Guide de vente sur la sécurité et la gouvernance des données pour les MSP

Ce guide vous aide à avoir les conversations avec les PME qui leur font savoir que vous comprenez leurs préoccupations tout en clarifiant leurs risques pour positionner votre MSP comme le partner de confiance pour sécuriser leur patrimoine de données.

pax8.com

Que sont la sécurité des données et la gouvernance

La sécurité des données et la gouvernance des données sont étroitement liées et toutes deux essentielles à une protection efficace de l'information.

- **Sécurité des données** signifie protéger les informations les plus précieuses de votre client contre l'accès non autorisé, la perte ou l'utilisation abusive, que ce soit par des cybercriminels, des employés ou des menaces alimentées par l'IA.
- **Gouvernance des données** est l'ensemble des politiques, rôles et procédures qui garantissent que les données sont gérées de manière responsable, restent conformes aux réglementations et sont dignes de confiance. Sans une gouvernance appropriée, les efforts de sécurité peuvent manquer des risques cachés, laissant vos clients vulnérables. Une sécurité des données solide et une gouvernance travaillent ensemble pour protéger l'ensemble du patrimoine de données.

Ensemble, ils créent une défense complète qui non seulement protège les données, mais garantit également qu'elles sont traitées de manière responsable, conformément aux réglementations et de façon fiable pour un usage commercial.

Rendre la sécurité des données réelle pour vos clients

74 % des organisations récemment sondées ont subi au moins un incident de sécurité de données au cours de la dernière année.[1] Mais lorsque vous parlez à vos clients de la sécurité des données, il ne s'agit pas seulement de faits et de fonctionnalités. Il s'agit de les aider à vraiment comprendre les risques auxquels leur entreprise fait face chaque jour.

Essayez d'ouvrir la conversation avec quelque chose comme :

« Imaginez laisser un coffre-fort ouvert sans aucune sécurité autour. Aucune caméra ou suivi pour voir qui entre et sort, juste demander à chaque employé de ne pas aller dans le coffre-fort. Ça semble risqué, n'est-ce pas ? Pourtant, c'est exactement ce qui se passe avec les données commerciales sensibles lorsque les bonnes protections, contrôles et surveillance ne sont pas en place. »

Les attaques deviennent plus sophistiquées chaque année avec les outils d'IA responsables de 40 % des incidents de sécurité de données en 2024, soit près du double du chiffre de 2023, et le coût moyen d'une cyberattaque dépasse 250 000 $ et peut atteindre 7 M$.[1]

La cybersécurité n'attend pas

Chaque jour, les organisations subissent des violations de données qui leur coûtent des millions, nuisent à leur réputation et mettent leurs clients et employés en danger. Les initiés sont responsables de 20 % des violations de données, ce qui augmente les coûts. Le coût total moyen des activités pour résoudre les menaces internes sur une période de 12 mois est de 15,4 millions de dollars.[1] La sécurité des données ne consiste pas seulement à respecter la conformité ou à cocher une case, il s'agit de protéger l'entreprise que vous avez travaillé si dur à bâtir.

Scénario	Ce qui se passe	Type de risque
L'employé clique sur un courriel d'hameçonnage et divulgue ses informations de connexion	Une personne externe obtient l'accès aux systèmes sensibles et aux données	Compromission de données par menace externe
Un membre du personnel copie des fichiers sur une clé USB et les téléverse sur son propre nuage	Des informations critiques de l'entreprise se retrouvent entre les mains d'un concurrent	Vol de données par un initié malveillant
Quelqu'un colle accidentellement des données sensibles dans un outil d'IA générative	Les données propriétaires fuient à l'extérieur de l'entreprise	Fuite de données par un initié négligent
Employé mécontent supprime ou modifie des données clés avant de partir	L'entreprise perd des informations essentielles, des projets ou de la propriété intellectuelle	Sabotage de données par un initié mécontent

Si vous ne feriez pas confiance à chaque employé avec un coffre-fort ouvert, ne leur faites pas confiance avec vos informations numériques les plus précieuses sans mesures de sécurité.

