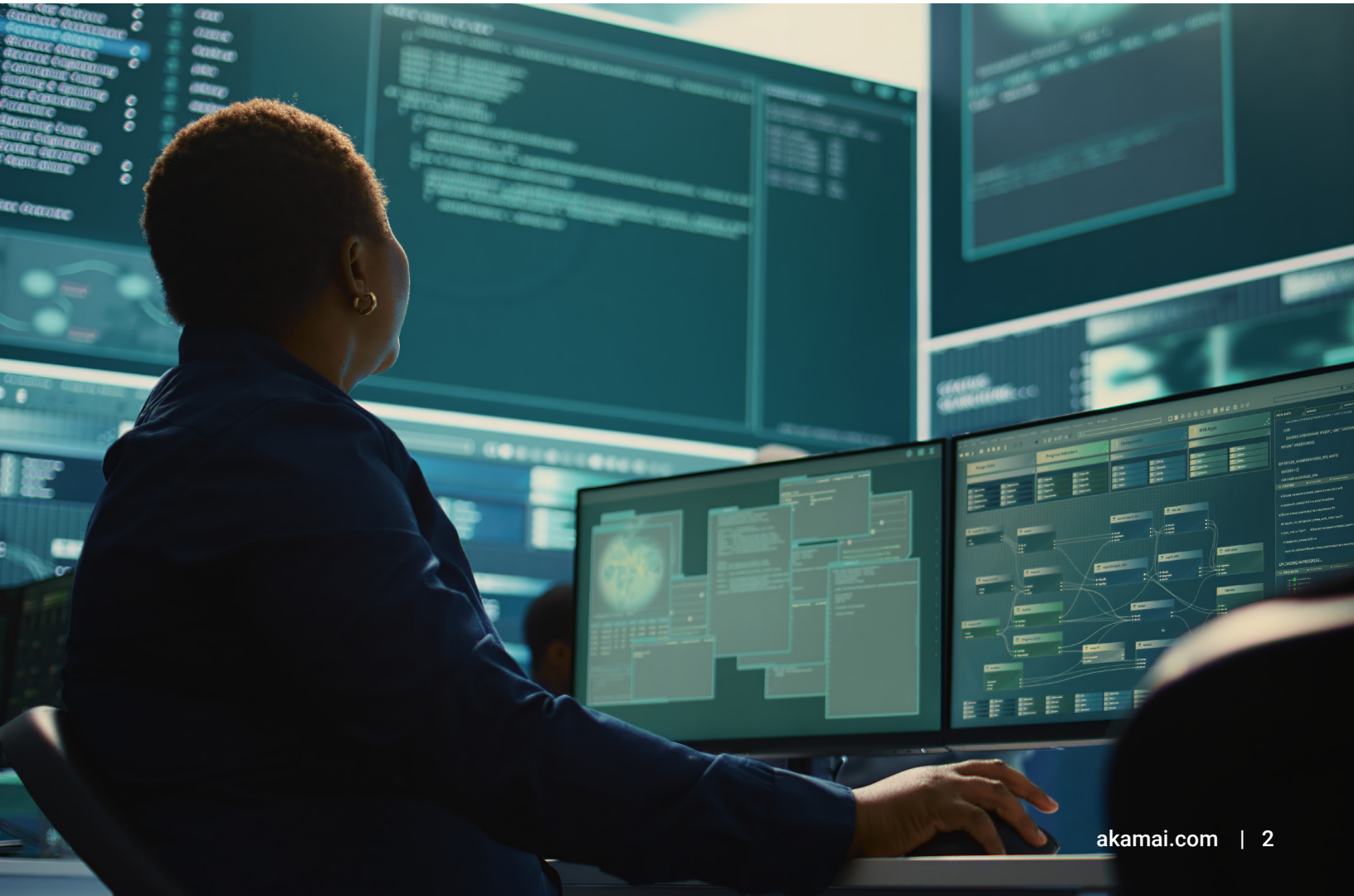
Akamai

LIVRE BLANC

Sécurité et conformité des API

Exigences implicites et explicites pour la protection des données

Dans ce rapport



Introduction

Respecter les réglementations en matière de protection des données a longtemps, traditionnellement, supposé d'importants investissements en énergie et en ressources pour faire face à des risques pour la plupart familiers. Mais la situation est en train de changer. Aujourd'hui, la surface d'attaque évolue rapidement pour inclure des menaces que la plupart des programmes de conformité des entreprises ne prennent pas entièrement en compte. Cela s'explique en partie par le fait que les organismes de réglementation eux-mêmes ne peuvent pas toujours suivre le rythme et être explicites sur toutes les facettes de la couverture nécessaire pour prévenir les violations.

C'est le cas de la protection des API. Chaque fois qu'un client, un partenaire ou un fournisseur entre en contact avec votre entreprise par voie digitale, il y a une API en coulisse qui facilite l'échange rapide d'informations qui comprennent souvent des données sensibles. Les attaquants savent désormais qu'ils peuvent simplifier leur stratégie de vol de données en ciblant directement les API.

Vous avez peut-être déjà vu dans les réglementations un nouveau langage indiquant la nécessité d'inventorier, d'évaluer ou de sécuriser les API. Mais même en l'absence d'un libellé spécifique sur les API, le fait qu'elles soient devenues un vecteur d'attaque évident *implique* la nécessité de les protéger de manière adéquate.

L'émergence des API en tant que problème majeur de conformité n'est pas surprenante. Les API exposées ou mal configurées sont courantes, faciles à compromettre et souvent non protégées. Et une seule API violée peut entraîner le vol de millions d'enregistrements. Les chiffres parlent d'eux-mêmes :

- Soixante-dix-huit pour cent des organisations ont été confrontées à un incident lié à la sécurité des API.[1]
- Quarante-quatre pour cent d'entre elles ont été condamnées à une amende par les autorités de réglementation en raison d'incidents liés à la sécurité des API.[2]

