Akamai

WHITE PAPER

Oito recomendações para segurança de APIs

Fatores críticos para uma postura robusta de segurança de APIs

Por que é tão complicado proteger APIs?

A segurança da APIs lidera a lista de prioridades de muitos executivos de TI, e com bons motivos. Considere o seguinte:

"A explosão de APIs proporciona uma superfície de ataque atraente, e a segurança de APIs continua intrigando os líderes de segurança."

— The Eight Components Of API Security, Forrester Research, Inc., 28 de setembro de 2023

Fatores no crescimento de riscos a APIs

Em resposta a esses riscos, as organizações devem entender o seguinte antes de começar a implementar uma segurança de API eficaz:

As APIs são alvos dinâmicos	
Compreensão interna sobre APIs	**Exposição externa das APIs**
Os processos de DevOps de rápida movimentação criam e desativam APIs continuamente, levando a um inventário incompleto de API	Práticas de API imaturas levam à exposição não intencional de APIs confidenciais a terceiros, incluindo muitas APIs sombra

As APIs são vulneráveis a dois tipos diferentes de ameaças	
Vulnerabilidades técnicas	**Uso incorreto e violação**
Os invasores podem explorar vulnerabilidades e configurações incorretas de software, incluindo as que fazem parte do OWASP API Security Top 10	O abuso de lógica de negócios e outros comportamentos, como captura agressiva de dados, podem ocorrer independentemente de uma vulnerabilidade técnica

Lidar com o desafio complexo da segurança de APIs requer uma abordagem bem pensada que inclua:

Incorporar os mais recentes avanços tecnológicos

Quebrar barreiras organizacionais

Encarar o cenário completo de ameaças de API

A seguir estão algumas estratégias essenciais a serem implementadas — e armadilhas a serem evitadas — à medida que você desenvolve uma estratégia de segurança de APIs mais sofisticada para sua organização.

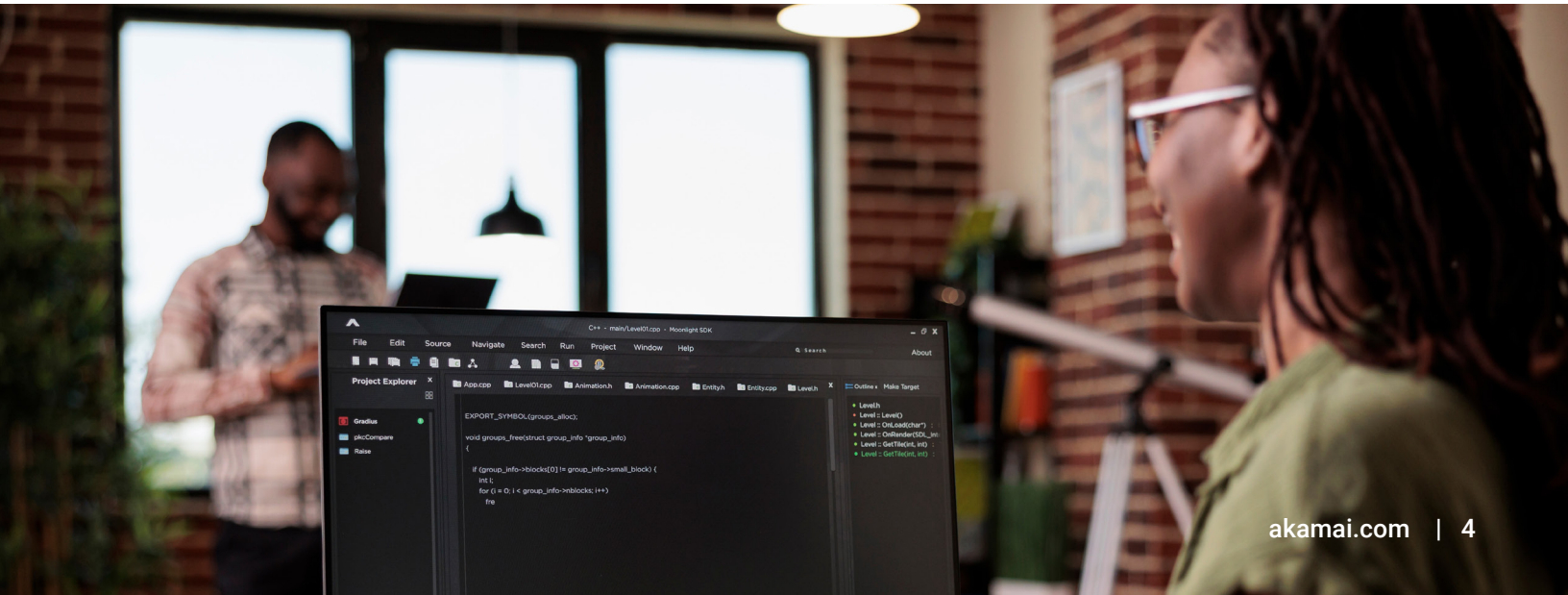
Oito recomendações para uma segurança eficaz de APIs

