Akamai

WHITE PAPER

Simplifique a segurança de seus aplicativos da Web

Ataques a aplicativos da Web

Os aplicativos da Web modernos tornaram-se complexos, especialmente com a adoção cada vez maior de arquiteturas baseadas em microsserviços. A forte dependência de APIs em praticamente todas as interações online contribui com essa complexidade e traz consigo o potencial para novos pontos de entrada de hackers. Enquanto isso, as vulnerabilidades conhecidas da Web continuam existindo e são reintroduzidas em aplicativos por cada nova geração de codificadores. Já os invasores atuais evoluíram com o uso de bots, ataques de negação de serviço distribuída por aluguel (DDoS-for-hire) e ataques multivetoriais que visam aplicativos da Web, APIs e até mesmo vulnerabilidades no lado dos clientes.

Contudo, os ataques oportunistas ainda são a forma mais comum na Web: eles não têm necessariamente sua organização como alvo, mas direcionam o ataque a ela após a descoberta de uma vulnerabilidade. Os scanners usam bots automatizados para rastrear websites aleatoriamente, sempre em busca de alguma vulnerabilidade dentre as milhares existentes. Uma vez descoberta uma vulnerabilidade, os invasores podem expor segredos dos bancos de dados, carregar arquivos mal-intencionados em servidores Web ou bombardear um website com um surto assustador de tráfego.

Quais são os riscos associados a ataques na Web?

As organizações com baixa tolerância a riscos precisam de resoluções de alta segurança para construir uma cadeia de confiança, tanto internamente (entre sistemas, cadeia de suprimentos, operações etc.) quanto externamente (com parceiros, clientes, órgãos reguladores etc.). As APIs, em particular, desde fluxos internos simples entre as partes de um aplicativo de microsserviço até grandes transações entre empresas, são especialmente importantes para garantir a segurança: elas atuam como um vínculo digital que conecta vários sistemas e ecossistemas de parceiros, além de permitirem experiências digitais e omnicanal aos clientes.

Os cibercriminosos, infelizmente, possuem um arsenal quase ilimitado de métodos de ataque na Web projetados para causar o máximo de danos. Uma invasão bem-sucedida que resulta na exfiltração de dados confidenciais ou um ataque de DDoS que deixa seus websites indisponíveis pode destruir essa confiança e causar danos significativos, tais como a perda da fidelidade dos clientes, multas regulatórias, ações judiciais e a queda da reputação da marca.

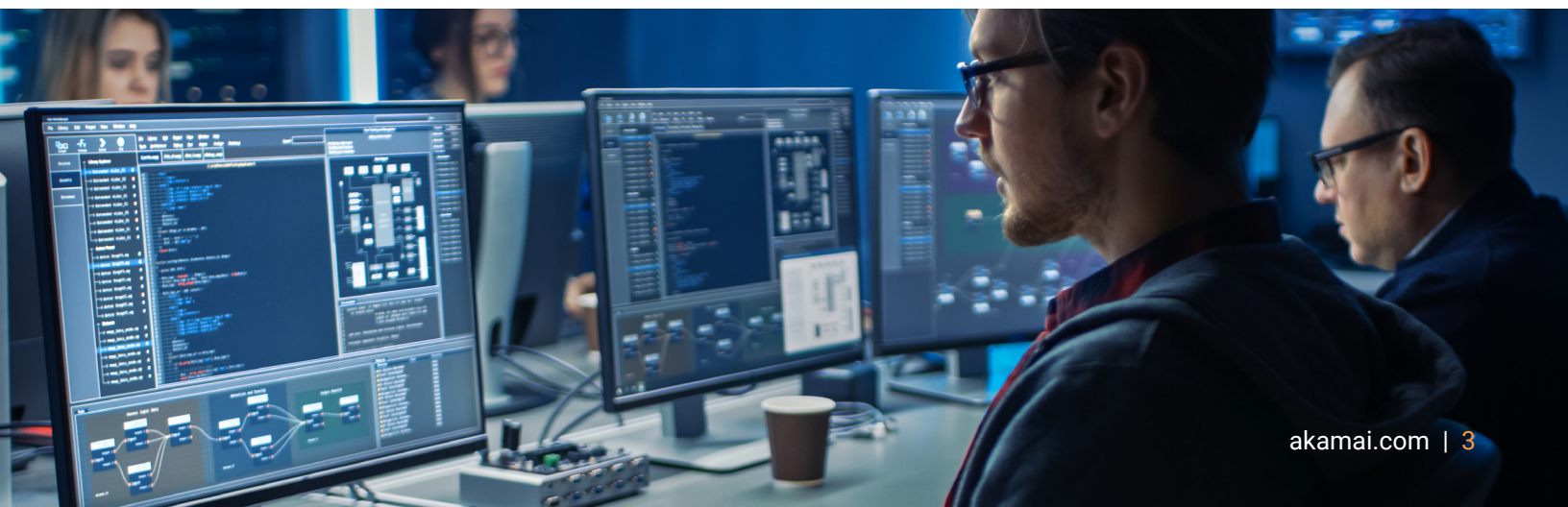
Desafios à segurança de aplicativos da Web

As soluções de proteção de aplicativos da Web e APIs (WAAP) baseadas na nuvem são projetadas para mitigar muitas formas de ataques de DDoS, ataques a aplicativos da Web e ataques baseados em APIs. No entanto, um dos principais desafios dos firewalls é que as equipes de AppSec devem analisar e ajustar as regras constantemente à medida que os aplicativos mudam, as ameaças evoluem e as atualizações se tornam disponíveis. A contratação de profissionais de segurança experientes continua sendo um desafio, com pessoas qualificadas muitas vezes mudando de função a cada dois anos. Esse é geralmente um processo manual demorado que requer operadores qualificados e não é dimensionável para a maioria das organizações devido à rotatividade, a ciclos de vida de aprendizagem e a arquiteturas especializadas de integração de tecnologias.

