ESTUDO SOBRE O IMPACTO DA SEGURANÇA DE APIS DE 2024

Governo

Os incidentes de API estão aumentando. Saiba como o governo está lidando com desafios críticos de segurança e descubra o que sua organização pode fazer para se proteger.

Em um cenário em que as APIs são protagonistas, governos de todo o mundo enfrentam crescente pressão para garantir a proteção dos serviços digitais. Em 2024, 86,1% das organizações do setor público relataram um incidente de segurança de APIs, um aumento significativo em relação aos 76,8% no ano anterior. Esse aumento coloca o setor público acima da média geral de 84% de todos os setores, evidenciando a escalada do problema. Desde o cumprimento dos requisitos do GDPR (General Data Protection Regulation, Regulamento Geral de Proteção de Dados) até a imposição da residência de dados em sistemas multinuvem e as agências precisam, mais do que nunca, ampliar a visibilidade, fortalecer a governança e garantir resiliência integrada.

O verdadeiro custo dos incidentes de segurança de APIs

As agências governamentais estão ampliando o uso de APIs para viabilizar serviços digitais, otimizar o compartilhamento de dados entre instituições e impulsionar a modernização da infraestrutura. Mas essa expansão trouxe nova gama de vulnerabilidades que criminosos digitais estão ávidos para explorar. Mecanismos de autenticação deficientes, configurações incorretas de APIs e falta de conscientização sobre riscos críticos deixaram o setor governamental especialmente vulnerável a violações de segurança de APIs. As consequências desses incidentes vão muito além do roubo de dados, comprometendo a continuidade das operações, a conformidade regulatória e, sobretudo, a confiança pública.

Como sabemos disso? A Akamai entrevistou mais de 1.200 profissionais de TI e segurança, desde diretores de segurança da informação até equipes de segurança de aplicativos, para entender suas experiências com ameaças relacionadas a APIs.

Aqui filtramos nossos resultados para os entrevistados do setor governamental, que indicaram os principais impactos de seus incidentes de segurança de APIs:

- "Aumento do estresse e/ou pressão para a equipe ou departamento" (28,5%)
- "Danos à reputação do departamento diante de líderes seniores e/ou o conselho de administração" (27,2%)
- "Multas regulatórias" (25,2%)

Essas consequências interligadas são fáceis de compreender, considerando que seus colegas estimaram o custo para lidar com incidentes de API em US$ 717.500, ou seja, 21,3% superior à média dos oito setores pesquisados.

Continue lendo para obter insights do setor a partir do Estudo sobre o impacto da segurança de APIs de 2024.

À medida que ataques aumentam, a visibilidade é uma preocupação crescente

Ao serem questionados sobre as principais causas de seus incidentes de segurança de APIs, seus colegas apontaram duas vulnerabilidades críticas:

- Falta de controles de autenticação de APIs (25,2%)
- Ferramentas tradicionais usadas para a segurança de APIs (25,2%)

Mesmo diante de evidências claras sobre os impactos das ameaças às APIs, desde custos elevados de correção até a perda de confiança, nossas descobertas indicam que a segurança de APIs ainda não é uma prioridade para muitas equipes governamentais. Na verdade, a segurança de APIs ocupa o sexto lugar entre as prioridades de cibersegurança para o próximo ano, com 17,9%.

86,1% das organizações governamentais relataram incidentes de segurança de APIs em 2024, um aumento significativo em relação aos 76,8% registrados em 2023

US$717.500 é o custo financeiro médio de uma violação de segurança de API para organizações governamentais nos Estados Unidos, excedendo a média de US$591.404 para todos os setores

66,9% das entidades governamentais mantêm um inventário de APIs, mas apenas 18,5% têm visibilidade total sobre quais APIs lidam com dados confidenciais, o que deixa as informações críticas em risco

Os três principais impactos

1. **Aumento do estresse e/ou da pressão sobre a equipe de segurança**
2. **Danos à reputação da equipe diante de líderes e conselhos**
3. **Multas regulamentares associadas à não conformidade**

Fonte:
Estudo sobre o impacto da segurança de APIs de 2024

Para agências governamentais, os custos de ataques de APIs são elevados, incluindo impactos financeiros e humanos. A perda da confiança da liderança devido a violações pode resultar em maior escrutínio, interrupções operacionais e uma carga de trabalho ainda maior para equipes já sobrecarregadas e em luta para atender às exigências de conformidade.

Akamai

Assim como no setor privado, as agências governamentais enfrentam dificuldades para distinguir entre atividades de API legítimas e maliciosas. Isso ocorre, em parte, devido à baixa visibilidade sobre os pontos exatos em que as APIs estão vulneráveis. Embora 66,9% dos profissionais da área afirmem ter um inventário completo de suas APIs, apenas 18,5% desse grupo sabem quais delas retornam dados confidenciais, incluindo informações de identificação pessoal (PII), como número de CPF, dados biométricos e informações de contato.

Imagine o que pode acontecer com uma API não autorizada, implantada por departamento ou subsidiária de uma organização governamental, sem colaboração ou supervisão de equipes centrais de TI ou segurança atualizadas.

