ÉTUDE 2024 DES IMPACTS SUR LA SÉCURITÉ DES API

Administration

Les attaques ciblant les API repartent à la hausse. Découvrez comment les organismes gouvernementaux font face à ce problème de sécurité majeur, et ce que votre organisation peut faire pour rester en sécurité.

Les organismes gouvernementaux du monde entier sont soumis à la pression croissante de devoir sécuriser les services digitaux à l'ère des API. En 2024, 86,1 % des organisations du secteur public ont signalé un incident de sécurité lié aux API, soit une hausse significative par rapport à l'année précédente, avec 76,8 %. Cette augmentation place le secteur public au-dessus de la moyenne de 84 % de tous les secteurs, ce qui montre l'ampleur grandissante du défi. De la conformité aux exigences du Règlement général sur la protection des données (RGPD) à l'application de la résidence des données dans l'ensemble des systèmes multicloud, en passant par la lutte contre les menaces de sécurité souveraines, les organismes gouvernementaux sont confrontés à un besoin universel d'une plus grande visibilité, d'une gouvernance renforcée et d'une résilience intégrée.

Le coût réel des incidents de sécurité liés aux API pour les organismes gouvernementaux

Les organismes gouvernementaux adoptent de plus en plus les API pour prendre en charge les services digitaux, faciliter le partage de données entre les organismes et moderniser l'infrastructure. Mais cette tendance a ouvert la voie à une multitude de nouvelles vulnérabilités que les cybercriminels s'empressent d'exploiter. Plus particulièrement, des mécanismes d'authentification médiocres, des erreurs de configuration d'API et un manque de connaissance des indicateurs de risque critiques exposent le gouvernement aux failles de sécurité des API. Les répercussions de ces incidents vont bien au-delà du vol de données. En effet, ceux-ci entraînent des risques pour la continuité opérationnelle, la conformité réglementaire et la confiance du public.

Comment savons-nous tout cela ? Akamai a interrogé plus de 1 200 professionnels de l'informatique et de la sécurité, des responsables des technologies de sécurité de l'information au personnel de sécurité des applications, pour en savoir plus sur leur expérience en matière de menaces liées aux API.

Ici, nous avons filtré les résultats de notre enquête auprès des organismes gouvernementaux, qui révèlent les principaux impacts des incidents de sécurité liés aux API dont ils ont été victimes :

- « Augmentation du stress et/ou de la pression pour l'équipe ou le service » (28,5 %)
- « Atteinte à la réputation du service auprès des dirigeants et/ou du conseil d'administration » (27,2 %)
- « Amendes des régulateurs » (25,2 %)

Ces conséquences interdépendantes sont faciles à comprendre, étant donné que vos pairs ont évalué à 717 500 $ le coût de la résolution des incidents liés aux API, soit 21,3 % de plus que la moyenne des huit secteurs étudiés.

Lisez la suite afin de découvrir les informations spécifiques à votre secteur révélées par l'Étude 2024 des impacts sur la sécurité des API.

Face à l'augmentation des attaques, la visibilité est une préoccupation croissante

Lorsqu'on leur demande de citer les principales causes des incidents de sécurité liés aux API dont ils ont été victimes, vos pairs ont identifié deux vulnérabilités majeures :

- L'absence de contrôles d'authentification des API (25,2 %)
- L'utilisation d'outils traditionnels pour la sécurité des API (25,2 %)

Malgré un nombre exponentiel de preuves des conséquences des menaces ciblant les API (tels que les coûts de résolution élevés ou l'érosion de la confiance des utilisateurs), nos conclusions suggèrent que de nombreuses équipes gouvernementales relèguent encore la sécurité des API au second plan. De fait, la sécurité des API se classe au sixième rang des priorités en matière de cybersécurité pour l'année à venir, à 17,9 %.

