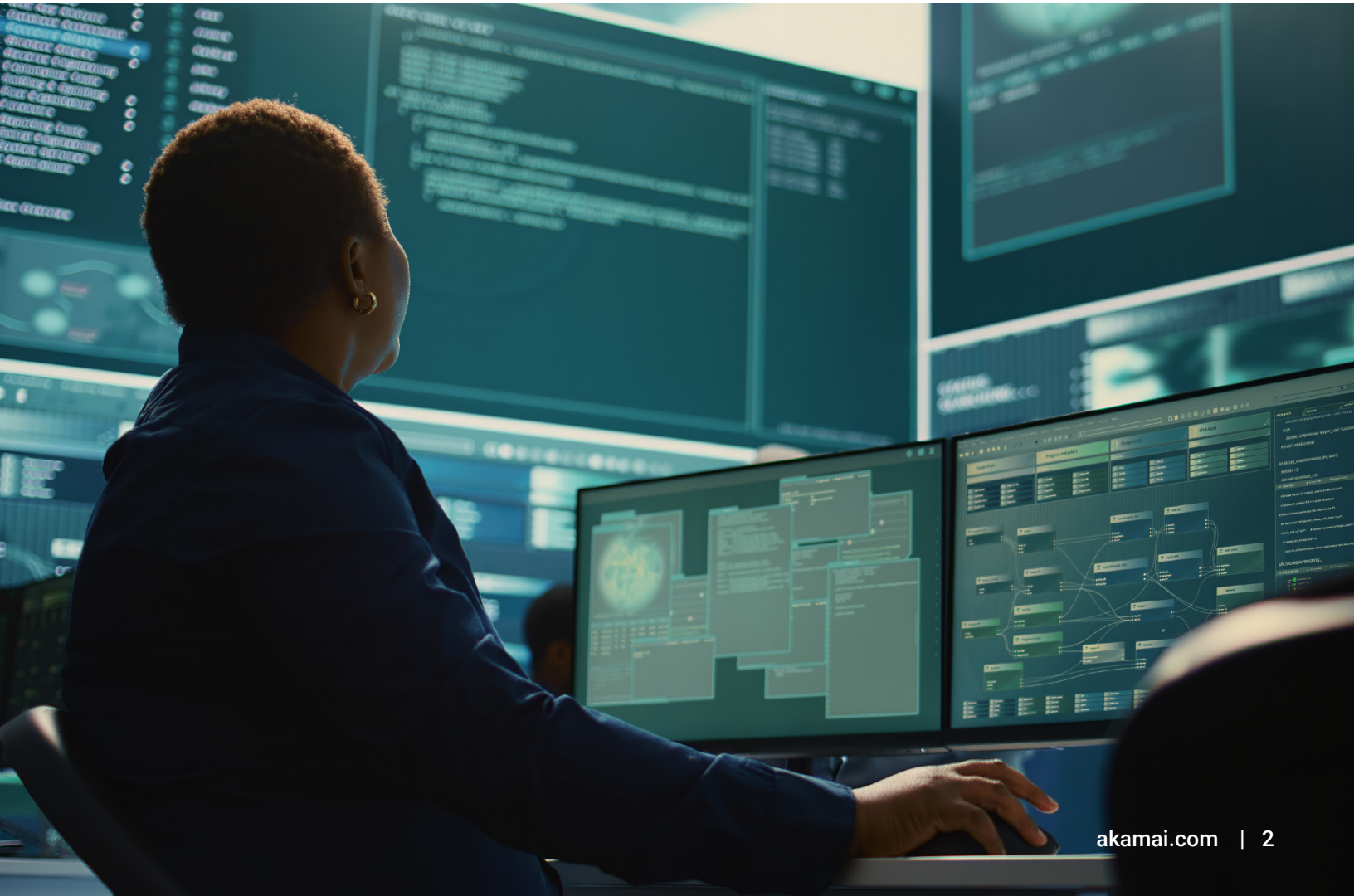
Akamai

WHITE PAPER

Segurança e conformidade de API

Requisitos implícitos e explícitos de proteção de dados

Neste relatório



Introdução

Demonstrar a conformidade com as normas de proteção de dados tem significado, tradicionalmente, gastar grandes quantidades de energia e recursos para acompanhar os riscos mais conhecidos. Mas isso está mudando. A superfície de ataque de hoje está evoluindo rapidamente para incluir ameaças que a maioria dos programas de conformidade corporativa não está considerando totalmente. Isso ocorre em parte porque os órgãos reguladores nem sempre conseguem acompanhar o ritmo e ser explícitos sobre todas as facetas da cobertura necessárias para evitar violações.