Comprendre les risques

Risques externes

- Les attaques de phishing, les logiciels malveillants et les pirates informatiques cherchent constamment des moyens d'entrer.
- Les cybercriminels exploitent les points faibles de vos défenses cyber.

81 % des PME croient que l'IA augmente le besoin de contrôles de sécurité supplémentaires.[2]

Risques internes

- Employés bien intentionnés commettant des erreurs avec des données sensibles.
- Initiés malveillants cherchant le profit ou la vengeance.
- Personnel partant emportant avec eux des données précieuses.

68 % des PME considèrent l'accès sécurisé aux données comme un défi pour les travailleurs à distance.[2]

De nombreux risques proviennent non seulement d'attaques directes ou d'actions d'initiés, mais aussi de lacunes dans la gouvernance des données. Des données mal classifiées, une propriété peu claire et des politiques d'accès faibles exposent les PME aux violations, aux amendes de conformité et à la perte de confiance des clients. Les FSG qui aident leurs clients à mettre en œuvre une gouvernance efficace géreront mieux ces risques et fourniront une sécurité des données plus solide et durable.

Risques nouveaux et amplifiés : IA générative

Ce ne sont plus seulement les menaces traditionnelles qui doivent vous préoccuper. L'IA générative apporte tout un nouvel ensemble de risques de données qui ne peuvent être ignorés. Comme elle introduit de nouvelles surfaces d'attaque et des risques de fuite de données, les clients doivent régir la façon dont les outils d'IA accèdent aux données sensibles et les utilisent. Des politiques de gouvernance solides, telles que la classification des données, l'accès contrôlé à l'IA et la surveillance, aident à s'assurer que l'adoption de l'IA améliore la productivité sans mettre la sécurité des données ou la conformité en péril. Voici les risques de données associés à l'IA générative :

Scénario	Ce qui se passe	Type de risque
Fuites de données sensibles	Les employés partagent accidentellement ou par négligence des données propriétaires ou réglementées avec des outils d'IA	Fuite de données
Menaces internes	Les initiés partagent excessivement ou divulguent intentionnellement des données confidentielles en utilisant l'IA générative, par accident ou par conception	Vol de données/fuite de données
Nouvelles surfaces d'attaque	Les systèmes d'IA générative vulnérables aux attaques (jailbreaks, injections de prompt, hallucinations)	Exfiltration/manipulation de données
Surfaces d'attaque élargies	L'orchestration d'IA, les plug-ins, les défauts de modèle ou les données d'entraînement non protégées introduisent de nouvelles lacunes	Vulnérabilités émergentes de l'IA

Vous ne laisseriez pas un coffre-fort ouvert sans surveillance. Alors pourquoi exposer les données de votre entreprise aux fuites liées à l'IA, aux erreurs ou aux abus internes ? Plus de 80 % des dirigeants craignent les fuites de données sensibles avec l'IA générative, tandis que 75 % des employés du savoir l'utilisent déjà. La menace est réelle : l'IA offre à chacun, employé ou attaquant, de nouveaux moyens de nuire, volontairement ou non.

Plan de sécurité et gouvernance des données pour vos clients PME

Lorsqu'il s'agit de sécurité des données avec vos clients PME, présentez-la comme une stratégie essentielle pour protéger leur entreprise aujourd'hui et à mesure qu'elle évolue, en tenant compte des risques liés à l'IA générative.

Découvrir et classifier les données :

Identifiez quelles données existent, où elles se trouvent, qui en est responsable, et classez-les selon leur sensibilité. Cette visibilité permet une meilleure protection et limite les risques d'exposition.

Gérer l'accès et appliquer les politiques :

Mettez en place des contrôles d'accès par rôle, l'authentification multifacteur et des politiques claires pour encadrer l'accès aux données et aux modèles d'IA.

Appliquer les contrôles de sécurité clés :

Implémentez la sécurité des courriels, la détection des points de terminaison, des sauvegardes isolées et une surveillance continue pour contrer les violations et les attaques liées à l'IA.

Former les employés :

Offrez une formation régulière sur l'hameçonnage, la gestion des données et les risques liés à l'IA. Un personnel bien informé constitue une défense essentielle.

Gouverner l'utilisation de l'IA et la conformité :

Définissez des politiques pour encadrer les flux de données dans les outils d'IA, en assurant confidentialité, usage éthique et conformité réglementaire.

