LIVRE BLANC

10 étapes pour une sécurité proactive

solarwinds msp

Il est devenu banal de dire que l'état de la cybersécurité change. C'est indéniable, les cybercriminels ne cessent de faire évoluer leurs modes d'attaque. Vous n'avez plus seulement à vous soucier d'individus malveillants : dans un monde toujours plus interconnecté, la probabilité d'une violation de données accidentellement provoquée en interne est plus grande que jamais.

Pour mesurer à quel point l'état de la cybersécurité est devenu critique, il suffit d'observer quelques violations de données ayant eu lieu en 2017. Celle dont a été victime Equifax® a conduit à la perte de plus de 143 millions de dossiers personnels[1]. Cette violation s'est produite dans une société qui protège les données personnelles privées. Imaginez l'enjeu que cela représente pour les entreprises dont les ressources de sécurité sont inférieures à celles d'Equifax. Les attaques de ransomwares telles que Petya, Wannacry et Bad Rabbit ont montré que les cybercriminels n'ont plus besoin de voler des données pour parvenir à leurs fins. Il leur suffit de les verrouiller et de les prendre en otage pour causer des ravages (et obtenir un gain financier).

Notre industrie a besoin d'un changement radical dans son approche de la sécurité afin de pouvoir anticiper davantage sa lutte contre les cybercriminels. Ce livre blanc présente dix étapes pour y parvenir.

Notre industrie a besoin d'un changement radical dans son approche de la sécurité afin de pouvoir anticiper davantage sa lutte contre les cybercriminels.

1. SE CONCENTRER SUR LES RISQUES

Aucune entreprise n'est jamais sécurisée à 100 %. Même si les meilleurs processus et technologies de sécurité sont en place, il existe toujours le risque qu'un nouveau type d'attaque vienne frapper vos clients en premier. Pourtant, la discussion reste centrée sur une vision quasi binaire, consistant à dire que l'entreprise est soit sécurisée, soit elle ne l'est pas. Cette proposition du « tout ou rien » nie la réalité de la situation.

Vous devez, au lieu de cela, vous intéresser à la notion de risque. La plupart des entreprises se soucient déjà des risques généraux pour leur activité, tels que la mauvaise réputation ou l'évolution de la demande du marché. La cybersécurité ne doit pas faire exception. Gardez à l'esprit ces éléments :

- **Posez-vous la question : « À quels risques l'entreprise est-elle confrontée ? »** Au lieu de vous concentrer d'abord sur les mesures de sécurité, déterminez les préjudices que peut avoir une violation de données sur la réputation ou les résultats de votre client. À l'évidence, une société de crédit comme Equifax s'expose à un risque important si elle perd des données, mais le danger peut être tout aussi grand pour une petite entreprise qui égare des informations clients. En réalité, les petites entreprises doivent s'inquiéter davantage, car elles représentent des cibles plus faciles pour les pirates informatiques (en particulier dans le cas d'attaques

automatisées). De plus, elles ne disposent pas de réserves financières pour se protéger des répercussions liées à une violation de données. Une conversation sur les risques permettra à vos clients et parties prenantes de connaître et de mesurer les enjeux, ce qui les conduira probablement à prendre la sécurité plus au sérieux.

- **Fixez des indicateurs de sécurité et observez-les attentivement.** La mise en place d'indicateurs de sécurité permet non seulement de démontrer la valeur de votre travail, mais aussi d'établir des contrôles et d'identifier les points à améliorer. Par exemple, le suivi des pourcentages de programmes ne disposant pas des derniers correctifs de sécurité vous alertera sur des failles potentielles. L'étude de cet indicateur aurait pu empêcher le piratage des données de la société Equifax ainsi que l'attaque WannaCry, ces deux violations ayant été opérées à partir de vulnérabilités pour lesquelles des correctifs étaient disponibles depuis plusieurs mois.[2,3]
- **Renforcez la sécurité grâce à une gestion adaptée.** Dans la suite du point précédent, l'analyse d'indicateurs clés au sein de votre environnement vous donne la possibilité d'améliorer vos processus. Comme on dit, « ce qui est mesuré peut être géré ». Par exemple, en évaluant la rapidité avec laquelle votre équipe répond aux incidents de sécurité, vous pouvez savoir si vos processus doivent être améliorés, et ainsi offrir de meilleurs services à vos clients.

