Akamai

WHITE PAPER

Como evitar uma violação de API

Cinco tipos de violações de API e como se proteger contra elas

Neste relatório

Introdução

As APIs conectam sua empresa pela troca de dados com parceiros, fornecedores e clientes. E mesmo assim, a segurança de APIs continua sendo pouco abrangente na maioria das empresas. De fato, as APIs vulneráveis se tornaram um ponto fraco das empresas nos últimos anos, com os invasores abusando dessas APIs para acessar dados confidenciais, vender esses dados a outros agentes de ameaças ou publicá-los para que o mundo os veja. Em 2024, marcas globais de telecomunicações para consumidores, computação corporativa e colaboração virtual viram violações de API liberarem grandes quantidades de dados dos clientes e de outros dados confidenciais, causando altos custos financeiros e na reputação.

O que é uma violação de API?

Em resumo, uma violação de API é qualquer uso indevido ou mau uso intencional de uma API, geralmente para obter acesso a dados confidenciais. Os tipos de violações de API podem ser subdivididos por vários critérios. Para identificar riscos e evitar violações nas operações de produção, é útil considerar o esquema a seguir, que divide os riscos em cinco categorias:

1. **Vulnerabilidades conhecidas**
   - Os invasores exploram vulnerabilidades conhecidas que não foram corrigidas.
2. **APIs sombras, não autorizadas, zumbis e obsoletas**
   - APIs não gerenciadas e esquecidas deixam as operações vulneráveis.
3. **Exposições externas**
   - Credenciais, chaves e outras exposições podem existir fora do seu controle.
4. **Configurações incorretas e erros do operador**
   - As configurações incorretas de segurança na infraestrutura e nos serviços criam pontos de entrada para exploração por agentes de ameaças.
5. **Vulnerabilidades e bugs desconhecidos**
   - Os agentes de ameaças procuram identificar bugs e vulnerabilidades que entraram no ambiente de produção apesar dos seus melhores esforços.

Este e-book explica onde ocorrem as falhas de segurança em cada um desses cinco tipos de violações de API e como evitá-las. Este e-book também tem como objetivo ajudar a identificar pontos fracos específicos no programa de segurança de APIs para maximizar a segurança de APIs e minimizar os riscos.

Tipo de violação: vulnerabilidades conhecidas

As violações de API que tiram proveito de vulnerabilidades conhecidas (que não foram corrigidas) talvez sejam as mais comuns. Se os cibercriminosos quiserem obter seus dados, uma primeira etapa comum é verificar se sua organização deixou alguma vulnerabilidade.

Em janeiro de 2024, um invasor comprometeu uma ferramenta de gerenciamento de projetos bastante utilizada ao explorar um ponto de extremidade de API sem controles de autenticação. Depois de violar a API, o agente da ameaça obteve acesso não autorizado a informações sobre milhões de usuários e, meses depois, vazou na Internet mais de 21 GB de dados, incluindo endereços de e-mail e membros da diretoria.

Os problemas de autenticação e autorização estão entre os problemas mais comuns de API. O relatório OWASP Top 10 API Security Risks fornece informações sobre as 10 vulnerabilidades de API mais críticas contra as quais as organizações devem se proteger, incluindo a autenticação corrompida.

Além de proteger as APIs contra os tipos de risco incluídos no OWASP Top 10, as organizações devem proteger o código da API contra a lista completa de CVEs (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) criada pelo FFRDC (Federally Funded Research and Development Center, centro de pesquisa e desenvolvimento financiado pelo governo federal) de cibersegurança dos EUA, operado pelo MITRE. Talvez você se lembre da vulnerabilidade bem divulgada do Apache Log4j 2 (CVE-2021-44228), também conhecida como “Log4Shell”. Devido a um bug na biblioteca Log4j, uma popular biblioteca de registro de código aberto para a linguagem de programação Java, os invasores conseguiram executar remotamente códigos arbitrários para obter acesso ao sistema. Agentes mal-intencionados sondam regularmente os sistemas empresariais em busca de vulnerabilidades conhecidas como essa.