Contrôler le cycle de vie des données :

Gérez les données de la création à la suppression sécurité pour minimiser les risques et maintenir la conformité.

Ce cadre aide les FSG à accompagner les PME dans la mise en place de programmes évolutifs de sécurité et de gouvernance, assurant la protection des données, la conformité et la préparation aux risques liés à l'IA.

Le coût d'une sécurité fragmentée

Les efforts de sécurité fragmentés s'accompagnent souvent d'une gouvernance fragmentée — de multiples politiques incohérentes, des rôles peu clairs et des efforts de conformité non coordonnés. Les FSG qui aident leurs clients à établir une gouvernance unifiée aux côtés d'outils de sécurité intégrés débloquent une visibilité renforcée, une réponse plus rapide et une gestion des risques d'IA plus facile. L'organisation typique utilise plus de 12 solutions différentes pour sécuriser son patrimoine de données. Cela mène à :

Lacunes d'infrastructure

Les systèmes disparates ne peuvent souvent pas « voir » ou se défendre contre les menaces qui se déplacent entre les silos, laissant des angles morts que les

Complexité opérationnelle

Jongler avec plusieurs outils signifie plus de frais généraux, des coûts plus élevés et une plus grande chance de mauvaises configurations ou de lacunes dans

Manque de visibilité unifiée

Sans une vue centralisée, il est presque impossible de repérer, d'enquêter et de répondre aux menaces, en particulier celles qui évoluent rapidement et qui sont

Une sécurité unifiée et intégrée comble ces lacunes—ainsi, vous ne vous protégez pas seulement contre les menaces d'aujourd'hui, mais aussi contre celles de demain.

Faire de Microsoft Purview un pilier de votre stratégie de conformité

Pour finaliser votre stratégie de sécurité des données, nous recommandons d'introduire Microsoft Purview par le biais de Microsoft 365 E5, du module complémentaire Microsoft 365 E5 Compliance ou de Purview Suite for Business Premium. Cette solution complète est spécialement conçue pour :

- Éliminez les silos de données et permettez une protection unifiée dans votre environnement.
- Améliorez la conformité réglementaire avec des outils intelligents et automatisés.
- Protégez les données Microsoft 365 Copilot avec des fonctionnalités de sécurité avancées, prêtes pour l'IA.

Le bundle de conformité Microsoft 365 E5 offre une sécurité des données et une préparation à la conformité de bout en bout. C'est idéal pour les organisations qui se préparent à l'IA générative et aux exigences réglementaires en évolution.

Connectez-vous avec un expert Pax8 pour en savoir plus sur la tarification de Microsoft Purview ou profitez de nos Pax8 Professional Services.

Sécuriser, innover et grandir avec Pax8

Renforcez la sécurité des données de vos clients. Partner avec Pax8 pour offrir des solutions complètes et unifiées qui protègent les informations sensibles contre les attaques externes, les menaces internes et les risques émergents comme l'IA générative.

Pour plus de soutien dans la conduite de conversations avec les clients, accédez à notre Piste de discussion de vente Sécurité des données et télécharger le guide complet "Fiche d'information sur la sécurité des données rempli d'informations et de messages adaptés pour vous aider à vendre en toute confiance des solutions de sécurité de données aux clients PME.

Avec Pax8, vous êtes habilité à établir la confiance, réduire les risques et stimuler une croissance d'entreprise personnalisée grâce à des stratégies de sécurité de données plus intelligentes et plus solides, adaptées aux PME.

pax8.com

1. Microsoft Data Sécurité Index, 2024 https://marketingassets.microsoft.com/gdc/gdcqTplAT/original
2. Woodgate, Scott. « 7 tendances en cybersécurité et conseils pour que les petites et moyennes entreprises restent protégées. » Microsoft, 31 octobre 2004. https://www.microsoft.com/en-us/sécurité/blog/2024/10/31/7-cybersécurité-trends-and-tips-for-small-and-medium-businesses-to-stay-protected/
3. Première étude annuelle sur l'IA générative : Récompenses commerciales vs risques de sécurité, T3 2023, ISMG, N=400