2. COMPRENDRE L'ENVIRONNEMENT ET IDENTIFIER LES « JOYAUX DE LA COURONNE »

Si vous avez déjà vu des films de braquages, vous savez que les voleurs cherchent toujours à réaliser les plus grands exploits. Dans Ocean's Eleven[4], leur objectif est de voler trois casinos. Dans d'autres films, ils visent des banques. Dans la série Sherlock[5] de la BBC, Moriarty s'empare des joyaux de la couronne (et se fait prendre volontairement).

Dans chaque situation, les victimes protègent leurs biens avec d'incroyables dispositifs de sécurité. Dans le cas de vos clients, vous devez savoir quels sont les « joyaux » de leurs environnements, afin de les tenir à l'écart des Moriarty.

Vous disposez probablement déjà d'un plan pour gérer la maintenance et la protection de leurs serveurs clés et principaux points de terminaison. Vous devez à présent observer les « joyaux » qu'ils contiennent, autrement dit, les données. En tant que fournisseur de services, vous connaissez la configuration du terrain et êtes en mesure d'effectuer un « repérage du réseau », comme le ferait un cybercriminel.

Pour commencer, identifiez les applications, systèmes et données de première importance. Vous devez également distinguer les employés stratégiques. Une fois ces étapes terminées, mettez en place des processus afin de les protéger.

Dans de nombreux cas, un seul employé touché suffit à anéantir une entreprise. Imaginez les conséquences que pourrait subir une organisation si l'ordinateur portable de son directeur financier était compromis.

Parfois, le problème touche un processus ou un point d'accès critique. Par exemple, dans le cas du piratage de Target®, la violation du système est passée par leur sous-traitant chargé de la climatisation[6] !

Il est par ailleurs essentiel de vous concentrer sur les données stratégiques. Les dossiers médicaux contiennent une quantité incroyable de données sensibles, pouvant constituer un butin avantageux pour les cybercriminels. Les informations de crédit attirent également de nombreux pirates informatiques.

En résumé, les entreprises doivent définir leurs éléments précieux et renforcer la sécurité de ces derniers. De plus, leurs stratégies de sécurité doivent être régulièrement revues, qu'elles concernent des individus, des systèmes, des points d'accès ou des données critiques. Bien qu'il soit impossible de tout sécuriser, la première priorité d'un fournisseur de sécurité informatique est d'identifier et de protéger les « joyaux » de son client.

3. METTRE EN PLACE UNE BONNE « CYBER-HYGIÈNE »

Jusqu'ici, nous avons vu qu'il était nécessaire d'orienter votre discours sur le risque plutôt que sur la sécurité lors de vos conversations avec vos clients. Les règles fondamentales de la cybersécurité n'en doivent pas moins être appliquées : pour améliorer la sécurité et réduire les risques, une technologie, des processus et des efforts appropriés sont nécessaires.

Vous devez toujours avoir une bonne « cyber-hygiène ». Rester vigilant sur la sécurité permet d'empêcher bien des catastrophes. Souvent, les attaques les plus simples, telles que les phishings ou les téléchargements d'e-mails malveillants, sont celles qui réussissent.

Veillez donc à respecter les points suivants :

- **Installez un antivirus puissant sur chaque point de terminaison (et assurez-vous qu'il fonctionne constamment).**
- **Établissez la cartographie des données de votre client pour éviter qu'elles ne tombent entre de mauvaises mains.**
- **Contrôlez fréquemment les droits d'administration et autorisations d'accès aux données sensibles.**
- **Installez régulièrement les correctifs des systèmes et logiciels (et restez informé des derniers bulletins de sécurité).**
- **Instaurez un plan de sauvegarde et de continuité d'activité solide.**
- **Méfiez-vous du spam (en équipant notamment vos serveurs de messagerie de dispositifs de sécurité).**
- **Réduisez au maximum la surface d'attaque potentielle en évitant de relier certains postes de travail au Web, ou en utilisant des machines virtuelles là où vous en avez la possibilité.**
- **Préparez à l'avance des plans de réponse aux incidents afin de disposer de procédures claires lorsqu'un sinistre frappe.**

Le plus important est peut-être de réaliser qu'il n'existe pas de solution miracle. Une vigilance et des efforts constants sont nécessaires. Cette nouvelle est positive pour votre activité de MSP : vous pouvez continuer à fournir à vos clients un service récurrent, d'une extrême valeur.

