GOUVERNANCE DE L'INFORMATION, QUID D'UN NOUVEL ENVIRONNEMENT ?

Be secure,

Be ahead

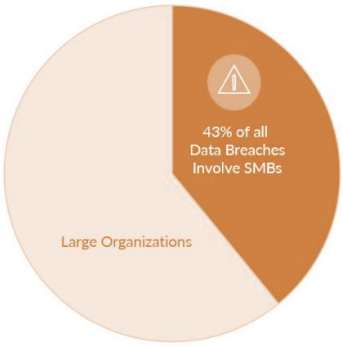
EUROPEAN CYBER SECURITY MONTH

Auteur : Pat DAWSON – Editrice : Catherine TALL
EVERTEAM, membre EFCSE
18/10/2019

La discipline autrefois sous-estimée de la gouvernance de l'information a fait couler beaucoup d'encre ces dernières années, en particulier depuis l'adoption du RGPD et la divulgation publique d'atteintes à la protection des données très médiatisées par de grandes entreprises et des géants des médias sociaux.

Le spectre de la conformité au RGPD et la nécessité d'atténuer le risque d'atteinte à la protection des données ne sont que deux exemples d'utilisation importants qui soulignent le besoin grandissant pour les organisations de toutes tailles de faire un meilleur travail de gouvernance de leurs actifs informationnels.

La plupart des gens comprennent l'importance de la gouvernance de l'information pour les grandes entreprises, les organismes du secteur public et les géants des réseaux sociaux. Toutefois, les petites et moyennes entreprises (PME) sous-estiment la pertinence d'une bonne gouvernance de l'information dans leurs activités quotidiennes.



Une étude récente de Verizon souligne le fait que 43 % des atteintes à la protection des données concernent des PME*... Le nombre d'incidents non détectés reste inconnu.

Elles divulguent par inadvertance des renseignements de nature délicate, mettant en danger leurs clients et leur entreprise.

Nous évoluons dans un environnement technologique et informationnel, qui lui évolue plus rapidement, accordons ensemble la priorité à la gouvernance de l'information. Considérez ce qui suit :

*https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

- Les atteintes à la protection des données causent des dommages considérables pour les PME : Les amendes et les litiges peuvent être coûteux et nuire aux résultats financiers des grands groupes, ils sont potentiellement dévastateurs pour les PME. Des études réalisées par la firme de consultants Switchfast Technologies ont conclu qu'au moins 60 % des PME sont obligées d'abandonner leurs activités dans les six mois suivant une infraction de ce type[1]. Les grandes entreprises disposent généralement des ressources financières nécessaires, mais avec moins d'investissements organisationnels, techniques et marketing nécessaires pour surmonter une telle perte de confiance, les revenus des PME diminuent à mesure que les clients se désengagent.

- Selon Cisco, la cyberattaque typique entraîne des dommages financiers de plus de 500 000 $US.[2] Pour les PME, ce coût élevé de défaillance impose une bonne gouvernance de l'information. Ce n'est plus un luxe, mais un investissement nécessaire à la continuité des affaires.
- Les petites organisations manquent souvent de ressources informatiques : Les services d'applications mobiles et cloud faciles à obtenir ont réduit le besoin perçu de support informatique au sein de nombreuses PME. Imprégnées d'une culture du " bricolage ", les PME ont souvent peu ou pas de personnel informatique formé pour les aider à protéger leur infrastructure. Le fournisseur de services de sécurité Underscore a interrogé 300 PME et a constaté que 29 % d'entre elles dépensent moins de 1 000 $US par année en sécurité informatique[3]. La même étude a révélé que 52 % de ces mêmes PME

1 https://solutionsreview.com/security-information-event-management/switchfast-majority-smbs-go-business-data-breach/
2 https://blogs.cisco.com/security/smbs-cybersecurity-risk-their-opportunity
3 https://www5.untangle.com/smbitsecurityreport2019

attribuaient la responsabilité informatique à des employés d'autres services[4]. Le manque de personnel formé en IT et de programmes de gouvernance de l'information sous-développés rend les PME vulnérables aux failles de la diligence raisonnable en matière de gouvernance de l'information, mettant en péril les données de leurs clients et la continuité de leurs activités.

- Les petites organisations mélangent souvent vie personnelle et vie professionnelle : Les propriétaires de petites entreprises et leur personnel utilisent souvent les mêmes ordinateurs portables, appareils mobiles et espaces de stockage dans le cadre de leur travail, mais aussi dans leur vie personnelle. Habituellement libres de toute politique interdisant l'utilisation d'appareils ou d'applications professionnelles à des fins personnelles, les petites organisations constituent une cible efficace pour les cybercriminels. Cela signifie que les violations mettent en danger à la fois l'entreprise et le personnel pour de nombreuses PME.

