acei

BÂTIR UN MEILLEUR
CANADA EN LIGNE

SONDAGE DE L'ACEI SUR LA SÉCURITÉ INTERNET AU CANADA 2018

Nous avons accès à une grande quantité de données d'enquête portant sur différents aspects de la cybersécurité, mais la plupart de ces renseignements ont été recueillis dans d'autres pays que le Canada ou concernent le Canada en tant qu'élément du marché nord-américain. Par conséquent, peu de données publiques portent sur la perspective canadienne dans ce domaine dynamique qui évolue rapidement.

Pour pallier ce manque de renseignements, nous avons réalisé le premier Sondage de l'ACEI sur la sécurité Internet au Canada à la fin de l'année 2017. Nous sommes heureux de publier les résultats dans le présent rapport. Nous avons invité les propriétaires de domaines .CA à participer au sondage et à partager leurs opinions sur de nombreux sujets liés à la cybersécurité.

Méthodologie

Entre novembre 2017 et janvier 2018, nous avons interrogé 1 985 Canadiens propriétaires d'au moins un domaine .CA enregistré pour une entreprise ou une institution. Les répondants ont été divisés en trois groupes principaux, selon leur utilisation de leur nom de domaine .CA. Environ 18 % des répondants utilisent leur nom de domaine pour un site Web personnel, habituellement une entreprise individuelle; 74 % l'utilisent pour un site Web de petite entreprise et le 8 % restant pour un site Web d'entreprise ou d'organisation de plus de 100 employés.

La grande majorité des professionnels que nous avons interrogés sont impliqués dans les TI et les décisions relatives à la sécurité de leurs organisations. 72 % des répondants propriétaires de petites entreprises ont indiqué qu'ils sont principalement responsables de la sécurité et des opérations de TI pour leurs organisations, alors que 90 % des répondants qui travaillent pour de plus grandes entreprises ont mentionné qu'ils sont impliqués dans la sécurité et dans le processus décisionnel lié aux TI.

Finalement, l'invitation pour le sondage en ligne a été envoyée par courriel et la participation était volontaire.

Utilisation de leur nom de domaine .CA

Principales conclusions

- **La connaissance des cybermenaces est approfondie chez tous les répondants —** La connaissance de l'ampleur et des types de cybermenaces est approfondie pour tous les répondants. Par exemple, 77 % des propriétaires de domaines personnels et 68 % des répondants liés à de petites entreprises affirment être conscients ou très conscients de l'ampleur des cybermenaces auxquelles ils sont confrontés chaque jour. Le fait que les petites entreprises sont moins conscientes que les propriétaires individuels peut indiquer une crainte plus élevée chez les propriétaires d'entreprises.

- **Tous les répondants sont préoccupés par les cyberattaques —** 68 % des propriétaires de domaines personnels et 77 % des propriétaires de domaines de petites entreprises affirment être préoccupés ou très préoccupés par des attaques potentielles.

- **Les cyberattaques ont une incidence généralisée —** Tous les groupes interrogés sont aux prises avec les conséquences de diverses cyberattaques. 41 % des répondants qui ont un site Web personnel ont indiqué qu'ils connaissaient quelqu'un qui a été victime d'un virus ou d'un logiciel rançonneur; 10 % des petites entreprises affirment que leur site Web a été paralysé par une attaque au cours des 24 derniers mois; 22 % des plus grandes organisations ont été victimes d'une attaque DDoS au cours des 12 derniers mois.

- **Les entreprises utilisent une gamme de solutions de sécurité pour se protéger —** Les petites et grandes entreprises utilisent de nombreuses solutions technologiques pour se protéger des cyberattaques en constante évolution. Ces solutions comprennent les logiciels antivirus, les appareils et les logiciels de pare-feu, le chiffrement du courrier électronique et des bloqueurs de requêtes DNS malveillantes.

- **La qualité et le soutien des fournisseurs sont les facteurs les plus importants dans le choix des solutions de sécurité —** Pour les petites et grandes entreprises, la qualité et le soutien sont les principaux facteurs qui influencent les décisions d'achat de solutions de sécurité des TI.

- **Les individus/propriétaires de maisons ne sont pas adéquatement protégés —** Dans l'ensemble, lorsque nous les avons interrogés sur leur expérience personnelle, les individus n'investissent pas assez dans les solutions de sécurité pour protéger leurs réseaux. Plus du tiers des répondants de ce groupe ne déboursent pas pour obtenir une solution de sécurité pour leurs ordinateurs ou appareils mobiles, même s'ils sont conscients des risques.

RÉSULTATS DU SONDAGE : PROPRIÉTAIRES DE DOMAINES PERSONNELS

13 % des personnes interrogées utilisent leurs domaines .CA pour un site Web personnel et plus. Dans plusieurs cas, ce sont des pigistes ou des personnes avec une activité parallèle. Nous leur avons posé plusieurs questions dans le but d'évaluer leurs connaissances des types de menaces en ligne, les conséquences que les cyberattaques ont eu pour eux jusqu'à maintenant et les mesures qu'ils prennent pour protéger leurs ordinateurs et appareils mobiles.

Trois quarts des propriétaires de domaines sont conscients des risques de cyberattaques

Dans l'ensemble, ce groupe démontre des connaissances approfondies des menaces en ligne, avec 77 % des répondants qui évaluent leurs connaissan-ces avec un 7 sur 10, 1 étant « aucune connaissance » et 10 étant « très bonnes connaissances ». Ce niveau de connaissances correspond aux résultats du Dossier documentaire 2017 de l'ACEI selon lesquelles 75 % des Canadiens sont préoccupés par la menace d'une cyberattaque contre une organisation qu'ils connaissent.

Près d'un quart des répondants (24 %) ont choisi 10 dans l'échelle, ce qui in-dique qu'ils considèrent que leurs connaissances sont très bonnes relativement aux menaces pour leurs ordinateurs et appareils numériques.

Par contre, seulement 7 % des propriétaires de domaines personnels ont affirmé avoir des connaissances limitées de l'ampleur et des types de menaces, évalu-ant leurs connaissances de 1 à 4 dans l'échelle.

En plus d'être généralement conscients de la nature des menaces à la sécurité en ligne, les répondants dans cette catégorie ont aussi indiqué qu'ils possé-daient de très bonnes connaissances des types de menaces à la sécurité les plus communes et des incidences de celles-ci. Ces menaces comprennent les virus, l'hameçonnage, les logiciels rançonneurs et le vol d'identité.

L'ampleur et la diversité des menaces à la cybersécurité représentent une préoccupation importante pour les propriétaires de domaines

Sans surprise, étant donné les connaissances généralement approfondies de l'ampleur des risques de sécurité dans ce groupe, une majorité importante des personnes interrogées sont très préoccupées par les cyberattaques.

Dans l'ensemble, 68 % des répondants dans cette catégorie indiquent qu'ils sont préoccupés par la possibilité d'être touchés personnellement et financièrement, tandis que 25 % des répondants indiquent qu'ils sont « très préoccupés ».

68 % des répondants dans cette catégorie indiquent qu'ils sont préoccupés par la possibilité d'être touchés personnellement et financièrement

Cette préoccupation est justifiée, car le nombre de personnes interrogées qui ont été victimes d'une cyberattaque est important, particulièrement en ce qui concerne les virus informatiques.

Par exemple, 24 % des répondants ont affirmé qu'ils savaient qu'un ordinateur ou un appareil mobile leur appartenant ou appartenant à un membre de leur famille avait été infecté par un virus au cours de la dernière année (excluant les logiciels rançonneurs).

Lorsqu'on leur demande s'ils ont été victimes d'une attaque de logiciel rançonneur sur leur ordinateur ou appareil mobile l'an dernier, seulement 3 % des répondants ont affirmé que leurs appareils avaient été verrouillés et qu'ils avaient été contraints de payer une rançon pour le déverrouiller. Toutefois, lorsqu'on leur demande s'ils connaissent une personne qui avait été victime d'un virus ou d'un logiciel rançonneur, la proportion grimpe à 41 %!

Sur le plan des attaques d'hameçonnage, une grande proportion des personnes interrogées (85 %) ont indiqué avoir reçu des courriels d'hameçonnage au cours de la dernière année. 6 % de tous les répondants ont indiqué que ces attaques avaient eu une incidence sur leurs transactions bancaires en ligne ou d'autres codes d'identification, et 17 % des répondants de cette catégorie ont été impliqués dans une transaction frauduleuse à l'égard d'un compte bancaire ou d'une carte de crédit au cours de la dernière année, ce qui sous-entend que des pirates informatiques ont utilisé d'autres méthodes pour voler leurs d'identifiants de connexion bancaire.

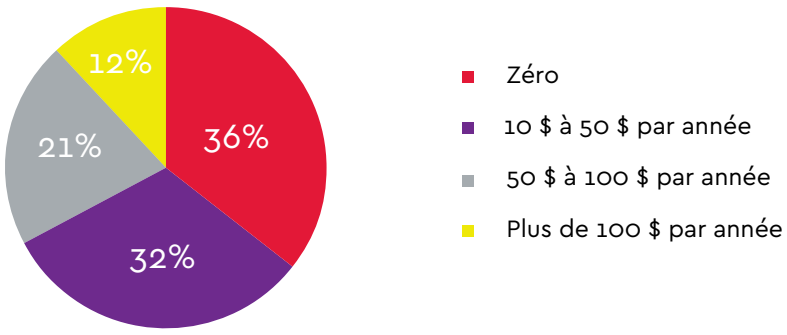
Écart important entre les connaissances en cybersécurité et la protection

Malgré de bonnes connaissances des incidences potentielles des menaces à la sécurité pour la majorité de propriétaires de domaines personnels, un nombre étonnamment faible de répondants réalisent un investissement important dans des solutions conçues pour protéger leurs appareils personnels et leurs données des nombreuses menaces potentielles.

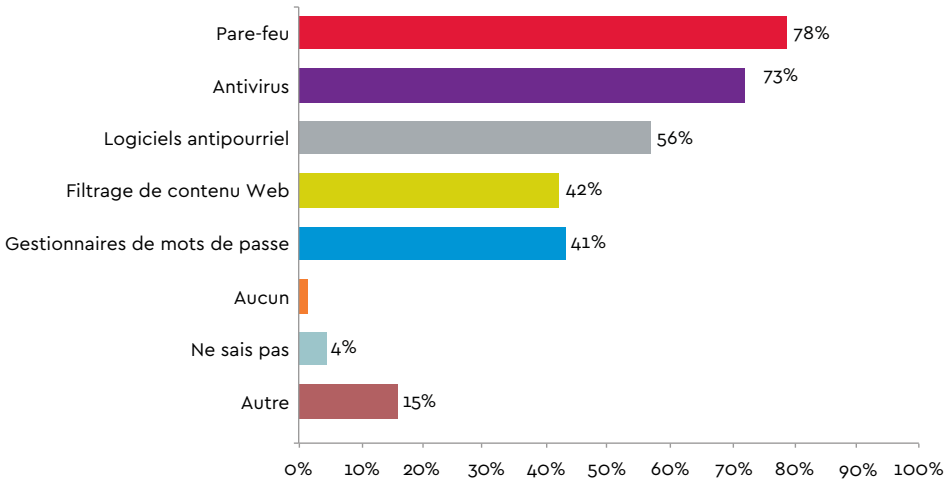
Par exemple, 36 % des répondants affirment qu'ils n'investissent actuellement dans aucune forme de protection pour leurs ordinateurs personnels et appareils mobiles.

Parmi ceux qui se procurent des antivirus, pare-feu et autres technologies de sécurité pour protéger leurs systèmes, les investissements demeurent relativement faibles. Par exemple, 32 % des personnes interrogées dépensent entre 10 $ et 50 $ par année, 21 % dépensent entre 50 $ et 100 $ et seulement 12 % dépensent plus de 100 $ par année.

Selon votre estimation, combien dépensez-vous pour des antivirus, pare-feu et autres technologies de sécurité pour votre réseau?



Quels types de logiciels de sécurité utilisez-vous actuellement pour protéger vos ordinateurs et appareils personnels?



Pour ceux qui ont investi dans un logiciel de sécurité pour leurs appareils personnels, les trois types de logiciels les plus utilisés sont les pare-feu (78 %), les protections antivirus (73 %) et les logiciels antipourriel (56 %). Parmi les autres types de logiciels de sécurité utilisés, on compte les filtres de contenu Web (41 %) et les gestionnaires de mots de passe (42 %).

RÉSULTATS DU SONDAGE : PETITES ENTREPRISES CANADIENNES

En plus de recueillir les réponses des propriétaires de domaines personnels, nous avons aussi interrogé les propriétaires d'un domaine .CA ou plus qu'ils utilisent exclusivement à des fins d'entreprises. Les entreprises comprennent les petites entreprises de 100 employés et moins et des organisations de plus de 100 employés. Parmi les plus grandes organisations, on compte 58 % de sociétés, 34 % d'organismes sans but lucratif et 8 % d'organisations gouvernementales.

Résultats du sondage : Petites entreprises canadiennes

En plus de recueillir les réponses des propriétaires de domaines personnels, nous avons aussi interrogé les propriétaires d'un domaine .CA ou plus qu'ils utilisent exclusivement à des fins d'entreprises. Les entreprises comprennent les petites entreprises de 100 employés et moins et des organisations de plus de 100 employés. Parmi les plus grandes organisations, on compte 58 % de sociétés, 34 % d'organismes sans but lucratif et 8 % d'organisations gouvernementales.

Nous avons posé à ces groupes une série de questions adaptées à la taille des organisations. Ces questions visaient à obtenir leurs perspectives sur leur connaissance des menaces actuelles, des conséquences de ces menaces et des mesures prises pour remédier à ces menaces, y compris les solutions de sécurité des TI utilisées actuellement et les investissements liés à ces solutions.

Dans la catégorie des petites entreprises, la majorité des répondants (72 %) indiquent qu'ils sont les principaux responsables des opérations et de la sécurité des TI de l'entreprise, tandis que 11 % des répondants affirment qu'ils se fient à des ressources techniques internes et 17 % utilisent un fournisseur externe ou un entrepreneur en TI.

Parmi les répondants qui travaillent pour de plus grandes organisations, qui comprennent des entreprises du secteur privé, des organismes sans but lucratif et des organisations gouvernementales, 90 % indiquent qu'ils sont impliqués dans le processus décisionnel lié à la sécurité des TI.

Les cybermenaces représentent une source importante de préoccupations pour les entreprises canadiennes

Comme leurs homologues qui gèrent leurs sites Web personnels avec des domaines .CA, les propriétaires de domaines d'entreprises sont très préoccupés par les conséquences potentielles de cyberattaques sur leurs opérations.

Dans l'ensemble, 77 % des répondants propriétaires de petites entreprises évaluent leur niveau de préoccupation à 7 et plus, 1 étant « aucunement préoccupé » et 10 étant « très préoccupé ».

Une proportion importante des répondants — environ 1/5 au total — établissent leur préoccupation au niveau le plus élevé, indiquant qu'ils sont « très préoccupés » par les conséquences qu'une cyberattaque pourrait avoir sur leurs entreprises.

