6 contrôles de sécurité à privilégier pour les PME (et un bonus)

DOCUMENT TECHNIQUE

La cybersécurité peut causer bien des maux de tête aux petites et moyennes entreprises (PME), mais elles ne disposent généralement pas des mêmes ressources qu'une grande organisation pour contrer les attaques. Voici quelques conseils et astuces pour les PME qui cherchent à protéger leurs actifs numériques.

Les menaces et les attaques de cybersécurité ne connaissent pas de frontières. Elles apparaissent dans les centres de données, à la périphérie du réseau, dans les bureaux distants et partout où les employés accèdent à des applications, des données ou des services via le réseau de l'entreprise ou le Web. C'est pourquoi les entreprises qui n'ont pas de gros budgets, de centre d'opérations et de sécurité de l'information (communément appelé SOC de l'anglais security operations center) ou d'abonnements à des services de renseignement sur les menaces en temps réel ne veulent pas se retrouver dans une situation de vulnérabilité.

Pour les PME, les enjeux sont de taille :

- 58 % des victimes d'attaques par logiciel malveillant sont des PME.
- Les cyberattaques ont coûté en moyenne plus de 2,2 milliards de dollars aux PME en 2017.
- 60 % des PME affirment que les attaques sont de plus en plus graves et sophistiquées.
- 81 % des PME constatent que les attaques et les logiciels malveillants ont échappé à leurs solutions antivirus.

1 "2018 Data Breach Investigations Report", Verizon, avril 2018.
2 "2017 State of Cybersecurity in Small & Medium-Sized Businesses", Ponemon Institute, septembre 2017.
3 Ponemon, Ibid.
4 Ponemon, Ibid.

Devolutions
Devolutions Server
TechTarget | Custom Media

Une chose que les PME peuvent faire en matière de cybersécurité est d'avoir une bonne planification, ce qui leur permettra de prendre des décisions intelligentes et opportunes sans avoir à embaucher un grand nombre d'analystes SOC ou à implorer le conseil d'administration pour obtenir des fonds supplémentaires. Pour aider les PME à établir les bonnes priorités en matière de sécurité, voici une liste de suggestions accompagnées des commentaires du Chef de la sécurité de Devolutions.

1 : Sécurisez la gestion des accès à distance.

Vos employés travaillent de plus en plus en dehors du traditionnel « bureau », que ce soit à domicile, chez des clients ou des espaces publics disposant du Wi-Fi. Assurez-vous de pouvoir gérer les accès de vos employés en toute sécurité, peu importe où ils travaillent.

Conseil d'expert : l'utilisation des RPV IPSEC et SSL est fortement recommandée lorsqu'il s'agit de sécuriser l'accès à distance. Ils sont faciles à déployer et abordables. Les services infonuagiques sont également excellents pour la mobilité et la disponibilité, mais assurez-vous de bien comprendre les risques associés et les limites des responsabilités de votre fournisseur de services. Les liens de communication doivent utiliser un chiffrement fort et un solide processus d'authentification.

2 : Utilisez un coffre sécurisé.

Comme de plus en plus d'entreprises font des affaires en ligne, elles doivent s'adapter et sécuriser tout : des mots de passe des employés à la propriété intellectuelle, en passant par les dossiers privés. C'est particulièrement difficile pour les PME, parce que la plupart n'ont que peu ou pas de visibilité sur les pratiques de gestion des mots de passe de leurs employés. Un coffre numérique sécurisé peut être utile dans ce cas, parce qu'il permet aux employés de stocker en toute sécurité les mots de passe et les informations d'identification numériques, tout en donnant aux organisations la possibilité de repérer les problèmes potentiels dans la façon dont leurs employés utilisent les mots de passe.

Conseil d'expert : De nombreuses brèches de sécurité sur internet entraînent une perte de données instantanée, parce que les informations confidentielles et privées n'ont pas été correctement sécurisées. La plupart des PME ont tendance à ne pas prendre cela en considération. Protégez soigneusement vos informations, autant celles qui se trouvent à l'interne que celles dans le nuage, en utilisant un coffre numérique sécurisé et bien chiffré.

3 : Sécurisez la gestion des mots de passe.

Actuellement, les organisations passent au numérique pour accéder à toutes sortes de ressources, des applications logicielles aux entrées des bâtiments. Bon nombre de ces ressources ne disposent pas de cadres de défense traditionnels en matière de cybersécurité. Il faut donc adopter une approche qui permette aux gentils d'entrer, mais qui bloquent les méchants.

