Ce que tous les cybercriminels savent :

Les petites et moyennes entreprises (PME) qui ont une cybersécurité faible ou inexistante sont des cibles idéales

CHUBB®

Collaborateurs :

Symantec™

COVERHOUND®

Lorsque la base de données de Rokenbok Education a été compromise par des cybercriminels, la petite entreprise californienne a catégoriquement refusé de payer une rançon élevée pour récupérer celle-ci. Elle s'est plutôt attelée à la reconstitution manuelle de son système de base et a repris ses activités quatre jours plus tard. Cela ne veut pas dire que l'entreprise spécialisée dans la conception de jouets éducatifs pour enfants n'a pas perdu des milliers de dollars de ventes pendant la période des fêtes de fin d'année en 2015. Rokenbok s'en sort bien mieux que de nombreuses petites entreprises confrontées aux menaces de rançongiciels et de maliciels, compte tenu du grand nombre de cyberrisques qui menacent de plus en plus les entreprises de toutes tailles.

En réalité, 93 % des petites et moyennes entreprises (PME) victimes d'un cyberincident ont déclaré que leur activité avait été gravement touchée. La plupart d'entre elles ont fait état d'une perte d'argent et d'épargne. 31 % ont mentionné une atteinte à leur réputation ayant entraîné la perte de clients, ainsi que des difficultés à attirer de nouveaux employés et à remporter de nouvelles affaires. Près de la moitié d'entre elles ont signalé une interruption de service ayant nui à leur capacité d'exploitation. Malgré ces chiffres, moins de 3 % d'entre elles ont souscrit une cyberassurance.

Qu'est-ce que l'effet domino?

Les risques liés à la cybersécurité représentent un défi particulièrement difficile pour les petites entreprises en raison des menaces fréquentes qui se manifestent sous la forme d'incidents de cybersécurité réels, des graves perturbations de l'activité et de leurs répercussions financières, ainsi que des ressources limitées dont disposent généralement les petites entreprises pour réagir face à un incident et s'en remettre. Cette cascade, phénomène que nous appellerons « l'effet domino », peut facilement conduire à la faillite de l'entreprise.

Le premier effet domino

Les attaques et la mise hors ligne des sites Web ou des systèmes informatiques des PME peuvent détruire leurs vitrines virtuelles et leur capacité à traiter des transactions. C'est comme si ces entreprises avaient cessé leurs activités, même si leurs points de vente traditionnels sont toujours ouverts. Par conséquent, les clients se tournent vers la concurrence et la plupart ne reviennent pas.

Le deuxième effet domino

Lorsqu'il s'agit d'un vol de données personnelles (par exemple, des numéros de carte bancaire), la spirale négative de la couverture médiatique et l'ébranlement de la confiance des clients peuvent considérablement entacher la réputation de la marque, et la perte de la clientèle peut ainsi ressembler à une fuite précipitée.

Le troisième effet domino

Les rançons informatiques peuvent atteindre des montants à six chiffres. Si la décision de payer une rançon est particulière à chaque cas (et officiellement déconseillée par le FBI), rien ne garantit qu'une fois la rançon payée, les cybercriminels coopéreront et décrypteront les données compromises. En outre, quel que soit le type d'incident de cybersécurité (rançon, code malveillant ou autre événement, malveillant ou non), la restauration des données numériques, des logiciels et des systèmes informatiques peut nécessiter un investissement en temps et en argent important et précipiter l'entreprise vers la faillite.

Le quatrième effet domino

Le dernier effet domino n'est pas le moins grave; en effet, les PME peuvent faire l'objet de poursuites en responsabilité lorsqu'une attaque touche des clients, des vendeurs, des fournisseurs ou d'autres personnes. Quelque que soit leur issue, de telles poursuites sont souvent si coûteuses et si longues qu'une cyberattaque peut devenir un moyen de mettre fin à l'existence d'une entreprise.

Plus de la moitié des cyberattaques sont dirigées contre des PME, et ce nombre ne cesse d'augmenter.

Pourquoi les PME sont-elles ciblées?

Compte tenu des résultats trop fréquents décrits ci-dessus, il convient de se poser cette question logique : Pourquoi les PME ne se protègent-elles pas davantage en adoptant des mesures de cybersécurité? Elles ont deux raisons communes de ne pas le faire.