Parmi les plus grandes organisations, les répondants indiquent qu'ils sont inquiets des conséquences de l'hameçonnage et des logiciels rançonneurs sur leurs organisations, avec 16 % indiquant qu'ils sont « assez inquiets » des logiciels rançonneurs et 57 % indiquant qu'ils sont inquiets ou très inquiets, entre 7 et 10 dans l'échelle.

L'hameçonnage représente aussi une préoccupation importante pour les plus grandes organisations, avec 18 % des répondants qui indiquent qu'ils sont « assez inquiets » et 55 % qui indiquent qu'ils sont inquiets ou très inquiets.

Le degré de préoccupation des entreprises canadiennes est justifié par les résultats de la recherche effectuée dans le Dossier documentaire 2017 de l'ACEI, qui indiquent que 44 % des Canadiens sont peu enclins à continuer d'effectuer des achats en ligne à la suite d'une cyberattaque d'envergure.

Dans l'ensemble, 77 % des répondants propriétaires de petites entreprises évaluent leur niveau de préoccupation à 7 et plus, 1 étant « aucunement préoccupé » et 10 étant « très préoccupé ».

L'impact et la fréquence des cyberattaques augmentent au Canada

Comme pour les sites Web personnels, l'impact des cyberattaques dans un contexte canadien des affaires est une cause importante d'inquiétude. La fréquence de ces attaques augmente quotidiennement, particulièrement pour les plus grandes organisations.

22 % des répondants liés à de grandes organisations — près d'un quart des répondants de cette catégorie — indiquent que leur organisation a été ciblée par une attaque DDoS au cours de la dernière année, ce qui a eu un impact négatif sur le rendement.

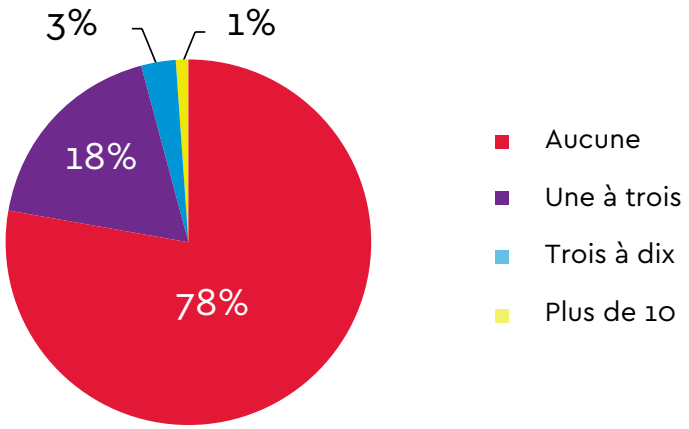
Dans l'ensemble, 17 % des répondants ont indiqué que leur organisation avait été la cible d'une à trois attaques DDoS, 3 % ont subi entre trois et dix attaques et 2 % plus de 10 attaques.

Les résultats sont semblables pour les logiciels rançonneurs, avec 19 % des répondants de cette catégorie qui affirment que leur organisation a été victime d'une attaque de ce type de logiciel. 17 % des répondants indiquent que leur organisation a subi entre une et trois attaques, contre 2 % qui ont été victimes entre trois et dix fois.

Les attaques d'hameçonnage représentent aussi une grande cause d'inquiétude pour les grandes organisations, avec 32 % des répondants indiquant que des utilisateurs au sein de leur organisation avaient involontairement divulgué des renseignements importants à des pirates informatiques au cours de la dernière année.

Les résultats sont semblables pour les logiciels rançonneurs, avec 19 % des répondants de cette catégorie qui affirment que leur organisation a été victime d'une attaque de ce type de logiciel.