Nous l'avons déjà mentionné, la sécurité des mots de passe va de pair avec la gestion des accès. Cette dernière couvre un large éventail d'applications et de cas d'utilisation. Par exemple, on doit s'assurer que les informations d'identification et les privilèges appropriés soient appliqués, qu'une gestion flexible et automatisée des politiques soit en place lorsque les employés changent de rôle. On doit aussi s'assurer que les identités soient vérifiées lorsque les employés se connectent à des applications, des bases de données et des services infonuagiques (ou même lorsqu'ils essaient d'entrer dans le bâtiment en dehors des heures de travail).

Conseil d'expert : Les feuilles de calcul protégées par mot de passe et autres solutions de gestion des mots de passe basées sur un seul utilisateur se sont avérées inefficaces pour les entreprises. Ces solutions sont difficiles à gérer et leurs fonctionnalités de sécurité sont limitées. Une solution centralisée, sécurisée et flexible permettra d'éviter, ou du moins de limiter, les impacts d'une éventuelle violation de données ou d'une attaque orchestrée par un employé mécontent.

4 : Implantez l'authentification multifacteur.

Ce n'est pas la fin des mots de passe, mais ils ne sont plus la seule mesure à prendre pour renforcer la sécurité. Les PME doivent se familiariser avec les clés numériques, la biométrie et d'autres compléments aux mots de passe traditionnels. Si vous ne comptez que sur les mots de passe, vous courrez un risque important. (Et ne pensez pas que vos employés trompent qui que ce soit en utilisant « mot de passe » comme mot de passe ou en plaçant un Post-it avec leur mot de passe à la vue de tous sur leur bureau.) L'authentification multifacteur est la voie que toutes les PME doivent suivre.

Conseil d'expert : L'authentification multifacteur sur le périmètre de réseau n'est même plus une option de nos jours. Les attaques par force brute ou de type « pulvérisation de mots de passe » sont largement utilisées par les pirates pour tenter de deviner les informations d'identification des utilisateurs. Ces attaques sont courantes et se produisent quotidiennement, même sur Outlook 365. Ils connaissent les adresses électroniques de votre entreprise : elles ne sont pas difficiles à trouver ou à deviner. Protégez vos actifs avec une véritable authentification à deux facteurs, combinant quelque chose que vous savez avec quelque chose que vous avez ou quelque chose que vous êtes.

2 Why small and mid-sized businesses are a huge target for cyber attacks CSO from IDG, octobre 2017

3 2016 State of Cyber Security in Small & Medium Size Businesses, *Ponemon Institute*, juin 2016

4 DDoS attack on Dyn came from 100,000 infected devices, *Computerworld*, octobre 2016

5 : Automatisez, automatisez, automatisez.

Il existe un fossé énorme et croissant entre le nombre d'offres d'emploi en cybersécurité et le nombre de personnes qualifiées pour occuper ces postes. Bien sûr, vous devez faire de l'embauche d'experts en cybersécurité une priorité (que ce soit pour le personnel interne ou par l'intermédiaire de spécialistes externes), mais vous ne résoudrez pas ce problème simplement en intensifiant le recrutement dans les universités ou en débauchant les talents de vos concurrents. Grâce aux nouveaux outils, les petites entreprises peuvent plus facilement gérer les problèmes de sécurité sans avoir à embaucher une armée d'ingénieurs ou à se doter d'un important centre d'opérations et de sécurité de l'information. Ces outils permettent également d'atténuer les problèmes de sécurité liés aux erreurs humaines.

Conseil d'expert : L'automatisation est un allié puissant pour renforcer la sécurité de bout en bout tout en évitant les erreurs humaines potentielles. Elle peut également accélérer les réponses aux incidents et les performances globales des opérations de sécurité. Cette valeur est ajoutée non seulement aux fonctions de sécurité, mais aussi aux fonctions d'exploitation. Si l'automatisation offre un retour sur investissement direct, sa mise en place nécessite des professionnels compétents (DevOps/DevSecOps) et les bons outils. Nous recommandons de faire appel à un expert en automatisation tant pour l'optimisation des opérations normales que pour les contrôles de sécurité afin d'optimiser votre utilisation des technologies d'automatisation.

6 : Formez vos utilisateurs finaux. Les meilleures pratiques de sécurité pour tous les types de PME et spécifiquement celles de votre organisation doivent être communiquées de manière claire et cohérente. Cette communication peut souvent provenir de votre chef de la sécurité ou de vos administrateurs système, mais elle doit également être soutenue de manière convaincante par la direction de votre entreprise. Vos dirigeants, y compris votre PDG et même votre conseil d'administration, doivent faire comprendre très clairement que la cybercriminalité est une menace majeure pour le bien-être de l'organisation et que prendre les mesures nécessaires pour assurer la cybersécurité est la responsabilité de tous, et pas seulement de l'équipe SecOps.