La première raison

Il est naturel de craindre un risque que soi-même ou un proche a connu. Même si les cyberattaques font souvent la une des journaux, les grands titres concernent principalement les grandes entreprises. La cybermenace semble tout simplement irréelle pour la plupart des PME, mais en réalité, plus de la moitié des cyberattaques sont dirigées contre des PME, et ce nombre ne cesse d'augmenter.

Les cibles que les cybercriminels recherchent sur Internet sont des entreprises faciles à pirater. Ils y parviennent facilement au moyen de logiciels qui analysent automatiquement le Web et détectent les entreprises qui ont des faiblesses de sécurité précises (par exemple, un logiciel obsolète ou non protégé, de mauvaises pratiques en matière de mots de passe, des ports Web ouverts, des données non cryptées en transit, une protection insuffisante des points terminaux, etc.).

Par conséquent, il est de plus en plus probable qu'une PME qui présente des faiblesses en matière de sécurité sera rapidement détectée. Ces entreprises sont à la portée des cybercriminels. Non seulement ces entreprises sont des cibles faciles, mais elles offrent également un gain cumulatif substantiel, sous la forme d'une rançon, du vol de numéros de cartes de crédit ou les coordonnées de comptes bancaires, permettant ainsi aux criminels de détourner facilement de l'argent en quelques secondes numériques. Enfin, les criminels peuvent également éviter de faire davantage d'efforts et de prendre le risque de pirater des grandes entreprises ou des entités gouvernementales. Par conséquent, les PME, qui investissent peu ou pas du tout dans les mesures de cybersécurité sont en réalité la cible idéale des cybercriminels, et donc la plus fréquente.

La deuxième raison

Les grandes entreprises dépensent souvent des sommes considérables à la cybersécurité, des dizaines, voire des centaines de millions pour mettre en place des systèmes de défense très sophistiqués et de haute technologie. Les PME sont généralement confrontées aux mêmes menaces. Cependant, la plupart des PME n'ont pas les moyens de réaliser l'investissement nécessaire à la mise en œuvre d'une protection intégrale. Les risques demeurent donc importants.

Comment les cybercriminels s'introduisent-ils dans un système?

Les criminels ont recours à toutes sortes de moyens d'accéder au site Web ou au serveur interne d'une PME. Voici les quatre méthodes d'attaque les plus courantes :

- **Attaques contre les systèmes physiques :** Les cybercriminels peuvent accéder au serveur ou au matériel interne d'une PME par l'intermédiaire d'appareils électroniques insuffisamment protégés qui ont un accès légitime, par exemple, les ordinateurs portables, les ordinateurs de bureau, les tablettes et les supports amovibles comme les clés USB. Ils peuvent également s'introduire dans une salle de serveurs par effraction ou en piratant le réseau interne, donnant ensuite à des tiers criminels la possibilité d'exercer une surveillance. Une chose aussi anodine que le branchement d'une clé USB infectée sur un ordinateur ou un appareil connecté à un réseau interne peut déclencher une attaque.

- **Authentification et attaques par élévation de privilèges :** Les criminels peuvent accéder à des données sensibles lorsque les personnes dont l'accès est légitime utilisent des mots de passe très faibles et faciles à pirater, ou lorsque des employés autorisés à accéder à des données stockées au cœur du réseau de l'entreprise adoptent une approche laxiste et prennent peu de précautions à l'égard des mots de passe. Le Web invisible contient un vaste répertoire de milliards de combinaisons d'identifiants et de mots de passe compromis. La fréquence de réutilisation des combinaisons d'identifiants et des mots de passe permet à un cybercriminel de trouver facilement des identifiants valables pour un seul employé afin d'obtenir un accès. Le sabotage délibéré par un employé mécontent, ou même le fait d'autoriser les employés de base à accéder aux données sensibles, ce que l'on appelle « accumulation de privilèges », peuvent également être un autre facteur.

- **Perte de service :** Il existe deux façons de perdre le service, c'est-à-dire de ne pas pouvoir accéder au site Web d'une PME en raison d'un problème de service Internet. L'une provient d'une action humaine et l'autre de défaillances du service qui entraînent un manque de puissance ou l'impossibilité de se connecter à Internet. Les attaques par déni de service distribué (DDos) consistent généralement à inonder de trafic le fournisseur d'accès à Internet d'une PME afin de saturer la bande passante et rendre le site Web inutilisable. Les attaques non délibérées concernent les défaillances d'un seul point de service, en raison d'une dépendance excessive à l'égard d'un système ou d'un fournisseur de services sans redondances adéquates. Ces types de cyberincidents peuvent être causés par des catastrophes naturelles ou par de simples défaillances technologiques.

