Das Internet neu gestalten

1. Hintergrund: Trotz der schnellen Einführung und des breiten Einsatzes des Internets, um de facto zur weltweiten Kommunikationsinfrastruktur zu werden, gab es immer eine nagende Besorgnis über seine Anfälligkeit für Sicherheitsverletzungen. Das heißt, warum braucht das Internet im Vergleich zum herkömmlichen PSTN, das den Anrufer lokalisieren kann, noch bevor ein Anruf entgegengenommen wird, so viel Zeit, Tage, Monate oder sogar noch länger, um nur damit zu beginnen, über den Täter eines großen Cyberangriffs zu spekulieren?

Die Ursache dieses Problems liegt in der Tatsache begründet, dass das ursprüngliche IPv4-basierte Internetdesign keinen ausreichend großen Adresspool hatte, um alle verwendeten IoTs explizit und eindeutig zu identifizieren. Verschiedene Übergangsregelungen wurden entwickelt, um dieses Handicap dynamisch zu bewältigen. Leider boten sie den Tätern auch die perfekte Tarnung, während die normalen Benutzer im Freien saßen. Obwohl die neue Version, IPv6, mehr als genug Adressen hat, um alle IoTs zu identifizieren, blieb die Verwendung der vorläufigen Schemata irgendwie bestehen. Darüber hinaus ist IPv6 komplizierter und teurer als IPv4, was es weniger glücklichen Regionen schwer macht, IPv6 einzuführen. Ein vollständiger Ersatz für ein kontinuierlich genutztes großes System wie das Internet kommt nicht in Frage. Um diese Pattsituation zu umgehen, ist ein System, das mit den derzeitigen Praktiken koexistieren und sie gleichzeitig zu einem langfristigen System ausbauen kann, der einzig realistische Weg.

2. Lösung: Glücklicherweise wurde entdeckt, dass ein erheblicher Teil (ein Sechzehntel, um genau zu sein) des IPv4-Adresspools, genannt 240/4-Netzblock, seit den frühen Tagen für die „zukünftige Verwendung“ „RESERVIERT“ wurde. Folglich ist keines der aktuellen Internetgeräte in der Lage, es zu verwenden. Dies bietet eine einzigartige Gelegenheit für eine neue Klasse von Routern, um bis zu 256 Millionen IoTs von jeder vorhandenen IPv4-Adresse zu identifizieren. Bei richtiger Verwaltung stellt ein vollständig durchgängig adressierbares weltweites Kommunikationssystem nicht nur alle gewünschten Dienste einheitlich für jeden Teilnehmer bereit, sondern mildert auch die Grundursache der Cyber-Sicherheitslücke, und das alles im Rahmen der bestehenden IPv4-Technologie.

3. Phasenweise Bereitstellung: Um sich in den aktuellen Internet-Server-Client-Betriebsmodus einzufügen, kann der obige Ansatz sofort mit einem degenerierten Format bereitgestellt werden, wobei der 240/4-Netzblock so verwendet wird, als wäre er der vierte private Netzwerkadresspool, in Ergänzung zu 192.168/16, 172.16/12 und 10/8. Diese Einführungsphase erfordert nur die Aktivierung des 240/4-Netzblocks, ohne irgendetwas anderes an bestehenden IPv4-Designs zu ändern.

4. Umsetzung: Dieser Ansatz erfordert kaum Engineering-Aufwand. Die Bereitstellungskosten sind die gleichen wie bei vergleichbaren aktuellen IPv4-Geräten. Und die Betriebskosten werden aufgrund der optimierten Praktiken gesenkt, die Störungen wie Cyberangriffe abmildern:

A. Produktentwicklung (ProDev): Deaktivieren Sie einfach die vorhandenen Softwarecodes, die die Verwendung des 240/4-Netzblocks deaktiviert haben.

B. Investitionsausgaben (CapEx): Die gleichen wie bei aktuellen IPv4-Geräten für die gleiche Servicekapazität, bei Verwendung der gleichen Hardware.

C. Betriebskosten (OpEx): Senken durch optimierte Praktiken, die nicht auf dynamischen Schemata beruhen.

D. Cybersicherheit: Verbessert durch deterministische Verwaltung der IoT-Identifikation (Adresse).

5. Vorgeschlagene Maßnahmen:

A. Mit den inhärenten Merkmalen, Internetdienste von einem privaten Netzwerk ohne Entwicklungsaufwand zu starten, kann dieses vorgeschlagene System von jeder interessierten Partei (Regierungsbehörden, Unternehmen, Unternehmer usw.) von einer verfügbaren gültigen IPv4-Adresse aus unter Verwendung vorhandener IPv4-Geräte bereitgestellt werden.

B. Da dieser Ansatz generischer Natur ist, wird empfohlen, ihn von der ITU-D auf seine Eignung für den universellen Einsatz zur Neugestaltung des Internets überprüfen zu lassen.

Verweise:

I. Status der Cyber-Sicherheitslücke

https://blog.apnic.net/2021/02/03/the-internet-of-trash/

II. Eine leicht nachvollziehbare Machbarkeitsdemonstration dieses Vorschlags.

https://www.avinta.com/phoenix-1/home/RegionalAreaNetworkArchitecture.pdf

III. Kommentar zu einem IAB-Blog: Vorschlag dieses Schemas, um die Teilnahme von Endbenutzern an Protokoll-/Produktentwicklungen zu erleichtern.

https://blog.apnic.net/2020/08/31/rfc-8890-the-internet-is-for-end-users/

IV. IETF-Entwurf: Technische Details dieses Vorschlags

https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-ipv4-address-space

V. Geistiges Eigentum: US-Patent Nr.: 11,159,425

Terminologie, Abkürzung & Akronym:

. CG-NAT: Netzadressübersetzung in Carrier-Qualität

. DHCP: Dynamisches Host-Konfigurationsprotokoll

. DNS: Domain-Name-System

. IAB: Internet Architecture Board

. IETF: Internet-Engineering-Taskforce

. IoTs: Internet der Dinge

. IPv4: Internetprotokoll Version 4

. IPv6: Internetprotokoll Version 6

. ITU-D: Internationale Fernmeldeunion – Entwicklungssektor

. PSTN: Öffentliches Telefonnetz

. 240/4 Netblock: IPv4-Adresspool von 240.0.0.0 bis 255.255.255.255, was ungefähr 256 Millionen (256 Millionen) oder einer Viertelmilliarde (0,25 Milliarden) Adressen entspricht

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml