Akamai

WHITE PAPER

Fundamentos da segurança de APIs: Desenvolva seu conhecimento, proteja a empresa

Introdução

As APIs evoluíram rapidamente de um detalhe de implementação para um facilitador estratégico da inovação digital. Toda vez que um cliente, parceiro ou fornecedor interage com uma empresa digitalmente, há uma API nos bastidores que facilita uma troca de dados perfeita.

À medida que as APIs se proliferam, o mesmo acontece com os riscos. Na corrida para criar e lançar rapidamente novos aplicativos e serviços aprimorados por IA, as APIs de base muitas vezes são mal configuradas, faltam controles de segurança e ficam vulneráveis a ataques fáceis de executar.

Como resultado, as APIs se tornaram um dos principais vetores de ataque, o que fez com que muitas equipes de segurança tivessem que se preocupar com suas estratégias de segurança de APIs. Portanto, a segurança de APIs está emergindo rapidamente como uma das principais prioridades estratégicas para os executivos de TI e segurança.

Quer você esteja procurando se basear nos conceitos básicos de segurança de API ou (esteja) montando uma lista das perguntas certas a serem feitas, este guia oferece os detalhes que você precisa saber, como:

- **Os diferentes tipos de APIs**
- **O que a segurança de APIs significa para as empresas hoje**
- **Práticas recomendadas para lidar com os riscos de segurança de APIs**
- **Métodos de ataque e violação comuns de APIs**

Para acessar diretamente as práticas recomendadas de segurança de APIs, você pode pular para a página 10.

Índice

Noções básicas sobre APIs

O que é uma API da Web?

Uma interface de programação de aplicativos da Web, ou API, consiste em um ou mais pontos de extremidade de um sistema de mensagens de solicitação-resposta definido, normalmente expresso em JSON ou XML, sendo expostos publicamente pela Web, mais comumente por meio de um servidor da Web baseado em HTTP.

Em outras palavras, uma API da Web é o que a maioria das pessoas pensa quando ouve "API". É uma coleção de pontos de extremidade. Os pontos de extremidade consistem em caminhos de recursos, as operações que podem ser realizadas nesses recursos e a definição dos dados de recursos (em JSON, XML, Protobuf ou outro formato).

As APIs da Web são diferentes de outras APIs, como as expostas pelo sistema operacional ou por bibliotecas de aplicativos executados no mesmo computador, mas o termo geral “API” geralmente se refere a uma API baseada em HTTP (Web), especialmente no contexto da transformação digital empresarial e da segurança de APIs.

Quais são os tipos mais comuns de APIs?

A tabela a seguir contém termos que se referem a diferentes modelos de uso e abordagens técnicas para implementações de APIs. As APIs da Web são definidas como sendo baseadas em HTTP, e os quatro principais tipos de APIs da Web hoje são RESTful, SOAP, GraphQL e gRPC. A tabela define esses tipos comuns, bem como outros.

Modelo de uso de API	Descrição
API pública	Uma API que é disponibilizada e compartilhada livremente com todos os desenvolvedores por meio da Internet
API externa	Frequentemente usado de forma intercambiável com API pública; esses tipos de APIs são expostos à Internet
API privada	Uma API implementada em um data center protegido ou em um ambiente de nuvem para uso por desenvolvedores confiáveis
API interna	Frequentemente usada de forma intercambiável com a API privada
API de terceiros	Fornece acesso programático a funcionalidades e/ou dados especializados de uma fonte de terceiros para uso em um aplicativo
API de parceiros	Um tipo de API de terceiros que é disponibilizada seletivamente a parceiros de negócios autorizados
API autenticada	Uma API que só pode ser acessada por desenvolvedores aos quais foi concedido acesso (ou agentes de ameaças que adquiriram acesso não autorizado a credenciais)
API não autenticada	Uma API que pode ser acessada programaticamente sem a necessidade de credenciais específicas
API HTTP	Uma API que usa o protocolo de transferência de hipertexto como um protocolo de comunicação para chamadas de API

API RESTful	A transferência de estado representacional (RESTful) é o tipo mais comum de API da Web que usa texto simples, HTML, XML, YAML ou JSON para fornecer dados; as APIs RESTful são fáceis de consumir por estruturas de front-end modernas (por exemplo, React e React Native) e facilitam o desenvolvimento de aplicativos móveis e da Web; elas se tornaram o padrão amplamente adotado para qualquer API da Web, inclusive as usadas para B2B (Business-to-business)
GraphQL	As APIs GraphQL são o padrão mais recente, desenvolvido pelo Facebook, que fornece acesso ao banco de dados por meio de um único ponto de extremidade POST (normalmente / graphql); ela resolve um problema comum da API RESTful, que é a necessidade de várias chamadas para preencher uma única página da interface do usuário
SOAP	SOAP usa o XML (eXtensible Markup Language) detalhado para RPCs (chamadas de procedimento remoto). Também pode ser encontrado nas APIs herdadas
XML-RPC	XML-RPC é um método de fazer chamadas de procedimento pela Internet que usa uma combinação de XML para codificação e HTTP como um protocolo de comunicação
gRPC	As APIs gRPC são um protocolo binário de alto desempenho desenvolvido pelo Google sobre HTTP/2.0 e são usadas principalmente para comunicação leste-oeste (na rede interna)
OpenAPI	OpenAPI é uma especificação de descrição e de documentação para APIs. Talvez seja útil saber que o termo Swagger se refere à especificação original, e OpenAPI se refere ao padrão aberto desenvolvido pela OpenAPI Initiative

Qual é a diferença entre APIs e pontos de extremidade?

