AZION

6 técnicas imprescindíveis para proteger o seu site

Com mais pessoas comprando, se comunicando e trabalhando online mais do que nunca, muitos sites da web estão presenciando um crescimento sem precedentes. Porém, quanto mais visitantes o site atrai, mais ele se torna um alvo para bad bots, fraudes e outras atividades maliciosas.

Isso significa que verificar a existência de vulnerabilidades e garantir que os melhores práticas de segurança venham sendo aplicadas é assunto crítico. Pensando nisso, compartilhamos algumas dicas com você. Confira!

Proteja-se contra DDoS Attacks

Independentemente do tamanho do site, os ataques DDoS dispararam desde o início da pandemia. DDoS, sigla para distributed denial of service - negação de serviço distribuída -, é um tipo de ataque projetado para tirar um site do ar, sobrecarregando-o com tráfego falso. Derrubando seu site, os hackers não apenas impedem o acesso de usuários legítimos, mas também prejudicam a reputação da marca ao fazer os serviços parecerem não confiáveis. Além de os ataques DDoS estarem ocorrendo com frequência cada vez maior, eles estão evoluindo tanto em tamanho como em complexidade, abrangendo diferentes tipos de dispositivos e visando diversas partes da rede-alvo.

Por isso, o DDoS Protection da Azion permite que você escolha o nível de proteção conforme as suas necessidades, oferecendo desde 5 Gbps até proteção ilimitada contra ataques de qualquer tamanho. A Azion usa sofisticados algoritmos de rede definidos por software, emparelhados com muitos pontos de presença geográfica, a fim de oferecer capacidade de mitigação de DDoS quase ilimitada. Além disso, todos os níveis de proteção DDoS da Azion fornecem mitigação sempre ativa com Deep Packet Inspection (DPI) e algoritmos avançados para detectar e bloquear imediatamente o tráfego malicioso.

Proteja seus sites contra vulnerabilidades críticas

Ano após ano, vemos as mesmas vulnerabilidades expondo sites a ameaças por longos períodos - consulte o relatório Veracode's State of Software Security v11. Apesar dos bilhões gastos em práticas de codificação segura, muitas vezes encontramos sites vulneráveis a ataques críticos, incluindo cross-site scripting (XSS) e SQL injections, que podem causar danos irreparáveis à reputação do seu site ao extrair dados confidenciais de clientes, levando a dispendiosas violações de dados. Mesmo que seus desenvolvedores sejam treinados em técnicas de codificação seguras, você não tem controle total sobre a sua cadeia de suprimentos de software e as bibliotecas de terceiros que provavelmente esteja usando.

Em vez de focar recursos preciosos de desenvolvimento na correção de todas as vulnerabilidades em sua cadeia de suprimentos de software, o Web Application Firewall (WAF) da Azion protege contra a exploração de vulnerabilidades críticas e outras importantes ameaças como as OWASP Top 10.

Impedir bots maliciosos e outras ameaças automatizadas

À medida que nos tornamos cada vez mais digitais, os hackers continuam a empregar bots para realizar todos os tipos de ataques e comportamentos maliciosos. Invasões a contas - Account Takeover (ATO) - são formas comuns para agentes mal-intencionados obterem acesso às contas online das vítimas, por meio de ataques de força bruta, adivinhando combinações de senha, ou de credential stuffing, técnica que consiste em testar credenciais roubadas com objetivo de violar dados.

O Azion Network Layer Protection bloqueia bots testando credenciais por meio de rate limit. Isso permite que você controle quantas vezes um usuário pode tentar fazer login antes de bloquear as tentativas subsequentes por um período de tempo definido. A limitação de taxa também pode ser usada para minimizar o spam que os bots poderiam inserir nos campos de formulário, desfigurando os painéis de mensagens do seu site e até mesmo prejudicando a classificação de SEO de seu site. O Network Layer Protection também pode bloquear solicitações de determinados IPs, como aqueles associados a bots. As listas de reputação de IP podem ser atualizadas de modo programático via API utilizando a própria pesquisa de ameaças da Azion ou qualquer feed de reputação de IP de terceiros.

Para cobrir toda a gama de ameaças automatizadas e de bots, a Azion possui parcerias com empresas líderes em segurança, incluindo o Bot Manager da Radware, para oferecer a melhor e mais completa segurança de aplicações web atuantes no mercado através do Azion Marketplace.

Ao mesmo tempo em que o Bot Manager complementa as próprias proteções da Azion contra invasão a contas, abuso de API, DDoS de aplicações e form spamming, também estende a proteção contra outros tipos de ataques automatizados importantes, incluindo web scraping, carding, abandono de carrinho, fraude de anúncio digital e muitos outros. A Radware utiliza várias técnicas para determinar se uma solicitação é legítima, incluindo machine learning, device fingerprint, rastreamento de redes proxy e TOR, análise comportamental e de intenção, entre tantas outras. Resultado? Proteção entregue com um índice muito baixo de falsos positivos e nenhum impacto sobre os usuários finais do seu site.

