Akamai

WHITE PAPER

11 mitos sobre DDoS que simplesmente não desaparecem

Os ataques DDoS (negação de serviço distribuída) aumentaram drasticamente em tamanho, escala, distribuição e sofisticação nos últimos anos, o que é destacado por alguns ataques que quebraram recordes. Infelizmente, muitas organizações ainda se prendem a algumas ideias ultrapassadas sobre como se defender, presumindo que suas defesas são suficientes ou, pior ainda, que é improvável que sejam um alvo. A verdade é: as vítimas desses ataques abrangem todos os principais setores, de serviços financeiros a comércio eletrônico e jogos. De fato, os ataques à infraestrutura pública essencial, incluindo saúde, energia e serviços públicos, educação e transporte, têm sido uma preocupação especial. Em 2023, a Akamai protegeu um cliente na região Ásia-Pacífico de um ataque massivo de 900 Gbps (gigabits por segundo). No final do mesmo ano, a Akamai impediu um ataque de 634 Gbps e 55 Mpps (milhões de pacotes por segundo) que apresentava uma combinação complexa de vetores de ataque, representando um dos maiores ataques já realizados contra um cliente de serviços financeiros dos EUA. Isso se soma ao maior ataque DDoS que a Akamai mitigou até o momento: um ataque distribuído globalmente de 1,44 Tbps e 385 Mpps que durou quase duas horas. Esses eventos deixam claro que os cibercriminosos continuam a atingir os pilares essenciais da economia.

Embora a escala desses ataques possa levar algumas organizações menores a acreditarem que seu risco de se tornar alvo de um ataque DDoS é baixo, a realidade é que os serviços e aplicativos essenciais para negócios em todos os setores são alvos fáceis. O aumento de hacktivistas com motivações políticas e ideológicas e o custo relativamente baixo do DDoS como serviço oferecido por grupos de cibercriminosos, como Killnet e Anonymous Sudan, tornaram quase todo mundo um possível alvo. Não é apenas com o ataque inicial que as organizações precisam se preocupar. Os ataques DDoS estão sendo cada vez mais usados como uma cortina de fumaça para distrair os recursos de rede e segurança, enquanto os invasores tentam ataques RDDoS (DDoS de ransomware) simultâneos ou outras explorações nefastas, como campanhas de extorsão tripla. Por fim, a adoção crescente e alarmante de ferramentas de inteligência artificial para orquestrar ataques DDoS altamente sofisticados e distribuídos cria um desafio defensivo significativo para empresas e instituições públicas que precisam garantir disponibilidade e desempenho consistentes.

Como as ameaças se tornam mais complexas e evoluem a cada dia, infelizmente ainda existem muitos mitos sobre a proteção contra DDoS, alguns deles até incentivados pelos fornecedores de segurança. A proteção contra DDoS deve ser um princípio fundamental de qualquer estratégia de segurança, portanto, compreender o perigo que esses mitos representam é essencial para sua defesa contra DDoS.

MITO 1

A capacidade total indica a extensão total dos recursos de mitigação disponíveis

Embora a capacidade total seja importante, um simples número de capacidade de rede pode ser enganoso, pois deixa de fora detalhes importantes. As organizações que estão avaliando as soluções tecnológicas de proteção contra DDoS precisam se perguntar:

- Quanta capacidade de rede é dedicada ao tráfego de ataques que consomem recursos?
- Quantos dos recursos do sistema de mitigação são **explicitamente dedicados** a impedir ataques?
- Quantos recursos de rede e sistema estão disponíveis para fornecer tráfego limpo para todas as origens de clientes nessa plataforma e para cada locatário exclusivo?

Essas perguntas são essenciais porque, se a capacidade total da rede incluir outros requisitos (como o fornecimento de conteúdo), a capacidade real de defesa contra DDoS poderá ser apenas uma fração do que o provedor está alegando.

A capacidade de defesa contra DDoS também não se limita apenas à tecnologia. Em algum momento, se a tecnologia parar de funcionar de forma eficaz, haverá recursos humanos dedicados para escalonamentos, resposta a incidentes e ajuste de mitigação? A mitigação mais robusta combina automação e inteligência de máquina com conhecimento humano para oferecer proteção aprofundada.

Dica

Analise mais detalhadamente as diferenças entre a capacidade total da rede de um provedor e a estabilidade de sua plataforma, bem como a capacidade que ele tem para mitigação de ataques e entrega de tráfego limpo. Esses elementos devem ser considerados segmentos exclusivos. Por exemplo, a capacidade deve ser dedicada por finalidade, como roteamento de rede do tráfego de ataque, interrupção ou mitigação do tráfego de ataque e fornecimento de tráfego limpo de volta ao data center.

MITO 2

A proteção contra DDoS de provedores de serviços de Internet e/ou provedores de serviços em nuvem é suficiente

Infelizmente, muitas organizações ainda acham que a proteção oferecida por seu ISP (provedor de serviços de Internet) é tudo o que precisam. A verdade é: em geral, os ISPs fornecem apenas proteção contra DDoS reformatada, comercial e pronta para uso, com largura de banda limitada. O hardware deles é compartilhado entre a própria infraestrutura e a sua, o que significa capacidade e ciclos de CPU limitados. Atualmente, os ataques de DDoS são tão grandes que podem sobrecarregar ambas as infraestruturas, e os ISPs farão o roteamento nulo (ou blackholing) do seu tráfego para evitar danos colaterais a outros recursos de produção. Ao rotear todo o tráfego para um buraco negro (blackhole), as empresas perdem o tráfego e os serviços legítimos dos usuários finais, tornando o ataque bem-sucedido ao colocar os negócios fora do ar para todos os fins práticos.

Além disso, embora os CSPs (provedores de serviços em nuvem) geralmente permitam que os clientes definam seus próprios controles e mantenham a soberania sobre sua postura de segurança no ambiente de nuvem do CSP, a maioria dos próprios CSPs geralmente rejeita qualquer responsabilidade e acaba cobrando dos clientes pelo tráfego DDoS ilegítimo. Isso pode levar a excedentes significativos para as vítimas, dada a escala e o tamanho dos ataques DDoS modernos.

Dica

Verifique atentamente e negocie as cláusulas de proteção contra DDoS com seu ISP ou CSP. Além disso, determine se o seu ISP usa hardware robusto de proteção contra DDoS no local com um backup na nuvem, de modo que ataques DDoS pequenos, mas rápidos, sejam mitigados no local, enquanto ataques volumétricos grandes possam ser mitigados adequadamente por um serviço de proteção contra DDoS na nuvem.

MITO 3

Todos os SLAs de tempo de mitigação são criados da mesma forma

Às vezes, os números podem induzir ao erro. O TTM (tempo para mitigar) é um número frequentemente comercializado pelos fornecedores de segurança. Idealmente, o TTM significa a rapidez com que o tráfego DDoS mal-intencionado é interrompido ou bloqueado, sem afetar o tráfego e os usuários legítimos. No fim das contas, há muito espaço para interpretações aqui. Por exemplo, um fornecedor pode não considerar um aumento no tráfego como um ataque DDoS até que ele tenha durado pelo menos cinco minutos consecutivos. Portanto, o cronômetro do SLA (Acordo de Nível de Serviço) pode não começar até que você já esteja sendo atacado. Como a duração média de um ataque é inferior a cinco minutos, dá para ver como isso pode ser um problema: isso significa que um tempo anunciado de 10 segundos para mitigar pode ser, na verdade, mais de cinco minutos.

Outros fornecedores definem o tempo de mitigação como a rapidez com que uma regra de mitigação pode ser implantada. Isso não reflete a interrupção do ataque, nem a qualidade ou a consistência com que esse controle é ativado. No final das contas, o que importa é o tempo necessário para que os ativos voltados para a Internet sejam protegidos e voltem a funcionar, **com o mínimo de impacto para os usuários ou serviços legítimos**. Certifique-se de ler cuidadosamente as letras miúdas do SLA de seu fornecedor.

Dica

Aprofunde-se nos detalhes sobre o tempo de mitigação informados em um SLA. Eles devem representar a equação: o tempo real que importa = tempo para detectar o ataque + tempo para aplicar controles de mitigação + tempo para bloquear/parar o ataque + qualidade/consistência da mitigação. Selecione um fornecedor que ofereça um **verdadeiro SLA de zero segundo** para mitigar ataques DDoS sem afetar usuários legítimos.