4. SÉCURISER L'ENVIRONNEMENT À DIFFÉRENTS NIVEAUX

Il n'existe pas de sécurité à toute épreuve. Et vous le savez sans doute, il n'y a pas non plus d'approche unique en matière de sécurité.

Vous devez viser les investissements les plus judicieux pour vos clients. Sans mettre la barre trop haut, car cela pourrait les surprendre et remettre en question la valeur de vos services. Ni trop bas, car vous les laisseriez au dépourvu face à des violations potentielles.

Déterminez cela au cas par cas : identifiez les « joyaux » de vos clients et étudiez avec eux les niveaux de sécurité les mieux adaptés à leurs situations (tout en suivant les principes de base d'une bonne cyber-hygiène). Dès le départ, discutez ensemble de leurs attentes afin de dresser le meilleur plan d'action.

En parallèle des services fournis, tenez-les régulièrement informés. Pensez sans cesse à la manière de leur prouver la valeur de vos prestations, et rassurez-les sur le fait qu'ils sont entre de bonnes mains. Il peut être utile de revoir le niveau de sécurité de vos clients tous les trois à six mois, afin qu'ils soient constamment prêts à lutter contre les menaces potentielles. Face à un paysage de la sécurité en constante évolution, ce point est essentiel. Souvenez-vous, il y a seulement quelques années, les ransomwares n'étaient pas un problème majeur. Aujourd'hui, ils sont devenus une arme de choix pour de nombreux cybercriminels.

5. FAIRE DE LA SÉCURITÉ RENFORCÉE UN ÉLÉMENT DIFFÉRENCIATEUR POUR VOUS COMME POUR VOS CLIENTS

Dans un monde où les menaces ne cessent jamais, la sécurité peut faire la différence pour vous comme pour vos clients.

Les avantages pour votre entreprise paraissent évidents. En offrant une sécurité renforcée, vous vous démarquez des concurrents qui se limitent à de simples services de maintenance et de supervision. Vous répondez à une demande manifeste, et accentuez votre crédibilité.

Ce qui saute moins aux yeux, c'est la manière dont les clients peuvent tirer profit de la sécurité. Imaginez, par exemple, que vous travailliez pour un fabricant qui s'adresse à des services publics. Une proposition de sécurité forte pourrait aider ce client à obtenir plus de contrats. Certaines entreprises opèrent dans un secteur où la sécurité détermine la réussite ou l'échec de leur activité. Les institutions financières, organismes de santé, sociétés pharmaceutiques, entreprises au service de la sécurité nationale et services publics en font partie. Parvenir à prouver une vigilance constante et des techniques de sécurité avancées peut les aider à soutenir la concurrence sur le marché.

Même si vos clients ne dépendent pas d'un secteur réglementé, la sécurité reste un argument de vente pour eux. Ils ne le savent peut-être pas. Prenez l'exemple d'un fabricant de thermostats intelligents. Ses appareils pourraient être piratés et pris en otages en échange d'une rançon, comme l'ont démontré certains hackers lors d'une conférence sur la sécurité en 2016[7]. Même si ces attaques ne se sont encore jamais produites, votre client peut montrer qu'il est préparé à cette éventualité. En réalité, tous les périphériques IoT (Internet of Things) présentent des risques pour les organisations. Si vos services permettent de gérer ces risques et d'assurer une bonne cyber-hygiène, elles disposent d'un argument de vente supplémentaire qui les place en tête de la concurrence.

