Kiteworks

2024

Prévisions comment gérer le risque d'exposition de vos contenus sensibles ?

12 prévisions concernant les communications de contenus sensibles, selon les dernières tendances en matière de cybercriminalité, de cybersécurité et de conformité.

RAPPORT

Introduction: comprendre la notion de risque d'exposition du contenu privé

La gestion des risques liés à la confidentialité des données et à la conformité devient de plus en plus difficile chaque année. Les cybercriminels continuent à faire évoluer leurs stratégies et leurs approches, ce qui rend plus difficile l'identification, l'arrêt et l'atténuation des dommages causés par les attaques malveillantes.[1] Conscients qu'ils peuvent attaquer des centaines, voire des milliers d'entreprises et des millions d'enregistrements en une seule attaque, de nombreux États-voyous et cybercriminels ont ciblé les supply chains. Tendance qui, selon nous, s'accentuera en 2024. Les fournisseurs tiers, y compris les prestataires de services technologiques, ont représenté 15 % de toutes les violations de données réussies l'an dernier.[2] Et comme les grands modèles de langage (LLM) de l'intelligence artificielle générative (GenAI) envahissent le monde numérique, le suivi et le contrôle de nos contenus sensibles sont devenus encore plus difficiles.

En réponse, les organismes réglementaires font évoluer les textes existants en matière de protection de la vie privée et en créent de nouveaux. Ils ont également augmenté les sanctions financières et pénales en cas d'infraction. Cette "réaction en chaîne" ne va pas ralentir, mais continuer à s'accélérer au cours de l'année à venir. En conséquence, les entreprises doivent suivre et contrôler l'accès au contenu et générer davantage de rapports d'audit pour prouver leur conformité.

Le rapport prévisionnel 2024 de Kiteworks sur les communications de contenu sensible présente les grandes tendances de l'année écoulée et les transpose à l'année à venir. De toute évidence, la gestion de la confidentialité et de la conformité de vos communications de contenu sensible (messagerie électronique, partage de fichiers, transfert de fichiers géré (MFT), SFTP et formulaires Web) est délicate, car la plupart des outils utilisés sont cloisonnés. En outre, comme beaucoup de ces outils ont été développés il y a au moins dix ans, ils ne sont pas dotés des systèmes de sécurité modernes nécessaires pour protéger les contenus sensibles contre les cyberattaques. C'est dans ce contexte qu'ont eu lieu cette année des violations de données importantes. Les organisations sont vigilantes et la plupart d'entre elles analysent les outils de communication utilisés actuellement et envisagent de nouvelles alternatives. Plutôt que de conserver ces outils dans des silos séparés, de plus en plus de structures vont chercher à les centraliser au sein d'une seule et même plateforme en 2024 (imaginez n'avoir qu'un seul journal d'audit et une gestion consolidée des politiques en un seul et même endroit).

12 prévisions 2024 sur la confidentialité et la conformité des communications de contenu

1. Risques liés à la confidentialité des données et à la conformité des LLMs

Malgré les interdictions et les restrictions, le nombre d'employés et de tiers utilisant les LLM de GenAI va probablement doubler par rapport à 2023, les atouts concurrentiels se révélant bien trop précieux pour être ignorés. 15 % des employés, par exemple, publient régulièrement des données d'entreprise dans les LLM de GenAI, et un quart de ces données sont considérées comme sensibles. Cela va augmenter le spectre des menaces et le potentiel d'exposition de la propriété intellectuelle, des données personnelles identifiables, des rapports financiers, des informations sur les fusions et acquisitions, ou encore des messages de l'IA. Ainsi, les risques de fuite de données sensibles vont s'accroître, avec les conséquences que cela implique en termes d'atteinte à l'image de marque, d'amendes et de sanctions réglementaires, et de frais de justice.

Même avec les progrès des mécanismes de sécurité, les violations de données résultant d'une mauvaise utilisation de la GenAI LLM augmenteront en 2024. Il est probable que des incidents très médiatisés viennent ébranler la confiance des clients et attirent l'attention des autorités de régulation. De ce fait, la sécurité des données devra être au cœur des stratégies de GenAI LLM. Les organisations qui tarderont à s'adapter s'exposeront à une dégradation de leur image de marque, à des pertes de chiffre d'affaires, à des amendes ainsi qu'à des frais de justice récurrents.

Pour limiter les risques, les meilleurs élèves déploieront des stratégies de sécurité zéro trust basée sur le contenu pour contrôler l'accès et la collaboration en fonction de la sensibilité des données. Dans l'idéal, ces organisations appliqueront des contrôles d'accès granulaires, le principe du moindre privilège et interdiront les accès non-authentifiés. Cette évolution vers le zéro trust basé sur le contenu implique également des politiques de prévention des pertes de données (DLP) en temps réel, ainsi que l'enregistrement et la surveillance de tous les accès et transferts de contenu.

Les fonctionnalités avancées de prévention des pertes de données (basées sur l'analyse du contenu et l'évaluation des risques) s'étendront aux appareils et aux e-mails et permettront de surveiller en temps réel les interactions entre les GenAI et les LLM. L'utilisation de la gestion des droits numériques (DRM) pour les contenus à haut risque se développera considérablement pour permettre la collaboration tout en empêchant le vol de données. En outre, il y aura plus de budget formation pour sensibiliser le personnel à la sécurité des données et à une utilisation responsable des GenAI LLM. Les entreprises qui entreprennent dès maintenant de sécuriser les données non structurées, d'instaurer une gouvernance stricte, un suivi et des contrôles de sécurité limiteront les risques liés à la sécurité et à la conformité.