MITO 4

Roteamento nulo/blackholing e limitação de taxa são defesas aceitáveis

O roteamento nulo (ou blackholing) é uma resposta defensiva comum e bastante primitiva de alguns provedores de mitigação de DDoS. Se um ativo estiver sendo atacado e essa capacidade de ataque estiver colocando em risco outros clientes ou serviços, o provedor poderá tentar evitar danos colaterais lançando o tráfego desse recurso em um buraco negro virtual. Isso realmente ajuda você? Do ponto de vista de um invasor, o blackholing significa que a missão foi cumprida: o alvo visado está efetivamente offline. Dependendo da infraestrutura do provedor, outros clientes também podem acabar ficando offline ou apresentar redução do desempenho.

Outra resposta primitiva de defesa contra DDoS oferecida por muitos provedores de segurança inclui a imposição de limites de taxa no tráfego do cliente como uma contramedida em ambientes compartilhados. Mas reduzir o tráfego legítimo em 20% a 40% para dar a impressão de que o ativo ou o serviço ainda está em operação não é um resultado bem-sucedido para o cliente que está sendo atacado. A limitação de taxa é eficaz como uma contramedida secundária ou terciária ao lidar com ataques DDoS nas camadas 3, 4 e 5. Ao confrontar ataques DDoS da camada 7, a limitação de taxa pode ser mais eficaz como um controle inicial, mas você deve sempre confiar na mitigação de assinatura primeiro. Você merece ter 100% da sua infraestrutura digital efetivamente protegida contra ataques DDoS, independentemente da camada do modelo de interconexão de sistemas abertos afetada, e certamente não apenas 60% ou menos.

Dica

Pergunte ao seu provedor com que frequência ele aplica blackholing ou limita a velocidade do tráfego durante momentos tranquilos e sob ataque. Determine quando (em que condições) um provedor aplica blackholing no tráfego e quais critérios você precisará atender para que ele restaure seus serviços.

MITO 5

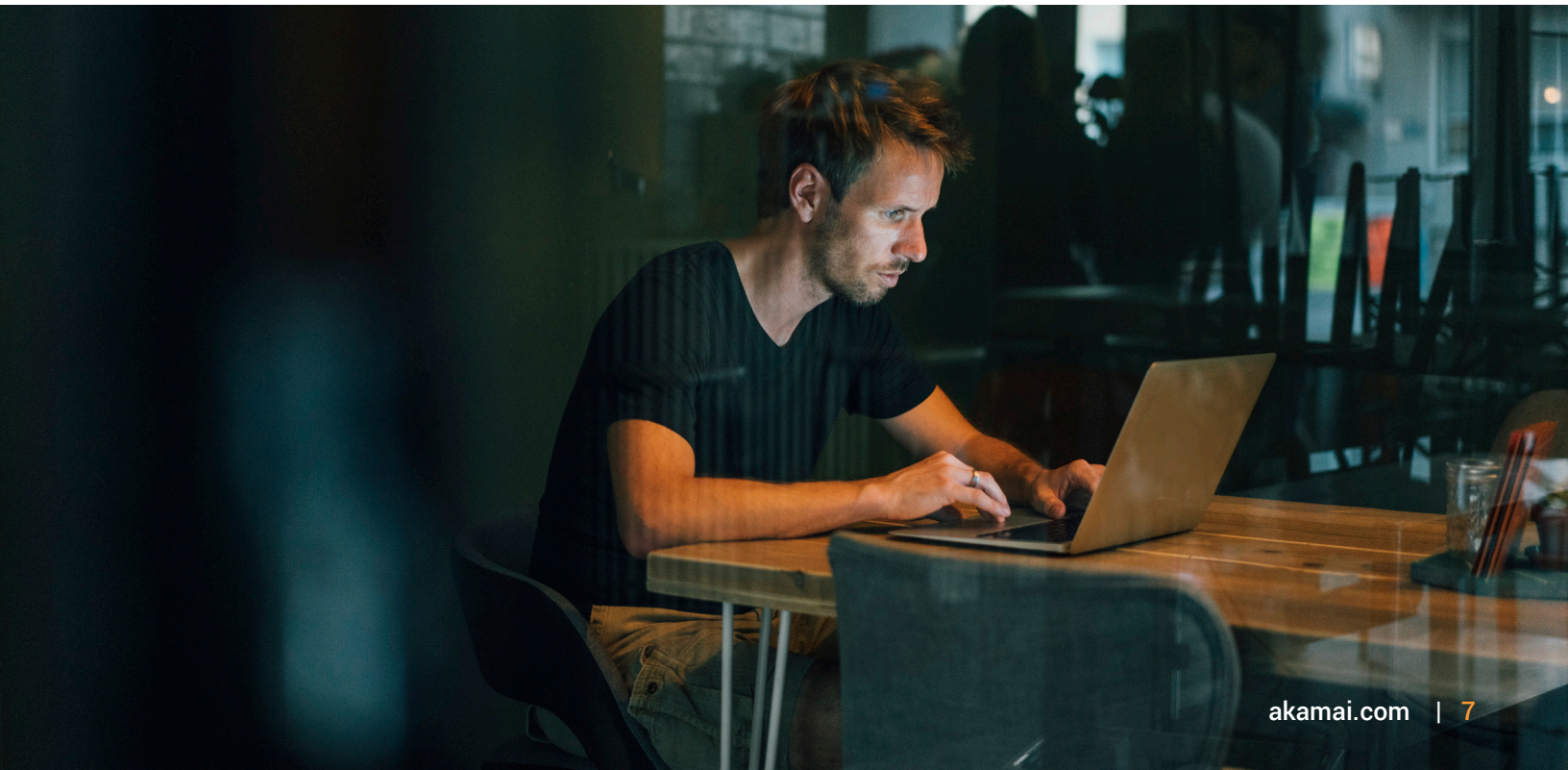
Não importa quem compartilha a plataforma em nuvem

