Akamai

LIVRE BLANC

Principes fondamentaux de la sécurité des API : étoffez vos connaissances, sécurisez l'entreprise

Introduction

Les API ont rapidement évolué, passant du statut de détail d'implémentation à celui de catalyseur stratégique de l'innovation digitale. Chaque fois qu'un client, un partenaire ou un fournisseur entre en contact avec une entreprise par voie digitale, il y a une API en coulisse qui facilite un échange fluide des données.

À mesure que les API prolifèrent, les risques qu'elles présentent se multiplient également. Dans la course à la création et au lancement rapides de nouvelles applications et de services améliorés par l'IA, les API sous-jacentes sont trop souvent mal configurées, manquent de contrôles de sécurité et sont vulnérables aux attaques faciles à exécuter.

Par conséquent, les API sont devenues l'un des principaux vecteurs d'attaque, obligeant de nombreuses équipes de sécurité à rattraper leur retard en matière de stratégies de sécurité des API. La sécurité des API est ainsi en passe de rapidement devenir l'une des principales priorités stratégiques des responsables de l'informatique et de la sécurité.

Que vous cherchiez à vous familiariser avec les notions de base sur la sécurité des API ou que vous rassembliez une liste des bonnes questions à poser, ce guide présente les détails à connaître, notamment les suivants :

- **Les différents types d'API**
- **Ce que la sécurité des API signifie pour les entreprises aujourd'hui**
- **Les meilleures pratiques pour gérer les risques liés à la sécurité des API**
- **Les méthodes d'attaque et d'exploitation les plus courantes en matière d'API**

Pour accéder directement aux meilleures pratiques en matière de sécurité des API, vous pouvez passer directement à la page 10.

Table des matières

Notions de base sur les API

Qu'est-ce qu'une API Web ?

Une interface de programmation d'applications Web, ou API, est constituée d'un ou de plusieurs points de terminaison d'un système de messages demande-réponse défini, généralement exprimé en JSON ou XML, exposés publiquement via le Web (le plus souvent au moyen d'un serveur Web basé sur le protocole HTTP).

En d'autres termes, une API Web est ce à quoi la plupart des gens pensent lorsqu'ils entendent « API ». Il s'agit d'un ensemble de points de terminaison. Les points de terminaison se composent des chemins d'accès aux ressources, des opérations pouvant être effectuées sur ces ressources et de la définition des données de ressources (en JSON, XML, Protobuf ou dans un autre format).

Les API Web sont différentes des autres API, telles que celles exposées par le système d'exploitation ou par les bibliothèques d'applications exécutées sur la même machine. Toutefois, le terme général « API » fait habituellement référence à une API (Web) basée sur HTTP, en particulier dans le contexte de la transformation digitale de l'entreprise et de la sécurité des API.

Quels sont les types d'API les plus courants ?

Le tableau suivant répertorie des termes qui font référence à différents modèles d'utilisation et différentes approches techniques pour les implémentations d'API. Les API Web sont définies comme étant basées sur HTTP, et les quatre principaux types d'API Web observés aujourd'hui sont RESTful, SOAP, GraphQL et gRPC. Le tableau définit les types les plus courants et d'autres.

Modèle d'utilisation de l'API	Description
API publique	API mise à disposition et partagée librement avec tous les développeurs via Internet
API externe	Souvent utilisée de manière interchangeable avec une API publique - ce type d'API est exposé sur Internet
API privée	API implémentée dans un centre de données ou un environnement cloud protégé pour être utilisée par des développeurs de confiance
API interne	Souvent utilisée de manière interchangeable avec une API privée
API tierce	Fournit un accès programmatique à des fonctionnalités spécialisées et/ou à des données provenant d'une source tierce, en vue d'une utilisation dans une application
API de partenaires	Type d'API tierce qui est mis à la disposition de partenaires commerciaux autorisés de manière sélective
API authentifiée	API accessible uniquement aux développeurs auxquels l'accès a été accordé (ou aux acteurs malveillants qui ont obtenu un accès non autorisé à des informations d'identification)
API non authentifiée	API à laquelle on peut accéder de manière programmatique sans avoir besoin d'informations d'identification
API HTTP	API qui utilise le protocole de transfert hypertexte comme protocole de communication pour les appels API

API RESTful	RESTful (transfert d'état représentationnel) est le type d'API Web le plus courant qui utilise du texte brut, ainsi que les formats HTML, XML, YAML ou JSON pour diffuser des données. Les API RESTful sont faciles à utiliser par les structures frontales actuelles (par exemple, React et React Native) et simplifient le développement d'applications Web et pour mobile. Elles sont devenues la norme de facto pour toute API Web, y compris celles utilisées pour le B2B.
GraphQL	Les API GraphQL sont la nouvelle norme développée par Facebook qui fournit un accès à la base de données sur un seul point de terminaison POST (généralement /graphql). Elles résolvent un problème courant des API RESTful, à savoir la nécessité d'effectuer plusieurs appels pour remplir une seule page d'interface utilisateur.
SOAP	SOAP utilise le langage XML (eXtensible Markup Language) pour les appels de procédure à distance (RPC). On le trouve encore dans les anciennes API.
XML-RPC	XML-RPC est une méthode permettant d'effectuer des appels de procédure sur Internet, qui utilise une combinaison de XML pour le codage et de HTTP comme protocole de communication
gRPC	Les API gRPC sont un protocole binaire haute performance développé par Google sur HTTP/2.0 et sont principalement utilisées pour la communication est-ouest (au sein d'un réseau interne)
OpenAPI	OpenAPI est une spécification de description et de documentation pour les API. Il peut être utile de savoir que les termes Swagger et OpenAPI font référence, respectivement, à la spécification d'origine et à la norme ouverte développée par OpenAPI Initiative.

Quelle est la différence entre les API et les points de terminaison ?