Près des deux tiers des entreprises expérimentent (29 %) ou développent (33 %) actuellement avec GenAI.[4]

Seulement 20 % des organisations ont mis en place des processus pour atténuer l'utilisation des informations personnelles identifiables dans les LLMs d'IA générative.[5]

2. Confidentialité des données et réglementations et normes relatives aux LLMs

Comme mentionné précédemment, l'émergence des LLM GenAI pose des problèmes importants de confidentialité des données et de conformité aux organisations, et les organismes réglementaires s'empressent d'instaurer des mesures en conséquence.

Au premier rang de ces initiatives réglementaires figure le décret de la Maison Blanche du 30 octobre (EO), qui vise à surveiller et à réglementer les risques liés à l'IA tout en exploitant son potentiel. Le décret appelle le Congrès à agir et demande spécifiquement aux agences fédérales de prendre des mesures au cours de l'année à venir. Il fixe de nouvelles normes en matière de sûreté et de sécurité de l'IA, protège la confidentialité des données des citoyens américains et promeut un écosystème et un marché équitables, ouverts et compétitifs pour l'IA et les technologies connexes.[6] Le texte s'appuie sur les recommandations du National Institute of Standards and Technology (NIST) et impose au gouvernement fédéral américain[7] des obligations concernant l'utilisation, l'évaluation et l'acquisition de logiciels et de systèmes d'IA. Outre l'accent porté sur les bouleversements causés par l'IA sur le marché du travail, ce décret exigera des développeurs de systèmes d'IA qu'ils partagent les résultats de leurs tests de sécurité avec le gouvernement fédéral avant de les rendre accessibles au public.

Le décret est la première étape du plan du gouvernement fédéral pour lutter contre l'IA, et devrait être suivie par des lois au niveau fédéral et au niveau des États en 2024. À l'heure actuelle, au moins 25 États américains envisagent de légiférer en matière d'IA et 15 ont déjà adopté des lois ou des résolutions.[8]

En dehors des États-Unis, l'Union européenne travaille à l'élaboration d'une loi sur l'IA, qui entrera en vigueur progressivement d'ici à 2026.[9] Cette loi vise à fournir aux développeurs, déployeurs et utilisateurs d'IA des exigences et des obligations claires concernant des utilisations spécifiques de l'IA, tout en réduisant les charges administratives et financières pour les entreprises, en particulier les PME. La loi définit quatre niveaux de risque en matière d'IA : risque inacceptable, risque élevé, risque limité et risque minimal ou nul. Les systèmes d'IA à haut risque seront soumis à des obligations strictes avant d'être mis sur le marché.

Le National Institute of Standards and Technology (NIST) voit émerger des normes en matière d'IA. Plus précisément, le NIST AI RMF Playbook met l'accent sur l'établissement de politiques visant à gérer les risques liés aux systèmes tiers, à tester la sécurité et la résilience par le biais d'exercices en équipe rouge. Il met également en œuvre des contrôles de gouvernance des données et de confidentialité, des mécanismes de transparence et de recours, documente la traçabilité des systèmes. Enfin, il renforce les procédures de surveillance et prévoit l'intégration de la gestion des risques dans les politiques et les procédures. [10] En 2024, les organisations utilisant le NIST AI RMF devront poursuivre leurs efforts concernant la gestion des risques liés aux contenus sensibles par des contrôles robustes combinés à des pratiques d'IA responsables (explicabilité, responsabilité, communication transparente des risques, etc.).

À mesure que les exigences et les normes de sécurité émergent, les organisations devront être en mesure de justifier aisément qu'elles sont conformes aux normes réglementaires, et le suivi de la gouvernance sera indispensable, notamment par le biais de journaux d'audit détaillés. Les experts estiment que les normes d'IA seront mises en œuvre et rendues obligatoires dans les 6 derniers mois de l'année 2024, car il faudra du temps pour les créer et les rendre opérationnelles.

Forrester prévoit au moins trois violations de données liées à un code non sécurisé généré par l'IA, et qu'au moins une entreprise se verra infliger une amende pour mauvaise manipulation des informations personnelles identifiables.[11]

3. Besoin d'une approche MFT plus moderne

De nombreuses solutions de transfert de fichiers gérés (MFT) sont basées sur des technologies vieilles de plusieurs décennies et présentent des lacunes intrinsèques en matière de sécurité. Les déploiements sur site privilégiés par de nombreux clients comportent des fonctionnalités variées qui résident dans des silos et ne sont pas protégées par le fournisseur ; les clients doivent définir et mettre en œuvre une stratégie de protection telle que des pare-feux réseau et d'application web, la détection d'intrusion, la suppression des services et du code inutilisés, et des technologies antivirus. L'approche cloisonnée fait également peser sur le client la responsabilité de la gestion des vulnérabilités : détection de la nécessité de mettre à jour le code, recherche de versions compatibles de tous les composants cloisonnés, tests d'intégration des composants mis à jour, puis migration vers la production. En outre, les solutions MFT existantes sont souvent dépourvues de technologies de sécurité avancées telles que la prévention des pertes de données (DLP), la prévention des menaces avancées (ATP) et le désarmement et la reconstruction du contenu (CDR).

En 2024, les entreprises chercheront une appliance virtuelle moderne permettant d'appliquer une mise à jour centralisée en un seul clic, fournie par le fournisseur de solution MFT. Mais aussi des solutions MFT qui intègrent des capacités de sécurité avancées pour faire face à la complexité et au nombre de cybermenaces sans précédent.