Toda organização precisa de segurança. Empresas polêmicas que atraem ataques frequentes, por exemplo mercados cinzas do tipo websites de jogos de azar e de conteúdo adulto, também precisam de defesas de segurança contra DDoS. Até mesmo organizações que promovem atividades criminosas e ataques terroristas adquiriram cibersegurança de fornecedores legítimos de nuvem.

É fácil pensar que esses sites não são importantes para você. No entanto, se sua empresa compartilha uma plataforma na nuvem com uma empresa ilegal ou que é atacada com frequência, o potencial de danos colaterais é alto. Os recursos do fornecedor podem estar ocupados ou sobrecarregados, deixando sua organização exposta.

Dica

Leia cuidadosamente a política de uso aceitável de um fornecedor de segurança na nuvem para confirmar que você não compartilhará recursos da plataforma de segurança com alvos de alto risco. Além disso, reveja as dicas que seguem o Mito 1 e o Mito 2 com relação à capacidade e ao recurso.



MITO 6

Um firewall de aplicativos da Web é suficiente para proteção contra DDoS

Os WAFs (firewalls de aplicativos da Web), que geralmente fazem parte de um grupo maior de soluções de WAAP (proteção de APIs e aplicativos da Web), oferecem proteção eficaz contra DDoS para ataques na camada de aplicativos (camada 7). Embora eles possam oferecer alguma proteção básica na camada de rede (camada 3) ou na camada de transporte (camada 4), isso não é suficiente para cobrir todos os IPs, portas e protocolos de forma abrangente.

Os ataques DDoS têm vários tipos e formatos e podem ter como alvo as camadas de infraestrutura (camadas 3 e 4), a camada de aplicativos HTTP(s) (camada 7) e a infraestrutura de DNS (Sistema de Nomes de Domínio). Além disso, os invasores costumam alternar dinamicamente os ataques que podem, por exemplo, começar com o DNS e, posteriormente, expandir para outras camadas ou protocolos. A verdadeira proteção contra DDoS vem de uma estratégia de defesa em profundidade que adota uma plataforma de soluções robustas com pontos fortes e recursos específicos para oferecer proteção à camada 3, camada 4, camada 7 e DNS. Uma única solução, por si só, nem sempre é suficiente para cobrir todas os aspectos e pode deixar sua organização vulnerável a ataques e a níveis mais altos de risco por excesso de mitigação de tráfego ou serviços legítimos.

Dica

Certifique-se de que sua solução de proteção contra DDoS não esteja voltada para um tipo específico de ataque DDoS ou projeto de implementação. A melhor defesa vem de um único fornecedor que pode fornecer vários recursos dedicados de proteção contra DDoS que mantêm a interoperabilidade e são apoiados por uma equipe unificada de serviços de segurança de resposta rápida para proteger seus recursos de produção. A situação se torna complexa quando esses ativos são implantados em redes híbridas e ambientes hospedados na nuvem. Os serviços de proteção devem ser independentes da rede ou do modelo de implementação.