Quel est l'impact sur votre programme de conformité ? Les régulateurs ont besoin de voir que votre organisation prend des mesures pour protéger tous les points d'accès aux données sensibles. Cela signifie que vous devez démontrer que votre organisation peut :

- rendre compte de chaque API, y compris les API fantômes insaisissables ;
- découvrir et corriger toutes les vulnérabilités des API ;
- appliquer des contrôles sur mesure pour prévenir les violations de données centrées sur les API.

Ce livre blanc explore la nature des risques croissants liés aux API, met en lumière six exemples de réglementations et de cadres qui exigent des protections des API (explicitement ou implicitement) et offre des conseils sur la manière de répondre aux exigences de conformité grâce aux meilleures pratiques en matière de sécurité des API.

1., 2. Akamai Technologies, « Déconnexion de la sécurité des API », 2023

Comprendre les risques liés aux API

Les API sont au cœur des produits, services et environnements cloud digitaux de votre entreprise. Leur accès permanent aux données en fait à la fois un moteur de revenus et un risque opérationnel. Le problème, c'est que la plupart des entreprises (même celles qui disposent de programmes de sécurité matures) n'accordent pas la même priorité aux menaces liées aux API qu'à d'autres menaces, telles que l'hameçonnage ou les ransomwares.

Certaines organisations utilisent des passerelles API et des pare-feux d'application Web (WAF) pour la protection de base des API, mais ces outils ne sont pas conçus pour fournir le même degré de visibilité, de protection en temps réel et de tests continus que les solutions spécialisées de sécurité des API. Voici pourquoi ces outils ne sont pas suffisants :

- Les passerelles API et les WAF ne peuvent observer que le trafic API *géré* qui est acheminé par leur intermédiaire.
- Ils ne peuvent pas protéger les API non gérées, qui, selon les analystes, représenteront près de la moitié de l'écosystème d'API d'une entreprise type d'ici 2025.
- Par conséquent, les équipes de sécurité ne sont pas totalement préparées à protéger la partie de leur surface d'attaque qui se développe le plus rapidement, car elles savent peu de choses sur l'acheminement des API, leur configuration, les types de données sensibles qu'elles échangent et les risques qu'elles présentent.