Políticas de segurança desatualizadas podem se tornar a fonte das frustrações, pois o excesso de alertas diminui drasticamente a capacidade de diferenciar com precisão falsos positivos de ataques reais. As equipes de segurança que não conseguem ajustar as regras com eficácia também podem tirar suas proteções de linha e aceitar conscientemente uma postura de risco elevada por medo de afetar usuários legítimos e interromper os negócios.

Por que o WAAP da Akamai?

O Akamai App & API Protector é uma solução de WAAP baseada na nuvem que inclui visibilidade e mitigação de bots, projetada para proteger seus aplicativos e APIs contra uma ampla variedade de ameaças na camada de aplicativo e de rede com menos esforços e custos. O assistente de integração por autoatendimento da Akamai reduz a necessidade de conhecimento prévio, fornecendo orientação e insights para proteger seus ativos com rapidez e facilidade. Nosso processo de configuração automatizado analisará os acionadores de segurança e aprenderá o comportamento dos aplicativos para autoajustar as proteções, resultando em mais economia de recursos. O App & API Protector elimina muitos dos problemas atuais dos firewalls que são uma fonte de atrito intraorganizacional, ônus operacional e obstrução de implantação.



As proteções automatizadas, que podem ser totalmente gerenciadas pela Akamai, são aplicadas na plataforma mais distribuída do mundo, permitindo que você adote uma abordagem prática de segurança de aplicativos e proteção de APIs. A proteção automática contra ataques na Web, como injeção de SQL, cross-site scripting e inclusão de arquivo local, fornece ampla cobertura com praticamente nenhuma manutenção contínua. E com a aplicação de machine learning e heurística, é possível aprimorar a identificação de padrões de falsos positivos em todo o tráfego de acordo com as políticas, e não com uma verificação genérica em toda a rede, para oferecer os resultados mais relevantes e práticos.

Valide sua postura de segurança com nossa ferramenta de pesquisa de CVEs, que fornece informações detalhadas por CVEs incluindo níveis de ameaça e insights sobre as proteções atuais da Akamai, para embasar suas estratégias internas de segurança e desenvolvimento. Além disso, melhore o alinhamento internamente e acelere o tempo de lançamento no mercado com as integrações de SecDevOps pré-criadas da Akamai, incluindo a Akamai como código, APIs, CLI, Terraform e integrações.

Padrão elevado com proteções adaptativas

Então, como o Akamai App & API Protector oferece simplicidade e precisão? Primeiramente, o Akamai Adaptive Security Engine, que é a tecnologia principal do App & API Protector, é diferenciado porque aprende padrões de tráfego e ataque exclusivos de cada cliente, analisa as caraterísticas de cada solicitação em tempo real e usa esse conhecimento para interceptar e adaptar-se a ameaças futuras. Essa tecnologia facilita as operações de segurança levando em conta todos os pontos de dados anômalos ou suspeitos e atribuindo uma pontuação de ameaça a cada solicitação. Quanto maior a incidência de ameaças, mais agressivas serão as proteções. Ao modificar dinamicamente as proteções para se adequarem ao nível da ameaça detectada, podemos identificar até mesmo os ataques mais evasivos, mantendo o número de falsos positivos ultrabaixo.

Os ataques a aplicativos geralmente envolvem alguma forma de reconhecimento. Porém, à medida que os invasores procuram vulnerabilidades, a Akamai reúne evidências sobre suas técnicas e táticas. Isso não só permite que a identificação ocorra em um ritmo constante, mas também proporciona um histórico do tráfego específico caso os invasores retornem. Quanto mais um invasor tentar, mais fortes serão suas proteções.

A Akamai tem insights sobre:

Mais de 780 milhões
de alertas diários sobre ataques a aplicativos da Web

Mais de 26 bilhões
de solicitações de bots

Mais de 932 TB
de dados analisados diariamente

Inteligência colaborativa contra ameaças

Muitos dos websites mais atacados na internet são de clientes da Akamai, incluindo 9 das 10 principais empresas de varejo, todos os 10 principais bancos, 9 das 10 principais empresas de saúde, todas as 6 forças armadas dos EUA e muito mais. Temos visibilidade de mais de 780 milhões de ataques diários a aplicativos da Web e 26 bilhões de solicitações de bots. Centenas de pesquisadores especializados em ameaças e cientistas de dados da Akamai consultam mais de 932 TB de novos dados diariamente em busca de ameaças. Esse nível de percepção global, aliado a machine learning, IA e análise humana, nos permite interromper ataques comuns e altamente sofisticados de modo proativo e preditivo.

A Akamai mitiga ataques a aplicativos há mais de uma década e demonstrou ser capaz de proteger os clientes e manter a disponibilidade das infraestruturas mesmo em meio aos maiores ataques já lançados. Continuamos a investigar e informar sobre ameaças emergentes e, à medida que os ataques continuam a evoluir e a se tornar cada vez mais sofisticados, continuamos a inovar e adaptar nossas soluções para ficar à frente de indivíduos mal-intencionados. E como o App & API Protector é desenvolvido na plataforma da Akamai, ele conta com recursos de desempenho pré-desenvolvidos, projetados para garantir que seus websites, aplicativos e APIs tenham o melhor desempenho possível.

Analise suas necessidades quanto à proteção de aplicativos da Web e APIs e descubra os benefícios do Akamai App & API Protector com esta avaliação gratuita.

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicativos e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. 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, antigo Twitter, e LinkedIn. Publicado em 06/24.