BlueFinch ESBD

Votre entreprise est-elle préparée contre les cyberattaques ?

INTRODUCTION

Le secteur de la cybersécurité se développe à un rythme croissant. Le nombre exponentiel de cyberattaques, de plus en plus sophistiquées, est préoccupant.

Le moyen le plus rapide et le plus simple d'améliorer votre sécurité consiste à réduire le nombre de vecteurs d'attaque. En analysant comment un attaquant pourrait s'introduire dans vos systèmes, vous pouvez mieux déterminer les faiblesses de l'entreprise.

Dans ce livre blanc, vous trouverez différentes questions à vous poser faisant l'inventaire de votre structure.

SOMMAIRE

ANALYSER LA SITUATION DE SON ENTREPRISE

Avez-vous effectué un audit de sécurité interne ?

C'est par cette étape que vous devez commencer.

Afin de pouvoir faire face aux menaces de cyberattaques, vous devez identifier les points faibles de votre structure et les renforcer. Déterminez quelles sont les menaces possibles, où se situent les vulnérabilités de votre infrastructure, où se trouvent vos données et qui en a l'accès.

Vous devez faire un état des lieux des capacités de votre stratégie de sécurité (solutions, politiques et ressources utilisées). Vous pourrez ainsi déterminer quels sont les incidents de sécurité auxquels l'entreprise peut être confrontée.

À quelles règles de conformité êtes-vous soumis ?

Stockez-vous des informations personnelles identifiables de citoyens de l'UE ? Traitez-vous des informations relatives aux cartes de crédit ? Êtes-vous un organisme de santé aux États-Unis ?

Si vous répondez oui à l'une de ces questions, alors vous êtes soumis à une réglementation.

Vous devez vous assurer d'être en accord avec ces réglementations grâce à différents dispositifs. S'il s'avérait que lors d'un contrôle, il est impossible de justifier votre conformité, vous pouvez alors être soumis à de lourdes sanctions.

Quelques exemples de réglementation :

RGPD : Le Règlement Général sur la Protection des Données s'applique à toutes les sociétés ou organismes qui traitent des données de citoyens européens.
Cette réglementation repose principalement sur la mise en place de moyens de protection des données par les entreprises, assurant ainsi la valorisation des droits d'une personne sur ses données personnelles (droit à l'oubli, droit d'accès, droit de rectification et retrait du consentement) ainsi que la confidentialité et la sécurité de ses informations.

PCI-DSS : PCI-DSS ou Payment Card Industry Data Security Standard, est un standard mondial qui s'applique à tous les acteurs de la chaine monétique. Il a été créé afin d'augmenter le contrôle des informations des titulaires de cartes dans le but de réduire l'utilisation frauduleuse des instruments de paiement.

SOX : SOX, alias Sarbanes-Oxley est une réglementation qui s'applique à toutes les sociétés aux États-Unis, sans exception. Elle impose de mettre en place des contrôles pour les documents financiers de l'entreprise, ainsi que des processus d'atténuation des risques. Elle stipule également que les documents de l'entreprise doivent être conservés pendant au moins 5 ans.

LSF : La loi de sécurité financière est une loi française qui permet de renforcer les dispositions légales en matière de gouvernance d'entreprise par des rapports détaillés. Cette réglementation est l'équivalence de la loi américaine SOX.

HIPAA : Health Insurance Portability and Accountability Act est une loi Américaine qui s'applique à toutes entités qui stockent, transmettent ou gèrent des informations médicales protégées. Cette réglementation impose de contrôler l'accès aux informations de santé, de fournir des pistes d'audit et d'assurer la confidentialité et la sécurité des informations médicales.

Savez-vous où se trouvent vos données sensibles et qui y accède ?

Savez-vous quels fichiers et dossiers présentent le plus grand risque ? Quels utilisateurs ont accès à quelles données ? Qui peut modifier, supprimer ou déplacer certains types de fichiers ?