La protection des informations des utilisateurs est une priorité pour les autorités de réglementation, qui infligent de lourdes amendes aux entreprises qui ne parviennent pas à protéger raisonnablement les données de leurs clients contre les accès non autorisés. Si l'on considère que seuls 4 professionnels de la sécurité sur 10 disposant d'un inventaire complet des API savent lesquelles de leurs API renvoient des données sensibles[3] et que de nombreux appels d'API proviennent d'attaquants qui testent les vulnérabilités, les violations de données via les API ne feront qu'augmenter, d'autant plus que les attaques par API sont actuellement assez faciles à mener.

3. Akamai Technologies, « Déconnexion de la sécurité des API », 2023

Quatre attaques d'API ayant des répercussions sur la conformité

Comment une violation d'API peut-elle affecter la posture de conformité d'une entreprise ? Exemples :

- Une application populaire de gestion de projets a été compromise par un pirate qui a exploité un point d'extrémité d'API dépourvu de contrôles d'authentification. L'attaquant a violé l'API, a obtenu un accès non autorisé à des informations sur des millions d'utilisateurs et, quelques mois plus tard, a divulgué plus de 21 Go de données (notamment des adresses e-mail et des données sur les membres de conseils d'administration) sur Internet.
- Plus de 11 millions de dossiers de clients d'une grande entreprise de télécommunications se sont trouvés en état de vulnérabilité, apparemment à cause d'une API qui était exposée à Internet sans le savoir et qui ne nécessitait pas d'authentification. Les attaquants se sont introduits dans l'API, ont constaté qu'elle n'avait pas d'identifiant unique, ont deviné son numéro d'identification et ont facilement récupéré des données sensibles.
- Une entreprise de médias sociaux aurait été touchée à deux reprises ces dernières années par une tactique de « scraping » rendue possible par une mauvaise utilisation de l'API. Dans le premier cas, des données privées ont été extraites de 500 millions de profils d'utilisateurs, puis vendues. Dans le second cas, un pirate a créé une base de données comprenant des numéros de téléphone et des données salariales extraites auprès de 700 millions d'utilisateurs.
- Cette même technique a été utilisée contre une autre entreprise de médias sociaux pour exfiltrer des données sur des millions d'utilisateurs. L'entreprise a été condamnée à une amende de 5 milliards de dollars parce qu'un fournisseur tiers a utilisé l'API de l'entreprise pour collecter des données sensibles. Peu importe que le fournisseur ait abusé de l'API ; l'entreprise *elle-même* a été condamnée à une amende parce qu'elle n'a pas surveillé son application.

Six exemples de réglementations et de cadres impliquant la sécurité des API

Dans de nombreux règlements et cadres, les API ne sont pas nécessairement mentionnées nommément, mais les exigences sont clairement axées sur la sécurisation des applications et de l'infrastructure au sein desquelles les API fonctionnent. Par exemple :

- La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v4.0 offre des conseils pour confirmer que le logiciel d'une organisation utilise en toute sécurité des fonctions de composants externes. Cela inclut les API qui transmettent les données de paiement d'une application pour mobile au système d'une banque.
- Le cadre de développement de logiciels sécurisés du NIST fournit des conseils sur la production de logiciels bien protégés, leur sécurisation continue et la réponse aux vulnérabilités. Les API sont au cœur du développement des logiciels.

Dans de nombreux cas, les réglementations suggèrent des objectifs vaguement définis pour la sécurisation des données, comme l'exigence du Règlement général sur la protection des données (RGPD) concernant les « mesures de sécurité appropriées ». Vos API peuvent recevoir des millions d'appels par jour pour servir ces données, de la part de clients *et* d'attaquants. Il vous incombe de déterminer les contrôles de sécurité requis, puis de démontrer leur fonctionnement.

Examinons de plus près les réglementations et les cadres ayant des implications directes sur votre écosystème d'API.

