ÉTUDE 2024 DE L'IMPACT SUR LA SÉCURITÉ DES API D'AKAMAI

Secteur de la vente au détail et de l'e-commerce

Comment les autres professionnels du secteur perçoivent et abordent la menace croissante qui pèse sur les API

Les API qui alimentent les initiatives digitales des entreprises de vente au détail et d'e-commerce sont victimes d'attaques. Les acteurs malveillants utilisent des méthodes de plus en plus innovantes pour accéder aux données contenues dans les API non protégées et voler des données de carte de crédit, siphonner l'argent des programmes de fidélité, lancer des attaques par credential stuffing et bien plus encore. Les équipes de sécurité en ressentent les conséquences et cherchent des moyens d'améliorer leur sécurité. Mais l'idée d'ajouter un nouveau vecteur d'attaque à leur charge de travail peut sembler décourageante, en particulier s'agissant des API, dont les erreurs de configuration ou les failles logiques peuvent être facilement détectées et exploitées.

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

Ce dossier filtre les résultats de cette enquête pour votre secteur d'activité, où 68 % des personnes interrogées ont déclaré avoir subi des incidents de sécurité des API au cours des 12 derniers mois. Quelles ont été les conséquences ? Les aspects les plus souvent mentionnés par vos pairs étaient l'augmentation des niveaux de stress au sein des équipes et la perte de crédibilité auprès des dirigeants et du conseil d'administration. Une réponse tout à fait compréhensible compte tenu des coûts signalés : les professionnels de la vente au détail et de l'e-commerce ont déclaré avoir déboursé 526 531 dollars pour résoudre les incidents liés aux API qu'ils ont subis.

Lisez la suite afin de découvrir les informations importantes pour votre secteur révélées par l'Étude 2024 de l'impact sur la sécurité des API.

Les attaques augmentent, mais la visibilité diminue

Bien qu'une nette majorité des professionnels de la vente au détail et du-commerce interrogés aient subi des incidents de sécurité des API, leur pourcentage (68 %) était inférieur à la moyenne obtenue dans les huit secteurs d'activité étudiés (84 %). Par ailleurs, les principales priorités de sécurité des professionnels de votre secteur pour les 12 prochains mois sont « la défense contre les attaques alimentées par l'IA générative » et « la sécurisation des API contre les acteurs malveillants ».

Existe-t-il un lien entre le fait de donner la priorité à la sécurité des API et la prévention des attaques ? Il est possible que les équipes de sécurité des entreprises de vente au détail et d'e-commerce aient pris conscience de l'importance de la protection des API et que leurs efforts aient permis de réduire le nombre d'incidents. Mais nos résultats suggèrent également que ces équipes ne détectent pas tous les cas d'exploitation des API.

Il reste difficile pour les entreprises de vente au détail et d'e-commerce de distinguer les activités API authentiques des activités malveillantes ou frauduleuses, mais aussi d'évaluer les risques. Bien que 67 % de vos concurrents déclarent disposer d'inventaires complets de leurs API, *seuls 29 %* d'entre eux savent lesquelles de leurs nombreuses API renvoient des données sensibles, par exemple des informations personnelles identifiables (PII) ou des données de carte de crédit.

Imaginons ce qui peut arriver à une API déployée par une unité commerciale sans la collaboration ou la supervision des services centraux d'informatique ou de sécurité de l'entreprise. Cette API peut :

- avoir été conçue pour renvoyer les données des clients sans que des contrôles d'autorisation appropriés aient été mis en œuvre et que des tests adéquats aient été réalisés pour détecter les erreurs de configuration ;
- avoir été remplacée par une nouvelle version sans être désactivée, restant ainsi exposée à Internet ;
- avoir échappé au radar des outils traditionnels qui ne détectent pas les API non gérées ;
- avoir été exploitée par des fraudeurs pour accéder au compte de fidélité de vrais clients et obtenir de l'argent en échange de leurs points.

68 % des entreprises de vente au détail/e-commerce ont subi un incident de sécurité des API au cours des 12 derniers mois[1]

Seules 29 % des entreprises de vente au détail/e-commerce disposant d'inventaires complets de leurs API savent quelles API renvoient des données sensibles[1]

526 531 $ = impact financier des incidents de sécurité des API pour les entreprises de vente au détail/e-commerce qui en ont été victimes au cours des 12 derniers mois[1]

3 principaux impacts[1]

1. **Augmentation du stress** et/ou de la pression pour l'équipe
2. **Coûts engagés** pour résoudre le problème
3. **Atteinte à la réputation du service** auprès des dirigeants et/ou du conseil d'administration

44 % des attaques Web contre les entreprises commerciales visaient les API[2]

Sources :
1. Akamai, « Étude de l'impact sur la sécurité des API », 2024
2. Rapport SOTI (État des lieux d'Internet) d'Akamai, « De l'ombre à la lumière : les tendances des attaques mettent en lumière les menaces ciblant les API », 2024

Akamai

Il ne s'agit pas d'un scénario purement hypothétique. Selon l'étude True Cost of Fraud™ réalisée en 2023 par LexisNexis® Risk Solutions, 50 % des pertes liées à la fraude peuvent être attribuées à l'ouverture abusive de nouveaux comptes, qui consiste à exploiter les API pour ouvrir des comptes en masse. De plus, notre scénario reflète les causes des incidents liés aux API les plus citées par les professionnels de l'informatique et de la sécurité.