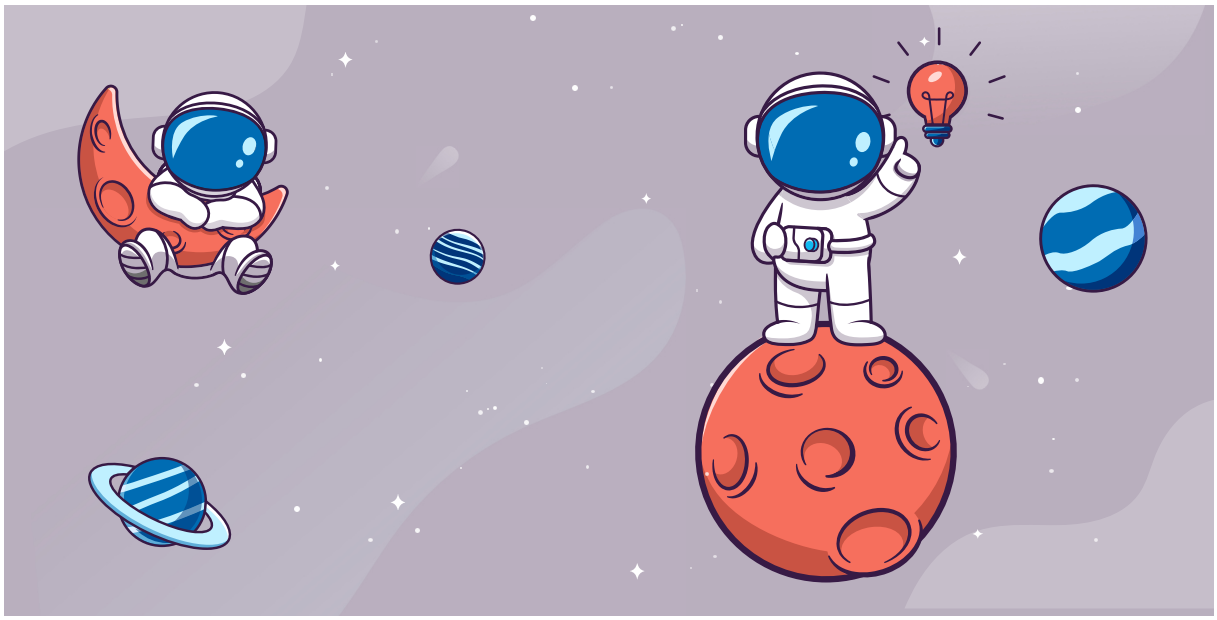
Utiliser des solutions de « data discovery » et de « data classification » vous aidera premièrement à identifier les données sensibles parmi les données d'utilité courante, les archives, etc.

Si vous souhaitez une meilleure visibilité des droits sur vos données, les solutions d'audit et de gouvernance vous y aideront. Vous serez en mesure de repérer facilement les changements non autorisés ou non désirés qui pourraient mener à une atteinte à la protection des données. Vous pourrez également détecter lorsqu'un utilisateur accède à des fichiers pour lesquels il n'a pas de permission.

Connaissez-vous les dernières nouveautés logiciels ?

Les codes malveillants étant de plus en plus élaborés, les solutions du marché évoluent elles aussi constamment. Cela peut prendre du temps, mais il est nécessaire de se renseigner à propos de ces solutions pour déterminer si votre entreprise possède les bonnes ressources pour continuer à sécuriser vos systèmes.

Si le temps vous manque, vous pouvez faire appel à des sociétés de services qui pourront vous aiguiller sur les différentes solutions du marché et les dernières mesures de sécurité à vous procurer. Vous devez prendre les précautions de sécurité appropriées lors du choix des logiciels et des fournisseurs, notamment lorsque les logiciels impliquent le transfert d'informations critiques d'une application à l'autre.



PRÉVENTION ET BONS COMPORTEMENTS

Quelles sont vos politiques en matière de sécurité informatique ?

Vous n'en possédez pas ? C'est malheureusement une erreur que font beaucoup d'entreprises. Peu importe la taille de votre infrastructure, une politique de bonnes pratiques en matière de sécurité est toujours nécessaire, ne serait-ce que pour faire de petits rappels ou avoir une référence en cas de doute.

Formez-vous vos employés ?

Vos collaborateurs sont susceptibles d'être la proie des cyberattaquants. C'est pourquoi il est important que vous les teniez informés des tendances et pratiques en matière de cybersécurité.