Nos Estados Unidos, a CISA (Cybersecurity and Infrastructure Security Agency, agência de cibersegurança e segurança de infraestrutura) mantém um catálogo de CVEs conhecidas. Provavelmente, outros países mantenham catálogos semelhantes.

O relatório OWASP Top 10 API Security Risks foi criado em 2019 e atualizado em 2023. Embora útil, ele não consegue acompanhar a velocidade das mudanças na superfície de ataque. Somente em 2024, mais de 24.000 novas CVEs foram adicionadas ao catálogo da CISA, das quais mais de 500 estão relacionadas a APIs (em meados de agosto de 2024).

Proteger totalmente sua organização contra vulnerabilidades conhecidas exige um esforço duplo:

1. Garantir que os processos de desenvolvimento e testes sejam robustos o bastante para evitar a introdução de vulnerabilidades conhecidas na produção.

2. Corrigir novas vulnerabilidades o mais rápido possível depois que elas forem identificadas.

Muitas organizações têm dificuldades com essas duas etapas. Além disso, elas usam APIs e códigos de fontes de terceiros que podem introduzir um conjunto separado de vulnerabilidades. Em 2022, uma equipe de pesquisadores descobriu falhas críticas em APIs que afetaram vários fabricantes do setor automotivo. Essas falhas poderiam ter exposto dados confidenciais de clientes e até mesmo a localização de um veículo, permitindo que um carro fosse destravado, ligado ou desativado por um sistema de gerenciamento remoto comprometido.

Como evitá-las

Uma maneira bem conhecida de proteger sua organização contra violações de API devido a vulnerabilidades conhecidas é atualizar rapidamente o software e os sistemas quando forem lançados patches de segurança. Também é essencial garantir que os processos de desenvolvimento e testes sejam abrangentes e estejam fundamentados nas práticas recomendadas de segurança de APIs. Isso inclui:

- **Proteger sua cadeia de suprimentos de software:** garanta que todas as bibliotecas, softwares de código aberto (OSSs) e outros códigos de terceiros que você usa estejam seguros.
- **Implementar o teste de segurança "shift-left":** mova as tarefas relacionadas à segurança de APIs e aos testes de software para o início do processo de desenvolvimento. Isso pode ajudar a descobrir vulnerabilidades, como erros de codificação e configurações incorretas feitas por equipes de desenvolvedores sob pressão para lançar rapidamente softwares ou atualizações.
- **Utilizar o gerenciamento da postura de segurança de APIs:** isso combina a descoberta de APIs com a identificação de dados confidenciais e a detecção de vulnerabilidades, garantindo que os esforços de correção se concentrem primeiro nas APIs mais críticas.

Como o API Security da Akamai pode ajudar

O API Security da Akamai permite que suas equipes reduzam as vulnerabilidades conhecidas a cada nova compilação, sem prejudicar a velocidade. O API Security é uma solução de teste de segurança de APIs desenvolvida para fins específicos que oferece cobertura completa de vulnerabilidades específicas de APIs. O teste ativo ajuda a incorporar o teste de segurança de APIs em todas as fases do desenvolvimento.

- **Encontre e teste cada API** com base em um entendimento da lógica comercial do aplicativo.
- **Use a abordagem "shift left"** com integrações em todo o ciclo de vida de desenvolvimento de software. As equipes obtêm visibilidade dinâmica de APIs em vários estados e ambientes durante todo o processo de CI/CD.
- **Capacite os desenvolvedores** com a melhor usabilidade da categoria, incluindo configuração e automação simples, resultados de testes em linha e orientação contextual para corrigir problemas identificados.

Além disso, o gerenciamento da postura do API Security oferece uma visão completa do tráfego, do código e das configurações para avaliar a postura da segurança de APIs. O API Security analisa o conjunto mais amplo possível de origens para detectar vulnerabilidades, incluindo arquivos de registro, repetições de tráfego histórico, arquivos de configuração e muito mais. Ele também detecta todas as vulnerabilidades apresentadas no relatório OWASP Top 10 API Security Risks (para saber mais sobre gerenciamento da postura, consulte a seção "Configurações incorretas e erros do operador").

