il valore è tuttavia sempre ancora basso: solo il 51 % si sente ben informato o perfettamente informato (2020: 47 %). Più grande è la PMI, meglio informati sulla tematica sono i dirigenti. Sono soprattutto i pionieri a sentirsi ben informati o perfettamente informati (77 %). Anche la cyber sicurezza continua a essere fondamentale: proprio come nel 2020, il 65 % dei dirigenti delle PMI svizzere considera la tematica importante o molto importante.

Domande per le PMI svizzere:

- Individuate regolarmente il potenziale di utilizzo delle nuove tecnologie e disponete di una strategia/una tabella di marcia per l'introduzione di nuove infrastrutture informatiche?
- Quali nuovi prodotti e servizi potreste lanciare con (maggior) successo sul mercato investendo nell'infrastruttura informatica e nella cyber sicurezza?
- Siete in grado di soddisfare le vostre esigenze (o quelle del mercato) in materia di cyber sicurezza?
- Come vi informate regolarmente su pericoli, programmi e soluzioni per aumentare la cyber sicurezza?

Informazione personale sulla tematica dei cyber rischi



Informazione personale sulla tematica dei cyber rischi («In generale, personalmente quanto si sente informato sulla tematica dei cyber rischi?» / n 2021 = 506, n 2020 = 503 / le categorie con un campionamento < 30 sono contrassegnate con un *)

digitalswitzerland

Su digitalswitzerland

digitalswitzerland è un'iniziativa nazionale e intersettoriale che mira a rafforzare e consolidare la Svizzera come leader mondiale dell'innovazione digitale.
Sotto il mantello di digitalswitzerland, più di 230 organizzazioni, composte da membri dell'associazione e fondazioni partner politicamente neutrali, lavorano insieme trasversalmente al perseguimento di questo obiettivo. digitalswitzerland è l'interlocutore per tutte le questioni di digitalizzazione e si adopera per la soluzione una vasta gamma di sfide.

Importanti strumenti per le PMI:

Test rapido di cyber sicurezza per PMI
cybersecurity-check.ch

Le PMI svizzere spesso non sono sufficientemente protette dalle gravi minacce provenienti dal cyberspazio e non ne sono consapevoli.
Un gruppo di lavoro avviato da ICTswitzerland e composto da rappresentanti dell'economia, delle associazioni e della Confederazione ha unito le forze per sensibilizzare le PMI nei confronti delle minacce del cyberspazio. Il risultato è il test rapido di cyber sicurezza per PMI che permette a chiunque di scoprire facilmente se la propria azienda è sufficientemente protetta contro i rischi informatici.

Un'iniziativa congiunta dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE), della Commissione di esperti per il futuro del trattamento e della sicurezza dei dati della Confederazione, di ICTswitzerland, dell'Organo direzione informatica della Confederazione (ODIC) – Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), dell'Information Security Society Switzerland (ISSS), dell'Accademia svizzera delle scienze tecniche (SATW), dell'Associazione svizzera di normalizzazione (SNV), dell'Associazione svizzera per i sistemi di qualità e di gestione (SQS) e dell'Associazione svizzera d'assicurazioni (ASA).

Con fornitori di servizi IT competenti per una maggiore cyber sicurezza
digitalsecurityswitzerland.ch

L'Alleanza Sicurezza Digitale Svizzera sviluppa il marchio di qualità CyberSeal «Fornitore di servizi IT certificato».
Il marchio CyberSeal evidenzia l'affidabilità di fornitori di servizi IT e aiuta le PMI a scegliere il loro partner IT. Contraddistingue i fornitori di servizi IT che garantiscono ai loro clienti un adeguato livello di protezione con le necessarie misure tecniche e organizzative.
CyberSeal aumenta così la sicurezza digitale delle PMI e contribuisce al posizionamento della digitalizzazione a un livello di qualità superiore.

Cyber attacchi riusciti e relativi danni

Oltre un terzo delle PMI svizzere è già stato attaccato con successo

Il 36 % delle PMI svizzere è già stato una volta vittima di cyber attacchi che hanno richiesto un notevole sforzo per rimediare ai danni (2020: 25 %). Ciò corrisponde a una crescita del 44 % in un anno. Notevolmente aumentata è la tecnica di attacco delle truffe online che, in molti casi, avviene tramite una frode a nome del CEO: ai collaboratori vengono inviate delle e-mail false il cui mittente è il CEO della propria azienda. Nei messaggi di posta elettronica il CEO chiede, con una storia inventata, di effettuare un pagamento a favore di una persona/ditta terza.

