Analyse de l'impact des violations de données

Conclusions du rapport Kiteworks 2024 sur la confidentialité et la conformité des communications de contenu sensible

PRÉAMBULE

Les violations de données sensibles posent de sérieux problèmes de confidentialité et de conformité

32%

des organisations déclarent avoir subi plus de 7 violations de communications sensibles en 2023

- 9% des personnes interrogées ont déclaré "ne pas savoir" combien de violations se sont produites
- Légère baisse par rapport à l'an dernier, où 36% des répondants en avaient déclaré plus de 7
- 42% des entreprises de défense et de sécurité en déclarent plus de 7
- 17% des répondants de l'administration fédérale ont déclaré en avoir subi plus de 10
- La région APAC a enregistré le plus grand nombre de violations : 43% en ont déclaré plus de 7

26%

des répondants ont déclaré avoir payé plus de 5 millions de dollars en frais de litiges suite à des violations de données

3 principaux vecteurs d'attaque pour les violations de données

- 52% phishing
- 51% malware
- 33% Exploitation des mots de passe et identifiants

- 49% ont payé plus de 5 millions de dollars dans le secteur le plus touché : l'enseignement supérieur
- 27% ont payé plus de 5 millions de dollars dans la région la plus touchée : Amériques
- 24% des organisations de plus de 30 000 salariés ont déclaré des frais de litiges à plus de 7 millions de dollars
- 8% ont déclaré que leurs frais de justice s'élevaient à plus de 7 millions de dollars

Kiteworks protège contre les violations de données

Le réseau de contenu privé (PCN) de Kiteworks est enveloppé dans une appliance virtuelle durcie	Consolide tous les canaux de communication de contenu sensible (messagerie électronique, partage de fichiers, SFTP, MFT, formulaires web) en une seule plateforme	Conserve des enregistrements de tous les accès aux données, transferts de fichiers et activités des utilisateurs pour une surveillance en temps réel	Applique un double chiffrement et des contrôles d'accès basés sur des attributs pour protéger les contenus sensibles au repos et en transit	Utilise la détection d'anomalies basée sur l'IA et intègre des systèmes de sécurité avancés tels que DLP et SIEM pour détecter et prévenir les violations de données potentielles le plus tôt possible

Pour connaître toutes les conclusions du rapport 2024 sur la confidentialité et la conformité des communications sensibles, vous pouvez le télécharger ici