Mythos Cybersicherheit

Einführung

Obwohl das Internet in den letzten Jahrzehnten phänomenale Fortschritte gemacht hat, bleibt es bis heute anfällig und verwundbar für große und kleine Angriffe. Die Nutzer sind von seinen komplexen Funktionsweisen verwirrt und können oft nicht zwischen einem Hackerangriff und einer Fehlfunktion der Schutzsoftware unterscheiden.

Ein solches Ereignis ereignete sich am 18. November 2025, als Cloudflare von einem globalen Ausfall betroffen war, der kurzzeitig einen großen Teil des Internets lahmlegte[1]. Dies war kein Einzelfall. Der vorherige Vorfall ereignete sich nur acht Monate zuvor, und es gab bereits weitere davor. Auch Amazon Web Services (AWS) war häufig von Störungen betroffen[2]. Diese Art von Internetausfällen ist fast schon alltäglich geworden, und die Zuverlässigkeit dieser Dienste, die eigentlich vor Cyberangriffen schützen sollen, wird zunehmend infrage gestellt.

Das Problem

Die Anfälligkeit des Internets ist seit Jahrzehnten ein Problem. Im vergangenen Jahr veröffentlichte die Federal Communications Commission (FCC) eine Bekanntmachung über geplante Regelungen (Notice of Proposed Rulemaking, NPRM)[3], in der das Border Gateway Protocol (BGP)[4] als Ansatzpunkt zur Risikominderung identifiziert wurde. Das Internet Architecture Board (IAB), das die Internet-Community vertritt, reagierte mit einer Stellungnahme, in der Bedenken geäußert wurden[5]. Dennoch veröffentlichte das Weiße Haus eine Roadmap[6], die sich auf die Integrität des BGP als Mittel zur Verbesserung der Internetsicherheit konzentrierte.

In diesem Zusammenhang ist es wichtig zu beachten, dass das BGP-Protokoll für den Transport von Paketen zwischen autonomen Systemen (AS)[7] zuständig ist, die vom Domain Name Server (DNS)[8] ausgewählt werden, basierend auf den IPv4-Adressen, die den Teilnehmern vom Dynamic Host Configuration Protocol (DHCP)[9] zugewiesen werden. Dieses Protokoll wurde entwickelt, um dem Mangel an IPv4-Adressen entgegenzuwirken. Dieser Protokollstapel hat zu einer komplexen Systemarchitektur geführt, die von vielen Seiten angreifbar ist und für jede Schwachstelle eine separate Sicherheitslücke erfordert.

Die Lösung

Ein fehlerhaftes System führt zu einer endlosen Reihe von Hacks und Notlösungen. Ein deutlich robusteres Internet kann durch eine vereinfachte und optimierte Architektur entstehen, die die Ursache des IPv4-Adressmangels beseitigt und somit die Notwendigkeit der oben genannten vier Protokolle überflüssig macht. Dies ist das Ergebnis eines deterministischen Systems namens EzIP[10].

(Bitte besuchen Sie uns https://avinta.com/gallery/CyberSecurityMyth-DE.pdf für den vollständigen Text.)