Proteger suas aplicações da Web pode ser uma tarefa assustadora, especialmente sem uma equipe de segurança dedicada ou treinamento. Um Web Application Firewall (WAF) mantém as ameaças afastadas e, ao mesmo tempo, preserva o desempenho das aplicações. Mas, com tantas soluções existentes, selecionar uma só não é tão simples. Vamos desfazer alguns mitos do WAF que ajudarão a avaliar o que é mais importante, para você se preocupar menos com ataques, e mais com o crescimento da sua empresa.

MITO 1: Operar um WAF é complicado.

Não deveria ser. O WAF da Akamai simplifica a segurança da camada de aplicações e contra DDoS (ataques distribuídos de negação de serviço) com conjuntos de regras fáceis de gerenciar. As regras do WAF são atualizadas automaticamente para oferecer proteção contra as ameaças de segurança cibernética mais recentes, para que as suas defesas permaneçam sempre atualizadas. As regras são testadas integralmente para manter as ameaças fora e os usuários legítimos dentro da rede, sem surpresas. E, se você precisar de experiência em segurança, a Akamai oferece acesso ao suporte 24 horas por dia, sete dias por semana e 365 dias por ano.

MITO 2: Mais regras personalizáveis entregam mais segurança.

Em termos de facilidade de uso, menos é mais. Ter mais regras para personalizar gera uma complexidade desnecessária, especialmente se sua organização não tiver uma equipe com experiência em segurança para se aprofundar nos detalhes das dependências e interações das regras. Os conjuntos de regras automatizados do WAF da Akamai são agrupados em oito categorias; tudo o que você precisa fazer é ativá-los. Com menos botões para ajustar, você fica menos propenso a causar um problema ao mexer com eles.

MITO 3: As interrupções são um dos custos de fazer negócios.

As interrupções não são mais uma parte aceitável de fazer negócios on-line. *A Network World* relata que uma hora de inatividade pode custar às pequenas empresas até US$ 8.000 e, às empresas de médio porte, até US$ 74.000. Oferecendo escala e resiliência com 100% de disponibilidade em mais de 130 países e em mais de 1.700 redes em todo o mundo, a Akamai é a empresa de confiança da maioria dos setores mais sensíveis à disponibilidade, incluindo oito das principais empresas globais de FinTech e 91 dos principais varejistas de Internet dos EUA.

MITO 4: As atualizações mais rápidas das regras proporcionam uma defesa mais rápida das aplicações.

Não se essas regras não forem devidamente verificadas. Quando colocadas em produção às pressas, as novas regras de WAF podem causar o efeito oposto. Para proteger nossos clientes, a Akamai testa as novas regras em duas fases: primeiro, em nosso laboratório, utilizando tráfego legítimo e mal-intencionado conhecido; depois, na plataforma, para analisar a mudança de falsos positivos e falsos negativos em relação ao tráfego da Internet em tempo real. Não troque velocidade por qualidade, permitindo que sua empresa experimente novas regras.

MITO 5: A análise de ameaças por crowdsourcing oferece proteção suficiente.

Uma análise que dependa exclusivamente de crowdsourcing não tem precisão, validação nem contexto para o comportamento, além de não considerar falsos positivos. Entregando mais de 95 exabytes de dados em bilhões de dispositivos para mais de seis mil das maiores empresas on-line, a Akamai tem uma invejável visibilidade sobre enormes quantidades de tráfego legítimo e mal-intencionado em todo o mundo e entre os setores. Observando esse tráfego, os especialistas em segurança da Akamai podem ver como os ataques e o tráfego legítimo evoluem. Essa percepção beneficia a precisão das regras em todos os setores.

MITO 6: Um maior número de acionadores de regras indica melhores resultados.

