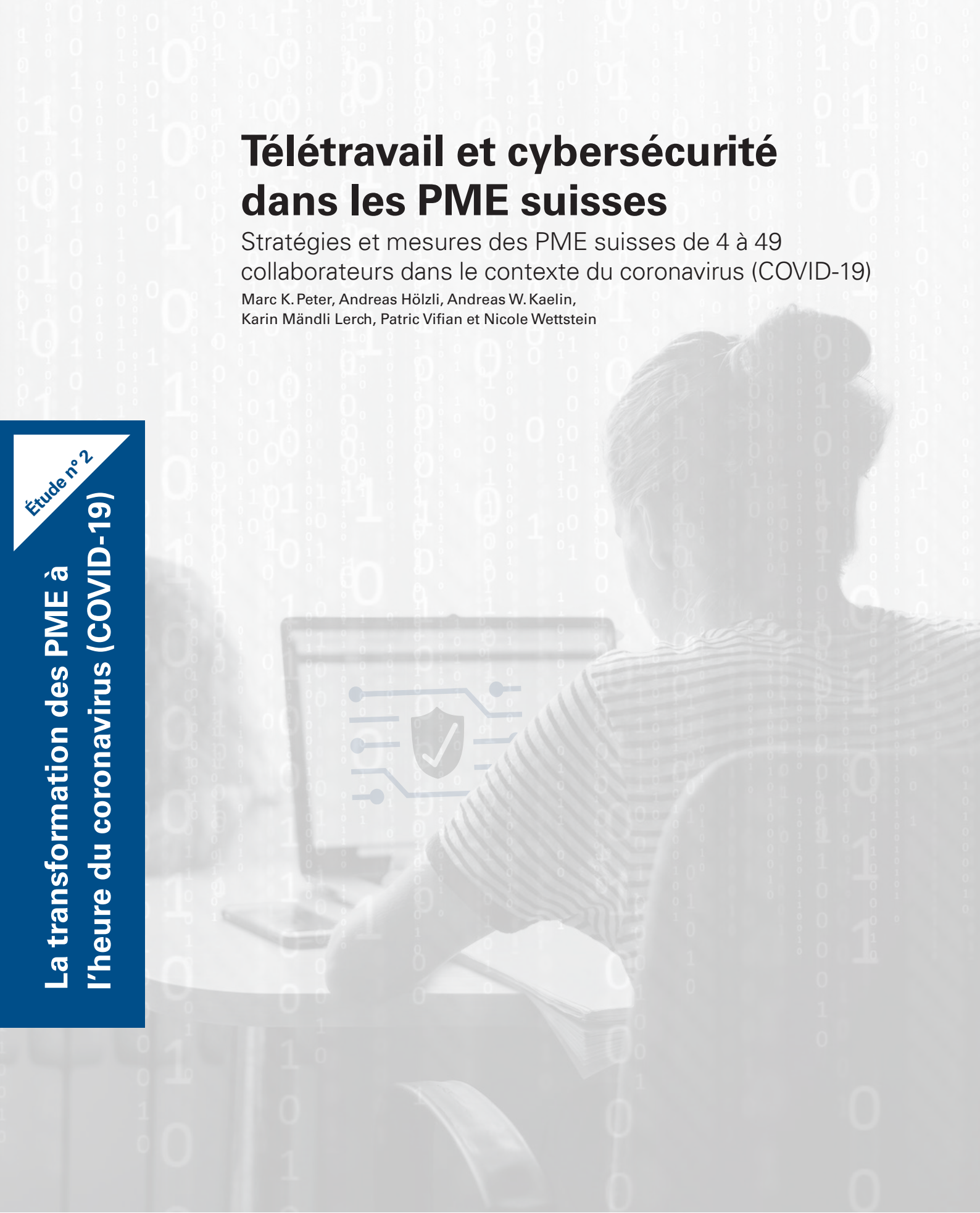
Télétravail et cybersécurité dans les PME suisses

Stratégies et mesures des PME suisses de 4 à 49 collaborateurs dans le contexte du coronavirus (COVID-19)

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

Étude n° 2

La transformation des PME à l'heure du coronavirus (COVID-19)



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

Impressum

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

Télétravail et cybersécurité dans les PME suisses :
Stratégies et mesures des PME suisses de 4 à 49 collaborateurs dans le contexte du coronavirus (COVID-19)

La Mobilière, digitalswitzerland, FHNW Hochschule für Wirtschaft, SATW, gfs-zürich

Berne, novembre 2021

Coordination : prof. Marc K. Peter, FHNW Hochschule für Wirtschaft (www.fhnw.ch/wirtschaft)

Conception : Polarstern SA, Soleure et Lucerne (www.polarstern.ch)
Traductions française et italienne : La Mobilière

Les diapositives et le rapport final détaillé peuvent être téléchargés depuis les sites Internet des partenaires de l'étude.

Méthode de l'enquête

Panel : PME de 4 à 49 collaborateurs situées en Suisse alémanique, en Suisse romande et au Tessin (soit env. 153 000 PME selon l'OFS, Statistique structurelle des entreprises, STATENT 2017, version du 22.08.2019).

Échantillon : 506 dirigeants de PME suisses
Représentativité : l'intervalle de confiance de l'échantillon total est de 95 %, avec une marge d'erreur de +/- 4 % pour 50/50.
Les données collectées étant représentatives des PME suisses, les résultats sont également valables pour le panel.

Méthode : enquête téléphonique assistée par ordinateur (CATI)

Méthode d'échantillonnage : quotas aléatoires (sélection de PME au hasard, préclassement par région, puis répartition des quotas selon la taille de l'entreprise)

Pondération : aucune

Période de l'enquête : du 16 juin au 27 juillet 2021

Sommaire

Introduction et aperçu

La présente publication est née de l'initiative d'un groupe de projet composé de collaborateurs de digitalswitzerland, de la Hochschule für Wirtschaft rattachée à la Fachhochschule Nordwestschweiz FHNW, de l'Académie suisse des sciences techniques (SATW), de gfs-zürich et de la Mobilière. Sur la base d'un relevé de la situation effective, les auteurs entendent contribuer à une meilleure compréhension et à un renforcement des PME suisses de 4 à 49 collaborateurs dans le contexte du coronavirus (COVID-19).

Les deux études représentatives menées donnent un aperçu de la situation en matière de télétravail et de cybersécurité dans les PME en lien avec la crise sanitaire vécue depuis le début de l'année 2020. La première enquête a été réalisée entre les deux premières vagues de l'épidémie, plus précisément entre le moment où le Conseil fédéral a levé la recommandation initiale de privilégier le télétravail (22 juin 2020) et celui où l'appel au télétravail a été lancé pour la deuxième fois, le 19 octobre 2020 (le télétravail est devenu obligatoire pour toutes les entreprises à partir du 18 janvier 2021). Cette deuxième étude a été réalisée après la levée de l'obligation de télétravail pour les entreprises effectuant des tests réguliers (à partir du 31 mai 2021). Elle a débuté peu avant que le télétravail ne soit recommandé pour toutes les entreprises à compter du 26 juin 2021. La deuxième étude a été menée auprès de 506 dirigeants de PME, du 16 juin au 27 juillet 2021.

Avant le premier confinement instauré en mars 2020, 10 % des collaborateurs employés par une PME dans laquelle au moins un collaborateur/une collaboratrice pouvait recourir au télétravail étaient passés à cette forme de travail. Cette valeur a pratiquement quadruplé pendant le premier confinement pour atteindre 38 %, avant de se replier à 16 % (ce qui correspond à une hausse de 60 % par rapport à la situation prévalant avant le confinement). Durant le deuxième confinement, cette valeur a presque triplé (elle est passée de 16 % après le confinement à 36 % pendant l'obligation de télétravail) et s'est désormais stabilisée à un niveau élevé (env. 20 %), tous secteurs confondus. Une comparaison des deux vagues montre que la part de collaborateurs qui travaillent depuis chez eux a doublé dans les PME suisses depuis le début de la crise sanitaire.

Comme ce fut le cas lors de la première étude, 19 % des PME de 4 à 49 collaborateurs se considèrent dans la deuxième étude comme des pionniers, 41 % comme des Early Followers (2020 : 44 %) et 37 % comme des Late Followers (2020 : 33 %) concernant l'utilisation des nouvelles technologies. Les pionniers n'hésitent pas à faire office de précurseurs en investissant dans les nouvelles technologies et dans l'innovation produit et marketing, ce qui leur confère un avantage concurrentiel. Ils sont suivis de près par les Early Followers pour ce qui est des innovations, tandis que les Late Followers ne se tournent vers ces dernières qu'au bout d'un certain temps, une fois la phase probatoire passée. En matière de télétravail, les pionniers se distinguent plus particulièrement : dans ces PME, 85 % de tous les collaborateurs ou de certains d'entre eux pourraient théoriquement faire du télétravail (et 91 % des collaborateurs sont déjà équipés à cette fin en tout ou en partie à leur domicile). Les Early Followers et les Late Followers disposent eux aussi d'un important potentiel en matière de télétravail; et ce, toutes PME confondues, étant donné que dans deux tiers environ de toutes les PME suisses, tous les collaborateurs ou une partie d'entre eux pourraient théoriquement télétravailler (et que deux tiers des PME ont déjà équipé tout ou partie de leurs collaborateurs à cet effet).

Les facteurs sociaux/émotionnels (p. ex. la cohésion des équipes), techniques (p. ex. l'accès externe à des données) et organisationnels (p. ex. le poste de travail) constituent les principaux défis dans la mise en œuvre du télétravail. Celle-ci s'effectue notamment avec de nouveaux outils de communication (outils de conférence en ligne ainsi que conseils et formations en ligne, en particulier). Plus la taille de la PME est importante, plus les tâches informatiques confiées à des prestataires externes sont nombreuses. En moyenne, 30 % des PME font appel à des prestataires informatiques externes pour mettre en place leur infrastructure informatique.

Sur fond de COVID-19 et de progression du télétravail, le nombre d'attaques a aussi augmenté dans le cyberespace. Les dirigeants de PME suisses estiment donc que la cybercriminalité est un problème à prendre au sérieux (noté 4,6 sur une échelle de 5) et que les mesures contre les cyberattaques sont importantes (4,4).