Le terme « API » est souvent utilisé pour désigner un point de terminaison d'API unique. Les API, parfois appelées services ou produits API, sont des ensembles de points de terminaison qui servent une fonction métier. Un point de terminaison, quant à lui, correspond à une ressource (ou un chemin d'accès, également appelé URI ou Uniform Resource Identifier) et à l'opération effectuée sur cette ressource (création, lecture, mise à jour ou suppression). Dans les API RESTful, ces opérations sont généralement mises en correspondance avec les méthodes HTTP (POST, GET, PUT et DELETE).

Qu'est-ce qu'une API nord-sud ?

Il s'agit d'une API qu'une entreprise laisse accessible au monde extérieur, principalement pour mener des activités avec ses partenaires commerciaux. C'est ce qu'on appelle l'exposition d'API. Par exemple :

> **Les banques qui adoptent la banque ouverte peuvent exposer leurs données à d'autres entreprises de technologie financière ou entreprises de services financiers via des API.**

> **Les organismes de santé peuvent exposer les dossiers des patients aux compagnies d'assurance et à d'autres organismes médicaux via des API.**

> **Les entreprises hôtelières peuvent exposer leurs systèmes de réservation aux agents de voyages ou aux agrégateurs via des API.**

Les API constituent le tissu conjonctif qui permet à des entreprises disparates d'échanger des données. Les API nord-sud sont souvent considérées comme sûres, car l'accès est autorisé et authentifié. En règle générale, ces API connaissent la croissance la plus rapide en nombre et en volume, et constituent donc la plus grande surface d'attaque pour la plupart des entreprises.

Qu'est-ce qu'une API est-ouest ?

Il s'agit d'une API qu'une entreprise utilise en interne et qui ne doit pas être accessible à des personnes extérieures à l'entreprise. Ces API relient des applications internes, des unités commerciales ou des départements. Il est possible qu'un développeur fasse une erreur qui rende les API est-ouest accessibles par accident. Ces API ne sont pas censées être accessibles ou même connues par des entités externes, mais des violations se produisent lorsque des acteurs malveillants trouvent des API est-ouest accessibles par le biais d'Internet.

Quelles sont les différences entre les API B2C et les API B2B ?

Les API B2C (Business-to-Consumer) alimentent les applications Web et pour mobile. Elles sont généralement utilisées par des clients frontaux actuels pour permettre aux utilisateurs finaux authentifiés d'accéder à la fonctionnalité métier de l'entreprise.

Les API B2B (Business to Business) sont proposées par une entreprise à d'autres entreprises pour mener leurs activités, et parfois pour fournir de la valeur à des clients communs.

Les API B2B permettent de rationaliser la façon dont une entreprise travaille avec ses fournisseurs, revendeurs et autres partenaires et offre de meilleures expériences à ses clients.

Voici quelques exemples d'API B2B :

API d'open banking

API de gestion de la chaîne d'approvisionnement

Facturation et paiements électroniques entre partenaires commerciaux

Étant donné la grande variété des utilisateurs d'API, les contrôles de sécurité disponibles pour protéger ces API varient également. Jusqu'à récemment, l'industrie s'est concentrée sur les cas d'utilisation B2C, mais sans se préoccuper véritablement de la sécurisation des API B2C. Les efforts portaient plutôt sur la sécurisation des applications Web. Les outils et contrôles de sécurité généralement utilisés pour sécuriser les applications Web B2C offrent certains avantages (pare-feu d'application Web [WAF]/protection d'applications Web et d'API [WAAP], par exemple), mais ne peuvent pas fournir le degré de visibilité, de surveillance en temps réel et de protection requis pour sécuriser les API B2C contre les attaques.

La protection des API B2B devient de plus en plus difficile. Ces API sont souvent des cibles plus faciles pour les pirates, car elles manquent souvent de mécanismes de protection essentiels. Les outils de sécurité des API précédents avaient une visibilité limitée sur les API B2B et avaient du mal à sécuriser les API qui facilitaient l'accès aux données en masse au nom d'utilisateurs partagés (dans le cas de l'open banking, par exemple, où les entreprises de technologie financière et les institutions financières partagent d'un commun accord les données de leurs clients). Cependant, les nouvelles solutions de sécurité des API offrent une analyse comportementale et peuvent reconnaître les activités anormales, répondant ainsi efficacement à ces préoccupations.

Qu'est-ce qui distingue les API privées des API publiques ?

Les API privées, parfois aussi appelées API internes, sont destinées à être utilisées par les développeurs et les sous-traitants de l'entreprise. Faisant souvent partie d'une initiative d'architecture orientée services (SOA), les API privées sont destinées à rationaliser le développement interne en permettant à différents départements ou différentes unités commerciales d'accéder aux données les uns des autres de manière efficace et efficiente.

En revanche, les API publiques, également connues sous le nom d'API externes, sont exposées à des internautes extérieurs à l'entreprise. Dans leur manifestation la plus extrême, en tant qu'API ouvertes, elles peuvent être consommées librement par n'importe qui. Dans tous les cas, elles nécessitent une gestion stricte et une excellente documentation, afin de pouvoir être utilisées par des ingénieurs extérieurs à l'entreprise.

Il est important de noter que les API privées auxquelles on peut accéder par le biais d'Internet ne sont pas vraiment privées, au sens strict du terme. Par exemple, supposons que l'API B2C d'ACME est utilisée uniquement par les applications pour mobile d'ACME (développées en interne par les ingénieurs d'ACME). Vous pourriez être tenté de dire qu'il s'agit d'une API privée, mais comme le trafic vers cette API provient d'Internet (« en dehors de l'entreprise »), cette API n'est pas vraiment privée : elle est simplement non publiée à des publics externes. Les pirates informatiques s'attaquent régulièrement à ces API en interceptant le trafic et en procédant à une rétro-ingénierie des applications pour mobile afin de trouver les API correspondantes.

