網路安全神話

介紹

儘管互聯網在過去幾十年中取得了驚人的發展，但至今仍然脆弱不堪，容易受到各種規模的攻擊。使用者對網路複雜的運作機制感到困惑，往往無法區分是駭客入侵還是防護軟體本身出現了故障。

最近發生的類似事件是在 2025 年 11 月 18 日，當時 Cloudflare 遭遇了全球性故障，導致網路大面積癱瘓了一段時間。這並非個案。上一次故障發生在僅僅八個月前，在此之前也發生過多次類似事件。同樣，亞馬遜網路服務 (AWS) 也頻繁出現故障。這種網路中斷幾乎已成為常態，人們開始質疑這些旨在抵禦網路入侵的服務是否可靠。

問題

網路的脆弱性問題已經存在了幾十年。去年，美國聯邦通訊委員會（FCC）發布了一份擬議規則制定通知（NPRM），其中指出邊界網關協定（BGP）是降低風險的關鍵目標。代表互聯網社區的互聯網架構委員會（IAB）對此發表評論，表達了擔憂。儘管如此，白宮還是發布了一份路線圖，重點在於 BGP 的完整性，以增強網路路由的安全性。

在這方面，重要的是要記住，BGP 協定負責在自治系統（AS）之間傳輸資料包，這些自治系統由網域名稱伺服器（DNS）根據動態主機配置協定（DHCP）分配給使用者的 IPv4 位址進行選擇。而 DHCP 協定最初是為了解決 IPv4 位址短缺問題而創建的。這種協定棧導致了複雜的系統架構，容易受到來自多個方面的攻擊，每一種攻擊都需要相應的修補程式來應對。

解決方案

一個有缺陷的系統會導致一系列永無止境的修補和改進。而一個簡化且精簡的架構可以建構一個更健壯的互聯網，徹底消除 IPv4 位址短缺的根本原因，因此無需使用上述四種協定。這正是名為 EzIP 的確定性系統所帶來的成果。

(請訪問 https://avinta.com/gallery/CyberSecurityMyth-RoC.pdf 查看全文)