L'étude révèle qu'un cinquième des patrons de PME s'estiment n'être pas ou pas du tout informés sur le thème de la cybersécurité. Tout comme en 2020, 65 % des dirigeants considèrent cette thématique comme importante ou très importante. Cela s'explique aussi par le fait qu'en 2021, 36 % des PME avaient déjà été victimes d'une cyberattaque ayant occasionné des frais considérables pour la réparation du dommage (2020 : 25 %). Ces attaques se traduisent par un dommage financier, une perte de données clients et un dommage de réputation.

Comme l'avait déjà révélé l'étude réalisée en 2020, les PME suisses se situent à un stade relativement avancé dans la mise en œuvre de mesures techniques visant à augmenter la cybersécurité. Une importante marge de progression subsiste toutefois au niveau de la planification et de la mise en œuvre sur un plan organisationnel des mesures de sécurité informatiques. À peine la moitié des PME suisses disposent en effet d'un concept de sécurité informatique et seuls deux cinquièmes forment régulièrement leurs collaborateurs ou mènent des audits de sécurité informatique. Pendant l'obligation de télétravail, un quart des PME ont donc investi dans des mesures de protection supplémentaires telles que des logiciels de sécurité, des pare-feux et des mots de passe plus forts. Les résultats de l'étude indiquent également que, dans de nombreux cas, les PME ont réglé la question de la responsabilité de la protection des données (deux tiers des PME) et défini des processus de gestion des données.

Le rapport d'étude complet, accompagné de l'ensemble des données et des tableaux, peut être téléchargé gratuitement au format PDF depuis les sites web des partenaires de recherche :

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

En règle générale, les dirigeants de PME sensibilisés au thème de la cybersécurité ont mis en œuvre davantage de mesures pour protéger leur infrastructure informatique et leurs données clients que ceux qui ne l'étaient pas. Les thèmes de la numérisation, du télétravail, de l'utilisation des technologies de communication et de la cybersécurité ont continué de gagner en importance dans un contexte de crise sanitaire. Dans le même temps, ces thèmes feront avancer les discussions sur la société, l'économie, la technologie et les transports.

Nous espérons que ce rapport et les résultats d'étude détaillés qui l'accompagnent (voir encadré) vous aideront à faire le point sur votre situation personnelle, à mieux comprendre votre entreprise et à la doter des outils nécessaires pour renforcer sa solidité.

Berne, novembre 2021

Andreas Hölzli
Responsable du centre de compétences Cyberrisques
La Mobilière, Berne

Andreas W. Kaelin
Directeur adjoint et responsable du dossier Cybersécurité
digitalswitzerland, Berne

Karin Mändli Lerch
Responsable de projet
gfs-zürich, Zurich

Marc K. Peter
Responsable du centre de compétences
Transformation numérique
FHNW Hochschule für Wirtschaft, Olten

Patric Vifian
Marketing Manager PME
La Mobilière, Berne

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
Académie suisse des sciences techniques SATW, Zurich

Importance et utilisation du télétravail

Il existe un important potentiel en matière de télétravail – et un tiers des collaborateurs sont déjà entièrement équipés pour télétravailler

Tous les collaborateurs ou du moins une partie d'entre eux pourraient théoriquement faire du télétravail dans environ deux tiers (65 %) des PME suisses (2020 : 67 %). Ces personnes ne doivent donc pas par exemple servir des clients sur place, conduire un véhicule ou travailler sur un chantier (14 % de tous les collaborateurs; 51 % d'une partie d'entre eux). Cette part élevée témoigne du potentiel offert en matière de télétravail et de ses retombées sociales, économiques et technologiques ainsi que sur le plan des transports.

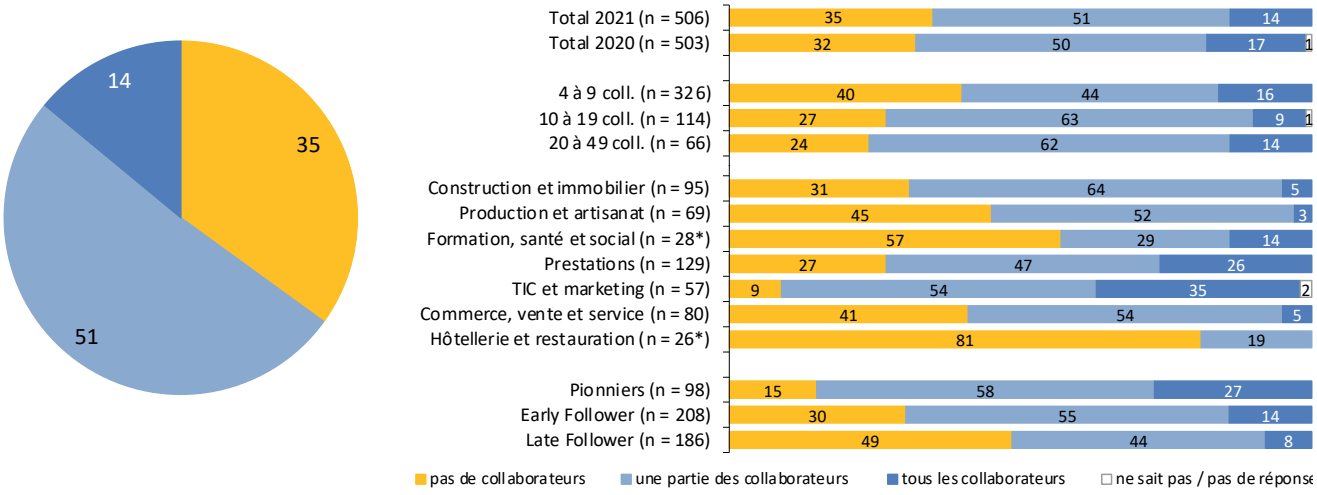
Aujourd'hui déjà, 29 % des collaborateurs de PME (2020 : 20 %) sont entièrement ou partiellement (39 %; 2020 : 46 %) équipés d'outils leur permettant de travailler depuis la maison, indépendamment du fait que ce soit du matériel appartenant à l'entreprise ou du matériel privé. La part des collaborateurs équipés entièrement ou partiellement pour le télétravail correspond à celle de 2020; le nombre de collaborateurs entièrement équipés pour le télétravail est toutefois en nette hausse.

Les pionniers méritent d'être mentionnés : dans ces PME, 85 % de tous les collaborateurs ou de certains d'entre eux pourraient théoriquement faire du télétravail; et 91 % des collaborateurs sont entièrement ou partiellement équipés pour travailler depuis leur domicile.

Questions posées aux PME suisses :

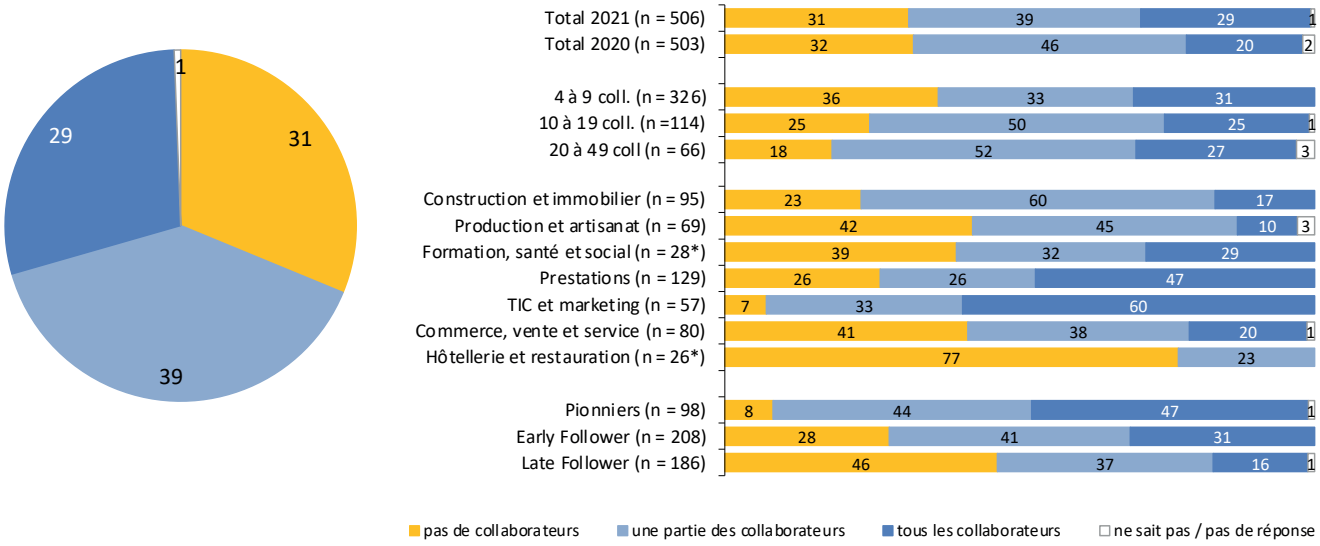
- Dans quelle mesure le télétravail vous permet-il d'accroître la flexibilité de vos collaborateurs, de renforcer l'attrait de votre entreprise aux yeux du personnel et de réduire votre structure des coûts?
- Avez-vous déjà discuté du télétravail avec vos collaborateurs et, sur cette base, développé des idées, identifié des potentiels et élaboré une feuille de route?
- Existe-t-il une convention de télétravail, p. ex. pour la prise en charge des frais liés à l'équipement de bureau privé?

Nombre de collaborateurs pouvant théoriquement faire du télétravail



Nombre de collaborateurs pouvant théoriquement faire du télétravail («Combien de vos collaborateurs pourraient théoriquement travailler depuis la maison, p. ex. ne doivent pas servir des clients sur place, pas conduire un véhicule ou pas travailler sur un chantier?»)./n 2021 = 506, n 2020 = 503/les catégories avec un volume d'échantillonnage < 30 sont marqués d'un *)

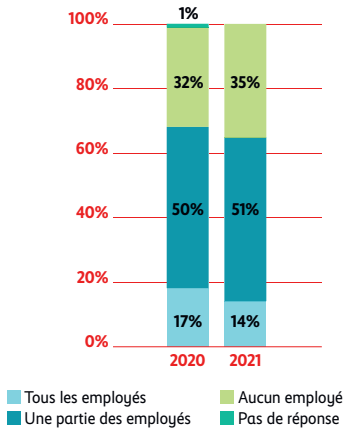
Nombre de collaborateurs équipés pour le télétravail



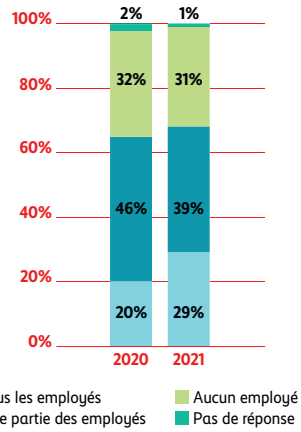
Nombre de collaborateurs équipés pour le télétravail («Combien de vos collaborateurs sont entièrement équipés d'outils leur permettant de travailler depuis la maison, indépendamment du fait que ce soit du matériel appartenant à l'entreprise ou du matériel privé?»/n 2021 = 506, n 2020 = 503/les catégories avec un volume d'échantillonnage < 30 sont marqués d'un *)

Infographie

Nombre d'employés qui pourraient potentiellement travailler à domicile



Nombre d'employés équipés pour travailler à domicile



Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

De vocation internationale avec un enseignement axé sur la pratique, la Hochschule für Wirtschaft FHNW (haute école d'économie de la Fachhochschule Nordwestschweiz) forme 3000 étudiantes et étudiants de Bachelor et de Master sur ses sites de Bâle, Brugg-Windisch et Olten. Son vaste programme de spécialisation en économie en fait l'un des leaders des hautes écoles spécialisées de Suisse.

Le professeur Marc K. Peter dirige le centre de compétences Transformation numérique à la Hochschule für Wirtschaft FHNW. Ce centre propose des prestations de recherche, de conseil et de formation en lien avec la transformation numérique, dans le but d'aider les organisations ainsi que les collaboratrices et les collaborateurs à développer et à mettre en place des stratégies de croissance numérique.

Outils clés pour la transformation numérique des PME (en allemand) :

Canevas d'atelier Transformation numérique
Grâce à cet outil gratuit, vous et vos collaborateurs pouvez identifier des idées et des potentiels pour la transformation de votre entreprise.
www.digital-transformation-canvas.net

Canevas d'atelier Développement stratégique à l'ère du numérique
Avec ce canevas d'atelier, vous et vos collaborateurs disposez d'un outil gratuit pour développer ensemble une stratégie axée sur la transformation numérique de votre entreprise.
www.act-strategy-canvas.ch

Canevas d'atelier Environnement de travail 4.0
Gratuit, cet outil vous permet d'identifier avec vos collaborateurs des idées et des potentiels pour votre stratégie liée à l'environnement de travail.
www.arbeitswelt-zukunft.ch/workshop-canvas

Évaluation de la maturité numérique
Cet outil d'analyse gratuit permet d'évaluer votre propre maturité et celle de votre entreprise sur les points suivants: quel est votre stade d'avancement en matière de numérisation? Avez-vous lancé ou déjà réalisé des projets dans tous les champs d'action? À quel niveau avez-vous identifié un potentiel (majeur)?
www.digitale-reife.net

Détermination des thèmes stratégiques
Le «Strategy Check» en ligne, gratuit, vous permet de définir les thèmes et les questions à discuter dans le cadre du développement stratégique à l'ère du numérique.
www.digital-strategy-check.ch

Guide pratique Développement stratégique à l'ère du numérique
Résultats de recherche, conseils pratiques, études de cas, modèles de stratégie et listes de contrôle pour la planification et la mise en œuvre de la transformation numérique:
www.strategische-transformation.ch

Guide pratique Transformation numérique pour les PME
Résultats de recherche, conseils pratiques, études de cas et listes de contrôle pour la transformation de votre PME:
www.kmu-transformation.ch

Guide pratique Environnement de travail 4.0
Résultats de recherche, conseils pratiques, études de cas et listes de contrôle pour votre nouvel environnement de travail:
www.arbeitswelt-zukunft.ch

Plus d'informations :
FHNW Hochschule für Wirtschaft
Institute for Competitiveness & Communication
Prof. Marc K. Peter
Centre de compétences Transformation numérique
Riggenbachstrasse 16
4600 Olten

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

Évolution des habitudes en matière de télétravail pendant et après le confinement

Multiplication par deux du télétravail dans les PME suisses sur deux ans

Avant le premier confinement en 2020, 10 % des collaborateurs employés par une PME qui proposait au moins un poste en télétravail avaient adopté ce mode de travail. Cette valeur a pratiquement quadruplé durant le premier confinement pour s'établir à 38 %, avant de reculer à 16 % (progression de 60 %).

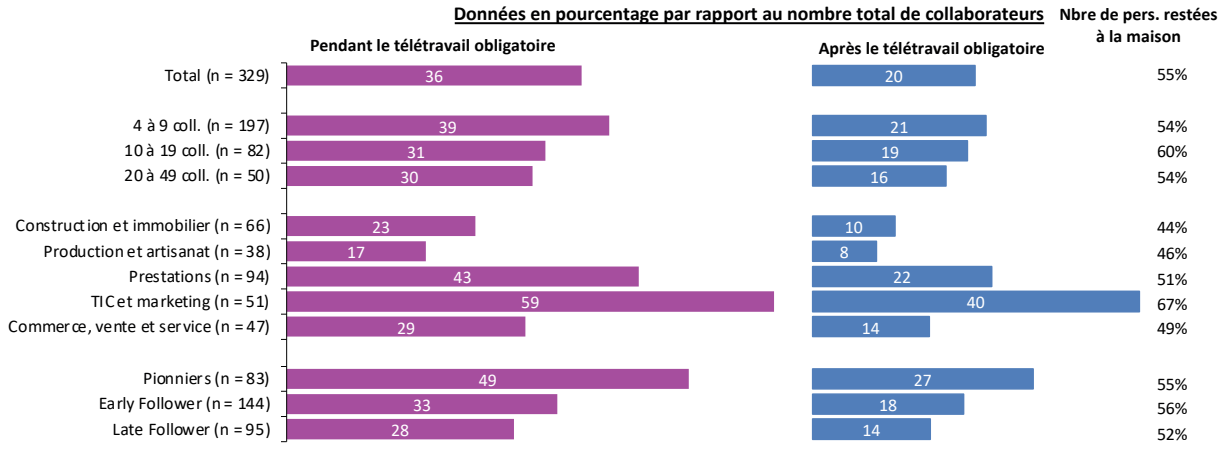
Durant le deuxième confinement, cette valeur a de nouveau presque triplé, passant de 16 % après le confinement à 36 % pendant l'obligation de télétravail. Depuis, elle s'est stabilisée à un niveau élevé de quelque 20 %, tous secteurs confondus. Ce taux atteint 27 % chez les pionniers et 14 % seulement chez les Late Followers.

La comparaison des deux vagues montre que la part des collaborateurs travaillant depuis chez eux a doublé dans les PME suisses depuis le début de la pandémie de coronavirus. Il se peut que cette valeur diminue légèrement à moyen terme, car si 15 % des PME s'attendent à une augmentation, 38 % tablent sur une réduction. Fait intéressant, ce taux est relativement élevé chez les pionniers (45 % anticipent une baisse). D'une manière générale, le nombre de dirigeants qui ne se réjouissent pas de voir leurs collaborateurs faire davantage de télétravail à l'avenir a augmenté par rapport à 2020. En 2020, 8 % des dirigeants jugeaient défavorablement cette évolution (valeurs 1 et 2 sur une échelle de 5); en 2021, ils étaient 15 %.

Questions posées aux PME suisses :

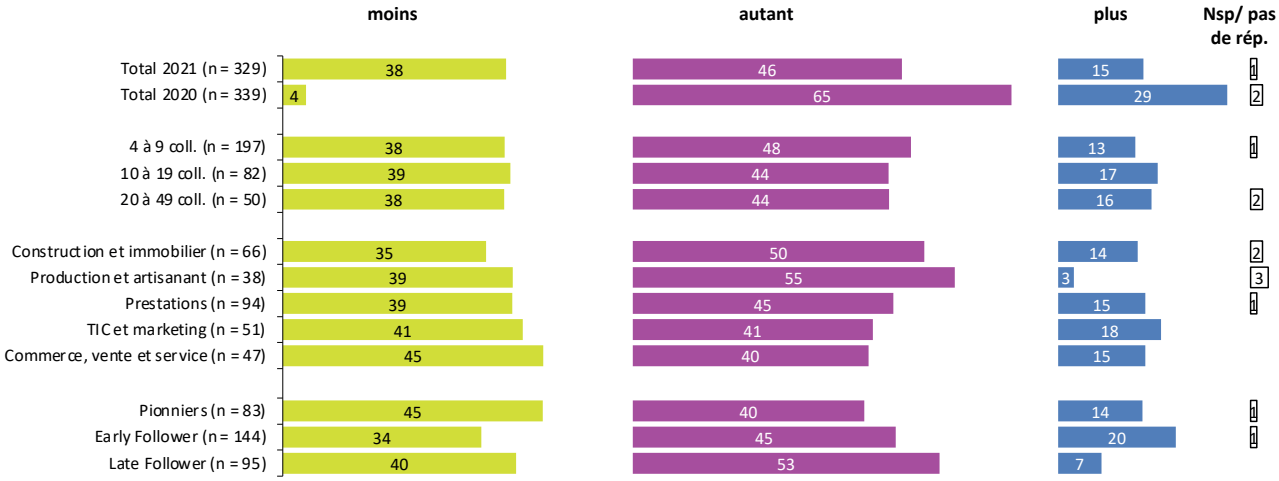
- Le télétravail est-il appelé à s'établir durablement dans votre entreprise? Avez-vous identifié des potentiels et en avez-vous discuté?
- Avez-vous identifié et défini les exigences posées par le «New Work» (environnement de travail 4.0) en matière de culture, de conduite et de communication?
- Avez-vous élaboré une stratégie et une feuille de route correspondante pour votre environnement de travail 4.0?

