Mythe de la cybersécurité

Introduction

Bien qu'Internet ait connu des avancées phénoménales au cours des dernières décennies, il reste fragile et vulnérable aux attaques, qu'elles soient de grande ou de petite ampleur. Les utilisateurs sont déconcertés par son fonctionnement complexe et sont souvent incapables de distinguer une intrusion malveillante d'une simple défaillance du logiciel de protection.

Un incident de ce type s'est produit récemment, le 18 novembre 2025, lorsque Cloudflare a subi une panne mondiale qui a brièvement paralysé une grande partie d'Internet. Il ne s'agissait pas d'un incident isolé. Le précédent avait eu lieu seulement huit mois auparavant, et d'autres l'avaient précédé. De même, Amazon Web Services (AWS) a connu de fréquentes interruptions. Ce type de panne Internet est devenu presque monnaie courante, et la fiabilité de ces services, censés protéger contre les intrusions informatiques, est désormais remise en question.

Le problème

La vulnérabilité d'Internet est un problème qui persiste depuis des décennies. L'année dernière, la Commission fédérale des communications (FCC) a publié un avis de proposition de réglementation identifiant le protocole BGP (Border Gateway Protocol) comme cible prioritaire pour atténuer ce risque. L'Internet Architecture Board (IAB), représentant la communauté Internet, a réagi en formulant des observations exprimant ses préoccupations. Malgré cela, la Maison Blanche a publié une feuille de route axée sur l'intégrité du protocole BGP comme moyen de renforcer la sécurité du routage Internet.

À cet égard, il est important de garder à l'esprit que le protocole BGP est nécessaire pour acheminer les paquets entre les systèmes autonomes (AS) sélectionnés par le serveur de noms de domaine (DNS), en fonction des adresses IPv4 attribuées aux abonnés par le protocole DHCP (Dynamic Host Configuration Protocol), conçu pour pallier la pénurie d'adresses IPv4. Cette pile de protocoles a engendré une architecture système complexe, vulnérable aux attaques sous de nombreux angles, chacune nécessitant l'application d'un correctif spécifique.

La solution

Un système défectueux engendre une série interminable de correctifs et de solutions de contournement. Un Internet beaucoup plus robuste peut être obtenu grâce à une architecture simplifiée et rationalisée qui élimine la cause profonde de la pénurie d'adresses IPv4, rendant ainsi inutiles les quatre protocoles mentionnés précédemment. Tel est le résultat d'un système déterministe baptisé EzIP.

(Veuillez visiter https://avinta.com/gallery/CyberSecurityMyth-FR.pdf pour le texte intégral.)