4 https://www5.untangle.com/smbitsecurityreport2019

Une gestion responsable du cycle de vie de l'information peut atténuer ces risques irréfutables.

Voici quelques outils et processus de base visant à donner aux PME les moyens de développer une meilleure capacité de gouvernance de l'information.

- Effectuez un inventaire des informations : Pour identifier les lacunes dans votre stratégie actuelle de gestion du cycle de vie et de gouvernance de l'information, effectuez un examen approfondi de vos renseignements. L'examen devrait englober tous les renseignements avec lesquels l'organisation interagit. Les informations particulièrement sensibles comprennent :

Informations personnellement identifiables (PII) présentes dans les systèmes transactionnels tels que les systèmes de planification, de facturation ou autres systèmes utilisés pour les opérations quotidiennes

Informations régies par des réglementations spécifiques à l'industrie -- informations médicales (PHI) ou données financières (PCI), par exemple.

Renseignements exclusifs : secrets commerciaux, dessins, formules ou autre propriété intellectuelle. Les secrets commerciaux volés peuvent être utilisés pour faire chanter l'entreprise ou miner la position concurrentielle d'une organisation.

Renseignements sur les clients et les prospects : il est particulièrement intéressant de voir dans quelle mesure les contacts de la base de données marketing de votre organisation ont consenti, par le biais du double consentement, à recevoir des communications par courriel.

- Effectuez une évaluation des besoins : les PME choisissent leurs logiciels en fonction de facteurs pragmatiques tels que le prix, la fonctionnalité et la facilité d'utilisation. Mais ce qui est souvent négligé dans le processus de sélection, c'est la fiabilité de l'éditeur de logiciels et la résilience de ses logiciels face à la menace que représentent les cybercriminels.

  Parmi les critères de cet examen, mentionnons les suivants :

Utilisation du chiffrement : le logiciel utilisé comprend-il l'utilisation du chiffrement pour des actions comme l'encodage des courriels, le stockage des fichiers ou l'accès sécurisé au site Web ? Si ce n'est pas le cas, le logiciel n'est probablement pas un bon choix pour héberger des informations sensibles ou propriétaires, et des alternatives devraient être recherchées

Conformité à toutes les réglementations et normes clés : par exemple, si l'application gère les paiements par carte de crédit, est-elle conforme à la norme PCI DSS ? Si la demande porte sur des renseignements personnels, ont-ils un énoncé de conformité à des règlements comme le RGPD ?

Existe-t-il des mesures de sécurité robustes ? Le logiciel, l'application ou le site Web dispose-t-il d'une bonne gestion de mots de passe et de permissions ? Ceci comprend la capacité à définir des autorisations d'accès basées sur les rôles et les groupes, la mise à jour régulière des mots de passe en fonction de critères définis, la complexité des mots de passe, l'utilisation de Captcha et autres mesures destinées à empêcher tout accès non autorisé aux informations ?

Politique de l'éditeur de logiciels en cas d'atteinte à la protection des données : la transparence est importante. Les éditeurs de logiciels avec lesquels vous travaillez ont-ils mis en place des politiques proactives de prévention et de signalement des brèches ? Si les politiques de protection des données sont inadéquates ou inexistantes, envisagez un autre fournisseur.

- Passez en revue vos pratiques et vos ressources en matière de marketing numérique : L'une des plus grandes sources d'informations personnelles identifiables est constituée par les données marketing, utilisées historiquement pour générer la demande par courrier électronique, par téléphone ou par publipostage direct. Lorsque vous examinez les informations marketing de votre organisation, portez une attention particulière aux :

Formulaires du site web : S'assurer que les formulaires sont conformes au RGPD. Plus précisément, est-ce qu'ils comportent un double consentement qui indique explicitement la volonté de recevoir des emails marketing de votre entreprise ?

Listes des contacts : Confirmer l'abonnement par double consentement, pour les contacts existants et les prospects futurs. Sécuriser le double consentement par le biais d'une campagne e-mail pour les actifs marketing non conformes dans l'intérêt de le devenir. Supprimer toute information de contacts non intéressés. Ce processus entraîne souvent une perte importante des actifs de la liste de diffusion. Toutefois, c'est la seule façon de se conformer aux exigences du RGPD et de protéger votre organisation contre les infractions à la vie privée qui peuvent entraîner des amendes importantes, des litiges ou pire encore.

Fournisseurs de services commerce et marketing : de nombreuses PME comptent sur des partenaires pour les aider à générer de nouveaux prospects par le biais du marketing ou des services de vente interne (c.-à-d. de démarchage téléphonique). Vous cherchez à accroître la maturité de votre organisation concernant la protection des données et la conformité, veillez à ce que chacun de vos partenaires soit conforme à votre but.