As pessoas costumam usar “API” quando, na verdade, estão se referindo a um único ponto de extremidade de API. As APIs, às vezes chamadas de serviços ou produtos de APIs, são coleções de pontos de extremidade que atendem a uma função de negócios. Um ponto de extremidade individual, por outro lado, é um recurso (ou caminho de recurso, também conhecido como URI ou identificador uniforme de recurso) juntamente com a operação executada nele (criar, ler, atualizar ou excluir). Nas APIs RESTful, as operações são normalmente mapeadas para os métodos HTTP (POST, GET, PUT e DELETE).

O que é uma API norte-sul?

Essas são APIs que uma organização deixa acessíveis para o mundo externo, principalmente para conduzir negócios com seus parceiros de negócios. Isso é chamado de exposição de APIs. Por exemplo:

> **Os bancos que adotam o serviço bancário aberto podem expor seus dados a outras fintechs ou organizações de serviços financeiros por meio de APIs.**

> **Organizações de saúde podem expor prontuários médicos a seguradoras e outras organizações médicas por meio de APIs.**

> **Organizações de hospedagem podem expor seus sistemas de reservas a agentes de viagens ou agregadores por meio de APIs.**

As APIs são o tecido conjuntivo que permite que organizações diferentes troquem dados. As APIs norte-sul são geralmente consideradas seguras porque o acesso é autorizado e autenticado. Normalmente, essas são as APIs de crescimento mais rápido e de maior volume e, consequentemente, é a maior superfície de ataque na maioria das organizações.

O que é uma API leste-oeste?

Essas são APIs que uma organização usa internamente e não devem estar acessíveis a ninguém fora da empresa. Essas APIs conectam aplicativos internos, unidades de negócios ou departamentos. É possível que um desenvolvedor cometa um erro que torne as APIs leste-oeste acessíveis por acidente. Essas APIs não devem ser acessíveis ou mesmo conhecidas por entidades externas, mas as violações acontecem quando os agentes de ameaças encontram APIs leste-oeste acessíveis pela Internet.

Quais são as diferenças entre APIs B2C (Business-to-consumer) e APIs B2B (Business-to-business)?

As APIs B2C (Business-to-consumer) potencializam os aplicativos da Web e móveis. Elas são normalmente consumidas por clientes front-end modernos para permitir que usuários finais autenticados acessem a funcionalidade de negócios da empresa.

As APIs B2B (Business-to-business) são oferecidas pela organização a outras organizações para realizar negócios e, às vezes, para fornecer valor a clientes conjuntos.

As APIs B2B (Business-to-business) ajudam a simplificar como uma empresa trabalha com seus fornecedores, revendedores e outros parceiros e como ela oferece melhores experiências aos clientes.

Exemplos de APIs B2B (Business-to-business) incluem:

API de serviços bancários abertos

API de gerenciamento de cadeia de fornecimento

Faturamento eletrônico e pagamentos entre parceiros comerciais

Como os consumidores de APIs diferem muito, os controles de segurança disponíveis para proteger as APIs também variam. Até pouco tempo atrás, o setor se concentrava em casos de uso B2C (Business-to-consumer), mas, mesmo assim, o foco não estava na proteção das APIs B2C (Business-to-consumer), e sim na proteção de aplicativos da Web. As ferramentas e os controles de segurança normalmente empregados para proteger os aplicativos da Web B2C (Business-to-consumer) oferecem determinados benefícios (por exemplo, firewall de aplicativo da Web [WAF]/proteção de aplicativos da Web e APIs [WAAP]), mas não podem fornecer o grau de visibilidade, monitoramento em tempo real e proteção necessários para proteger as APIs B2C (Business-to-consumer) contra ataques.

A proteção das APIs B2B (Business-to-business) está se tornando cada vez mais desafiadora. Essas APIs costumam ser alvos mais fáceis para os invasores, pois frequentemente carecem de mecanismos de proteção essenciais. As ferramentas de segurança de APIs anteriores tinham visibilidade limitada das APIs B2B (Business-to-business) e tinham dificuldades para proteger as APIs que facilitavam o acesso a dados em massa em nome de usuários compartilhados (como visto no serviço bancário aberto, em que as empresas de fintech e as instituições financeiras compartilham consensualmente os dados dos clientes). Porém, as soluções mais recentes de segurança de APIs oferecem análise comportamental e podem reconhecer atividades anômalas, abordando efetivamente essas preocupações.

Quais são as diferenças entre as APIs privadas e públicas?

As APIs privadas, às vezes também chamadas de APIs internas, destinam-se ao uso de desenvolvedores e prestadores de serviço da empresa. Muitas vezes, como parte de uma iniciativa de arquitetura orientada a serviços (SOA), as APIs privadas visam simplificar o desenvolvimento interno, permitindo que diferentes departamentos ou unidades de negócios acessem dados uns dos outros com eficiência e eficácia.

Por outro lado, as APIs públicas, também chamadas de APIs externas, ficam expostas a clientes fora da empresa. Em sua manifestação mais extrema, como APIs abertas, podem ser livremente consumidas por qualquer pessoa. Em todos os casos, elas precisam de um gerenciamento rigoroso e de excelente documentação para poderem ser usadas por engenheiros de fora da empresa.

É importante observar que APIs privadas que possam ser acessadas pela Internet não são realmente privadas no sentido estrito da palavra. Por exemplo, digamos que a API B2C (Business-to-consumer) da ACME seja usada apenas pelos apps móveis da ACME (desenvolvidos internamente pelos engenheiros da ACME). Você pode se sentir tentado a chamá-la de API privada, mas como o tráfego para essa API chega da Internet ("fora da empresa"), essa API não é realmente privada, ela só não é publicada para públicos externos. Hackers atacam essas APIs com frequência, interceptando o tráfego e revertendo a engenharia de aplicativos móveis para encontrar suas APIs correspondentes.

Segurança de APIs explicada

O que é segurança de APIs?

A segurança de APIs é uma estratégia para ganhar visibilidade, testar rigorosamente e proteger cada API em uma empresa. Isso inclui APIs essenciais para aplicativos, processos de negócios e cargas de trabalho na nuvem. No entanto, como as APIs internas e externas estão sendo produzidas tão rapidamente e em tão grande número, pode ser difícil ter uma compreensão completa de todo o cenário de APIs da sua organização. Muitas organizações não têm conhecimento de quantas APIs realmente possuem e quais APIs retornam dados confidenciais quando chamadas. A identificação e a atenuação dos riscos de segurança de APIs exigem controles de segurança avançados o suficiente para oferecer esse tipo de visibilidade e análise de dados.
As APIs que precisam de proteção podem incluir:

- As APIs que permitem fácil acesso a dados por clientes ou parceiros de negócios
- As APIs consumidas de parceiros de negócios
- As APIs que são implementadas e usadas internamente para tornar a funcionalidade e os dados do aplicativo disponíveis para vários sistemas e interfaces de usuário de maneira padronizada e escalável

Uma estratégia eficaz para segurança de APIs deve incluir técnicas sistemáticas para avaliar riscos e possíveis impactos, bem como implementar medidas de mitigação apropriadas. A primeira etapa na avaliação de riscos é criar um inventário de todas as APIs sancionadas e não sancionadas publicadas e usadas pela organização. Esse inventário deve incluir atributos como:

- Classificações de dados que, no mínimo, façam distinção entre dados "não confidenciais", "confidenciais" e "muito confidenciais"
- Indicadores de risco, como vulnerabilidades de APIs e configurações incorretas

Além disso, a visibilidade de APIs e as medidas de mitigação de riscos devem considerar uma coletânea diversificada de possíveis ameaças, incluindo:

- Detecção e prevenção do uso de APIs sombra não sancionadas (consulte a barra lateral)
- Identificação e correção de vulnerabilidades e de configurações incorretas de APIs que agentes de ameaça possam explorar
- Prevenção de instâncias de uso incorreto de APIs, como violação de lógica de negócios e captura de dados

Em que a segurança de APIs difere da segurança de aplicativos?

Embora a segurança de APIs e a segurança de aplicativos tradicionais sejam disciplinas relacionadas, a segurança de APIs é um desafio distinto por dois motivos principais: a escala e a complexidade do problema.

Maior escala

Três fatores contribuem para o rápido crescimento do uso de APIs:

1. O uso de microsserviços, uma arquitetura que exige o uso de APIs para comunicação de serviço a serviço, está crescendo.
2. No canal de usuário direto, modernas estruturas de aplicativos de front-end, como React, Angular e Vue, usam APIs e estão deslocando aplicativos da Web herdados.
3. APIs também são adicionadas para lidar com canais completamente novos (por exemplo, parceiros, IoT [Internet das Coisas] e automação de negócios).

Flexibilidade que leva à complexidade

Diferente dos aplicativos da Web, as API são preparadas para serem usadas de forma programática de várias maneiras diferentes, o que torna extremamente desafiador diferenciar o uso legítimo de ataques e abusos.

Há uma taxonomia de API que as equipes de segurança devem entender?

A seguir estão as categorizações e descrições comuns de API que podem surgir em um contexto de segurança.

APIs sancionadas

API publicada (com documentação do Swagger ou semelhante)

APIs não sancionadas

- API sombra
- API não autorizada
- API zumbi
- API oculta

APIs desatualizadas

- API descontinuada
- API legada
- API zumbi
- API órfã

Quais são as práticas recomendadas para proteção das APIs?

O aprimoramento da segurança de suas APIs começa com as seguintes práticas recomendadas:

- Integre padrões e práticas de segurança de APIs ao ciclo de vida de desenvolvimento de software da sua organização.
- Inclua documentação de API e testes de segurança automatizados em seus pipelines de integração contínua/entrega contínua (CI/CD).
- Certifique-se de que os controles apropriados e eficazes de autenticação e autorização sejam aplicados às suas APIs.
- Implemente medidas de limitação de incidência para ajudar a impedir violação ou sobrecarga das APIs.
- Aumente a limitação de taxa e outras medidas de nível de aplicativo com gateways especializados e/ou CDNs (redes de entrega de conteúdo) para mitigar o risco de ataques de negação de serviço distribuída (DDoS).
- Faça do teste de segurança de APIs uma parte integrante de seus processos mais amplos de teste de aplicativos.
- Execute a detecção contínua de APIs.
- Implemente uma abordagem sistemática para identificar e corrigir vulnerabilidades comuns de API, incluindo os riscos de segurança a APIs incluídos na lista OWASP Top 10.
- Use detecção e prevenção de ameaças baseadas em assinaturas, como um nível padrão de proteção para ataques conhecidos contra API.
- Aumente a detecção baseada em assinaturas com IA e análise comportamental para tornar a detecção de ameaças de APIs mais escalonável, precisa, relevante para os negócios e resiliente contra novas ameaças.
- Garanta que o processo de monitoramento e análise da segurança de APIs se estenda por várias semanas e sessões de API.
- Complemente o monitoramento e o alerta de segurança de APIs com acesso sob demanda ao inventário de API e aos dados de atividade para uso por caçadores de ameaças, desenvolvedores, DevOps e equipe de suporte.