Évolution des habitudes en matière de télétravail pendant le confinement/l'obligation de télétravail



Évolution des habitudes en matière de télétravail pendant le confinement/l'obligation de télétravail («Parmi vos collaborateurs, combien ont travaillé principalement depuis la maison depuis début 2021, soit pendant la phase de télétravail obligatoire?», «Et maintenant, depuis que l'obligation est levée, combien travaillent-ils encore depuis la maison?»/n = 329 (Filtre : dans le cas où au moins un collaborateur peut théoriquement faire du télétravail)

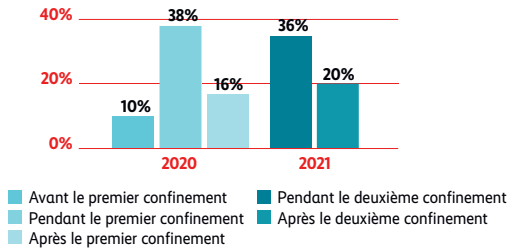
Estimation relative à l'évolution des postes en télétravail



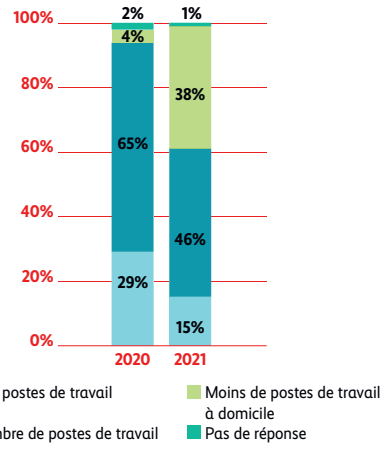
Estimation relative à l'évolution des postes en télétravail («Comment évaluez-vous le développement sur le long terme : Y aura-t-il à l'avenir plus, autant ou moins de collaborateurs qui travailleront depuis la maison qu'avant le confinement?»/n 2021 = 329, n 2020 = 339 (Filtre : dans le cas où au moins un collaborateur peut théoriquement faire du télétravail)

Infographie

Changement dans les habitudes de télétravail pendant le confinement COVID



Évaluation de l'évolution des postes de travail à domicile



Défis dans la mise en œuvre du télétravail

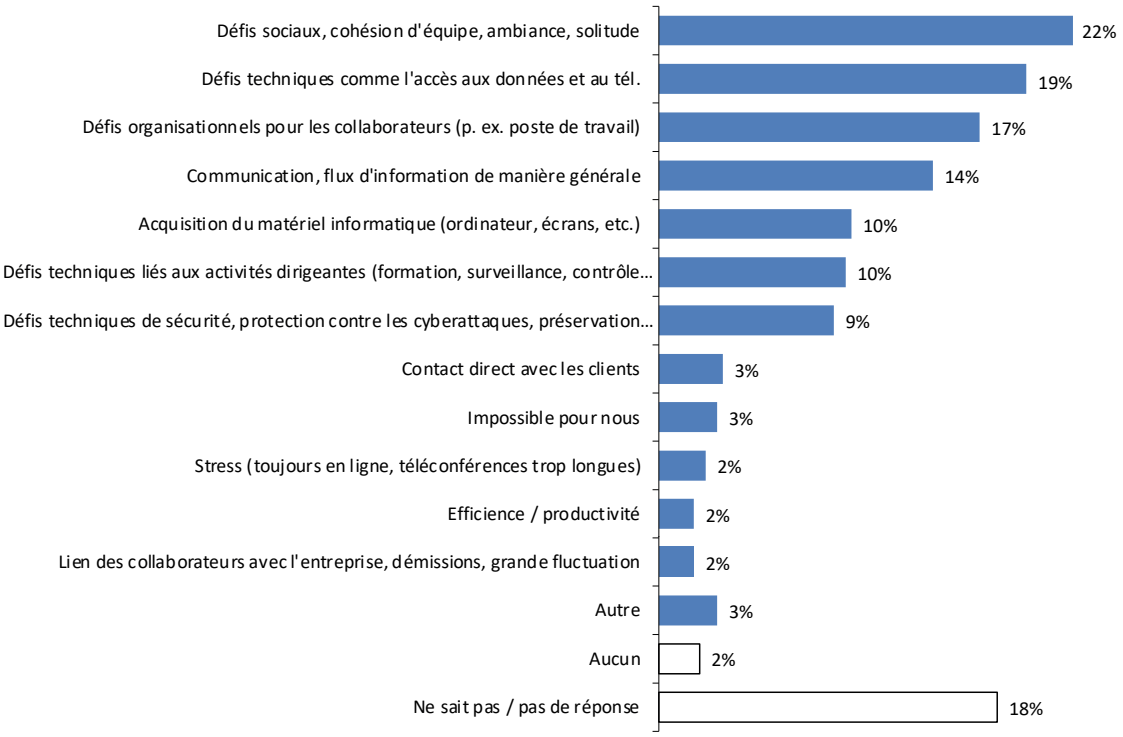
La collaboration, le management et l'organisation, facteurs de succès importants

Pour près d'un cinquième des PME, le facteur social/émotionnel (défis d'ordre social, cohésion des équipes, ambiance, isolement), le facteur technique (défis techniques tels que l'accès aux données et le recours au téléphone) ainsi que le facteur organisationnel (problèmes d'organisation du côté du personnel, p. ex. poste de travail) constituent les principaux défis dans la mise en œuvre du télétravail. Cela englobe aussi bien des défis de management que des problèmes techniques liés à la sécurité pour environ un dixième des PME suisses.

C'est ce que confirme une étude menée en 2019 par la Hochschule für Wirtschaft FHNW qui décrivait les paramètres People (collaborateurs), Place (environnement de travail) et Technology (technologie) comme étant des facteurs de succès dans l'aménagement de l'environnement de travail 4.0 (cf. encadré avec conseil de lecture).

Questions posées aux PME suisses :

- Quelles expériences positives et/ou négatives avez-vous tirées du télétravail pendant les confinements? Quels enseignements en sont ressortis et quelles améliorations pouvez-vous apporter?
- Pourquoi n'avez-vous pas davantage recours au télétravail et ne l'utilisez-vous pas dans une stratégie de renouvellement de votre entreprise (p. ex. afin d'accroître votre réputation en tant qu'employeur)?



Défis dans la mise en œuvre du télétravail («Du point de vue de l'entreprise, quels sont les principaux défis dans la mise en œuvre du télétravail?»/n = 329, plusieurs réponses possibles (Filtre : dans le cas où au moins un collaborateur peut théoriquement faire du télétravail)

Utilisation des outils de communication

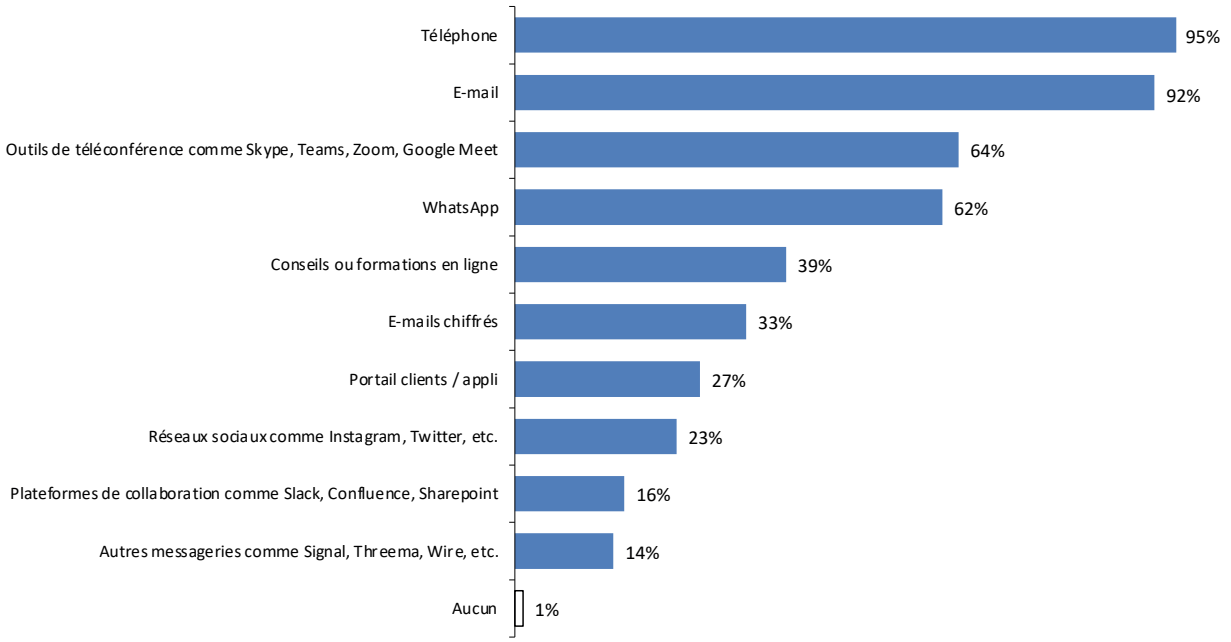
Les outils de conférence en ligne et les conseils/les formations en ligne comme nouvelles plateformes importantes

Le téléphone et les e-mails restent les principaux outils de communication. Dans la deuxième étude réalisée en 2021, une question portait pour la première fois sur le nombre d'e-mails cryptés : un tiers des PME suisses utilisent déjà cette forme de communication. Cette proportion est élevée si l'on tient compte des préparatifs et de la charge de travail supplémentaires que cela implique sur les plans technique et organisationnel. L'utilisation des outils de conférence en ligne (2020 : 46 %, 2021 : 64 %) ainsi que le recours aux conseils et aux formations en ligne (2020 : 20 %, 2021 : 39 %) ont fortement augmenté.

Questions posées aux PME suisses :

- Un concept a-t-il été mis au point pour l'utilisation des outils de communication (et les plateformes les plus appropriées ont-elles par la suite été implémentées)?
- Avez-vous élaboré un concept et des directives sur la sécurité des données dans le cadre de l'utilisation des plateformes de communication à des fins professionnelles?
- Ces plateformes sont-elles sécurisées? Quelles sont les données/informations qui sont ou peuvent y être échangées, et quelle est la nature de ces plateformes?

