Zusammenfassung

Der Mythos der Cybersicherheit:

Warum schrittweise Korrekturen nicht ausreichen – und wie EzIP einen einfacheren und sichereren Weg bietet

Das Internet ist die Grundlage der modernen Gesellschaft, bleibt aber anfällig. Jüngste globale Ausfälle bei Cloudflare (November 2025) und häufige Störungen bei Amazon Web Services verdeutlichen die anhaltende Fragilität, selbst bei führenden Anbietern, die eigentlich für erhöhte Sicherheit und Zuverlässigkeit sorgen sollen. Initiativen der US-Regierung (FCC NPRM, 2024) und die Roadmap des Weißen Hauses zur Verbesserung der Internetsicherheit (2024) zielen auf das Border Gateway Protocol (BGP) ab, um dessen Überwachung und Validierung zu stärken. Diese Schritte sind zwar hilfreich, bekämpfen aber nur die Symptome eines tieferliegenden Problems: den ursprünglichen Mangel an IPv4-Adressen. Um mit den begrenzten Adressen umzugehen:

• Die dynamische IP-Adressvergabe (DHCP) machte IP-Adressen temporär.
• DNS verfolgte die Änderungen.
• Netzwerke wurden in Tausende von Domänen (Autonome Systeme) fragmentiert, die über BGP miteinander verbunden wurden.
• Content Delivery Networks (CDNs) zentralisierten den Datenverkehr, um die Komplexität zu bewältigen.

Dieser Ansatz führt zu Verwirrung, einzelnen Schwachstellen und Vorteilen für Angreifer: Gefälschte Adressen lassen sich leicht verwenden und schwer zurückverfolgen, während legitime Nutzer eindeutige Spuren hinterlassen. Zentralisierte CDNs werden zu Hauptzielen, und Patches fügen weitere Ebenen hinzu, ohne die eigentliche Ursache zu beheben. EzIP (Easy IPv4) löst dieses Problem, indem es den lange reservierten IPv4-Block 240/4 reaktiviert, um Millionen von Standorten eindeutige, statische öffentliche Adressen bereitzustellen – ausreichend, um ganze Regionen ohne dynamische Neuzuweisung oder starke Abhängigkeit von problematischen Protokollen zu versorgen. Hauptvorteile:

• Höhere inhärente Sicherheit – Statische Adressen machen Spoofing erkennbar, verbessern die Nachverfolgbarkeit und reduzieren die Angriffsfläche.
• Höhere Zuverlässigkeit – Die geringere Komplexität senkt das Ausfallrisiko; die präzise Geolokalisierung erleichtert Management und Reaktion.
• Minimale Beeinträchtigung – Das System wird über das bestehende Internet gelegt, schrittweise über verbesserte regionale Router implementiert und erfordert keine massenhaften Geräte-Upgrades.
• Umfassendere Vorteile – Reduziert Zentralisierungsrisiken, verbessert die Internetarchitektur und unterstützt eine bessere Zuordnung von Straftaten durch die Strafverfolgungsbehörden.

EzIP ergänzt IPv6 und bestehende Tools, indem es die grundlegende Ressourcenknappheit angeht, die das Internet anfällig gemacht hat. Es steht im Einklang mit den Zielen einer widerstandsfähigeren und gerechteren digitalen Infrastruktur. Für eine vollständige Analyse besuchen Sie bitte:

https://avinta.com/gallery/CyberSecurityMyth-DE.pdf

Hergestellt von: Abraham Y. Chen / Avinta Communications, Inc.
Kontakt: AYChen@Avinta.com / +1(650)248-1829
Januar 2026