Sicheres und effizientes BGP-Routing

Beim Border Gateway Protocol (BGP) handelt es sich um ein grundlegendes Merkmal des Internets. Das Protokoll dient vor allem dazu, die Vielzahl an Netzwerken, aus denen das Internet besteht, zusammenzuhalten und die riesigen Datenmengen, die tagtäglich um die Welt geschickt werden, zu transportieren.

Gerade weil es sich um solch ein wichtiges Teil im Internet-Puzzle handelt, ist es besonders wichtig, dass es reibungslos funktioniert, und dass Schwachstellen, Unterbrechungen und Sicherheitsprobleme vermieden werden.

Das Internet verlässt sich dabei vor allem darauf, dass die Netzwerkbetreiber die richtigen Maßnahmen ergreifen, damit die jeweiligen Informationen an die richtigen Adressaten gelangen. Zugleich bedeutet die Bereitstellung einer stabilen und sicheren BGP-Routingfilterung für viele Organisationen eine Herausforderung.

Das BGP-Protokoll funktioniert sehr gut, wurde aber zu einer Zeit eingeführt, als die heutigen spezifischen Sicherheitsprobleme noch nicht existierten. Zudem arbeitet es mit Netzwerken zusammen, die auf der ganzen Welt verteilt sind, wodurch es potenziell eine Angriffsfläche für Piraterie und Datenlecks bietet. Die Internet Society schätzte beispielsweise, dass es 2017 mehr als 5.000 Datenlecks und Piraterievorfälle beim Routing gab.

Die zu diesem Phänomen vom Global IP Network bei NTT zusammengetragenen Informationen zeigen in den USA ein bestimmtes Muster: Die meisten derartigen Datenlecks scheinen in der Wochenmitte, um Dienstag herum, aufzutreten, während es aber auch eine Zunahme an Freitagen (also kurz vor dem Wochenende) gibt. Deshalb sollte man besonders zu diesen Zeiten wachsam sein.

Bei den BGP-Routing-Datenlecks handelt es sich um versehentliche Falschkonfigurationen oder die unrechtmäßige Veröffentlichung von Präfixen, oder auch um Blöcke von IP-Adressen, die über Netzwerke hinweg weitergegeben werden und zu einem suboptimalen Routing oder gar zu Piraterie führen können.

In den letzten zehn Jahren sind derartige Datenlecks wiederholt aufgetreten, und zwar Jahr für Jahr. Um den sich daraus ergebenden Problemen entgegenzuwirken, lohnt es sich daher, Filter einzusetzen.

Es gibt mehrere solcher Mechanismen, mit denen man sich vor Datenlecks schützen kann. NTT und das Global IP Network leisten gern die erforderliche Unterstützung.

Peerlock „Lite“

Eine Art der Filterung beruht auf einer Methode, die von NTT „Peerlock Lite“ genannt wird. Dabei werden Präfixe zurückgewiesen, die von Kunden oder Peers über Tier 1-Netzwerke empfangen wurden (siehe Link zu den Netzwerken, die sich üblicherweise auf dieser Stufe befinden).

So ist NTT beispielsweise nur über kostenfreies Peering erreichbar. Daher handelt es sich bei allen Routings zu NTT, die man von einem Kunden oder Peer empfängt, um Datenlecks. Durch den Einsatz von Schutzmechanismen zum Abweisen dieser Tier 1-Netzwerke bei privatem Peering oder beim Internetaustausch lassen sich auf recht einfache Weise viele potenzielle Probleme bereits im Vorfeld blockieren.

Der Nachteil besteht darin, dass hierfür eine statische Liste mit autonomen Systemnummern (Autonomous System Numbers, ASN) benötigt wird, anhand derer einzelne Netzwerke identifiziert werden können. Gerade weil sie statisch ist, muss die Liste immer dann aktualisiert werden, wenn es bei diesen Netzwerken zu Veränderungen kommt oder die Weiterleitung unterbrochen wird. Es ist deshalb sehr wichtig, eine halbjährliche oder jährliche Überprüfung durchzuführen, um die Liste auf aktuellem Stand zu halten. Weiter sind implizite oder explizite Kenntnisse der Weiterleitungsbeziehungen zu gesperrten ASNs erforderlich. Dennoch kann man sagen, dass diese Methode beim Aufspüren von Routinglecks als besonders effektiv gilt.