Les outils MFT sont utilisés pour le transfert numérique de données de manière automatisée, fiable et sécurisée en interne et avec des tiers, grâce à un suivi de la gouvernance et à des contrôles de conformité réglementaire. En tant qu'élément de la supply chain logicielle, le risque lié aux anciennes solutions de MFT est considérable. Au cours des dernières années, nous avons assisté à la multiplication des cyberattaques contre les logiciels supply chain par les États-voyous et les cybercriminels. Au début de l'année, IBM a révélé que 12 % des violations de données impliquaient la supply chain logicielle, dans son rapport annuel sur le coût des violations de données. Dans le même temps, les tiers, partie intégrante de la supply chain logicielle, représentent un élément de risque important (15 % des violations de données leur sont imputables).[12]

En 2023, deux grands outils MFT ont été victimes d'exploits de type "zero-day" par Clop, un cyber-gang russe ayant l'habitude de s'en prendre aux outils de MFT. Dans les deux cas, plusieurs vulnérabilités de type "zero-day" étaient visées ; une exécution de code à distance (RCE) dans le cas de Fortra GoAnywhere qui a touché plus de 130 organisations[13], et une injection SQL dans le cas de MOVEit qui a touché plus de 2 000 organisations et 62 millions d'individus.[14]

Si l'on en croit les deux attaques MFT de 2023, les États-voyous et les cybercriminels continueront d'exploiter les vulnérabilités de type "zero-day" dans les solutions MFT existantes en 2024. En cas de violation d'un outil MFT, les conséquences sur la supply chain peuvent exposer les données sensibles de centaines, voire de milliers d'organisations représentant des millions de personnes. L'impact réglementaire pourrait être spectaculaire en termes d'amendes et de sanctions, de coûts juridiques, de recours collectifs et d'atteinte à l'image de marque.

12 % des violations de données survenues l'année dernière concernaient des logiciels supply chain.[15]

4. Nécessité d'une passerelle de protection des e-mails moderne

L'e-mail reste le premier vecteur d'attaque des logiciels malveillants et de l'hameçonnage. Les attaques de logiciels malveillants par voie électronique ont augmenté de 29 % au cours de l'année écoulée, et les attaques par hameçonnage de 29 %.[16] Les attaques par compromission de messagerie professionnelle (BEC) ont quant à elles connu une hausse de 66 %. Le rapport Verizon sur les violations de données révèle que les attaques par BEC ont doublé par rapport à l'année dernière et que le montant moyen dérobé par attaque atteint 50 000 dollars.[17] En ce qui concerne les attaques de phishing et de BEC, l'absence de filtres efficaces et de visibilité sur le contexte des courriels complique la détection et le blocage des attaques par ingénierie sociale.[18] Plus de 8 violations de données sur 10 ciblent les utilisateurs comme première ligne d'accès en utilisant des stratégies d'ingénierie sociale. Enfin, les approches traditionnelles de sécurité de la messagerie ne sont pas efficaces contre les attaques de type "zero-day" et s'appuient sur la sensibilisation des utilisateurs pour détecter et signaler les messages suspects; or ces derniers peuvent être facilement dupés.

Tout comme les anciennes solutions MFT, les anciens systèmes de messagerie n'ont pas les capacités de sécurité modernes. La bonne nouvelle, c'est que le chiffrement des e-mails s'est considérablement amélioré. Une enquête menée auprès de responsables informatiques a révélé que 90 % d'entre eux privilégiaient la protection des documents et des informations transmis par e-mail à d'autres organisations.[19] Lorsque ces documents sont partagés en interne, les chiffres ne sont pas aussi bons : 79 % des entreprises indiquent partager des données commerciales sensibles par e-mail sans les chiffrer.[20] Par ailleurs, bien que les entreprises utilisent le chiffrement, une étude récente a révélé que seules 35 % d'entre elles déclaraient avoir déployé un chiffrement généralisé à tous les niveaux.[21]

Il y a plusieurs raisons pour lesquelles les organisations continuent à se battre avec le chiffrement des e-mails. La première est qu'il peut être complexe et difficile à utiliser.[22] Il existe différents types et niveaux de chiffrement (PGP, S/MIME, DANE, STARTTLS, par exemple), et l'échange de clés publiques peut s'avérer fastidieux et source de risques. Par exemple, lorsque les e-mails chiffrés ne peuvent pas être déchiffrés, les organisations doivent recourir à des options moins idéales (et moins sûres), comme s'inscrire à un service de messagerie gratuit mais non autorisé pour transmettre le contenu, demander à l'expéditeur d'utiliser un lien de lecteur partagé non chiffré mais non publié, ou demander à l'expéditeur d'envoyer un fichier Zip chiffré par un mot de passe.

D'autres lacunes dans la sécurité de la messagerie existent, telles que l'absence de gestion des droits numériques (DRM), de prévention de la perte de données (DLP) et de détection avancée des menaces, un stockage cloud non sécurisé qui ne dispose pas de chiffrement et de contrôles d'accès, une mauvaise gestion des identités et des accès, et des serveurs de messagerie sur site obsolètes ou mal configurés.

D'après les données ci-dessus, la sécurité de la messagerie électronique restera un enjeu majeur pour les entreprises en 2024. Tant que les professionnels n'adopteront pas une passerelle de protection des e-mails pour gérer les politiques zéro trust et un hébergement à locataire unique, la sécurité des e-mails restera un facteur de risque important, tant en termes de confidentialité des données que de conformité réglementaire.

Les attaques par hameçonnage ont augmenté de 47,2 % au cours de l'année passée, les secteurs de l'enseignement et de la finance étant les principales cibles.[23]

5. Multiplication des réglementations et des normes en matière de confidentialité des données

L'année 2023 a été marquée par la démultiplication des réglementations et des normes en matière de protection de la vie privée. Gartner prévoit que les données personnelles des trois quarts de la population mondiale soient couvertes par des réglementations d'ici fin 2024, et que le budget annuel moyen alloué à la protection de la vie privée en entreprise dépasse les 2,5 millions de dollars[24]. Les efforts de réglementation en matière de protection des données personnelles vont s'étendre à des dizaines de juridictions au cours des deux prochaines années. Outre la Californie, quatre autres États américains ont promulgué des lois sur la confidentialité des données en 2023, dix autres ont adopté à ce jour des lois en la matière et les promulgueront en 2024 et 2025. De nombreux autres États ont des lois sur la confidentialité des données à divers stades de délibération législative.

La confidentialité des données n'est pas qu'un phénomène américain. Le problème est mondial et il est certain que l'année 2024 mettra davantage l'accent sur les réglementations en matière de confidentialité des données. Le RGPD, par exemple, est suivi de nombreuses législations européennes, comme la loi sur les marchés numériques, la loi sur les services numériques et le règlement sur l'intelligence artificielle.

En juillet 2023, l'UE a approuvé le nouveau cadre de confidentialité des données qui facilite les transferts de données de l'UE, du Royaume-Uni et de la Suisse vers les États-Unis, en précisant le processus d'autocertification pour les organisations qui souhaitent y participer. Pour participer, une entreprise américaine doit s'auto-certifier auprès du ministère du commerce et s'engager à respecter les principes du (des) cadre(s) concerné(s). La conformité est obligatoire une fois que l'organisation s'est auto-certifiée. Le ministère du commerce tient à jour une liste publique des organisations participantes. Pour pouvoir faire valoir sa participation et recevoir des données à caractère personnel conformes, une organisation doit figurer sur la liste. Si elle est retirée de la liste, elle ne peut plus se prévaloir de sa participation et de sa conformité. Toutefois, elle doit continuer à appliquer ces principes aux données reçues précédemment. Les référentiels facilitent les flux de données transatlantiques essentiels aux entreprises, tout en garantissant la protection des données à caractère personnel.

Le Cadre de protection de la vie privée du NIST a été publié en 2020 et s'est avéré être un guide précieux. Sur la base des projets de mise à jour du cadre de cybersécurité du NIST (CSF), il sera probablement élargi en 2024 afin de mieux prendre en compte la gestion des risques d'entreprise dans les domaines juridique, financier et de la protection de la vie privée. Les organisations seront ainsi mieux à même d'évaluer et d'atténuer les risques liés à la protection de la vie privée de manière globale. L'alignement du cadre de protection de la vie privée sur le projet de loi fédérale indique qu'il s'agira d'un outil de conformité incontournable. Les mises à jour attendues en 2024 prévoient une meilleure intégration avec le cadre de cybersécurité du NIST afin de mieux prendre en compte la protection de la vie privée en tant que risque d'entreprise. Au même titre que le risque financier et juridique, le cadre de protection de la vie privée fournit des conseils sur la gestion des risques liés à la protection de la vie privée dans l'ensemble de l'entreprise, et non pas uniquement dans les systèmes informatiques[25], et s'aligne sur les nouvelles réglementations en matière de protection de la vie privée pour faciliter la mise en conformité.[26]

Les modifications prévues du Cadre de Cybersecurité du NIST (CSF) méritent également d'être soulignées. Le NIST a publié un projet de mise à jour du CSF en août 2023 et prévoit de publier la version finale du CSF 2.0 début 2024.[27] Le cadre mis à jour vise à attirer davantage d'organisations tout en élevant les pratiques de gestion des risques. Les principaux changements sont l'évaluation continue des risques, l'amélioration continue, le renforcement de la gestion des risques de la supply chain et la multiplication des exemples de mise en œuvre. Pour beaucoup d'organisations, il reste difficile de prouver qu'elles sont en conformité avec les réglementations en matière de confidentialité des données. En 2024, un plus grand nombre d'organisations centraliseront la gouvernance et l'utilisation des journaux d'audit utilisés pour le suivi et le reporting. Toutefois, de nombreuses organisations font encore état d'approches cloisonnées en matière de communication des contenus sensibles, ce qui peut compliquer la démarche.

6. Importance croissante de la souveraineté des données

En 2024, localiser les données est un défi majeur de la souveraineté des données pour les organisations.[28] La Conférence des Nations unies sur le commerce et le développement indique que 70 % des pays réglementent la manière dont les entreprises collectent, stockent et utilisent les données de leurs citoyens.[29] Nombre de nouvelles lois sur la protection de la vie privée obligent les organisations à contrôler le pays où se trouvent les données, ce qui peut poser problème aux organisations multinationales. Dans le même temps, la démocratisation des données, qui consiste à rendre les données accessibles et utilisables par tous les membres d'une entreprise quelles que soient leurs compétences techniques, aura un impact sur la souveraineté des données. Cette tendance obligera les organisations à s'assurer que les données sont accessibles à tous les interlocuteurs tout en maintenant la souveraineté des données. La souveraineté des données s'applique à tous les types de données, informations personnelles identifiables (PII) et autres données liées aux activités et aux opérations d'une entreprise.

Les organisations de tous les secteurs économiques (secteur public, technologie, santé et finance) accordent de plus en plus d'importance aux initiatives de souveraineté des données du fait de leurs avantages. La souveraineté des données permet de rester conforme aux réglementations locales et internationales, ce qui minimise les risques juridiques, renforce la réputation d'une gestion responsable des données et aide les entreprises à éviter de lourdes amendes. En priorisant la souveraineté des données, les organisations renforcent la confiance des clients et des partenaires, améliorent leur réputation et évitent des problèmes juridiques coûteux.