1. PCI DSS v4.0

Créée par le Conseil des normes de sécurité de l'industrie des cartes de paiement, PCI DSS est devenue une norme mondiale de protection des données de paiement. Si votre entreprise accepte les principales cartes de crédit et traite, stocke ou transmet électroniquement les données des titulaires de cartes, vous devez respecter cette norme.

Les exigences de la version originale couvrent les piliers de la sécurité qui sont aussi importants aujourd'hui qu'ils l'étaient lorsque la norme PCI DSS a été publiée en 2006, comme l'attribution de l'accès aux données du système et des titulaires de carte en fonction des besoins et la définition des exigences d'accès par rôle.

Toutefois, avec l'entrée en vigueur de la norme PCI DSS v4.0, les entreprises doivent adapter leurs programmes de conformité pour tenir compte des acteurs de la menace qui ciblent fréquemment les milliers d'API présentes dans les technologies de paiement. Dans l'ensemble, la norme PCI DSS v4.0 est centrée sur quatre objectifs principaux :

1. Continuer à répondre aux besoins de sécurité du secteur des paiements
2. Préconiser la sécurité en tant que processus continu
3. Donner aux entreprises une certaine flexibilité (par exemple, de nouveaux outils, de nouveaux contrôles) dans leur manière de répondre aux exigences
4. Améliorer les méthodes et les processus de validation

L'exigence 6.2.3 de la norme PCI DSS v4.0 est axée sur la nécessité pour les organisations d'examiner le code de leurs applications personnalisées (c'est-à-dire le code développé par un fournisseur tiers, mais pas les applications commerciales prêtes à l'emploi standard) afin de s'assurer qu'aucune vulnérabilité n'est introduite dans la production. Propre aux API, cette exigence offre des conseils pour confirmer que le logiciel d'une organisation utilise en toute sécurité les fonctions de composants externes (bibliothèques, cadres, API, etc.). De telles exigences soulignent le rôle clé que jouent les API dans la chaîne d'approvisionnement des logiciels au sens large (et ce qu'il faut pour la protéger).

Les API sont devenues la méthode de connectivité et d'échange de données par défaut dans les environnements applicatifs. Dans cette optique, sécuriser les API avec une approche de pré-production (shift-left) et une approche de post-production (shield-right) est essentielle pour garantir la résilience de votre entreprise digitale face aux attaques. Voici quelques meilleures pratiques en matière de sécurité des API qui vous aideront à respecter la conformité avec l'exigence 6.2.3 :

- Confirmer l'utilisation des composants basés sur l'API et leur posture de sécurité (par exemple, trouver toute erreur de configuration entraînant des vulnérabilités, y compris l'utilisation de chiffrements de cryptage).
- Valider le comportement normal et attendu de l'utilisation de l'API et mettre en place des contrôles pour empêcher les acteurs suspects d'abuser de vos systèmes (par exemple, vérifier le comportement de l'application pour détecter les vulnérabilités logiques).
- Détecter les cadres tiers utilisés pour alimenter vos API, en déterminant ceux qui peuvent être obsolètes et vulnérables.
- Établir un inventaire complet de toutes vos API, y compris les différentes versions des API que vous exécutez. Cela fournit un aperçu des portes dérobées et des fonctionnalités non documentées potentielles que vous devez gérer.
- Valider la sécurité de votre code API et éviter d'intégrer dans la production des vulnérabilités liées aux API.
- Mettre en œuvre les meilleures pratiques de codage sécurisé pour les API, ce qui vous permettra d'adopter une approche programmatique pour fournir du code en toute sécurité et en continu.

2. Le Règlement général sur la protection des données (RGPD)

Le RGPD est un texte législatif de l'Union européenne (UE) qui vise à renforcer et à unifier la protection des données pour les individus au sein de l'UE. Cependant, le RGPD ne se limite pas aux organisations basées dans l'UE ; toute entreprise offrant des biens de consommation ou des services dans l'UE doit s'y conformer.

