PETITES ENTREPRISES

Voici trois mesures simples qui vous aideront à protéger votre entreprise contre les cyberattaques.

Bonne nouvelle, il est infiniment plus simple d'éviter une cyberattaque que d'essayer de s'en remettre.

Bon nombre de propriétaires de PME pensent que cela n'arrive qu'aux autres et que leur entreprise est trop petite pour être la cible de piratages, d'attaques par rançongiciel et d'autres types de cybercriminalité. D'autres sont conscients de l'importance de la cybersécurité, mais estiment qu'ils n'ont pas les ressources nécessaires pour en faire une priorité. Ce sont là quelques-unes des raisons pour lesquelles **pas moins de 90 % des PME n'ont pas établi de système de protection pour leurs données ou celles de leurs clients.**[1]

Les cybercriminels ont pris conscience de ces vulnérabilités. Dans une autre étude récente, plus d'une PME sur cinq a déclaré avoir déjà été victime d'une cyberattaque.[2]

Il faut parfois plusieurs mois avant qu'une société se rende compte qu'elle a été victime d'une cyberattaque et, à ce moment-là, les dommages causés sont importants : les coûts moyens s'élèvent alors à entre 84 000 et 148 000 dollars, sans parler de la perte de confiance des clients.[3] Trop souvent, ces dommages sont insurmontables. Une étude de Better Business Bureau de 2017 a révélé que « seulement 35 % des entreprises pourraient rester rentables pendant plus de trois mois si elles perdaient définitivement l'accès aux données essentielles."[4]

MESURE Nº 1 :

Restreindre l'accès

Les hackers sont très doués pour contourner les mots de passe. Ils trouvent souvent un moyen soit de les deviner, soit de les voler. C'est pourquoi les experts en sécurité recommandent d'ajouter une couche de protection supplémentaire souvent appelée « authentification à deux facteurs » ou « authentification multi-facteurs ». L'ajout de cette deuxième barrière est un moyen efficace d'éloigner les hackers. Voici quelques exemples d'authentification multi-facteurs souvent utilisés au niveau du matériel informatique ou sur des sites Web et applications populaires :

Un code PIN à quatre chiffres ou une réponse secrète à une question, comme : « Quel était le nom de votre premier animal domestique ? »

Un code unique envoyé par SMS/Texto (forme la plus populaire)

Des capteurs biométriques qui permettent un accès incroyablement rapide et personnalisé, comme les scanners rétiniens, les lecteurs de reconnaissance faciale ou d'empreintes digitales. Par exemple, les ordinateurs portables Latitude et certains PC Vostro équipés de Windows Hello permettent aux utilisateurs de se connecter en toute sécurité d'un simple geste ou d'un simple regard.

MESURE Nº 2 :

Repérer et éviter les menaces

Le mot anglais « Malware », contraction de « malicious software » (logiciel malveillant), est un terme générique qui englobe une multitude d'envahisseurs néfastes : logiciels espions, virus, chevaux de Troie, rootkits, rançongiciels, pour n'en citer que quelques-uns. Les perturbations qu'ils provoquent peuvent aller de la panne d'ordinateur à l'usurpation d'identité, en passant par l'arrêt complet du réseau dans le cas d'une demande de rançon. Le hacker vous empêche alors d'accéder à vos données jusqu'à ce que vous lui versiez une rançon.

L'un des moyens les plus courants pour infiltrer le système d'un collaborateur est l'hameçonnage par e-mail. Ces e-mails semblent bel et bien légitimes. Cependant, si votre collaborateur clique sur un lien dans cet e-mail, il pourrait être invité à fournir des informations sensibles, ou un logiciel malveillant pourrait pénétrer dans le système. Sensibilisez vos collaborateurs à l'importance de contrôler minutieusement les e-mails et les URL pour y déceler tout signe suspect (fautes d'orthographe dans une URL, par exemple) avant de cliquer sur ceux-ci.

McAfee

Outre la vigilance des collaborateurs, des sociétés de logiciels comme McAfee proposent une protection transparente qui s'exécute automatiquement en arrière-plan et qui recherche tous types de menaces et les élimine avant qu'elles n'aient une chance de pénétrer dans le système. Un package logiciel complet peut également avertir les utilisateurs du risque de certains sites Web et contribuer à prévenir les téléchargements dangereux.

MESURE Nº 3 :

Prévoir un plan de sauvegarde

Les propriétaires de PME en arrivent à prévoir l'inattendu : erreurs, pannes de systèmes, surprises. Bien que les deux premières mesures que nous avons évoquées permettent d'éliminer un grand nombre de menaces, une brèche est toujours possible. Si vous utilisez un système de sauvegarde, il vous sera alors beaucoup plus facile de récupérer vos données. Il existe deux solutions de sauvegarde principales : une solution matérielle comme les disques de stockage ou une solution de stockage Cloud (serveurs sur site).

Les disques durs externes sont simples d'utilisation : il vous suffit de les brancher, de télécharger vos données et ensuite de les stocker. L'inconvénient est qu'ils ont besoin d'un système de refroidissement et qu'ils occupent un espace physique, ce qui implique un risque de perte ou d'endommagement.

mozy BY DELL

Sinon, la protection des données dans le Cloud proposée par des sociétés comme MozyPro constitue une solution pratique. Vous n'aurez plus à vous soucier de télécharger manuellement vos données sur des disques durs et à les stocker physiquement quelque part.

Une fois vos données téléchargées, MozyPro détecte automatiquement les modifications et les enregistre dans le Cloud, en synchronisant les changements sur tous vos appareils. Cette solution assure également la sécurité de vos données grâce à un chiffrement de qualité militaire et offre une couche de protection supplémentaire contre les attaques par rançongiciel. Une attaque par rançongiciel ne fonctionne que si vous n'avez aucun autre moyen d'accéder à vos données. La sauvegarde dans le Cloud rend par conséquent ce genre d'attaque inefficace.

Des questions ? Les conseillers Dell spécialisés en technologies pour les PME sont prêts à vous aider en vous proposant des solutions de sécurité fiables afin de protéger votre entreprise.

CONTACTEZ UN CONSEILLER DÈS AUJOURD'HUI AU :

0801 800 001*

CLIQUEZ | APPELLEZ | CHATTEZ

[1] https://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron | [2] https://www.bbb.org/stateofcybersecurity/
[3] https://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron | [4] https://www.bbb.org/stateofcybersecurity/

*09h00-18h00 du lundi au vendredi Numéro Vert Gratuit.