Este é o caso com a proteção de API. Toda vez que um cliente, parceiro ou fornecedor se envolve com sua empresa digitalmente, há uma API nos bastidores, facilitando uma rápida troca de informações que geralmente inclui dados confidenciais. Os invasores agora sabem que eles podem simplificar a estratégia para roubar esses dados atacando diretamente as APIs.

Você pode já ter visto uma menção nos regulamentos indicando a necessidade de inventariar, avaliar ou proteger APIs. Mas mesmo sem uma menção específica sobre APIs, o fato de que elas se tornaram um vetor de ataque claro *implica* que sua proteção adequada é necessária.

O surgimento de APIs como um grande problema de conformidade não é surpreendente. APIs expostas ou mal configuradas são predominantes e fáceis de comprometer e, muitas vezes, estão desprotegidas. E a violação de apenas uma API pode resultar no furto de milhões de registros. Os números falam por si:

- Setenta e oito por cento das organizações sofreram um incidente de segurança relacionado a APIs.[1]
- Quarenta e quatro por cento foram multadas pelos reguladores por incidentes com a segurança de API.[2]

Como isso afeta seu programa de conformidade? Os reguladores precisam ver que sua organização está tomando medidas para proteger todos os pontos de acesso a dados confidenciais. Isso significa que você precisa demonstrar que sua organização pode:

- Se responsabilizar por cada API, incluindo APIs sombra elusivas
- Descobrir e corrigir quaisquer vulnerabilidades de API
- Aplicar controles sob medida para evitar violações de dados centradas em API

Este white paper explora a natureza do crescimento dos riscos de API, destaca seis exemplos de regulamentações e estruturas que exigem proteções de API (explícita ou implicitamente) e oferece conselhos sobre como atender aos requisitos de conformidade por meio das melhores práticas de segurança de API.

1., 2. Akamai Technologies, "The API Security Disconnect," 2023

Entendendo os riscos de API

As APIs estão no centro dos produtos e serviços digitais e ambientes de nuvem da sua empresa. Seu acesso constante aos dados as torna tanto um gerador de receita quanto um risco operacional. O problema é que a maioria das empresas, mesmo aquelas com programas de segurança maduros, não está priorizando as ameaças relacionadas à API no mesmo nível em que se concentra em outras ameaças, como phishing ou ransomware.

Algumas organizações dependem de gateways de API e firewalls de aplicativos da web (WAFs) para a proteção básica da API, mas essas ferramentas não foram projetadas para oferecer o grau de visibilidade, proteção em tempo real e testes contínuos que as soluções especializadas em segurança de API podem oferecer. Veja por que essas ferramentas não são suficientes:

- Os gateways de API e os WAFs só podem observar o tráfego de API *gerenciado* que é encaminhado por eles.
- Eles não podem proteger APIs não gerenciadas, que, segundo os analistas, representarão quase metade do ecossistema de APIs de uma empresa típica até 2025.
- Como resultado, as equipes de segurança não estão totalmente preparadas para proteger a parte da sua superfície de ataque que se expande mais rapidamente, sabendo pouco sobre onde as APIs são roteadas, como elas são configuradas, que tipos de dados confidenciais trocam e os riscos que elas representam.

A proteção das informações dos usuários é uma prioridade para os órgãos reguladores, que aplicam multas severas às empresas que não protegem os dados de seus clientes de forma razoável contra acesso não autorizado. Considerando que apenas 4 em cada 10 profissionais de segurança com inventários de API completos sabem qual de suas APIs retornam dados confidenciais[3] e que muitas chamadas de API vêm de invasores que testam vulnerabilidades, as violações de dados via APIs só aumentarão, especialmente porque os ataques de API são atualmente bastante fáceis de realizar.

