ESTUDO SOBRE O IMPACTO DA SEGURANÇA DE

APIs 2024

Como os incidentes de API afetam você e sua equipe

Akamai

Uma publicação afiliada dos **relatórios SOTI (State of the Internet) da Akamai**

Índice

Resumo executivo

Agora em seu terceiro ano, o Estudo sobre o impacto da segurança de APIs (antigo API Security Disconnect Report) explora o estado da proteção de APIs com base em uma pesquisa com 1.207 líderes e profissionais nos EUA, no Reino Unido e (novidade em 2024) na Alemanha. O estudo examina como as empresas vivenciam os eventos de segurança de APIs, sua frequência, causas e impactos, e como os departamentos de segurança estão lidando com as APIs como um vetor de ataque.

Para obter o quadro mais completo, pesquisamos uma amostra equilibrada de:

- CISOs, CIOs, CTOs, profissionais de segurança seniores e membros da equipe de AppSec de organizações que variam de menos de 500 a mais de 1.000 pessoas
- Oito setores: serviços financeiros, varejo/comércio eletrônico, saúde, governo/setor público, fabricação/produção, energia/serviços públicos e (novo em 2024) automotivo e seguros

Introdução

As APIs são frequentemente vistas como um vetor de ataque *emergente*, mesmo em meio a dados que mostram que esses ataques são predominantes e prejudiciais. Considere estas estatísticas:

- 108 bilhões de ataques de API foram registrados de janeiro de 2023 a junho de 2024, de acordo com o recente relatório SOTI (State of the Internet) da Akamai.
- "Os dados atuais indicam que a violação média de APIs leva a um vazamento de dados pelo menos 10 vezes maior do que a violação média de segurança", de acordo com o Market Guide for API Protection, da Gartner®, de maio de 2024.*
- Os ataques também estão aumentando. O SOTI também informa que os ataques a aplicativos da Web e APIs juntos aumentaram 49% entre o primeiro trimestre de 2023 e o primeiro trimestre de 2024.

Esses aumentos não são surpreendentes. Nos bastidores, as APIs facilitam a comunicação e troca de dados entre quase todas as tecnologias que impulsionam suas iniciativas digitais: ferramentas de IA generativa, aplicativos voltados para o cliente, serviços de nuvem, entre outros. No entanto, muitas APIs não são suficientemente protegidas, seja porque são criadas sem autenticação, mal configuradas ou totalmente esquecidas, o que as torna um vetor de ataque atraente e econômico para os cibercriminosos. Eles só precisam encontrar uma API vulnerável e, *pronto*, obtêm acesso direto a todos os dados que ela retorna quando chamada, que podem ser milhares de registros.

Muitas APIs não são suficientemente protegidas, o que as torna um vetor de ataque atraente e econômico para os cibercriminosos.

Em um nível elevado, nossa pesquisa mostrou que a segurança da API ainda não se tornou um elemento-chave em uma estratégia de segurança abrangente. As organizações, em sua maioria, tratam as ameaças à API como emergentes, quando os dados de ataque, bem como os impactos financeiros e o estresse das equipes que vieram à tona em nosso estudo, mostraram que elas estão crescendo em número e, muitas vezes, são bem-sucedidas. Nossas descobertas de 2024 oferecem uma visão de como os incidentes de segurança de APIs afetam outros profissionais e suas organizações. Esperamos que esses dados ajudem a posicionar sua própria equipe para avaliar melhor as proteções da API e aprimorá-las quando necessário.

Conclusões de alto nível: incidentes de API afetam o negócio e causam estresse nas equipes

As descobertas do nosso estudo de 2024 mostraram que as APIs são um vetor de ataque que está crescendo e criando desafios de segurança consideráveis para as equipes. Nossos entrevistados demonstraram um consenso notável sobre os seguintes aspectos:

- Incidentes de segurança de APIs aumentam por três anos consecutivos
- Mais de meio milhão de dólares, em média, é o que se gasta para tratar e se recuperar de incidentes relacionados à API (US$ 943.162 é o impacto financeiro médio, de acordo com nossos altos executivos entrevistados dos EUA)
- Sentir o custo humano dos incidentes de API, com o impacto do estresse e dos danos à reputação de suas equipes (especialmente o controle interno que amplia essa pressão), que é ainda maior do que os custos para corrigir os incidentes

Os entrevistados ofereceram opiniões variadas sobre a integridade de seus inventários de APIs, e essa variabilidade foi ainda mais acentuada quando dividida por função (consulte a página 11). Surpreendentemente, as empresas com inventários completos de API que também sabem quais de suas APIs retornam dados confidenciais caíram de 40%, já baixos, em 2023 para apenas 27% em 2024.

Os entrevistados também indicaram que as ferramentas tradicionais com as quais eles contam para proteger as APIs não cobrem totalmente os riscos. Essas ferramentas, como firewalls de aplicativos da Web (WAFs), gateways de API e firewalls de rede, geralmente são as primeiras a serem responsabilizadas pelo sucesso de um ataque (consulte a lista completa de causas na página 17 e uma observação sobre WAF e WAAP na página 12).

As descobertas de nosso estudo também nos permitem inferir alguns motivos principais pelos quais as estratégias de segurança de APIs ainda não receberam maior prioridade, apesar das evidências de que merecem foco. Um fator importante: a falta de alinhamento entre as principais funções de segurança quanto ao número, ao local e aos atributos de risco das APIs que precisam ser protegidas, provavelmente devido à pouca visibilidade das APIs e à ausência de uma única fonte confiável.

Também observamos uma falta de consenso entre líderes de segurança e profissionais sobre causas de ataques de API. São as ferramentas que eles usam, os erros que seus programadores cometeram no desenvolvimento ou os ataques a brechas nas inovações da IA generativa? Depende da pessoa a quem você perguntar.