- **Attaques par contenu Internet malveillant :** C'est le type d'attaque que Rokenbok a subi. Le système de l'entreprise était infesté par un rançongiciel, une forme de logiciel malveillant qui permet aux criminels d'accéder à la base de données d'une entreprise et de la verrouiller en chiffrant les données et en demandant le paiement d'une rançon en échange de la clé de déchiffrement. Il existe de nombreux autres types d'attaques de contenu. Par exemple, l'hameçonnage consiste à envoyer à un employé un courriel contenant un lien qui, lorsqu'on clique dessus, télécharge automatiquement un logiciel malveillant sur l'ordinateur de l'employé. L'hameçonnage est souvent associé à des techniques d'ingénierie sociale pour faire croire que ces courriels proviennent d'un collègue ou d'une autre source interne. Les autres techniques sont des virus, des chevaux de Troie et des vers, ainsi que des téléchargements furtifs et des attaques d'applications Web.

Comment les PME peuvent-elles se protéger des cyberattaques?

Si empêcher les cybercriminels d'accéder aux fonds et aux données des PME semble être un défi colossal, les entreprises peuvent toutefois adopter un certain nombre de mesures pour créer leur propre programme de gestion des cyberrisques et limiter leur exposition. Après s'être assurées que leur antivirus et autres logiciels de sécurité sont à jour et avoir demandé à un consultant en cybersécurité de déceler les zones à haut risque, les PME peuvent prendre les cinq mesures d'atténuation des risques suivantes :

- **Élaborer et appliquer une politique officielle et écrite à l'égard des mots de passe :** L'un des moyens le plus rapide et le plus facile pour les cybercriminels d'accéder aux actifs des PME consiste à franchir la « porte ouverte » virtuelle que les employés leur fournissent au moyen de mots de passe faibles ou réutilisés. Pour remédier à cette situation, il est conseillé aux PME d'établir une politique exigeant des mots de passe robustes (par exemple, l'utilisation simultanée de lettres, de chiffres et de symboles) qui doivent être changés fréquemment. Il convient également de modifier les mots de passe automatiquement ou de marquer les comptes comme inactifs lorsque les employés quittent l'entreprise, au cas où un employé mécontent déciderait plus tard de nuire à l'entreprise en utilisant son ancien mot de passe. L'utilisation d'un bon logiciel de gestion des mots de passe peut faciliter cette étape cruciale.

- **Sensibiliser régulièrement tous les employés à la vigilance cyber :** Les PME devraient également informer leurs employés du rôle qu'ils jouent dans la prévention des cyberattaques. Il est facile d'introduire un logiciel malveillant dans le serveur de l'entreprise lorsque des ordinateurs portables ou d'autres appareils de l'entreprise sont utilisés en dehors du site puis connectés au réseau interne. La meilleure façon d'instaurer des habitudes saines et sûres au sein du personnel de votre entreprise est d'organiser régulièrement des formations. Il est tout aussi important d'instaurer une politique de restriction des données sensibles en n'autorisant l'accès qu'aux cadres formés ou à ceux qui ont besoin de ces données pour les opérations de l'entreprise.

Si empêcher les cybercriminels d'accéder aux fonds et aux données des PME semble être un défi colossal, les entreprises peuvent toutefois adopter un certain nombre de mesures simples pour créer leur propre programme de gestion des cyberrisques et limiter leur exposition.

- **Mettre à jour les équipements informatiques et déployer des logiciels de sécurité :** Les problèmes potentiels de cybersécurité sont faciles à résoudre lorsqu'il s'agit d'équipement informatique. Les systèmes d'exploitation et les ordinateurs obsolètes peuvent représenter un risque, car ils sont facilement accessibles aux criminels, étant vulnérables à des techniques de piratage plus sophistiquées et à de nouvelles formes de logiciels malveillants. Il est important que les PME surveillent simultanément les personnes qui ont un accès légitime à leur réseau informatique et le réseau lui-même pour détecter rapidement toute activité anormale, et ainsi limiter les dommages subis par l'entreprise. Bien que les PME ne disposent généralement pas d'experts en sécurité de l'information au sein de leur organisation, elles peuvent télécharger des logiciels de base qui déploient en quelques minutes certaines des solutions technologiques que les entreprises du classement Fortune 500 utilisent.