3. Akamai Technologies, "The API Security Disconnect," 2023

Quatro ataques de API com implicações de conformidade

Como uma violação de API pode afetar a postura de conformidade de uma empresa? Aqui estão alguns outros exemplos:

- Um popular aplicativo de gerenciamento de projetos foi comprometido por um invasor que explorou um ponto de extremidade de API sem controles de autenticação. O invasor violou a API, obteve acesso não autorizado a informações sobre milhões de usuários e, meses depois, vazou mais de 21 GB de dados, incluindo endereços de e-mail e participações no conselho de administração.
- Mais de 11 milhões de registros de clientes de uma grande empresa de telecomunicações foram expostos, supostamente por causa de uma API que estava exposta à internet e não precisava de autenticação. Os invasores violaram a API, viram que ela não tinha um identificador exclusivo, adivinharam seu número de ID e solicitaram dados confidenciais facilmente.
- Uma empresa de mídia social foi atingida duas vezes nos últimos anos por uma tática de scraping viabilizada pelo uso inadequado da API. No primeiro caso, os dados privados foram coletados de 500 milhões de perfis de usuário e, em seguida, vendidos. No segundo, um invasor criou um banco de dados, incluindo números de telefone e dados salariais, retirados de 700 milhões de usuários.
- Essa mesma técnica foi usada contra outra empresa de mídia social para exfiltrar dados em milhões de usuários. A empresa recebeu uma multa de US$ 5 bilhões porque um fornecedor terceirizado usou a API da empresa para coletar dados confidenciais. Não importa que o fornecedor abusou da API, a *empresa* foi multada porque não conseguiu monitorar sua aplicação.

Seis exemplos de regulamentos e estruturas que envolvem a segurança de API

Em muitos regulamentos e estruturas, as APIs não são necessariamente mencionadas pelo nome, mas os requisitos se concentram claramente em proteger os aplicativos e a infraestrutura dentro dos quais as APIs operam. Por exemplo:

- O PCI (Payment Card Industry) v4.0 oferece orientação para confirmar que o software de uma organização usa com segurança funções de componentes externos. Isso inclui APIs que transmitem dados de pagamento de um app móvel para o sistema de um banco.
- A Estrutura de Desenvolvimento de Software Seguro do NIST fornece orientação sobre a produção de software bem guardado, sua proteção contínua e resposta a vulnerabilidades. As APIs estão no centro do desenvolvimento de software.

Em muitos casos, os regulamentos sugerem objetivos vagamente definidos para a proteção de dados, como o requisito da lei GDPR (General Data Protection Regulation) sobre "medidas de segurança apropriadas". Suas APIs podem receber milhões de chamadas por dia para fornecer esses dados, de *clientes* e invasores. Cabe a você determinar quais controles de segurança são necessários e, em seguida, demonstrar como eles funcionarão.

Vamos analisar as regulamentações e estruturas com implicações diretas para o seu ecossistema de API.

1. PCI DSS v4.0

Criado pelo Payment Card Industry Data Security Council, o PCI DSS se tornou um padrão global para proteção de dados de pagamento. Se a sua empresa aceita os principais cartões de crédito e processa, armazena ou transmite dados de titulares de cartões eletronicamente, precisa cumpri-lo.

Os requisitos da versão original abrangem os pilares de segurança que são tão importantes agora quanto eram quando o PCI DSS foi publicado em 2006, como atribuir acesso a dados do sistema e do titular do cartão com base na necessidade de conhecimento e definir requisitos de acesso por função.

No entanto, com o PCI DSS v4.0 em vigor, as empresas precisam adaptar seus programas de conformidade para responder aos agentes de ameaças que frequentemente visam as milhares de APIs internas às tecnologias de pagamento. No geral, o PCI DSS v4.0 concentra-se em quatro objetivos principais:

1. Continuar atendendo às necessidades de segurança do setor de pagamentos
2. Promover a segurança como um processo contínuo
3. Oferecer flexibilidade às empresas (por exemplo, novas ferramentas e novos controles) quanto às maneiras pelas quais elas atendem aos requisitos
4. Aprimorar os métodos e processos de validação

O requisito 6.2.3 do PCI DSS v4.0 se concentra na necessidade das organizações revisarem seus códigos de aplicativos personalizados (ou seja, códigos desenvolvidos por um fornecedor terceirizado, mas não aplicativos comerciais padrão prontos para uso) para garantir que nenhuma vulnerabilidade seja liberada na produção. Específico para APIs, esse requisito oferece orientação para confirmar se o software de uma organização usa com segurança as funções de componentes externos (bibliotecas, estruturas, APIs etc.). Requisitos como esses enfatizam o papel fundamental que as APIs desempenham na cadeia de suprimentos de software mais ampla e o que é preciso para protegê-la.