Durch den Einsatz von Schutzmechanismen … bei privatem Peering oder beim Internetaustausch lassen sich auf recht einfache Weise **viele potenzielle Probleme bereits im Vorfeld blockieren.**

BGP-Communities

Datenlecks können auch dadurch verhindert werden, dass Präfixe von kostenfreien Peering-Partnern niemals anderen Peering-Partnern mitgeteilt werden. Eine Möglichkeit hierzu besteht darin, bestimmte Routen mit BGP-Communities abzustecken bzw. Routen mit gemeinsamen Eigenschaften zu etikettieren. Filter können dann so eingestellt werden, dass Präfixe ohne die entsprechenden Communities schon beim Austritt von einem Grenzrouter zurückgewiesen werden.

Wenn zudem bestimmten Routen gar keine Community zugeordnet ist, sollten diese einer anderen Partei gar nicht erst mitgeteilt werden. Wenn diese Präfixe doch einmal in Ihr Netzwerk gelangen, werden sie zumindest nicht weitergegeben. Der Einsatz von BGP-Communities kann also ein wichtiges Mittel gegen Routinglecks sein.

Zu den bekanntesten BGP-Communities zählen „no-export“ und „no-advertise“. Erstere steht im Zusammenhang mit Routen, die nicht über die unternehmenseigene ASN hinaus publiziert werden sollen, während letztere für Routen verwendet wird, die nicht über den empfangenden Router hinaus bekanntgegeben werden sollen. Man muss das Verhalten dieser Communities verstehen, bevor man auf diese zugreift, um dafür zu sorgen, dass bei der Datenweitergabe das erforderliche Maß an Verfügbarkeit gewährleistet ist.

Communities können für Kategorien festgelegt werden, die berücksichtigen, woher die Routinginformationen stammen (beispielsweise von einem Transit-Kunden oder einem Peering-Partner), oder die geografische Orte (beispielsweise Europa oder eine bestimmte Stadt) einbeziehen. Gleichwohl gibt es zahlreiche Möglichkeiten für BGP-Communities, was zugleich ein großes Potenzial für deren Kontrolle bietet.

Ein typisches Beispiel für derartige Communities ist eine NTT-Community, mit der Ankündigungen an die Peering-Partner des Netzbetreibers unterdrückt werden können. Ein Kunde kann damit beispielsweise den Datenverkehr von einem Peer ablenken, der in seinem Netzwerk gerade einen Datenstau verzeichnet oder einen Netzwerkausfall erlebt, und auf einen anderen Peer umleiten. Eine Alternative besteht darin, den Datenverkehr umzuleiten, aber den Peer in Routingmitteilungen als ultimativen Backup anzubieten, falls es auch mit anderen Peers zu Verbindungsproblemen kommt.

Die Möglichkeiten lassen sich auf alle Peers anwenden, können aber auch selektiv eingesetzt werden. Das Ziel besteht darin, dass der Kunde ein Höchstmaß an Flexibilität erhält, um Routingmitteilungen gemäß den geschäftlichen Anforderungen einzusetzen.

Zugleich bietet NTT breitere Communities für regionale Lösungen und Community-gesteuertes Blackholing. Dazu gehören auch ein selektives und ein regionales Blackholing, was den Kunden Tools mit noch feineren Abstimmungen bietet.

Whitelists

Ein weiterer Ansatz besteht in der Nutzung sogenannter „Whitelists“. Diese enthalten Präfixe, die ein Kunde gegenüber jeder kundenseitigen externen BGP-Sitzung (eBGP) bekanntgeben kann, wodurch der Betrieb entsprechend sicherer wird.

Es handelt sich um ein Verfahren, bei dem NTT für solche Sitzungen die Daten von Internet-Routingregistern (Internet Routing Registry, IRR) nutzt. Tatsächlich nutzt das Unternehmen eine eigene Whitelist für jeden Kunden, was die Gefahr und das Ausmaß eines Schadens drastisch reduziert, und bei den von Kunden akzeptierten Routen eine strenge Kontrolle ermöglicht.

Neben den von NTT zu diesem Zweck angebotenen Mechanismen, gibt es zahlreiche Open-Source-Tools, die bei der Anwendung von Präfixfiltern nützlich sein können und sich in ein Format konvertieren lassen, das für die jeweilige Router-Plattform geeignet ist, beispielsweise BGPQ3.

NTT nutzt eine **eigene** Whitelist für **jeden Kunden,** was die Gefahr und das Ausmaß des Schadens drastisch reduziert.

Begrenzungen für maximal zulässige Präfixe

Eine weitere Methode, Routinglecks zu verhindern, besteht darin, Begrenzungen für maximal zulässige Präfixe festzulegen. So kann für eine eBGP-Sitzung beispielsweise eine Begrenzung von 1.000 Routen angewendet werden, wodurch die Sitzung beim Überschreiten dieser Zahl automatisch geschlossen wird.