1 Obtenha visibilidade completa de APIs

Vale a pena repetir: você não pode proteger APIs que você não sabe que possui. Quanto mais tempo uma API ficar sem identificação e sem monitorização, maior a probabilidade de se tornar um alvo para um intruso. A melhor maneira de obter visibilidade completa é garantir que sua plataforma de segurança de API possa ingerir informações da mais ampla variedade possível de fontes de dados, incluindo gateways de API, dispositivos de rede, soluções de orquestração de microsserviços, provedores de nuvem e muito mais. Especificamente, sua solução de segurança de API deve ser capaz de fazer o seguinte:

Tempo	Localização
• Descobrir APIs continuamente • Monitorar chamadas de API individuais • Registrar a atividade de sessões de curto prazo • Analisar o comportamento das APIs ao longo do tempo	• Descobrir APIs em toda a empresa • Descobrir APIs legadas • Descobrir APIs sombra

A visibilidade completa da API ajudará a evitar violações de dados, especialmente porque a mais recente técnica de violação de dados envolve invasores que usam ataques lentos e baixos para extrair dados das APIs. Saber onde estão todas as suas APIs é a primeira etapa para evitar esse tipo emergente de ataque.



2 Não tenha medo da nuvem

Os Web Application Firewalls (WAFs) usam técnicas baseadas em assinatura para impedir que APIs não autorizadas entrem na sua organização. À medida que os ataques à API evoluem, você precisa de uma camada extra para defender totalmente as APIs de toda a gama de possíveis riscos usando análise comportamental. Agora, é essencial monitorar o comportamento de suas APIs dentro de sua organização, não apenas aquelas expostas externamente.

Para usar a análise comportamental de forma eficaz, o tráfego de APIs precisa ser analisado na nuvem. Às vezes, as equipes de segurança relutam em enviar informações confidenciais sobre a atividade de sua organização para a nuvem. No entanto, realizar análises comportamentais verdadeiras usando técnicas estendidas de detecção e resposta no volume de dados de APIs que a maioria das empresas gera é altamente impraticável sem a escala e a elasticidade que a nuvem fornece.

Além disso, como as equipes de segurança têm seus recursos limitados, implantações de produtos longas e complexas são um grande obstáculo para o progresso. Devido ao crescente risco representado pelo uso mais amplo de APIs, as equipes de segurança não podem se dar ao luxo de ficar para trás. Portanto, é essencial migrar para a nuvem como parte da sua estratégia de segurança de APIs.

3 Torne o contexto empresarial central para sua estratégia

Descobrir APIs e identificar riscos de segurança é apenas o início da jornada para uma menor superfície de ataque a APIs. Pense nas três perguntas seguintes:

1. Como você saberia se as credenciais de API de um parceiro específico estivessem comprometidas?

2. Como você saberia se a espionagem corporativa estivesse acontecendo na forma de captura de dados em uma API?

3. Como você saberia se sua API de faturamento estivesse sendo corrompida por um usuário através de números de fatura para roubar dados de contas?