Il peut être utile de revoir le niveau de sécurité de vos clients tous les trois à six mois, afin qu'ils soient constamment prêts à lutter contre les menaces potentielles.

6. RÉALISER QUE LES RÉGLEMENTATIONS SONT DE VOTRE CÔTÉ

Lorsqu'une nouvelle législation apparaît, comme très récemment le Règlement Général sur la Protection des Données (RGPD), de nombreux acteurs du secteur informatique, en particulier la presse, peinent à comprendre les enjeux potentiels. S'ensuivent panique et confusion.

Pourtant, dans de nombreux cas, ces réglementations présentent de nouvelles opportunités pour les MSP qui ont une longueur d'avance (et de sérieux avantages pour les personnes dont les données doivent être protégées). Gardez à l'esprit ces éléments :

- **Réalisez que les réglementations favorisent la sécurité.** Les nouvelles exigences du RGPD, ou même d'anciennes mesures telles que la loi HIPAA (Health Insurance Portability and Accountability Act) ont forcé les entreprises à améliorer leur sécurité. En suivant les réglementations, vous incitez vos clients à prendre la sécurité au sérieux, et obtenez des directives pour réduire les risques de violation de données (dans les réglementations elles-mêmes, mais aussi dans la presse informatique au moyen de ressources pédagogiques conçues pour vous aider à vous mettre en conformité).
- **Soyez attentif aux réglementations de vos clients potentiels.** Certaines organisations sont soumises à des réglementations spécifiques en fonction des régions où elles exercent leur activité. (C'est le cas notamment du RGPD, qui s'applique à toutes les entreprises qui traitent les données de citoyens européens.) D'autres peuvent dépendre de secteurs réglementés tels que la santé, la finance, l'éducation ou l'entrepreneuriat public. Même si, à terme, il vous faut solliciter un conseiller juridique (et structurer scrupuleusement vos contrats afin d'éviter à votre entreprise de services gérés des responsabilités supplémentaires), vous devez suivre de près les réglementations qui vous permettront d'offrir une protection adaptée à vos clients.
- **Les règles de confidentialité se multiplient.** Le RGPD a considérablement élargi l'étendue des réglementations en matière de respect de la vie privée. Désormais, les entreprises implantées en dehors de l'Union européenne doivent se conformer à la réglementation si elles accèdent aux données personnelles de citoyens européens. Voyez cela comme le signe précurseur d'une portée et d'une importance plus grandes accordées à la confidentialité des données.

Les réglementations en matière de sécurité sont de véritables alliées. Elles améliorent la protection de chaque organisation, mais aussi de tous (ce qui est essentiel dans l'univers interconnecté du Web). Pour les MSP, les secteurs réglementés représentent souvent les marchés spécialisés les plus lucratifs.

7. AUGMENTER VOTRE SAVOIR-FAIRE EN MATIÈRE DE SÉCURITÉ

Tel que nous l'avons évoqué précédemment, le paysage de la cybersécurité évolue en permanence. Il n'y a pas si longtemps, les sauvegardes sur site suffisaient aux utilisateurs pour récupérer leurs données. Aujourd'hui, une copie supplémentaire dans le Cloud est presque impérative, car certains types de programmes malveillants ciblent spécifiquement les fichiers de sauvegarde.

La clé est d'actualiser sans cesse les connaissances de votre organisation dans le domaine de la sécurité (qu'elles concernent des clients spécifiques ou le secteur en général). Voici quelques recommandations :

La clé est d'actualiser sans cesse les connaissances de votre organisation dans le domaine de la sécurité (qu'elles concernent des clients spécifiques ou le secteur en général).