Utilisation des outils de communication



Utilisation des outils de communication («Je vais vous lire une liste de quelques moyens de communication numériques. Parmi ceux-ci, lesquels sont-ils actuellement utilisés par vos collaborateurs pour communiquer avec des partenaires, clients et d'autres membres du personnel?»/n = 506, plusieurs réponses possibles)

Degré personnel d'information concernant la thématique des cyberrisques

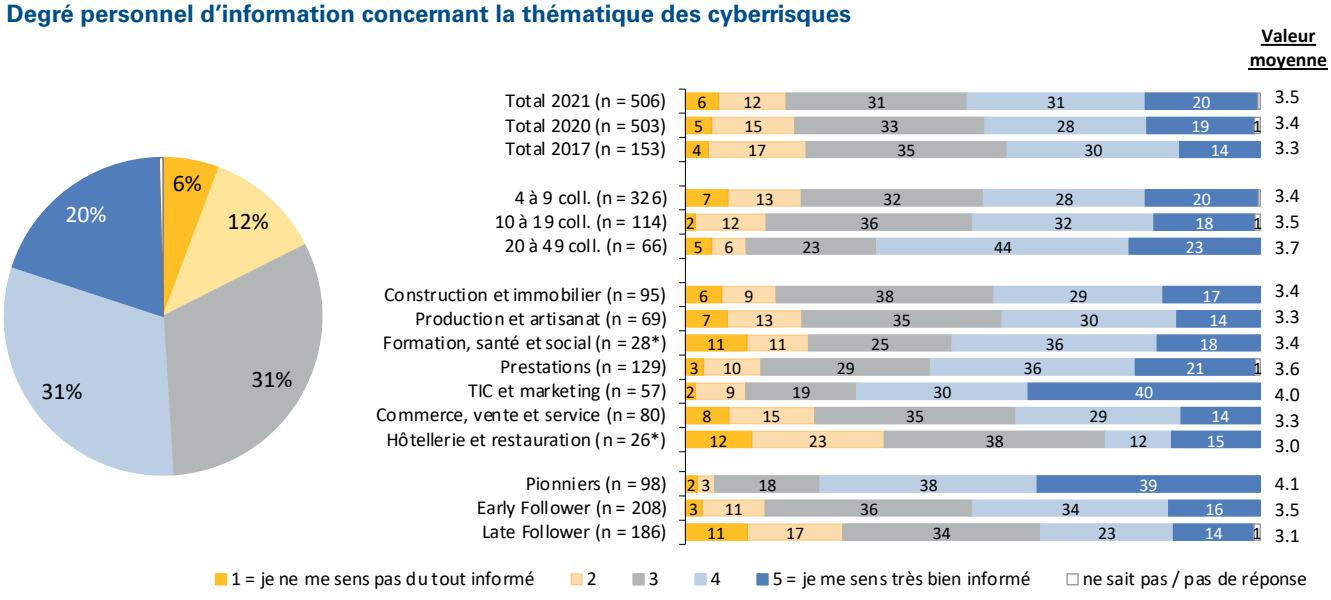
Un cinquième des dirigeants de PME estiment n'être pas/pas du tout informés

Les dirigeants de PME suisses se considèrent un peu mieux informés qu'il y a un an. Mais la valeur reste faible : seuls 51 % s'estiment bien ou très bien informés (2020 : 47 %). Plus la PME est grande, plus les dirigeants sont bien informés sur cette thématique. Les pionniers en particulier s'estiment bien ou très bien informés (77 %). La cybersécurité demeure un thème important : tout comme en 2020, 65 % des dirigeants de PME suisses considèrent la cybersécurité comme importante ou très importante.

Questions posées aux PME suisses :

- Procédez-vous à l'identification régulière du potentiel lié à l'utilisation de nouvelles technologies et avez-vous défini une stratégie/feuille de route pour la mise en place d'une nouvelle infrastructure informatique?
- Quels sont les nouveaux produits et services que vous pourriez commercialiser avec (davantage de) succès en investissant dans l'informatique et la cybersécurité?
- Répondez-vous à vos propres exigences (ou à celles du marché) en matière de cybersécurité? Comment procédez-vous pour vous informer régulièrement sur les dangers qui vous menacent ainsi que sur les concepts et solutions destinés à augmenter la cybersécurité?

Degré personnel d'information concernant la thématique des cyberrisques



Degré personnel d'information concernant la thématique des cyberrisques («Dans l'ensemble : comment estimez-vous personnellement être informé sur la problématique des menaces de la cybercriminalité?» /n 2021 = 506, n 2020 = 503/les catégories avec un volume d'échantillonnage < 30 sont marqués d'un *)

digitalswitzerland

Portrait

digitalswitzerland est une initiative nationale intersectorielle qui entend positionner la Suisse en tant que pôle d'innovation numérique de premier plan sur la scène internationale. Cet objectif mobilise sous la bannière digitalswitzerland plus de 230 organisations composées de membres d'associations et de partenaires de fondations politiquement neutres. Véritable interlocuteur pour toutes les questions touchant à la numérisation, digitalswitzerland s'engage en faveur de solutions visant à répondre aux divers enjeux.

Outils clés pour les PME :

Test rapide de cybersécurité pour PME
cybersecurity-check.ch

Nombre de PME suisses n'ont pas conscience d'être insuffisamment protégées contre les risques sérieux liés au cyberespace. C'est pour les sensibiliser à cette thématique que l'organisation ICTswitzerland a créé un groupe d'experts composé de représentants de l'économie, d'associations et de la Confédération. Le fruit de leurs travaux est le «Test rapide de cybersécurité pour PME», grâce auquel chacun peut déterminer en toute simplicité si son entreprise dispose des outils nécessaires pour faire face aux cyberrisques.

Une initiative commune lancée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE), la commission d'experts de la Confédération chargée du traitement et de la sécurité des données, ICTswitzerland, l'Unité de pilotage informatique de la Confédération (UPIC), la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), l'Information Security Society Switzerland (ISSS), l'Académie suisse des sciences techniques (SATW), l'Association suisse de normalisation (SNV), l'Association Suisse pour Systèmes de Qualité et de Management (SQS) et l'Association Suisse d'Assurances (ASA).

Des prestataires informatiques compétents pour une cybersécurité accrue
digitalsecurityswitzerland.ch

L'Alliance Sécurité Digitale Suisse a développé le label de qualité «Prestataire de services informatiques certifié» CyberSeal.
Ce label rend visible la fiabilité des prestataires de services informatiques au premier coup d'œil et soutient les PME dans le choix de leur partenaire informatique. Il distingue les prestataires de services informatiques qui garantissent à leur clientèle un niveau de protection approprié en appliquant les mesures techniques et organisationnelles nécessaires. CyberSeal renforce ainsi la sécurité numérique des PME et porte la numérisation à un niveau de qualité supérieur.

Cyberattaques réussies et dommages consécutifs

Plus d'un tiers des PME suisses ont déjà été attaquées avec succès

36 % des PME suisses ont déjà été victimes d'une cyberattaque ayant nécessité un travail considérable pour réparer les dommages (2020 : 25 %). Cela correspond à une hausse de 44 % sur un an. La technique de la fraude en ligne connaît une forte progression. Dans de nombreux cas, elle s'effectue par le biais d'une arnaque au CEO : les collaborateurs reçoivent des e-mails prétendument envoyés par le CEO de l'entreprise. Dans ces e-mails, le CEO demande, en invoquant une histoire inventée de toute pièce, qu'un versement soit effectué en faveur d'une personne/société tierce.

Techniques utilisées en 2021 pour des cyberattaques réussies contre des PME suisses
(entre parenthèses les valeurs de 2020)

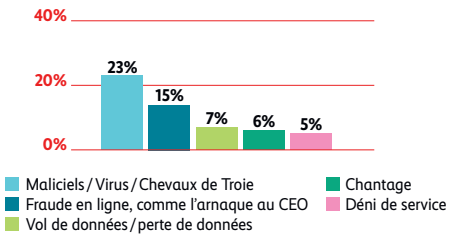
- Maliciel/virus/cheval de Troie : 23 % (18 %)
- Fraude en ligne, p. ex. arnaque au CEO : 15 % (6 %)
- Vol de données/perte de données : 7 % (5 %)
- Chantage : 6 % (4 %)
- Déni de service : 5 % (5 %)

Les cyberattaques entraînent des dommages financiers (25 % des PME ayant fait l'objet d'une cyberattaque ont subi des dommages considérables), une perte des données clients (7 %) et un dommage de réputation (6 %).

Questions posées aux PME suisses :

- Les collaborateurs connaissent-ils les divers types de cyberattaques? Comment les sensibilisez-vous à cette thématique?
- Quelles mesures techniques et organisationnelles avez-vous mises en place pour augmenter la cybersécurité dans votre entreprise?
- En quoi consiste l'examen régulier de vos concepts et mesures en matière de cybersécurité?

Infographie



Cyberattaques réussies («Votre entreprise a-t-elle déjà été une fois attaquée avec succès par l'une des techniques suivantes, ce qui a nécessité un travail considérable pour réparer les dommages?»/n = 506, part de «oui» en pourcentage)

L'Académie suisse des sciences techniques (SATW) est le principal réseau suisse d'experts dans le domaine des sciences techniques. Sur mandat de la Confédération, la SATW identifie les évolutions technologiques capitales sur le plan industriel et informe le monde politique et la société de leur importance et de leurs conséquences. En tant qu'organisation spécialisée politiquement indépendante, la SATW s'engage pour que l'ensemble des acteurs puissent évoluer dans le cyberespace en toute sécurité.