Tipo de violação: APIs sombras, não autorizadas, zumbis e obsoletas

Não é possível proteger o que não se pode ver, e muitas empresas têm uma grande porcentagem de APIs não gerenciadas, o que faz com que as APIs sombras, não autorizadas, zumbis e obsoletas (consulte a barra lateral na próxima página) sejam alvos invisíveis ou não contabilizados no patrimônio de APIs. Além disso, os invasores geralmente procuram variações nas APIs que possam explorar, examinando as APIs expostas de uma organização e fazendo fuzzing ou modificando os valores para encontrar versões antigas.

Foi o que aconteceu com uma grande empresa de telecomunicações australiana que expôs acidentalmente mais de 11,2 milhões de registros dos clientes, incluindo nomes, endereços, datas de nascimento e alguns números de identidade emitidos pelo governo. O ataque aproveitou-se de uma API usada para testes que, de alguma forma, tornou-se acessível à Internet aberta. Como essa API não autorizada não tinha verificações de autenticação, um invasor podia solicitar e receber milhões de registros.

A maioria das organizações opera usando uma variedade de APIs novas e herdadas. Infelizmente, é muito comum encontrar, ao lado delas, APIs não autorizadas, zumbis e sombras que expõem a empresa a uma série de riscos de cibersegurança e dificuldades operacionais.

Essas APIs invisíveis têm uma variedade de origens:

- **APIs comerciais:** alguns pacotes de software comercial incluem APIs para se conectar com outros aplicativos e fontes de dados externas. Eles podem ser ativados sem que ninguém perceba (um problema que pode ser resolvido com a descoberta completa da API).
- **Versões antigas de APIs:** em muitos casos, pode acontecer de uma versão mais antiga de uma API, possivelmente com segurança mais fraca ou uma vulnerabilidade conhecida, nunca ser removida. Uma versão antiga pode precisar coexistir com uma nova versão por algum tempo enquanto o software é atualizado, mas quando as falhas do processo impedem que a API antiga seja encerrada, ela se transforma em uma API zumbi.
- **Atalhos e falhas de processo:** as APIs sombras resultam da falha em informar as pessoas certas. Por exemplo, uma equipe de linha de negócios pode criar APIs para atender a necessidades específicas sem informar as equipes de TI ou de segurança, ou um desenvolvedor pode não seguir o procedimento.
- **APIs herdadas:** as APIs herdadas como parte de fusões ou aquisições também são frequentemente ignoradas e se tornam APIs sombras.
- **Código reativado:** em alguns casos, versões antigas de APIs podem ser reativadas acidentalmente.

Como evitá-las

Uma auditoria manual de API para documentar todos os registros que devem ser inventariados com precisão pode levar várias horas, especialmente considerando o tempo necessário para avaliar e agir em cada API encontrada. Essa não é uma tarefa realista para equipes de segurança já sobrecarregadas. Para proteger a sua empresa contra explorações de APIs não autorizadas, zumbis e sombras, você precisa de uma descoberta de API automatizada capaz de identificar todas as APIs em uso, de todos os tipos. É essencial localizar e inventariar todas as APIs em suas operações e descobrir APIs e domínios de APIs que não são gerenciados por um gateway de APIs.

Como o API Security da Akamai pode ajudar

O API Security utiliza uma vasta coleção de origens de integração para ingerir dados de APIs, como tráfego bruto, registro em log e muito mais. Os dados derivados dessas origens permitem que o API Security identifique APIs, suas configurações incorretas, vulnerabilidades e mau uso de APIs. Nossas ferramentas de descoberta detectam todas as vulnerabilidades do relatório OWASP Top 10 API Security Risks.

Recursos adicionais para descoberta permitem:

- Localizar e fazer o inventário de todas as suas APIs, independentemente da configuração ou do tipo, incluindo RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC
- Descobrir APIs inativas, legadas e zumbis
- Identificar domínios esquecidos, negligenciados ou de sombra desconhecidos
- Manter inventários de API e garantir a precisão da documentação de API

APIs não gerenciadas de alto risco que os invasores procuram

As APIs sombras (também conhecidas como “APIs não documentadas”) existem e operam fora dos canais oficiais monitorados de uma organização. Elas podem ser criadas por desenvolvedores bem-intencionados para acelerar o trabalho, ou podem ser um resquício de versões anteriores do software.

