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].

Technologische und architektonische Entwicklungen

Als das Internet entstand, wurden den fünf regionalen Internet-Registrierungsstellen (RIRs) klar definierte, große IPv4-Adressblöcke zugewiesen. Beispielsweise waren die Hilbert-Kurven[11], die die damaligen Zuweisungen von AFRINIC (Afrika), APNIC (Asien-Pazifik), ARIN (Nordamerika), LACNIC (Lateinamerika und Karibik) und RIPE (Europa, Naher Osten und Zentralasien) darstellten, leicht erkennbar[12].

Obwohl jede RIR (Regional Internet Registry) die ihr zugewiesenen Adressen an Internetzugangsanbieter (IAPs) innerhalb ihrer eigenen Region vergab, waren die IAPs selbst nicht verpflichtet, dieselbe Beschränkung einzuhalten. Dies öffnete Tür und Tor für die Fragmentierung von IP-Adressen und ermöglichte es, dass der physische Standort eines Abonnenten nicht mehr geografisch mit der Region übereinstimmte, in der die zugewiesene IP-Adresse ursprünglich vergeben wurde.

Da der IPv4-Adresspool allmählich erschöpft war, sicherte DHCP den Betrieb der Internetzugangspunkte (IAP), indem es verfügbare öffentliche IPv4-Adressen dynamisch wiederverwendete. Anschließend wurde DNS eingeführt, um die Belastung der Nutzer in dieser sich ständig verändernden Umgebung zu verringern. Da dieses Protokollpaar die damaligen dringenden Bedürfnisse zu erfüllen schien, entwickelte es sich zum Standardbaustein des Internets. (Siehe Fußnote für die Auswirkungen dieser ungewöhnlichen Kombination.)

Nachdem erste Institutionen zugestimmt hatten, überschüssige IPv4-Adressblöcke zur öffentlichen Versteigerung freizugeben, um den Druck durch die Verknappung des IPv4-Adresspools zu verringern, war es nicht mehr praktikabel, von einer IPv4-Adresse aussagekräftige Informationen zum physischen Standort zu erwarten, geschweige denn die Möglichkeit, einen Teilnehmer geografisch zu lokalisieren. Ein separater Zweig der Branche entstand, um diesen Bedarf zu decken. Die Auflösung und Genauigkeit der Berichte waren jedoch oft bestenfalls fragwürdig.[13]

Im Laufe der Zeit entwickelten die Internetdienstanbieter (IAPs), die über einen oder mehrere IPv4-Adressblöcke verfügten, ihre jeweiligen IP-Paketübermittlungsverfahren. Adressblöcke mit derselben Transportrichtlinie wurden zu einem autonomen System (AS) zusammengefasst. Da der Umfang jedes AS variiert und oft begrenzt ist, wurde das BGP-Protokoll für die Weiterleitung von IP-Paketen über die AS-Grenzen hinweg eingesetzt. Mit der wachsenden Anzahl von AS stieg auch die Komplexität des BGP-Protokolls, das für die Übertragung von Paketen über größere Entfernungen – oft sogar nur innerhalb des lokalen Netzes – verantwortlich ist, ganz zu schweigen von Paketen mit globalen Zieladressen, die mehrere AS-Grenzen überschreiten müssen.

Obwohl jedes dieser Protokolle von Natur aus dezentralisiert ist, erfordern ihre Abläufe eine erhebliche Koordination, die auf zentralisierten Maßnahmen beruht. Dies führt zur Dominanz einiger weniger ressourcenstarker Unternehmen, wie beispielsweise Betreiber von Content Delivery Networks (CDN)[14], zu denen Cloudflare, AWS usw. gehören. Diese bilden die Kerninfrastruktur für den Datentransport im Internet.

Widersprüche

Es gibt mehr als nur eine Handvoll Internetpraktiken, die dessen Prinzipien und Funktionsweise verwirrend erscheinen lassen:

Das Internet fördert die Chancengleichheit. Doch die Vatikanstadt erhält 21,4 IPv4-Adressen pro Einwohner, während über ein Dutzend anderer Entitäten gar keine erhalten und andere Nationen alle möglichen Werte dazwischen aufweisen.[15] (Anmerkung: Die Zuteilung von 58,4 Adressen an die Seychellen ist eine Besonderheit, da Unternehmen die lokalen politischen Gegebenheiten für globale Geschäftsmöglichkeiten nutzen.)

Das Internet versprach eine durchgängige Konnektivität. Das derzeit vorherrschende Betriebsmodell, das Content Delivery Network (CDN), behindert dieses Ziel jedoch, selbst innerhalb einer lokalen Gemeinschaft.

Das Internet kritisierte einst das Monopol der Telekommunikationsunternehmen und die staatliche Regulierung des öffentlichen Telefonnetzes (PSTN). Doch heute wird das Internet von multinationalen Konzernen beherrscht, die in ihren jeweiligen Geschäftsbereichen praktisch Monopole bilden und dabei Verantwortung ignorieren und Vorschriften umgehen. Steht diese Art der Zentralisierung nicht im Widerspruch zur ursprünglichen Vision eines dezentralen Internets?