Cybersécurité: les défis pour la Suisse
À l'aide de brèves fiches d'information, les membres du comité consultatif de cybersécurité de la SATW donnent un aperçu des évolutions technologiques actuelles, pertinentes du point de vue de la cybersécurité. Cette démarche est complétée par la description d'un champ d'action à court et moyen terme pour chacune des évolutions citées.
www.satw.ch/fr/cybersecurite/cybersecurity-map

Technology Outlook
La SATW identifie en amont les évolutions technologiques qui jouent un rôle central pour l'économie. Elle informe la société et la classe politique de l'importance et des conséquences de ces technologies, notamment par la voie de la publication «Technology Outlook», qui paraît tous les deux ans.
ttps://www.satw.ch/to2021

Réseau d'autodétermination numérique
Le réseau d'autodétermination numérique s'engage pour une utilisation innovante et autodéterminée des données en Suisse. Son but est de saisir et de promouvoir pleinement le potentiel de notre économie et de notre société de données. La SATW a mis ce réseau sur pied conjointement avec la Direction du droit international public du DFAE, l'Office fédéral de la communication et Swiss Data Alliance.
https://www.satw.ch/digitale-selbstbestimmung

Promotion de la relève
À travers la promotion de la relève, la SATW entend rapprocher les jeunes des métiers technologiques. Elle s'engage en faveur d'une formation technique complète, apportant ainsi une réponse active à la pénurie de main d'œuvre qualifiée. Un accent particulier est mis sur la promotion féminine.
https://www.satw.ch/fr/promotion-de-la-releve

Plus d'informations:

SATW
Académie suisse
des sciences techniques SATW
St. Annagasse 18
8001 Zurich
www.satw.ch

Risques de cyberattaques mineures/mettant en péril l'existence de l'entreprise

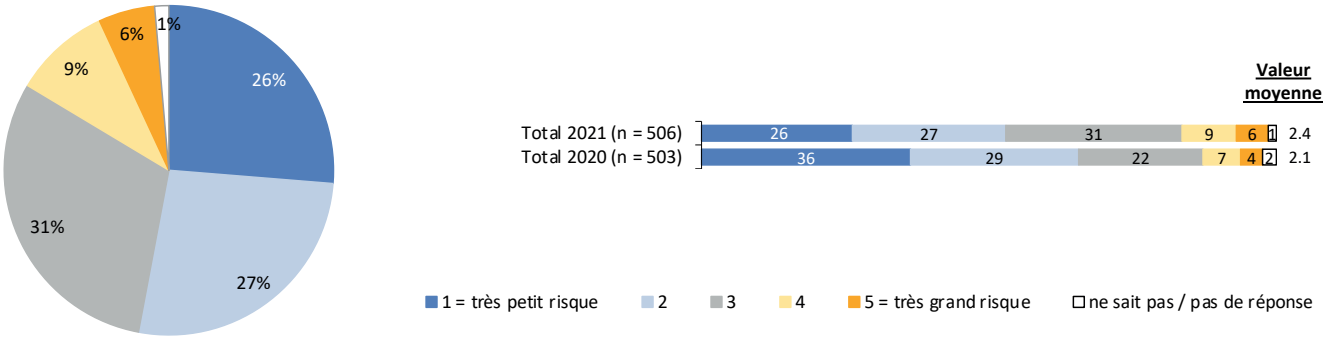
L'évaluation du risque d'une cyberattaque est revue à la hausse, mais elle reste à un faible niveau

La numérisation, le télétravail et les affaires lucratives de la cybercriminalité font revoir à la hausse l'évaluation des risques des PME suisses : en 2021, 15 % des dirigeants estimaient que le risque était élevé ou très élevé que leur entreprise fasse l'objet d'une cyberattaque d'ici les 2–3 prochaines années qui immobiliserait leur entreprise durant au moins un jour (2020 : 11 %). En s'inscrivant à 4 %, la valeur pour l'évaluation des cyberattaques mettant en péril l'existence de l'entreprise a augmenté en comparaison annuelle, mais elle reste nettement inférieure à la probabilité d'une immobilisation pendant un jour (2020 : 2 %).

Questions posées aux PME suisses :

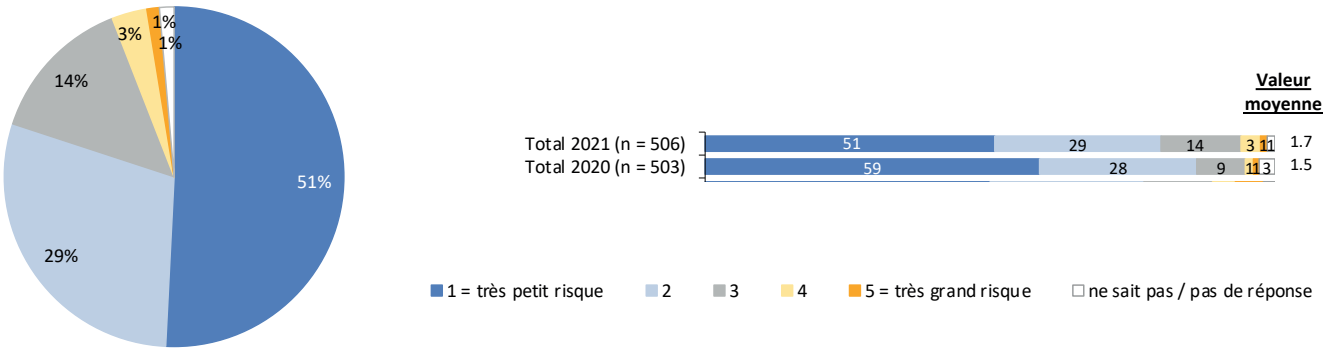
- Quelle est l'infrastructure informatique critique pour la fourniture de prestations dans votre entreprise ou quelle importance attachez-vous à la cybersécurité?
- Quelles sont les prestations que vous ne seriez pas en mesure de fournir en cas de défaillance des systèmes informatiques?
- Quelle protection de votre infrastructure informatique avez-vous définie?
- Quelles solutions alternatives (concepts de restauration des données) avez-vous mises au point?
- De quels concepts/plans d'urgence disposez-vous ou quels éléments vous manquent?

Évaluation d'un risque de cyberattaque «mineure»



Évaluation d'un risque de cyberattaque «mineure» («Comment évaluez-vous le risque que votre PME fasse l'objet d'une cyberattaque d'ici les 2–3 prochaines années qui immobiliserait votre entreprise durant au moins un jour?»/n 2021 = 506, n 2020 = 503)

Évaluation d'un risque de cyberattaque mettant en péril l'existence de l'entreprise



Évaluation d'un risque de cyberattaque mettant en péril l'existence de l'entreprise («Comment évaluez-vous le risque que votre PME fasse l'objet d'une cyberattaque d'ici les 2–3 prochaines années qui mettrait en péril l'existence de votre entreprise?»/n 2021 = 506, n 2020 = 503)

Mesures techniques et organisationnelles visant à augmenter la cybersécurité

On observe un important potentiel au niveau de la planification et de la mise en œuvre de mesures de sécurité informatiques sur le plan organisationnel

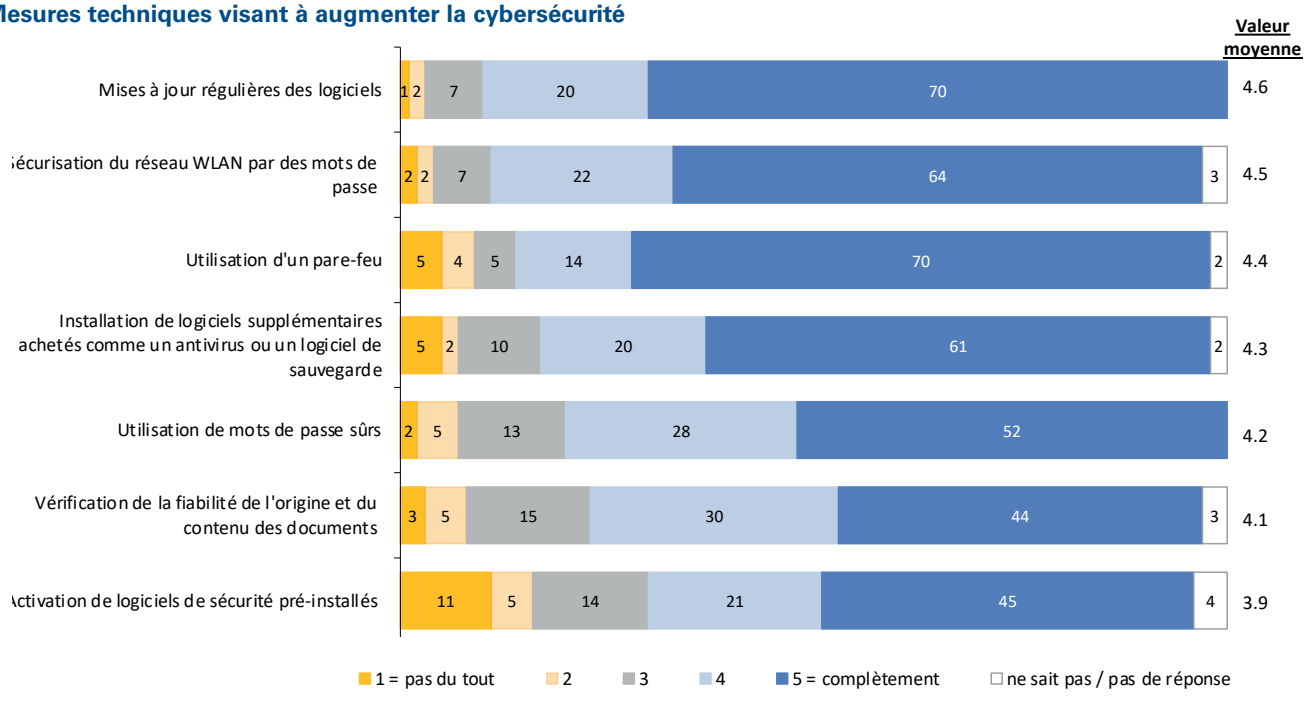
Comme l'avait déjà révélé l'étude réalisée en 2020, les PME suisses se situent à un stade relativement avancé dans la mise en œuvre de mesures techniques visant à augmenter la cybersécurité. Tout comme en 2020, un important potentiel subsiste en 2021 au niveau des mesures organisationnelles. À peine la moitié des PME suisses disposent en effet d'un concept de sécurité informatique (47 % pleinement/pleinement et entièrement) et seuls deux cinquièmes forment régulièrement leurs collaborateurs (39 %) ou mènent des audits de sécurité informatique (37 %).

Dans un tiers des PME (30 %), les dirigeants établissent un budget séparé pour la sécurité informatique. Cette valeur est plus élevée dans le cas des PME qui ont déjà été attaquées (31 %) et dont les dirigeants se sentent plutôt informés sur les thèmes relatifs à la cybersécurité (37 %).

