

O que é uma chave de API e o que acontece se ela for roubada?

Resposta curta: Uma chave de API é uma cadeia de caracteres secreta que identifica e autoriza um programa — em vez de uma pessoa — quando este chama um serviço. Uma chave roubada permite que um atacante faça pedidos em nome da sua aplicação, muitas vezes sem qualquer interação do utilizador, sem MFA e sem qualquer sinal evidente de que algo está errado.

Por que são alvos atrativos

- **Sem intervenção humana.** As chaves foram concebidas para uso automatizado e sem supervisão, pelo que não existe qualquer pedido de MFA a interferir.
- **Frequentemente com âmbito demasiado amplo.** As chaves são muitas vezes emitidas com mais permissões do que a tarefa requer.
- **De longa duração.** Muitas nunca são rotacionadas, pelo que uma chave roubada hoje pode continuar a funcionar meses depois.
- **Armazenadas em locais previsíveis.** Ficheiros de configuração, variáveis de ambiente e repositórios de credenciais — todos locais que a automação consegue enumerar.

Consequências típicas

Dependendo do que a chave autoriza: leitura ou exportação de dados de clientes, envio de mensagens em nome da sua organização, gastos financeiros numa conta cloud, ou pivotagem para outros sistemas ligados.

Como os pedidos estão devidamente autenticados, normalmente aparecem nos registos como tráfego normal da aplicação. A deteção ocorre habitualmente muito depois do facto, através de uma fatura ou de uma auditoria.

Redução da exposição

Defina o âmbito das chaves de forma restrita, rotacione-as regularmente e mantenha-as fora do controlo de código-fonte. Estas são boas práticas, mas limitam o raio de impacto em vez de

prevenirem o roubo.

A Cyber Crucible visa o próprio roubo. Os locais de credenciais e configuração são protegidos, e um programa que os lê é avaliado em contexto: dados falsos ou recusa em caso de uso excessivo legítimo, rejeição ou suspensão em caso de processo desconhecido ou comprometido. A chave não é entregue em nenhum dos casos.

Revision #1

Created 2026-07-24 05:42:19 UTC by Dennis Underwood

Updated 2026-07-24 05:42:19 UTC by Dennis Underwood