Le règlement stipule que les données personnelles sont des informations qui peuvent être reliées ou connectées à un individu. Les données régies par le RGPD peuvent inclure le nom d'une personne, ses coordonnées, ses données bancaires et financières et ses informations médicales. D'un point de vue plus technique, les données couvertes comprennent également les données de géolocalisation telles que les adresses IP et les cookies.

Qu'est-ce que cela signifie pour la sécurité des API ? Que vous développiez des applications, des microservices ou des terminaux de l'Internet des objets (IoT), les API qui vivent au cœur de ces technologies échangent probablement des données réglementées par le RGPD. Par conséquent, les organisations qui développent des API accessibles sur Internet doivent intégrer la protection des données dans la conception des API dès le début, et non après coup.

Prenons le principe du moindre privilège, qui consiste à s'assurer que les utilisateurs ne disposent que des autorisations minimales nécessaires à l'accomplissement de leur travail.

L'article 25 du RGPD est *fondé* sur le principe du moindre privilège, exigeant des entreprises qu'elles mettent en œuvre « des mesures techniques et organisationnelles pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires pour chaque finalité spécifique [...] sont traitées ». De leur côté, les développeurs d'API doivent mettre en œuvre des contrôles d'authentification et d'autorisation des utilisateurs afin de protéger les données sensibles qui transitent par leurs API. Les équipes de développement d'API doivent également veiller à ce que les données restent confidentielles en transit en utilisant des protocoles de communication sécurisés pour chiffrer l'échange d'informations entre le client et le serveur.

Mais qu'en est-il de l'écosystème existant d'API que les organisations ont construit au cours des dernières années, voire des dernières décennies ? Une grande partie des API d'entreprise ne sont pas gérées, sont oubliées ou fonctionnent perpétuellement sans contrôle. Dans ces cas, la conformité au RGPD exige les actions suivantes :

- Découvrir toutes les API dans votre environnement informatique
- Évaluer leurs facteurs de risque (par exemple, les types de données qu'elles ont échangées et qui ou quoi peut accéder à ces données)
- Corriger les vulnérabilités telles que les erreurs de configuration ou les mécanismes d'authentification faibles
- Tester en continu la résilience des API face aux méthodes d'attaque et de violation traditionnelles et émergentes

3. Le Règlement sur la résilience opérationnelle digitale (DORA)

Compte tenu du rôle du secteur financier de l'UE en tant qu'opérateur d'infrastructures critiques, les exigences du règlement DORA visent à aider les organisations des États membres de l'UE à résister aux cyberattaques et à s'en remettre. Avec DORA, le secteur disposera d'un cadre contraignant et complet de gestion des risques pour les technologies de l'information et de la communication (TIC). La loi vise à harmoniser et à renforcer les exigences pour les entreprises financières de l'UE, car le paysage actuel comporte une myriade de réglementations et de normes.

Au total, plus de 22 000 institutions financières et fournisseurs de services informatiques de l'UE sont concernés par le règlement DORA. Il convient de noter que cela inclut les tiers qui fournissent aux entreprises financières de l'UE des systèmes et des services TIC, y compris les fournisseurs de services cloud. La loi demande aux institutions financières d'élaborer des stratégies de gestion des risques liés aux TIC pour les tiers et de procéder à des vérifications préalables pour s'assurer de l'adéquation des fournisseurs.

Le règlement DORA définit plusieurs exigences ayant une incidence sur la sécurité de l'API, notamment la stabilité opérationnelle digitale, qui exige des organisations qu'elles mettent en œuvre des programmes de test réguliers permettant d'identifier les lacunes, les vulnérabilités et/ou les déficiences potentielles en matière de stabilité opérationnelle digitale. Pensez aux tests de sécurité du réseau, aux tests de pénétration, aux tests d'applications Web, etc. Il est important de procéder à des examens obligatoires fondés sur des tests de pénétration basés sur les menaces (TLPT), en fonction de la taille, du risque et du profil commercial de l'entreprise financière. Il est tout aussi important de tester régulièrement les vulnérabilités de vos API.