La sécurité des API expliquée

Qu'est-ce que la sécurité des API ?

La sécurité des API est une stratégie qui permet de bénéficier d'une meilleure visibilité de toutes les API d'une entreprise, de les tester de manière rigoureuse et de les protéger. Cela inclut les API qui font partie intégrante des applications, des processus métier et des charges de travail dans le cloud. Cependant, étant donné que les API internes et externes sont produites rapidement et en nombre, il peut être difficile de bien comprendre l'ensemble du paysage d'API de votre entreprise. De nombreuses entreprises manquent de visibilité sur le nombre d'API dont elles disposent et sur les API qui renvoient des données sensibles lorsqu'elles sont appelées. L'identification et l'atténuation des risques de sécurité des API nécessitent des contrôles de sécurité suffisamment pointus pour fournir ce type de visibilité et d'analyse des données. Les API suivantes, par exemple, nécessitent une protection :

- API destinées à rendre les données facilement accessibles aux clients ou aux partenaires commerciaux
- API consommées par des partenaires commerciaux
- API implémentées et utilisées en interne pour mettre les fonctionnalités et les données d'une application à la disposition de divers systèmes et interfaces utilisateur d'une manière normalisée et évolutive

Une stratégie de sécurité des API efficace doit comprendre des techniques systématiques d'évaluation des risques et de des conséquences potentielles, ainsi que l'exécution de mesures d'atténuation appropriées. La première étape de l'évaluation des risques consiste à dresser l'inventaire de toutes les API approuvées et non approuvées publiées et utilisées par l'entreprise. Cet inventaire doit comprendre différents attributs, dont les suivants :

- Classification des données établissant au minimum une distinction entre les données « non sensibles », « sensibles » et « très sensibles »
- Indicateurs de risque, tels que les vulnérabilités et les erreurs de configuration des API

De plus, les mesures de visibilité des API et d'atténuation des risques doivent prendre en compte un ensemble diversifié de menaces possibles, notamment via les actions suivantes :

- Détection et prévention de l'utilisation d'API « fantômes » non autorisées (voir encadré)
- Identification et correction des vulnérabilités et des erreurs de configuration des API susceptibles d'être exploitées par des acteurs malveillants
- Prévention des cas d'utilisation abusive des API, tels que l'exploitation de logique métier et l'extraction de données

En quoi la sécurité des API diffère-t-elle de la sécurité des applications ?

Bien que la sécurité des API et la sécurité des applications traditionnelles soient des disciplines apparentées, la sécurité des API constitue un défi distinct pour deux raisons essentielles : l'échelle et la complexité du problème.

L'échelle

Trois facteurs contribuent à la croissance rapide de l'utilisation des API :

1. Le développement des microservices, une architecture qui impose l'utilisation d'API pour la communication de service à service.
2. Dans le canal de l'utilisateur direct, les structures des applications frontales actuelles, comme React, Angular et Vue, utilisent des API et remplacent les applications Web héritées.
3. Des API sont ajoutées pour répondre à des canaux entièrement nouveaux (partenaires, IoT et automatisation des activités, par exemple).

La flexibilité menant à la complexité

Contrairement aux applications Web, les API sont conçues pour être utilisées par programmation de différentes manières, ce qui rend extrêmement difficile la différenciation entre une utilisation légitime et les attaques et exploitations.

Existe-t-il une taxonomie des API que les équipes de sécurité doivent comprendre ?

Les catégories et descriptions des API suivantes sont courantes et peuvent être utilisées dans un contexte de sécurité.

API approuvées

API publiées (avec documentation Swagger ou similaire)

API non approuvées

- API fantômes
- API indésirables
- API zombies
- API masquées

API obsolètes

- API vouées à disparaître
- API héritées
- API zombies
- API orphelines

Quelles sont les meilleures pratiques pour protéger les API ?

Pour améliorer la sécurité de vos API, commencez par appliquer les meilleures pratiques suivantes :

- Intégrer les normes et pratiques de sécurité des API dans le cycle de développement logiciel de l'entreprise.
- Incorporer la documentation des API et les tests de sécurité automatisés dans les pipelines d'intégration continue/de diffusion continue (CI/CD).
- S'assurer que des contrôles d'authentification et d'autorisation appropriés et efficaces sont appliqués aux API.
- Mettre en œuvre des mesures de limitation du débit pour éviter que les API ne soient exploitées ou qu'elles ne soient saturées.
- Renforcer les mesures de limitation du débit et autres mesures au niveau de l'application avec des passerelles spécialisées et/ou des réseaux de diffusion de contenu afin d'atténuer le risque d'attaques par déni de service distribué (DDoS).
- Faire des tests de sécurité des API une partie intégrante des processus de test des applications plus larges.
- Effectuer une découverte continue des API.
- Mettre en œuvre une approche systématique afin d'identifier les vulnérabilités courantes des API et d'y remédier, notamment le classement des 10 principaux risques pour la sécurité des API de l'OWASP.
- Utiliser la détection et la prévention des menaces basées sur les signatures comme niveau de protection de base contre les attaques connues des API.
- Augmenter la détection basée sur les signatures avec l'IA et l'analyse comportementale afin de rendre la détection des menaces liées aux API plus évolutive, plus précise, plus pertinente pour l'entreprise et plus résiliente face aux nouvelles menaces.
- Veiller à ce que le processus de surveillance et d'analyse de la sécurité des API s'étende sur plusieurs semaines et sessions API.
- Compléter la surveillance de la sécurité des API et les alertes par un accès à la demande à l'inventaire des API et aux données d'activité à l'intention des détecteurs de menaces, des développeurs, de DevOps et du personnel d'assistance.

Votre capacité à mettre en œuvre ces meilleures pratiques de sécurité API dépend de là où vous en êtes dans votre transition vers une stratégie de sécurité API mature (voir encadré).

Étapes pour atteindre la maturité en matière de sécurité des API

Étape 1 : Visibilité et détection

Vous êtes en train de découvrir toutes vos API et les microservices qu'elles prennent en charge en utilisant une approche automatisée. L'étendue de la couverture est essentielle, car les API négligées (comme celles qui ne sont plus utilisées) sont une cible privilégiée pour les acteurs malveillants.

Étape 2 : Test

Vous testez toutes vos API pour vous assurer qu'elles sont codées correctement et qu'elles remplissent leur fonction. Les tests effectués avant le déploiement d'une API constituent l'ultime phase de cette étape de maturité. Le risque est éliminé avant l'entrée en production de l'API et tout correctif nécessaire est exponentiellement moins coûteux.

Étape 3 : Audit des risques

Vous auditez continuellement l'ensemble de votre environnement API pour identifier celles qui sont mal configurées ou toutes autres erreurs. Votre audit garantit également une documentation adéquate de toutes les API et détermine si elles contiennent des données sensibles ou si les contrôles de sécurité appropriés sont insuffisants.

Étape 4 : Protection de la durée d'exécution

Vous utilisez une solution qui assure la protection automatisée de la durée d'exécution, qui peut faire la différence entre les activités normales et anormales des API. En surveillant ainsi les interactions des API, vous êtes en mesure de détecter les comportements indiquant une menace en temps réel.

Étape 5 : Réponse

Vous avez mis en place des solutions pour répondre aux comportements suspects des API, telles qu'un WAF ou une passerelle d'API qui bloque le trafic suspect avant qu'il puisse accéder aux ressources critiques. Vos solutions utilisent des règles personnalisées et automatisées.

Étape 6 : Recherche des menaces

Vous analysez régulièrement les données des menaces antérieures pour savoir si les alertes ont correctement identifié les menaces et si des modèles permettant une recherche proactive des menaces ont émergé en combinant des outils sophistiqués et l'intelligence humaine.

Risques et exploitations liés à la sécurité des API

Qu'est-ce qu'une vulnérabilité d'API ?

Une vulnérabilité d'API est un bogue logiciel ou une erreur de configuration système qu'un attaquant peut exploiter pour accéder à des fonctionnalités ou aux données sensibles d'une application, ou encore pour utiliser abusivement une API. Les 10 principaux risques pour la sécurité des API de l'OWASP offrent un aperçu utile de certaines des vulnérabilités d'API les plus largement exploitées que les entreprises devraient tenter d'identifier et de corriger.

Toutes les vulnérabilités des API sont-elles répertoriées dans le classement des 10 principaux risques pour la sécurité des API de l'OWASP ?

Le classement des 10 principales vulnérabilités des API de l'OWASP est un excellent point de départ pour les entreprises qui cherchent à améliorer leur stratégie de sécurité des API. Les catégories définies couvrent un large éventail de risques possibles liés aux API. Les catégories incluses dans les 10 principaux risques pour la sécurité des API selon l'OWASP étant assez larges, il est important d'approfondir les sous-domaines de chacune d'entre elles. Les attaquants d'API tentent souvent d'exploiter les problèmes d'autorisation (largement couverts par l'OWASP), mais il existe également des risques liés aux API qui échappent totalement au classement des 10 principaux risques pour la sécurité des API selon l'OWASP, tels que l'exploitation de bogues logiques.

Comment peut-on exploiter les API ?

Les API peuvent être attaquées et exploitées de différentes manières, mais voici certaines des méthodes les plus courantes :

- **Exploitation de vulnérabilités :** les vulnérabilités techniques de l'infrastructure sous-jacente peuvent servir à compromettre le serveur. Parmi ces vulnérabilités, vous trouverez par exemple les vulnérabilités Apache Struts (CVE-2017-9791, CVE-2018-11776) ou les vulnérabilités Log4j (CVE-2021-44228).

- **Exploitation de logique métier :** il y a exploitation de logique lorsqu'un acteur malveillant exploite les failles de conception ou d'implémentation d'une application pour provoquer un comportement inattendu et non approuvé. Ces scénarios sont source de stress pour les RSSI et leurs équipes, car les contrôles de sécurité hérités ne peuvent rien contre eux.

- **Accès non autorisé aux données :** une autre forme courante d'exploitation des API consiste à profiter de mécanismes d'autorisation défaillants pour accéder aux données auxquelles l'on ne devrait pas pouvoir accéder. Ces vulnérabilités portent de nombreux noms, tels que BOLA (défaillance de l'autorisation au niveau de l'objet) et IDOR (accès direct non sécurisé à un objet), ainsi que BFLA (défaillance de l'autorisation au niveau de la fonction).

- **Piratage de comptes :** après un vol d'informations d'identification ou même une attaque XSS, un compte peut être piraté. Une fois que cela se produit, il est possible d'exploiter même l'API la mieux écrite et la mieux sécurisée. Utiliser une solution de sécurité des API qui offre une analyse comportementale vous permet de faire la différence entre une activité authentifiée et une utilisation illégitime.

- **Extraction de données :** à mesure que les entreprises mettent des ensembles de données à disposition via des API publiques, des acteurs malveillants peuvent interroger ces ressources de manière agressive pour effectuer une capture élargie d'ensembles de données volumineux et précieux.