Obviamente, o outro motivo pelo qual a segurança de APIs não ganhou mais destaque estrategicamente é que as equipes já estão sobrecarregadas para lidar com outras ameaças urgentes, que provavelmente também estão ocupando a maior parte do orçamento, do foco da equipe e do esforço. Vamos nos aprofundar nos resultados.

Os profissionais de segurança estão sentindo o custo humano dos incidentes de API, com os impactos do estresse e dos danos à reputação de suas equipes sendo ainda maiores do que os custos para corrigir os incidentes.

Estudo sobre o impacto da segurança de APIs – 2024
Resumo das principais descobertas

84% dos entrevistados sofreram um incidente de segurança de APIs nos últimos 12 meses

Custo médio para lidar com incidentes de API nos últimos 12 meses:

EUA	Reino Unido	Alemanha
US$ 591.404,00	£ 420.103,00	€ 403.453,00

Baixa visibilidade

Apenas 27% das empresas com inventários completos de APIs sabem quais APIs retornam dados confidenciais, em comparação com 40% em 2023.

Alto nível de estresse

Impacto nº 1 dos incidentes de API. *CISOs*: Prejudicou a reputação do nosso departamento com os líderes seniores/diretoria. *CIOs*: Aumentou o estresse e/ou a pressão da minha equipe/departamento.

Poucos testes

Apenas 13% e 18% dos entrevistados testam suas APIs em tempo real e diariamente, respectivamente, desde o desenvolvimento da API até a produção.

O custo financeiro dos incidentes de segurança de APIs exacerba o impacto em equipes e líderes. Violações dispendiosas atraem o escrutínio e podem fazer parecer, para as partes interessadas influentes, como o conselho de administração, que as equipes não estão fazendo bem seu trabalho. Isso é estressante. Na verdade, os participantes de todas as regiões geográficas citaram o estresse em suas equipes como o principal impacto de um incidente de segurança de API.

O cenário atual da segurança de APIs

Nos últimos três anos, o número de organizações que relatam incidentes de segurança de APIs tem aumentado consistentemente, atingindo uma alta de 84% em 2024 (veja abaixo). Como esses ataques a APIs afetam as organizações? O que eles estão fazendo (ou ainda não estão fazendo) para reduzir o risco? Estruturamos nossas descobertas como respostas a essas perguntas.

Os ataques a APIs estão causando um impacto significativo nas organizações e em suas equipes de segurança?

A resposta curta é "sim". Este foi o primeiro ano em que coletamos dados sobre o impacto financeiro de um incidente de segurança de APIs, e o resultado foi significativo: o custo, em média, para remediar incidentes de API (incluindo reparos no sistema, tempo de inatividade, taxas legais, multas e quaisquer outras despesas associadas) para os 84% que sofreram esses incidentes nos últimos 12 meses foi de:

- **US$ 591.404,00** nos EUA
- **£ 420.103,00** no Reino Unido
- **€ 403.453,00** na Alemanha

Algumas funções consideraram os custos muito mais altos, especialmente os entrevistados da diretoria executiva dos EUA, que relataram US$ 943.162,00, quase 60% a mais do que a média do total de entrevistados nos EUA.

Você sofreu algum incidente de segurança de APIs nos últimos 12 meses?

Ano	Total	EUA	Reino Unido	Alemanha
2022	76%	75%	77%	–
2023	78%	85%	69%	–
2024	84%	83%	83%	84%

Não importa o número exato, o custo financeiro dos incidentes de segurança de APIs exacerba os impactos humanos. Violações dispendiosas atraem o escrutínio e podem fazer parecer, para as partes interessadas influentes, como o conselho de administração, que as equipes não estão fazendo bem seu trabalho. Isso é estressante. Na verdade, os participantes de todas as regiões geográficas citaram o "estresse" (especificamente, o estresse em suas equipes) como o principal impacto de um incidente de segurança de APIs, seguido por "prejudicou a reputação do nosso departamento com os líderes seniores e/ou com o conselho de administração", com "custos para resolver" em terceiro lugar. Notavelmente, os impactos internos que mais afetam o moral reaparecem e dominam os três impactos inferiores, que estão praticamente empatados (veja abaixo).

Os resultados foram semelhantes quando divididos por setor: "Aumento do estresse e/ou da pressão para a equipe após uma violação de API" também foi o impacto mais bem classificado em quatro dos oito setores pesquisados (veja a tabela na página 9). Isso inclui os serviços financeiros, que notavelmente relataram o maior impacto financeiro de todos os setores, com US$ 832.801,00.

Principais impactos citados, decorrentes dos incidentes de segurança de APIs

1. Aumento do estresse e/ou pressão para a equipe ou departamento – **27%**
2. Danos à reputação do departamento diante de líderes seniores e/ou o conselho de diretores – **26,6%**
3. Custos incorridos para ajudar a corrigir o problema – **25,8%**
4. Multas regulatórias – **25,4%**
5. Perda da fidelidade dos clientes e rotatividade de contas – **25%**
6. Perda de produtividade – **24,1%**
7. Perda de confiança e reputação – **23,8%**
8. Perda da fidelidade dos funcionários – **23,8%**
9. Levou a um maior escrutínio interno da nossa equipe/departamento pela empresa – **23,5%**

Com base na pergunta: Quais custos e/ou impactos, se houver, os incidentes com a segurança de APIs tiveram em sua empresa?
(Selecione até 3); n=1.207