Le règlement DORA donne des exemples de tests de sécurité qui comprennent des tests d'applications et d'API basées sur le Web. Il s'agit notamment d'utiliser des ressources publiques telles que l'Open Worldwide Application Security Project (OWASP). La liste des 10 principaux risques pour la sécurité des API de l'OWASP, en particulier, aide les organisations à identifier les erreurs de configuration, les faiblesses, les failles logiques et les problèmes de code qui permettent aux attaquants d'accéder aux ressources de l'organisation, de les manipuler ou de les contrôler d'une manière ou d'une autre.

4. La Loi HIPAA (Health Insurance and Portability and Accountability Act)

La loi HIPAA se concentre sur les règles de confidentialité et de sécurité des données afin de sauvegarder les informations protégées de santé (IPS) dans les dossiers de santé électroniques (DSE), les plateformes de saisie informatisée des ordonnances médicales et d'autres systèmes informatiques de soins de santé. Tout prestataire de soins de santé, administrateur de régime ou centre d'échange américain qui stocke ou transmet électroniquement des IPS doit se conformer à la loi HIPAA. Il s'agit de garantir la confidentialité, l'intégrité et la disponibilité des IPS et de les protéger contre la divulgation non autorisée et l'utilisation inappropriée.

L'HIPAA est un exemple de réglementation qui a des implications significatives pour les API, même si elle ne mentionne pas explicitement les API dans ses exigences.

Prenons l'exemple d'un fournisseur de technologie qui crée des portails patients pour des cliniques de soins de santé fonctionnant 24 h/24, 7 j/7. L'une des fonctions sous-jacentes de ces portails est la capacité de donner aux patients un accès efficace et sécurisé aux données relatives à leurs visites chez le médecin, aux résultats des tests, aux paiements, etc. Les API facilitent cet échange. La clinique et le fournisseur sont tous deux tenus de respecter les exigences de la loi HIPAA.

La règle de confidentialité de l'HIPAA précise que les entités concernées « doivent développer et mettre en œuvre des politiques et des procédures qui limitent l'accès et l'utilisation des informations de santé protégées en fonction des rôles spécifiques des membres de leur personnel ». Par conséquent, les développeurs d'API d'une organisation doivent intégrer des mesures de protection techniques telles que l'authentification, des identifiants d'utilisateur uniques et des contrôles d'accès basés sur les rôles afin de garantir la mise en place d'un moindre privilège.

La visibilité est également essentielle pour les organisations couvertes par la HIPAA, qu'il s'agisse d'un fournisseur dont l'équipe informatique crée des API sur mesure ou d'un fournisseur qui développe des API pour le fournisseur. Les organisations ont besoin d'une évaluation et d'un rapport en temps réel sur la position de risque de chaque API, y compris les types d'IPS qu'elles transmettent. C'est un élément essentiel pour la conformité et pour satisfaire l'exigence de l'HIPAA impliquant de répondre aux personnes qui demandent des informations sur quand, où, pourquoi et à qui leurs IPS ont été divulguées.

5. Directive sur la sécurité des réseaux et des systèmes d'information (NIS2)

L'UE a adopté la version 2.0 de la directive NIS en janvier 2023, qui s'appuie sur les directives de la version originale pour sécuriser l'infrastructure informatique et signaler les incidents. Bien que la version 2.0 ne mentionne pas spécifiquement les API, ses exigences ont des implications significatives pour la protection et la gestion des API, car elles font partie intégrante du fonctionnement de nombreux services numériques dans les organisations soumises à la directive. Il convient de noter que la directive NIS2 inclut :

- Un éventail plus large de secteurs - par exemple, les fournisseurs de services cloud et les entreprises de médias sociaux rejoignent la liste existante, qui comprend les opérateurs d'infrastructures critiques. Pour ces secteurs, où les API sont largement utilisées pour l'intégration et la fourniture de services, assurer la sécurité des API devient une priorité.
- Une nouvelle importance accordée à la sécurisation des chaînes d'approvisionnement - les entreprises doivent évaluer les risques et sécuriser leurs chaînes d'approvisionnement informatiques et les relations avec les fournisseurs tiers. Les API étant souvent utilisées pour intégrer des services externes, il est essentiel de garantir leur sécurité pour assurer la conformité.
- L'obligation de mettre en place un système de gestion de la sécurité de l'information qui évalue les personnes, les politiques et la technologie afin de protéger les ressources sensibles et de garantir la résilience opérationnelle. Les API étant des vecteurs d'attaque à croissance rapide, elles doivent être incluses dans les stratégies de gestion des risques.
- Le signalement des incidents importants en matière de cybersécurité, y compris les violations d'API. Les organisations doivent donc mettre en place des mécanismes pour surveiller, détecter et signaler les incidents liés aux API.