Darüber hinaus wird das Potenzial von rund 200 globalen Jurisdiktionen, die das Internet fragmentieren und so ein geopolitisches „Splinternet“[16] entstehen lassen könnten, von der Internet-Community kritisiert. Gleichzeitig haben die autonomen Systeme (AS) das Internet bereits in ein Zwiebelnetz mit mindestens 77.000 Schichten[7] verwandelt. Da die meisten autonomen Systeme nur bestimmte Teile der Welt bedienen, gleicht jede Schicht dieser Zwiebelstruktur eher einem unvollständigen Fischernetz mit Löchern!

Die verblüffendste Tatsache ist, dass das Internet sein grenzenloses Prinzip vehement verteidigt, während sich sein primärer Routing-Mechanismus zu BGP entwickelt hat, wobei das „B“ für die Grenzen um jedes autonome System (AS) steht!

Aufgrund der komplexen Dynamik und der verteilten Natur dieser Protokolle ist das Internet insgesamt anfällig für eine Vielzahl bösartiger Sicherheitsverletzungen, von alltäglicher Belästigung bis hin zu Ransomware-Angriffen.

An dieser Stelle sei erwähnt, dass IPv6, ohne seinen eigenen riesigen Adressraum auszunutzen, die durch vorübergehende Bedürfnisse entstandenen Praktiken von IPv4 übernommen hat. Die Bedeutung von IPv6 scheint nun allmählich zu schwinden[17], und vom geplanten Abschalttermin für IPv4 ist keine Rede mehr. Da IPv6 keine nennenswerten Vorteile gegenüber IPv4 bietet, wird in den meisten aktuellen Internet-Diskussionen nicht mehr zwischen den beiden Protokollen unterschieden.

Referenzen

1. Cloudflare Ausfallhistorie (2019-2025)
   https://controld.com/blothe/biggest-cloudflare-outages/

2. Eine Geschichte der AWS-Cloud- und Rechenzentrumsausfälle
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. Berichterstattung über Fortschritte bei der Risikominderung im Zusammenhang mit dem Border Gateway Protocol; sicheres Internet-Routing
   https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. Border Gateway-Protokoll
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. Stellungnahmen der Internet Society, des Internet Architecture Board und der Internet Corporation for Assigned Names and Numbers in der Angelegenheit „Berichterstattung über Fortschritte bei der Risikominderung des Border Gateway Protocol“
   https://datatracker.ietf.org/doc/statement-iab-comments-of-the-internet-society-internet-architecture-board-and-internet-corporation-for-assigned-names-and-numbers-in-the-matter-of-reporting-on-border-gateway-protocol-risk-mitigation-progress/

6. Fahrplan zur Verbesserung der Sicherheit des Internet-Routings
   https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. Autonomes System (Internet)
   https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

8. Domainnamensystem
   https://en.wikipedia.org/wiki/Domain_Name_System

9. Dynamisches Hostkonfigurationsprotokoll
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. Ein deterministisches Internet
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

11. Hilbert-Kurve
    https://en.wikipedia.org/wiki/Hilbert_curve

12. Visualisierung des IPv4-Adressraums mithilfe von Hilbert-Kurven
    https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. Internet-Standortbestimmung
https://en.wikipedia.org/wiki/Internet_geolocation

14. Content-Bereitstellungsnetzwerk
https://en.wikipedia.org/wiki/Content_delivery_network

15. Liste der Länder nach IPv4-Adresszuweisung
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

16. Splinternet
https://en.wikipedia.org/wiki/Splinternet

17. Geoff Huston: Die Vergangenheit, Gegenwart und Zukunft des Internets
(TM: 1:08:18, „IPv6 – Zunehmend irrelevant“)
https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

Fußnote

DHCP und DNS bilden das wohl verwirrendste Technologiepaar im Internet, das uns seit Jahren ständig begegnet. DHCP verspricht individuelle Privatsphäre, indem es Abonnenten dynamisch und bedarfsgerecht IP-Adressen zuweist. Dieses Versprechen wird jedoch sofort und vollständig durch DNS zunichte gemacht, das auf Anfrage die jeweils aktuellste IP-Adresse einer Partei preisgibt – basierend lediglich auf deren Identität! Dadurch wähnen sich normale Internetnutzer in falscher Sicherheit, während gleichzeitig viele IT-Ingenieure gut bezahlte Arbeitsplätze haben. Dies ist ein perfektes Beispiel für das chinesische Sprichwort „Speer gegen Schild“ (矛盾).

Dennoch entstanden auf Basis dieses Schemas weitere Protokollebenen, von AS über BGP bis hin zur Einrichtung von Content Delivery Networks (CDNs), die die Dominanz multinationaler Konzerne ermöglichten. Dies führte schließlich zu großen Diensten wie Cloudflare und AWS, die einen zuverlässigen Pakettransport mit verbesserter Sicherheit versprachen. Die Robustheit dieser Dienste stand jedoch immer wieder im Fokus der öffentlichen Aufmerksamkeit. Und als das Internet gehackt wurde, schien niemand bereit, die Verantwortung zu übernehmen und nach Alternativen zur Verringerung der Anfälligkeit zu suchen. Vielleicht war es schwierig, Schuldige zu finden, weil das gesamte Internet so dezentral aufgebaut ist?

Andererseits bietet die aktuelle Internetkonfiguration ideale Voraussetzungen für einen Täter, der einfach eine beliebige fiktive IP-Adresse als gültigen, gewöhnlichen Internet-Teilnehmer verwenden kann, um den Angriff zu starten, und diese anschließend wieder aufgibt, wodurch kaum dauerhafte Spuren mit gültiger Identität für die forensische Nachverfolgung hinterlassen werden.