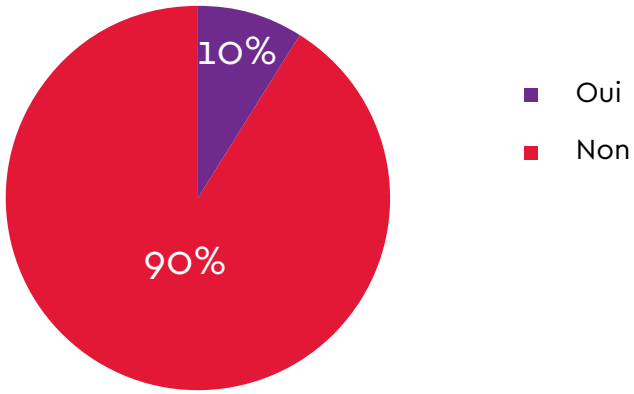
Au cours des 12 derniers mois, combien d'attaques DDoS ayant eu une incidence sur le rendement ont été perpétrées?



Les résultats étaient semblables pour les petites entreprises canadiennes. Le nombre de petites entreprises canadiennes qui ont été touchées par des cyberattaques, même s'il représente moins de la moitié du taux indiqué pour les grandes organisations, est important et représente une source de préoccupation.

10 % des répondants dans la catégorie des petites entreprises indiquent que leur site Web a été paralysé par un piratage ou une cyberattaque au cours des 24 derniers mois.

Au cours des 24 derniers mois, votre site Web a-t-il été piraté ou paralysé par une cyberattaque réelle ou soupçonnée?