As APIs não autorizadas ou mal-intencionadas representam um risco de segurança para um sistema ou rede.

As APIs zumbis incluem qualquer API que permaneça em execução mesmo depois de ser substituída por novas versões ou por outras APIs.

APIs obsoletas são APIs que não são mais recomendadas para uso devido a alterações nas APIs. Embora as classes, os métodos e os campos obsoletos ainda estejam implementados, eles podem ser removidos em implementações futuras, portanto, não os use em novos códigos.

Tipo de violação: exposições externas

As vulnerabilidades de APIs externas geralmente resultam de práticas inadequadas ou erros de procedimento, como vazamento de chaves e credenciais de API, exposição de códigos e esquemas de API, documentação perdida e vulnerabilidades de repositório. A capacidade de descobrir possíveis vetores de ataque fora dos limites de suas operações tornou-se imperativa. No ano passado, várias violações de alto perfil resultaram da exposição acidental de chaves de APIs ou outras credenciais de origens externas. Por exemplo, os hackers usaram uma campanha de phishing para obter acesso não autorizado a 130 dos repositórios de código-fonte do Dropbox. Isso permitiu que eles acessassem chaves de APIs armazenadas inadequadamente no GitHub. Esse tipo de exposição se tornou tão comum que o GitHub tomou medidas para impedir que ocorressem vazamentos de chaves de APIs e outros segredos, mas outros repositórios públicos ainda podem estar vulneráveis.

Em outro exemplo bem divulgado de exposição externa, os pesquisadores descobriram mais de 3.000 aplicativos móveis que expuseram as chaves de APIs do Twitter ao público. Esse tipo de erro é surpreendentemente comum porque os desenvolvedores geralmente incorporam chaves de APIs no código do aplicativo durante o desenvolvimento por conveniência. Se eles não conseguirem remover essas chaves incorporadas antes de um lançamento público, isso se tornará uma possível origem de exposição de chaves.

Como evitá-las

Reduzir ou eliminar esses tipos de exposições externas requer um ataque em duas frentes:

- Reforçar os procedimentos para identificar e eliminar fontes de exposição, como chaves e credenciais vazadas, uso inadequado de repositórios, entre outras.
- Examinar regularmente a superfície de ataque externa para detectar e corrigir vulnerabilidades.

Para se proteger contra a maior variedade de ameaças às APIs, você precisa tanto da descoberta de dentro para fora (conforme descrito na seção "Violações de APIs não autorizadas") quanto da descoberta de fora para dentro, que pode identificar exposições e reduzir sua superfície de ataque externa.

Como o API Security da Akamai pode ajudar

O API Security ajuda você a ficar à frente dos invasores, simulando as técnicas de reconhecimento que os hackers usam e permitindo que você encontre e corrija problemas rapidamente. Com a descoberta de fora para dentro, o API Security examina automaticamente sua superfície de ataque externa em intervalos regulares para encontrar vulnerabilidades antes que os invasores o façam, o que permite a você:

- **Encontrar vulnerabilidades públicas:** encontre e corrija rapidamente problemas essenciais, como vazamento de chaves de APIs e credenciais, exposição de código, configurações incorretas, vulnerabilidades de repositório e muito mais.
- **Descobrir domínios e subdomínios relacionados à sua empresa:** utilize dados coletados de várias origens, incluindo registradores de Internet, registradores de certificados e códigos abertos.
- **Incorporar métodos de ataque reais:** simule um invasor realizando reconhecimento externo para coletar informações, executando consultas limitadas aos domínios ou subdomínios da empresa.

Tipo de violação: configurações incorretas e erros do operador

Muitos cibercriminosos conseguem entrar ao explorar a configuração incorreta dos servidores, redes, gateways de APIs e firewalls que intermedeiam e protegem o tráfego de APIs. Um estudo da IBM Security X-Force descobriu que dois terços das violações na nuvem estão vinculadas a APIs configuradas incorretamente. As configurações incorretas de segurança podem ser causadas por configurações padrão inseguras, armazenamento na nuvem sem controle de acesso (surpreendentemente comum) e configurações incompletas ou ad hoc. À medida que sua pegada digital se expande, suas operações podem se expandir para mais locais, incluindo várias zonas de disponibilidade de nuvem pública ou nuvens públicas, como AWS, Microsoft Azure e Google Cloud. Esses ambientes geralmente operam sob diferentes controles de segurança, o que torna complexo e difícil garantir que a segurança seja configurada corretamente em todos os lugares.