MITO 7

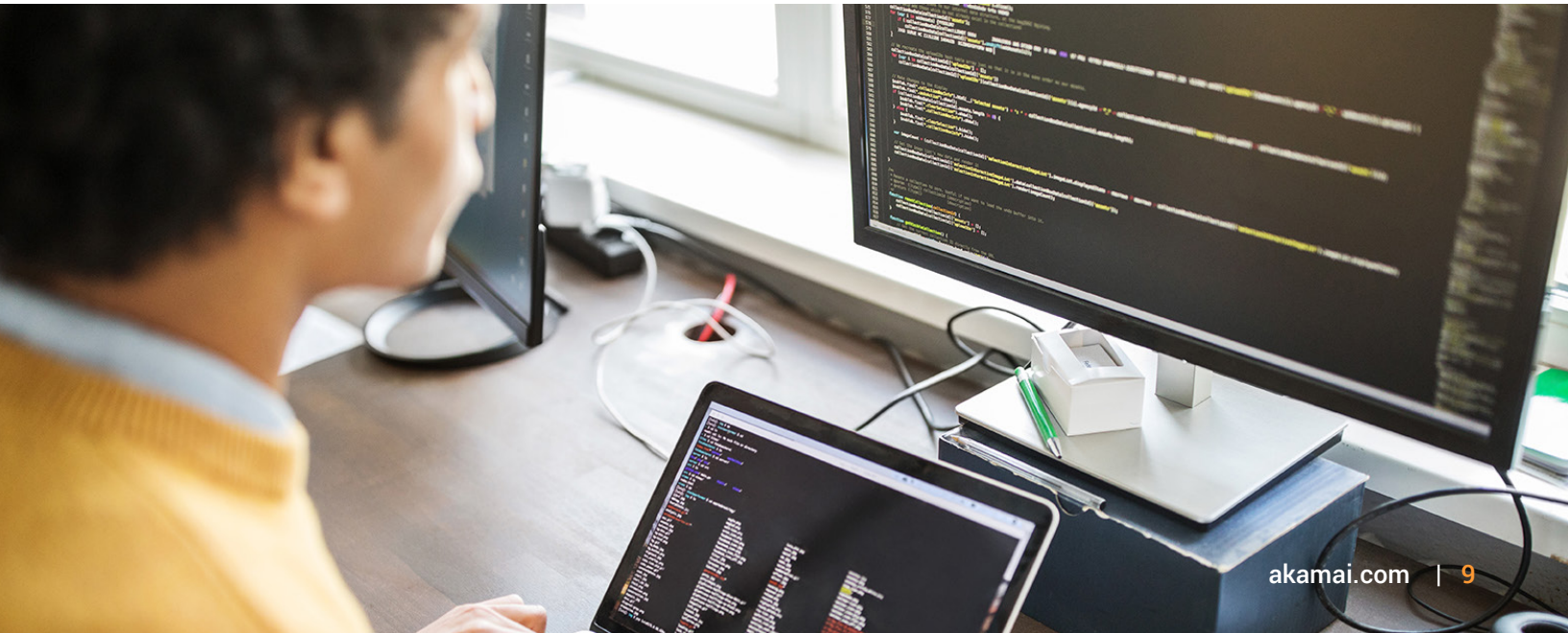
Uma plataforma de segurança abrangente = uma melhor experiência de segurança

Alguns provedores oferecem uma variedade de serviços empilhados sobre uma única plataforma de nuvem. Isso pode reduzir a complexidade técnica da implementação e integração de controles de segurança no curto prazo, mas vários serviços que compartilham a mesma infraestrutura e redes de back-end são vulneráveis a interrupções de plataforma, danos colaterais e problemas de resiliência se outras partes do ambiente forem interrompidas. Muitas vezes, fornecedores que oferecem vários serviços como esse sacrificam a funcionalidade dos recursos devido às limitações de sua abordagem de plataforma única.

Uma malha transparente de plataformas ou soluções de proteção de CDN (Rede de Entrega de Conteúdo), DNS e DDoS criadas para fins específicos, projetadas para solucionar desafios técnicos e de segurança específicos, significa mitigação e desempenho de maior qualidade em escala para otimizar as posturas defensivas.