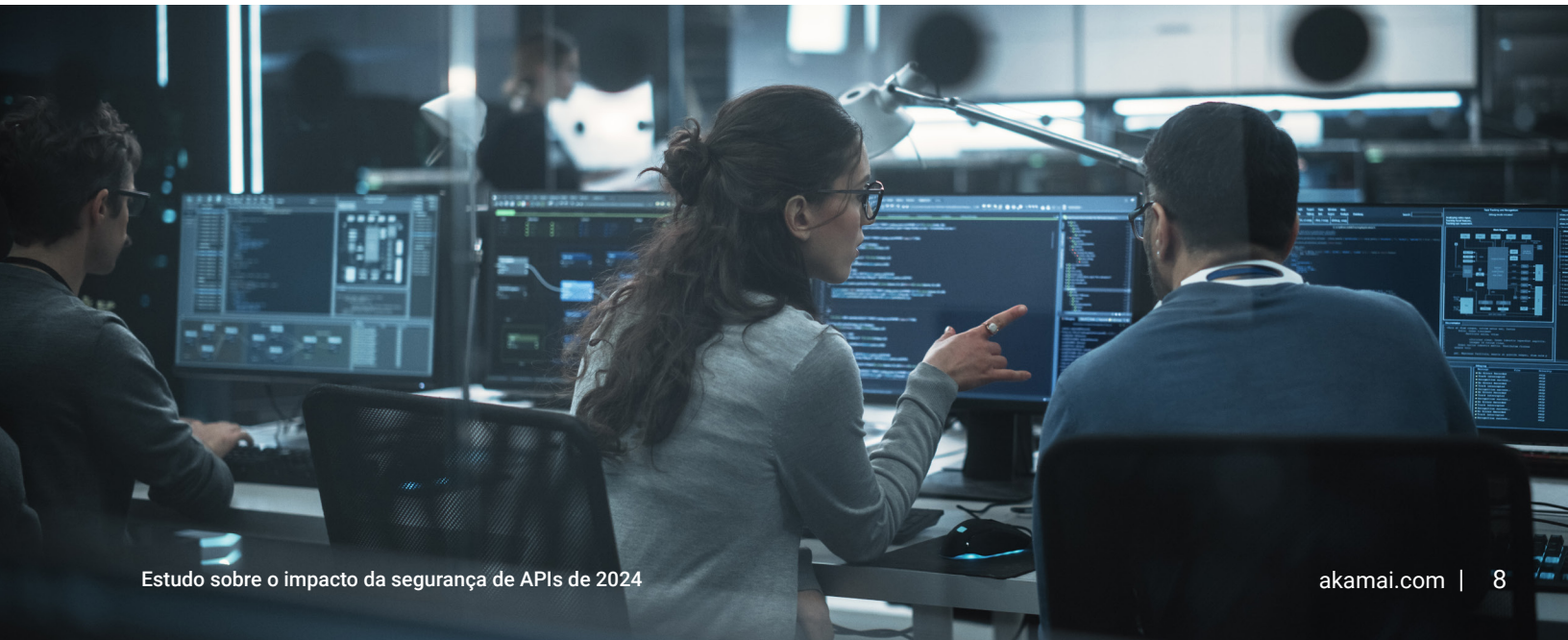
A relação entre os custos financeiros e humanos dos ataques a APIs também ficou evidente em alto e bom som nas respostas dos líderes de TI e segurança sobre os impactos dos incidentes (cada entrevistado podia escolher até três). Uma área que mostrou consenso geral entre todas as funções em todas as regiões foi a de que os maiores impactos dos incidentes de segurança de APIs são sobre a equipe.

- Os dois principais dados relatados pelos CISOs: "prejudicou a reputação do nosso departamento com os líderes seniores/conselho de administração" e "perda da fidelidade do cliente e rotatividade de clientes", revelaram um empate exato entre os impactos humanos e financeiros em 31%.
- Da mesma forma, os principais impactos relatados pelos CIOs indicaram um empate entre "maior estresse e/ou pressão para minha equipe/departamento" e "custos para resolver", com 34%.

Esses resultados fazem sentido para CISOs e CIOs: e se as equipes que eles lideram continuarem a ser atingidas por incidentes de segurança que criam condições de trabalho ruins, estouram os orçamentos e incomodam os clientes? Esses líderes não querem ver o talento de qualidade sair ou a reputação de seu departamento despencar. Adicione a isso pressões financeiras, como custos de remediação e/ou rotatividade do cliente, e o estresse sobre CISOs e CIOs aumenta consideravelmente. Na verdade, "perda da fidelidade do cliente e da rotatividade de contas" foi o impacto de classificação mais alta de um incidente de segurança de APIs para os entrevistados dos setores de seguros e automotivo (veja a tabela na próxima página para obter mais descobertas do setor).

As principais respostas para as demais funções foram:

- CTO, 30%, "perda da fidelidade dos funcionários"
- Profissional de segurança sênior, 27%, "Prejudicou a reputação do nosso departamento com nossos líderes seniores/conselho"
- Equipe da AppSec, 31%, "levou ao aumento do estresse e da pressão para minha equipe/departamento"



Principais impactos citados de incidentes de segurança de APIs por setor	
Automotivo	Perda da fidelidade dos clientes e rotatividade de contas – **33%**
Energia/serviços de utilidade pública	Danos à reputação do departamento diante dos nossos líderes seniores e/ou o conselho de diretores – **36%**
Serviços financeiros	Empate: Levou a um aumento do estresse/pressão para a minha equipe/departamento e multas regulatórias – ambos **29%**
Governo/Setor Público	Aumentou o estresse/pressão para minha equipe/departamento – **29%**
Área da saúde	Empate: Perda de confiança e reputação e perda de produtividade – ambos **29%**
Seguro	Perda da fidelidade dos clientes e rotatividade de contas – **28%**
Fabricação	Aumentou o estresse e ou pressão para minha equipe/departamento – **34%**
Varejo/comércio eletrônico	Aumentou o estresse e ou pressão para minha equipe/departamento – **29%**

Com base na pergunta: Quais custos e/ou impactos, se houver, os incidentes com a segurança de APIs tiveram em sua empresa? (Selecione até 3); n=1.207

Há visibilidade adequada das APIs e dos riscos potenciais?

Não. Mais precisamente, na verdade, piorou. Este ano, a porcentagem de participantes que têm um inventário completo de APIs e também sabem quais APIs trocam dados confidenciais caiu de 40%, um índice que já era baixo, em 2023 para apenas 27% em 2024. (Essa descoberta pode ter um lado positivo, se considerarmos que mais organizações estão tentando realizar um inventário completo, mas não têm as ferramentas necessárias para localizar cada API e identificar a atividade que está ocorrendo em cada uma delas.)

A porcentagem de participantes que têm um inventário completo de APIs e também sabem quais APIs trocam dados confidenciais **caiu de 40%, um índice que já era baixo, em 2023** para apenas **27% em 2024**.

Cenário atual dos inventários de API e conhecimento, todos os entrevistados

	2024	2023
Sim, **e nós sabemos** quais retornam dados confidenciais	27%	40%
Sim, **mas não sabemos** quais retornam dados confidenciais	43%	32%
Temos um inventário parcial de nossas APIs **e sabemos** quais retornam dados confidenciais	23%	24%
Temos um inventário parcial, **mas não sabemos** quais retornam dados confidenciais	6%	4%
Não, **nós não** temos nenhum inventário	1%	–

Com base na pergunta: Você tem um inventário completo de suas APIs e sabe quais retornam dados confidenciais? (Selecione uma das cinco opções); n=1.207

Analisando os líderes dos três países e dos oito setores pesquisados, os CIOs tendem a acreditar, por uma margem significativa em relação aos CISOs, que suas organizações têm inventários completos de APIs. No nível do profissional, tanto os profissionais de segurança seniores quanto os membros da equipe de AppSec estão amplamente alinhados com a visão do CIO médio de que todas as APIs são contabilizadas.

Mas como as cinco funções se comparam, em média, quando se trata de saber (ou não saber) quais de suas APIs retornam dados confidenciais quando chamadas? A resposta é importante, pois muitas dessas chamadas são provenientes de fontes mal-intencionadas, buscando explorar vulnerabilidades comuns de API.

Quatro tipos de APIs não gerenciadas que os invasores usam para acessar dados

1. As **APIs sombra** (também conhecidas como "APIs não documentadas") existem e operam fora dos canais oficiais monitorados de uma organização.
2. As **APIs não autorizadas** ou mal-intencionadas representam um risco de segurança para um sistema ou rede.
3. As **APIs zumbi** incluem qualquer API que tenha sido deixada em execução mesmo depois de ser substituída por novas versões ou por outras APIs.
4. As **APIs obsoletas** não são mais recomendadas para uso, devido a alterações na API.

Essas descobertas oferecem algumas conclusões curiosas sobre a visibilidade do risco das APIs. A maioria dos CISOs e CTOs respondeu que tinha um inventário completo *sem* saber quais APIs retornam informações confidenciais (vamos nos referir a esse conhecimento como "conhecimento de dados confidenciais") ou tinha um inventário parcial *com* conhecimento de dados confidenciais.

A maioria dos CIOs relatou ter um inventário completo de APIs e, desses CIOs, 42,9% relataram também ter conhecimento completo de dados confidenciais, enquanto 36,3% relataram não ter esse conhecimento. Os profissionais de segurança seniores estavam alinhados com os CIOs (75% relataram um inventário completo), mas a situação *se inverteu* em relação ao conhecimento de dados confidenciais: 32,5% dos profissionais de segurança seniores disseram ter conhecimento de dados confidenciais, e 42,5% disseram que não.

Por fim, os membros da equipe de AppSec, provavelmente os que têm mais conhecimento prático de todos os entrevistados, relataram a maioria mais acentuada em todas as cinco funções. Quase metade relatou um inventário completo sem conhecimento de dados confidenciais. A outra metade foi dividida aproximadamente entre:

- Inventário completo com conhecimento completo de dados confidenciais
- Inventário parcial com conhecimento total de dados confidenciais dessas APIs

Podemos ver que a medição de inventários ainda não foi padronizada o suficiente para produzir uma contagem de API de fonte única. Dada a variabilidade, também é provável que mais empresas com inventários completos *não* tenham conhecimento total de dados confidenciais. Saber quais APIs retornam dados confidenciais é sempre significativo. No entanto, um inventário parcial pode ser o mais perigoso, uma vez que as APIs sombra, não autorizadas, zumbi e obsoletas são altamente visadas, mal protegidas e geralmente passam despercebidas pelas ferramentas de segurança tradicionais.

Cenário atual dos inventários de API e conhecimento, discriminados por função

	CISO	CIO	CTO	Profissional sênior de segurança	AppSec
Temos um inventário completo **e sabemos** quais retornam dados confidenciais	17,2%	42,9%	16,5%	32,5%	26,4%
Temos um inventário completo, **mas não** sabemos quais retornam dados confidenciais	41,4%	36,3%	34,8%	42,5%	47,4%
Temos um inventário parcial de nossas APIs **e sabemos** quais retornam dados confidenciais	32,5%	15,4%	39,9%	18,3%	20,4%
Temos um inventário parcial, **mas não sabemos** quais retornam dados confidenciais	8,3%	5,5%	8,2%	5,8%	5,2%

Com base na pergunta: Você tem um inventário completo de suas APIs e sabe quais retornam dados confidenciais? (Selecione uma das cinco opções); n=1.207

Em um momento em que as APIs não gerenciadas se espalharam e provaram ser evasivas para as ferramentas de segurança tradicionais, essas descobertas revelam uma lacuna de segurança comum que torna o vetor de ataque de APIs mais atraente para os agentes de ameaças.