A sua capacidade de implementar essas práticas recomendadas de segurança de APIs depende de onde você está em sua jornada para uma estratégia madura de segurança de APIs (consulte a barra lateral).

Estágios da maturidade da segurança de APIs

Estágio 1: Visibilidade e descoberta

Você está no processo de descoberta de todas as suas APIs e dos microsserviços aos quais elas oferecem suporte por meio de uma abordagem automatizada. A extensão da cobertura é fundamental, pois as APIs negligenciadas (como as que não estão mais em uso) são o principal alvo dos agentes de ameaças.

Estágio 2: Testes

Você testa todas as suas APIs para garantir que elas sejam codificadas corretamente e que desempenhem a função prevista. O teste realizado antes da implantação de uma API é o limite máximo desse estágio de maturidade; o risco é eliminado antes de a API entrar em produção, e qualquer correção necessária é consideravelmente mais barata.

Estágio 3: Auditoria de riscos

Você audita constantemente todo o seu ambiente de APIs para identificar APIs mal configuradas ou outros erros. A auditoria também garante a documentação adequada de todas as APIs e determina se elas contêm dados confidenciais ou se não possuem controles de segurança adequados.

Estágio 4: Proteção de tempo de execução

Você está usando uma solução com proteção automatizada de tempo de execução, que pode diferenciar entre atividade normal e incomum da API. Ao monitorar as interações das APIs dessa forma, você pode detectar comportamentos que indicam uma ameaça em tempo real.

Estágio 5: Resposta

Você tem soluções implementadas que respondem a comportamentos suspeitos das APIs, como um WAF ou gateway de API que bloqueia o tráfego suspeito antes que ele possa acessar recursos essenciais. As soluções usam regras personalizadas e automatizadas.

Estágio 6: Busque por ameaças

Você realiza regularmente análises forenses de dados de ameaças anteriores para saber se os alertas identificaram corretamente as ameaças e se surgiram padrões que permitem a detecção proativa de ameaças usando uma combinação de ferramentas avançadas e inteligência humana.

Riscos de segurança e violação de APIs

O que é uma vulnerabilidade de API?

Uma vulnerabilidade de API é um bug de software ou erro de configuração do sistema que um invasor pode explorar para acessar dados ou funcionalidades confidenciais de aplicativos ou para usar indevidamente uma API. O documento OWASP Top 10 com os principais riscos à segurança de APIs oferece uma visão geral útil de algumas das vulnerabilidades das APIs mais exploradas que as organizações devem tentar identificar e corrigir.

Todas as vulnerabilidades de API são rastreadas no OWASP Top 10 com os principais riscos à segurança de APIs?

O OWASP Top 10 com os principais riscos à segurança de APIs é um excelente ponto de partida para organizações que buscam melhorar sua postura de segurança das API. Suas categorias abrangem uma ampla variedade de possíveis riscos de API. Mas as categorias incluídas no OWASP Top 10 em Segurança de API são bastante abrangentes, por isso é importante detalhar as subáreas de cada uma delas. Invasores de API tentam frequentemente explorar problemas de autorização (extensivamente cobertos pelo OWASP), mas também há riscos de API que estão completamente fora do OWASP Top 10 em Segurança de API, como a violação de bugs lógicos.

Como pode acontecer a violação de APIs?

As APIs podem ser atacadas e usadas de várias maneiras, mas alguns dos exemplos mais comuns incluem:

- **Exploração de vulnerabilidade:** Vulnerabilidades técnicas na infraestrutura subjacente podem levar a comprometimento do servidor. Os exemplos vão desde as vulnerabilidades do Apache Struts (CVE-2017-9791, CVE-2018-11776) até as vulnerabilidades do Log4j (CVE-2021-44228).
- **Violação de lógica de negócios:** A violação de lógica ocorre quando um agente de ameaças explora falhas de design ou de implementação de aplicativos para incitar comportamentos não esperados e não sancionados. Esses cenários causam estresse para os CISOs e suas equipes porque os controles de segurança legados são inúteis contra eles.
- **Acesso não autorizado a dados:** Outra forma comum de violação de API é a exploração de mecanismos de autorização corrompidos para acessar dados que não deveriam estar acessíveis. Essas vulnerabilidades têm muitos nomes, como Autorização em nível de objeto corrompida (BOLA), Referência direta de objeto inseguro (IDOR) e Autorização em nível de função corrompida (BFLA).