As APIs se tornaram o método padrão de conectividade e troca de dados em ambientes modernos de aplicativos. Com isso em mente, proteger APIs de uma perspectiva de pré-produção (shift-left) e pós-produção (shield-right) é essencial para tornar seu negócio digital resiliente contra ataques. Aqui estão algumas práticas recomendadas de segurança de API a serem seguidas para conformidade com o requisito 6.2.3:

- Confirme o uso de componentes baseados em API e sua postura de segurança (por exemplo, encontre configurações incorretas que levem a vulnerabilidades, incluindo o uso de cifras de criptografia fracas).
- Valide o comportamento normal e esperado do uso da API e implemente controles para bloquear atores suspeitos de abusar de seus sistemas (por exemplo, verifique o comportamento do aplicativo para detectar vulnerabilidades lógicas).
- Detecte estruturas de terceiros usadas para acionar suas APIs, determinando qualquer uma que possa estar desatualizada e vulnerável.
- Crie um inventário completo de todas as APIs, incluindo as diferentes versões que você está executando, pois isso fornece informações sobre backdoors e potenciais recursos não documentados que precisa gerenciar.
- Valide a segurança do seu código de API e evite colocar em produção qualquer vulnerabilidade relacionada à API.
- Implemente práticas recomendadas de codificação segura de APIs, o que permitirá que você adote uma abordagem programática para entregar o código de forma segura e contínua.

2. General Data Protection Regulation (GDPR)

O GDPR é uma lei da União Europeia (UE) que visa reforçar e unificar a proteção de dados de indivíduos dentro desse território. No entanto, o GDPR não se limita a empresas baseadas na UE. Qualquer organização que ofereça bens de consumo ou serviços na União Europeia deve estar em conformidade.

O regulamento estabelece que os dados pessoais são informações que podem ser ligadas ou vinculadas a um indivíduo. Os dados regulados sob o GDPR podem incluir o nome de um indivíduo, informações de contato, dados bancários e financeiros e informações médicas. Do lado mais técnico, os dados cobertos também incluem dados de geolocalização, como endereços IP e cookies da web.

O que isso significa para a segurança de APIs? Seja desenvolvendo aplicativos, microsserviços ou dispositivos de Internet das Coisas (IoT), as APIs internas a estas tecnologias provavelmente trocam dados regulados pelo GDPR. Portanto, as organizações que desenvolvem APIs acessíveis pela Internet devem considerar a proteção de dados no projeto da API desde o início, e não após o fato.

Considere o princípio do mínimo privilégio, o que requer garantir que os usuários tenham apenas as permissões mínimas necessárias para executar seus trabalhos.

O artigo 25 do GDPR está *enraizado* no privilégio mínimo, exigindo que as empresas implementem "medidas técnicas e organizacionais para garantir que, por padrão, apenas os dados pessoais necessários para cada finalidade específica... sejam processados." Por sua vez, os desenvolvedores de APIs devem implementar controles de autenticação e autorização de usuários para proteger os dados confidenciais que são transmitidos através de suas APIs. As equipes de desenvolvimento de API também devem garantir que os dados permaneçam confidenciais em trânsito usando protocolos de comunicação seguros para criptografar a troca de informações entre cliente e servidor.

No entanto, o que dizer do ecossistema existente de APIs que as organizações criaram nos últimos anos ou até mesmo décadas? Uma parte substancial das APIs corporativas não é gerenciada, é esquecida ou é executada perpetuamente sem verificações e apurações. Nestes casos, a conformidade com o GDPR exige:

- Descoberta de cada API em seu ambiente de TI
- Avaliação de seus fatores de risco (por exemplo, os tipos de dados que elas têm trocado e quem ou o que pode acessar esses dados)
- Correção de quaisquer vulnerabilidades, como configurações incorretas ou mecanismos de autenticação fracos
- Testes contínuos de APIs para resiliência contra métodos tradicionais e emergentes de violação e ataque

3. Lei de Resiliência Operacional Digital (DORA)

Dado o papel do setor financeiro da UE como operador crítico de infraestrutura, os requisitos da DORA destinam-se a ajudar as organizações dos Estados-Membros da UE a suportar e a recuperar-se de ciberataques. Com a DORA, o setor terá um quadro vinculativo e abrangente de gestão de riscos para a tecnologia da informação e comunicação (TIC). A lei visa harmonizar e reforçar os requisitos para as empresas financeiras da UE, uma vez que o cenário atual implica uma infinidade de regulamentos e normas.

No total, mais de 22.000 instituições financeiras e prestadores de serviços de TI na UE são afetadas pela DORA. Note-se que isso inclui terceiros que fornecem às empresas financeiras da UE sistemas e serviços de TIC, incluindo prestadores de serviços em nuvem. A lei exige que as instituições financeiras desenvolvam estratégias de risco de terceiros de TIC e conduzam a devida diligência para verificar a adequação dos provedores.

A DORA estabelece vários requisitos com implicações de segurança de APIs, incluindo estabilidade operacional digital, o que exige que as organizações implementem programas de teste regulares que identifiquem possíveis lacunas, vulnerabilidades e/ou deficiências na estabilidade operacional digital. Pense em testes de segurança de rede, de penetração, de apps web e muito mais. É importante realizar revisões obrigatórias com base em testes de penetração liderados por ameaças (TLPT), dependendo do tamanho, risco e perfil comercial da empresa financeira. Igualmente importante é testar regularmente suas APIs em busca de vulnerabilidades.

A DORA descreve exemplos de testes de segurança que incluem testes de aplicativos e API baseados na web. Isso inclui a utilização de recursos de atendimento, como o Open Worldwide Application Security Project (OWASP). Os 10 principais riscos de segurança da API do OWASP, em particular, ajudam as organizações a identificar erros de configuração, fraquezas, falhas lógicas e problemas de código que permitem que os invasores tenham acesso, manipulem ou controlem recursos organizacionais.

4. Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA)

A HIPAA se concentra em regras de privacidade e segurança de dados para resguardar informações de saúde protegidas (PHI) em prontuários eletrônicos (EHRs), plataformas computadorizadas de entrada de pedidos médicos e outros sistemas de TI de saúde. Qualquer prestadora de serviços de saúde dos EUA, administradora de planos ou centro coordenador que armazene ou transmita PHI eletronicamente deve estar em conformidade com a HIPAA. Isso envolve garantir a confidencialidade, integridade e disponibilidade de PHI e protegê-la contra divulgação não autorizada e uso indevido.

A HIPAA é exemplo de um regulamento que tem implicações significativas para APIs, mesmo que não mencione explicitamente as APIs em seus requisitos.

Considere um fornecedor de tecnologia que constrói portais de pacientes para clínicas de saúde. Uma função desses portais é a capacidade de dar aos pacientes acesso eficiente e seguro aos dados em suas visitas médicas, resultados de testes e pagamentos, entre outros. As APIs são os facilitadores dessa troca. Tanto a clínica como o fornecedor estão obrigados a aderir aos requisitos da HIPAA.

A regra de privacidade da HIPAA especifica que as entidades abrangidas "devem desenvolver e implementar políticas e procedimentos que restrinjam o acesso e o uso de informações de saúde protegidas com base nas funções específicas dos membros de sua força de trabalho". Portanto, os desenvolvedores de APIs de uma organização devem integrar proteções técnicas, como autenticação, IDs de usuário exclusivos e controles de acesso baseados em funções para garantir que o privilégio mínimo esteja em vigor.

A visibilidade também é essencial para as organizações cobertas pela HIPAA, seja um provedor cuja equipe de TI cria APIs sob medida ou um fornecedor que desenvolve APIs para o provedor. As organizações precisam de avaliação em tempo real e relatórios sobre a postura de risco de cada API, incluindo os tipos de PHI que transmitem. Isso é relevante para a conformidade e para cumprir a exigência da HIPAA de responder a pessoas que solicitam informações sobre quando, onde, por que e a quem seu PHI foi divulgado.