Dica

Lembre-se de que você não precisa compartilhar a mesma infraestrutura para obter uma experiência unificada de segurança. Uma abordagem de defesa diversificada usa arquiteturas subjacentes que podem oferecer uma experiência de usuário perfeita, bem como mitigação de segurança de alto desempenho.



MITO 8

A proteção contra DDoS não é necessária para o IPv6

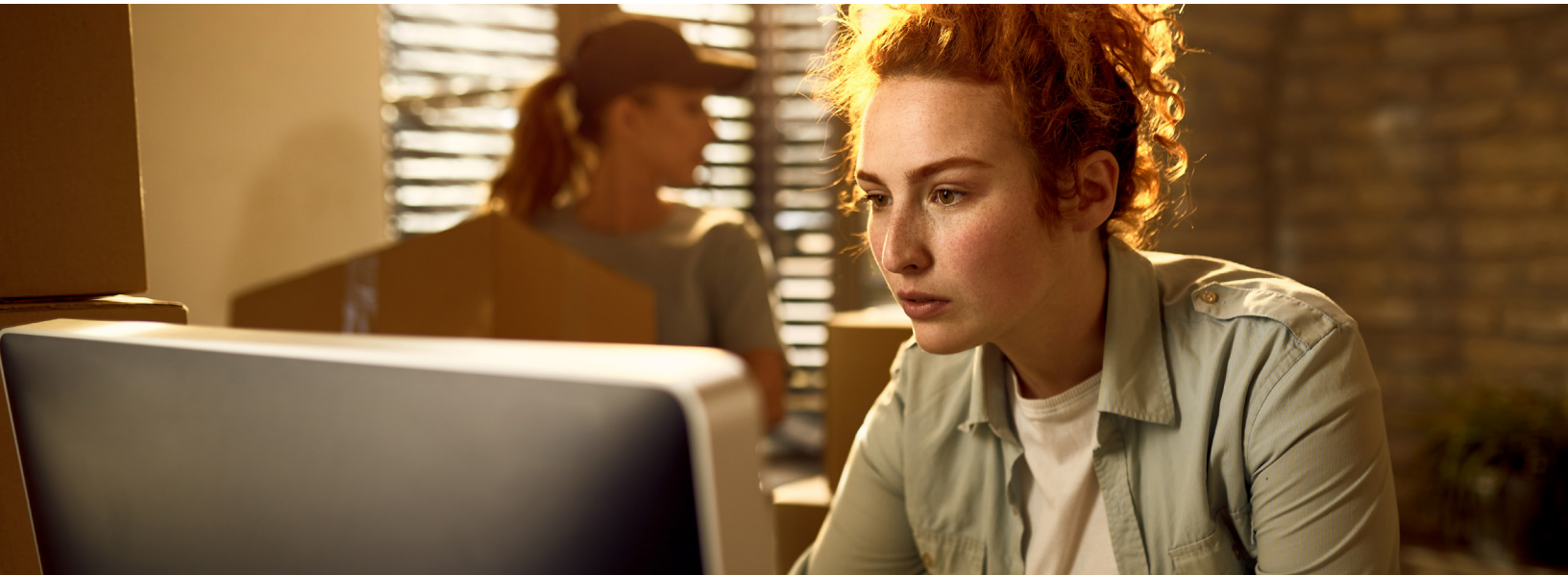
De acordo com o Google, cerca de 45% do tráfego de Internet tem origem em dispositivos compatíveis com IPv6. Em termos de ataques DDoS, o IPv6 apresenta algumas melhorias em relação ao IPv4, como um espaço de endereço maior e recursos de segurança integrados, como o IPsec, mas não protege inerentemente contra esses tipos de ataques.

Os ataques DDoS podem ter como alvo redes IPv4 e IPv6, sobrecarregando-as com um grande volume de tráfego, explorando vulnerabilidades ou usando vários vetores de ataque que são independentes da versão do IP. Os cibercriminosos já estão usando o espaço IP significativamente expandido do IPv6 para criar ataques DDoS volumétricos ainda maiores. Em alguns casos, os invasores enviaram tráfego para endereços aleatórios em uma rede, criando uma tempestade de transmissão na camada de rede física e sobrecarregando e esgotando recursos do roteador ou da rede.

A fragmentação atual entre o IPv4 e o IPv6 acrescenta mais complexidades, já que normalmente não se pode presumir ambientes IPv6 limpos.

