Mito da cibersegurança

Introdução

Embora a internet tenha apresentado avanços fenomenais nas últimas décadas, continua frágil e vulnerável a ataques de todas as dimensões até aos dias de hoje. Os utilizadores ficam confusos com o seu funcionamento complexo e muitas vezes não conseguem distinguir entre um ataque de um atacante e uma falha no software de proteção.

Um desses acontecimentos recentes ocorreu a 18 de novembro de 2025, quando a Cloudflare sofreu uma interrupção global que afetou brevemente uma grande parte da internet. Este não foi um incidente isolado. O anterior tinha acontecido apenas oito meses antes, e houve outros antes disso. Da mesma forma, a Amazon Web Services (AWS) tem sofrido interrupções frequentes. Este tipo de interrupção da internet tornou-se quase rotineiro, e a fiabilidade destes serviços, concebidos para proteger contra intrusões cibernéticas, tem sido questionada.

O problema

A vulnerabilidade da internet é um problema há décadas. No ano passado, a Comissão Federal de Comunicações (FCC) emitiu um Aviso de Proposta de Regulamentação (NPRM) que identificava o Protocolo de Gateway de Fronteira (BGP) como o alvo para a mitigação do risco. O Conselho de Arquitetura da Internet (IAB), em representação da comunidade da internet, respondeu com um comentário expressando preocupações. Apesar disso, a Casa Branca publicou um roteiro que se focava na integridade do BGP como meio para melhorar a segurança do encaminhamento da internet.

Neste sentido, é importante ter em conta que o BGP é necessário para transportar pacotes entre Sistemas Autónomos (ASes) que são selecionados pelo Servidor de Nomes de Domínio (DNS), com base em endereços IPv4 atribuídos aos subscritores pelo Protocolo de Configuração Dinâmica de Hosts (DHCP), que foi criado para lidar com a escassez de endereços IPv4. Esta pilha de protocolos resultou numa arquitetura de sistema complexa e vulnerável a ataques por diversos ângulos, cada um dos quais requer uma correção específica.

A solução

Um sistema com falhas convida a uma série interminável de correções e remendos. Uma internet muito mais robusta pode resultar de uma arquitetura simplificada e otimizada que elimine a causa raiz da escassez de endereços IPv4, eliminando assim a necessidade de qualquer um dos quatro protocolos anteriormente mencionados. Este é o resultado de um sistema determinístico denominado EzIP.

(Por favor visite https://avinta.com/gallery/CyberSecurityMyth-PT.pdf para o texto integral.)