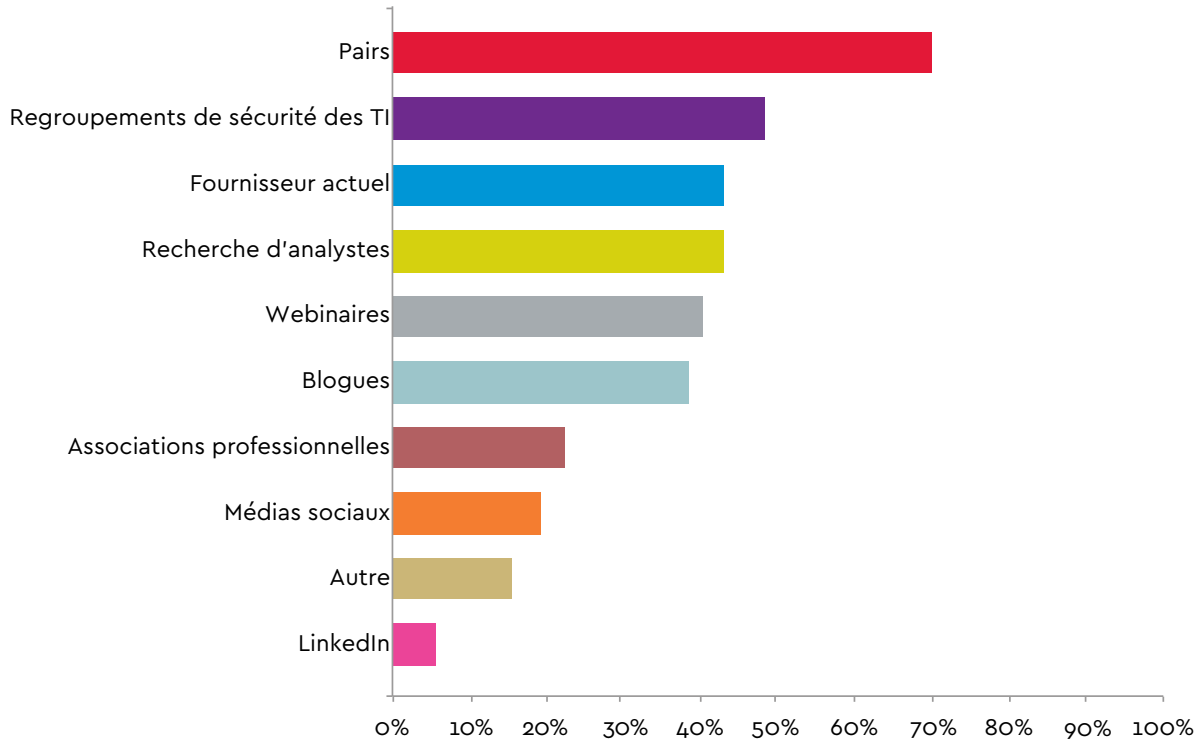


Les entreprises canadiennes considèrent leurs homologues dans le domaine de la cybersécurité comme des ressources dignes de confiance

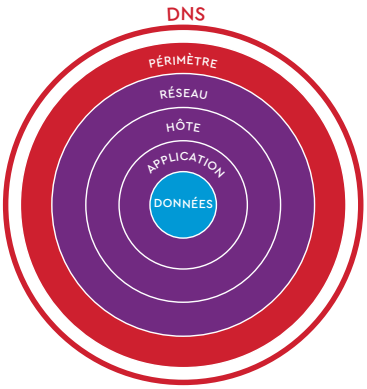
En matière de ressources d'éducation pour les professionnels des TI sur les services de sécurité, les répondants des petites entreprises et des grandes organisations ont indiqué que leurs pairs représentaient leur principale référence. Nous avons exclu les moteurs de recherche de cette question pour inclure les autres ressources choisies par les organisations.

Les petites entreprises se tournent vers leur fournisseur actuel (35 %) et les blogues (32 %) comme deuxième et troisième choix, tandis que les répondants des grandes entreprises choisissent les regroupements de sécurité des TI (48 %) et leur fournisseur actuel (43 %).

Où prenez-vous l'information dont vous avez besoin pour vous renseigner sur les services de sécurité des TI (en excluant les moteurs de recherche)



Les entreprises canadiennes reconnaissent la valeur de la défense en profondeur



Les petites et grandes entreprises canadiennes reconnaissent la valeur des couches de cybersécurité et investissent dans une gamme de solutions de sécurité des TI pour se protéger — un concept que nous appelons la défense en profondeur.

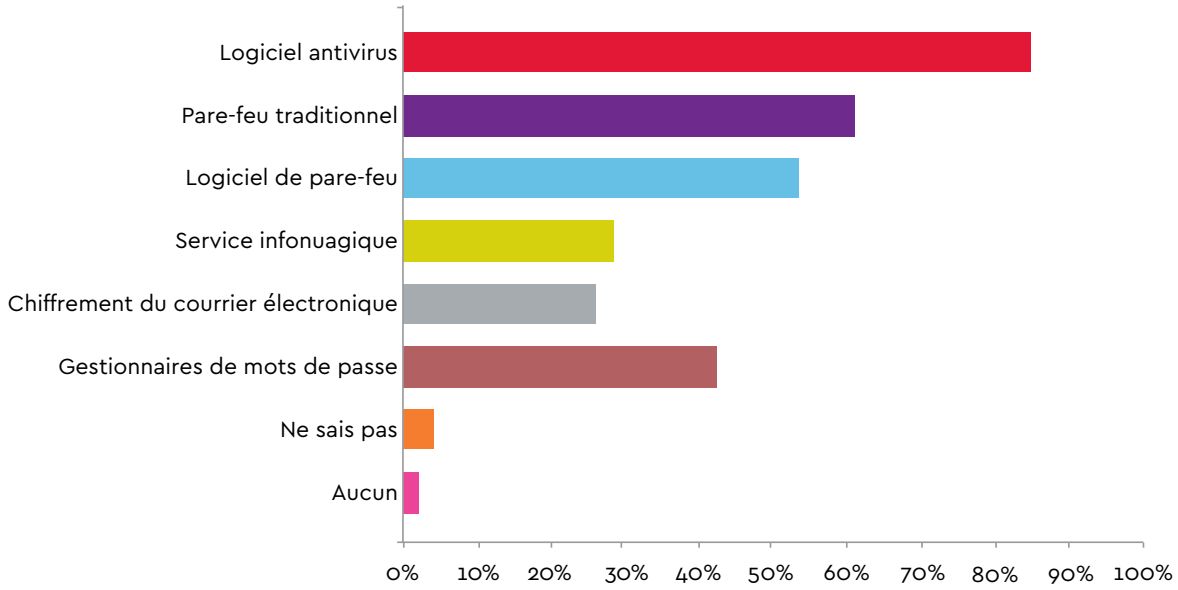
La locution « défense en profondeur » est d'origine militaire et consiste à miser sur plusieurs couches de défense (chacune possédant différentes aptitudes) pour se protéger mutuellement et protéger le centre. Le pare-feu DNS est donc une première couche de protection extérieure de l'entreprise qui peut être comparée à la protection aérienne d'un champ de bataille. Doté d'une perspective unique et de capacités de détection rapide des menaces, il peut stopper les activités malveillantes avant qu'elles n'atteignent votre réseau.