- **Apropriação indevida de contas:** Após um roubo de credencial ou mesmo um ataque XSS, uma conta pode ser roubada. Quando isso acontece, é possível que aconteça abuso até mesmo da API mais bem escrita e perfeitamente protegida. O uso de uma solução de segurança de APIs que ofereça análise de comportamento permite que você diferencie a atividade autenticada do uso ilegítimo.
- **Captura de dados:** Conforme organizações disponibilizam conjuntos de dados por meio das APIs públicas, agentes de ameaças podem consultar de forma agressiva esses recursos para a captura indiscriminada de grandes conjuntos de dados valiosos.
- **Negação de serviço (DoS) de negócios:** Ao solicitar que o back-end realize tarefas pesadas, invasores de API podem causar erosão do serviço ou uma DoS completa na camada de aplicativo (uma vulnerabilidade muito comum em GraphQL, mas algo que pode acontecer com qualquer implementação de ponto de extremidade de API com uso intenso de recursos).

O que é uma API zumbi?

Impulsionadas pelas mudanças nos requisitos de mercado e de negócios, as APIs estão em fluxo constante. À medida que novas implementações de ponto de extremidade são lançadas para atender às novas necessidades de negócios, corrigir bugs e introduzir melhorias técnicas, versões mais antigas desses pontos de extremidade são desativadas. O gerenciamento do processo de desativação de pontos de extremidade antigos não é simples. Muitas vezes, as implementações de ponto de extremidade que deveriam ter sido descontinuadas permanecem vivas e acessíveis. Eles são chamados de pontos de extremidade zumbis.

Como posso encontrar os vários tipos de APIs sombra?

Uma das maneiras de realizar a descoberta de APIs sombra em toda a empresa é coletar e analisar o tráfego de APIs em sua rede. Entre os exemplos de fontes de tráfego de APIs, incluem-se:

Uma vez que os dados brutos de todas as fontes disponíveis são coletados, as técnicas de IA podem ser usadas para transformá-los em um inventário completo de todas as APIs, pontos de extremidade e parâmetros. A partir daí, análises adicionais podem ser feitas para classificar esses elementos e identificar as APIs sombra que devam ser eliminadas ou introduzidas em processos formais de governança.

Como proteger as APIs internas e as APIs B2B (Business-to-business)?

Na verdade depende da definição de "interna". Algumas equipes se referem às APIs expostas pela Internet para aplicativos para a web e móveis de suas próprias organizações como "APIs internas". E, embora a documentação dessas APIs possa, de fato, ser acessível apenas para funcionários e contratados da empresa, os hackers se tornaram aptos a analisar aplicativos e a fazer engenharia reversa das APIs por meio de kits de ferramentas de desmontagem de app e proxies como o Burp Suite.

No entanto, se "API internas" forem definidas como APIs leste-oeste, que não podem ser acessadas de fora da organização, a principal ameaça será reduzida a uma ameaça interna. Proteja as APIs leste-oeste e suas APIs B2B (Business-to-business) como a maioria das outras APIs: Comece protegendo o ciclo de vida de desenvolvimento de software (SDLC) e continue garantindo que o acesso seja autenticado e autorizado. Você também pode implementar o gerenciamento de cotas, limites de taxas e bloqueios de picos. Além disso, você pode proteger suas APIs contra ameaças conhecidas usando WAFs/WAAPs. Para APIs B2B (Business-to-business), considere adicionar mecanismos de autenticação rígidos, como mTLS, devido à natureza confidencial e frequentemente em massa das transações.

E, para ambas, APIs leste-oeste e B2B (Business-to-business), recomendamos que você empregue análises comportamentais, especialmente se você tiver muitas entidades envolvidas, o que pode dificultar o processo de distinção entre comportamento legítimo e ilegítimo. Por exemplo:

> **Como você sabe se as credenciais de API de um usuário específico foram comprometidas?**

> **Como você saberia se sua API de faturamento estivesse sendo corrompida por um parceiro que enumera faturas para roubar dados de contas?**

A proteção de APIs B2B (Business-to-business) e de APIs leste-oeste requer um contexto de negócios que não pode ser obtido pela simples análise de elementos técnicos, como endereços IP e tokens de API. O uso de aprendizado de máquina e análise comportamental para obter visibilidade de entidades relevantes para os negócios é a única maneira de entender e gerenciar os riscos efetivamente. O contexto de negócios e benchmarks históricos para uso normal de APIs por entidades específicas, como seus usuários ou parceiros, ou até mesmo entidades de processos de negócios (fatura, pagamento, pedido etc.) possibilitam a percepção de anomalias que não seriam detectadas de outra forma.

Os gateways de API oferecem proteção suficiente contra riscos?

Muitas organizações que adotam uma abordagem estratégica para APIs usam gateways de API. A maioria dos gateways de API tem recursos de segurança integrados avançados dos quais as organizações podem se beneficiar. O primeiro deles é a autenticação (e a autorização, também, se você puder usar o OpenID Connect). No entanto, a simples execução de autenticação, autorização e gerenciamento de cotas no gateway de API não é suficiente, por vários motivos:

A lacuna de descoberta de gateways de API: Gateways de API só têm visibilidade e controle sobre as APIs que estejam configuradas para gerenciar, sendo ineficazes para detecção das APIs sombra e pontos de extremidade.

A lacuna de segurança dos gateways de API: Os gateways de API podem reforçar a autenticação e, até certo ponto, os esquemas de autorização, mas não verificam as cargas úteis (como fazem os WAFs e WAAPs), nem criam perfis de comportamento para detectar violações.

