ÉTUDE 2024 DES IMPACTS SUR LA SÉCURITÉ DES API

Secteur de l'assurance

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

Lorsqu'une catastrophe se produit, qu'il s'agisse d'un accident de voiture ou de la dégradation d'équipements professionnels, les assurés comptent sur les services digitaux pour déclarer des sinistres et recevoir l'assistance de leur assureur. Derrière ces services, les API des compagnies d'assurance traitent des informations sensibles qui révèlent des éléments de la vie d'un assuré sous forme de données.

Dans un secteur où la confiance des clients est primordiale, les compagnies d'assurance sont confrontées à un problème de plus en plus important dans le domaine de la sécurité : les vulnérabilités des API.

Selon l'enquête complète d'Akamai, 76,7 % des professionnels du secteur de l'assurance ont signalé des incidents de sécurité liés aux API au cours des 12 derniers mois. L'impact financier est considérable : rien qu'aux États-Unis, le coût de résolution de ces incidents s'élève à 625 634 $ pour les compagnies d'assurance.

Mais ce qui soulève le plus d'inquiétude est l'impact sur l'activité : la « perte de la bonne volonté de la clientèle et comptes perdus » (28 % des réponses) est la principale préoccupation des compagnies d'assurance suite à des incidents liés aux API. Dans un marché concurrentiel où les clients peuvent facilement changer d'assureur, cette atteinte à la réputation peut avoir des effets durables au-delà des coûts immédiats.

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

Face à l'augmentation des attaques, la visibilité reste un défi majeur

Les attaques ciblant les API représentent un coût financier conséquent pour les compagnies d'assurance. La moyenne aux États-Unis (625 634 $) dépasse la moyenne de tous les secteurs (591 404 $). Qu'est-ce qui provoque ces incidents ?

D'après les équipes de sécurité du secteur de l'assurance, les principales causes sont les suivantes :

1. API non gérées, telles que les API dormantes ou zombies (22 %)
2. API exposées involontairement à Internet (21,3 %)
3. Les outils traditionnels pour sécuriser les API peinent à détecter les menaces (20 %)
4. Vulnérabilités en matière d'autorisation (19,3 %)
5. Erreurs de configuration des API (18,7 %)

De nombreuses entreprises sont conscientes des origines des attaques ciblant leurs API, mais elles manquent de visibilité sur un indicateur de risque crucial : la capacité d'une API à renvoyer des données sensibles lorsqu'elle est appelée. Alors que 56,7 % des compagnies d'assurance déclarent disposer d'un inventaire complet de leurs API (en dessous de la moyenne de 69,7 % de tous les secteurs), seules 20,7 % d'entre elles savent quelles API renvoient des données sensibles.

Ces lacunes en matière de visibilité entraînent des implications importantes en matière de conformité et de sécurité, dans un secteur qui traite des données personnelles et financières hautement réglementées.

76,7 % des compagnies d'assurance ont été victimes d'un incident de sécurité lié aux API au cours des 12 derniers mois

Seules 20,7 % des compagnies d'assurance disposant d'inventaires d'API complets savent lesquelles de leurs API renvoient des données sensibles

625 634 $: l'impact financier des incidents de sécurité liés aux API pour les compagnies d'assurance qui en ont été victimes au cours des 12 derniers mois aux États-Unis

3 principaux impacts

1. **Perte de la bonne volonté de la clientèle et comptes perdus (28 %)**
2. **Atteinte à la réputation du service auprès de la direction (25,3 %)**
3. **Coûts engagés pour résoudre le problème (24,7 %)**

Source :
Akamai, Étude des impacts sur la sécurité des API, 2024

Akamai

Nous avons relevé plusieurs tendances qui entravent la protection des API :

- **La prolifération constante des API** : à chaque initiative digitale, les API se multiplient et évoluent en permanence, ce qui complexifie la gestion des inventaires.
- **Des normes incohérentes** : de nombreux assureurs disposent de plusieurs équipes de développement qui travaillent de manière isolée dans différentes unités commerciales, sans guide général pour concevoir en toute sécurité.
- **Des risques invisibles** : les API transmettent des données sensibles sur les assurés, mais la plupart des entreprises sont incapables d'identifier desquelles il s'agit.

Imaginons ce qui peut arriver à une API déployée par un service sans la supervision d'une équipe de sécurité. Cette API a peut-être été conçue pour partager des dossiers sans contrôles appropriés ou laissée active après que le système a été mis à niveau, créant ainsi des points d'exposition potentiels pour les données sensibles des clients.

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

Il n'est pas surprenant que les compagnies d'assurance soient parfaitement conscientes des conséquences financières que peuvent avoir les menaces ciblant les API. Dans notre enquête, nous avons demandé aux participants de nous indiquer les coûts estimés des incidents de sécurité liés aux API qu'ils ont subis au cours des 12 derniers mois.

	Secteur de l'assurance	Moyenne de tous les secteurs
États-Unis	625 633,70 $	591 404,01 $
Royaume-Uni	493 000,50 £	420 103,18 £
Allemagne	373 918,72 €	403 453,26 €

Bien que les impacts financiers soient significatifs, il est apparu clairement dans les réponses des participants que les coûts reflètent à la fois des préoccupations financières et réputationnelles. Nous leur avons demandé quel était pour eux l'impact principal des incidents de sécurité liés aux API :

- 28 % ont indiqué « perte de la bonne volonté de la clientèle et comptes perdus »
- 25,3 % ont indiqué « atteinte à la réputation de l'équipe auprès des dirigeants et du conseil d'administration »
- 24,7 % ont indiqué « coûts engagés pour résoudre le problème »

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

Les attaques ciblant les API des compagnies d'assurance 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, 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 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 ce document :

- **Akamai API Security** : détecte les API, évalue leur niveau de risque, analyse leur comportement et empêche les menaces de pénétrer dans votre réseau
- **Akamai Account Protector** : 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

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.