Obviamente, as APIs não gerenciadas são apenas um dos pelo menos cinco atributos de APIs que uma equipe de segurança precisa ver e avaliar. A variedade inclui:

- **APIs com vulnerabilidades conhecidas** que não foram corrigidas
- **APIs não gerenciadas ou esquecidas (** sombra, não autorizada, zumbi, obsoleta)
- **APIs com exposições externas** (como credenciais, chaves e variáveis fora do seu controle)
- **APIs com erros de operador** (configurações incorretas de segurança em infraestrutura e serviços)
- **APIs com vulnerabilidades e bugs desconhecidos** que os agentes de ameaças identificam e exploram

No mínimo, o intervalo de respostas entre funções relacionadas aos inventários de API e a visibilidade das vulnerabilidades de API sugere que:

- As empresas ainda estão confiando em produtos de segurança que não são projetados especificamente para descobrir e proteger APIs, especialmente as de alto risco e não gerenciadas.
- Os departamentos de segurança ainda precisam definir os atributos de risco de uma API que precisam ser vistos e avaliados ou criar um consenso entre suas várias unidades de negócios, equipes de desenvolvedores e fornecedores sobre a estratégia de descoberta e inventário de APIs.

Abordar essas desconexões pode ser um ótimo primeiro passo para defender efetivamente o investimento em recursos mais fortes para proteger e proteger todas as APIs (consulte "Como adotar uma postura mais madura para a segurança de APIs" na página 18). Da forma como está, o foco e a defesa necessários para receber alocação orçamentária muitas vezes não existem para a segurança de APIs, dificultando a priorização e o financiamento de iniciativas que poderiam melhorar não apenas as defesas de APIs e aplicativos Web, mas a postura geral de segurança de uma organização.

Melhor juntos: proteções específicas de WAAP e API

Projetada para identificar e atenuar rapidamente as ameaças de vários vetores de ataque, a proteção de APIs e aplicativos Web (WAAP) amplia as proteções tradicionais de um WAF. **Uma solução de segurança de APIs, trabalhando em conjunto, estende as proteções ainda mais além do firewall para criar a defesa mais forte possível**.

As APIs estão sendo testadas com frequência suficiente para reduzir o risco de abuso ou violações?

Não, muitas vezes não o suficiente. As APIs voltadas para o público que estão mal configuradas, sem controles de autenticação, incorporadas com erros de codificação ou que abrigam outros riscos evitáveis são exatamente o que os invasores estão procurando, e esses invasores estão cada vez melhores em encontrá-las.

Portanto, toda vez que sua equipe de desenvolvimento envia APIs como essas para a produção, sem testá-las exaustivamente antes, é como se estivesse plantando involuntariamente uma carga de trabalho futura para sua equipe de segurança (uma carga de trabalho que, sem dúvida, é urgente e contribui para o que nossas descobertas revelaram sobre o estresse).

Mas observe que dissemos riscos *evitáveis*.

Se você testar as APIs no desenvolvimento, com frequência e eficiência por meio da automação, *antes* de serem lançadas na produção, sua organização, seus desenvolvedores e sua equipe de segurança estarão em vantagem. E essa vantagem é imediata em termos de redução do estresse causado por vulnerabilidades desconhecidas e da certeza de que os erros não serão encontrados na produção, quando são exponencialmente mais difíceis e caros de corrigir.

Até o momento, no entanto, os testes não estão sendo aplicados, de acordo com nossos entrevistados. Os testes frequentes de API, em tempo real e diários, diminuíram em relação ao ano passado, em todo o ciclo de vida da API, inclusive na produção.

- Em 2023, 18% dos entrevistados dos EUA e do Reino Unido disseram que executavam testes em tempo real. Entre a mesma coorte **em 2024, esse número caiu para 13%**.
- Em 2023, 37% dos entrevistados nos EUA e no Reino Unido disseram que executavam testes pelo menos uma vez por dia. **Em 2024, apenas 13% executaram testes com essa frequência**, embora 26% dos entrevistados alemães realizassem testes uma vez por dia.

Se você testar as APIs no desenvolvimento, com frequência e eficiência por meio da automação, *antes* de serem lançadas na produção, sua organização, seus desenvolvedores e sua equipe de segurança estarão em vantagem.

O teste semanal de API é mais comum para os participantes em todas as regiões geográficas, mas em nenhuma delas chegou a 50%. Além disso, a frequência dos testes de API variou muito entre as regiões geográficas, de *tempo real* a *nenhum teste*. Notavelmente, apenas 6% dos entrevistados responderam "Nós só testamos a segurança de APIs antes de liberá-las para produção". O ideal é que as equipes passem a fazer testes contínuos durante todo o ciclo de vida da API.

O que significa testar APIs continuamente?

As vulnerabilidades podem ser introduzidas nas APIs em qualquer ponto do seu ciclo de vida, desde erros de codificação cometidos no desenvolvimento até falhas de segurança que surgem quando os usuários começam a interagir com a API. É por isso que, idealmente, os testes de API são feitos durante o desenvolvimento (shift-left) e também continuamente enquanto estão em produção (shift-right).

Exemplos de testes de API em desenvolvimento:

- Executar testes automatizados que simulam tráfego malicioso.
- Inspecionar as especificações de APIs em relação às políticas de governança estabelecidas.
- Executar teste de APIs sob demanda ou como parte de um pipeline de CI/CD.

Exemplos de testes de API na produção:

- Monitorar continuamente o tráfego da API e avaliar metadados de tráfego.
- Identificar alterações nas APIs existentes por meio de análise automatizada.
- Encontrar problemas em tempo real e remediar antes que os atacantes notem.

