INTERNET | LA CYBERCRIMINALITÉ, MAL DU XXIe SIÈCLE

Les PME, premières vic

Les dirigeants de PME sont conscients de la fragilité de leur système informatique face à l'agressivité des hackers. L'UCM a mené l'enquête et confirme la tendance, chiffres à l'appui.

Ce ne sont pas moins de 284 indépendants ou chefs de PME qui ont répondu à cette enquête, menée en collaboration avec l'Agence pour l'entreprise et l'innovation (AEI) et l'Agence du numérique (AdN). Une enquête consacrée à la cybersécurité et qui d'emblée, révèle que les PME sont conscientes que cette problématique les concerne aussi. D'ailleurs, seuls 2 % d'entre elles considèrent la cybersécurité comme l'affaire des grandes entreprises. Près de neuf entrepreneurs sur dix accordent de l'importance à la sécurité informatique de leur entreprise, et c'est le patron qui s'en charge dans près de deux tiers des cas (62,3 %).

Par contre, les patrons sont peu au courant des mesures publiques existantes pour les soutenir dans ce domaine : à peine 16 % connaissent la déduction fiscale pour les investissements en sécurité informatique. Le point de contact fédéral en matière de cybersécurité n'est, lui, connu que d'une PME sur dix seulement. Même résultat pour les guides et sites recensant les bonnes pratiques.

Poursuivre les délinquants

L'étude a apporté une bonne nouvelle puisque les pratiques des PME en matière de cybersécurité semblent s'améliorer. Plus de neuf sur dix (94 %) utilisent un antivirus, 70 % protègent leurs accès wifi, 62,8 % mettent régulièrement à jour leurs logiciels et plus de la moitié (58 %) réalisent des sauvegardes hebdomadaires de leurs données. Les tests de sécurité réguliers ainsi que le cryptage des données stockées ne sont effectués que par un répondant sur dix à l'enquête.

Une part importante des répondants (61,3 %) utilise régulièrement ou constamment internet à des fins privées sur un appareil professionnel, ce qui accroît les risques. Près de cinq PME sur dix n'ont rencontré aucun couac lié à la cybersécurité, ce qui est en soi positif.

Trois problèmes principaux ont été identifiés : la perte de données suite à un virus (19 %), le piratage de compte de messagerie (17,4 %) et l'usurpation d'adresse électronique (15,6 %).

Lorsqu'un problème s'est présenté, l'indépendant ou la PME n'a porté plainte auprès des autorités que dans 18 % des cas, plus de la moitié d'entre elles ont eu recours aux compétences d'un professionnel afin de régler le problème. On constate également de manière assez rassurante que dans deux tiers des cas (62,5 %), les entreprises qui ont rencontré un problème lié à la cybersécurité n'en ont subi aucune conséquence.

Les attentes et besoins des PME en matière de lutte contre la cybercriminalité sont très diversifiés mais trois priorités se dégagent : une répression plus forte des piratages informatiques, une baisse des coûts d'acquisition de certains logiciels de sécurité ou systèmes de sauvegarde, et enfin

Recommandations aux entrepre

Pour une PME, peu importe sa taille et son degré d'utilisation des outils informatiques, investir dans la sécurité est devenu une nécessité face au développement de la cybercriminalité. Concrètement, comment faire ? Des experts ont rédigé des guides, édités par l'Unizo (l'équivalent flamand de l'UCM), la Fédération des entreprises de Belgique (FEB), la CGPME (Confédération générale du patronat des petites et moyennes entreprises, en France)... L'UCM a compilé et synthétisé les conseils les plus utiles et souvent cités dans ces publications. Il s'agit généralement de questions de bon sens mais adopter ces petits réflexes peut faire la différence.

Faire un backup journalier de ses données reste la meilleure manière de limiter les conséquences de la plupart des problèmes que l'on peut rencontrer. S'assurer en outre que ces backups soient stockés dans des endroits distincts, et de préférence éloignés des sources copiées et non connectés au poste de travail principal.

Mettre régulièrement ses logiciels et en particulier son antivirus à jour afin d'être protégé contre les nouvelles menaces et sécuriser ses accès wifi, tout en dotant ses appareils mobiles (GSM, smartphone, tablette...) de mot de passe est une bonne alternative. Également être vigilant dans la manipulation des clés USB et disque dur externe qui contiennent des données sensibles. Utiliser des mots de passe complexes et les modifier régulièrement. Surtout, ne pas les écrire, a fortiori sur un support qui se trouve à proximité des outils qu'ils protègent. Ensuite, éviter d'utiliser à des fins personnelles des outils professionnels, expressément lorsqu'il s'agit de télécharger des logiciels ou d'acheter en ligne. Enfin, on

© Ph. Turpin/Belpress.com

times des hackers

les réductions/déductions fiscales sur les investissements de sécurisation de l'infrastructure informatique.

neurs

ne peut qu'inciter à recourir aux points de contact et outils existants en matière de cybercriminalité (Cert, l'équipe d'intervention d'urgence en sécurité informatique fédérale) en cas d'incident et à déposer plainte auprès de la police. Cela n'aura pas toujours d'effet direct mais permettra aux autorités de mieux poursuivre les cyberdélinquants.

