Um Guia de Segurança de APIs Indispensável para CISOs

Um Guia de Segurança de APIs Indispensável para CISOs

Sumário executivo

Os diretores de segurança da informação (CISOs) têm que lidar com uma situação delicada. Eles precisam proteger a empresa de um cenário de risco de segurança em constante evolução e, ao mesmo tempo, permitir que ela tenha bastante agilidade para lançar suas principais iniciativas no mercado. Nenhum CISO pode se dar ao luxo de atrapalhar ou retardar programas vitais.

Está cada dia mais difícil avaliar os riscos. Como o ritmo de desenvolvimento ficou mais acelerado, os CISOs precisam avaliar os riscos mais rápido e, ainda assim, manter a segurança dos negócios. Cabe a eles determinar o valor de cada iniciativa, o risco que ela representa e priorizar os investimentos de segurança com base nessas avaliações.

> Em seu relatório *State of Cybersecurity Resilience 2021*, a Accenture diz que os melhores CISOs são aqueles que conseguem "encontrar um ponto de equilíbrio entre a resiliência cibernética e os objetivos da empresa, com um forte alinhamento com a estratégia comercial que melhor proteja os principais ativos de uma organização".

As iniciativas de transformação digital de hoje são um exemplo claro do grau de equilíbrio que o CISO precisa ter. Elas oferecem vantagens competitivas, melhoram a eficiência da empresa e abrem caminhos para o crescimento. Mas as APIs que viabilizam essa transformação digital representam uma nova superfície de ataque importante e um ponto de alto risco de exposição potencial dos dados.

Em uma pesquisa global da Statista, 94,5% dos responsáveis por segurança citaram a proteção de suas iniciativas de transformação digital como a principal prioridade pós-pandemia. Os CISOs precisam ser proativos nos processos de segurança para manter o curso da transformação digital e cumprir as regulamentações para evitar multas caras. Para fazer isso, o foco deles deve estar na segurança das APIs.

Por que as APIs representam o maior risco para os CISOs

As APIs foram criadas especificamente para serviços que compartilham dados críticos com seus clientes, parceiros e funcionários. Elas são a base dos apps móveis. Pesquisas mostram que mais de 80% do tráfego da Internet é de APIs. Hoje, as empresas têm milhares de APIs e que estão sempre mudando. O 2021 State of the API Report da Postman descobriu que mais da metade dos desenvolvedores implantam novas APIs nos sistemas ao vivo pelo menos uma vez por dia, por semana ou por mês.

Além disso, as APIs também são usadas em canais externos de parceiros e clientes, viabilizando serviços móveis e online novos e transformadores. Mas, ao fazer isso, elas também facilitam a conectividade para o uso de dados altamente confidenciais, como informações de identificação pessoal, dados financeiros e registros médicos. Como as APIs detêm a chave de um tesouro de dados, elas se tornaram um alvo atrativo para os invasores, como mostra o número crescente de ameaças cibernéticas que visam as APIs das empresas.

Muitas empresas como a Parler, Experian, Facebook e Peloton sofreram ataques a APIs. Os ataques podem diminuir a confiança do cliente, causar perda de receita e danificar para sempre a reputação de uma empresa. No caso da plataforma de câmbio de criptomoedas Coinbase, se a vulnerabilidade na API não fosse detectada, ela poderia ter ido à falência.

Apesar de todos esses riscos, as APIs continuam mal protegidas. De acordo com a última pesquisa da Salt Labs, mais de um terço das empresas não têm uma estratégia de segurança para APIs.

As soluções existentes não conseguem suprir as necessidades de segurança das APIs. Os ataques às APIs ocorrem em uma sequência de eventos relacionados, mas as soluções tradicionais, como os WAFs, só conseguem ver uma transação por vez.

Elas são criadas para caminhos já "conhecidos", enquanto as APIs são únicas e exigem a detecção de atividades de reconhecimento mais lentas. Para identificar e se proteger das ameaças, os responsáveis pela segurança precisam conseguir ver todas as atividades.

Mesmo usando as APIs como se deve, ainda assim há risco de invasão. Dados empíricos da pesquisa da Salt Labs revelam que 94% das explorações de APIs ocorrem em APIs autenticadas. Você não pode simplesmente confiar na autenticação para proteger as APIs.

> "Um WAF na frente de uma API cai. Ele não oferece proteção contra essas ameaças. Ele não fornece a visibilidade de que você precisa, sem mencionar que, se você não conhece todas as suas APIs, ou mesmo quais APIs existem, fica muito difícil protegê-las."
> - Tyler Warren, Diretor-adjunto de segurança da informação, Prologis

A exposição excessiva dos dados, como descrito no OWASP API Security Top 10, também pode permitir involuntariamente o acesso a mais dados do que o necessário para uma determinada solicitação. Nos exemplos da Experian e Peloton mencionados acima, as APIs foram o veículo para a exfiltração de dados e usadas de acordo com seu propósito, ou seja, em resposta a consultas legítimas.