Seus protocolos de segurança de APIs atendem aos mandatos de conformidade?

Em muitos regulamentos de proteção de dados, as APIs não são mencionadas pelo nome, mas os requisitos se concentram claramente na segurança dos aplicativos e da infraestrutura em que as APIs operam. Os mandatos de conformidade estão sempre evoluindo, e outras regulamentações estão a caminho com implicações de API, incluindo a Lei Americana de Direitos de Privacidade (atualmente em projeto de lei) e a Lei de Resiliência Cibernética da UE.

Os regulamentos e as estruturas com implicações atuais e diretas para a segurança de APIs incluem:

- PCI DSS (atualmente v4.0.1)
- General Data Protection Regulation (GDPR)
- Lei de Resiliência Operacional Digital (DORA)
- Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA)
- Diretiva de Segurança de Redes e Informações (NIS2)

A segurança de APIs recebe atenção, mas permanece em segundo plano

Se os ataques às APIs são caros e geram multas, se contribuem para a perda de confiança dos clientes, se causam estresse crescente na equipe e perda de credibilidade junto aos conselhos de administração das empresas, por que as equipes não tomam medidas mais decisivas? As respostas para as seguintes perguntas nos ajudam a entender.

Como as diferentes funções empresariais priorizam a segurança de APIs?

Pedimos aos nossos participantes que identificassem suas principais prioridades de segurança cibernética para os próximos 12 meses, permitindo que eles selecionassem até três em uma lista extensa (veja a tabela). As seis principais prioridades diferiam em apenas 2% e as seis últimas em apenas 1%, o que sugere que as prioridades são semelhantes em todas as regiões geográficas e setores e que as equipes muitas vezes são obrigadas a fazer malabarismos com todas elas.

Em alguns setores, no entanto, as diferenças de classificação centrais para as APIs contam uma história diferente. Por exemplo, o setor de energia/serviços de utilidade pública classifica a segurança de APIs como a prioridade mais baixa em relação a todos os outros setores, com 13,2% (e abaixo da média de 18% de todos os participantes da pesquisa). Ao mesmo tempo, o setor de energia/serviços de utilidade pública também teve a maior taxa de notificação de incidentes de segurança de APIs, 91%, a maior de todos os oito setores e acima da média de 84%. O que está acontecendo aqui? A baixa prioridade dada à segurança de APIs e a alta taxa de ataque.

As principais prioridades de segurança citadas nos próximos 12 meses

1. Defesa contra ataques alimentados pela IA generativa – **21,2%**
2. Defesa contra ransomware – **20,5%**
3. Segurança da autenticação para usuários da força de trabalho – **19,7%**
4. Gerenciamento e proteção dos segredos do desenvolvedor – **19,6%**
5. Proteção de pontos de extremidade – **19,2%**
6. Soluções de segurança na nuvem – **19,1%**
7. Proteção do acesso privilegiado à TI – **18,6%**
8. Prevenção contra perda de dados – **18,6%**
9. Segurança de APIs contra agentes de ameaças – **17,9%**
10. Proteção de aplicativos – **17,7%**
11. Informações de segurança e gerenciamento de eventos – **17,6%**
12. Resposta e gestão de incidentes – **17,6%**

Com base na pergunta: Quais são as principais prioridades de segurança cibernética da sua empresa nos próximos 12 meses? (Favor selecionar até 3); n=1.207

Dados mais reveladores surgiram do corte dos dados de resposta por função:

- Os CISOs citaram os ataques assistidos pela IA generativa e a proteção de API como os mais altos, com **25,5%** e **24,8%**, respectivamente.
- A equipe de AppSec se alinhou com os CISOs, citando os ataques assistidos pela IA generativa como sua maior prioridade, com **22,5%**.
- Tanto os CIOs quanto os CTOs se concentraram no acesso privilegiado, e os CTOs empataram na resposta a incidentes.
- Somente os profissionais de segurança seniores classificaram o ransomware como sua maior prioridade.

Essas diferenças nos levam novamente a fazer perguntas como: Por que as diferentes camadas da organização de segurança de TI parecem estar operando a partir de manuais diferentes? E por que os principais líderes de segurança e os funcionários da linha de frente parecem estar alinhados quanto ao grande papel que as APIs, e seus riscos, desempenham nos ataques assistidos pela IA generativa, enquanto outras funções não estão?

Talvez seja porque os CISOs veem suas unidades de negócios implementando apressadamente inovações como aplicativos com tecnologia de IA generativa para atender à demanda, enquanto os membros da equipe de AppSec veem o mesmo. Somente *eles* conhecem a extensão das incógnitas em relação às vulnerabilidades dos componentes de IA (como LLMs) que tocam em dados confidenciais. Além disso, essa equipe conhece em primeira mão os muitos sinais de alerta de que os invasores estão criando a IA generativa em seus métodos de ataque.

Mas a principal razão pode ser a mais simples: as comunicações de cima para baixo e de baixo para cima não acontecem com a frequência necessária, especialmente em grandes empresas, o que leva a uma desconexão entre as prioridades do topo e o que as equipes *precisam* fazer no dia a dia.

Por fim, vamos comparar as principais prioridades de segurança cibernética dos entrevistados com as causas que eles deram para seus incidentes de segurança de APIs. Conforme mostrado na página 17, três das causas mais citadas referem-se a ferramentas tradicionais de segurança de APIs que não conseguiram detectar problemas de API. A comparação oferece uma boa oportunidade para iniciar uma discussão sobre como as soluções de descoberta e teste de APIs poderiam melhorar não apenas a segurança de APIs, mas quase todas as outras prioridades de segurança.