Les décisions relatives au déploiement des applications sont fortement influencées par les exigences en matière de souveraineté des données, en particulier dans les pays dotés de lois strictes comme l'Allemagne et la Chine. Le CLOUD Act des États-Unis, qui oblige les entreprises américaines à fournir des données en cas de mandat ou de citation à comparaître, quel que soit l'endroit où elles sont stockées, complique les opérations internationales et risque d'enfreindre des réglementations telles que le RGPD. Les options d'hébergement multi-locataires risquent d'entraver le respect de la souveraineté des données et de compliquer la tâche des entreprises qui doivent prouver qu'elles respectent les lois sur la localisation des données.

Les clients qui exigent la souveraineté des données préfèrent souvent s'adresser à des fournisseurs qui hébergent leurs services dans leur pays. Pour les services cloud, les zones d'hébergement nationales peuvent suffire, à moins qu'elles ne soient affectées par une législation telle que le CLOUD Act américain. Dans les scénarios plus complexes, les entreprises opteront de plus en plus pour un hébergement sur leur propre sol ou utiliseront des fonctions de souveraineté des données dans leurs applications pour gérer les déploiements multi-pays, bien que cela puisse poser des problèmes lors des audits de conformité.[30]

Lorsque les clusters d'applications s'étendent sur plusieurs pays, la fonctionnalité de zone de souveraineté des données est bien utile. Pour contrebalancer, il faut s'attendre en 2024 à ce que les entreprises se tournent vers l'hébergement à locataire unique, pour simplifier la souveraineté des données et leur aptitude à la démontrer.

Les entreprises opteront de plus en plus pour l'hébergement sur leur propre territoire ou utiliseront les fonctionnalités de souveraineté des données dans leurs applications pour gérer les déploiements multi-pays, même si cela pose des problèmes de conformité.

7. Augmentation des amendes pour violations de la confidentialité des données

Les amendes et les pénalités associées aux violations de la confidentialité des données ont augmenté au cours des deux dernières années, atteignant des records pour les violations du RGPD. Cela devrait se poursuivre en 2024. Parmi les amendes les plus importantes infligées en 2023, 1,3 milliard de dollars infligés à Meta (Facebook) par la Commission irlandaise de protection des données, 391,5 millions de dollars infligés à Google dans le cadre d'un accord avec 40 États américains, 61,7 millions de dollars infligés à Amazon par la FTC, et 2,1 millions de dollars infligés à Uber, également par la FTC.

Les autorités de régulation se concentrent sur l'application des lois relatives à la protection de la vie privée et sur l'imposition d'amendes en cas d'infraction. Une gouvernance et une sécurité laxistes font des entreprises une cible facile qui servira d'exemple avec des sanctions lourdes. Par exemple, les récentes amendes infligées à Marriott et British Airways dans le cadre du RGPD étaient en grande partie dues à des lacunes en matière de sécurité des données. Ce précédent indique que les régulateurs vont sévir contre les entreprises qui exposent des données personnelles par négligence. Au fur et à mesure que de nouvelles lois sur la confidentialité des données seront adoptées, tant par les États américains que dans le monde entier, les répercussions financières continueront de croître.

L'application des réglementations sur la protection des données ne diminuera pas en 2024, la majeure partie de la population mondiale étant désormais couverte par des réglementations en la matière. L'accent est mis de plus en plus sur la protection des données, de sorte que de plus en plus d'organisations adopteront des pratiques spécifiques en matière de confidentialité des données. Pour les organisations opérant dans plusieurs pays, une nouvelle approche de la conception et de l'acquisition du cloud à travers les modèles de service sera utile pour s'adapter aux différentes stratégies de localisation en 2024.

Plus d'amendes RGPD ont été imposées au cours du premier semestre 2023 qu'en 2019, 2020 et 2021 réunis, atteignant plus de 1,8 milliard de dollars.[31]

75 % de la population mondiale aura ses données personnelles couvertes par des réglementations sur la confidentialité d'ici la fin de 2024.[32]

8. Adoption de solutions de communication de contenu sensible autorisées par FedRAMP

La loi James M. Inhofe sur l'autorisation de la défense nationale (NDAA) pour l'exercice fiscal 2023, signée par le président Joe Biden, codifie le programme FedRAMP au sein de l'Administration des services généraux. Elle met en œuvre des modifications importantes conçues pour simplifier davantage les processus d'adoption et d'utilisation des services cloud par le gouvernement. Le Bureau de la gestion et du budget (OMB) a également publié un projet de directives pour moderniser FedRAMP et répondre aux défis actuels du cloud. Pour cela, FedRAMP va renforcer son approche de l'examen de la sécurité, et accélérer l'adoption sécurisée des produits et services cloud au sein du gouvernement fédéral.[33]

D'ici 2024, l'autorisation FedRAMP, aujourd'hui obtenue sous couvert d'un processus annuel d'audit rigoureux, sera probablement une exigence de base pour tout fournisseur de services cloud souhaitant travailler avec le gouvernement fédéral américain. Pour les prestataires de la base industrielle de la défense (DIB), la CMMC 2.0 inclut les exigences FedRAMP, et le fait d'avoir des communications de données de fichiers et d'e-mails autorisées par FedRAMP leur facilite grandement la tâche. Comme les prestataires du DIB chercheront à obtenir la certification CMMC Niveau 2 en 2024, ils se tourneront vers des technologies adaptées, y compris pour les communications de fichiers et d'e-mails.