Como evitá-las

Uma das melhores maneiras de se proteger contra configurações incorretas de segurança no lado da infraestrutura é evitar ao máximo a configuração manual de servidores, dispositivos de rede, gateways e firewalls. Se as equipes de administradores da sua empresa configuram regularmente os controles de segurança da infraestrutura e dos aplicativos de forma manual, ou os "ajustam" regularmente, a chance de introduzir vulnerabilidades de configuração aumenta.

A automação é sua melhor amiga quando se trata de segurança. Algumas empresas estão adotando a ideia de infraestrutura imutável como uma forma de evitar erros manuais.

Mesmo que você tenha feito tudo o que pode para garantir que a infraestrutura, os serviços e as APIs sejam à prova de falhas, você ainda precisa do gerenciamento da postura de APIs. O gerenciamento da postura oferece as ferramentas para gerenciar, monitorar e manter a segurança de APIs durante todo o ciclo de vida da API.

Como é a ajuda do API Security

O módulo de gerenciamento da postura do API Security analisa as chamadas de APIs e a infraestrutura para identificar configurações incorretas. Essas configurações incorretas geralmente são problemas de bucket do Amazon S3, dados confidenciais em APIs não autenticadas e diferentes configurações incorretas baseadas em acesso ao Kubernetes.

O módulo de gerenciamento da postura fornece uma visão abrangente do tráfego, do código e das configurações, oferecendo uma visão de toda a superfície de ataque nas APIs e nos aplicativos da Web, incluindo todas as formas de dados confidenciais que transitam pelas APIs, como informações de identificação pessoal. Também ajuda a confirmar que a ferramenta de gerenciamento de APIs está usando protocolos e cifras fortes para evitar criptografia fraca que poderia expor esses dados confidenciais. Além disso, as APIs não devem aceitar tokens da Web JSON expirados, pois isso permitiria o acesso não autorizado e aumentaria os riscos de segurança. O módulo também ajuda a evitar configurações incorretas, como balanceadores de carga de aplicativos que escutam em portas inseguras sem redirecionamento. Todas essas medidas fortalecem coletivamente a postura de segurança de APIs, garantindo uma defesa mais resiliente contra possíveis ameaças.

Tipo de violação: vulnerabilidades desconhecidas

Como acontece com a maioria dos tipos de violação, os cibercriminosos que examinam a sua infraestrutura procuram regularmente por CVEs, o OWASP Top 10 em segurança de API e outras configurações incorretas comuns, além de APIs não autorizadas, zumbis e sombras. Eles também sondam as APIs expostas em busca de novas vulnerabilidades que possam ser exploradas em bibliotecas, código-fonte aberto e outros tipos de código público, bem como em erros de codificação, bugs e configurações incorretas no patrimônio de APIs. Essas vulnerabilidades permitem que os cibercriminosos manipulem as chamadas de APIs e insiram cadeias de fuzzing nas solicitações. Como resultado, as técnicas usadas pelos cibercriminosos estão em constante evolução.

Como evitá-las

Uma parte importante da prevenção é garantir que o seu código esteja o mais livre possível de bugs e vulnerabilidades (consulte a seção "Vulnerabilidades conhecidas"). No entanto, ainda se deve presumir que os agentes de ameaças encontrarão bugs ou obterão acesso a chaves ou credenciais que lhes permitam explorar as APIs.

A proteção de tempo de execução de APIs foi projetada para identificar qualquer vulnerabilidade, conhecida ou desconhecida, sendo explorada por hackers. É a única maneira de proteger seu patrimônio de API contra bugs não identificados anteriormente e configurações incorretas que entram na produção, além de ser a melhor proteção contra credenciais e chaves que foram comprometidas.