Dica

A proteção contra DDoS para IPv6 requer estratégias e tecnologias semelhantes às do IPv4, incluindo monitoramento de rede, filtragem de tráfego, limitação de taxa e emprego de serviços especializados de mitigação de DDoS.



MITO 9

Você não precisa de várias camadas de defesa

A maioria das organizações não acredita de fato nesse mito, mas, às vezes, elas criam sua estratégia de defesa como se fosse verdade. Ao proteger sua casa, trancar sua porta da frente não significa que você pode deixar a porta dos fundos e as janelas destrancadas. A verdadeira defesa contra DDoS é obtida por meio da criação de camadas de segurança que trabalham juntas de forma integrada para impedir que os invasores atinjam seu objetivo em um único golpe.

A defesa contra DDoS de classe mundial começa com um firewall de nuvem de rede que alivia a carga de seus firewalls para a edge de sua rede. Em seguida, um modelo híbrido de proteção contra DDoS incluirá proteção no local, baseada em dispositivos de hardware, contra ataques DDoS curtos, mas acentuados, e recorrerá à proteção dedicada baseada em nuvem para ataques DDoS grandes, complexos e volumétricos. Sua infraestrutura de DNS também precisa ser protegida com uma estratégia em camadas semelhante, que inclua o uso de um serviço de proxy que possa implementar dinamicamente políticas de segurança na edge da rede e que seja ainda mais estruturada com uma solução de DNS autoritativo no modo primário ou secundário. Por fim, você deve proteger todos os seus aplicativos e APIs com uma solução WAAP robusta que inclua a funcionalidade WAF.

Dica

Coloque em camadas as melhores tecnologias e soluções da categoria com pontos fortes diferentes e dedicados para criar uma estratégia abrangente de defesa em profundidade que torne extremamente desafiador para os cibercriminosos terem sucesso em seus ataques.

MITO 10

Todo centro de operações de segurança oferece o mesmo nível de suporte

Muitos fornecedores anunciam o suporte do SOC (Centro de operações de segurança). Mas ter um SOC que opera 24/7 não é o que mais importa. O importante é o nível de serviço e experiência que você poderá esperar receber quando seus ativos estiverem sob ataque. Algumas considerações relevantes ao avaliar os provedores de mitigação de DDoS devem incluir:

- Que tipo de suporte e análise você receberia antes, durante e depois de um ataque?
- Como é feita a alocação de pessoal do SOC para garantir a continuidade da defesa?
- Se você entrar em contato com o SOC, a pessoa para quem você ligou será o analista que de fato está realizando a mitigação ou apenas a pessoa do contato de encaminhamento?
- Seu provedor tem profissionais de segurança treinados em mitigação ou eles são simplesmente "policiais de trânsito" que direcionam o tráfego para equipamentos de mitigação prontos para uso?
- Eles oferecem um guia personalizado de runbook?

O SOC de seu provedor de segurança deve atuar como uma extensão de sua equipe de resposta a incidentes para agregar valor real.

Dica

Avalie a qualidade esperada do suporte que você receberia do SOC do provedor de serviços. Além de detecção e mitigação de ataques, determine se ele oferece integração e testes, solução de incidentes, análise após o evento (lições aprendidas) e suporte a projeto para ajudar a reduzir sua superfície de ataque.

