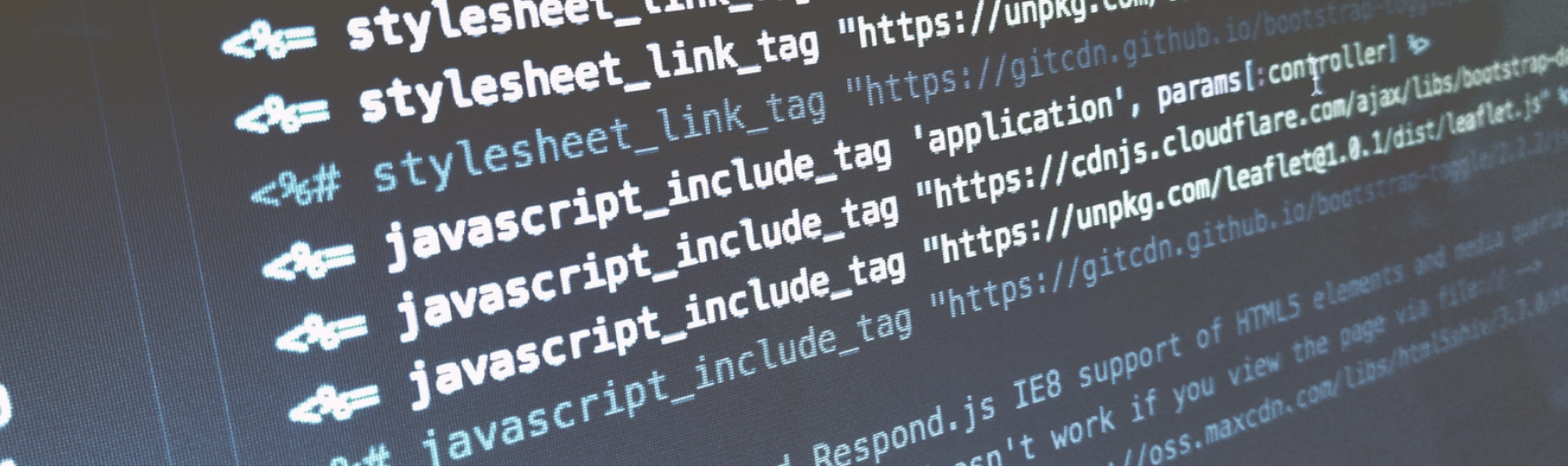

covalen

Hiver 2025

Cyber savoir : les données fantômes, un risque en matière de cybersécurité

Selon Cybercrime Magazine, le stockage mondial de données devrait dépasser 200 zettaoctets en 2025. Un zettaoctet équivaut à un milliard de téraoctets. Cela représente beaucoup de données à sécuriser.

À l'intérieur de ces systèmes de stockage se cachent des données fantômes : des données non contrôlées et incontrôlées qui pourraient exposer les informations sensibles de votre entreprise aux criminels.

Que sont les données fantômes?

Les données fantômes sont des informations créées, stockées et gérées dans des systèmes ou des applis qui ne sont pas sous le contrôle de votre entreprise ou qui échappent au radar des analyses de cybersécurité internes. Cela se produit généralement lorsque les employés utilisent des applis non approuvées ou non standard pour des activités liées au travail. C'est ce qu'on appelle le « shadow IT ». Les employés sont souvent bien intentionnés lorsqu'ils installent ces applis pour augmenter leur rendement ou faire quelque chose que les logiciels de bureau ne leur permettent pas actuellement de faire.

Un exemple de données fantômes

Supposons que votre employé télécharge une appli pour une présentation qu'il fait à son équipe. Ils téléchargent des données propriétaires de l'entreprise dans le cadre de la présentation. Leur application enregistre les informations dans un emplacement de fichier inconnu sur votre réseau et dans le cloud. L'emplacement du fichier ne fait pas partie des analyses de cybersécurité habituelles et échappe à votre radar.

Quelques semaines plus tard, quelqu'un s'infiltre dans votre réseau et reconnait une appli malveillante, Il peut ainsi récupérer les infos de vos fichiers de sauvegarde, sachant qu'ils peuvent contenir des informations précieuses et non cryptés.

Dans cet exemple, le pirate obtient les notes techniques de votre présentation sur le lancement de votre produit top secret. Ils exigent une rançon en échange de la non-divulgation de vos données exclusives.

