DELL Technologies

DDoS: Fortalecendo a segurança cibernética e a resiliência com a Dell Technologies

Ameaça crescente dos ataques DDoS

Os ataques de negação de serviço distribuída (DDoS) surgiram como uma das ameaças mais difundidas e disruptivas da era digital. Utilizando vastas redes de dispositivos comprometidos, os ataques DDoS inundam sistemas, servidores ou redes alvo com um volume avassalador de tráfego. Esse aumento implacável desacelera as operações ou as paralisa completamente, muitas vezes levando a empresa à beira da inoperância.

De startups a corporações multinacionais, nenhuma organização está imune ao crescente espectro dos ataques DDoS. À medida que as empresas dependem cada vez mais da infraestrutura digital, esses ataques têm consequências devastadoras, que vão desde perdas financeiras até danos à reputação. A Dell Technologies reconhece a criticidade desse desafio e oferece soluções dimensionáveis e inovadoras que ajudam as empresas a reforçar suas defesas e resistir à tempestade.

O que são os ataques DDoS?

Um ataque DDoS busca interromper o funcionamento normal de uma rede, serviço ou servidor, sobrecarregando-o com um grande volume de tráfego de várias fontes. Esses ataques são executados explorando botnets, que são redes de dispositivos infectados controlados remotamente por invasores.

Como funcionam os ataques DDoS

1. **Recrutamento de botnet:** Os criminosos cibernéticos infectam milhares ou milhões de dispositivos com malware, formando uma botnet que pode ser mobilizada para um ataque que torna sua empresa inoperante.
2. **Inundação de tráfego:** Os invasores direcionam as botnets para enviar um grande número de solicitações para o servidor de destino, fazendo com que o sistema fique lento, trave ou fique indisponível para usuários legítimos.
3. **Sobrecarga do sistema:** O sistema, sobrecarregado por tráfego ilegítimo, se torna incapaz de atender a solicitações legítimas, resultando em interrupções de serviço ou grandes atrasos.

Técnicas comuns

- **Ataques baseados em volume** aproveitam o grande volume de tráfego para esgotar a largura de banda de uma rede.
- **Ataques de protocolo** exploram vulnerabilidades em protocolos como TCP/IP para consumir recursos.
- **Ataques na camada de aplicação** visam aplicativos específicos, como um site ou banco de dados, para interromper a funcionalidade.

Esses ataques evoluem constantemente, o que os torna um grande desafio para empresas que tentam proteger suas operações.

O impacto nos negócios

Impacto financeiro

Um único ataque DDoS pode custar milhões de dólares em perdas de receita, tempo de inatividade e despesas de recuperação. Até mesmo minutos de indisponibilidade de serviço podem impactar significativamente empresas que dependem de transações em tempo real, como plataformas de comércio eletrônico e serviços financeiros.

Disrupção operacional

As interrupções causadas por um ataque DDoS reduzem a produtividade, atrasam processos críticos e dificultam o acesso a serviços essenciais. Para setores como saúde ou fabricação, o tempo de inatividade operacional pode resultar em consequências de longo alcance.

Danos à reputação

Quando consumidores ou clientes enfrentam interrupções de serviço, a confiança enfraquece. Os incidentes prolongados ou repetidos podem resultar em danos a longo prazo à reputação de uma organização, levando à perda de clientes e à redução da confiança do mercado.

Exemplo do mundo real

Um caso de grande repercussão ocorreu em 2020, quando uma grande instituição financeira foi vítima de um ataque DDoS prolongado que derrubou seus serviços bancários on-line por várias horas. As perdas diretas de receita, combinadas com uma reputação manchada, resultaram em danos superiores a **US$ 50 milhões.**

Estatísticas alarmantes

O Relatório de insights de DDoS do Zayo Group (fevereiro de 2024) indica que as organizações desprotegidas tiveram um prejuízo médio de **US$ 6.000** por minuto, levando a um custo médio por incidente de cerca de **US$ 408.000** em 2023. Além disso, a frequência desses ataques está aumentando, com mais de **10 milhões de ataques relatados anualmente**. Essas estatísticas destacam a necessidade urgente de mecanismos preventivos robustos.