5. Diretiva de Segurança de Redes e Informações (NIS2)

A União Europeia adotou a versão 2.0 da diretiva NIS em janeiro de 2023, que se baseia nas diretrizes da versão original para a proteção de infraestruturas de TI e a comunicação de incidentes. Embora a v2.0 não mencione especificamente APIs, seus requisitos têm implicações significativas para a proteção e gerenciamento de APIs, pois são parte integrante do funcionamento de muitos serviços digitais em organizações sujeitas à diretiva. A NIS2 inclui:

- Uma gama mais ampla de setores, por exemplo, provedores de serviços em nuvem e empresas de mídia social se juntam à lista existente, que inclui operadores de infraestrutura crítica. Para esses setores, onde as APIs são amplamente utilizadas para integração e entrega de serviços, é preciso garantir que a segurança da API se torne uma prioridade.
- Uma nova ênfase na proteção das cadeias de suprimentos: as empresas devem avaliar o risco e garantir suas cadeias de suprimentos de TI e relacionamentos com fornecedores terceirizados. Como as APIs são frequentemente usadas para integrar serviços externos, garantir a segurança é fundamental para a conformidade.
- Um requisito para construir um sistema de gerenciamento de segurança da informação que avalia pessoas, políticas e tecnologia para proteger recursos sensíveis e garantir resiliência operacional. Como as APIs são vetores de ataque de rápido crescimento, elas devem ser incluídas em estratégias de gerenciamento de risco.
- Relatórios de incidentes significativos de cibersegurança, incluindo violações de API. Portanto, as organizações precisam implementar mecanismos para monitorar, detectar e relatar incidentes relacionados à API.

6. Orientação para reguladores de serviços financeiros dos EUA

O Federal Financial Institutions Examination Council (FFIEC) cria a orientação e os padrões para reguladores federais supervisionarem o setor financeiro dos EUA. Isso inclui o Federal Reserve, FDIC, OCC e NCUA. A missão do conselho é proteger os consumidores e os investidores contra fraudes, violações e más condutas. Embora não seja um regulamento, a orientação do FFIEC é fundamental para garantir que as empresas financeiras saibam se alinhar com as medidas de segurança recomendadas.

Este é um exemplo chave de um documento que inclui orientações específicas sobre como proteger APIs e, por sua vez, proteger os consumidores contra fraudes e roubo de identidade. Aqui está uma visão geral:

- **Inventário:** O FFIEC recomenda a criação de um inventário de todos os sistemas de informação, incluindo APIs, que exigem autenticação e controles de acesso. Isso se aplica não apenas a instituições financeiras, mas também a seus terceiros, como provedores de serviços em nuvem.
- **Autenticação:** A API só deve permitir o acesso a usuários autorizados. É fundamental identificar todos os usuários (por exemplo, clientes) para os quais os controles de acesso são necessários. Também é importante identificar usuários que mereçam controles aprimorados, como autenticação multifator.
- **Autorização:** A API só deve permitir o acesso a recursos específicos para usuários autorizados. Sendo assim, o FFIEC recomenda a implementação de segurança em camadas; por exemplo, o monitoramento, o registro e a comunicação de atividades para identificar e rastrear o acesso não autorizado a APIs.
- **Gerenciamento de riscos:** Há uma série de práticas eficazes de gestão de riscos que o FFIEC identifica em suas orientações mais recentes. No entanto, eles destacam explicitamente APIs na categoria Inventário de Sistemas de Informação, o que significa que você precisa de um inventário preciso de suas APIs.

Uma organização pode lidar bem com ameaças bem conhecidas, como phishing ou ransomware, mas o FFIEC exige *identificar qualquer* ciberameaça com "probabilidade razoável de afetar os sistemas de informação da instituição financeira" e seus dados. Conforme citado na introdução, 78% das organizações enfrentaram incidentes de segurança de APIs, portanto, você pode contar com a proteção de APIs como um imperativo de conformidade à medida que os requisitos dos reguladores financeiros continuam a evoluir.

Supere os desafios de conformidade com as melhores práticas de proteção de API

O cenário de ameaças de hoje exige uma solução completa de segurança de API que fornece descoberta de APIs, gerenciamento de postura, proteção de tempo de execução e testes de segurança de API. Essa abordagem abrangente funciona como um complemento para qualquer gateway WAF ou API que já esteja em vigor.

