ÉTUDE 2024 DES IMPACTS SUR LA SÉCURITÉ DES API

Secteur de la santé

Les attaques ciblant les API repartent à la hausse. Découvrez comment le secteur de la santé fait face aux défis de sécurité des API et ce que vous pouvez faire pour vous défendre contre les menaces en constante évolution.

Dans un secteur où la confiance des patients et des membres est primordiale, les établissements de santé sont confrontés à un problème de plus en plus important dans le domaine de la sécurité : les vulnérabilités des API.

Les dossiers médicaux électroniques, la télémédecine et les appareils médicaux connectés sont devenus des cibles privilégiées pour les cybercriminels. Les informations médicales protégées accessibles via des API non sécurisées peuvent conduire à des violations de la loi HIPAA, compromettre la confidentialité des patients et nuire à leur confiance, qui prend des années à reconstruire.

L'ampleur de ce défi est importante. Dans l'enquête complète d'Akamai, 84,7 % des professionnels de la santé ont enregistré des incidents de sécurité liés aux API au cours de l'année passée, légèrement supérieurs à la moyenne globale de 84 % dans tous les secteurs.

Mais l'impact sur la confiance est peut-être le point le plus inquiétant : les personnes interrogées dans le secteur de la santé déclarent que la « perte de confiance et l'atteinte à la réputation » (28,7 %) est l'une de leurs principales préoccupations lorsqu'un incident lié aux API survient. Dans un monde où les patients peuvent facilement changer de fournisseur, 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 est une préoccupation croissante

Les attaques ciblant les API entraînent un coût financier considérable : les établissements de santé dépensent en moyenne 510 600 $ dans la résolution de ces incidents.

Malgré ces risques, les données révèlent une lacune préoccupante en matière de priorités. À la question concernant leurs principales priorités en matière de cybersécurité au cours des 12 prochains mois, les établissements de santé ont classé « la sécurisation des API contre les acteurs malveillants » à la 11e place (16,7 %) sur 12 options proposées. L'enquête dévoile qu'ils se concentrent plutôt sur la sécurisation de l'authentification pour le personnel accédant aux systèmes (24,7 %) et la gestion des secrets des développeurs (22,7 %).

Les prestataires de santé ont toujours des difficultés à faire la distinction entre les activités API légitimes et malveillantes. Alors que 65 % de vos pairs déclarent disposer d'inventaires d'API complets, seulement 24 % de ce sous-ensemble sait quelles API gèrent les données sensibles, soit une baisse inquiétante par rapport aux 40 % enregistrés en 2023. Pour le secteur de la santé, où la confidentialité des données n'est pas seulement une bonne pratique mais une obligation légale, ce manque de visibilité entraîne des risques importants.

Imaginons ce qui peut arriver à une API déployée par un service clinique sans la supervision des services centraux d'informatique ou de sécurité. Cette API peut avoir été :

- conçue pour partager les dossiers des patients sans vérification de la conformité à la norme HIPAA ;
- laissée active après des mises à jour du système, créant des points d'accès inconnus ;
- ignorée par les outils de sécurité traditionnels, qui ne sont pas conçus pour détecter les API non gérées ;
- exploitée par des attaquants pour accéder à des informations de santé protégées ;
- utilisée de manière abusive par un partenaire authentique, pour des cas d'utilisation non souhaités.

84,7 % des établissements de santé ont connu un incident de sécurité lié aux API au cours des 12 derniers mois

65 % des établissements de santé disposent d'inventaires d'API complets, mais seuls 24 % savent quelles API renvoient des données sensibles

510 600 $: l'impact financier des incidents de sécurité liés aux API pour les établissements de santé qui en ont été victimes au cours des 12 derniers mois

3 principaux impacts

1. **Perte de confiance et atteinte à la réputation** (28,7 %)
2. **Perte de productivité** (28,7 %)
3. **Surveillance interne accrue** (27,3 %)

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

Akamai

Il ne s'agit pas que d'une hypothèse. Les violations de données de santé atteignent des chiffres records et les coûts moyens des violations de données s'élèvent à 4,88 millions de dollars[1]. Les vulnérabilités des API représentent donc une menace grandissante en matière de conformité et de sécurité. De plus, ce scénario reflète les causes des incidents liés aux API les plus citées par vos pairs.

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[2], « 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 pas étonnant que les exigences de conformité HIPAA se concentrent de plus en plus sur la sécurité des API. Bien que la loi HIPAA ne mentionne pas explicitement les API, elle demande à ce que l'accès aux informations protégées de santé soit restreint en fonction des rôles des employés. Pour ce faire, il faut mettre en place une méthode d'authentification et des contrôles d'accès dans les API responsables du transfert des données des patients. Les professionnels et investisseurs du secteur de la santé, ainsi que les organismes de réglementation auxquels ils rendent des comptes, doivent savoir quels types de données transitent via leurs API et celles de leurs partenaires et fournisseurs, ce qui complexifie la gestion des risques liés aux tiers dans le secteur.

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 du secteur de la santé 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 les coûts estimés des incidents de sécurité liés aux API qu'ils ont subis au cours des 12 derniers mois.

	Secteur de la santé	Moyenne de tous les secteurs
États-Unis	510 600 $	591 404 $
Royaume-Uni	363 885 £	420 103 £
Allemagne	643 884 €	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.

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. Comme mentionné précédemment, les personnes interrogées ont mis en évidence « la perte de confiance et l'atteinte à la réputation » (28,7 %) et « la perte de productivité » (28,7 %). Ces conséquences ont des effets durables : une perte de confiance des patients peut nuire au chiffre d'affaires des années à venir, tandis que les pertes de productivité des équipes médicales déjà tendues peuvent accélérer le burnout et le désengagement du personnel.

[1] Rapport IBM sur le coût d'une violation de données, 2024

[2] 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 établissements de santé 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

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.