6. Orientations pour les régulateurs américains des services financiers

Le conseil Federal Financial Institutions Examination Council (FFIEC) élabore des recommandations et des normes à l'intention des régulateurs fédéraux chargés de superviser le secteur financier américain. Il s'agit notamment de la Réserve fédérale, de la FDIC, de l'OCC et de la NCUA. La mission du conseil est de protéger les utilisateurs et les investisseurs contre les fraudes, les abus et les fautes professionnelles. Bien qu'il ne s'agisse pas d'une réglementation, les orientations du FFIEC sont essentielles pour que les entreprises financières sachent comment s'aligner sur les mesures de sécurité qu'elle recommande.

Il s'agit d'un exemple clé d'un document qui comprend des conseils spécifiques sur la façon de sécuriser les API et, par conséquent, de protéger les consommateurs contre la fraude et l'usurpation d'identité. Voici un aperçu :

- **Inventaire :** le FFIEC recommande de dresser un inventaire de tous les systèmes d'information, y compris les API, qui nécessitent une authentification et des contrôles d'accès. Cela s'applique non seulement aux institutions financières, mais aussi à leurs tiers, tels que les fournisseurs de services cloud.
- **Authentification :** l'API ne doit permettre l'accès qu'aux utilisateurs autorisés. Il est essentiel d'identifier tous les utilisateurs (par exemple, les clients) pour lesquels des contrôles d'accès sont nécessaires. Il est également important d'identifier les utilisateurs qui justifient des contrôles renforcés, tels que l'authentification multifactorielle.
- **Autorisation :** l'API ne doit permettre l'accès à des ressources spécifiques qu'aux utilisateurs autorisés. Cela dit, le FFIEC recommande de mettre en place une sécurité à plusieurs niveaux (par exemple, des activités de surveillance, de journalisation et de reporting afin d'identifier et de suivre les accès non autorisés).
- **Gestion des risques :** le FFIEC identifie un certain nombre de pratiques efficaces de gestion des risques dans ses dernières orientations. Cependant, il mentionne explicitement les API dans la catégorie Inventaire des systèmes d'information, ce qui signifie que vous devez disposer d'un inventaire précis de vos API.

Une organisation peut être au fait des menaces bien connues telles que l'hameçonnage ou les ransomwares, mais le FFIEC demande d'identifier *toute* cybermenace ayant une « probabilité raisonnable d'avoir un impact sur les systèmes d'information des institutions financières » et sur leurs données. Comme indiqué dans l'introduction, 78 % des organisations ont été confrontées à des incidents liés à la sécurité des API. Vous pouvez donc vous attendre à ce que la protection des API devienne un impératif de conformité à mesure que les exigences des régulateurs financiers continuent d'évoluer.

Relever les défis de la conformité grâce aux meilleures pratiques de protection des API

Le paysage actuel des menaces exige une solution complète de sécurité des API qui assure la découverte des API, la gestion de la posture, la protection de la durée d'exécution et les tests de sécurité des API. Cette approche globale fonctionne en complément de tout WAF ou toute passerelle d'API déjà en place.