- **Créez une base de connaissances.** Vous devez d'abord vous assurer que votre entreprise dispose des informations et compétences nécessaires pour servir correctement vos clients. Chacun de vos employés doit être formé sur les éléments de base (tels que les fondamentaux de la supervision et d'une bonne cyber-hygiène). Certains deviendront, au fil de leur travail avec vos clients, des spécialistes de leurs environnements. Ils connaîtront leurs points faibles et seront indispensables en cas de problème. Veillez néanmoins à ce qu'ils ajoutent des informations (telles que des configurations) dans un référentiel centralisé, par exemple une base de connaissances ou votre logiciel d'assistance, de sorte que votre organisation ne parte pas d'un unique point de défaillance.
- **Restez à la pointe de l'actualité.** Garder une longueur d'avance sous-entend de nombreuses recherches et lectures. Commencez par parcourir rapidement les articles quotidiens et ressources de références majeures. Si l'une d'elles vous plaît, inscrivez-vous à sa newsletter ou suivez son blog. Voici quelques bons exemples :
  - US-CERT (United States Computer Emergency Readiness Team) : https://www.us-cert.gov
  - SANS.org (propose des newsletters et des blogs) : https://www.sans.org
  - CSA (Cloud Security Alliance) : https://cloudsecurityalliance.org
  - ZDnet : http://www.zdnet.com
  - Dark Reading : https://www.darkreading.com
  - CSO Magazine : https://www.csoonline.com
- **Pensez aux certifications.** Les certifications peuvent aider vos employés à maîtriser les dernières tendances, et à fournir un cadre pour lutter contre les utilisateurs malveillants. Elles constituent, en outre, un excellent outil marketing, qui donne de la crédibilité à votre entreprise de services gérés. Essayez notamment

de décrocher les certifications CISSP (Certified Information Security Services Professional), CEH (Certified Ethical Hacker) ou ISC² (International Information System Security Consortium).

» **Rejoignez des communautés.** Faire connaissance avec d'autres professionnels de la sécurité de l'information peut également vous aider. Envisagez de rejoindre l'association ISACA et d'obtenir des certifications par l'intermédiaire de celle-ci. Par ailleurs, plusieurs conférences ont probablement lieu chaque année dans votre région. Parmi celles-ci, on retrouve de grands noms tels que RSA, Black Hat, DEFCON, Cloud Security Expo ou Cybersecurity Europe.

8. DÉVELOPPER UNE CULTURE DE LA SÉCURITÉ

La sécurité doit faire partie de l'ADN de presque toutes les organisations. La technologie, bien qu'utile, n'est pas toujours suffisante. L'apparition au quotidien de nouveaux types d'e-mails de phishing, de logiciels et de sites Web malveillants contraint la technologie à rattraper sans cesse son retard.

C'est pourquoi il est important de dispenser des formations régulières à vos clients (et à vos propres employés). Leur enseigner les bonnes habitudes de sécurité—telles que changer de mot de passe fréquemment, utiliser un identifiant différent pour chaque service (en se servant, par exemple, d'un gestionnaire de mots de passe) et activer le chiffrement sur leurs appareils mobiles—les protégera en plus de préserver votre entreprise. Des formations « régulières » signifient qu'elles ne doivent pas se produire une seule fois. Vous devez effectuer des piqûres de rappel aussi souvent que possible.

De plus, pensez à envoyer des mises à jour de sécurité fréquentes aux utilisateurs de vos clients (surtout en cas d'incident majeur). Par exemple, bien que sophistiquée, l'attaque de Google® Docs en 2017 a utilisé un e-mail de phishing qui a piégé les utilisateurs en les faisant entrer leurs identifiants Google sur un faux site Web. Les pirates ont ainsi pu accéder aux comptes et contacts, et reproduire la même technique sur les amis et collègues de leurs victimes. Un simple e-mail prévenant vos clients de ne pas ouvrir tel ou tel message lors d'une attaque majeure peut vous éviter bien des soucis.

Rester en contact avec une communauté d'experts en sécurité vous aidera à mener la bataille de front.

9. UTILISER LA SÉCURITÉ POUR VOUS OUVRIR DES PORTES

La cybersécurité est un besoin qui ne semble pas voué à disparaître. En relevant les défis de la sécurité (et en suivant les dernières tendances à l'aide des étapes mentionnées ci-dessus), votre entreprise trouvera toujours les moyens de se développer.