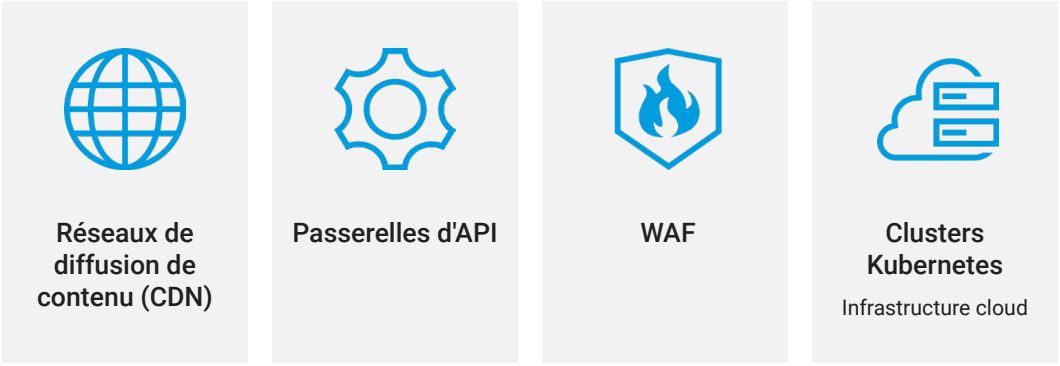
- **Déni de service (DoS) :** en demandant au back-end d'effectuer des tâches lourdes, les attaquants d'API peuvent provoquer une « érosion du service » ou un déni de service complet au niveau de la couche applicative (une vulnérabilité très courante dans GraphQL, mais qui peut arriver avec toute implémentation de point de terminaison d'API gourmande en ressources).

Qu'est-ce qu'une API zombie ?

En raison de l'évolution des exigences du marché et des entreprises, le flux des API est constant. Au fur et à mesure que de nouvelles implémentations de points de terminaison sont publiées pour répondre aux nouveaux besoins des entreprises, corriger les bogues ou introduire des améliorations techniques, les anciennes versions de ces points de terminaison deviennent obsolètes. La gestion du processus de déclassement des anciens points de terminaison ne doit pas être prise à la légère. En effet, il est fréquent que des implémentations de points de terminaison qui auraient dû être déclassés restent en service et accessibles ; on parle alors de points de terminaison zombies.

Comment trouver les différents types d'API fantômes ?

L'une des façons d'identifier les API fantômes à l'échelle de l'entreprise consiste à capter et à analyser le trafic d'API sur votre réseau. Voici quelques exemples de sources de trafic d'API :



Une fois que les données brutes provenant de toutes les sources disponibles sont collectées, l'utilisation de techniques d'IA permet de les transformer en un inventaire complet de l'ensemble des API, points de terminaison et paramètres. À partir de là, des analyses supplémentaires peuvent être effectuées pour classer ces éléments et identifier les API fantômes qui doivent être éliminées ou intégrées dans des processus de gouvernance formels.

Comment protéger les API internes et les API B2B ?

Tout dépend de la définition du terme « interne ». Certaines équipes qualifient d'« API internes » les API exposées sur Internet aux applications Web et pour mobile de leur propre entreprise. Et même si la documentation de ces API n'est en effet accessible qu'aux employés et aux sous-traitants de l'entreprise, les pirates informatiques sont devenus experts dans l'analyse des applications et l'ingénierie inverse des API par le biais de boîtes à outils de désassemblage d'applications et des proxys tels que Burp Suite.

Toutefois, si les « API internes » sont définies comme des API est-ouest, auxquelles il est impossible d'accéder depuis l'extérieur de l'entreprise, la principale menace se réduit alors à une menace interne. Protégez les API est-ouest et vos API B2B comme la plupart des autres API : commencez par sécuriser le cycle de développement de logiciels (SDLC), puis poursuivez en garantissant un accès authentifié et autorisé. Vous pouvez également assurer la gestion des quotas, des limites de débit et des arrêts d'urgence. De plus, vous pouvez protéger vos API contre les menaces connues en utilisant des WAF/WAAP. Pour les API B2B, envisagez d'ajouter des mécanismes d'authentification stricts, tels que mTLS, en raison de la nature sensible et souvent volumineuse des transactions.

Pour les API est-ouest comme B2B, nous vous recommandons d'utiliser l'analyse comportementale, en particulier si de nombreuses entités sont impliquées, ce qui peut rendre difficile le processus de distinction entre les comportements légitimes et illégitimes. Par exemple :

> **Comment savoir si les informations d'identification d'API d'un utilisateur spécifique ont été compromises ?**

> **Comment savoir si votre API de facturation est exploitée par un partenaire qui énumère des numéros de facture pour dérober des données de compte ?**

La protection des API B2B et des API est-ouest nécessite un contexte opérationnel qui ne peut pas être obtenu en analysant uniquement des éléments techniques tels que les adresses IP et les jetons API. L'utilisation de l'apprentissage automatique et de l'analyse comportementale pour obtenir une visibilité sur les entités pertinentes pour l'entreprise est la seule façon de comprendre et de gérer efficacement les risques. Le contexte opérationnel et les références historiques pour l'utilisation normale des API par des entités spécifiques telles que vos utilisateurs ou partenaires, ou même des entités de processus métier (facture, paiement, commande, etc.), permettent de repérer des anomalies qui, autrement, passeraient inaperçues.

Les passerelles d'API offrent-elles une protection suffisante contre les risques ?

De nombreuses entreprises qui adoptent une approche stratégique des API utilisent des passerelles d'API. La plupart de ces passerelles disposent de fonctions de sécurité intégrées performantes dont les entreprises doivent tirer parti, la première d'entre elles étant l'authentification (ainsi que l'autorisation, si vous avez la possibilité d'exploiter OpenID Connect). Toutefois, l'authentification, l'autorisation et la gestion des quotas au niveau de la passerelle d'API ne suffisent pas à elles seules, et ce pour plusieurs raisons :

L'écart de découverte des passerelles d'API : la visibilité et le contrôle dont disposent les passerelles d'API sont limitées aux API qu'elles doivent gérer conformément à la configuration, ce qui les rend inefficaces pour détecter les points de terminaison et les API fantômes.