1. Découverte des API

Il n'est pas rare d'avoir des API dont personne ne connaît l'existence. La plupart des organisations n'ont que peu ou pas de visibilité sur un pourcentage important de leur trafic API, souvent parce qu'elles supposent que toutes leurs API sont acheminées via une passerelle d'API. Mais ce n'est pas le cas. Sans un inventaire complet et précis, votre entreprise est exposée à toute une série de risques. Capacités de base nécessaires :

- Localiser et inventorier toutes vos API, indépendamment de leur configuration ou leur type
- Détecter les API inactives, héritées et zombies
- Identifier les domaines fantômes oubliés, négligés ou autrement inconnus
- Éliminer les angles morts et déceler les voies d'attaque potentielles

2. Gestion de la posture des API

Avec un inventaire complet des API en place, il est essentiel de comprendre quels types de données circulent à travers vos API et comment cela affecte votre capacité à vous conformer aux exigences réglementaires. La gestion de la posture des API fournit une vue complète du trafic, du code et des configurations pour évaluer la posture de sécurité des API de votre organisation. Capacités de base nécessaires :

- Analyser automatiquement l'infrastructure et découvrir les erreurs de configuration ainsi que les risques cachés
- Créer des workflows personnalisés pour informer les principales parties prenantes des vulnérabilités
- Identifier les API et les utilisateurs internes capables d'accéder aux données sensibles
- Attribuer des niveaux de gravité aux problèmes détectés afin de hiérarchiser les mesures correctives

3. Sécurité de la durée d'exécution des API

Vous êtes sans doute familier avec le concept de présomption de violation. Les violations et les attaques propres aux API atteignent le même degré d'inévitabilité. Pour toutes vos API en production, vous devez être en mesure de détecter et de bloquer les attaques en temps réel. Capacités de base nécessaires :

- Surveiller la falsification et la fuite de données, les violations de règles, les comportements suspects et les attaques d'API
- Analyser le trafic API sans modifications supplémentaires du réseau ni agents difficiles à installer
- Intégrer les flux de travail existants (système de tickets, SIEM, etc.) pour alerter les équipes chargées de la sécurité/des opérations
- Prévenir les attaques et les abus en temps réel grâce à une correction partielle ou entièrement automatisée

4. Test de sécurité des API

Les équipes de développement d'API sont contraintes de travailler aussi vite que possible. La rapidité est essentielle pour chaque application développée, ce qui facilite l'apparition d'une vulnérabilité ou d'un défaut de conception qui peut ensuite passer inaperçu. Tester les API en cours de développement avant qu'elles ne soient mises en production réduit considérablement les risques et le coût de la correction d'une API vulnérable. Capacités de base nécessaires :

- Exécuter une large gamme de tests automatisés qui simulent le trafic malveillant
- Découvrir les vulnérabilités avant que les API n'entrent en production afin de réduire le risque de réussite des attaques
- Inspecter les spécifications de vos API par rapport aux politiques et règles de gouvernance établies
- Exécuter des tests de sécurité axés sur les API à la demande ou dans le cadre d'un pipeline CI/CD

Comment Akamai API Security peut rationaliser les complexités liées à la conformité des API

Les API sont l'une des principales causes des violations que les réglementations actuelles sont censées prévenir. Que faut-il pour sécuriser votre entreprise face à la multiplication des API (et des risques qui y sont liés) ? Les outils existants que de nombreuses organisations utilisent pour la protection de base des API offrent une certaine protection, mais c'est loin d'être suffisant. Si vous cherchez un meilleur moyen de sécuriser les API de votre organisation et de démontrer votre capacité à respecter les réglementations, nous aimerions vous aider.

Pour chaque exigence et conseil couverts dans ce livre blanc, Akamai API Security renforce la protection dont les entreprises ont besoin, non seulement pour se conformer aux réglementations, mais aussi pour sécuriser les données et la confiance de vos clients.

La solution complète d'Akamai protège les API dès les premières étapes de leur développement et jusqu'à la post-production, ce qui vous permet d'adhérer aux meilleures pratiques fondamentales :

- Découverte des API
- Gestion de la posture
- Protection de la durée d'exécution
- Tests de sécurité

En savoir plus sur les API et sur la manière de les protéger contre les attaques.

Découvrez comment Akamai API Security peut aider votre organisation.

Akamai Security 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, rendez-vous sur akamai.com et akamai.com/blog ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 09/24.