9. Émergence de la gestion des droits numériques pour protéger les contenus sensibles

L'adoption de la gestion des droits numériques (GDN) s'accélérera pour que les organisations puissent protéger le contenu sensible et être conformes aux futures réglementations.[34] Les études de marché prévoient une forte croissance de la GDN, pouvant potentiellement dépasser les 5 milliards de dollars d'ici 2024.[35] Gartner indique que l'intégration de la GDN aux futures technologies sera impactante et certainement un point important pour les organisations en 2024.[36] Pour la gestion des politiques basées sur le contenu, les organisations se tourneront vers les normes de sécurité comme le Cadre de Cybersecurity du NIST (CSF) et le NIST 800-53.

Les motivations sont l'augmentation des cyberattaques, les lois sur la confidentialité des données, et la demande pour le contrôle du partage de contenu interne et externe. La GDN nouvelle génération est cruciale pour la confidentialité des données, car elle offre une protection efficace des données sensibles lorsqu'elles quittent le périmètre de l'organisation. Pour réussir avec la GDN, les organisations ont besoin d'un suivi unifié, d'un contrôle, et d'une visibilité à travers leurs écosystèmes numériques. Et donc le respect des bonnes pratiques en matière de gouvernance, de flux de travail et de contrôles d'accès.

Pour 2024, la classification des données et la GDN pousseront les organisations à adopter le principe du moindre privilege et les filigranes pour les données à faible risque, la GDN en mode lecture seule pour les données à risque modéré, jusqu'à l'édition en streaming vidéo sécurisé qui bloque les téléchargements et le copier-coller pour les données à haut risque. Les secteurs d'activité très réglementés seront les premiers à adopter la GDN nouvelle génération. La santé, par exemple, est l'un des secteurs les plus visés par cyberattaques, et doit protéger d'immenses volumes de données personnelles partagées, envoyées, reçues, et stockées au sein de leurs organisations et en externe. Les établissements financiers, les industriels, les cabinets d'avocats, les agences gouvernementales, et les établissements d'enseignement supérieur sont particulièrement concernés par les échanges de données par e-mail à haut risque. Par conséquent, ils seront les premiers à se tourner vers la GDN nouvelle génération pour gérer les risques en matière de confidentialité des données et de conformité.

Seules 22 % des organisations ont déjà instauré des règles de suivi et de contrôle des accès aux contenus sensibles pour savoir à qui ils sont envoyés et partagés.[37]

10. Outils de sécurité avancée dans les communications de contenu sensible

Des outils de cybersécurité avancés peuvent s'intégrer à des solutions pour l'envoi, le partage et le stockage de contenu sensible : prévention des pertes de données dans le cloud (DLP), protection avancée contre les menaces (ATP) pour l'antivirus nouvelle génération et la detection sandbox, Content Disarm and Reconstruction (CDR). En 2024, les organisations adopteront des outils de cybersécurité avancés pour appliquer des politiques et des analyses sur les données en transit et au repos. Avec la DLP, les organisations peuvent analyser les emails sortants et les pièces jointes pour prévenir les fuites accidentelles de données sensibles. Le CDR peut filtrer les documents entrants en supprimant le contenu actif pour la sécurité. Les plateformes MFT prennent souvent en charge nativement la DLP, l'antivirus, la sandbox et les protections avancées. Leur intégration dans le processus de transfert de contenu favorise la sécurité et prévient la fuite et la perte de données en bloquant les transferts qui violeraient les politiques. Les malwares sont bloqués à l'entrée de l'environnement grâce à l'analyse antivirus et à la detection sandbox. Enfin, le contenu entrant est assaini via le CDR.

En 2024, les organisations chercheront à avoir plus de visibilité sur les flux de données pour améliorer leur surveillance et obtenir des journaux d'audit détaillés. L'application des politiques de sécurité sera simplifiée par le recours à des plateformes centralisées comme le MFT. Les outils de communication de contenu sensible comme l'e-mail, le partage sécurisé de fichiers, le MFT et les formulaires web bénéficient tous de l'intégration étroite de l'ATP.

Le marché du désarmement et de la reconstruction du contenu (CDR) devrait croître à un taux de croissance annuel composé (TCAC) de 15,7 % jusqu'en 2026 en raison du coût des violations de données et d'une réglementation et conformité plus strictes pour la sécurité du contenu.[38]

Le marché de la prévention des pertes de données (DLP) devrait croître à un taux de croissance annuel composé (TCAC) de 22,3 % jusqu'en 2030 en raison d'une attention portée à la découverte de données, à l'application des politiques, à la classification des données et à la réponse aux incidents.[39]

11. Centralisation des communications de contenu sensible et le réseau de contenu privé (PCN)

Les architectures traditionnelles zéro trust se concentrent sur la sécurisation du périmètre du réseau et la vérification des utilisateurs et des appareils qui tentent de se connecter. Or, le contenu vit au-delà du périmètre, et les réseaux ne tiennent pas compte de la sensibilité du contenu. C'est là tout l'intérêt du réseau de contenu privé (PCN), qui gère l'importance de la sensibilité du contenu par rapport à la topologie du réseau. Un PCN exploite les principes de confiance définis par le contenu, attribuant des étiquettes de sensibilité et appliquant les mesures de protection appropriées ; chiffrement et contrôle d'accès. Ainsi, les mesures de sécurité sont proportionnées au niveau de sensibilité du contenu et non plus simplement à son emplacement dans l'infrastructure réseau.

L'architecture PCN transcende les modèles traditionnels zéro trust en intégrant une gestion complète des politiques qui s'ajuste dynamiquement à la classification de sensibilité du contenu. Ce système applique automatiquement des politiques de risque en fonction du rôle utilisateur, de la classification du contenu et des actions prévues, déterminant ainsi la légitimité et l'étendue des permissions d'accès ou de transfert. Cette granularité dans l'application des politiques est cruciale pour maintenir des postures de sécurité rigoureuses, en particulier lorsqu'il s'agit de données sensibles qui nécessitent des étapes de vérification supplémentaires comme des formulaires de justification ou des approbations managériales.