Tecniche impiegate nel 2021 per cyber attacchi riusciti nelle PMI svizzere
(tra parentesi i valori del 2020)

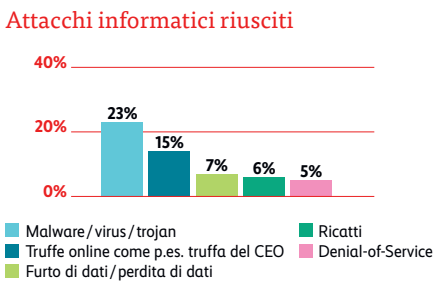
- Malware/virus/trojan: 23 % (18 %)
- Truffa online come ad es. frode a nome del CEO: 15 % (6 %)
- Furto di dati/perdita di dati: 7 % (5 %)
- Estorsione: 6 % (4 %)
- Denial of Service: 5 % (5 %)

I cyber attacchi provocano danni finanziari (nel 25 % delle PMI in cui un attacco ha causato notevoli danni), perdita dei dati dei clienti (7 %) e danni alla reputazione (6 %).

Domande per le PMI svizzere

- I collaboratori conoscono le varie tecniche di attacco? Come vengono sensibilizzati e formati i vostri dipendenti?
- Quali misure tecniche e organizzative adottate per aumentare la cyber sicurezza nella vostra azienda?
- Come verificate regolarmente le vostre strategie e misure per la cyber sicurezza?

Infografica



Cyber attacchi andati a buon fine («La sua azienda ha mai subito un attacco mediante una delle seguente tecniche che abbia richiesto un notevole sforzo per rimediare ai danni?» / n = 506, percentuale di sì)

L'Accademia svizzera delle scienze tecniche (SATW) è la rete principale di esperti nel settore delle scienze ingegneristiche in Svizzera. Su incarico della Confederazione, identifica gli sviluppi tecnologici rilevanti a livello industriale e informa la politica e la società sul loro significato e le loro conseguenze. Come organizzazione specializzata e politicamente indipendente, promuove il comportamento sicuro di tutti gli attori del cyberspazio.

Sfide di cyber sicurezza per la Svizzera
Sulla base di brevi testi, i membri dell'Advisory Board Cybersecurity della SATW forniscono una visione degli attuali sviluppi tecnologici rilevanti dal punto di vista della cyber sicurezza. Per ogni sviluppo, viene spiegata la necessità di agire a breve e medio termine.
https://www.satw.ch/fr/cybersecurite/cybersecurity-map

Technology Outlook
La SATW individua sviluppi tecnologici economicamente rilevanti e informa la politica e la società del loro significato, della loro importanza e delle loro conseguenze. A tale scopo, redige anche il Technology Outlook, pubblicato ogni due anni.
https://www.satw.ch/to2021

Rete Autodeterminazione Digitale
La Rete Autodeterminazione Digitale si adopera per l'utilizzo dei dati innovativo e autodeterminato in Svizzera. L'obiettivo è cogliere appieno e promuovere i potenziali dell'economia dei dati e della società dei dati. La rete è stata fondata dalla SATW, assieme alla Direzione del diritto internazionale pubblico del DFAE, all'Ufficio federale delle comunicazioni e a Swiss Data Alliance.
https://www.satw.ch/digitale-selbstbestimmung

Promozione nuove leve
La promozione delle nuove leve da parte della SATW incoraggia l'interesse e la comprensione della tecnologia da parte dei giovani. Sostiene un'educazione tecnologica completa e contrasta attivamente la carenza di personale qualificato. Uno dei suoi intenti principali è la promozione delle ragazze nella tecnologia.
https://www.satw.ch/it/formazione-tecnica

Ulteriori informazioni:

SATW
Accademia svizzera
delle scienze tecniche
St. Annagasse 18
8001 Zurigo
www.satw.ch

Rischi di cyber attacchi piccoli e che mettono a repentaglio la sopravvivenza dell'azienda