Des formations régulières sur les politiques concernant les mots de passe, les bonnes pratiques (verrouillage de la session avant son départ), les escroqueries par hameçonnage, les réseaux, l'authentification, les appareils, etc. semblent répétitives, mais nécessaires.

Faites-vous régulièrement des sauvegardes ?

Et si vous perdiez tout d'un moment à l'autre, seriez-vous capable de restaurer vos données et vos systèmes tels qu'ils étaient auparavant ?

Assurez-vous qu'une sauvegarde cloud ainsi qu'une sauvegarde physique ont été réalisées afin de vous préparer au pire des scénario. En cas d'attaque et de paralysie des systèmes, vous aurez toujours une trace de vos données grâce aux sauvegardes de secours. Le blocage ne sera donc que temporaire.

Avez-vous pensé à l'authentification multifactorielle ?

L'authentification multi-facteurs est une sécurité supplémentaire pour vous assurer que votre compte est plus difficile à compromettre. Un mot de passe seul est assez vulnérable surtout s'il ne respecte pas les recommandations de mots de passe forts.

Il existe plusieurs possibilités d'authentification multifactorielle comme :

- La vérification par moyen détenu, tel qu'un compte e-mail ou un smartphone,
- La vérification par quelque chose de propre, comme une empreinte digitale,
- La vérification par la connaissance d'une information clé, comme l'adresse du tout premier lieu de votre résidence ou autre.

Vos systèmes sont-ils à jour ?

On peut se l'avouer, faire une mise à jour Windows est souvent fastidieux, cependant ne l'ignorez pas.

La plupart des microprogrammes et des logiciels mis à jour comprennent des correctifs pour se défendre contre les dernières cyberattaques. Il est donc préférable de s'assurer que tous les dispositifs sont à jour. Toutefois, une mise à jour ne remplace pas le travail d'un logiciel antivirus.

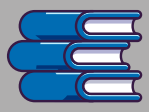
Pourquoi renforcer le travail à distance ?

De plus en plus demandé et instauré par les entreprises, les risques de sécurité liés au télétravail ne sont pas inexistants. Assurez-vous que les employés peuvent se connecter à votre réseau en toute sécurité, peu importe où ils se trouvent. Il est conseillé d'utiliser un service VPN pour accéder au serveur.

Vérifiez que vos salariés n'utilisent pas des appareils qui n'ont pas été approuvés par le service informatique, tels que les téléphones ou ordinateurs portables personnels car ceux-ci pourraient être compromis par des logiciels malveillants ou douteux. Exigez de vos utilisateurs qu'ils utilisent un réseau WiFi protégé, car les connexions ouvertes (en particulier dans les lieux publics) sont vulnérables aux programmes « sniffer » qui peuvent lire et voler les données transmises.

Décorrélez-vous vos comptes ?

Si vous possédez un compte administrateur, utilisez-le avec prudence. Le compte administrateur est un peu votre coffre-fort. Vous devez disposer d'un compte standard pour assurer les tâches quotidiennes qui ne demandent pas de droits élevés ou de requêtes particulières.

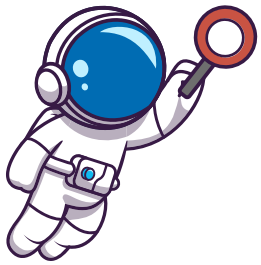


En résumé

Faites de la sécurité et des risques encourus en cas d'attaques informatiques un sujet de discussion dans votre entreprise. La sécurité de l'infrastructure et des données doit être une prise de conscience générale. Demandez à la direction ou au service informatique s'ils prévoient de créer un programme de sensibilisation ou des politiques de sécurité pour informer les collaborateurs internes. Pour finir, vous pouvez appliquer vous-même vos propres règles de sécurité simples à mettre en œuvre.