Crie múltiplas camadas de segurança

Dizer que as equipes de segurança enfrentam uma infinidade de desafios atualmente é um eufemismo. O crescimento de aplicações SaaS, infraestrutura em cloud e arquiteturas de microsserviços, combinado com uma crescente força de trabalho móvel e base de clientes que acessam aplicações em qualquer tipo de dispositivo, expandiu o perímetro corporativo e abriu novas planos de ameaças. Por isso é importante implementar segurança multicamadas, evitando que um único ponto de falha comprometa suas aplicações web críticas.

Na Azion, atualizamos constantemente nossa plataforma a fim de ajudar clientes a implementar segurança multicamadas. O Azion WAF oferece às equipes de segurança capacidade de proteção contra ameaças conhecidas como OWASP Top 10 e também ataques zero-day, com conjuntos de regras personalizados, flexíveis o suficiente para proteger qualquer tipo de aplicação. Para proteção contra ataques DDoS de alto volume que usam a infraestrutura da DNS, a Azion desenvolveu algoritmos de roteamento sofisticados utilizados no Intelligent DNS, o que manteve disponível a infraestrutura crítica de nosso cliente com sucesso, mesmo em meio a ataques multiGbps.

O Origin Shield permite que os clientes da Azion implementem redes zero trust, limitando o acesso de origem apenas aos endereços de IP da Azion, enquanto bloqueiam solicitações de todas as outras redes. Contudo, você não consegue impedir as ameaças que você não vê. Então, a Azion desenvolveu os produtos Data Streaming e Real-Time Metrics para aumentar sua capacidade de observability e proporcionar uma visão correta de forma a manter seus sites totalmente protegidos - de hackers externos, membros da equipe mal-intencionados, por exemplo.

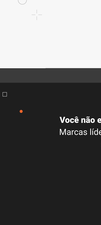
Impedir o abuso de API

Atualmente,APIs são componentes fundamentais para sites e serviços. Mas quando ficam desprotegidas, são facilmente exploradas por invasores automatizados em busca de dados privados. Para explorar as vulnerabilidades lógicas do negócio, os invasores podem fazer repetidas chamadas de API de alto volume em servidores de aplicações ou tornar as solicitações POST lentas, resultando em negação de serviço.

O Network Layer Protection da Azion permite que as empresas limitem a taxa desse tipo de solicitação para mitigar chamadas de API em grande escala. O Network Layer Protection também possibilita aos clientes bloquear chamadas de API maliciosas, baseadas em IP, que podem ser atualizadas de modo programático com feeds de reputação de IP próprios da Azion ou de terceiros.

Finalmente, você ainda conta com o Origin Shield, um recurso opcional de Network Layer Protection, que permite aos nossos clientes ocultar os servidores de aplicações, os quais costumam ser alvos de ataques DDoS em APIs.

Mitigar campanhas de phishing



Até mesmo a base de usuários mais treinada e vigilante clicará involuntariamente nos links de um e-mail de phishing. A maioria desses ataques utilizará cross-site scripting (XSS) para injetar código, normalmente HTML ou JavaScript, no conteúdo de uma página da web infectada - a página da web para a qual o hacker envia suas vítimas. Quando a vítima visita a página infectada, o script malicioso é refletido de volta ao navegador, permitindo que o hacker roube seus cookies de sessão e sequestre sua conta.

O WAF da Azion pode evitar a injeção de código HTML e JavaScript malicioso em um site que não tenha sanitização de entrada suficiente ou simplesmente bloquear solicitações suspeitas. Para derrotar ataques de phishing que tentam alavancar seu próprio conteúdo - imagens estáticas, por exemplo -, o Azion WAF permite que você inclua na lista de permissões quais domínios podem ser referências para seus assets e, assim, bloqueia todos os outros.

Além disso, o Data Streaming da Azion reúne e transmite eventos de aplicações em tempo real por meio de conectores com sua infraestrutura de análise existente - SIEMs, Elastic, Kafka, por exemplo -, de forma a detectar anomalias. No caso de um ataque de phishing, o Data Streaming registrará alguns indicadores de anormalidades, incluindo um HTTP Referer vazio ou malicioso.

Por meio do Data Streaming, uma grande empresa brasileira de e-commerce identificou mais de 8.000 tentativas de phishing em um mês - mais de 10x o que eles detectavam anteriormente! Os insights do Data Streaming podem ser usados para atualizar as regras do Azion WAF de modo programático utilizando APIs para obter maior proteção contra ataques de phishing.

Você não está sozinho na luta para proteger seus sites e aplicações da web.
Marcas líderes confiam na Azion para potencializar sites e aplicações da web seguros e de alto desempenho por quase uma década.
Adoraríamos ajudar você também!

Contate a Azion hoje!

Entre em contato conosco