A proteção de tempo de execução identifica padrões incomuns e anomalias no uso da API e no acesso aos dados para que ataques contínuos que podem escorregar sob o radar possam ser identificados e remediados antes que milhares ou milhões de registros de dados sejam extraídos.

A proteção de tempo de execução de API ajuda a identificar e bloquear solicitações de API mal-intencionadas, incluindo:

- Ataques que extraem grandes volumes de dados confidenciais de uma API
- Ataques BOLA (Broken Object Level Authorization, autorização em nível de objeto corrompida)

Uma solução de proteção de tempo de execução de APIs pode detectar:

- Vazamento de dados
- Violações da política de dados
- Ataques de segurança de APIs
- Adulteração de dados
- Comportamento suspeito

Além disso, a proteção de tempo de execução registra o tráfego de APIs, monitora o acesso a dados confidenciais, detecta ameaças e bloqueia ou corrige vetores de ataque.

Como é a ajuda do API Security

Pense na proteção de tempo de execução como sua última linha de defesa quando outras medidas de prevenção não forem suficientes. A principal função da proteção de tempo de execução é detectar e bloquear ataques à APIs em tempo real. O monitoramento autônomo baseado em machine learning (ML) é usado para realizar análises do tráfego em tempo real e fornecer informações contextuais sobre vazamento de dados, adulteração de dados, violações de políticas de dados, comportamento suspeito e ataques à segurança de APIs. O API Security detecta anomalias e possíveis ameaças no tráfego de APIs e facilita a correção com base nas políticas de resposta a incidentes pré-selecionadas.

Com o ML, o API Security cria um modelo de comportamento para cada API. Essa linha de base de comportamento normal é então usada para detectar ataques à lógica comercial da API. Cada problema gerado pela proteção de tempo de execução inclui gravidade, status, um mapeamento para o OWASP API Security Top 10 e detalhes do invasor, quando aplicável. Os problemas também incluem evidências como os detalhes da sessão do invasor e uma cópia da solicitação e da resposta da API para ajudar na triagem e na correção do problema.

A proteção de tempo de execução do API Security oferece detecção e prevenção em tempo real de ataques a APIs com a detecção constante de configurações incorretas de API, além de muitas integrações populares de fluxo de trabalho que simplificam as operações e a correção.

Talvez a melhor notícia para a sua equipe seja que o API Security se integra a WAFs, gateways de APIs, ITSMs, SIEMs e outras ferramentas de fluxo de trabalho para oferecer uma defesa completa contra ataques. Você pode optar por automatizar totalmente a correção de ameaças ou exigir diferentes níveis de intervenção manual para obter maior visibilidade e controle.

Cinco tipos de violações, cinco princípios de prevenção

Agora que você entende melhor como as APIs são usadas pelos cibercriminosos, pode se concentrar em protegê-las. Aqui estão as cinco ferramentas de prevenção e perspectivas estratégicas que devem ser usadas em conjunto:

1. Segurança de APIs "shift-left"

- Segurança de APIs "shift-left" significa testar extensivamente as APIs em desenvolvimento para que você não exponha vulnerabilidades no ambiente de produção onde os cibercriminosos possam encontrá-las.

2. Descoberta de dentro para fora

- Identifique todas as APIs em toda a sua operação.

3. Descoberta de fora para dentro

- Identifique e elimine fontes de exposição, como chaves e credenciais vazadas e uso inadequado de repositórios, e examine regularmente a superfície de ataque externa para detectar e corrigir vulnerabilidades.

4. Gerenciamento abrangente da postura

- Sempre dê o seu melhor quando se trata de segurança de APIs, evitando configurações incorretas e vulnerabilidades

5. Proteção de tempo de execução

- Detecte atividades anômalas de APIs e proteja-se contra todas as ameaças possíveis, incluindo vulnerabilidades e bugs não identificados anteriormente

Solicite uma demonstração

Experimente como é fácil identificar e corrigir configurações incorretas de APIs e se proteger de ataques mal-intencionados às APIs vendo o Akamai API Security em ação. Saiba em primeira mão por que as principais empresas escolhem nossa solução de segurança de APIs.

Obtenha uma demonstração

Akamai

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e LinkedIn. Publicado em 11/24.