1. Detecção de API

É comum ter APIs que ninguém conhece. A maioria das organizações tem pouca ou nenhuma visibilidade sobre uma grande porcentagem do tráfego de API, muitas vezes porque elas pressupõem que todas as APIs são roteadas por meio de um gateway de API. Mas esse não é o caso. Sua empresa está exposta a uma série de riscos sem um inventário completo e preciso. Recursos essenciais necessários:

- Localizar e inventariar todas as suas APIs, independentemente da configuração ou tipo
- Detectar APIs inativas, legadas e zumbis
- Identificar domínios esquecidos, negligenciados ou de sombra desconhecidos
- Eliminar pontos cegos e revelar possíveis caminhos de ataque

2. Gerenciamento de postura de APIs

Com um inventário de API completo, é fundamental entender quais tipos de dados fluem através de suas APIs e como isso afeta sua capacidade de cumprir os requisitos regulamentares. O gerenciamento de postura da API fornece uma visão abrangente do tráfego, código e configurações para avaliar a postura de segurança da API da sua organização. Recursos essenciais necessários:

- Verificar automaticamente a infraestrutura para descobrir configurações incorretas e riscos ocultos
- Criar fluxos de trabalho personalizados para notificar as principais partes interessadas sobre vulnerabilidades
- Identificar quais APIs e usuários internos podem acessar dados confidenciais
- Atribuir classificações de gravidade aos problemas detectados para priorizar a correção

3. Segurança de tempo de execução da API

Sem dúvida, você está familiarizado com o conceito de "presumir uma violação". Violações e ataques específicos de API estão atingindo esse mesmo grau de inevitabilidade. Para todas as APIs que estão em produção, você precisa ser capaz de detectar e bloquear ataques em tempo real. Recursos essenciais necessários:

- Monitorar a violação e o vazamento de dados, violações de políticas, comportamento suspeito e ataques a APIs
- Analisar o tráfego de APIs sem alterações de rede adicionais ou agentes de difícil instalação
- Integrar fluxos de trabalho existentes (emissão de tickets, SIEMs etc.) para alertar equipes de segurança/operações
- Evitar ataques e uso indevido em tempo real com correção parcial ou totalmente automatizada

4. Teste de segurança de API

As equipes de desenvolvimento de API estão sob pressão para trabalhar o mais rápido possível. A velocidade é essencial para cada aplicativo desenvolvido, tornando mais fácil para uma vulnerabilidade ou falha de design acontecer e não ser detectada. Testar APIs em desenvolvimento antes de serem lançadas na produção reduz muito o risco e o custo de corrigir uma API vulnerável. Recursos essenciais necessários:

- Executar uma ampla gama de testes automatizados que simulam tráfego malicioso
- Descobrir vulnerabilidades antes que as APIs entrem em produção para reduzir o risco de um ataque bem-sucedido
- Inspecionar as especificações de API em relação às políticas e regras de governança estabelecidas
- Executar testes de segurança com foco em API sob demanda ou como parte de um pipeline de CI/CD

Como o Akamai API Security pode simplificar as complexidades de conformidade de API

As APIs são uma das principais causas das violações que os regulamentos de hoje pretendem evitar. O que é preciso para proteger sua empresa à medida que as APIs, e seus riscos, se multiplicam? As ferramentas existentes que muitas organizações usam para proteção básica da API fornecem alguma proteção, mas não o suficiente. Se você está procurando uma maneira melhor de proteger as APIs da sua organização e demonstrar conformidade, podemos ajudar.

Para todos os requisitos e orientações abordados neste white paper, o Akamai API Security fortalece a proteção de que as empresas precisam, não só para cumprir os regulamentos, mas também para proteger os dados e a confiança de seus clientes.

A solução abrangente da Akamai protege as APIs em seus estágios iniciais de desenvolvimento até a pós-produção, proporcionando a capacidade de aderir às melhores práticas principais:

- Detecção de API
- Gerenciamento de postura
- Proteção de tempo de execução
- Teste de segurança

Saiba mais sobre APIs e como protegê-las de ataques.

Saiba como o Akamai API Security pode ajudar sua organização.