Questions posées aux PME suisses :

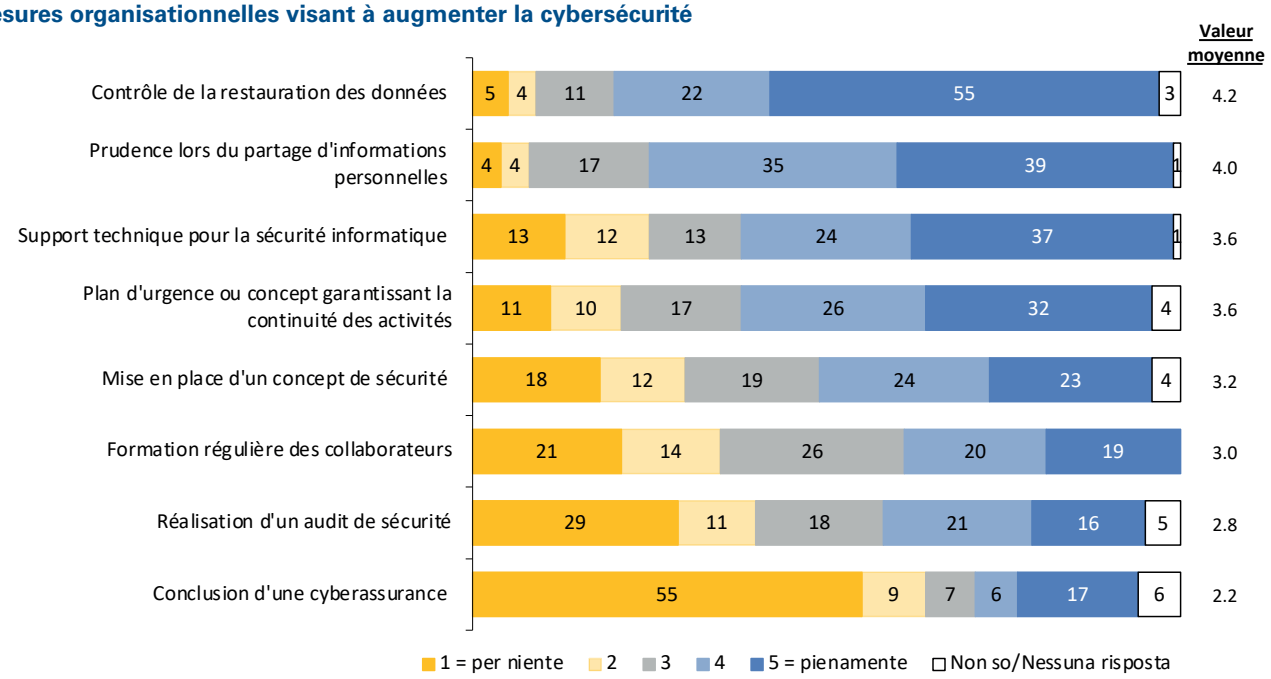
- Avez-vous réalisé un inventaire de votre infrastructure informatique? Disposez-vous d'une liste répertoriant le matériel informatique et les logiciels (avec numéros de série, date et prix d'achat, version logicielle, etc.)?
- Quelle infrastructure informatique fait l'objet de mises à jour? Qui s'en charge et à quelle fréquence?
- Quelle protection de votre infrastructure informatique avez-vous définie pour garantir la continuité des activités en cas d'attaques ou d'autres problèmes?
- Quelles mesures organisationnelles concrètes devraient être planifiées et mises en œuvre?
- Devriez-vous éventuellement réaliser un audit de sécurité informatique et souscrire une cyberassurance?

Mesures techniques visant à augmenter la cybersécurité



Mesures techniques visant à augmenter la cybersécurité («Jusqu'à quel point les mesures techniques ci-après sont-elles appliquées chez vous pour augmenter la cybersécurité?»/n = 506/échelle de 1 = pas du tout à 5 = pleinement et entièrement, indication en valeurs moyennes)
L'illustration comprend les valeurs 4 et 5 sur une échelle de 5.

Mesures organisationnelles visant à augmenter la cybersécurité



Mesures organisationnelles visant à augmenter la cybersécurité («Jusqu'à quel point les mesures organisationnelles ci-après sont-elles appliquées chez vous pour augmenter la cybersécurité?»/n = 506/échelle de 1 = pas du tout à 5 = pleinement, indication en valeurs moyennes)
L'illustration comprend les valeurs 4 et 5 de l'échelle de 5.

la Mobilière

Le Groupe Mobilière («la Mobilière») est le leader suisse de l'assurance standard et le numéro un des assurances ménage, PME et vie risque. Fondée en 1826, la Mobilière est la plus ancienne société d'assurances privée de Suisse et opère encore, à ce jour, sur une base coopérative.
Pas moins de 80 agences générales entrepreneuriales dotées de leur propre service des sinistres offrent des prestations de proximité à plus de 2,2 millions de clientes et clients sur 160 sites. Un ménage sur trois et une entreprise sur trois en Suisse sont ainsi assurés à la Mobilière. En tant qu'assureur toutes branches, la Mobilière emploie 5856 collaboratrices et collaborateurs et offre 338 places d'apprentissage.

Aperçu de l'offre de cyberprotection pour les PME

valuation succincte de la cybersécurité
Cette analyse consiste en un contrôle gratuit de la cybersécurité des entreprises, doublé de recommandations concrètes sur les mesures à prendre en vue de renforcer le niveau de sécurité. Pour les PME, les avantages d'un tel service sont multiples :

- analyse neutre, basée sur les normes en vigueur, de la cybersécurité actuelle de l'entreprise
- comparaison entre la situation en matière de risques de la PME et celle d'autres entreprises
- recommandations de mesures concrètes personnalisées, assorties de renvois vers des sources d'information supplémentaires

Plus d'informations sur
www.mobiliere.ch/analyse-cybersecurite

Cyberformation pour les entreprises
Il suffit de peu de choses: un collaborateur ouvre un e mail douteux et toute votre entreprise se retrouve paralysée. Cette formation sensibilise les collaborateurs aux risques liés à l'utilisation d'Internet et des e-mails.
À l'issue du cours, les collaborateurs connaissent les méthodes utilisées par les pirates informatiques et savent comment réagir en cas d'attaque.
Le programme de sensibilisation aux cyberrisques se compose de différents modules:

- séquences d'exercices en ligne pour apprendre comment réagir face aux menaces d'Internet
- simulation d'attaques par phishing avec évaluation de la réaction des collaborateurs
- rapport rassemblant les principaux résultats de la formation

Plus d'informations sous
ww.mobiliere.ch/cyberformation

Cyberassurance
La cyberassurance consiste en un paquet complet de mesures qui permet de sécuriser l'exploitation d'une PME à la suite d'une cyberattaque. Cette assurance intervient comme suit :

- prise en charge des frais des spécialistes qui suppriment les maliciels, restaurent l'accès aux données et s'emploient à empêcher la divulgation de celles-ci
- indemnisation d'une éventuelle interruption d'exploitation dont la durée excède douze heures
- soutien financier et juridique si un client reproche à la PME d'avoir provoqué un dommage en raison d'un e mail contenant un virus

Plus d'informations sous
www.mobiliere.ch/cyberprotection-entreprises

Vous trouverez également une compilation d'informations utiles pour les PME sur le thème de la cybersécurité à l'adresse www.mobiliere.ch/pme

Mesures de cybersécurité liées à l'obligation de télétravail

Investissements supplémentaires dans des logiciels, des pare-feux et des mots de passe

Le nombre croissant de cyberattaques et le travail à domicile pratiqué par de nombreux collaborateurs ont incité les PME suisses à mettre en place des mesures de cybersécurité supplémentaires. 23 % des PME (2020 : 9 %) ont engagé des mesures supplémentaires en raison de l'obligation/de la recommandation de télétravail. Cela concerne une nouvelle fois plus particulièrement les PME dont les dirigeants s'estiment (plutôt) bien informés au sujet des cyberrisques (30 %).

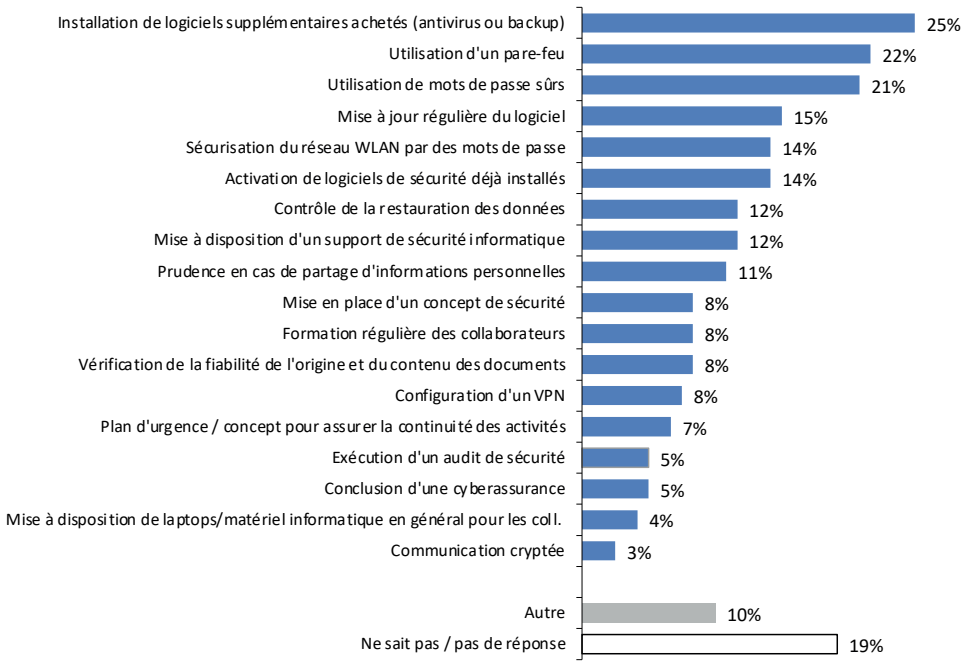
Les principales mesures consistent en l'installation de logiciels supplémentaires (25 %), en l'utilisation de pare-feux (22 %) et de mots de passe sûrs (21 %) et en la mise à jour régulière des logiciels (15 %).

Parmi les mesures appliquées figurent également la désignation de responsables de la protection des données au sein de l'entreprise (dans 64 % des PME suisses), des processus relatifs à la publication et à la suppression de données (28 %) et la tenue d'un inventaire du traitement des données.