MITO 11

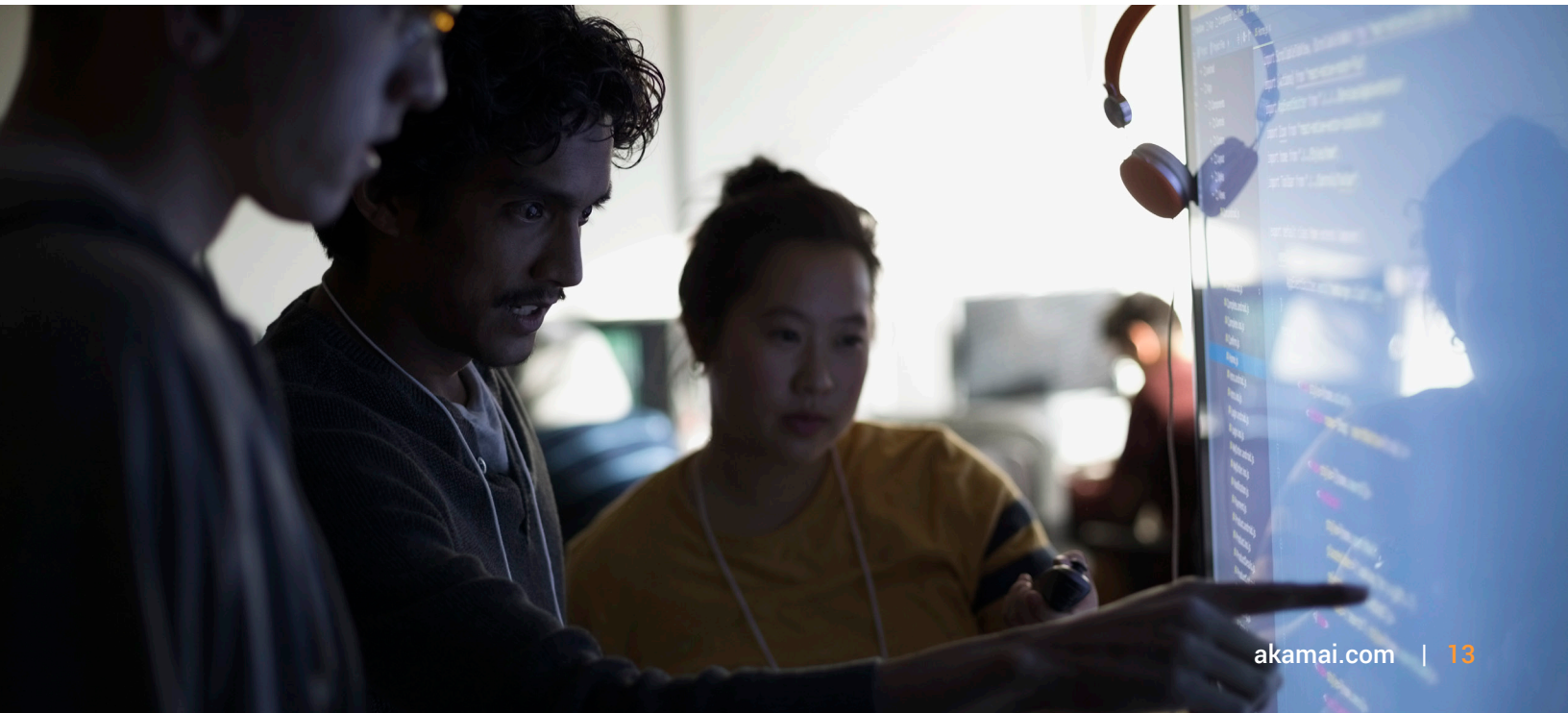
O DDoS é um produto antigo, portanto, a proteção mais barata será suficiente

A máxima "Nada vem de graça" é provavelmente mais relevante na proteção contra DDoS. Embora um preço mais baixo possa parecer atraente, muitas vezes há custos ocultos.

Alguns fornecedores oferecem um preço de etiqueta baixo, mas restringem o número ou o tamanho dos ataques que serão mitigados. Se você for alvo de muitos ataques ou de ataques muito grandes, eles pedirão que você faça upgrade para um nível de serviço mais alto (e mais caro) antes de interromper o ataque, tudo isso enquanto você está tentando colocar sua empresa online novamente. Os fornecedores maduros de segurança contra DDoS permitem que os clientes tenham a flexibilidade de escolher entre a proteção contra DDoS "sempre ativa" e "sob demanda" e alternar entre elas sem problemas, para manter os custos operacionais baixos e, ao mesmo tempo, oferecer a melhor proteção da categoria. Ao comparar fornecedores e preços, certifique-se de entender as vantagens e desvantagens e o impacto delas em sua postura de segurança contra DDoS.

Dica

Saiba o que está incluído no preço cotado antes de assinar o contrato.



A segurança contra DDoS é complexa e requer tempo e recursos significativos no cenário atual em rápida evolução. O que funcionou ontem pode não funcionar hoje ou amanhã. Manter-se em sintonia com seus usuários finais, clientes e funcionários é a base do sucesso da sua empresa. Aqui, não há espaço para erros, e você não precisa arcar com o alto custo de tentar fazer isso por conta própria. Como a plataforma de proteção contra DDoS mais abrangente, flexível e confiável, a Akamai pode ajudar.

Saiba mais sobre soluções de segurança contra DDoS da Akamai.

Sobre as soluções de segurança da Akamai

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. 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 10/24.