Le guide de la cybersécurité pour les très petites entreprises

Introduction

Les très petites entreprises (TPE) constituent le pilier de l'économie mondiale et représentent une réelle opportunité pour les partenaires de répondre à leurs besoins en matière de cybersécurité. Malgré leur taille, les TPE détiennent des données clients, des propriétés intellectuelles et des informations financières précieuses qui constituent des cibles de choix pour les cybercriminels. De plus, l'absence perçue de mesures de sécurité ne fait qu'accroître l'attractivité de ces cibles. Ce guide aborde le problème de la cybersécurité pour les TPE, en mettant en évidence les menaces auxquelles elles sont confrontées, leur approche actuelle de la sécurité et leurs principaux besoins. Enfin, ce document explique comment Norton Small Business répond à ces besoins essentiels, en offrant une solution complète.

1 Opportunité de marché pour les partenaires

Le marché des TPE, définies comme les entreprises comptant moins de 10 collaborateurs, représente une gigantesque opportunité de 3,9 milliards de dollars. En outre, le marché mondial des moins de 10 collaborateurs connaît un taux de croissance annuel composé (TCAC) de 8 %.

Il est important de noter que 86 % des TPE font appel à des partenaires tels que des revendeurs, des distributeurs à valeur ajoutée, des entreprises d'infogérance et des entreprises de télécommunications pour répondre à leurs besoins en matière de technologies de l'information. Ces données montrent à quel point les partenaires ont l'opportunité de capitaliser sur les préoccupations croissantes des TPE en matière de cybersécurité.

2 Les cyberrisques auxquels sont confrontés les TPE

Les TPE sont particulièrement vulnérables aux cybermenaces en raison de leurs ressources et de leur expertise limitées. Voici quelques statistiques et analyses clés :

Données clients vulnérables : 87 % des petites entreprises possèdent des données clients susceptibles d'être compromises[1].

Incidence élevée des violations de données : Plus de 57 % des petites entreprises ont subi une violation de sécurité ou de données en 2022[2].

Délai de récupération accru : 65 % des petites entreprises ont déclaré en 2022 qu'il leur fallait plus d'un an pour retrouver leur niveau d'avant la violation[3].

Types de données menacées

- **Données personnelles :** Notamment les informations sur les clients, les partenaires commerciaux et les collaborateurs.
- **Propriété intellectuelle :** Savoir-faire de l'entreprise et informations propriétaires.
- **Données financières :** Registres comptables et plans financiers.

Pertes potentielles

- **Coûts de récupération :** Dépenses importantes pour restaurer les systèmes et les données.
- **Pertes de bénéfices :** Interruption des activités entraînant une perte de chiffre d'affaires.
- **Amendes pour non-respect de la réglementation :** Sanctions en cas de non-respect des réglementations.
- **Atteinte à la réputation :** Perte de la confiance des clients et de la crédibilité de l'entreprise.
- **Responsabilité juridique :** Coûts engendrés par les procédures judiciaires.

En moyenne en 2022, près de la moitié des petites entreprises (45 %) ont dépensé entre 250 000 et 500 000 dollars pour faire face aux conséquences des violations[3]. En outre, le coût médian par incident impliquant un ransomware a plus que doublé au cours des deux dernières années pour atteindre 26 000 dollars[4].

3 L'approche actuelle des TPE en matière de cybersécurité

Malgré le risque élevé, de nombreuses TPE ne sont pas protégées de manière adéquate :

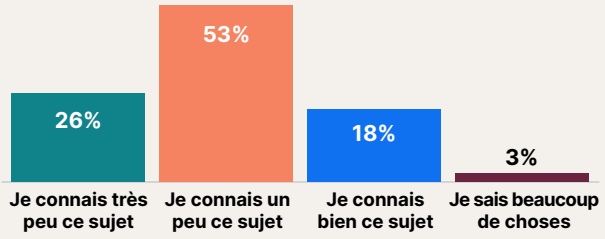
Préoccupation majeure, peu de mesures : Environ 60 % des petites entreprises se disent préoccupées par les menaces de cybersécurité telles que le phishing, les malwares et les ransomwares[5].

Incidence sur les activités : 48 % des PME ont subi un incident de cybersécurité au cours de l'année écoulée[6].

Manque de protection : Une grande partie des TPE ne disposent pas de mesures de cybersécurité de base. Pas moins de 20 % ne disposent d'aucun logiciel de protection des terminaux[7], et des études montrent que jusqu'à 51 % n'ont aucune politique ou procédure de cybersécurité en place[8].

Prise de décision, manque de connaissances : Dans 67 % des TPE, le propriétaire ou le PDG assume la responsabilité des solutions de cybersécurité, alors qu'il ne dispose souvent pas de l'expertise technique nécessaire.

Connaissances en cybersécurité (tous)



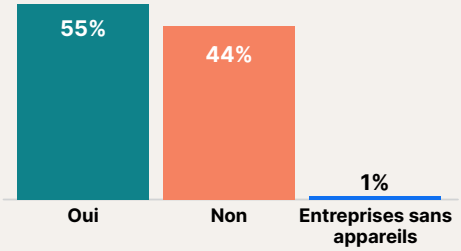
Source : Étude Gen Quant 2023 - Connaissances en matière de cybersécurité (tous) - SC1 Dans quelle mesure vous considérez-vous bien informé sur l'état actuel de la cybersécurité ? (n=1,011)

Pratiques courantes

Le chevauchement entre les appareils professionnels et personnels constitue un défi de taille, car il entraîne des mesures de sécurité inadéquates. De nombreuses TPE s'appuient sur un logiciel antivirus de base, et de nombreuses fonctions avancées ne sont pas utilisées en raison d'un manque de compétences techniques.

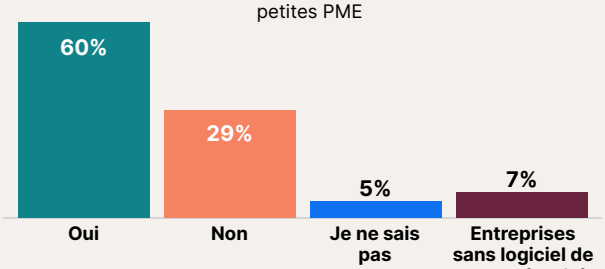
L'appareil professionnel comme principal appareil personnel (Tous)

Aucune différence significative selon la taille de l'entreprise



Le même logiciel de sécurité pour l'entreprise et la maison (Tous)

Le mélange entreprise/domicile est plus fréquent dans les petites PME



Source : Étude Gen Quant 2023 - Appareil professionnel comme principal appareil personnel (redéfini pour tous) - O5 Certains de vos collaborateurs utilisent-ils leur appareil professionnel comme principal appareil personnel ? (n=1,011). Utilisez-vous le même logiciel de sécurité en ligne pour vos appareils personnels et professionnels ? (n=1,011)

4 Principaux besoins de cybersécurité pour les propriétaires de TPE

D'après l'étude qualitative de Norton SoHo 2023, les propriétaires de TPE ont les principaux besoins suivants en matière de cybersécurité :

Confiance dans leur cybersécurité : Les propriétaires de TPE doivent avoir la certitude que leurs appareils et leurs logiciels sont protégés contre toute forme de cybermenace.

Protection des données : Protéger les données des entreprises et des clients contre les violations, le chiffrement par ransomware ou le vol.

Atténuation des risques : Les TPE ont besoin de solutions qui contribuent à réduire les risques de cybersécurité causés par les actions des collaborateurs.

Évolutivité : À mesure que les TPE se développent, leurs besoins en matière de cybersécurité évoluent. Elles ont besoin de solutions capables de s'adapter à l'évolution de leurs attentes.

Comment Norton Small Business répond aux besoins des TPE en matière de cybersécurité

Norton Small Business offre une protection complète adaptée aux défis spécifiques des TPE. Voici comment Norton répond aux principaux risques et attentes :

Avantages principaux

- **Cyberprotection facile à utiliser :** Norton Small Business est facile à installer et à utiliser, ne nécessitant aucune compétence informatique, ce qui permet aux propriétaires de TPE de se concentrer sur leurs activités principales.
- **Support technique disponible 24 h/24 et 7 j/7 :** Accès à un support technique pour les entreprises assuré 24 h/24 par l'équipe d'experts de Norton, prête à conseiller le propriétaire de l'entreprise et ses collaborateurs sur les produits et services Norton, ainsi que sur la suppression des virus.
- **Réduction des risques :** Des fonctions de sécurité avancées, notamment un VPN, un navigateur sécurisé et un gestionnaire de mots de passe, permettent aux collaborateurs de travailler à distance de manière plus sûre, même sur des appareils mobiles.
- **Sauvegarde automatisée des données :** Les sauvegardes automatiques vers un stockage sécurisé sur le cloud aident à éviter les pertes de données dues aux ransomwares, au vol ou aux pannes matérielles.
- **Des PC plus rapides pendant plus longtemps :** Le nettoyage automatisé des PC, les mises à jour logicielles et l'optimisation aident à préserver le fonctionnement optimal des ordinateurs.

Avantage concurrentiel

Norton Small Business Premium se distingue de ses concurrents par les avantages suivants :

- **Support technique pour les entreprises 24 h/24 et 7 j/7 :** Accès immédiat à l'assistance d'un expert pour la suppression des virus et le support technique des produits.
- **Navigateur privé et VPN avec transfert de données illimité :** Outils permettant de renforcer la confidentialité des communications professionnelles et des transactions financières, essentiels pour le travail mobile et à distance.
- **500 Go de stockage cloud :** Un vaste espace de stockage sécurisé sur le cloud avec des sauvegardes automatiques pour les données critiques de l'entreprise.
- **Outils d'optimisation pour PC :** l'outil de nettoyage du PC, le Gestionnaire de mises à jour et la Mise à jour des pilotes permettent d'optimiser les PC et de réduire les pannes, afin d'aider à assurer un fonctionnement plus rapide et plus stable.

Conclusion

La croissance et l'évolution des très petites entreprises nécessitent une nouvelle approche de la cybersécurité. Face à la multiplication des menaces, les TPE ont besoin de solutions fiables et conviviales qui non seulement protègent leurs données, mais leur donnent également les moyens de s'épanouir dans un monde numérique. En s'associant à Norton, les propriétaires de TPE peuvent faire face aux complexités de la cybersécurité en toute confiance et se concentrer sur l'atteinte de leurs objectifs commerciaux.

Sources

[1]D'après une enquête menée par Digital.com auprès de 1 250 petites entreprises, mars 2022.

[2]D'après l'étude d'impact sur les entreprises réalisée en 2022 par Identity Theft Resource Centre (Centre de ressources sur l'usurpation d'identité)

[3]Août 2022, 227 personnes interrogées dans des entreprises de moins de 500 salariés

[4]Étude de Verizon sur les violations de données 2023

[5]L'indice MetLife et la Chambre de commerce des États-Unis sur les petites entreprises pour le premier trimestre 2024

[6]StationX

[7]BullGuard : Une nouvelle étude révèle qu'une PME sur trois utilise une cybersécurité grand public gratuite et qu'une sur cinq n'utilise aucune sécurité des terminaux. PRNewswire, février 2020

[8]Verizon Business : La vérité derrière 5 idées fausses sur la cybersécurité des petites entreprises