Le manque de sécurité des passerelles d'API : les passerelles d'API peuvent imposer l'authentification et, dans une certaine mesure, des schémas d'autorisation, mais elles n'inspectent pas les charges utiles (comme le font les WAF et les WAAP) et ne profilent pas les comportements pour détecter les exploitations.

Quelles sont les erreurs de configuration d'API les plus courantes ?

Étant donné le grand nombre de façons dont les API sont utilisées, le nombre d'erreurs de configuration d'API possibles est presque infini. Cependant, voici quelques thèmes communs en matière de mauvaise configuration :

Authentification défaillante ou inexistante

L'authentification est indispensable à la sécurisation des données sensibles mises à disposition par le biais des API. La première étape consiste à s'assurer que toutes les API transportant des données sensibles disposent d'une authentification initiale. Toutefois, il est également important de protéger les mécanismes d'authentification contre les attaques par force brute, le credential stuffing et l'utilisation de jetons d'authentification volés par le biais de la limitation du débit. Des erreurs de configuration permettant aux utilisateurs d'API de contourner les mécanismes d'authentification peuvent parfois se produire, souvent au niveau de la gestion des jetons (par exemple, certains problèmes notoires de validation JWT, ou le fait de ne pas vérifier la portée d'un jeton).

Autorisation défaillante

L'une des utilisations les plus courantes des API consiste à donner accès à des données ou à du contenu, y compris à des informations sensibles. L'autorisation est le processus qui consiste à vérifier qu'un utilisateur d'API a le droit d'accéder aux données qu'il tente d'obtenir, avant de les mettre à sa disposition. Cela peut se faire au niveau de l'objet ou de la ressource (par exemple, je peux accéder à mes commandes mais pas à celles de quelqu'un d'autre) ou au niveau de la fonction (comme c'est souvent le cas avec les capacités administratives). Il est difficile d'obtenir une autorisation correcte en raison du grand nombre de cas limites et de conditions, ainsi que des différents flux que les appels API peuvent emprunter entre les microservices. Si vous ne disposez pas d'un moteur d'autorisation centralisé, votre implémentation d'API comporte probablement certaines de ces vulnérabilités, telles que BOLA et BFLA.

Mauvaise configuration de sécurité

Outre les problèmes d'authentification et d'autorisation susmentionnés, il existe de nombreux types possibles de mauvaises configurations de la sécurité, notamment des communications non sécurisées (la non-utilisation de SSL/TLS ou l'utilisation de suites de chiffrement vulnérables, par exemple), un stockage cloud non protégé et des règles de partage de ressources d'origines croisées trop permissives.

Manque de ressources et limitation de débit

Lorsque les API sont implémentées sans aucune limite quant au nombre d'appels que les utilisateurs d'API peuvent effectuer, des acteurs malveillants peuvent submerger les ressources du système, entraînant une dégradation des services ou un DoS (déni de service) à grande échelle. Au minimum, des limites de débit doivent être appliquées à l'accès à tout point de terminaison non authentifié, les points de terminaison d'authentification étant d'une importance cruciale. Sinon les attaques par force brute, le credential stuffing, ainsi que les attaques de validation d'informations d'identification sont tout simplement inévitables.

Que sont les attaques d'API ?

Les attaques d'API sont des tentatives d'utilisation d'API à des fins malveillantes ou non autorisées. Il existe de nombreuses formes d'attaques d'API, dont les suivantes :

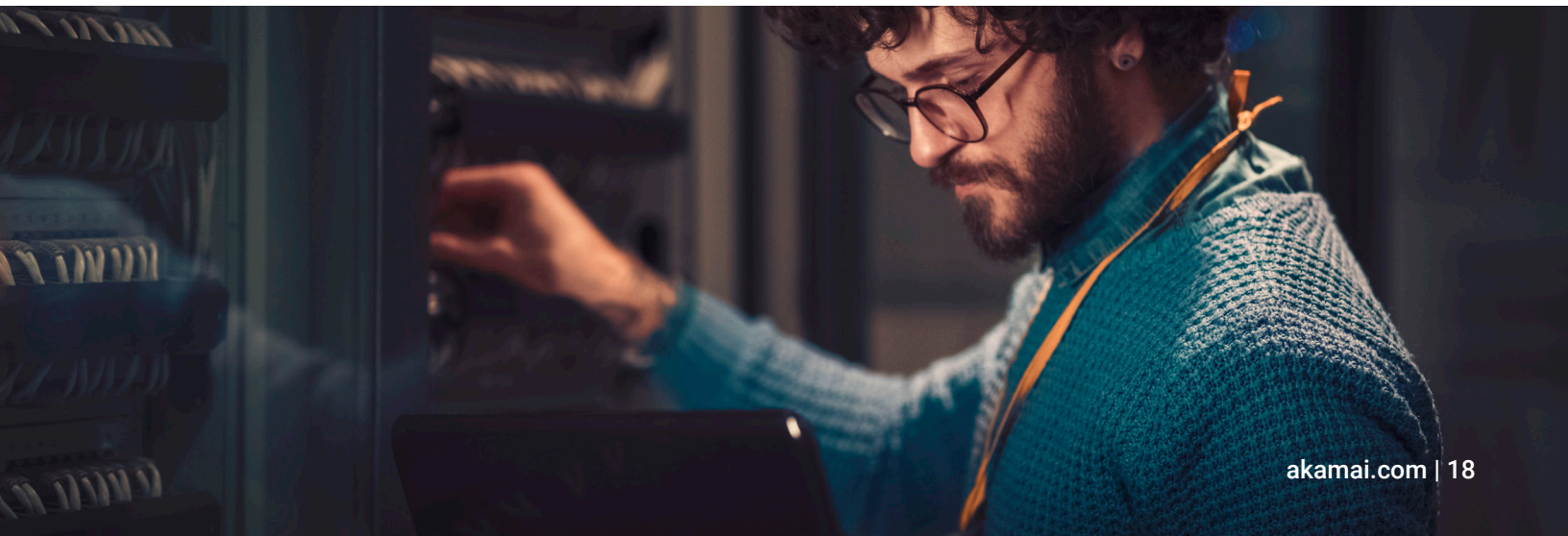
- Exploitation de vulnérabilités techniques lors de la mise en œuvre d'API
- Utilisation d'informations d'identification volées et d'autres techniques de piratage de compte pour se faire passer pour un utilisateur légitime
- Exploitation de logique métier permettant d'utiliser les API de manière inattendue

Qu'est-ce que le credential stuffing pour les API ?

