Akamai

WHITE PAPER

Proteja sua empresa contra ataques avançados

À medida que os ambientes de TI se tornaram complexos, os ataques cibernéticos evoluíram para aproveitar os novos pontos de falha. Aplicativos, APIs, microsserviços e componentes estão em constante expansão e mudando a forma como você faz negócios online. Infelizmente, eles também criam novas vulnerabilidades e superfícies de ameaças para que os invasores explorem. As soluções de cibersegurança devem lidar com as ameaças existentes no interior (protegendo seus próprios dados) e no exterior (bloqueando ransomware, DDoS, esgotamento de recursos e outros ataques).

Sabemos disso em primeira mão porque os pesquisadores da Akamai analisam, em média, 788 TB de dados diariamente, e inovamos continuamente nossos produtos com o conhecimento adquirido, protegendo você e seus usuários contra os invasores mais perigosos e campanhas avançadas, mesmo à medida que os ataques evoluem.

Quais são os ataques mais perigosos que sua empresa pode enfrentar e como você pode estar preparado para eles?

Os ransomwares estão em alta

A perda de acesso aos seus dados, e aos de seus clientes, é uma das maiores ameaças para sua empresa. Entre o primeiro trimestre de 2022 e o primeiro trimestre de 2023, o número de ataques de ransomware aumentou 143% em todo o mundo, com os invasores aproveitando as vulnerabilidades de dia zero e de dia um, de acordo com o relatório Ransomware on the Move da Akamai. Você pode diminuir a probabilidade e os impactos de ataques avançados por meio da segmentação.

Enquanto a segmentação é uma abordagem arquitetônica que divide uma rede em segmentos menores para melhorar o desempenho e a segurança, a microssegmentação é uma técnica de segurança que permite dividir logicamente uma rede em segmentos de segurança distintos até o nível de carga de trabalho individual. Os controles de segurança e a prestação de serviços podem então ser definidos para cada segmento exclusivo.

A Akamai Guardicore Segmentation, parte do Akamai Guardicore Platform for Zero Trust, atua para conter ataques em todos os seus sistemas críticos, impedindo que eles se espalhem por seus ativos, o que é conhecido como viagem leste-oeste, e, em seguida, acionando a resposta e a recuperação. O resultado é a proteção contra danos à reputação, perda de dados e perda de receita que vêm com uma violação bem-sucedida.

Como é uma solução sem agente para microssegmentação, a Akamai Guardicore Platform pode ser implantada de forma rápida e fácil, sem ter que fazer alterações físicas em sua rede ou se preocupar com onde seus servidores e dispositivos estão. Ela gera uma imagem interativa de todas as conexões em sua rede, ajudando você a superar um dos principais obstáculos à implantação, uma falta de visibilidade. Além disso, a Akamai criou maneiras ativas de lidar com possíveis gargalos de desempenho e requisitos de conformidade, além de aplicação de políticas que podem cobrir muitos tipos diferentes de infraestruturas. Isso significa ampla visibilidade e controle granular, entre diversos ambientes, tudo em uma única plataforma.

A Akamai tem visibilidade inigualável do tráfego online em toda a nossa rede global amplamente distribuída. A Akamai Guardicore Platform aproveita isso para fornecer visibilidade profunda de seu próprio ambiente, ativos, acesso e fluxos de rede. São informações em tempo real que darão a confiança de que a sua empresa não será prejudicada.

Aplicativos e APIs sob ameaça

Quantos aplicativos sua empresa está usando? É muito provável que use mais do que você sabe. A média das empresas usa mais de 1.000 aplicativos. A forte dependência das APIs para quase todas as transações online e a crescente adoção de arquiteturas baseadas em microsserviços também significam que os aplicativos estão se tornando mais complexos. Infelizmente, a pressão para crescer rapidamente por meio da inovação geralmente leva as empresas a liberar aplicativos antes de serem rigorosamente testados quanto a possíveis problemas de segurança, introduzindo mais risco em todo o ecossistema de aplicativos.

O recente relatório State of the Internet da Akamai descobriu que 29% dos ataques globais visavam interfaces de programação de aplicativos (APIs), que estão no centro da maioria das transformações digitais. Na região da Europa, Oriente Médio e África, o índice foi pouco mais de 47%. As APIs são um vetor de ataque comum para cibercriminosos que usam técnicas tradicionais e específicas de API. Bots, ataques distribuídos de negação de serviço (DDoS) e ataques de vários vetores devem ser considerados.

Defender seus aplicativos Web com o Akamai App & API Protector protegerá seu fluxo de trabalho, seus usuários e sua empresa contra atividades mal-intencionadas e fraudes. Ele fornece proteções de firewall configuráveis que podem absorver ataques direcionados à camada de aplicativo, incluindo aqueles iniciados por meio de APIs. Com visibilidade em tempo real do tráfego de bots, você pode investigar análises distorcidas da Web, evitar a sobrecarga de origem e personalizar permissões para permitir o acesso a bots de terceiros e parceiros sem obstrução.

Mas, voltando à pergunta original, e se você não souber quais são todos os seus aplicativos e APIs? A visibilidade é, mais uma vez, essencial: o Akamai API Security identificará todas as suas APIs, avaliará seus níveis de risco e responderá aos ataques. Isso impede que os invasores acessem seus dados, carreguem arquivos maliciosos em servidores ou sobrecarreguem servidores com picos de tráfego.