Principales causes des incidents liés aux API citées par les équipes de sécurité du secteur de la vente au détail/de l'e-commerce

1. Les API dans les outils d'IA générative, par exemple les LLM – 24,7 %
2. L'API a été exposée involontairement à Internet – 24 %
3. Erreur de configuration de l'API – 22,0%
4. Le pare-feu d'application Web ne l'a pas détecté – 21,3%
5. La passerelle d'API ne l'a pas détecté – 20,7%
6. Vulnérabilité due à des erreurs de codage de l'API – 20,0%
7. Outil/service technologique bien connu – 20 %
8. Le pare-feu réseau ne l'a pas détecté – 18,7%
9. Vulnérabilités en matière d'autorisation – 17,3%
10. Solution logicielle téléchargée depuis Internet – 16,7%
11. Absence de contrôles d'authentification de l'API – 16,0%
12. Solution logicielle de niveau intermédiaire – 14,7 %
13. API non gérées (par exemple : zombies) – 13,3 %

Q. Selon vous, quelles sont les causes des incidents de sécurité des API que votre entreprise a connus ? (Sélectionnez jusqu'à 3 réponses) n=1207

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

Selon le Gartner® Market Guide for API Protection de mai 2024, « les données actuelles indiquent que la violation moyenne des API entraîne au moins 10 fois plus de fuites de données que la violation moyenne de la sécurité ».[3] Il n'est pas étonnant que la norme PCI DSS v4.0, l'une des normes de sécurité les plus suivies, ait intégré de nouvelles exigences en matière de protection des API. Les entreprises — et les organismes de réglementation auxquels elles rendent des comptes — doivent savoir quels types de données transitent via leurs API et celles de leurs partenaires et fournisseurs, ce qui vient augmenter la complexité de la gestion des risques liés aux tiers dans le secteur de l'e-commerce.

La perte de confiance des régulateurs peut entraîner une surveillance accrue et une surcharge de travail pour les équipes qui peinent déjà à répondre aux exigences de conformité. Elle risque également d'entraîner des amendes coûteuses. Il est clair que les entreprises de vente au détail et d'e-commerce, soucieuses des coûts, sont parfaitement conscientes des conséquences financières des menaces liées aux 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 des API qu'ils ont subis au cours des 12 derniers mois.

[3] GARTNER est une marque commerciale et une marque de service déposée de Gartner, Inc. et/ou de ses filiales aux États-Unis et dans le monde entier, et est utilisée dans le présent document avec son autorisation. Tous droits réservés.

	Vente/e-commerce	Moyenne de l'ensemble du secteur
États-Unis	526 531 $	591 404 $
Royaume-Uni	258 815 £	420 103 £
Allemagne	348 467 €	403 453 €

Q. 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. n = 1 207

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'impact principal des incidents de sécurité liés aux API. Les professionnels de la vente au détail et de l'e-commerce interrogés ont mis l'accent sur les conséquences humaines, à savoir le stress et la pression qui pèsent sur leurs équipes.

5 principaux impacts des incidents de sécurité des API pour les entreprises de vente au détail et d'e-commerce

1. Cela a conduit à une augmentation du stress et/ou de la pression pour notre équipe/service – **28,7 %**

2. Coûts engagés pour résoudre le problème – **28,0 %**

3. Cela a nui à la réputation de notre service auprès des dirigeants et/ou du conseil d'administration – **25,3 %**

4. Cela a conduit à un contrôle interne minutieux accru de notre équipe/service par l'entreprise – **23,3 %**

5. Amendes des régulateurs – **25,3 %**

Q. Quels coûts et/ou impacts, le cas échéant, les incidents de sécurité des API ont-ils eus sur votre entreprise ? (Sélectionnez jusqu'à 3 réponses) n=1207

Étapes suivantes : réduire le risque et le stress en mettant en œuvre des mesures de sécurité proactives des API

Les attaques d'API contre les entreprises de vente au détail et d'e-commerce gagnent en ampleur et en sophistication, comme en témoignent par exemple les attaques de bot alimentées par l'IA générative, qui s'adaptent rapidement pour contourner les outils de sécurité des API traditionnels et les 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 entreprise pourra mieux protéger ses revenus et alléger la charge de travail des équipes de sécurité, tout en préservant la confiance durement acquise du conseil d'administration et des clients. 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 de l'impact 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

La solution de sécurité d'Akamai protège 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 11/24.