Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: BETREIBER UND UNTERNEHMEN

How-To: RPKI

Maßnahmen gegen Prefix-Hijacking

Das Internet ist ein Zusammenschluss vieler eigenständiger Netze, die als autonome Systeme (AS) bezeichnet werden. Jedes dieser autonomen Systeme ist für die Erreichbarkeit eines oder mehrere IP-Präfixe(s) verantwortlich. Der Austausch der hierzu notwendigen Routing-Informationen erfolgt über das Border Gateway Protokoll (BGP). Dieser Austausch basiert häufig auf Vertrauensbeziehungen, die sehr anfällig für eine Vielzahl von Bedrohungen sind.

Dieses Dokument stellt eine dieser Bedrohungen, das sogenannte Prefix-Hijacking vor, beschreibt mit der Resource Public Key Infrastructure (RPKI) eine Gegenmaßnahme und erläutert die Einrichtung von RPKI anhand eines Beispiels.

1 Prefix-Hijacking

Prefix-Hijacking bezeichnet die unerlaubte Annoncierung eines IP-Präfixes, das einem anderen autonomen System zugeordnet ist. Ist das Hijacking erfolgreich, wird der Internet-Verkehr für dieses Präfix an ein falsches autonomes System geleitet. Dies kann entweder zur Unerreichbarkeit der damit verbundenen IP-Adressen führen (Denial of Service) oder auch zum Mitlesen von Daten (Man in the Middle) genutzt werden.

In den letzten Jahren gab es einige prominente Beispiele für Prefix-Hijacking. Der vermutlich bekannteste Vorfall ist die Übernahme von YouTube durch Pakistan Telecom im Februar 2008, bei dem der Video-Dienst mehrere Stunden nicht erreichbar war. Im April 2010 wurde Datenverkehr aus den USA und anderen Ländern zu China Telecom umgeleitet, weil China Telecom 37.000 fremde IP-Präfixe annoncierte. Prefix-Hijacks sind ein alltägliches Phänomen, auch wenn sie nur in seltenen Fällen ein großes Presseecho erzeugen. Sie sind die Folge von Fehlkonfigurationen aber auch von aktiven Angriffen.

Um das Internet-Backbone vor solchen Bedrohungen zu schützen, sind zwei Schritte notwendig:

1. Die kryptographisch gesicherte Zuordnung von IP-Präfixen zu einem oder mehreren legitimierten autonomen System.
2. Die Überprüfungen der Annoncierungen auf den Internet-Knoten.

Im Folgenden konzentrieren wir uns auf den ersten Punkt.

2 Resource Public Key Infrastructure

Um der Bedrohung durch Prefix-Hijacking zu begegnen, wurde die *Resource Public Key Infrastructure* – kurz RPKI – entwickelt [RFC6480]. Diese Public-Key-Infrastruktur basiert auf X.509-Zertifikaten, die speziell der Absicherung des Internetroutings dient. Die

Zertifikatshierarchie entspricht der Vergabehierarchie von IP-Adressen, d. h. von der IANA über die regionalen Internet-Registrierungsstellen (RIR[1]) zu deren Mitgliedern (LIR[2]).

Jede LIR kann sich ein Ressourcenzertifikat ausstellen lassen, in dem alle ihr zugeordneten Internet-Ressourcen (AS-Nummern und IP-Präfixe) aufgeführt sind. Mit diesem Zertifikat können dann wiederum *Route Origin Authorisations* erzeugt werden, die es ermöglichen die Gültigkeit einer Annoncierung kryptografisch zu überprüfen.

2.1 Resource Certificate Authority

Prinzipiell gibt es zwei Möglichkeiten, eine RPKI zu betreiben. