ÉTUDE 2024 DES IMPACTS SUR LA SÉCURITÉ DES API

Secteur des services financiers

Les attaques ciblant les API repartent à la hausse. Découvrez comment le secteur des services financiers fait face à ce problème de sécurité majeur, et ce que votre entreprise peut faire pour rester en sécurité.

L'année dernière, 88,7 % des entreprises de services financiers ont subi une attaque sur les API qui gèrent leurs données et connectent les clients et partenaires à des services stratégiques. 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 personnelles et financières, notamment les soldes des comptes et l'historique des transactions.

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 responsable 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 nos résultats pour les personnes interrogées du secteur des services financiers, qui ont déclaré que les principaux impacts de leurs incidents de sécurité liés aux API étaient les « amendes des régulateurs » et « l'augmentation du stress et/ou de la pression pour mon équipe/service ». Ces conséquences interdépendantes sont faciles à comprendre, étant donné que vos pairs ont évalué à 832 800 dollars le coût de la résolution des incidents liés aux API, soit 40 % de plus que la moyenne des huit secteurs étudiés et plus que tout autre secteur d'activité.

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

La visibilité diminue alors que les attaques augmentent

Alors que 84 % des entreprises de tous les secteurs ont connu des incidents de sécurité liés aux API, les entreprises de services financiers ont été ciblées plus fréquemment que la moyenne, à 88,7 %. Vos pairs ont identifié deux vulnérabilités clés à l'origine de ces attaques : les pare-feux réseau qui ne parviennent pas à détecter les menaces (26,5 %) et les vulnérabilités au sein des API dans les outils d'IA générative tels que les grands modèles de langage (LLM) (23,2 %).

Malgré les preuves de plus en plus nombreuses des menaces liées aux API, des incidents fréquents aux coûts de résolution élevés et aux amendes réglementaires, nos résultats suggèrent que de nombreuses équipes de services financiers n'ont pas encore fait de la sécurité des API une priorité absolue. En fait, la sécurité des API se classe au neuvième rang des priorités en matière de cybersécurité pour l'année à venir, à 18,5 %.

Distinguer une activité API authentique d'une activité malveillante ou frauduleuse reste un défi pour le secteur financier, en particulier lorsqu'il s'agit d'avoir une visibilité sur les nombreux risques liés aux API. Alors que 73,5 % de vos pairs déclarent disposer d'un inventaire complet de leurs API, seulement 28,5 % d'entre eux savent quelles API renvoient des données sensibles, notamment des informations personnelles identifiables (PII) et des données allant de l'historique de crédit des titulaires de cartes aux dossiers financiers des grands clients des banques commerciales.

88,7 % des entreprises de services financiers ont subi un incident de sécurité des API au cours des 12 derniers mois

Seules 28,5 % des entreprises de services financiers disposant d'inventaires complets de leurs API savent quelles API renvoient des données sensibles

832 800 $ = impact financier des incidents de sécurité des API pour les entreprises de services financiers qui en ont été victimes au cours des 12 derniers mois

3 principaux impacts

1. **Augmentation du stress et/ou de la pression** sur l'équipe de sécurité
2. **Amendes** des régulateurs
3. **Perte de confiance** et atteinte à la réputation

Source :
Akamai, « Étude de l'impact sur la sécurité des API », 2024

Akamai

Imaginons ce qui peut arriver à une API fantôme déployée par un département ou une filiale d'un fournisseur de services financiers sans la collaboration ou la supervision des équipes centrales d'informatique ou de sécurité de l'entreprise. Cette API peut :

- avoir été conçue pour renvoyer les données de transaction 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 cybercriminels qui accèdent aux comptes de clients réels pour voler leurs actifs.

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.

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 la divulgation d'au moins 10 fois plus de données que la moyenne ». Il n'est donc pas étonnant que la norme PCI DSS v4.0, largement suivie, ait ajouté des exigences en matière de sécurité des API. La norme exige désormais que les entreprises valident les codes de leur API avant la publication, testent régulièrement les vulnérabilités et confirment l'utilisation sécurisée des composants basés sur l'API, ce qui est particulièrement important dans un secteur où les API facilitent des millions de transactions financières chaque jour.

La perte de confiance des organismes de réglementation peut entraîner une surveillance accrue et une surcharge de travail pour les équipes qui peinent déjà à répondre aux exigences de conformité. Elle peut également entraîner des amendes coûteuses.

Il est donc clair que les entreprises des secteurs financiers sont parfaitement conscientes des conséquences 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.

	Secteur des services financiers	Moyenne de tous les secteurs
États-Unis	832 800 $	591 404 $
Royaume-Uni	297 189 £	420 103 £
Allemagne	604 405 €	403 453 €

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.

* Gartner, Market Guide for API Protection, 29 mai 2024. 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.

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

Les attaques ciblant les API des entreprises des secteurs financiers 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 entreprise pourra mieux protéger ses revenus et alléger la charge de travail des équipes de sécurité. Ces mesures, ainsi que le renforcement des connaissances de votre équipe sur les menaces avancées liées aux API et les capacités dont vous avez besoin pour vous défendre contre elles, peuvent contribuer à préserver la confiance durement acquise des clients et du conseil d'administration.

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 propose des solutions conçues pour aider les entreprises à réduire les risques liés aux menaces évoquées dans cet article :

- API Security d'Akamai, qui détecte vos API, évalue leur niveau de risque, analyse leur comportement et empêche les menaces de pénétrer dans votre réseau.
- Akamai Account Protector, qui aide à prévenir les abus d'ouverture de compte en surveillant le comportement des utilisateurs en temps réel et en s'adaptant à l'évolution des profils de risque

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 : 03/25.