Questions posées aux PME suisses :

- La hausse du télétravail a-t-elle aggravé la vulnérabilité informatique de votre entreprise?
- Quelles mesures de cybersécurité devriez-vous impérativement ou immédiatement mettre en œuvre en prévision des prochains mois?
- Quelles autres mesures devraient être planifiées pour augmenter durablement la cybersécurité?
- Un collaborateur a-t-il été désigné responsable de la protection des données et des règlements/processus correspondants ont-ils été introduits?

Mesures de cybersécurité liées à l'obligation de télétravail



Mesures de cybersécurité liées à l'obligation de télétravail («Quelles mesures de sécurité avez-vous prises durant le confinement?/n = 118 (Filtre : lorsque des mesures de sécurité supplémentaires contre les cyberattaques ont été prises dans le cadre du confinement)/question précodée, semi-ouverte)

Mise en œuvre pratique pour les PME suisses

Thématiques et questions pour une mise en œuvre dans votre entreprise

À partir de l'étude, des thématiques identifiées et des défis posés aux PME, les auteurs ont établi la liste de contrôle ci-dessous, destinée à servir de base de discussion et d'outil dans le cadre d'un travail de projet.

Nous vous souhaitons beaucoup de succès dans la mise en œuvre de ces thématiques clés.

Stratégie concernant l'environnement de travail et mise en place du télétravail

- ☐ Dans quelle mesure le télétravail vous permet-il d'accroître la flexibilité de vos collaborateurs, de renforcer l'attrait de votre entreprise aux yeux du personnel et de réduire votre structure des coûts?
- ☐ Avez-vous déjà discuté du télétravail avec vos collaborateurs et, sur cette base, développé des idées, identifié des potentiels et élaboré une feuille de route?
- ☐ Le télétravail est-il appelé à s'établir durablement dans votre entreprise? Avez-vous identifié des potentiels et en avez-vous discuté?
- ☐ Existe-t-il une convention de télétravail, p. ex. pour la prise en charge des frais liés à l'équipement de bureau privé?
- ☐ Avez-vous identifié et défini les exigences posées par le «New Work» (environnement de travail 4.0) en matière de culture, de conduite et de communication?
- ☐ Avez-vous élaboré une stratégie et une feuille de route correspondante pour votre environnement de travail 4.0?
- ☐ Quelles expériences positives et/ou négatives avez-vous tirées du télétravail pendant les confinements? Quels enseignements en sont ressortis et quelles améliorations pouvez-vous apporter?
- ☐ Pourquoi n'avez-vous pas davantage recours au télétravail et ne l'utilisez-vous pas dans une stratégie de renouvellement de votre entreprise (p. ex. afin d'accroître votre réputation en tant qu'employeur)?
- ☐ Un concept a-t-il été élaboré pour l'utilisation des outils de communication (et les plateformes les plus appropriées ont-elles par la suite été implémentées)?
- ☐ Avez-vous élaboré un concept et des directives sur la sécurité des données dans le cadre de l'utilisation des plateformes de communication à des fins professionnelles?
- ☐ Ces plateformes sont-elles sécurisées? Quelles sont les données/informations qui sont ou peuvent y être échangées, et quelle est la nature de ces plateformes?

Stratégies et mesures de cybersécurité

Acquisition de connaissances et sensibilisation

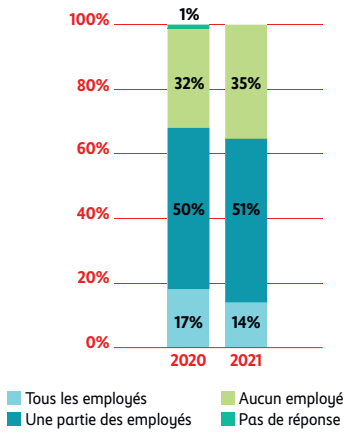
- ☐ Procédez-vous à l'identification régulière du potentiel lié à l'utilisation de nouvelles technologies et avez-vous défini une stratégie/feuille de route pour la mise en place d'une nouvelle infrastructure informatique?
- ☐ Quels sont les nouveaux produits et services que vous pourriez commercialiser avec (davantage de) succès en investissant dans l'informatique et la cybersécurité?
- ☐ Répondez-vous à vos propres exigences (ou à celles du marché) en matière de cybersécurité?
- ☐ Comment procédez-vous pour vous informer régulièrement sur les dangers qui vous menacent ainsi que sur les concepts et solutions destinés à augmenter la cybersécurité?
- ☐ Les collaborateurs connaissent-ils les divers types de cyberattaques? Comment les sensibilisez-vous à cette thématique?
- ☐ Quelles mesures techniques et organisationnelles avez-vous mises en place pour augmenter la cybersécurité dans votre entreprise?
- ☐ En quoi consiste l'examen régulier de vos concepts et mesures en matière de cybersécurité?

Concepts et mesures

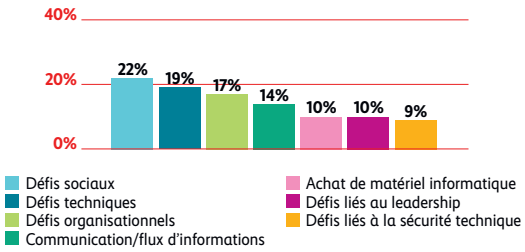
- ☐ Quelle est l'infrastructure informatique critique pour la fourniture de prestations dans votre entreprise ou quelle importance attachez-vous à la cybersécurité?
- ☐ Quelles sont les prestations que vous ne seriez pas en mesure de fournir en cas de défaillance des systèmes informatiques?
- ☐ Quelle protection de votre infrastructure informatique avez-vous définie?
- ☐ Quelles solutions alternatives (concepts de restauration des données) avez-vous mises au point?
- ☐ De quels concepts/plans d'urgence disposez-vous ou quels éléments vous manquent?
- ☐ Avez-vous réalisé un inventaire de votre infrastructure informatique? Disposez-vous d'une liste répertoriant le matériel informatique et les logiciels (avec numéros de série, date et prix d'achat, version logicielle, etc.)?
- ☐ Quelle infrastructure informatique fait l'objet de mises à jour? Qui s'en charge et à quelle fréquence?
- ☐ Quelle protection de votre infrastructure informatique avez-vous définie pour garantir la continuité des activités en cas d'attaques ou d'autres problèmes?
- ☐ Quelles mesures organisationnelles concrètes devraient être planifiées et mises en œuvre?
- ☐ Devriez-vous éventuellement réaliser un audit de sécurité informatique et souscrire une cyberassurance?
- ☐ La hausse du télétravail a-t-elle aggravé la vulnérabilité informatique de votre entreprise?
- ☐ Quelles mesures de cybersécurité devriez-vous impérativement ou immédiatement mettre en œuvre en prévision des prochains mois?
- ☐ Quelles autres mesures devraient être planifiées pour augmenter durablement la cybersécurité?
- ☐ Un collaborateur a-t-il été désigné responsable de la protection des données et des règlements/processus correspondants ont-ils été introduits?

Infographie
«Télétravail et cybersécurité dans les PME suisse 2021»

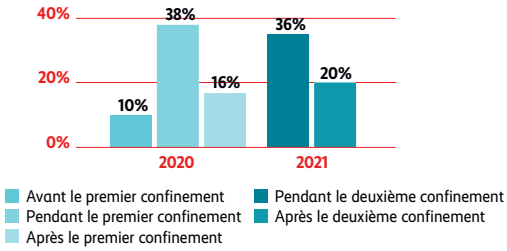
Nombre d'employés qui pourraient potentiellement travailler à domicile



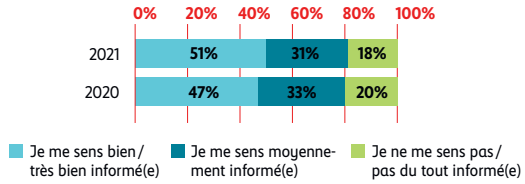
Les sept plus grands défis de la mise en œuvre du télétravail



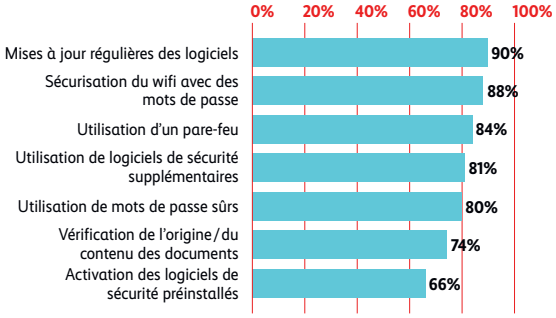
Changement dans les habitudes de télétravail pendant le confinement COVID



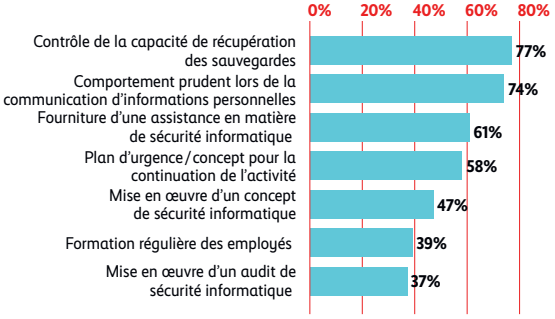
Information personnelle



Mesures techniques pour renforcer la cybersécurité



Mesures organisationnelles pour renforcer la cybersécurité



Contact/auteurs

Marc K. Peter
Responsable du centre de compétences Transformation numérique FHNW Hochschule für Wirtschaft, Olten
marc.peter@fhnw.ch

Andreas Hölzli
Responsable du centre de compétences Cyberrisques La Mobilière, Berne
andreas.hoelzli@mobi.ch

Andreas W. Kaelin
Directeur adjoint et responsable du dossier Cybersécurité digitalswitzerland, Berne
andreas@digitalswitzerland.com

Karin Mändli Lerc
Responsable de projet gfs-zürich, Zurich
karin.maendlilerch@gfs-zh.ch

Patric Vifian
Marketing Manager PME La Mobilière, Berne
patric.vifian@mobi.ch

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité Académie suisse des sciences techniques
SATW, Zurich
nicole.wettstein@satw.ch

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

Télétravail et cybersécurité dans les PME suisses : stratégies et mesures des PME suisses de 4 à 49 collaborateurs dans le contexte du coronavirus (COVID-19)

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

www.cyberstudie.ch
Berne, novembre 2021