Essa API pode:

- Ter sido criada para permitir acesso a dados pessoais ou financeiros dos cidadãos, sem controles adequados de autorização, potencialmente expondo informações confidenciais
- Ter sido substituída por nova versão, mas sem a devida desativação, deixando um ponto de extremidade desatualizado e vulnerável à exploração
- Estar operando fora do alcance das equipes centrais de TI e segurança, escapando das ferramentas tradicionais de monitoramento e das verificações de conformidade
- Estar sendo explorada por agentes mal-intencionados para obter acesso não autorizado a sistemas governamentais, potencialmente resultando em vazamentos de dados, roubo de identidade ou fraudes financeiras

Isso não é apenas hipotético. O cenário de cibersegurança das agências governamentais dos EUA enfrenta desafios significativos. De acordo com o Cybernews Business Digital Index, muitas agências e departamentos governamentais estão lutando para manter posturas de segurança robustas, com quase 4 em 10 (38,8%) recebendo classificações de "risco crítico" em suas avaliações, e 75% enfrentando um incidente de violação de dados.

Esses números refletem a complexidade dos desafios enfrentados pelas equipes governamentais de segurança, que devem equilibrar objetivos estratégicos, sistemas legados e ameaças em constante evolução, tudo isso sob restrições e escrutínio rigoroso. Com o aumento desses desafios, especialmente no âmbito da segurança de APIs, as agências devem contar com parceiros que compreendam suas necessidades específicas e ofereçam soluções adaptadas ao ambiente governamental.

Como os incidentes de API afetam a confiança, o custo e o estresse da equipe

Diante da crescente frequência e dos custos elevados dos ataques a APIs, proteger esses ativos digitais se tornou uma prioridade essencial para governos em todo o mundo. Nos Estados Unidos, a iniciativa Data.gov, gerenciada pela General Services Administration, padroniza APIs entre agências federais para melhorar a consistência, segurança e interoperabilidade. Esforços semelhantes estão em andamento globalmente, desde estruturas de dados abertas na União Europeia e no Reino Unido até iniciativas de transformação digital em todas as regiões da Ásia-Pacífico e do Oriente Médio, onde os governos estão adotando APIs padronizadas para garantir trocas de dados seguras e contínuas.

Muitas dessas iniciativas estão alinhadas com regulamentações regionais, como o GDPR da UE, o esquema de Violações de dados notificáveis da Austrália e a lei My Number do Japão. Ao aplicar padrões e estruturas comuns, os governos estão trabalhando para garantir a troca segura de dados e, ao mesmo tempo, reduzir os riscos de integrações de terceiros e acessos não autorizados.

	Governo	Média de todos os setores
Estados Unidos	$ 717.500,50	$ 591.404,01
Reino Unido	£ 378.140,69	£ 420.103,18
Alemanha	€ 296.975,79	€ 403.453,26

P3. Se você sofreu um incidente de segurança de APIs, qual foi o impacto financeiro total estimado da combinação desses incidentes? Inclua todos os custos relacionados, como reparos no sistema, tempo de inatividade, taxas legais, multas e quaisquer outras despesas associadas.

Está claro que as agências governamentais têm plena consciência das consequências das ameaças às APIs. Pela primeira vez, solicitamos aos entrevistados dos três países pesquisados que compartilhassem a estimativa do impacto financeiro causado pelos incidentes de segurança de APIs que enfrentaram nos últimos 12 meses.

Embora os impactos financeiros sejam significativos, ouvimos em alto e bom som dos participantes do estudo que os custos vão muito além disso.

O custo não foi o item principal citado quando pedimos para listar o principal impacto de um incidente de segurança de APIs. Conforme foi mencionado, nossos entrevistados apontaram "aumento do estresse e/ou pressão para a equipe/departamento" e "impacto negativo na reputação do departamento junto aos líderes seniores e/ou ao conselho de administração" como as duas principais preocupações.

Essas consequências deixam um impacto duradouro. As violações comprometem a confiança, o que pode afetar futuras fontes de financiamento e abalar a credibilidade junto ao público. Além disso, a queda na produtividade em agências sobrecarregadas pode levar ao burnout e reduzir o engajamento da equipe.

No entanto, essa pressão não está restrita a apenas algumas regiões. Embora este relatório aborde mercados específicos, a segurança de APIs é uma preocupação global para organizações do setor público. Agências na Ásia-Pacífico, América Latina e outras regiões enfrentam desafios semelhantes na proteção da infraestrutura digital, conformidade com regulamentações e defesa de dados confidenciais contra ameaças cada vez mais sofisticadas.

Reduza o risco e o estresse com a segurança de APIs proativa

Os ataques a APIs contra o governo continuam a se expandir em termos de escopo, magnitude, sofisticação e impacto financeiro. Isso inclui ataques de bots alimentados por IA generativa que se adaptam rapidamente para contornar as ferramentas tradicionais de segurança de APIs e outras defesas de perímetro. Muitas equipes de segurança do seu setor estão vivenciando essas ameaças em primeira mão e sentindo os impactos, tanto financeiros quanto humanos. Porém, mesmo quando as organizações entendem a importância das ameaças a APIs, elas ficam com a dúvida: o que podemos fazer a respeito disso?

Tomar medidas agora para proteger melhor suas APIs e os dados que elas trocam pode capacitar sua organização a proteger sua receita e os dados confidenciais, aliviar o fardo das equipes de segurança, tudo isso preservando a confiança arduamente conquistada de líderes governamentais e conselhos de administração. Essas medidas incluem o desenvolvimento do conhecimento da equipe sobre ameaças avançadas de APIs e os recursos necessários para a proteção contra elas.

Para ler o relatório completo e saber mais sobre as práticas recomendadas de visibilidade e proteção de APIs, faça o download do **Estudo sobre o impacto da segurança de APIs de 2024**.

Pronto para conversar sobre seus desafios e como a Akamai pode ajudar?

Solicite uma demonstração personalizada do Akamai API Security

Akamai

As soluções de segurança da Akamai protegem as aplicações essenciais para o sucesso da empresa em cada ponto de interação, garantindo proteção 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 e LinkedIn. Publicado em 05/25.