网络安全神话

介绍

尽管互联网在过去几十年取得了惊人的发展，但至今仍然脆弱不堪，容易受到各种规模的攻击。用户对互联网复杂的运作机制感到困惑，往往无法区分是黑客入侵还是防护软件本身出现了故障。

最近发生的一起类似事件是在 2025 年 11 月 18 日。当时 Cloudflare 遭遇了全球性故障，导致互联网大面积瘫痪了一段时间。这并非孤立事件。上一次故障发生在仅仅八个月前，而在此之前也发生过多次类似事件。同样，亚马逊网络服务 (AWS) 也频繁出现故障。这种互联网中断几乎已成为常态，人们开始质疑这些旨在抵御网络入侵的服务是否可靠。

问题

互联网的脆弱性问题已经存在了几十年。去年，美国联邦通信委员会（FCC）发布了一份拟议规则制定通知（NPRM），其中指出边界网关协议（BGP）是降低风险的关键目标。代表互联网社区的互联网架构委员会（IAB）对此发表评论，表达了担忧。尽管如此，白宫还是发布了一份路线图，重点关注 BGP 的完整性，以此增强互联网路由的安全性。

在这方面，重要的是要记住，BGP 协议负责在自治系统（AS）之间传输数据包，这些自治系统由域名服务器（DNS）根据动态主机配置协议（DHCP）分配给用户的 IPv4 地址进行选择。而 DHCP 协议最初是为了解决 IPv4 地址短缺问题而创建的。这种协议栈导致了复杂的系统架构，容易受到来自多个方面的攻击，每一种攻击都需要相应的补丁来应对。

解决方案

一个存在缺陷的系统会导致一系列永无止境的修补和改进。而一个简化且精简的架构可以构建一个更加健壮的互联网，彻底消除 IPv4 地址短缺的根本原因，从而无需使用上述四种协议。这正是名为 EzIP 的确定性系统所带的成果。

(请访问 https://avinta.com/gallery/CyberSecurityMyth-CN.pdf 查看全文.)