Você sabia?

Os ataques DDoS aumentaram 50% entre 2021 e 2023

Mais de 60% do total de ataques DDoS em 2023 tiveram um componente DNS

Defenda-se contra DDoS e esgotamento de recursos

Entre as maiores e mais conhecidas ameaças online está o ataque distribuído de negação de serviço. Desde que surgiu a Internet, houve ataques DDoS, e seus impactos aumentaram com tudo o que há online. Nos últimos anos, os ataques DDoS estão mais potentes, mais longos e mais sofisticados, com vários vetores e destinos de ataque. O número de ataques DDoS altamente volumétricos aumentou em 50% entre 2021 e 2023. E mais de 60% do total de ataques DDoS em 2023 tiveram um componente DNS (Sistema de Nomes de Domínio).

Até mesmo as maiores empresas podem ser detidas por esses botnets hostis, interrompendo o serviço para milhões de clientes e fazendo com que os negócios travem. Cibercriminosos altamente capacitados, atores de estados-nação e hacktivistas motivados geopoliticamente aproveitam botnets grandes e distribuídos não apenas para derrubar as maiores empresas, mas também instituições públicas críticas que vão de escolas e hospitais a aeroportos e provedores de serviços públicos. Ataques devastadores de DDoS e esgotamento de recursos são direcionados a todas as camadas, portas, protocolos e até mesmo ao DNS de empresas e instituições.

Proteger sua infraestrutura contra ataques DDoS requer inteligência contra ameaças em tempo real. Os dados que coletamos são usados para alimentar o Prolexic, nossa solução de proteção e mitigação de ataques DDoS. Capaz de proteger a infraestrutura digital que alimenta os aplicativos e experiências digitais de uma empresa, ele interrompe os ataques em todas as suas portas e protocolos – na nuvem, no local ou em ambos – antes que eles afetem sua empresa.

Nos últimos anos, houve um ressurgimento significativo em ataques de esgotamento de recursos destinados à infraestrutura de DNS de uma empresa. O DNS é o elemento fundamental da presença online de uma empresa. Se o sistema DNS ficar inativo, a presença online da organização desaparecerá. O Edge DNS e o Shield NS53 da Akamai derrubam o tráfego de esgotamento de recursos de DNS na edge e permitem que apenas consultas legítimas de DNS alcancem a origem de um cliente.

Há muito tempo, a proteção contra DDoS é uma grande aposta para empresas online, com o tamanho dos ataques dobrando a cada dois anos e um aumento concomitante na complexidade. Proteger todos os pontos potenciais de falha contra eles é necessário para evitar a perda de receita e a confiança dos clientes.

O que acontece quando há um ataque?

É seguro pensar que, se você tiver uma presença digital, ela será alvo de um ataque em algum momento. Um dos objetivos de uma estratégia de segurança é proteger você antes do ataque: tornar você um alvo menos visado, protegendo ativos críticos, fornecendo visibilidade em toda a sua rede para que você possa ver o que está acontecendo e detectando os ataques quando eles começarem.

Mas e se algo acontecer como um ataque de dia zero? É aí que entra a análise comportamental que é essencial para soluções como o Akamai App & API Protector.

A Akamai combina soluções altamente automatizadas e inteligência de máquina juntamente com inteligência humana de mais de 225 respondentes da linha de frente em nosso SOCC (Security Operations Command Center, centro de comando de operações de segurança) global para defender os dados dos clientes, a infraestrutura e as experiências digitais dos usuários finais.

A Akamai analisa mais de 13 trilhões de consultas ao Sistema de Nomes de Domínio (DNS) diariamente e defende mais de 12 bilhões de ataques de firewall de aplicativos da Web (WAF) a cada trimestre. Vemos e vivenciamos tudo isso por meio de nossos clientes e transformamos nossa análise de ataques em pontos fortes. A Akamai usa essa inteligência de ameaças para tornar nossas soluções mais ágeis e eficazes.

Mesmo que você ainda não esteja usando as soluções de segurança da Akamai, se estiver sob ataque, entre em contato conosco por meio de nossa linha direta de ciberameaças. Um especialista em segurança entrará em contato com você com as próximas etapas para mitigar os ataques.

Segurança em todos os lugares em que sua empresa se conecta com o mundo

Como a morte e os impostos, os ataques cibernéticos são uma das certezas deste mundo. Mas você pode proteger sua organização e seus clientes com soluções de segurança que usam inteligência de ameaças atualizada, fornecem alta visibilidade de seus aplicativos e redes e evoluem com o cenário de ameaças.

A Akamai protege a experiência, os sistemas e os dados de seus clientes, ajudando a incorporar a segurança em tudo o que você cria, em qualquer lugar em que o desenvolva e em qualquer lugar em que o entregue. Aproveitando a visibilidade de ameaças de nossa plataforma global, nosso amplo portfólio de soluções oferece confiabilidade líder do setor, para que você possa ficar à frente das ameaças e se adaptar rapidamente ao cenário de segurança em constante mudança.

Mais recursos

Conheça as cinco etapas necessárias para quebrar a cadeia de destruição do ransomware

Ofereça suporte à sua estratégia de nuvem híbrida e defenda-se dos ataques DDoS

Defenda os componentes básicos de sua empresa com uma forte segurança de API

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.