O número de acionadores de regras é apenas o ruído da máquina. O que realmente importa é a correlação e a pontuação dos acionadores que resultam no número de ataques detectados pelo WAF. A Akamai oferece mais de dois trilhões de interações na Internet e interage com mais de 100 milhões de endereços IP todos os dias, o que nos dá inteligência e percepções incomparáveis. A maioria dos ataques começa em um setor antes de avançar para outros. Com centenas de milhões de ataques na Web em vários mercados verticais observados todas as semanas, a perspectiva exclusiva da Akamai ajuda você a se antecipar às ameaças e a se proteger dos ataques virtuais antes que eles se espalhem.

MITO 7: Você não precisa proteger suas APIs.

Em um mundo digital cada vez mais conectado, não é suficiente proteger suas páginas da Web. A segurança adequada das APIs reduz sua superfície de ataque. O WAF da Akamai pode proteger as APIs contra ataques DDoS e a aplicações Web, bloqueando o tráfego da API com base no endereço IP, na localização geográfica, no acesso anormal ou em uma taxa excessiva de solicitações. O WAF da Akamai inspeciona automaticamente as solicitações de API (incluindo JSON e XML) em busca de conteúdo mal-intencionado, estendendo um alto nível de proteção dos websites às APIs.

MITO 8: Um WAF pode oferecer proteção contra todos os ataques do dia zero.

Por definição, um ataque do dia zero ainda não é conhecido; portanto, nenhum fornecedor pode fazer essa promessa. Mas isso não significa que um WAF não possa ajudar. Por exemplo, o WAF da Akamai usa regras baseadas em anomalias para identificar ataques do dia zero que compartilham semelhanças com casos conhecidos. Projetado como um mecanismo de pontuação de anomalias, o WAF da Akamai tem detectado ataques que exploram vulnerabilidades do dia zero sem nenhum ajuste adicional necessário. Além disso, as regras do WAF da Akamai são atualizadas automaticamente, para que você não precise acompanhar o cenário de ameaças em constante mudança.

MITO 9: Um WAF atenua todos os bots.

Embora um WAF ofereça uma camada importante de proteção contra bots, o WAF da Akamai bloqueia os bots conhecidos *e* aqueles que enviam muito tráfego. Quando deixados sem supervisão, os bots com alta geração de tráfego danificam os sistemas e afetam o tráfego legítimo. Um WAF é uma maneira fácil de gerenciar bots que drenam recursos sem causar qualquer outro dano. Se os operadores de bots mais sofisticados direcionarem ataques a uma organização, eles encontrarão uma forma de contornar o WAF. Nesses casos, a Akamai também oferece soluções especializadas de gerenciamento de bots que detectam e oferecem proteção contra ameaças avançadas de bots, como roubo de credenciais.

MITO 10: As soluções pontuais individuais são superiores em suas áreas de especialização.

Quando se trata de oferecer proteção contra as mais recentes ameaças de segurança virtual, a transferência de conhecimentos que acompanha uma variedade de ofertas de segurança (e o volume de incidentes observados juntamente com elas) cria uma proteção automatizada mais eficaz, uma melhor detecção de anomalias e conjuntos de regras de melhor qualidade. Uma estratégia de segurança que usa soluções pontuais de vários fornecedores, geralmente, é mais difícil de gerenciar, requer mais treinamento e apresenta desafios de integração.

Para saber mais sobre como o WAF da Akamai pode facilitar a segurança para você com proteção da camada de aplicações e contra ataques DDoS, visite Akamai.com/Security.

Akamai

A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A plataforma de borda inteligente da Akamai cerca tudo, da empresa à nuvem, para que os clientes e seus negócios possam ser rápidos, inteligentes e protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a alcançar a vantagem competitiva por meio de soluções ágeis que estendem a potência de suas arquiteturas multinuvem. A Akamai mantém as decisões, aplicações e experiências mais próximas dos usuários, e os ataques e ameaças cada vez mais distantes. O portfólio de soluções de segurança de borda, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeo da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, sete dias por semana, durante todo o ano. Para saber por que as principais marcas mundiais confiam na Akamai, visite **akamai.com**, **blogs.akamai.com** ou **@Akamai** no Twitter. Encontre nossas informações de contato globais em **akamai.com/locations**. Publicado em 04/19.