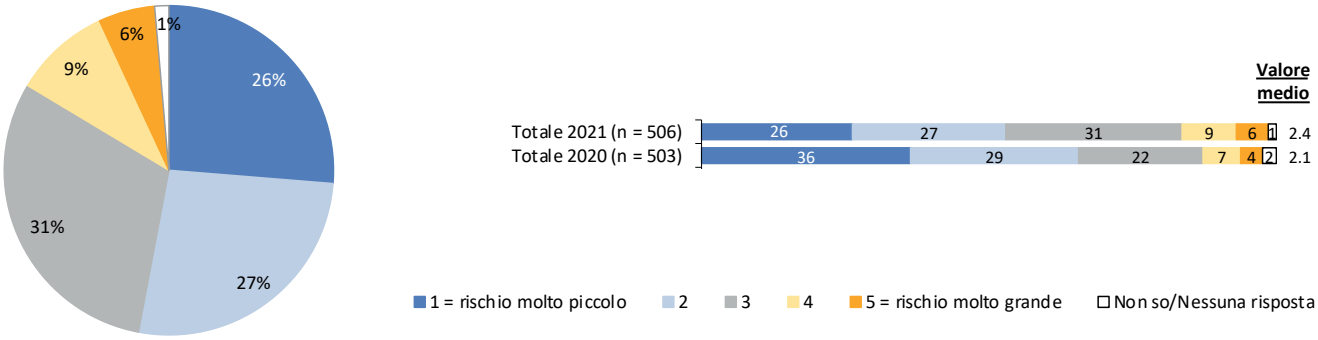
La valutazione dei rischi di cyber attacchi cresce a un livello basso

La digitalizzazione, l'home office e l'attività lucrativa della cyber criminalità accrescono la valutazione dei rischi delle PMI svizzere: nel 2021 il 15 % dei dirigenti ritiene alto o molto alto il rischio che la propria azienda possa essere vittima entro i prossimi due-tre anni di un cyber attacco che metta «fuori combattimento» l'impresa per almeno un giorno (2020: 11 %). Il valore della valutazione di cyber attacchi che mettono a repentaglio la sopravvivenza dell'azienda aumenta rispetto all'anno precedente, ma si attesta al 4 %, una percentuale nettamente inferiore alla probabilità che si verifichi una sospensione delle attività di un giorno (2020: 2 %).

Domande per le PMI svizzere

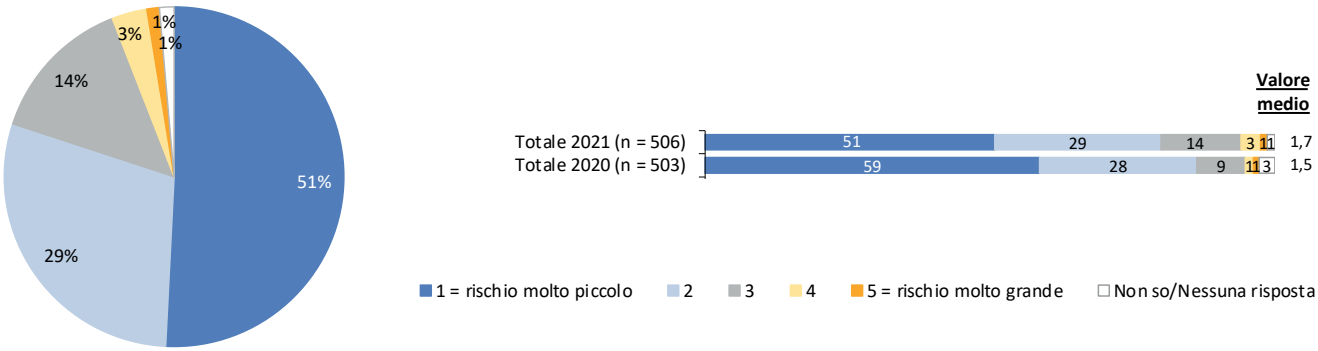
- Quale infrastruttura informatica è fondamentale per la fornitura di servizi nella vostra azienda risp. quanto è importante per voi la cyber sicurezza?
- Quali prestazioni non potete fornire se l'infrastruttura informatica non funziona?
- Come proteggete questa infrastruttura informatica?
- Quali alternative (cosiddette strategie di recovery) avete preparato?
- Di quali strategie/piani d'emergenza disponete e quali componenti mancano?

Valutazione del rischio «piccolo» cyber attacco



Valutazione del rischio «piccolo» cyber attacco («Quanto ritiene alto il rischio che nei prossimi 2–3 anni la sua PMI venga colpita da un cyber attacco che ne comprometta l'attività per almeno un giorno?» / n 2021 = 506, n 2020 = 503)

Valutazione del rischio cyber attacco che mette a repentaglio la sopravvivenza dell'azienda



Valutazione del rischio cyber attacco che mette a repentaglio la sopravvivenza dell'azienda («Quanto ritiene alto il rischio che nei prossimi 2–3 anni la sua PMI venga colpita da un cyber attacco che ne metta a repentaglio la sopravvivenza?» / n 2021 = 506, n 2020 = 503)