Le PCN facilite également le processus de journalisation, lequel enregistre méticuleusement toutes les interactions de contenu pour fournir un historique complet pour la conformité réglementaire et l'audit interne. Cette visibilité sur le flux et l'utilisation des données sensibles est la pierre angulaire de l'approche zéro trust, qui repose sur le principe de ne jamais faire confiance, toujours vérifier.

La dynamique pour étendre la sécurité et la conformité à la couche de contenu continuera en 2024. Les organisations chercheront les meilleurs outils de protection et de gestion des canaux de communication de contenu sensible dans une plateforme PCN unifiée utilisant des politiques de sécurité et de conformité zéro trust.

Près de 75 % des organisations indiquent que l'évaluation et la gestion des communications de contenu sensible nécessitent soit une amélioration significative, soit une amélioration certaine.[40]

12. Multiplication des échanges de fichiers très volumineux contenant du contenu sensible

Les défis autour de la gestion des fichiers volumineux contenant du contenu sensible deviendront de plus en plus centraux. Ils concernent de plus en plus de secteurs d'activité. L'industrie biotechnologique, par exemple, assiste à une explosion de la taille des fichiers de données de séquences d'ADN à mesure que la recherche génétique et la médecine personnalisée gagnent du terrain. De même, les progrès en matière de conception et d'ingénierie conduisent à des fichiers CAD plus lourds et plus complexes. Dans l'application de la loi, l'utilisation de preuves vidéo devient de plus en plus courante et nécessite des solutions de stockage et de transfert sécurisées et efficaces. Les services marketing exploitent la vidéo et les graphiques haute résolution pour avoir un impact commercial. La finance, la science et la recherche médicale voient leurs fichiers augmenter en taille et en sensibilité. Ces tailles de fichiers croissantes nécessitent des solutions robustes pour les manipuler et les stocker en toute sécurité.

Comme mentionné plus haut, un autre aspect à surveiller est les ensembles de données d'entraînement pour les LLMs privés, un domaine émergent qui se développe très vite. À mesure que ces modèles deviennent plus avancés et adaptés aux besoins spécifiques des organisations, les ensembles de données sur lesquels ils s'entraînent augmenteront en taille et en confidentialité. Cette tendance suggère que la gestion de grands ensembles de données d'entraînement sensibles va devenir un point critique.

L'aspect du service client pour les produits logiciels a mis en lumière l'importance de la gestion de grands fichiers de logs et d'archives HTTP (HAR), qui contiennent une richesse d'informations sensibles. La faille de sécurité d'Okta illustre les vulnérabilités que ces fichiers peuvent présenter.[41] Ce défi est accentué par le recours des employés à des méthodes non approuvées et non sécurisées de transfert de fichiers lourds, augmentant ainsi les risques pour la vie privée. Bien que des solutions de stockage cloud pour professionnels comme Microsoft 365 et Box aient augmenté les limites de taille de fichiers pour accueillir jusqu'à 250 Go, celles-ci restent largement insuffisantes par rapport aux besoins réels d'utilisation. Ces plateformes, et d'autres, continueront à être sous pression pour soutenir le transfert sécurisé et le stockage de fichiers de plus en plus volumineux, alors que les limites traditionnelles des produits sont à la traîne par rapport aux besoins modernes gourmands en données.

De nombreuses organisations se heurtent à des freins technologiques pour partager et transférer des données sensibles en raison des limitations de 250 Go imposées par les solutions actuelles de partage sécurisé de fichiers et de transfert sécurisé de fichiers.

Conclusion: résumé des 12 prévisions

L'univers des communications de contenu sensible se transforme rapidement en raison des innovations technologiques et de l'augmentation des mesures réglementaires. Les entreprises sont sous pression pour protéger les données confidentielles face aux cybermenaces croissantes et pour assurer le respect des normes réglementaires internationales en plein essor.

Notre rapport prévisionnel 2024 identifie les grandes tendances 2024 en matière de sécurité et de conformité réglementaire du contenu sensible. Voici quelques points clés à retenir :

- Les technologies avancées de l'IA, y compris les modèles de langage génératif de grande taille, présentent de nouveaux défis pour la confidentialité des données et la conformité qui requièrent une gouvernance rigoureuse, des mesures de sécurité complètes et une utilisation éthique de l'IA.
- Les réglementations à venir, comme le projet de loi sur l'IA de l'UE et la législation fédérale américaine anticipée, imposeront de nouvelles normes pour la gestion des données personnelles que les organisations devront mettre en œuvre efficacement.
- La propagation des mandats de localisation des données nécessite la refonte des applications et des configurations cloud pour répondre aux exigences de souveraineté des données.
- L'augmentation des amendes et des pénalités pour violation de la confidentialité des données nécessite d'améliorer les cadres de gouvernance et de sécurité pour prévenir les infractions.
- L'avancement de la GDN est essentiel pour la protection continue des informations confidentielles.
- L'intégration de technologies de sécurité avancées (prévention des pertes de données basées sur le cloud, protection avancée contre les menaces et Content disarm & reconstruction) dans les infrastructures de contenu sensible aide à combler les lacunes de sécurité.
- Consolider les canaux de communication comme la messagerie électronique, le partage sécurisé de fichiers, le transfert sécurisé de fichiers et les formulaires web dans un réseau de contenu privé simplifie la sécurité et le respect des réglementations.
- Les applications émergentes dans divers secteurs génèrent des fichiers exceptionnellement volumineux, mettant à l'épreuve la capacité des systèmes traditionnels.