Quais são os erros mais comuns de configuração incorreta de API?

O número de possíveis configurações incorretas de API é quase infinito, dado o grande número de formas como as APIs são usadas. No entanto, há alguns temas comuns na configuração incorreta:

Autenticação com problema ou falta de autenticação

A autenticação é fundamental para proteger dados confidenciais disponibilizados por meio de APIs. A primeira etapa é garantir que todas as APIs que transportam dados confidenciais dependam de autenticação desde o início. Mas também é importante proteger os mecanismos de autenticação contra ataques de força bruta, preenchimento de credenciais e uso de tokens de autenticação roubados por meio de limitação de taxa. Às vezes, podem ocorrer configurações incorretas que permitem que os consumidores da API ignorem os mecanismos de autenticação, geralmente em torno do gerenciamento de tokens (por exemplo, alguns problemas conhecidos de validação de JWT ou a não verificação do escopo do token).

Autorização com problema

Um dos usos mais comuns das APIs é fornecer acesso a dados ou conteúdo, incluindo informações confidenciais. Autorização é o processo de verificar se um consumidor de API está qualificado para acessar os dados que esteja tentando acessar, antes que sejam disponibilizados. Isso pode ser feito no nível de objeto ou do recurso (por exemplo, posso acessar meus pedidos, mas não os de outra pessoa) ou no nível de função (como é frequentemente o caso com recursos administrativos). A autorização é difícil de ser feita por causa do alto número de casos e condições de edge e, por causa dos vários fluxos que as chamadas de API podem seguir entre microsserviços. Se você não tiver um mecanismo de autorização centralizado, sua implementação de API provavelmente incluirá algumas dessas vulnerabilidades, como BOLA e BFLA.

Má configuração de segurança

Além dos problemas de autenticação e autorização mencionados acima, há muitos tipos possíveis de configurações incorretas de segurança, incluindo comunicação desprotegida (por exemplo, falha no uso de SSL (Secure Sockets Layer)/TLS ou uso de conjuntos de cifras vulneráveis), armazenamento em nuvem desprotegido e políticas de compartilhamento de recursos entre origens excessivamente permissivas.

Falta de recursos e limitação de taxa

Quando as APIs são implementadas sem qualquer limite no número de chamadas que os consumidores da API podem fazer, os agentes de ameaças podem sobrecarregar os recursos do sistema, levando à degradação do serviço ou à DoS em grande escala. No mínimo, os limites de taxa devem ser aplicados ao acesso a qualquer ponto de extremidade não autenticado, com pontos de extremidade de autenticação de importância crítica. Caso contrário, outros ataques de força bruta, além de ataques de preenchimento de credenciais e validação de credenciais, simplesmente acabam acontecendo.

O que são ataques a APIs?

Ataques de APIs são tentativas de usar as APIs para fins mal-intencionados ou não sancionados. Ataques de APIs assumem muitas formas, incluindo:

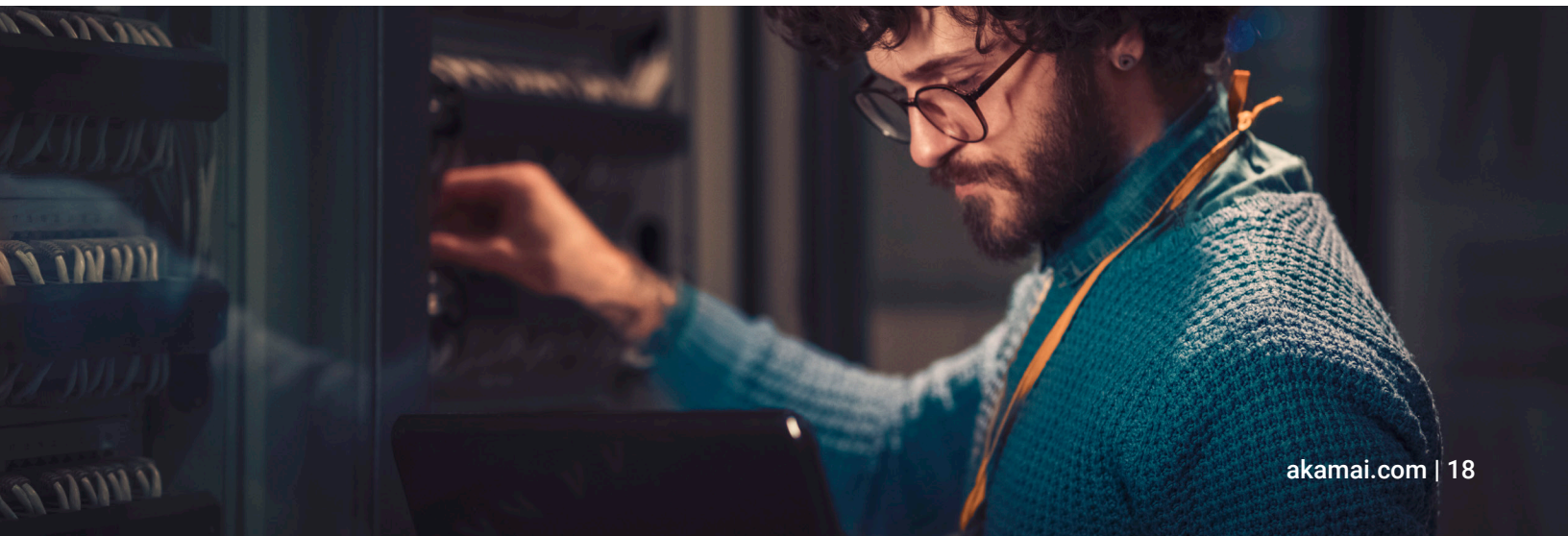
- Exploração de vulnerabilidades técnicas em implementações de API
- Uso de credenciais roubadas e de outras técnicas de apropriação de contas para se mascarar como um usuário legítimo
- Abuso de lógica de negócios que permite o uso das API de maneiras inesperadas

O que é preenchimento de credenciais para APIs?