DIFFÉRENCIATION DES TYPES DE SOLUTIONS

Audit des données : analyse et orientation

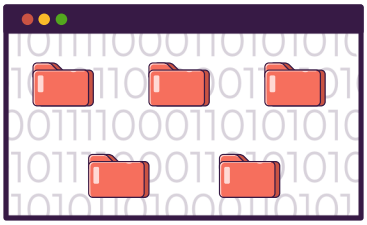


L'audit est une inspection en profondeur de votre situation d'entreprise : « Êtes-vous en conformité ? », « Où se trouvent les vulnérabilités ? », « Quel plan d'actions doit être mis en œuvre pour corriger les faiblesses ? », etc.

L'audit permet de collecter des données issues de vos systèmes et d'identifier les lacunes de sécurité concernant les données et l'infrastructure, pour prendre les mesures correctives afin de réduire votre surface d'attaque.

L'audit aide aussi à savoir si vous rentrez dans les points essentiels de normes et réglementations gouvernementales. Obtenez rapidement les informations requises par les auditeurs et commissaires aux comptes, grâce à des tableaux de bord et rapports d'audit attestant votre

Classification des données : identification et visibilité

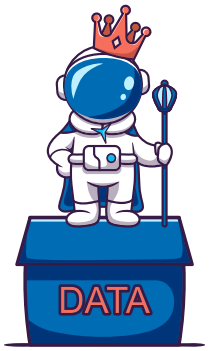


La plupart des solutions d'audit comprennent des fonctionnalités de classification ou de gouvernance des données. Comme mentionné plus haut, partir à la découverte de ses données et les classifier répond à la question simple « Savez-vous où se trouvent vos données sensibles ? ». Cela parait élémentaire, cependant trouver les contenus sensibles (données financières, dossiers médicaux, informations personnelles identifiables) pour les classer logiquement et les protéger est un enjeu majeur.

Une fois ces données identifiées, décorrélées et classées, vous pourrez les sécuriser afin de minimiser leur exposition. Vous pourrez ainsi passer à l'étape suivante : l'assainissement et le suivi de celles-ci.

Une meilleure qualité des données permettra de prendre de meilleures décisions pour l'entreprise.

Gouvernance des données : contrôle et gestion



Les initiatives de gouvernance des données sont souvent motivées par la nécessité de se conformer aux politiques internes, normes et réglementations. La gouvernance répond à différentes questions telles que « Savez-vous qui a accès aux données ? », « Pouvez-vous gérer des habilitations et droits utilisateurs de votre entreprise ? », etc.

Toutefois, les avantages à établir des règles et des procédures claires pour les activités relatives aux données dépassent la simple conformité. Un bon programme de gouvernance des données, c'est une sécurité renforcée, obtenue par la localisation des données critiques en amont, l'identification des propriétaires et des utilisateurs des données, l'évaluation et la correction des risques relatifs aux données critiques. La gouvernance vous donne un contrôle, une gestion et une visibilité accrus de ce qui se passe en temps réel dans votre organisation.

La gouvernance des données n'est pas un projet ponctuel mais un processus continu. A mesure de l'évolution de vos politiques internes, des réglementations, normes gouvernementales et des exigences opérationnelles, votre programme de gouvernance des données doit s'adapter. Vérifiez régulièrement que vos processus et vos technologies continuent de soutenir les objectifs du programme pour apporter des ajustements si nécessaire.

POUR FINIR...

Les solutions d'audit, de classification et de gouvernance des données vous donnent toutes les informations utiles lors de vos recherches sur les incidents potentiels de violation de données. Vous aurez une analyse claire et précise de votre environnement et répondrez facilement aux questions « qui accède à quoi, où et quand ? ». Les autorisations et habilitations jouent un rôle important dans la protection de vos données. C'est pourquoi il faut les modérer, car attribuer un accès complet aux données à tous vos collaborateurs qui ont en réalité besoin d'un accès ponctuel ou limité, revient à donner les clés de toutes les portes de votre entreprise.

En résumé, ces solutions vous aideront à :

- classer toutes vos données,
- sécuriser les informations sensibles,
- surveiller les autorisations dans votre infrastructure,
- alerter lors d'actions suspectes dans vos SI,
- détecter les menaces,
- gérer plus aisément les incidents de sécurité,
- faciliter votre mise en conformité,
- visualiser l'activité interne dans des tableaux de bord,
- justifier votre régularité avec des rapports détaillés.