Misure tecniche e organizzative per aumentare la cyber sicurezza

La pianificazione e l'adozione di misure di sicurezza informatica a livello organizzativo presentano tanto potenziale

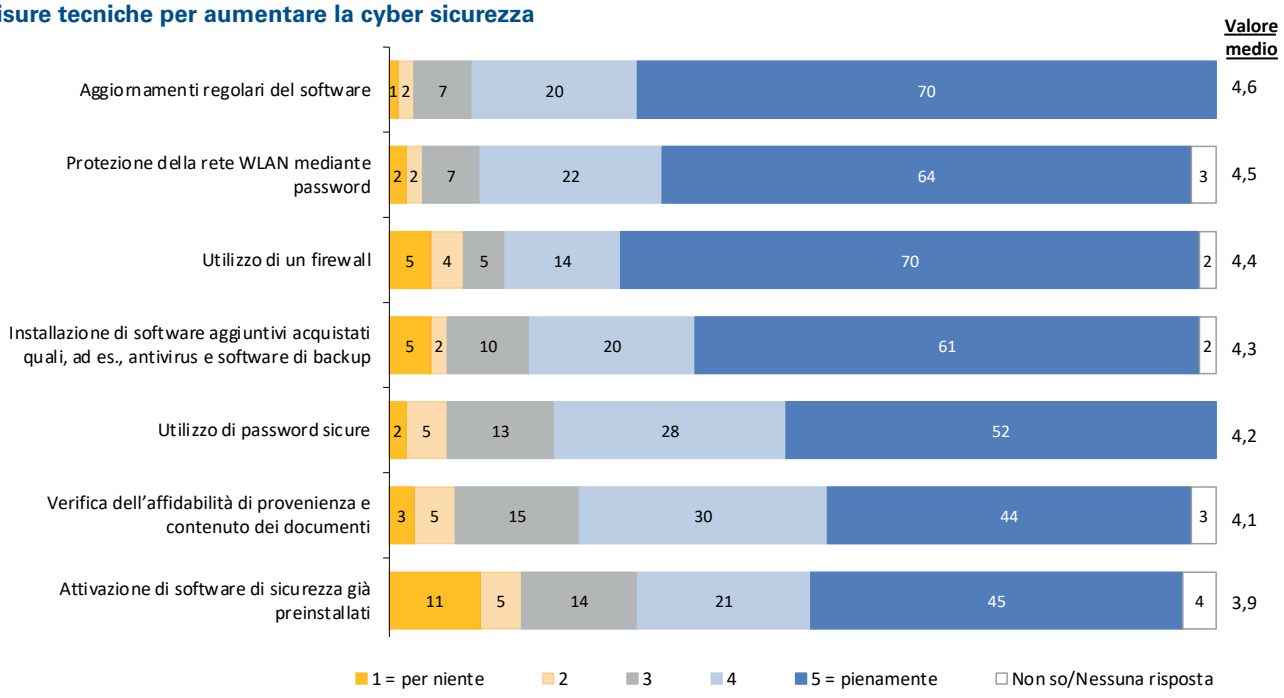
Analogamente al sondaggio condotto nel 2020, le PMI svizzere sono in una fase relativamente molto avanzata per quanto riguarda l'attuazione delle misure tecniche per aumentare la cyber sicurezza. A livello di misure organizzative sussiste tanto potenziale anche nel 2021 (parimenti al 2020). Solo circa la metà delle PMI svizzere dispone di una strategia in materia di sicurezza informatica (47 % del tutto/pienamente) e soltanto due quinti di esse formano i loro collaboratori regolarmente (39 %) oppure eseguono audit sulla sicurezza informatica (37 %).

In un terzo delle PMI (30 %) i dirigenti mettono a disposizione un budget separato per la sicurezza informatica. Questo valore è più alto per quelle PMI che sono già state vittima di un attacco (31 %) e i cui dirigenti si sentono piuttosto informati in fatto di cyber sicurezza (37 %).