Gestion des risques liés aux données fantômes

La prolifération des données rend plus difficile leur suivi et leur sauvegarde. Le risque lié aux données fantômes est un problème de cybersécurité qui fait son apparition dans le rapport IBM de 2024 sur le coût d'une violation de données. Selon ce rapport, les violations de données fantômes augmentent en fréquence et en coût :

- 35 % de toutes les violations concernaient des données fantômes.
- Le vol de données fantôme coûte 16 % de plus qu'une violation classique.
- Les violations de données fantômes sont plus difficiles à identifier et à contenir, en particulier dans plusieurs environnements de données (cloud public, cloud privé et sur site).
- 35 % des violations impliquent des données fantômes dans plusieurs environnements de stockage (cloud public, cloud privé et sur site).

Pour lutter contre les données fantômes, vous aurez besoin d'une cybersécurité robuste. Cela inclut une architecture Zero Trust et des politiques strictes sur les logiciels et les appareils. (L'architecture Zero Trust traite tout le trafic réseau comme une menace potentielle.)

Considérations additionnelles de cybersécurité

Voici quelques autres considérations de sécurité :

- Les données fantômes sont des données non sécurisées.
- Les données fantômes peuvent enfreindre le RGPD (règlement général sur la protection des données), la Loi sur la protection des renseignements personnels et les documents électroniques ou la Loi 25 sur la protection des renseignements personnels des citoyens du Québec.
- Les applis non contrôlées peuvent devenir obsolètes ou manquer de cybersécurité, ce qui en fait une cible privilégiée pour les pirates. Ils pourraient conduire à une vulnérabilité Zero Day dans votre système. (Il s'agit d'une vulnérabilité inconnue des développeurs de logiciels, jusqu'à ce que les cybercriminels l'exploitent.)
- Le Shadow IT augmente les risques de vol ou de manipulation de vos données.
- Les données fantômes peuvent retarder la détection et la réponse aux cybermenaces, entraînant ainsi une augmentation des dégâts et des coûts substantiels.

Voici quelques façons d'atténuer les risques liés aux données fantômes :

- Établissez des politiques claires sur l'utilisation d'applics non sanctionnées. Communiquez-les à vos collaborateurs.
- Exécutez des audits réguliers pour découvrir les applis non autorisées au sein de votre entreprise.
- Formez vos employés aux risques liés aux données fantômes lors de l'utilisation d'applis non autorisées. Promouvoir des pratiques logicielles plus sûres.

- Mettre en œuvre des solutions technologiques qui découvrent, contrôlent et protègent le Shadow IT.
- Impliquez vos équipes informatiques afin qu'elles puissent évaluer la sécurité des applis et s'intégrer dans l'écosystème informatique de votre entreprise.
- Établissez des processus pour sauvegarder régulièrement les données critiques.
- Restez au courant de l'évolution des directives technologiques.
- Utilisez des outils de confidentialité des données pour identifier les données sensibles stockées sur vos réseaux, en particulier sur les systèmes d'IA générative.

Le rapport d'IBM aborde également la nécessité pour les entreprises de sécuriser les systèmes d'IA. Mettez en place des mesures de sécurité si vous utilisez l'IA dans n'importe quelle partie de votre flux de travail.

Sécurisez vos données d'IA, y compris les données de formation de l'IA, pour éviter le vol et l'utilisation abusive. Les pirates pourraient polluer les données de formation de votre IA pour fausser ses résultats, ou les voler.

Considérations additionnelles de cybersécurité

Imaginez que vous déployez une appli d'IA générative sur vos réseaux internes. L'équipe de direction a décidé de partager un résumé de ses mises à jour trimestrielles sur les problèmes de performance, les finances et les plans stratégiques avec certains chefs de service. Ils demandent à AI de résumer le document de la réunion sur une seule page, en gardant tous les noms anonymes. L'IA génère un résumé précis sans aucune information personnelle.

À leur insu, l'IA a incorporé le document exécutif original dans son référentiel de données de formation pour référence future, laissant les informations sur les employés et les finances dans une zone non sécurisée. Ces données fantômes exposent votre entreprise à un risque de non-respect des lois sur la confidentialité, laissant la porte ouverte à des poursuites judiciaires et à d'autres responsabilités.

Connaissance des données fantômes

Soyez transparent sur vos politiques de cybersécurité et sur les raisons pour lesquelles il est essentiel de respecter les limites technologiques. S'il existe une appli que vos employés utilisent régulièrement, il est peut-être temps d'intégrer officiellement ce logiciel afin que les employés puissent l'utiliser en toute sécurité. Que ce soit dans le cloud ou sur votre réseau interne, assurez-vous que votre plan de cybersécurité fonctionne pour mettre en lumière les données fantômes.

N'hésitez pas à nous contacter pour discuter de vos besoins d'assurance et découvrir comment nous pouvons vous aider à assurer votre avenir.