Sur le plan des appareils individuels, les répondants des petites entreprises indiquent qu'ils utilisent différents types de solutions de protection. 84 % des répondants affirment qu'ils utilisent un logiciel antivirus, tandis que 61 % utilisent des pare-feu matériels et 54 % comptent sur des logiciels de pare-feu.

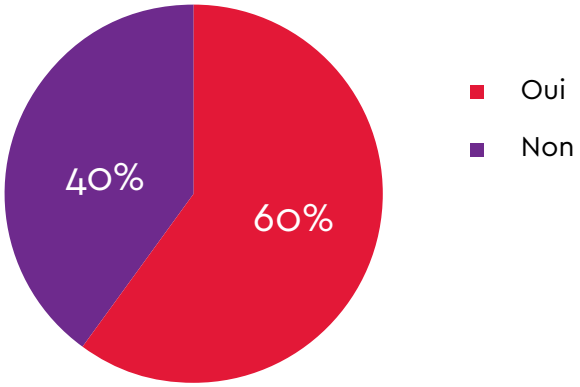
Parmi les autres systèmes utilisés par les petites entreprises, on compte les gestionnaires de mots de passe (42 %), le chiffrement du courrier électronique (26 %) et les systèmes infonuagiques, qui bloquent les requêtes malveillantes comme les maliciels et les liens d'hameçonnage.

Une majorité de répondants des grandes organisations (60 %) indiquent qu'ils utilisent des solutions de sécurité qui bloquent les requêtes DNS malveillantes et que cette méthode leur permet de se protéger des maliciels et de l'hameçonnage. De cette proportion, un pourcentage étonnant de 55 % des répondants indiquent qu'ils bloquent du contenu (filtrage Web) avec cette méthode. Nous croyons que ce type de blocage est effectué en combinant les serveurs récursifs sur place, les pare-feu traditionnels et les pare-feu DNS infonuagiques. Nous n'avons pas poussé les recherches plus loin dans le sondage, car la plupart des organisations suivent l'adage « sécurité par l'obscurité » et ne répondent pas à des questions très pointues sur leur système de sécurité.

Quels logiciel ou matériel utilisez-vous pour vos ordinateurs et appareils?



Utilisez-vous des outils qui protègent contre les logiciels malveillants et l'hameçonnage au niveau du DNS?



Conclusion

Notre premier sondage sur la cybersécurité auprès des titulaires .CA de domaines pour entreprises démontre que le Canada n'est pas à l'abri des cybermenaces qui planent sur les organisations d'autres pays. Les répondants sont très préoccupés par les risques et investissent dans plusieurs solutions pour les minimiser. Malgré tout, les malfaiteurs continuent leurs attaques. Par conséquent, les améliorations de la sécurité sont essentielles pour toute organisation qui utilise la technologie.