Le conseil en or serait de suivre une formation en "intelligence stratégique". Il s'agit d'une pratique managériale de gestion de l'information qui se traduit de manière concrète en actions de veille (captation de l'information), d'influence (capitalisation de l'information) et de protection de l'information dont la cybersécurité.

L'Agence pour l'entreprise et l'innovation propose formations et accompagnements en la matière.

infos-entreprises.be/fr/intelligence-strategique-formation-2603

Recommandations aux pouvoirs publics

À partir des constats de l'enquête, l'UCM formule une série de propositions à l'intention des pouvoirs publics.

En priorité, elle demande de renforcer l'investissement des pouvoirs publics en matière de répression de la cybercriminalité qui risque de devenir bientôt aussi problématique que d'autres formes de criminalité comme les vols à l'étalage ou les cambriolages pour les PME.

Ensuite, il faut faire connaître les outils publics existants, comme la déduction fiscale fédérale en matière d'investissement en sécurité informatique. Cette dernière pourrait d'ailleurs être adaptée pour couvrir des investissements légers en matière de cybersécurité tels que les systèmes de sauvegarde des données.

De même, au niveau régional, la consultance en matière de sécurité informatique devrait être intégrée dans le dispositif "petites aides" wallon avec un taux d'intervention plus élevé pour les TPE.

Enfin, il est essentiel de continuer à sensibiliser, en partenariat avec l'UCM, les PME et indépendants aux bonnes pratiques en matière de cybersécurité via des guides pratiques adaptés aux PME ou encore des outils d'auto-évaluation des entreprises quant à leur niveau de cybersécurité. Cela passe également par la mise en place de formations adaptées aux indépendants et PME qui viendraient en complément de l'accompagnement par des experts qualifiés.

"Plus jamais de site internet !"

Sébastien Schoonbroodt est décorateur en région liégeoise. En 2012, sur les conseils de sa graphiste, il achète un nom de domaine et crée un site internet. "Assez rapidement, j'ai reçu un mail de la société, me disant qu'elle n'avait pas su prélever le montant de la réservation du nom de domaine. J'ai forcément demandé une facture en bonne et due forme, reçue quelque temps plus tard mais sans numéro de compte ! Je n'ai pas su faire le paiement, et heureusement car la société s'est approprié mon site et l'a dévié. Je ne maîtrise plus rien, et cela m'a fait perdre certainement pas mal de clients car ma camionnette avait été lettrée du nom du site, qui ne renvoyait à rien. J'ai bien essayé de faire valoir mes droits mais vous communiquez avec des machines quand vous envoyez un mail."

Sébastien ne recréera pas de sitôt un site internet !

Sébastien est maintenant très méfiant. "Je n'aurai jamais plus de site internet ! J'utilise la bonne vieille méthode du bouche à oreille, même si je reçois des propositions de création de site quasi toutes les semaines."

Deux conseils de la Police fédérale


Olivier Bogaert.

Olivier Bogaert est commissaire à la Computer crime unit, la section de la Police fédérale spécialisée dans la traque de la cybercriminalité. L'homme en voit des vertes et des pas mûres ! "Les entreprises sont le plus souvent victimes de deux sortes de piratage. D'abord, le mail qui invite à cliquer sur un lien, permettant d'installer un virus qui crypte l'entièreté des données. Je pense au récent exemple d'un mail utilisant l'image de Bpost. Ensuite, ce qu'on appelle "la fraude au président", qui consiste en un mail frauduleux, soi-disant envoyé par un manager (en déplacement) à la personne en charge des opérations financières, qui autorise un versement dans les plus brefs délais. Michelin vient de perdre deux millions d'euros de la sorte." Des manipulations rendues possibles grâce à l'hypercommunication d'employés détaillant leur vie professionnelle sur des réseaux sociaux pros. Les hackers n'ont aucune peine à identifier le "who's who" de l'entreprise et suivre les déplacements des managers, avec les conséquences que l'on connaît.

"Deux conseils : faire des backups réguliers et déconnecter les disques durs externes contenant ces informations du reste de l'installation informatique, et ne jamais surfer sur un wifi public avec son PC pro. Cela équivaut à partager les données de l'entreprise avec le monde entier."