Les outils de communication de contenu sensible obsolètes et cloisonnés sont devenus insuffisants, car dépourvus des fonctionnalités avancées nécessaires, des défenses intégrées et d'une gouvernance holistique pour faire face à l'évolution de l'environnement des menaces. En adoptant des architectures zéro trust, des modèles de sécurité détaillés basés sur le contenu, une gestion d'accès solide, la GDN et la DLP, les organisations sont en mesure d'atténuer les risques et de rester conforme malgré la multiplication des réglementations. En préparant 2024, veillez à réinitialiser vos stratégies de communication de contenu sensible et à vous appuyer sur les outils technologiques adaptés pour protéger vos communications de contenu.

BIBLIOGRAPHIE

[1] "Cybersecurity Forecast 2024: Insights for future planning," Google Cloud, November 2023.

[2] "Sensitive Content Communications Privacy and Compliance 2023 Report," Kiteworks, August 2023.

[3] Stephanie Schappert, "Workers regularly post sensitive data into ChatGPT," cybernews, June 16, 2023.

[4] Matthew Guarini, "Predictions 2024: Tech Leaders Boost Ops To Grow With AI," Forrester Blog, October 24, 2023.

[5] "The state of AI in 2023: Generative AI's breakout year," McKinsey, August 1, 2023.

[6] "FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence," The White House, October 30, 2023.

[7] Shiva Aminian, et al., "President Biden Issues Long-Awaited Artificial Intelligence Executive Order," Akin, October 30, 2023.

[8] "Artificial Intelligence 2023 Legislation," National Conference of State Legislatures, September 27, 2023.

[9] "Regulatory framework proposal on artificial intelligence," European Commission, accessed November 8, 2023.

[10] "NIST AI RMF Playbook," NIST, accessed November 8, 2023.

[11] Phil Muncaster, "Forrester: GenAI Will Lead to Breaches and Fines in 2024," Forrester, November 2, 2023.

[12] "Cost of a Data Breach Report 2023," IBM, May 2023.

[13] Becky Bracken, "Clop Keeps Racking Up Ransomware Victims With GoAnywhere Flaw," DARKREADING, March 27, 2023.

[14] Wes Davis, "MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023," The Verge, November 10, 2023.

[15] "Cost of a Data Breach Report 2023," IBM, May 2023.

[16] "Worldwide 2022 Email Phishing Statistics and Examples," Trend Micro, May 31, 2023.

[17] "Data Breach Investigations Report 2023," Verizon, March 2023.

[18] "Worldwide 2022 Email Phishing Statistics and Examples," Trend Micro, May 31, 2023.

[19] "90% of Organizations Prioritizing Email Encryption," Echoworx Blog, May 4, 2021.

[20] "Survey: 83 Percent of U.S. Organizations Have Accidentally Exposed Sensitive Data," Egress Press Release, February 21, 2019.

[21] "How to Protect Your Sensitive Information With Email Encryption," Pulse Technology, September 18, 2023.

[22] "Why Is Email Encryption Not Widely Used," Trustifi, February 8, 2021.

[23] Deepen Desai, et al., "2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year," Zscaler Blog, April 18, 2023.

[24] "Gartner Identifies Top Five Trends in Privacy Through 2024," Gartner, May 31, 2022.

[25] "NIST Drafts Major Update to Its Widely Used Cybersecurity Framework," NIST, August 8, 2023.

[26] Valdez Ladd, "NIST's Privacy Framework for Proposed US Federal Privacy Law," ISACA, February 15, 2023.

[27] "NIST Drafts Major Update to Its Widely Used Cybersecurity Framework," NIST, August 8, 2023.

[28] "How to Achieve Data Compliance in 2024," Exadel, October 16, 2023.

[29] "Data Sovereignty: Definition, Requirements, and How To Ensure It," Spanning, accessed November 8, 2023.

[30] "Understanding the Implications of Data Sovereignty and Why Data Residency may be a Better Choice for Your Business," Trustwave, October 27, 2023.

[31] Alexis Porter, "Lessons Learned From GDPR Fines in 2023," CPO Magazine, August 2, 2023.

[32] "Gartner Identifies Top Five Trends in Privacy Through 2024," Gartner Press Release, May 31, 2022.

[33] Billy Mitchell, "With draft guidance, OMB kickstarts effort to modernize FedRAMP for today's cloud challenges," FEDSCOOP, October 27, 2023.

[34] Katie Walsh, "13 Key Digital Asset Management Best Practices for 2024," Brandfolder, October 26, 2023.

[35] "Digital Rights Management Market Research Report 2024-2030 | 98 Pages Report," Market Reports World, November 3, 2023.

[36] Rick Dagley, "Gartner Predicts Top 10 Strategic Technology Trends for 2024," ITProToday, October 16, 2023.

[37] "Sensitive Content Communications Privacy and Compliance Report 2023," Kiteworks, July 2023.

[38] "Content Disarm and Reconstruction Market by Component (Solutions and Services), Application Area (Email, Web, FTP, and Removable Devices), Deployment Mode, Organization Size, Vertical, and Region—Global Forecast to 2026," MarketsandMarkets, February 2022.

[39] "Data Loss Prevention Market to be Worth $9.33 Billion by 2030," Grand View Research, July 17, 2023.

[40] "Sensitive Content Communications Privacy and Compliance Report 2023," Kiteworks, July 2023.

[41] Bob Ertl, "How the Okta Customer Support Hack Exposed Sensitive Data and Access Credentials," Kiteworks Blog, October 28, 2023.