Les fuites d'informations relatives aux identifiants et aux mots de passe des sites Web et des plateformes de logiciels en tant que service (SaaS) sont devenues monnaie courante. Souvent, ces incidents se traduisent par la diffusion en ligne d'un grand nombre d'informations d'identification. Le credential stuffing est la pratique consistant à utiliser des informations d'authentification divulguées à partir de sites Web précédemment piratés pour effectuer des tentatives de connexion automatisées vers d'autres sites Web. Cette technique part du principe qu'un certain pourcentage d'utilisateurs utilise les mêmes identifiants pour plusieurs sites. Les pirates s'attaquent de plus en plus aux API et ciblent leurs mécanismes d'authentification. Cela leur permet d'automatiser l'attaque plus facilement puisque les API sont créées pour faciliter la consommation.

Qu'est-ce que l'exfiltration de données via les API ?

L'exfiltration de données est un résultat fréquent d'abus et d'attaques d'API réussis. Dans certains cas, cela fait référence à des informations hautement sensibles et non publiques qui ont été volées par un acteur malveillant par d'une attaque d'API. Cependant, il peut également s'agir de types d'abus d'API moins graves, notamment l'extraction agressive de données accessibles au public pour assembler de grands ensembles de données utiles sous forme agrégée.



Solutions et tendances en matière de sécurité des API

Quelles sont les dernières tendances en matière de sécurité des API ?

Voici les principales tendances que les responsables de la sécurité doivent prendre en compte lors de l'élaboration d'une stratégie de sécurité des API :

Analyse comportementale et détection des anomalies : plutôt que d'essayer de prédire les attaques possibles et de s'appuyer uniquement sur la détection basée sur les signatures et les règles prédéfinies (par exemple, WAF) pour atténuer les risques, les entreprises ajoutent de plus en plus l'apprentissage automatique et l'analyse comportementale pour voir l'activité des API dans le contexte opérationnel et détecter les anomalies.

Transition d'une solution sur site à une solution SaaS : alors que de nombreux produits de sécurité des API de première génération étaient déployés sur site, les approches basées sur une solution SaaS gagnent en popularité en raison de leur rapidité, de leur facilité de déploiement et de leur capacité à exploiter la puissance de l'apprentissage automatique à grande échelle.

Analyse de fenêtres temporelles plus larges : les approches de sécurité des API qui analysent uniquement les appels d'API individuels ou l'activité des sessions à court terme sont supplantées par des plateformes qui peuvent analyser l'activité des API sur plusieurs jours, voire plusieurs semaines. Cela va de la réalisation d'une optimisation automatisée de base des règles WAF jusqu'à l'exécution d'analyses comportementales et la détection d'anomalies.

DevSecOps – Intégrer les parties prenantes non liées à la sécurité : l'un des meilleurs moyens de réduire les risques liés aux API consiste à créer des liens plus étroits entre les stratégies et outils de sécurité des API et les développeurs et systèmes impliqués dans la création, la mise en œuvre et la configuration d'API.

Sécurité des API basée sur les API : s'il est essentiel de détecter et d'atténuer les attaques d'API actives et les instances d'exploitation, les entreprises tournées vers l'avenir trouvent des moyens d'utiliser l'accès à la demande aux données et aux informations de sécurité des API pour améliorer la recherche des menaces, la réponse aux incidents et les pratiques de développement d'API.

Qu'est-ce que la sécurité des API basée sur les signatures ?

Les techniques de sécurité des API basées sur les signatures surveillent les caractéristiques et les modèles d'attaque connus et génèrent des alertes de sécurité et d'autres réponses automatisées lorsque des correspondances sont observées. Cette technique est typique d'un WAF. L'avantage : si une entreprise est informée d'un trafic d'API entrant qui est compromis ou qui se comporte de manière anormale, elle peut utiliser la sécurité des API basée sur les signatures pour le bloquer immédiatement. Autrement dit, si une entreprise est informée d'un trafic d'API entrant qui est compromis ou qui se comporte de manière anormale, elle peut utiliser la sécurité des API basée sur les signatures pour le bloquer immédiatement.

Il est essentiel de trouver un WAF qui fait partie d'une solution WAAP plus large et qui peut offrir des capacités de détection avancées utilisant l'apprentissage automatique pour apprendre à partir des modèles de signature d'attaques et pouvoir rester agile à grande échelle. Une solution WAAP intégrée à une solution de sécurité des API proposant des analyses comportementales et des réponses personnalisées vous permettra d'obtenir le meilleur des deux mondes. Ensemble, ces solutions offrent une visibilité des API, une détection et une réponse complètes en interne et en externe.

Qu'est-ce que la détection et la réponse API ?

La détection et la réponse API correspond à une catégorie émergente de sécurité des API axée sur l'analyse approfondie des données historiques. Elle a pour but de :

- déterminer une base de référence du comportement de tous les utilisateurs d'API ;
- détecter les attaques et les anomalies qui indiquent une éventuelle exploitation ou mauvaise utilisation d'API.

Pour être efficace à grande échelle, la détection et la réponse API doivent être fournies dans le cadre d'un modèle SaaS, en raison des grands ensembles de données impliqués et des besoins des techniques d'apprentissage automatique gourmandes en ressources.