86,1 % des organisations gouvernementales ont déclaré avoir été victimes d'un incident de sécurité lié aux API en 2024, soit une augmentation significative par rapport à 2023, avec 76,8 %

717 500 $: il s'agit du coût financier moyen d'une violation de la sécurité des API pour les organisations gouvernementales aux États-Unis, un chiffre supérieur à la moyenne de 591 404 $ de tous les secteurs

66,9 % des entités gouvernementales tiennent un inventaire des API qu'elles utilisent, mais seulement 18,5 % d'entre elles ont une visibilité totale sur quelles API gèrent les données sensibles, ce qui expose les informations critiques à des risques

3 principaux impacts

1. **Augmentation du stress et/ou de la pression sur les équipes de sécurité**
2. **Atteinte à la réputation de l'équipe auprès des dirigeants et du conseil d'administration**
3. **Amendes réglementaires pour des raisons de non-conformité**

Source :
l'étude 2024 des impacts sur la sécurité des API d'Akamai

Pour les organismes gouvernementaux, les attaques ciblant les API ont des impacts importants, qu'ils soient financiers ou humains. La perte de confiance au niveau de la direction en raison des violations peut entraîner une surveillance accrue, des interruptions opérationnelles et une augmentation de la charge de travail pour les équipes déjà sous pression et qui peinent à répondre aux exigences de conformité.

Akamai

Tout comme dans le secteur privé, les organismes gouvernementaux peinent à faire la distinction entre les activités d'API authentiques et malveillantes. Cela s'explique en partie par un manque de visibilité sur les points faibles des API. Alors que 66,9 % de vos pairs déclarent disposer d'un inventaire complet de leurs API, seulement 18,5 % d'entre eux savent quelles API renvoient des données sensibles, notamment des informations personnelles identifiables (PII) telles que les numéros d'identification nationaux, les données biométriques et les coordonnées.

Imaginons qu'une API non autorisée soit déployée par un service ou la branche d'un organisme gouvernemental sans la collaboration ou la supervision d'équipes centrales d'informatique ou de sécurité équipées des dernières technologies.

Cette API peut :

- avoir été conçue pour permettre l'accès aux données personnelles ou financières des citoyens sans contrôles d'autorisation appropriés, ce qui pourrait conduire à l'exposition d'informations sensibles ;
- avoir été remplacée par une nouvelle version sans avoir été correctement mise hors service, ouvrant la voie à l'exploitation d'un point de terminaison obsolète ;
- agir en dehors de la visibilité des équipes centrales d'informatique et de sécurité, en échappant à la vigilance des outils de surveillance et des contrôles de conformité traditionnels ;
- avoir été exploitée par des acteurs malveillants pour obtenir un accès non autorisé aux systèmes gouvernementaux, ce qui peut entraîner des violations de données, des vols d'identité ou des fraudes financières.

Ces situations ne sont pas seulement hypothétiques : le paysage de la cybersécurité des organismes gouvernementaux américains rencontre des difficultés majeures. Selon le Business Digital Index de Cybernews, de nombreux organismes et services gouvernementaux peinent à maintenir des postures de sécurité solides, avec près de 4 organismes sur 10 (38,8 %) recevant des notes de « risque critique » lors de leurs évaluations, et 75 % ayant été victimes d'une violation de données.

Ces statistiques reflètent la complexité à laquelle sont confrontées les équipes de sécurité gouvernementales, qui doivent gérer à la fois les objectifs, les systèmes existants et les menaces en constante évolution, tout en faisant face à des contraintes et à des exigences uniques. Alors que ces défis s'intensifient, en particulier dans le domaine de la sécurité des API, les organismes ont besoin de partenaires qui comprennent leurs exigences spécifiques et peuvent leur fournir des solutions adaptées aux environnements gouvernementaux.

En quoi les incidents liés aux API affectent la conformité, les coûts et le niveau de stress des équipes

Compte tenu de la fréquence et des coûts des attaques ciblant les API, il n'est pas surprenant que la sécurisation des API s'impose de plus en plus comme la priorité des organismes gouvernementaux du monde entier. Aux États-Unis, l'initiative Data.gov, gérée par la General Services Administration (Administration des services généraux), définit des normes relatives aux API pour l'ensemble des agences fédérales afin d'améliorer la cohérence, la sécurité et l'interopérabilité. Des efforts similaires sont en train d'être mis en place à l'échelle mondiale, des structures de données ouvertes dans l'Union européenne et au Royaume-Uni aux initiatives de transformation digitale dans les régions Asie-Pacifique et Moyen-Orient, où les organismes gouvernementaux adoptent des API standardisées pour garantir des échanges de données sécurisés et fluides.