Domande per le PMI svizzere

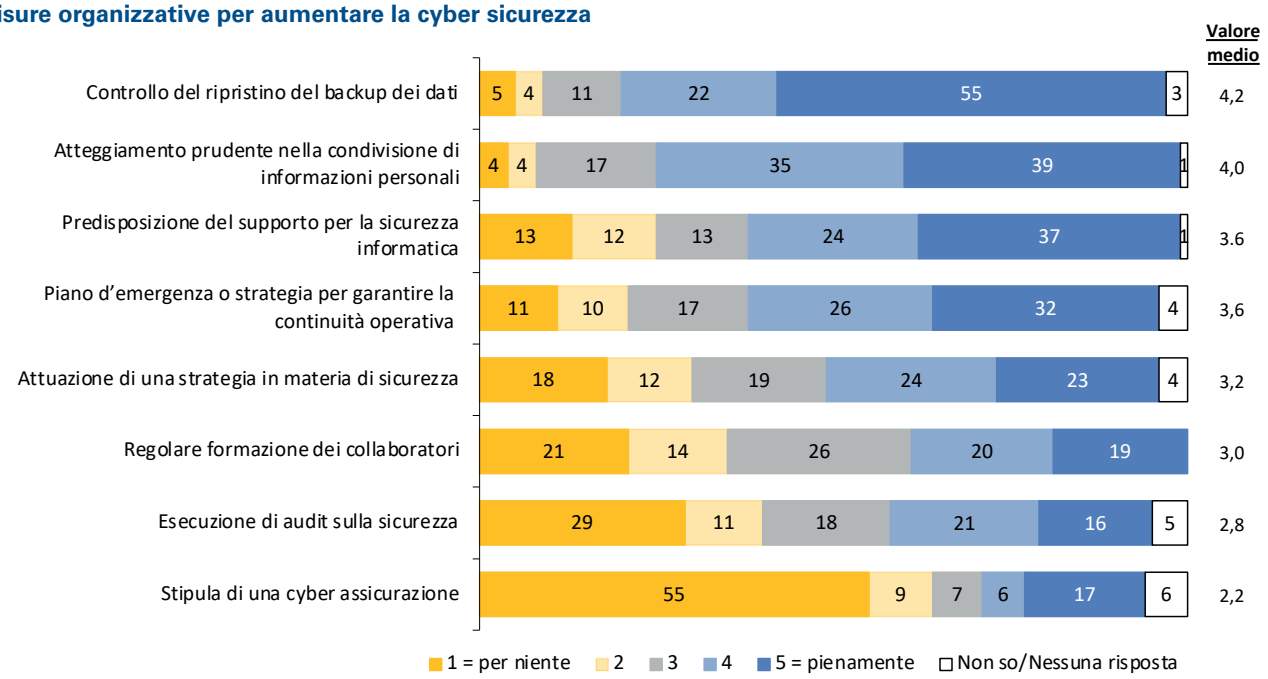
- Avete fatto un inventario della vostra infrastruttura informatica? Esiste un elenco dell'hardware e del software (con numeri di serie, data di acquisto/prezzo, versioni software ecc.)?
- Quale infrastruttura informatica viene aggiornata da chi e con quale frequenza?
- Come proteggete la vostra infrastruttura informatica per garantire la continuità dell'attività in caso di attacchi e altri problemi?
- Quali misure organizzative concrete dovrebbero essere pianificate e attuate?
- Sarebbe eventualmente utile effettuare un audit sulla sicurezza informatica e stipulare una cyber assicurazione?

Misure tecniche per aumentare la cyber sicurezza



Misure tecniche per aumentare la cyber sicurezza («Fino a che punto nella sua azienda sono attuate le seguenti misure tecniche per aumentare la cyber sicurezza?» / n = 506 / scala da 1 = per niente fino a 5 = pienamente, dati in valori medi)
La figura rappresentata contiene i valori 4 e 5 della scala da 5 punti.

Misure organizzative per aumentare la cyber sicurezza



Misure organizzative per aumentare la cyber sicurezza («Fino a che punto nella sua azienda sono attuate le seguenti misure organizzative per aumentare la cyber sicurezza?» / n = 506 / scala da 1 = per niente fino a 5 = pienamente, dati in valori medi)
La figura rappresentata contiene i valori 4 e 5 della scala da 5 punti.

la Mobiliare

Il Gruppo Mobiliare («Mobiliare») è il leader in Svizzera nel settore retail e il numero uno per le assicurazioni economia domestica, PMI e rischio vita. Fondata nel 1826, la Mobiliare è la più antica società privata d'assicurazioni della Svizzera e ancora oggi rimane fedele alle proprie radici cooperative.
Le sue 80 agenzie generali, gestite da imprenditori indipendenti e dotate di un proprio servizio sinistri, garantiscono in 160 sedi la vicinanza agli oltre 2,2 milioni di clienti.
In Svizzera, un'economia domestica su tre e un'impresa su tre sono assicurate presso la Mobiliare. La Mobiliare in qualità di assicuratore generale impiega 5856 collaboratrici e collaboratori e offre 338 posti di apprendistato.