Qu'est-ce que la protection avancée contre les menaces liées aux API ?

La protection avancée contre les menaces liées aux API est une approche de la sécurité des API basée sur une solution SaaS associant analyse comportementale et détection des menaces, et destinée à :

- découvrir toutes les API utilisées par une entreprise, y compris les API fantômes ou zombies ;
- appliquer l'apprentissage automatique pour superposer le contexte opérationnel sur la façon dont les API sont utilisées et exploitées ;
- effectuer une analyse comportementale et une recherche des menaces sur les API et les données d'activité des API.

Qu'est-ce qu'une plateforme de sécurité des API ?

Une plateforme de sécurité des API est une offre SaaS spécialement conçue pour :

- Créer un inventaire actualisé en permanence de toutes les API utilisées à l'échelle de l'entreprise (qu'elles soient approuvées ou non)
- Analyser les API et leur utilisation pour découvrir le contexte opérationnel et déterminer une base de référence du comportement attendu
- Détecter les anomalies dans l'utilisation des API et, le cas échéant, fournir des alertes et des données de soutien à la gestion des événements et des informations de sécurité (SIEM) et aux flux de travail d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR)
- Fournir un accès à la demande à l'inventaire des API, à l'activité et aux informations sur les menaces pour les parties prenantes liées et non liées à la sécurité

Qu'est-ce qu'une entreprise de sécurité des API ?

Maintenant que les responsables de l'informatique et de la sécurité utilisent les API de manière plus stratégique, ils peuvent avoir besoin d'engager des partenaires API spécialisés. Les trois types d'entreprises d'API les plus courants sont les suivants :

- Les entreprises de passerelles API qui fournissent une technologie permettant d'accepter les appels API de manière centralisée et de les acheminer vers les ressources et microservices dorsaux appropriés.
- Les entreprises de plateformes de sécurité des API qui veillent à ce que les entreprises soient au courant de toutes les API actives et de leurs risques potentiels, peuvent détecter les cas d'attaques et d'exploitation, effectuer des tests de sécurité complets et fournir des données riches sur la manière dont les API sont utilisées.
- Les entreprises de plateformes WAAP et de sécurité des API qui peuvent aider à transférer facilement les données relatives au trafic des API tout en offrant la possibilité de découvrir les API sur la plateforme et hors plateforme ; cette solution est idéale pour la consolidation des fournisseurs et la réduction de la fracture digitale.

Qu'est-ce que la recherche des menaces au niveau des API ?

La détection des menaces consiste à rechercher activement des menaces inconnues ou non détectées auparavant. Cette approche proactive est essentielle pour identifier les menaces nouvelles et émergentes qui n'ont peut-être pas été détectées auparavant afin de les atténuer avant qu'elles ne causent des dommages importants. L'analyse comportementale est une autre technique importante utilisée pour la recherche des menaces. Elle consiste à analyser le comportement des API afin d'identifier toute activité suspecte ou anormale. Par exemple, si une API demande soudainement des milliers d'enregistrements sur une courte période, cela peut indiquer que la logique commerciale de l'API est compromise. Les solutions de sécurité des API actuelles proposent des capacités spécifiques de recherche des menaces pour permettre aux équipes de sécurité d'identifier rapidement les menaces éventuelles et d'y remédier par le biais de contre-mesures.

Qu'est-ce qu'une solution WAAP ?

La protection des applications Web et des API (WAAP) est une catégorie que le cabinet de recherche Gartner utilise pour couvrir le secteur des solutions de protection des applications Web et des API émergentes. Il s'agit d'une évolution de la couverture sectorielle antérieure du marché du WAF en réponse à l'importance stratégique croissante de la sécurité des API, mais aussi au passage des plateformes WAF au cloud en tant que SaaS géré.

Quelle forme prend la documentation des API ?

La forme la plus courante de documentation des API pour les API RESTful (le type d'API Web le plus courant) est une collection de fichiers Swagger basés sur la spécification OpenAPI. Dans l'idéal, la documentation est créée par les développeurs lors de la conception ou de l'implémentation d'une API. Cependant, la documentation des API est en fait souvent obsolète, ce qui entraîne un décalage entre l'utilisation réelle d'une API et sa documentation. Pour résoudre ce problème, certaines plateformes de sécurité des API peuvent générer des fichiers Swagger à partir de l'activité réelle des API, mettant en évidence les écarts entre ce qui est documenté et ce qui est réellement déployé (un composant intégral de toute évaluation des risques liés aux API).

Existe-t-il une liste de contrôles de sécurité des API recommandés aux entreprises ?

Une sécurité efficace des API nécessite de nombreuses étapes détaillées et des pratiques continues spécifiques à une entreprise. Toutefois, voici une liste de contrôles des API que les équipes de sécurité peuvent utiliser comme point de départ pour faire évoluer la sécurité de leurs API :

- Votre approche de la sécurité des API inclut-elle un mécanisme de découverte continue des API à l'échelle de l'entreprise ?
- La gestion de la posture des API est-elle intégrée aux pratiques de gestion des risques et de la sécurité au sens large de l'entreprise ?
- Implémentez-vous une approche de sécurité des API à usage général qui ne vous enfermera pas dans des modèles spécifiques de centre de données ou d'infrastructure cloud ?
- Votre approche donnera-t-elle à vos équipes le contexte opérationnel dont elles ont besoin pour comprendre réellement l'activité des API et les risques éventuels observés ?
- Avez-vous une stratégie d'automatisation bidirectionnelle entre votre plateforme de sécurité des API et d'autres processus métier connexes tels que SIEM/SOAR, détection des menaces, documentation, outils DevOps, etc. ?
- Prenez-vous des mesures pour accueillir les parties prenantes non liées à la sécurité, comme les développeurs, dans vos outils et processus de sécurité des API ?

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 : 09/24.