- Elaborez et mettez en œuvre une stratégie de gestion du cycle de vie de l'information : les résultats d'un inventaire de données et d'une vérification des applications permettent de combler les lacunes relevées et de corriger les problèmes connus seulement à un moment précis dans le temps. Cet effort demeure temporaire jusqu'à ce qu'une stratégie de gestion du cycle de vie documentaire utilise et mette en œuvre les outils et processus suivants de façon durable :

Nommez un délégué à la protection des données (DPO) : Un DPO est une personne au sein de l'organisation qui est responsable des aspects humains, système et processus de la gouvernance de l'information. Sa responsabilité ne requiert pas un équivalent temps plein - c'est un rôle assumé par un leader au sein de l'organisation qui comprend l'importance de la protection des données pour le bien-être de l'entreprise, et qui peut agir dans le rôle de superviseur.

Affecter un budget approprié : Le budget de la gouvernance de l'information ne doit pas nécessairement être exorbitant, mais il doit être réaliste. Il peut servir à l'achat de logiciels pour faciliter la protection des données et la conformité réglementaire. Le budget peut également être alloué dans le temps - le temps nécessaire aux ressources internes pour effectuer des audits réguliers des données et des applications.

Envisagez l'utilisation d'outils pour faciliter le travail : implémenter les outils et les processus pour régler les problèmes et appuyer la gestion de l'information.

- Découverte systématique de données sensibles.
- Définition et mise en œuvre des politiques de conservation
- Suppression des données redondantes, obsolètes ou triviales (RoT)
- Définition et mise en œuvre des process de gestion de demande d'accès à l'information (SARs)
- Mise en œuvre des process pour signaler une atteinte à la protection des données, le cas échéant.

- Découverte systématique de données sensibles dans des endroits où elles ne devraient pas être stockées, comme les serveurs de fichiers, le stockage local d'emails non cryptés sur les ordinateurs portables ou les téléphones, etc. Les solutions de recherche transverse peuvent fournir un inventaire complet des données sensibles et de leur emplacement.
- Définition et mise en œuvre des politiques de conservation tout au long du cycle de vie de l'information. Veiller à ce que l'information soit gérée de façon appropriée, de sa création à sa destruction. Les petites entreprises peuvent choisir de suivre ce processus à l'aide d'un tableur, mais les produits disponibles sur le marché peuvent automatiser ce processus, ce qui réduit considérablement les erreurs et les délais.
- Suppression des données redondantes, obsolètes ou triviales (RoT : les données ROT peuvent fournir de l'information désuète aux membres de votre équipe et porter atteinte à la sécurité de ces données. Optimisez régulièrement vos systèmes d'information et supprimez les données obsolètes ou non pertinentes, soit manuellement, soit dans le cadre d'une politique de conservation gérée par une solution.
- Définition et mise en œuvre des process de gestion de la demande d'accès à l'information (SARs). Bien que ces demandes concernent généralement les gros groupes, chaque personne a le droit de demander comment ses renseignements personnels sont utilisés. Les PME doivent mettre en place des procédures pour reconnaître la demande et y répondre au regard du RGPD.
- Mise en œuvre des processus pour signaler une atteinte à la protection des données, le cas échéant : tout comme vous vérifiez la transparence de vos fournisseurs dans le traitement des problèmes liés à la protection des données, vos clients s'attendent à un niveau élevé de transparence de de votre part. Faites de la protection et de la confidentialité des données un élément clé de votre marque [promouvoir vos actions pour assurer la confidentialité des données, communiquer les politiques et interagir proactivement avec les clients si un problème survient]. Inc. Magazine a noté que 73 % des consommateurs indiquent que la transparence est plus importante que le prix[5] dans le choix des entreprises avec lesquelles ils font affaire.

5 https://www.inc.com/rhett-power/trust-is-as-important-as-price-for-todays-consumer.html

La confidentialité et la protection des données peuvent être un obstacle complexe pour les PME qui ne connaissent pas bien la gouvernance de l'information. Comme le démontre ce bref survol, les PME prêtes à relever ce défi peuvent éviter des amendes, préserver la confiance de leurs clients et contribuer à assurer la viabilité de leur entreprise. Une gouvernance diligente de l'information n'a pas besoin d'investissements massifs ou de changements radicaux et perturbateurs ; elle peut être mise en œuvre sous la forme d'une série d'étapes progressives, visant à identifier, classer et gérer vos actifs informationnels.

Les changements décrits dans ce document peuvent apporter à votre organisation des améliorations qui, non seulement protégeront vos opérations, mais augmenteront également la fidélité des clients et la valeur de votre marque.

En gardant ces avantages à l'esprit, nous vous encourageons à commencer la transition !

La gouvernance de l'information est un sujet majeur dans le contexte de transition et de transformation numérique, EFCSE a dédié un de ses Working Groups à ce thème.

Contactez-nous sur efcse.eu