- **Établir un plan d'intervention en cas de cyberincident :** Si la plupart des PME ne disposent pas de l'expertise interne nécessaire pour résoudre une attaque majeure de cybersécurité, il existe des incidents moins dommageables qu'elles peuvent résoudre grâce à l'intervention d'une équipe d'experts en cybersécurité dédiée et préparée, composée à la fois d'employés et de prestataires de services externes. Une équipe entière travaillant sur un incident a l'avantage d'accélérer les délais de réponse et de résolution, selon les capacités de l'équipe.

- **Souscrire une cyberassurance :** Outre les mesures susmentionnées, les PME peuvent mieux protéger leurs actifs et la viabilité de leur entreprise en souscrivant une cyberassurance. Le coût de l'assurance sera toujours inférieur au coût de la fermeture d'une entreprise par suite d'une ou de plusieurs cyberattaques. La cyberassurance peut être combinée à certains des services mentionnés ci-dessus.

Pourquoi la cybersécurité est-elle essentielle à la survie des PME?

Contrairement à Rokenbok Education, la plupart des PME ne sont pas en mesure de faire comme cette entreprise spécialisée dans la conception de jouets, c'est-à-dire de restaurer leurs systèmes de base en interne. En réalité, la grande majorité des entreprises ne sauraient même pas par où commencer. Les statistiques montrent que plus de la moitié des cyberattaques étaient dirigées contre des PME il y a trois ans et que ce pourcentage est susceptible d'augmenter; le risque pour ces entreprises est donc trop important pour être ignoré.

Pourtant, en raison d'une perception erronée de l'énormité et de la gravité de ce risque, moins de 3 % des PME ont souscrit une cyberassurance, contre 40 % des grandes entreprises. En réalité, les PME ont tendance à consacrer des ressources, du temps et des fonds inadéquats à la cybersécurité, 67 % d'entre elles ne disposant d'aucune politique de sécurité des données. Sur les 33 % qui en ont une, 87 % n'ont aucune politique écrite formelle en place. Si elles deviennent la cible d'une cyberattaque, leur vulnérabilité est d'autant plus grande qu'elles n'investissent pas suffisamment dans la cybersécurité et que la plupart d'entre elles n'ont pas de cyberassurance. Il n'est donc pas étonnant que 93 % des PME victimes d'une cyberattaque aient vu leur activité gravement touchée.

Dans le monde d'aujourd'hui, il incombe aux PME d'assurer l'avenir de leur entreprise en adoptant des mesures de cybersécurité adéquates. Heureusement pour celles-ci, même si la cybersécurité a toujours représenté un défi hautement technique et coûteux, des mesures aussi simples que celles mentionnées ci-dessus peuvent fournir une protection efficace à un faible niveau de coût et de complexité.

À propos des auteurs

Pascal Millaire est vice-président et directeur général de la cyberassurance chez Symantec. À ce titre, il est responsable des partenariats et de l innovation des produits à l intersection de la sécurité et de l assurance, ainsi que de la création d outils de modélisation de la souscription et de l agrégation pour les cyberassureurs.

Anita Sathe, directrice de la stratégie chez CoverHound, est une professionnelle de l assurance avec plus de 13 ans d expérience dans ce secteur. Elle possède une vaste expérience allant de la stratégie en matière de produits et de souscription à la mise en œuvre de technologies et aux analyses actuarielles. Elle est l une des douze personnes à détenir un diplôme d actuaire dans les domaines de l assurance de biens et de dommages, de l assurance vie et de l assurance maladie. Avant de rejoindre CoverHound, Anita était directrice principale chez Deloitte Consulting.

Patrick Thielen est vice-président principal chez Chubb et spécialiste des produits d assurance erreurs et omissions pour les domaines des cyberrrisques et de la technologie en Amérique du Nord. Il dirige actuellement les projets de Chubb pour étendre l accès de la cyberassurance aux petites entreprises. Vous pouvez communiquer avec M. Thielen à l'adresse suivante Patrick.Thielen@chubb.com.

Notes en fin d'ouvrage

Toutes les données proviennent de recherches effectuées par Janet & Mark L. Goldenson pour le Center for Actuarial Research de l'Université du Connecticut. Pour télécharger le rapport complet, visitez le site http://goldensoncenter.uconn.edu/cyber-risk/(en anglais seulement).

Chubb. Insured.[MS]

Mise à jour 02/23