Bon nombre de ces initiatives s'alignent sur les réglementations régionales telles que le RGPD de l'UE, le programme australien Notifiable Data Breaches et le My Number Act au Japon. En appliquant des normes et des cadres communs, les gouvernements s'efforcent d'assurer la sécurité des échanges de données tout en réduisant les risques liés aux intégrations tierces et aux accès non autorisés.

	Administration	Moyenne de tous les secteurs
États-Unis	717 500,50 $	591 404,01 $
Royaume-Uni	378 140,69 £	420 103,18 £
Allemagne	296 975,79 €	403 453,26 €

Q3. Si vous avez subi un incident de sécurité lié aux API, quel a été l'impact financier total estimé de ces incidents combinés ? Veuillez inclure tous les coûts connexes tels que les réparations du système, le temps d'arrêt, les frais juridiques, les amendes et toute autre dépense associée.

Il est clair que les organismes gouvernementaux sont parfaitement conscients des conséquences que peuvent avoir les menaces ciblant les API. Pour la première fois, nous avons demandé aux participants des trois pays sur lesquels portait notre enquête de nous indiquer l'impact financier estimé des incidents de sécurité liés aux API dont ils ont été victimes au cours des 12 derniers mois.

Bien que les impacts financiers soient importants, il est apparu clairement dans les réponses des participants que les répercussions des attaques dépassaient largement l'aspect économique.

Ces derniers n'ont pas cité le coût comme l'un des principaux impacts des incidents de sécurité liés aux API. Comme mentionné précédemment, les deux principaux impacts d'après nos participants étaient l'« augmentation du stress et/ou de la pression pour l'équipe ou le service » et l'« atteinte à la réputation du service auprès des dirigeants et/ou du conseil d'administration ».

Ces répercussions laissent un impact durable. Les violations érodent la confiance, ce qui peut compromettre les futurs financements et affaiblir la confiance du public. Dans le même temps, les pertes de productivité dans les organismes déjà sous pression peuvent conduire le personnel au burn-out ou à une baisse de motivation.

Mais ces quelques régions ne sont pas les seules à être touchées. Bien que ce rapport se concentre sur certains marchés, la sécurité des API est devenue un problème critique pour les organisations du secteur public dans le monde entier. En effet, les organismes gouvernementaux en Asie-Pacifique, en Amérique latine et au-delà sont confrontés à des défis similaires en matière de sécurisation de l'infrastructure digitale, de conformité réglementaire et de protection des données sensibles contre les menaces en constante évolution.

Réduire le risque et le stress en mettant en œuvre des mesures de sécurité proactives des API

Les attaques ciblant les API des organismes gouvernementaux prennent de l'ampleur en termes de portée, d'échelle, de complexité et de coût. Cela inclut les attaques de bot alimentées par l'IA générative, qui s'adaptent rapidement pour contourner les outils de sécurité des API traditionnels et d'autres défenses périmétriques. Bon nombre de professionnels de la sécurité de votre secteur sont directement confrontés à ces menaces et en ressentent les conséquences, tant financières qu'humaines. Mais même lorsqu'elles sont conscientes de l'importance des menaces liées aux API, les entreprises se posent la question : que pouvons-nous faire ?

En prenant dès maintenant des mesures pour mieux sécuriser vos API (et les données qu'elles échangent), votre organisation pourra mieux protéger ses revenus et données sensibles et alléger la charge de travail des équipes de sécurité, tout en préservant la confiance durement acquise du conseil d'administration et des responsables gouvernementaux. Votre plan d'action doit notamment prévoir le renforcement des connaissances de vos équipes sur les menaces avancées liées aux API et le développement des capacités dont vous avez besoin pour les repousser.

Pour lire le rapport complet et en savoir plus sur les meilleures pratiques en matière de visibilité et de protection des API, téléchargez l'**Étude 2024 des impacts sur la sécurité des API**.

Prêt à discuter de vos défis et de la manière dont Akamai peut vous aider ?

Demandez une démonstration personnalisée d'Akamai API Security

Akamai

Les solutions de sécurité d'Akamai protègent les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 05/25.