L'offerta cyber protezione per PMI in sintesi

Breve valutazione della cyber sicurezza
Questo servizio comprende una verifica gratuita della cyber sicurezza, accompagnata da raccomandazioni concrete per migliorare la sicurezza e offre alle PMI i seguenti valori aggiunti:

- valutazione imparziale della cyber sicurezza basata su standard;
- confronto della situazione di rischio della PMI con altre imprese;
- raccomandazioni concrete e personalizzate sugli interventi con rimando a ulteriori fonti d'informazione.

Ulteriori informazioni su
www.mobiliare.ch/valutazione-cyber-sicurezza

Cyber training per imprese
A volte basta un attimo: un collaboratore distratto apre un'e-mail e all'improvviso tutta l'impresa è paralizzata. Il cyber training sensibilizza i collaboratori sull'utilizzo di Internet e della posta elettronica.
Dopo il training di sensibilizzazione i collaboratori dell'azienda conosceranno i diversi metodi impiegati dagli hacker e sapranno come reagire nel migliore dei modi.
Il cyber traning di sensibilizzazione si compone di diversi moduli:

- training online per il riconoscimento delle minacce provenienti da Internet;
- simulazioni di attacchi di phishing con valutazione della reazione dei dipendenti;
- rapporto finale con i dati più rilevanti per ciascuna unità del training.

Ulteriori informazioni su
www.mobiliare.ch/cyber-training

Cyber assicurazione
La cyber assicurazione è un vasto pacchetto di misure con le quali si protegge l'attività della PMI a seguito di un cyber attacco. L'assicurazione copre:

- spese per gli specialisti incaricati di rimuovere i malware, ripristinare i dati e intervenire per evitare la minaccia di una diffusione illecita;
- indennizzo per l'interruzione d'esercizio se la PMI non può lavorare per più di dodici ore;
- assistenza finanziaria e giuridica se un cliente si rivale sulla PMI poiché una e-mail conteneva un virus che gli ha arrecato danni.

Ulteriori informazioni su
www.mobiliare.ch/cyberprotezione-aziende

Una raccolta di informazioni utili per le PMI, anche sul tema della cyber sicurezza, si trova su
www.mobiliare.ch/pmi

Misure di cyber sicurezza in seguito all'obbligo di home office

Investimenti supplementari in software, firewall e password

Con l'aumento dei cyber attacchi e del ricorso all'home office come luogo di lavoro per tanti collaboratori, le PMI svizzere hanno reagito anche con misure supplementari in termini di cyber sicurezza. Il 23 % delle PMI (2020: 9 %) ha attuato ulteriori misure in seguito all'obbligo/alla raccomandazione di home office. Ancora una volta, ciò è avvenuto soprattutto nelle PMI i cui dirigenti si ritengono (piuttosto) informati in merito alla tematica dei cyber rischi (30 %).

Tra le misure principali rientrano l'installazione di software aggiuntivi acquistati (25 %), l'utilizzo di firewall (22 %), l'utilizzo di password sicure (21 %) e gli aggiornamenti regolari del software (15 %).

Tra i provvedimenti sono inoltre contemplati anche la nomina di responsabili della protezione dei dati nelle imprese (nel 64 % delle PMI svizzere), la definizione di processi per la divulgazione/cancellazione dei dati (28 %) e la conduzione di un inventario per il trattamento dei dati (20 %).

Domande per le PMI svizzere

- L'esposizione agli attacchi informatici è aumentata con il maggior ricorso all'home office?
- Quali misure di cyber sicurezza dovreste implementare tassativamente o immediatamente in preparazione ai prossimi mesi?
- Quali altre misure dovrebbero essere pianificate per aumentare la cyber sicurezza a lungo termine?
- È stato nominato un collaboratore responsabile della protezione dei dati e sono stati introdotti i rispettivi regolamenti/processi?

Misure di cyber sicurezza in seguito all'obbligo di home office

Misure di cyber sicurezza in seguito all'obbligo di home office («Quali misure di sicurezza ha adottato durante il lockdown?» / n = 118 (filtro: se in occasione del lockdown sono state adottate misure di sicurezza supplementari contro i cyber attacchi)/domanda precodificata/semiaperta)

Applicazione pratica per le PMI svizzere

Argomenti e domande per l'implementazione in azienda

Sulla base del presente studio, degli argomenti e delle sfide individuati nelle PMI, gli autori hanno compilato questa lista di controllo come stimolo per la discussione e la progettazione.

Vi auguriamo buon lavoro con l'implementazione di questi importanti temi.