Os três pilares de segurança das APIs

A maneira como se protegia várias APIs antes não funciona mais, porque as empresas estão criando dezenas e até centenas de APIs por semana e, em alguns casos, por dia. Com um ritmo de desenvolvimento tão rápido, a superfície de ataque das APIs não para de aumentar. Para proteger efetivamente um cenário em evolução, os CISOs precisam de uma solução de API que ofereça estes três recursos:

- Visibilidade automática de todo o tráfego das APIs
- Análise contínua no tempo de execução
- Insights de correção para segurança proativa

Visibilidade total do tráfego das APIs

É cada vez maior o número de APIs dentro das empresas. Os sistemas, os aplicativos, as APIs e os dados com os quais elas interagem abrangem vários ambientes. Se você não tiver visibilidade de todas as suas APIs, não conseguirá protegê-las. Você também precisa entender quais APIs podem estar expondo dados confidenciais.

Com um inventário de referência preciso das suas APIs, que possa ser atualizado de forma rápida e fácil, os CISOs conseguem eliminar os pontos cegos. Sem isso, eles não terão ideia do nível de exposição da empresa e nem poderão definir as prioridades no gerenciamento de riscos.

Análise contínua e dinâmica em tempo de execução

Você precisa ter uma base de referência do tráfego normal das APIs para conseguir identificar abusos ou ataques. Como as APIs não são apenas códigos onde você pode procurar falhas no desenvolvimento e nos testes, mas sim instâncias de lógica de negócios, você precisa ver suas APIs em ação para detectar as falhas. Conseguir ver padrões no tempo de execução durante o uso das APIs oferece às empresas mais contexto quando se trata de segurança das APIs para identificar atividades maliciosas e eliminar pontos cegos. Sem isso, eles não terão ideia do nível de exposição da empresa e nem poderão definir as prioridades no gerenciamento de riscos.

Insights de correção para uma segurança proativa

É importante que você compartilhe com as equipes de P&D e DevOps o que está aprendendo sobre as as APIs e suas possíveis vulnerabilidades. Os insights de correção ajudam a levar o que você descobriu sobre segurança das APIs para o treinamento e aperfeiçoamento dos desenvolvedores, e dar a eles mais informações para reforçar a segurança das APIs. Os detalhes da correção viabilizam práticas "shift-left" para obtenção contínua de valor das suas APIs, porque você poderá identificar os riscos antes que eles sejam explorados. Esses insights ajudam os desenvolvedores a programar APIs melhores mesmo quando criam novas. Você também deve aproveitar o que aprendeu do tempo de execução e ganhar mais insights sobre correção.

Garantir uma implementação bem-sucedida

Em um painel com CISOs no recente API Security Summit, o veredito foi unânime. O sucesso do CISO começa quando ele consegue implementar a cultura certa de segurança. Essa necessidade é ainda mais forte com as APIs. As APIs estão presentes em quase todas as partes da empresa, exigindo um esforço interfuncional que reconheça e compreenda a importância da segurança das APIs na redução dos riscos para a empresa.

Além disso, as empresas precisam de segurança específica para as APIs. Elas devem ter seu próprio programa. Ao considerar a segurança das APIs como uma categoria própria e essencial na proteção dos serviços da plataforma em 2021, o Gartner validou esse requisito.

Aproveitando os benefícios da automação, big data e inteligência

Para acompanhar o aumento exponencial de APIs, os CISOs também precisam de soluções que possam ser integradas aos fluxos de trabalho de DevOps e SecOps existentes. A descoberta, a detecção de anomalias e o compartilhamento de insights de correção de APIs devem estar vinculados a sistemas de CI/CD e de resposta a incidentes, todos automatizados.

Para obter o contexto necessário para identificar com precisão os ataques a APIs, as soluções de segurança de API devem contar com recursos de big data, IA e ML na nuvem para resolver o problema. Os ataques a APIs duram dias, semanas ou meses porque os hackers precisam investigar minuciosamente como as APIs funcionam para encontrar falhas na lógica de negócios. As soluções de segurança de APIs precisam ser capazes de processar grandes quantidades de dados por um longo período para desenvolver o contexto necessário que possibilite distinguir o tráfego de ataque do tráfego normal. Você não consegue obter esse nível de contexto tão rico com soluções on premises baseadas em VM. Só a combinação de big data na nuvem com inteligência artificial (IA) e aprendizado de máquina (ML) permite rastrear milhões de usuários ao mesmo tempo durante dias, semanas ou meses.

Não deixe que as falhas de segurança nas APIs inibam a inovação nos negócios

Em um momento em que a segurança cibernética se transformou em um tema tão importante, as APIs tornaram-se o elo mais fraco dos sistemas de TI. Sem segurança nas APIs, os CISOs não conseguem maximizar o valor das iniciativas de modernização digital e de TI. Pior ainda, os pontos fracos das APIs colocam a possibilidade de lucro para as empresas em risco. Para ser um CISO de sucesso, você precisa entender muito de ameaças, estar alinhado aos negócios e ser proativo. Ao implementar um programa de segurança específico para APIs, os CISOs ajudam a empresa a acelerar a inovação digital, criam uma cultura mais centrada na segurança e promovem o crescimento dos negócios.

Para saber como a Salt Security API Protection Platform evita os ataques às APIs, solicite uma demonstração personalizada.