O vazamento de informações de ID de usuário e senha de websites e plataformas de software como serviço (SaaS) se tornou uma ocorrência regular. Muitas vezes, esses incidentes resultam em grandes conjuntos de credenciais sendo compartilhados amplamente online. O preenchimento de credenciais é a prática de usar credenciais de autenticação vazadas de websites previamente violados em tentativas de login automatizadas em outros websites. Essa técnica é baseada na premissa de que alguma porcentagem dos usuários usam as mesmas credenciais para vários websites. Cada vez mais, os invasores estão indo direto para as APIs e atacando os mecanismos de autenticação. Isso permite que invasores automatizem o ataque mais facilmente, pois as API são criadas para facilitar o consumo.

O que é a exfiltração de dados por meio de APIs?

A exfiltração de dados é um resultado frequente de ataques e violações bem-sucedidas contra APIs. Em alguns casos, refere-se a informações altamente confidenciais e não públicas que foram roubadas por um agente de ameaças por meio de ataques à API. No entanto, também pode se aplicar a tipos menos graves de violação de APIs, incluindo captura agressiva de dados disponíveis publicamente para montar grandes conjuntos de dados que são valiosos na forma agregada.



Soluções e tendências de segurança de APIs

Quais são as tendências mais recentes em segurança de APIs?

Confira a seguir as principais tendências que os executivos de segurança devem considerar ao desenvolver uma estratégia de segurança de APIs:

Análise comportamental e detecção de anomalias: em vez de tentar prever possíveis ataques e confiar apenas na detecção baseada em assinaturas e em políticas predefinidas (por exemplo, WAFs) para mitigar os riscos, as organizações estão adicionando cada vez mais o aprendizado de máquina e a análise comportamental para visualizar a atividade da API em um contexto comercial e detectar anomalias.

Transição de no local para SaaS: Embora muitos produtos de segurança de APIs de primeira geração tenham sido implantados "no local", abordagens baseadas em SaaS estão ficando mais populares devido à sua velocidade, facilidade de implantação e capacidade de aproveitar em escala o poder do aprendizado de máquina.

Análise de janelas de tempo maiores: Abordagens de segurança de APIs que analisam apenas chamadas de API individuais ou atividade de sessão de curto prazo estão sendo suplantadas por plataformas que podem analisar a atividade de API ao longo de dias e, às vezes, semanas, desde a conclusão da otimização básica automatizada da política WAF até a realização de análises comportamentais e a detecção de anomalias.

DevSecOps – abrangendo partes interessadas não relacionadas à segurança: Uma das melhores maneiras de reduzir os riscos de API é criar mais conexões entre as estratégias e ferramentas de segurança de APIs e os desenvolvedores e sistemas envolvidos na criação, implementação e configuração de APIs.

Segurança de APIs habilitada por API: Embora a detecção e a mitigação de ataques ativos de API e instâncias de violação sejam fundamentais, organizações inovadoras estão encontrando maneiras de usar o acesso por demanda a dados e insights de segurança de APIs para melhorar a detecção de ameaças, a resposta a incidentes e as práticas de desenvolvimento de API.

O que é segurança de APIs baseada em assinatura?

Técnicas de segurança de APIs baseada em assinatura monitoram caraterísticas e padrões de ataque conhecidos e, em seguida, geram alertas de segurança e outras respostas automatizadas quando correspondências são observadas. Isso é típico de um WAF. O valor: se uma organização tiver informação sobre tráfego de API recebido que esteja comprometido ou se comportando de forma anormal, ela poderá usar a segurança de APIs baseada em assinatura para bloqueá-lo imediatamente.

Você deve encontrar um WAF que faça parte de uma solução WAAP maior, que possa oferecer detecções avançadas por meio do aprendizado de máquina, que aprenda com os padrões de assinatura de ataques e que possa continuar ágil em escala. Um WAAP integrado a uma solução de segurança de APIs que ofereça análise comportamental e respostas personalizadas dará a você o melhor dos dois mundos. Juntas, essas soluções oferecem visibilidade, detecção e resposta completas da API interna e externamente.

O que é detecção e resposta de APIs?

Detecção e resposta de APIs é uma categoria emergente para segurança de APIs voltada para a análise profunda de dados históricos, a fim de:

- Determinar um padrão de comportamento de todos os consumidores de API
- Detectar ataques e anomalias que indiquem possível abuso e uso indevido de API

Detecção e resposta efetivas em escala para as API só podem ser proporcionadas por um modelo SaaS devido aos grandes conjuntos de dados exigidos por técnicas de aprendizado de máquina com uso intenso de recursos.

O que é proteção avançada contra ameaças de APIs?