20,5 milhões

Os ataques DDoS foram bloqueados no primeiro trimestre de 2025

Fonte: 2024: Relatório de ameaças DDoS da Cloudflare

Combatendo ataques DDoS com a Dell Technologies

A Dell Technologies oferece um conjunto avançado de soluções para ajudar as empresas a antecipar, detectar e se recuperar de incidentes de DDoS.

Endpoints fortalecidos com Dell Trusted Devices

Os endpoints são pontos de entrada cruciais para ameaças relacionadas a DDoS. Os Dell Trusted Devices oferecem recursos de segurança robustos integrados ao hardware, como o Secure BIOS e o SafeID, que protegem contra acesso não autorizado e mantêm a integridade do sistema.

Segurança do servidor

As soluções de servidor da Dell, equipadas com medidas de segurança incorporadas, como a tecnologia Dell Trusted Server, que inclui:

- **Raiz de confiança de hardware:** Esse recurso garante que os componentes de hardware do servidor sejam verificados no momento da inicialização, fornecendo assim uma camada básica de segurança contra adulteração ou modificações não autorizadas.
- **Recursos de segurança integrados:** Os servidores Dell vêm com unidades com criptografia automática e verificação de inicialização completa, que protegem contra acesso não autorizado e inspiram confiança na integridade dos dados.
- **Resiliência cibernética:** A abordagem inclui recursos para detectar anomalias, violações e operações não autorizadas, permitindo que as organizações se recuperem rapidamente de incidentes cibernéticos.
- **Proteção de dados abrangente:** As soluções de servidor confiável da Dell apresentam mecanismos de segurança integrados que protegem dados em repouso e em trânsito. Isso inclui técnicas avançadas de criptografia e opções para recuperação automatizadas para garantir a continuidade dos negócios.

Esses recursos garantem que os servidores possam suportar picos de tráfego, mantendo a estabilidade operacional. As soluções de armazenamento protegem a integridade e a disponibilidade de dados críticos durante um ataque, minimizando as interrupções.

Segurança do armazenamento

O Dell Storage ajuda a proteger contra ataques DDoS por meio de várias medidas de segurança integradas e tecnologias avançadas projetadas para minimizar vulnerabilidades, detectar ameaças logo no início e garantir recuperação rápida caso ocorra um ataque. Os principais métodos incluem:

- **Detecção proativa de ameaças:** As soluções de armazenamento da Dell empregam monitoramento inteligente e detecção de anomalias orientada por IA para identificar padrões de acesso incomuns que podem indicar um ataque DDoS. Essas ferramentas fornecem insights de segurança em tempo real e podem desencadear respostas automatizadas a ameaças para reduzir o impacto de um ataque
- **Arquitetura de raiz de confiança:** Integrada aos controladores de armazenamento, essa arquitetura garante a autenticidade do firmware e impede modificações não autorizadas, aumentando assim a segurança do hardware de armazenamento e reduzindo as chances de comprometimento durante um ataque DDoS
- **Autenticação baseada em vários fatores (MFA) e controles de acesso:** A implementação da MFA e do controle de acesso baseado em função (RBAC) ajuda a impedir o acesso não autorizado aos sistemas de armazenamento, protegendo ainda mais contra ameaças associadas a ataques DDoS
- **Microssegmentação e isolamento de rede:** Ao isolar os sistemas de armazenamento e restringir o acesso entre as cargas de trabalho, a Dell minimiza possíveis vetores de ataque e protege os sistemas de armazenamento contra movimentação lateral em caso de violação
- **Snapshots seguros e logs imutáveis:** As soluções de armazenamento da Dell fornecem snapshots seguros e logs imutáveis que garantem a integridade dos dados e ajudam as organizações a se recuperar rapidamente de ataques DDoS. Esses recursos facilitam a análise forense e a investigação de incidentes, permitindo que as equipes de TI detectem e analisem vetores de ataque
- **Cyber Recovery Vault:** Soluções como o Dell PowerMax e o PowerProtect Cyber Recovery Vault criam backups com air gap que são imutáveis e protegidos contra ransomware e outros ataques. Esses backups podem ser restaurados para garantir a continuidade dos negócios sem risco de reinfecção

Ao integrar esses recursos e tecnologias de segurança abrangentes, o Dell Storage e a resiliência cibernética ajudam efetivamente as organizações a se defenderem contra ataques DDoS e a manterem ambientes de TI resilientes e seguros.

Monitoramento proativo com a CrowdStrike

O monitoramento em tempo real e a lógica analítica avançada são essenciais para detectar padrões de tráfego anormais antes do encaminhamento. A CrowdStrike se integra ao ecossistema da Dell para usar lógica analítica comportamental e insights com inteligência artificial a fim de diferenciar atividades legítimas de tráfego de ataque, permitindo uma rápida remediação.

Dell PowerProtect para integridade dos dados

O Dell PowerProtect garante que dados críticos permaneçam seguros e acessíveis em meio a um ataque DDoS. Recursos imutáveis de backup e ambientes de recuperação isolados permitem que as empresas restaurem sistemas e minimizem o tempo de inatividade após um incidente.

Segurança de rede avançada e microssegmentação com o Dell PowerSwitch Networking e o SmartFabric OS

Fortalece as defesas contra ataques de dia zero, oferecendo segmentação de rede avançada, controles de acesso rigorosos e análise de tráfego em tempo real em toda a sua infraestrutura.

Implementação do mundo real

Recentemente, uma plataforma global de comércio eletrônico aproveitou as soluções PowerProtect da Dell, juntamente com recursos de detecção proativa, para se defender de um ataque DDoS sofisticado. Ao isolar sistemas críticos e implementar processos de recuperação de emergência, a empresa retomou as operações completas em tempo recorde, reduzindo perdas financeiras e preservando a confiança do cliente.

A abordagem de segurança multicamadas

O sucesso contra ataques DDoS vem de defesas adaptáveis e em camadas. A Dell defende as seguintes estratégias para complementar suas ofertas tecnológicas:

Principais etapas para aprimorar a defesa

- **Arquitetura Zero Trust** Implemente um modelo "nunca confie, sempre verifique" para examinar cada usuário e dispositivo
- **Criptografia avançada** Criptografe a comunicação em todas as camadas para proteger dados confidenciais transmitidos durante possíveis tentativas de ataque.
- **Treinamento de funcionários** Instrua funcionários sobre como identificar atividades suspeitas e seguir protocolos seguros para evitar violações inadvertidas.
- **Testes regulares do sistema** Realize avaliações de rotina, incluindo testes de penetração e testes de carga, para avaliar a preparação do sistema para altos volumes de tráfego.

Essas ações, combinadas com as soluções da Dell Technologies, criam um mecanismo de defesa robusto contra ameaças sofisticadas.

Parcerias que fortalecem a segurança cibernética

Para ampliar seus recursos, a Dell Technologies colabora com líderes do setor, como **Microsoft**, **CrowdStrike** e **Secureworks**, por exemplo. Essas parcerias fornecem camadas adicionais de proteção, incorporando a melhor inteligência de ameaças e metodologias avançadas de detecção à estrutura abrangente da Dell.

Aproveitando o Dell Professional Services

Além da tecnologia, os serviços profissionais da Dell oferecem orientação especializada para empresas que enfrentam desafios de DDoS. Da resposta a incidentes a consultas personalizadas sobre arquitetura de segurança, a equipe da Dell garante que as organizações possam se recuperar rapidamente e reforçar futuras defesas.

Crie um futuro resiliente

A Dell Technologies é mais do que um provedor de tecnologia; é um parceiro comprometido em proteger sua empresa contra a crescente ameaça de ataques DDoS. Ao combinar tecnologia de ponta, parcerias profundas e insights práticos, a Dell ajuda as empresas a proteger as operações, manter a confiança do cliente e buscar ativamente o crescimento.

Dê o primeiro passo em direção à resiliência hoje. Entre em contato com a Dell Technologies para fortalecer sua empresa contra ameaças DDoS e proteger seu futuro.

A Dell Technologies capacita empresas a superar os desafios da segurança cibernética contra DDoS, provando que uma base segura é a chave para o sucesso em um mundo interconectado.

Saiba como enfrentar alguns dos principais desafios de segurança cibernética atuais em **Dell.com/SecuritySolutions**

Saiba mais sobre Soluções da Dell

Entre em contato com um especialista da Dell Technologies

Veja mais recursos

Participe da conversa com #HashTag

DELL Technologies