La sécurité ouvre la voie à d'autres services importants. Par exemple, vous pouvez engager vos conversations sur le thème de la sécurité multicouche, puis vous servir de celle-ci pour convaincre vos clients de la valeur d'un environnement géré de façon globale. Vous pouvez les attirer avec la sécurité, mais qu'en est-il de l'amélioration des performances du réseau ou de la sauvegarde des documents clés si un utilisateur vient à supprimer un fichier par accident ? Une fois que vous avez commencé à discuter de la sécurité avec votre prospect, interrogez-le sur les autres services qui pourraient lui être utiles.

10. TROUVER DES ALLIÉS ET LUTTER CONTRE LES CYBERCRIMINELS

Les cybercriminels ont leurs propres communautés. Ils apprennent leur métier à la fois sur le Web et sur le « dark Web ».

Pour les combattre, il est important que vous trouviez des alliés. Que ce soit en rejoignant des organisations professionnelles, en participant à des rencontres ou à des conférences, en lisant des articles en ligne et en les partageant, rester en contact avec une communauté d'experts en sécurité vous aidera à mener la bataille de front.

Ne vous limitez pas à des communautés sur la cybersécurité. Assister aux réunions pour MSP et professionnels de l'informatique est également bénéfique. Par exemple, une formation commerciale peut vous apprendre à mieux positionner vos services de sécurité. Ou à mieux situer le risque, afin de remporter encore plus d'affaires.

Vous n'avez pas à combattre les cybercriminels seul.

LES OPPORTUNITÉS QUI SE PRÉSENTENT À VOUS

Le paysage changeant de la cybersécurité est synonyme de nombreuses opportunités pour votre entreprise. Nos propres recherches le confirment.

Dans une récente étude ayant rassemblé plus de 400 entreprises du Royaume-Uni et des États-Unis, 80 % des organisations ont indiqué qu'elles prévoyaient de modifier leur façon de gérer la sécurité dans les 12 prochains mois. De plus, parmi celles qui gèrent actuellement leur sécurité en interne, 82 % prévoient d'en externaliser au moins une partie dans les 12 prochains mois[8].

Ces chiffres parlent d'eux-mêmes : les MSP qui proposent des services de sécurité ont de belles perspectives de développement. Si l'on tient compte de la nature omniprésente des menaces de sécurité, ce marché n'est pas prêt de disparaître.

Veillez simplement à ne pas oublier ces conseils : concentrez-vous sur les risques, faites des investissements judicieux, ayez une bonne cyber-hygiène et restez à l'affût des tendances et changements. Ces actions vous permettront de rester proactif dans votre lutte contre les cybercriminels, pour le plus grand bonheur de vos clients.

RÉFÉRENCES

[1,2] « Equifax Officially Has No Excuse », Wired. https://www.wired.com/story/equifax-breach-no-excuse (consulté en décembre 2017).

[3] « The 'WannaCry' Ransomware Attack Could Have Been Prevented. Here's What Businesses Need to Know », CNBC. https://www.cnbc.com/2017/05/17/the-wannacry-ransomware-attack-what-businesses-need-to-know-commentary.html (consulté en décembre 2017).

[4] Warner Bros. Pictures (visionné en décembre 2017).

[5] BBC One (visionné en décembre 2017).

[6] « Target Hackers Broke in Via HVAC Company », Krebs on Security. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company (consulté en décembre 2017).

[7] « #DefCon: Thermostat Control Hacked to Host Ransomware », Infosecurity Magazine. https://www.infosecurity-magazine.com/news/defcon-thermostat-control-hacked (consulté en décembre 2017).

[8] « Devenir MSSP », SolarWinds MSP. http://pages.solarwindsmsp.com/path-to-mssp-wp-ungated.html (consulté en décembre 2017).

SolarWinds MSP offre aux fournisseurs de services informatiques les technologies garantes de leur réussite. Axées sur la sécurité multicouche, l'intelligence collective et l'automatisation intelligente, les solutions de SolarWinds MSP sont disponibles sur site ou dans le Cloud, s'accompagnent de recommandations pratiques, et aident les fournisseurs de services informatiques à réaliser leurs tâches plus facilement et plus rapidement. Ils peuvent ainsi se concentrer sur l'essentiel : respecter leurs accords de niveau de service et fournir des services de manière efficiente et efficace.