No primeiro cenário, a atividade pareceria originar-se de um usuário legítimo. Portanto, a única maneira de detectar intenção maliciosa é observar uma mudança do comportamento esperado na API em questão. O segundo e o terceiro cenários também são exemplos de comportamento não sancionado que explora modelos legítimos de acesso a APIs. Esses são outros casos em que é essencial entender o contexto de negócios, além do que está ocorrendo tecnicamente.

4 Não pense nos dados como uma via de mão única

Um dos recursos fundamentais de uma abordagem de segurança de APIs eficaz é a capacidade de enviar alertas e eventos para as ferramentas preferidas de monitoramento de segurança e de fluxo de trabalho de TI. Um erro comum cometido pelos fornecedores de segurança e pelas equipes que implementam os alertas é visualizar alertas de segurança e respostas automatizadas como um fluxo de comunicação unidirecional.

Assim como muitos processos de negócios legítimos, os ataques podem ocorrer por um longo período. Para ser eficaz, a análise comportamental para uso de APIs deve ser realizada por um período de pelo menos 30 dias. Isso fornece uma imagem mais completa e precisa do comportamento esperado da linha de base. Também é possível detectar ataques que são executados lentamente em vários dias ou semanas e várias sessões de APIs. Considere um ataque de captura de dados baixo e lento que esteja abaixo de um limite de taxa definido: esse comportamento só seria encontrado examinando o comportamento histórico versus quaisquer alterações.

Um alerta sem detalhes adicionais seguramente traz mais desvantagens do que vantagens. Um alerta com contexto rico sobre a causa e o impacto, no entanto, é muito mais prático. Mas a verdadeira vitória vem de fornecer um alerta prático e repleto de contexto e dar ao destinatário a capacidade de consultar um conjunto de dados mais abrangente para analisar o incidente. Em seguida, você pode aproveitar as proteções WAF para bloquear imediatamente o tráfego que representa uma ameaça potencial para sua empresa.

5 Priorize a colaboração entre departamentos

Alguns dos maiores ganhos da segurança de APIs podem vir da prevenção proativa de vulnerabilidades durante as fases de projeto, desenvolvimento e implantação. Para realizar isso de forma eficaz, você precisa de colaboração entre suas equipes.

Inicie esse processo colaborativo, dando às equipes de APIs visibilidade de como as APIs estão sendo usadas (e violadas) em condições reais. Com o tempo, essa exposição promoverá uma cultura de pensamento sobre segurança mais cedo nos processos de desenvolvimento e implantação de APIs. Além disso, certifique-se de que:

- Existam benefícios não relacionados à segurança que ajudam as equipes de API a trabalhar com mais eficiência, além dos principais recursos de segurança de sua abordagem
- Seja fácil para usuários que não são da área de segurança, como desenvolvedores, visualizar e consultar informações de inventário e atividade de APIs
- Haja o uso de respostas contextuais, como integrações a ferramentas de desenvolvimento, como Jira, que abrem proativamente tíquetes para correções de segurança que os desenvolvedores precisam fazer

Ao pensar na segurança de APIs como um trabalho conjunto e facilitar o envolvimento dos interessados fora da equipe de segurança, a culpabilização mútua é eliminada, e torna-se possível que as equipes de desenvolvimento, operações e segurança trabalhem juntas de formas benéficas para todos.

6 Não ignore APIs de terceiros

Outro erro comum a ser evitado na estratégia de segurança de API é presumir que você só precisa se preocupar com suas próprias APIs. Apesar de ser desejável acreditar que o WAF ou o gateway de API que você comprou padroniza toda a sua estratégia de segurança de API, isso nem sempre acontece.

Por exemplo, só porque uma estratégia de gateway de API centralizada é implementada, não suponha que as APIs sombra não contornarão a principal abordagem de governança de APIs. Se a sua empresa usar APIs de terceiros, seu gateway verá essas APIs como autenticadas, mesmo que elas fossem comprometidas antes de se conectaram ao seu ecossistema.

Sua estratégia de proteção deve estar em contato com suas principais tecnologias de API, como gateways de API, enquanto também coleta o máximo possível de informações de outras fontes, como dispositivos de rede, plataformas de nuvem e ferramentas de orquestração de microsserviços. Essa é a única maneira de criar uma imagem completa de sua superfície de ataque de API e de preparar sua estratégia de segurança para o futuro, pois inevitavelmente ocorrem transições de tecnologia e infraestrutura.

