Mito de la ciberseguridad

Introducción

Aunque internet ha experimentado avances extraordinarios en las últimas décadas, sigue siendo frágil y vulnerable a ataques de todo tipo. Los usuarios desconocen su complejo funcionamiento y a menudo no pueden distinguir entre un ataque informático perpetrado por un intruso y un fallo en el software de seguridad.

Uno de estos incidentes recientes ocurrió el 18 de noviembre de 2025, cuando Cloudflare sufrió una interrupción global que afectó brevemente a una gran parte de internet. Este no fue un incidente aislado. El anterior había ocurrido solo ocho meses antes, y hubo otros más con anterioridad. De forma similar, Amazon Web Services (AWS) ha sufrido interrupciones frecuentes. Este tipo de interrupciones de internet se ha vuelto casi habitual, y la fiabilidad de estos servicios, diseñados para proteger contra intrusiones cibernéticas, ha sido puesta en entredicho.

El problema

La vulnerabilidad de internet ha sido un problema durante décadas. El año pasado, la Comisión Federal de Comunicaciones (FCC) emitió un Aviso de Propuesta de Reglamentación (NPRM) que identificaba el Protocolo de Puerta de Enlace de Frontera (BGP) como el objetivo para mitigar el riesgo. La Junta de Arquitectura de Internet (IAB), en representación de la comunidad de internet, respondió con un comentario expresando sus preocupaciones. No obstante, la Casa Blanca publicó una hoja de ruta que se centraba en la integridad del BGP como medio para mejorar la seguridad del enrutamiento en internet.

En este sentido, es importante tener en cuenta que el protocolo BGP es necesario para transportar paquetes entre sistemas autónomos (AS) seleccionados por el servidor de nombres de dominio (DNS), basándose en las direcciones IPv4 asignadas a los suscriptores por el Protocolo de Configuración Dinámica de Host (DHCP), que fue creado para solucionar la escasez de direcciones IPv4. Esta pila de protocolos ha dado lugar a una arquitectura de sistema compleja y vulnerable a ataques desde múltiples frentes, cada uno de los cuales requiere una solución específica.

La solución

Un sistema defectuoso da lugar a una serie interminable de soluciones provisionales y parches. Una Internet mucho más robusta puede lograrse mediante una arquitectura simplificada y optimizada que elimine la causa fundamental de la escasez de direcciones IPv4, lo que anularía la necesidad de cualquiera de los cuatro protocolos mencionados anteriormente. Este es el resultado de un sistema determinista denominado EzIP.

(Por favor, visite https://avinta.com/gallery/CyberSecurityMyth-ES.pdf para ver el texto completo.)