Strategia del mondo del lavoro e attuazione dell'home office

- ☐ Come utilizzate strategicamente l'home office per aumentare la flessibilità e l'attrattiva per i collaboratori e ridurre la struttura dei costi?
- ☐ Avete già discusso del tema home office con i vostri collaboratori e avete individuato idee/potenziali sviluppi nonché realizzato una tabella di marcia?
- ☐ A lungo termine l'home office si affermerà nella vostra azienda? Ne avete individuato e discusso il potenziale?
- ☐ È disponibile un accordo di home office, ad es. per regolamentare l'assunzione dei costi dell'equipaggiamento privato per l'ufficio?
- ☐ Avete identificato e definito i requisiti per il «new work» (mondo del lavoro 4.0) in relazione ai temi della cultura, della conduzione e della comunicazione?
- ☐ Avete sviluppato una strategia accompagnata da una tabella di marcia per il mondo del lavoro 4.0?
- ☐ Quali esperienze positive e negative avete raccolto con l'home office durante il lockdown? Cosa vi ha consentito di imparare e migliorare?
- ☐ Perché non utilizzate maggiormente e in modo strategico l'home office per rinnovare la vostra azienda, ad es. per rafforzare la vostra reputazione come datore di lavoro?
- ☐ È stata elaborata una strategia per l'utilizzo dei tool di comunicazione (e sono state in seguito implementate le piattaforme più opportune)?
- ☐ Esistono un piano di sicurezza dei dati e le relative direttive per l'uso professionale di queste piattaforme di comunicazione?
- ☐ Le piattaforme sono sicure? Quali informazioni/dati vengono risp. possono essere scambiati e attraverso quali piattaforme?

Strategie e misure per la cyber sicurezza

Acquisizione di conoscenze e sensibilizzazione

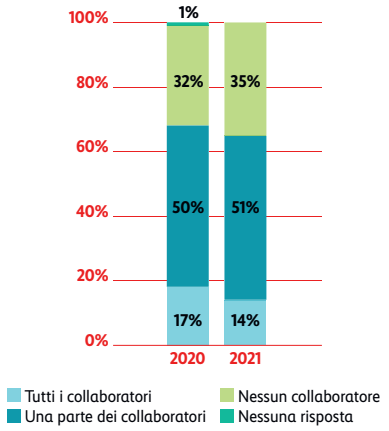
- ☐ Individuate regolarmente il potenziale di utilizzo delle nuove tecnologie e disponete di una strategia/una tabella di marcia per l'introduzione di nuove infrastrutture informatiche?
- ☐ Quali nuovi prodotti e servizi potreste lanciare con (maggior) successo sul mercato investendo nell'infrastruttura informatica e nella cyber sicurezza?
- ☐ Siete in grado di soddisfare le vostre esigenze (o quelle del mercato) in materia di cyber sicurezza?
- ☐ Come vi informate regolarmente su pericoli, programmi e soluzioni per aumentare la cyber sicurezza?
- ☐ I collaboratori conoscono le varie tecniche di attacco? Come vengono sensibilizzati e formati i vostri dipendenti?
- ☐ Quali misure tecniche e organizzative adottate per aumentare la cyber sicurezza nella vostra azienda?
- ☐ Come verificate regolarmente le vostre strategie e misure per la cyber sicurezza?

Strategie e misure

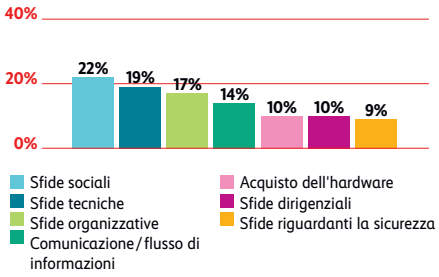
- ☐ Quale infrastruttura informatica è fondamentale per la fornitura di servizi nella vostra azienda risp. quanto è importante per voi la cyber sicurezza?
- ☐ Quali prestazioni non potete fornire se l'infrastruttura informatica non funziona?
- ☐ Come proteggete questa infrastruttura informatica?
- ☐ Quali alternative (cosiddette strategie di recovery) avete preparato?
- ☐ Di quali strategie/piani d'emergenza disponete e quali componenti mancano?
- ☐ Avete fatto un inventario della vostra infrastruttura informatica? Esiste un elenco dell'hardware e del software (con numeri di serie, data di acquisto/prezzo, versioni software ecc.)?
- ☐ Quale infrastruttura informatica viene aggiornata da chi e con quale frequenza?
- ☐ Come proteggete la vostra infrastruttura informatica per garantire la continuità dell'attività in caso di attacchi e altri problemi?
- ☐ Quali misure organizzative concrete dovrebbero essere pianificate e attuate?
- ☐ Sarebbe eventualmente utile effettuare un audit sulla sicurezza informatica e stipulare una cyber assicurazione?
- ☐ L'esposizione agli attacchi informatici è aumentata con il maggior ricorso all'home office?
- ☐ Quali misure di cyber sicurezza dovreste implementare tassativamente o immediatamente in preparazione ai prossimi mesi?
- ☐ Quali altre misure dovrebbero essere pianificate per aumentare la cyber sicurezza a lungo termine?
- ☐ È stato nominato un collaboratore responsabile della protezione dei dati e sono stati introdotti i rispettivi regolamenti/processi?