7 Não apenas responda e prossiga

Embora a resposta rápida e eficaz a alertas seja excelente, se você estiver concentrado apenas em atenuar alertas depois que eles acontecerem, perderá a oportunidade de evitar alertas completamente. Em vez disso, considere a busca proativa de ameaças. Se o seu parceiro de segurança de APIs permitir que você realize consultas de dados, você poderá testar suas próprias hipóteses, entender relacionamentos e identificar possíveis ameaças antes que elas se agravem para um incidente de segurança. Por exemplo, se você identificar um mau comportamento de uso de API por um parceiro específico, poderá procurar comportamento semelhante por outros parceiros ou fornecedores com alguns cliques.

Qualquer parceiro de segurança de APIs deve armazenar dados históricos em um data lake e fornecer acesso a esses dados para permitir investigações e busca de ameaças.

O ideal é que esses tipos de recursos avançados de consulta sejam disponibilizados de duas maneiras:

1. Como uma interface da Web de usuário simples e intuitiva

2. Como um conjunto de interfaces de API nos próprios provedores de segurança de API para uso no desenvolvimento de fluxos de trabalho mais sofisticados

8 Encare a segurança de APIs como um ciclo contínuo

A melhor maneira de integrar a segurança de APIs diretamente à sua empresa é por meio de testes de API. Ao adicionar essa ferramenta ao ciclo de vida da API, você pode limitar as chances de que uma API mal configurada ou vulnerável seja colocada em produção. Esse teste e a correção no início do ciclo de desenvolvimento reduzem as dores de cabeça, economizam tempo e diminuem as despesas.

Em seguida, as equipes de segurança devem começar seus esforços de proteção de API criando um inventário de APIs em uso por sua organização. Como as APIs são adicionadas e desativadas continuamente, é essencial que as equipes de segurança mantenham um inventário vivo das interfaces de APIs em suas aplicações e repositórios de dados confidenciais. Quando a descoberta contínua de APIs é realizada de forma eficaz, APIs sombra, invasoras, esquecidas, zumbis, órfãs e descontinuadas viram problemas do passado.

As equipes de segurança devem ter a visibilidade de que precisam para detectar e atenuar uma ampla variedade de ameaças emergentes à segurança de APIs. Mas detectar ameaças também deve acontecer durante o tempo de execução. O abuso da lógica de negócios é encontrado apenas em APIs em produção. Comparar o comportamento do tempo de execução com os padrões de uso normais da linha de base ajuda a revelar comportamento abusivo.

Por fim, é importante realmente parar as ameaças que podem aproveitar suas APIs a qualquer momento durante o tempo de execução. O bloqueio automático pelo WAF é essencial para essa etapa porque simplesmente ter alertas para tudo não será suficiente para proteger sua empresa no nível macro. Outras respostas automatizadas podem ser variadas e personalizáveis, como a redução de um limite de taxa no gateway de API, a abertura de um tíquete Jira para um desenvolvedor investigar ou o envio de um e-mail para a equipe de segurança. A capacidade de responder adequadamente a cada ameaça detectada só é possível quando o contexto é compreendido e o mecanismo de resposta é personalizável.

Resumo

O que fazer	O que não fazer
✔ Obter visibilidade completa de APIs	✘ Não ter medo da nuvem
✔ Tornar o contexto de negócios central para sua estratégia	✘ Não pensar nos dados como uma via de mão única
✔ Priorizar a colaboração entre departamentos	✘ Não ignorar APIs de terceiros
✔ Encarar a segurança de APIs como um ciclo contínuo	✘ Não apenas responder e prosseguir

Comece hoje mesmo

Você está pronto para dar o primeiro passo em direção a uma abordagem moderna e sistemática de segurança de APIs?

Saiba mais sobre o Akamai API Security.

A abordagem baseada em nuvem da Akamai facilita o início em minutos. Em poucas horas, você terá uma visão completa do uso de APIs em sua organização, incluindo uma compreensão detalhada das relações entre sua lógica de negócios e suas APIs.