Em outras palavras, se as ferramentas corretas de segurança de APIs puderem proteger não apenas as APIs, mas também melhorar a segurança de campos como dados, nuvem e aplicativos, isso fará com que a segurança de APIs não pareça um campo de nicho isolado para as partes interessadas. Falar sobre o panorama geral pode facilitar a obtenção de aprovação para elevar as APIs na lista de prioridades.

Se as ferramentas corretas de segurança de APIs puderem proteger não apenas as APIs, mas também melhorar a segurança de campos como dados, nuvem e aplicativos, isso fará com que a segurança de APIs não pareça um campo de nicho isolado para as partes interessadas.

A falta de alinhamento em relação aos incidentes de segurança de APIs indica não haver uma única fonte de verdade?

Destacamos as diferenças entre a diretoria-executiva e a equipe da linha de frente em suas prioridades gerais de segurança, e essas diferenças persistem em questões mais específicas das ameaças de APIs. Por exemplo, os CIOs estão alinhados com a equipe de AppSec em termos de conhecimento sobre os ataques à API (cerca de 88% em cada função relatam ter sofrido incidentes). Enquanto isso, o CISO, o CTO e o profissional sênior de segurança ficaram cerca de oito pontos percentuais abaixo, com cerca de 80% informando que haviam sofrido incidentes.

A causa mais citada por trás dos incidentes de segurança de APIs também variou de acordo com a função, com a maioria dos CISOs e profissionais de segurança seniores citando que o gateway de APIs não detectou o incidente, enquanto as outras três funções apontaram um culpado diferente:

- CISO: o gateway da API não detectou o problema – **26.8%**
- CIO: exposição não intencional à internet – **28.6%**
- CTO: o WAF não detectou o problema – **25.9%**
- Profissional de segurança sênior: o gateway da API não detectou o problema – **23.3%**
- Equipe AppSec: configuração incorreta da API – **23.2%**

Principais causas citadas de incidentes de segurança de APIs, todos os respondentes

1. A API tinha exposição não intencional à internet – 21,8%
2. O firewall de aplicativos da Web não detectou o problema – 21,8%
3. O gateway da API não detectou o problema – 20,2%
4. APIs em ferramentas/tecnologias de IA generativa, por exemplo, LLMs – 20%
5. Configuração incorreta da API – 19,9%
6. O firewall de rede não detectou o problema – 19,6%
7. Ferramenta/serviço de tecnologia bem conhecida, por exemplo, Microsoft – 19,2%
8. Vulnerabilidade devido a erros de codificação da API – 19,1%
9. APIs não gerenciadas, por exemplo, APIs inativas ou zumbi – 18,9%
10. Falta de controles de autenticação de API – 18,8%
11. Vulnerabilidades de autorização – 18,7%
12. Solução de software descarregada da internet – 17,6%
13. Solução de software de nível médio, por exemplo, Slack – 16,3%

Com base na pergunta: Em sua opinião, quais são as causas dos incidentes de segurança de APIs que sua organização sofreu? (selecione até 3); n=1.207

O custo relatado dos incidentes de segurança de APIs também mostrou uma falta de alinhamento das funções mais seniores para as menos seniores, embora seja importante observar que o corte dos dados por função e região resulta naturalmente em um tamanho de amostra menor. Ainda assim, as diferenças entre esses subconjuntos são dignas de nota, especialmente nos EUA, onde os CIOs e CTOs informaram que o custo dos incidentes é de cerca de US$ 1 milhão e os CISOs de cerca de US$ 737 mil, enquanto os profissionais de segurança seniores e a equipe de AppSec informaram cerca de US$ 375 mil e US$ 444 mil, respectivamente.

No Reino Unido, os custos foram, em geral, mais alinhados entre subconjuntos específicos de funções, embora os membros da equipe de AppSec tenham relatado o valor mais alto, de £ 749.000, e os CISOs, o mais baixo, de £ 190.000. (As funções intermediárias variaram de £ 374.000 a £ 222.000, de cima para baixo.) A disparidade da Alemanha em relação aos relatórios de custos foi semelhante à do Reino Unido, com a estimativa mais alta sendo feita pela equipe com papel mais prático e de menor classificação, no valor de € 345.000, e o custo mais baixo pelos CISOs de mais alto escalão, no valor de £ 197.000 (resultados opostos aos dos EUA). Uma área que mostrou consenso geral entre todas as funções em todas as regiões foi a de que os maiores impactos dos incidentes de segurança de APIs são sobre a equipe (veja os Impactos, página 7).

Como adotar uma postura mais madura para a segurança de APIs

Conforme mencionado, nossas descobertas deixam claro que os membros das equipes de segurança em diferentes estratos da organização não estão vendo a segurança de APIs da mesma forma. Mas há um outro lado: O que também está claro é que eles têm um terreno em comum para se basear. Eles conhecem os custos (financeiros e humanos) e reconhecem que as ferramentas com as quais contam não são suficientes.

Como a segurança de APIs tem um impacto tão grande sobre as organizações, suas próximas etapas podem ser decidir o que desenvolver, o que mudar e mostrar aos líderes como a segurança de APIs pode ajudar no resultado final. Obter alinhamento dentro do seu departamento de segurança, do CISO à equipe de AppSec, sobre como priorizar a segurança de APIs é um bom ponto de partida, seguido pela promoção de uma comunicação aberta entre a liderança e os membros da equipe de AppSec da linha de frente, bem como as camadas gerenciais intermediárias.

Medidas que você pode tomar

Para encerrar nosso estudo, reunimos uma série de passos progressivos que sua equipe de segurança pode usar para iniciar ou construir sua estratégia de segurança de APIs e avançar para uma proteção de API madura.