Proteção avançada contra ameaças de API é uma abordagem da segurança de APIs baseada em SaaS que combina análise comportamental com busca de ameaças para:

- Revelar todas as API em uso por uma organização, incluindo API sombra e zumbi
- Usar o aprendizado de máquina para sobrepor o contexto de negócios ao modo como as API estão sendo usadas e violadas
- Realizar análise comportamental e detecção de ameaças em APIs e dados de atividade de API

O que é uma plataforma de segurança de APIs?

Uma plataforma de segurança de APIs é uma oferta baseada em SaaS especialmente projetada para:

- Criar um inventário continuamente atualizado de todas as APIs em uso em toda a organização (sancionadas ou não)
- Analisar APIs e seu uso para descobrir o contexto comercial e determinar uma linha de base do comportamento esperado
- Detectar anomalias de uso de APIs e, quando necessário, produzir alertas e dados de suporte para fluxos de trabalho de gerenciamento de eventos e informações de segurança (SIEM) e orquestração de segurança, automação e resposta (SOAR)
- Fornecer acesso sob demanda ao inventário de APIs, atividades e informações sobre ameaças para partes interessadas, estejam elas relacionadas ou não à segurança

O que é uma empresa de segurança de APIs?

Agora que os líderes de TI e segurança estão usando as API de forma mais estratégica, podem precisar envolver parceiros de API especializados. Os três tipos mais comuns de empresas de API são:

- Empresas de gateway de API, que oferecem tecnologia para aceitação central de chamadas de API e seu encaminhamento para recursos e microsserviços de back-end apropriados
- Empresas de plataformas de segurança de APIs que garantem que as organizações estejam cientes de todas as APIs ativas e de seus possíveis riscos, que possam detectar instâncias de ataques e violações, que permitam testes de segurança completos e que forneçam dados detalhados sobre como as APIs estão sendo usadas
- Empresas de plataforma de segurança de WAAP e API podem ajudar a transferir dados de tráfego de API sem sobressaltos e, ao mesmo tempo, oferecer a capacidade de descobrir as API dentro e fora da plataforma. Isso é ideal para a consolidação de fornecedores e para o fechamento de lacunas digitais

O que é a detecção de ameaças em APIs?

A detecção de ameaças envolve a busca ativa de ameaças desconhecidas ou não detectadas anteriormente. Essa abordagem proativa é fundamental para identificar ameaças novas e emergentes que talvez não tenham sido detectadas antes e para mitigá-las antes que possam causar danos significativos. Uma das principais técnicas empregadas na detecção de ameaças é a análise comportamental. Isso envolve a análise do comportamento das APIs para identificar qualquer atividade suspeita ou atípica. Por exemplo, se uma API solicitar repentinamente milhares de registros em um curto período, isso pode indicar que a lógica comercial da API está comprometida. As soluções modernas para segurança de APIs oferecem recursos específicos de detecção de ameaças que permitem que as equipes de segurança identifiquem possíveis ameaças com antecedência e respondam com contramedidas.

O que é WAAP?

A proteção de aplicativos da Web e APIs (WAAP) é uma categorização que a empresa de pesquisa Gartner usa para sua cobertura do setor de soluções de proteção emergentes para Web e API. É uma evolução da cobertura anterior do setor de WAF em resposta à crescente importância estratégica para segurança de APIs e à mudança das plataformas WAF para a nuvem como SaaS gerenciada.

Quais são exemplos de documentação de API?

A forma mais comum de documentação de API para API RESTful (que são o tipo mais comum de API da Web) é uma coletânea de arquivos Swagger com base na especificação OpenAPI. O ideal é que a documentação de API seja criada pelos desenvolvedores quando uma API é concebida ou implementada. No entanto, a realidade é que documentações de API estão frequentemente desatualizadas, resultando em uma incompatibilidade entre o uso da API no mundo real e sua documentação. Para resolver esse problema, algumas plataformas de segurança de APIs podem gerar arquivos Swagger a partir da atividade real da API, destacando as lacunas entre o que está documentado e o que é realmente implantado, o que é um componente integral em qualquer avaliação de risco de API.

Há uma lista de verificação de segurança de API que as empresas devem seguir?

A segurança de APIs eficaz requer muitas etapas detalhadas e práticas contínuas específicas para uma organização. No entanto, veja a seguir uma lista de requisitos de APIs que equipes de segurança podem usar como ponto de partida, enquanto desenvolvem sua segurança de APIs:

- Sua abordagem de segurança de APIs inclui um mecanismo de descoberta contínua de API em toda a empresa?
- O gerenciamento da postura da API está integrado às práticas mais abrangentes de segurança e gerenciamento de riscos da organização?
- Você está implementando uma abordagem de segurança de APIs de finalidade geral que não restringirá você a modelos específicos de data center ou infraestrutura em nuvem?
- Sua abordagem dará às suas equipes o contexto de negócios de que precisam para realmente entender a atividade de API e os possíveis riscos que estão sendo observados?
- Você tem uma estratégia para automação bidirecional entre sua plataforma de segurança de API e outros processos de negócios relacionados, como SIEM/SOAR, busca de ameaças, documentação, ferramentas de DevOps etc.?
- Você está tomando medidas para acolher partes interessadas não relacionadas à segurança, como desenvolvedores, em suas ferramentas e processos de segurança de APIs?

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 09/24.