Diese Präfixbegrenzungen bieten eine wichtige Sicherheitsmaßnahme, mit der das Netzwerk dem globalen Routingsystem möglichst wenig Schaden zufügt und gleichzeitig gegen Datenlecks schützt und somit die Sicherung von Routern und Netzwerken gewährleistet. Sie können als äußerst wirksamer Netzwerkschutz dienen, falls wirklich einmal ein Routingleck vorliegt, da sie eine Weiterverbreitung verhindern.

Maximale Begrenzungen für Präfixe lassen sich sowohl vor als auch nach der Richtlinie anwenden, auch wenn der größtmögliche Effekt vor der Richtlinie erzielt wird. Alle bedeutsamen Probleme werden dann vorzeitig abgewendet, ohne dass Präfixe versehentlich durchgelassen werden. Gleichwohl unterscheiden sich die Präfix-Filterrichtlinien je nach Routingplattform, und einige lassen die Filterung erst nach der Richtlinie zu.

Peerlocking

NTT hat bereits erfolgreich eine umfassendere Form des Peerlocking bereitgestellt. Damit lässt sich das Risiko von fälschlicherweise zugelassenen Präfixen auf einer globalen Ebene reduzieren.

Im Wesentlichen geht es dabei um eine „von Menschen definierte Sicherheit für Netzwerke“. Einfach ausgedrückt verlässt sich das System darauf, dass Peering-Partner NTT mitteilen, welche Netzwerke evtl. autorisierte Transit-Anbieter sind, wobei die Partner diese als „gesicherte ASNs“ bekannte Information liefern. Anschließend können all diejenigen Routen ausgeschlossen werden, die von nicht autorisierten Transit-Anbietern stammen.

Es ist unbedingt ratsam, dass die zu schützenden Netzwerke informiert werden und mit der Anwendung dieser Filter einverstanden sind, damit es nicht nachträglich zu unerwünschten Überraschungen kommt, wobei man sich erneut auf die Kommunikation mit Peers verlassen muss. Partner müssen immer wissen, was mit dem Netzwerk gerade geschieht, wofür auch ein entsprechendes Engagement erforderlich ist.

Ebenso wichtig ist, dass diese Peerlock-Filter auf alle eBGP-Sitzungen Anwendung finden, ganz gleich, ob diese für Kunden oder Peers bestimmt sind. Nur so ist sichergestellt, dass dieser zentrale Schutzmechanismus auch uneingeschränkt genutzt wird.

Zusammenfassend lässt sich sagen, dass das Peerlocking von NTT eine sehr effiziente Methode für eine Behebung von Routinglecks darstellt, und unser Unternehmen hat bei Netzwerken, die dem ASN-Schutz zugestimmt haben, eine signifikante Verbesserung festgestellt.

Das NTT Peerlocking kann deshalb **die Auswirkungen von Routinglecks reduzieren** und deren Ausbreitung eindämmen.

Flexibilität

NTT entspricht den regionalen Erwartungen und bietet zugleich eine globale und kostenfreie Flexibilität für all diejenigen Peers, die ihren Betrieb auf unterschiedlichen Kontinenten ausüben. Zudem bietet NTT ein Handbuch, das für jeden Peer mit Peerlocking eigens erstellt wird. Dabei werden die unterschiedlichsten Aspekte der Technologie und ihrer Funktionsweise in einer Dokumentation festgehalten, was auch für Unternehmen mit Personalfluktuation von Vorteil ist.

Insgesamt kann der NTT-Peerlocking-Mechanismus die Auswirkungen und die Verbreitung von Routinglecks deutlich reduzieren, wobei auch das aktive Monitoring der Zone ohne Default-Router (Default-free Zone, DFZ) hilft.

Ein Grund für den Technologie-Bereitstellungserfolg von NTT ist der GIN Unified Management System SDN-Controller (GUMS). Mit dem GUMS kann NTT Änderungen an Whitelists, Communities, Peerlocking und BGP-Richtlinien generell auf programmatische Weise bereitstellen. Das wiederum führt zu einheitlich bereitgestellten Konfigurationen und deutlich geringeren Fehlerraten bei der Konfiguration.

Der Betreiber nimmt Änderungen an der GUMS-Web-Schnittstelle vor und stellt diese über den GUMS-Server bereit, statt sich bei Routern anzumelden und die Änderungen von Hand vorzunehmen. Hierdurch wird der Prozess effizienter, und die Effektivität des Gesamtsystems wird verbessert.

Together we do great things

Um weitere Informationen oder Feedback zu erhalten, kontaktieren Sie uns unter: gin@ntt.net

Folgen Sie uns auf Twitter
@GinNTTnet
#globalipnetwork #AS2914

Oder besuchen Sie uns: gin.ntt.net