1 Comece com a descoberta e a visibilidade da API

Para realizar um inventário completo de todo o seu patrimônio de APIs, procure ferramentas com uma abordagem automatizada para descobrir APIs e os microsserviços que elas suportam. A extensão da cobertura é fundamental, já que APIs não gerenciadas (veja a tabela na página 10) são um alvo principal para os agentes de ameaças.

2 Invista em testes

Selecione uma solução de segurança de APIs que permita testar facilmente se as APIs estão codificadas corretamente para desempenhar a função pretendida. O ideal é que o teste seja realizado antes da implantação, mas também é importante testar todas as APIs já em produção com análise em tempo real do tráfego e das possíveis vulnerabilidades.

3 Realize a documentação completa de APIs

É essencial auditar todo o seu ambiente de API para identificar APIs mal configuradas ou outros erros. Seus recursos de auditoria também devem garantir a documentação adequada de cada API e se ela contém dados confidenciais ou não possui controles de segurança adequados. Isso também o ajuda a se preparar para as exigências de conformidade que envolvem a segurança de APIs, implícita ou explicitamente (consulte a página 14).

4 Use detecção de tempo de execução

Uma solução de segurança de APIs com detecção automatizada de tempo de execução permite diferenciar entre atividade de API "normal" e "anormal". Ao monitorar as interações da API dessa forma, você pode detectar comportamentos que indicam uma ameaça em tempo real e tomar medidas.

5 Responda a comportamentos suspeitos

Ao integrar uma solução de segurança de APIs à sua pilha de segurança existente (por exemplo, WAF ou WAAP), você poderá detectar comportamentos de alto risco e bloquear o tráfego suspeito antes que ele possa acessar recursos críticos.

6 Investigue e busque ameaças

No estágio mais maduro da segurança de APIs, você usará a análise forense dos dados de ameaças anteriores para saber se os alertas identificaram corretamente as ameaças e se surgiram padrões que permitem a caça proativa de ameaças usando uma combinação de ferramentas sofisticadas e inteligência humana.

Conclusão

O relatório deste ano deixou bem claro que a segurança, neste caso, a segurança de APIs, não se trata apenas de listas de ameaças ou ferramentas; trata-se de pessoas.

Nosso estudo confirma que as equipes de segurança estão sobrecarregadas e que a noção de adicionar um vetor de ataque totalmente novo à carga de trabalho da sua equipe pode parecer assustadora. Mas a proliferação de APIs não vai parar, e tomar medidas para proteger suas APIs tem um forte efeito cascata em várias outras prioridades, como as vulnerabilidades da IA generativa (para proteger as APIs que trocam dados com LLMs) e a segurança na nuvem (para reduzir o risco em cada API incluída nas cargas de trabalho que você migrar).

Acreditamos profundamente que ser proativo em relação à segurança de APIs não apenas protege a sua empresa, mas também posiciona a sua equipe para se tornar muito mais crível e confiável em sua visão desse vetor de ataque crítico entre colegas, líderes e a diretoria. Isso traz o enorme benefício de reduzir os níveis de estresse da sua equipe, que, segundo nosso estudo, é altamente afetada por incidentes de segurança de APIs e pelo escrutínio e pela perda de fidelidade que eles geram, tanto nos colegas de trabalho quanto nos clientes.

Tomar medidas agora também facilita preventivamente o planejamento e a geração de relatórios de conformidade, sem mencionar a prevenção oportuna de multas regulatórias. Por que não começar?

- Se você estiver pronto para considerar as próximas etapas de sua jornada rumo a uma postura madura de segurança de APIs, recomendamos que comece com nosso white paper, Fundamentos de segurança de APIs.
- Se você estiver pronto para uma conversa sobre seus desafios e como podemos ajudar, é fácil solicitar uma demonstração personalizada do Akamai API Security.

Sobre o Estudo sobre o impacto da segurança de APIs

A pesquisa para o Estudo sobre o impacto da segurança de APIs de 2024 foi realizada pela Opinion Matters entre 12 de junho de 2023 e 7 de julho de 2024. Sua equipe pesquisou um total de 1.207 entrevistados, com a seguinte divisão por residência da empresa: 404 do Reino Unido, 402 dos EUA e 401 da Alemanha. Um terço dos entrevistados eram CIOs ou CISOs; um terço eram profissionais de segurança seniores; e um terço era de equipes de segurança de aplicativos que trabalhavam em empresas de menos de 500 a mais de 1.000 pessoas, em oito setores principais: automotivo, serviços financeiros, varejo/comércio, saúde, seguros, governo/setor público, manufatura e energia/serviços de utilidade pública.

A Opinion Matters respeita e emprega membros da Market Research Society e segue o código de conduta da MRS e os princípios da ESOMAR. A Opinion Matters também é membro do British Polling Council.

Créditos

Redator principal
Annie Brunholzl

Editor gerente
John Natale

Diretor de pesquisa
Mitch Mayne

Editor de redação
Randi Kravitz

Promoções
Barney Beal

Marketing e publicação
Georgina Morales Hampe

Análise e contribuição do assunto
Pam Cobb
Jim Lubinskas
Kimberly Gomez
Stas Neyman

State of the Internet/Security

Leia as edições anteriores e fique por dentro das próximas versões dos aclamados relatórios State of the Internet/Security da Akamai. **akamai.com/soti**

Pesquisa sobre ameaças da Akamai

Mantenha-se em dia com as mais recentes análises de inteligência de ameaças, relatórios de segurança e pesquisas sobre cibersegurança. **akamai.com/security-research**

Akamai API Security

Saiba como a Akamai protege as APIs durante todo o seu ciclo de vida, desde o desenvolvimento até a produção, com recursos críticos em descoberta de APIs, gerenciamento de postura, proteção de tempo de execução e testes de segurança de API. **https://www.akamai.com/products/api-security**