Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Inter-Domain-Routing

Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen

1 Ausgangslage

Das Internet ist der Zusammenschluss vieler autonomer Netze (autonome Systeme). Für die Wegführung (Routing) von Datenströmen zwischen diesen Netzen wird im Internet das Border Gateway Protocol (BGP) verwendet. Benachbarte Router können eine BGP-Session etablieren, um über diese Session Routinginformationen auszutauschen.

Wie bei nahezu allen Internetprotokollen wurden auch bei der Entwicklung von BGP keine Sicherheitsmechanismen vorgesehen. Eine systematische Analyse der Angriffsmöglichkeiten auf Routingprotokolle findet sich in [RFC4593].

Grundsätzlich kann zwischen *Gefährdungen für die BGP-Session* und *Gefährdungen durch falsche Routinginformationen* unterschieden werden. In der Praxis hat es aufgrund von Nachrichten mit gefälschten Informationen zahlreiche Vorfälle mit weitreichenden Auswirkungen gegeben.

Dieses Dokument fasst gängige Best Practice Ansätze zusammen und gibt Empfehlungen zur Verbesserung der Sicherheit des Routings. Es basiert auf einer aktuellen Zusammenstellung gängiger Best Practices, die in der IETF-Arbeitsgruppe *Opsec* erstellt wurden [RFC7454] sowie auf den Empfehlungen der NIST [SP 800-54].

2 Schutz der BGP-Session

BGP verwendet TCP als Transportprotokoll. Die TCP-Session sollte mit den üblichen Maßnahmen (z. B. ACLs und Rate-Limits) gegen Gefährdungen – wie Denial of Service Angriffe – geschützt werden.

Die eigentliche BGP-Session sollte nur mit definierten Nachbarn aufgebaut werden. Eine Authentisierung dieser Nachbarn erfolgt üblicherweise durch die Vereinbarung eines Schlüssels, der dann beispielsweise für **TCP MD5** [RFC2385] verwendet wird. Aufgrund bekannter Sicherheitsmängel sollte MD5 durch andere Verfahren ersetzt werden. Bessere Alternativen sind eine Authentisierung über den IPSec Authentication Header (**IPsec AH** [RFC4302]) oder die TCP Authentisierungsoption (**TCP-AO** [RFC5925]). Letzteres Verfahren ist noch nicht in vielen Produkten implementiert, sollte aber bei entsprechender Verfügbarkeit bevorzugt werden, da es den veralteten Standard TCP MD5 offiziell ablöst.

Für eine Authentisierung auf IP-Ebene kann der Generalized TTL Security Mechanism (**GTSM**) [RFC5082] genutzt werden. Die Idee des GTSM ist es, die Time to Live (TTL) von ausgehenden Paketen auf 255 zu setzen. Da Peers in der Regel direkt benachbart sind, sollte die TTL beim empfangenden Router ebenfalls 255 sein. Eine kleinere TTL deutet darauf hin, dass der Absender kein direkter Nachbar ist.

Wenn ein Router neu gestartet werden muss, kann der sogenannte Graceful Restart [RFC4724] verwendet werden, um unnötige BGP-Updates zu vermeiden. Beim Graceful Restart werden Pakete auch während des Neustarts auf Basis der alten, d. h. vor dem Neustart vorhandenen, Forwarding Information Base (FIB) weitergeleitet.

3 Schutz der Routinginformationen

3.1 Einsatz von Filtern

Um sich vor falschen Routinginformationen zu schützen, sollten eingehende Annoncierungen gefiltert werden (**ingress Filter**). Insbesondere sollten unzulässige Adressbereiche (z. B. RFC1918-Adressen) und die eigenen Adressen gefiltert werden. Von Kunden sollten nur die Routen akzeptiert werden, zu deren Annoncierung die Kunden auch autorisiert sind. Letzteres ist bei großen Peers und Upstreams häufig jedoch nicht sinnvoll umsetzbar.

Analog zum ingress Filter sollten auch ausgehende Routen gefiltert werden (**egress Filter**). Hier sind insbesondere unzulässige Adressbereiche, private AS-Nummern und Default-Routen zu nennen.

Zu spezifische Präfixe sollten generell gefiltert werden. In der Praxis ist das längste zulässige Präfix bei IPv4 ein /24 und bei IPv6 ein /48. Ebenfalls grundsätzlich gefiltert werden sollten die Peering-LAN-Präfixe von IXPs.

Quelle für unzulässige und reservierte Adressbereiche sind u. a. [IANA_v4], [IANA_v6] , [RFC6890] und [Bogon]. Detailliertere Empfehlungen zur Konstruktion von Filtern finden sich in [RFC7454].

3.2 Generierung von Filtern

Traditionell werden in Europa Filter aus den Daten der Internet Routing Registry (IRR) des RIPE NCC generiert. Dort sind Routinginformationen in Form von Objekten hinterlegt, die in der Routing Policy Specification Language (**RPSL**) definiert sind. Die Informationen in der IRR sind jedoch keine verlässliche Datenquelle, da sie nicht immer gut gepflegt werden.

Eine modernere Datenbasis bilden die sogenannten Route Origination Authorizations (**ROA**). Mit ROAs lassen sich Aussagen über Präfixe machen, beispielsweise welche autonomen Systeme das Präfix annoncieren dürfen und in welchen Längen es annonciert werden darf. ROAs sind somit eine Art Bescheinigung für die Eigenschaften von Präfixen. Diese Bescheinigungen sind mit einem Ressource Certificate signiert, das Bestandteil der Resource Public Key Infrastructure (**RPKI** [RFC6480]) ist.