Infografica
«Home office e cyber sicurezza nelle PMI svizzere (2021)»

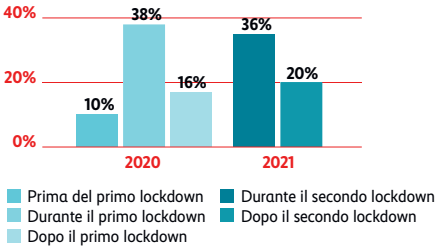
Numero di collaboratori che potenzialmente potrebbero lavorare in homeoffice



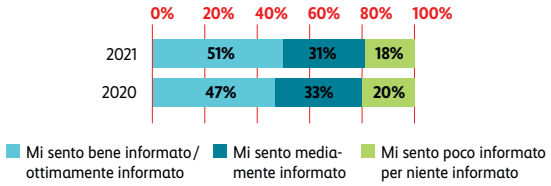
Le sette maggiori sfide nell'attuazione dell'homeoffice



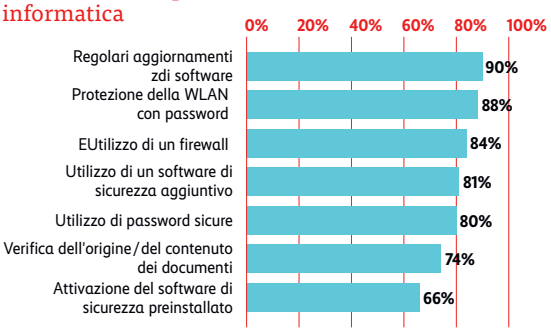
Cambiamento delle abitudini rispetto all'homeoffice durante il lockdown dovuto al coronavirus



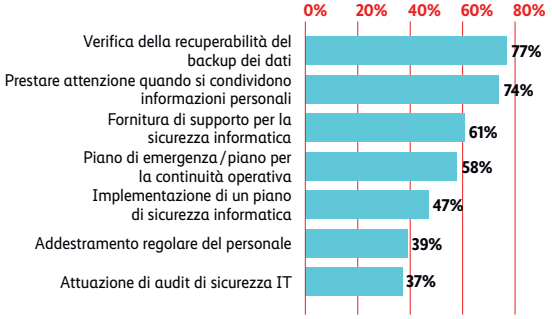
Livello d'informazione personale



Misure tecniche per aumentare la sicurezza informatica



Misure organizzative per aumentare la sicurezza informatica



Contatto/Autori

Marc K. Peter
Responsabile del centro di competenza Trasformazione digitale
FHNW Hochschule
für Wirtschaft, Olten
marc.peter@fhnw.ch

Andreas Hölzli
Responsabile del centro
di competenza Cyber Risk
la Mobiliare, Berna
andreas.hoelzli@mobi.ch

Andreas W. Kaelin
Amministratore delegato
supplente e responsabile
del dossier Cybersecurity
digitalswitzerland, Berna
andreas@digitalswitzerland.com

Karin Mändli Lerch
Responsabile di progetto
gfs-zürich, Zurigo
karin.maendlilerch@gfs-zh.ch

Patric Vifian
Marketing Manager PMI
la Mobiliare, Berna
patric.vifian@mobi.ch

Nicole Wettstein
Responsabile del programma
Cybersecurity
Schweizerische Akademie
der Technischen
Wissenschaften SATW, Zurigo
nicole.wettstein@satw.ch

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

Home office e cyber sicurezza nelle PMI svizzere: strategie e misure adottate dalle PMI svizzere con 4–49 collaboratori nel contesto del coronavirus (COVID-19)

— la Mobiliare
— digitalswitzerland
— FHNW Hochschule für Wirtschaft
— SATW
— gfs-zürich

www.cyberstudie.ch
Berna, novembre 2021