Conseil d'expert : La sécurité est l'affaire de tous. Les utilisateurs finaux jouent un rôle clé pour assurer la sécurité d'une entreprise. Ils sont des cibles communes et participent à l'ensemble de la détection, de la prévention et de l'atténuation de l'impact des incidents de sécurité. Cependant, pour qu'ils puissent remplir leur rôle, ils doivent partager la vision de la direction en matière de sécurité et être formés correctement. Un plan de sensibilisation à la sécurité de l'utilisateur final bien exécuté incitera vos employés à suivre les procédures de l'entreprise, à signaler les anomalies sans craindre des sanctions et à aider réellement votre équipe technique à résoudre les problèmes.

BONUS : CONSEIL DE NOTRE CHEF DE LA SÉCURITÉ

Comprendre et mesurer les risques.

Tous les contrôles mentionnés ici aideront votre organisation à atténuer les risques de cybersécurité liés aux menaces extérieures et intérieures. Cependant, les mêmes questions reviendront à chaque réunion avec la haute direction et le conseil d'administration : « Qu'en est-il du retour sur investissement? Utilisons-nous ici de l'argent qui pourrait être plus utile ailleurs? Est-ce que cela va ralentir les opérations? » Si votre programme de cybersécurité n'est pas bien compris et adopté par le conseil d'administration et les autres membres de la direction, il ne bénéficiera pas d'un budget et d'un soutien suffisants.

Pour obtenir les ressources nécessaires à l'implantation d'un bon programme en matière de cybersécurité, il faut d'abord que les dirigeants définissent leur tolérance au risque. Ensuite, les menaces de l'entreprise doivent être évaluées en fonction de ces limites afin de déterminer quels sont les risques inacceptables et les traiter en priorité. Pour les entreprises qui ne sont pas familières avec cette pratique, il a été prouvé qu'elle est très efficace lorsqu'elle est réalisée avec des partenaires expérimentés spécialisés dans l'évaluation des risques. Ainsi, votre direction générale comprendra mieux les risques liés à la sécurité et, par conséquent, vos demandes budgétaires.

Les risques sont généralement exprimés qualitativement comme « élevés », « moyens » ou « faibles ». Vous devez également miser sur des mesures quantitatives du risque. Par exemple, un risque élevé pourrait engendrer une perte supérieure à 1 million de dollars ou une exposition médiatique négative. Cela est particulièrement utile pour convaincre les décideurs, qui peuvent ainsi mieux comprendre les impacts financiers, plutôt que de se faire dire : « Votre compte de messagerie pourrait être piraté. »

5 Global Economic Crime Survey, *PwC*, 2016

DES CONSEILS PRATIQUES ET DES OUTILS DE QUALITÉ FOURNIS PAR UN CONSEILLER DE CONFIANCE : DEVOLUTIONS

Aucune PME ne peut faire cavalier seul en matière de cybersécurité. C'est pourquoi il est essentiel de travailler avec un tiers de confiance qui a des compétences techniques avancées en matière de cybersécurité et qui comprend comment mettre en œuvre et gérer les outils et services de cybertechnologie dans un contexte commercial réel.

Devolutions offre aux PME une large gamme de solutions technologiques pour garantir la sécurité et la disponibilité des données, des applications et des services, même face à l'augmentation du nombre, de la diversité et de la sophistication des cybermenaces. Depuis près de dix ans, Devolutions a aidé d'innombrables petites entreprises à devenir plus efficaces grâce à des outils de gestion innovants qui permettent à leurs employés de travailler de manière flexible, mais sécurisée depuis le centre de données d'un siège social jusqu'à la connexion au nuage d'un café équipé d'une connexion Wi-Fi.

Par exemple, Devolutions offre :

- **Devolutions Server**, un système de gestion des mots de passe pour les utilisateurs privilégiés et les utilisateurs professionnels qui permet de réduire les accès non autorisés aux actifs critiques et de prévenir les attaques internes.

- **Remote Desktop Manager**, un outil de gestion des accès privilégiés qui réduit les risques liés aux menaces internes et aux failles de sécurité, tout en contribuant à répondre aux exigences de gouvernance, d'audit et de conformité.

- **Devolutions Cloud**, un portail hautement sécurisé qui offre un large éventail de services infonuagiques, notamment les bases de données des utilisateurs, la sauvegarde en ligne, etc.

Pour plus d'informations sur la façon dont Devolutions peut aider les PME comme la vôtre à se protéger contre les menaces de cybersécurité, consultez le site https://devolutions.net/fr.