Die für Europa zuständige Internet Registry – das RIPE NCC – bietet ihren Mitgliedern die Erstellung von ROAs als Dienstleistung an. Ähnliche Angebote gibt es auch bei anderen regionalen Internet Registries. ISPs sollten die Möglichkeit nutzen, für ihre IP-Bereiche ROAs anzulegen und dies selbst als Dienstleistung für Ihre Kunden anbieten.

Eine detailliertere Betrachtung von RPKI inklusive einer Anleitung zur Einrichtung findet sich in [BSI_RPKI].

3.3 Weitere Maßnahmen

Max Prefix
Als zusätzliche Maßnahme gegen Route-Leaks und unerwartete Routen von Peers sollte eine maximale Anzahl an Präfixen pro Peer definiert werden. Diese Maßnahme kann jedoch keinesfalls die Erstellung von Filtern ersetzen. Die Begrenzung an Präfixen pro Peer ist vielmehr eine Heuristik um sich vor Fehlkonfigurationen der BGP-Peers zu schützen, wie z. B. im AS7007-Vorfall [AS7007].

Route Flap Damping
In der Vergangenheit kam es bei einigen Implementierungen zu einer unnötig hohen Anzahl von BGP-Updates, die sich de facto wie ein DoS-Angriff auswirkten. Um die Stabilität von Routen zu erhöhen, wurde das sogenannte Route Flap Damping (**RFD** [RFC2439]) entwickelt. Die im ursprünglichen RFC vorgeschlagenen Parameter haben jedoch erhebliche Nebenwirkungen und sollten daher nicht verwendet werden. In der Praxis hat RFD ohnehin kaum Relevanz. Sollte es dennoch eingesetzt werden, so müssen die Standardwerte, die heute noch in vielen Implementierungen vorhanden sind, angepasst werden. Eine auf Messungen basierende Empfehlung für verwendbare Parameter findet sich in [RFD].

Max AS
Zu große BGP-Updates können sich ebenfalls wie ein DoS-Angriff auswirken [CVE140616]. BGP-Updates können beispielsweise durch sehr lange AS-Pfade oder viele Communities zu groß werden. Daher sollten die Anzahl der ASe im Pfad als auch die Anzahl der Communities begrenzt werden. Beim AS-Pfad sollte die Anzahl der Wiederholungen einer AS-Nummer (AS-Path Prepending) überprüft und per Filter limitiert werden. Communities mit der eigenen AS-Nummer im oberen Word sollten aus den BGP-Announcements von Peers und Upstreams entfernt werden.

uRPF
Moderne Router unterstützen mit Unicast Reverse Path Forwarding (**uRPF**) eine Technik, mit der sich das Problem von IP-Spoofing adressieren lässt. uRPF wurde in [RFC3704] spezifiziert, welches das bekanntere BCP38 aktualisiert. Die Idee hinter uRPF ist, dass Router die Informationen aus ihren Routingtabellen nutzen, um den Absender eines Paketes auf Plausibilität zu überprüfen, bevor sie ein Paket weiterleiten. RFC3704 definiert drei Operations-Modi: Strict, Feasible und Loose. Der strikte Modus darf nicht bei asymmetrischem Routing eingesetzt werden, da sonst legitime Pakete verworfen werden. In solchen Fällen sollten der Feasible Mode (falls implementiert) oder ansonsten der Loose Mode verwendet werden.

3.4 Ausblick

Aufbauend auf RPKI wird zudem von der IETF im Rahmen der Arbeitsgruppe *sidr* an einem Verfahren zur Validierung von AS-Pfaden gearbeitet [BGPSEC]. Die Standardisierung ist zur Zeit jedoch noch nicht abgeschlossen.

4 Literatur

[AS7007] http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html

[BGPSEC] An Overview of BGPSEC, http://tools.ietf.org/html/draft-lepinski-bgpsec-overview

[Bogons] Team Cymru Bogon, http://www.team-cymru.org/Services/Bogons/

[BSI_RPKI] How-To: RPKI - Maßnahmen gegen Prefix-Hijacking, https://www.allianz-fuercybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-118.pdf

[IANA_v4] http://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

[IANA_v6] http://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xml

[CVE140616] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0616

[RFC3704] Ingress Filtering for Multihomed Networks, http://tools.ietf.org/html/rfc2827

[RFC4593] Generic Threats to Routing Protocols, http://tools.ietf.org/html/rfc4593

[RFC4724] Graceful Restart Mechanism for BGP, http://tools.ietf.org/html/rfc4724

[RFC6480] An Infrastructure to Support Secure Internet Routing, http://tools.ietf.org/html/rfc6480

[RFC6890] Special-Purpose IP Address Registries, http://tools.ietf.org/html/rfc6890

[RFC7454] BGP operations and security, http://tools.ietf.org/html/rfc7454

[RFD] Making Route Flap Damping Usable, http://tools.ietf.org/html/draft-ietf-idr-rfd-usable

[SP 800-54] BGP Security, http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf

Diese BSI-Empfehlung ist unter Mitwirkung der als Partner der Allianz für Cyber-Sicherheit registrierten Internet-Service-Provider (*1&1 Internet AG, Deutsche Telekom, Kabel Deutschland, Unity Media KabelBW, Vodafone und Strato AG*) entstanden.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.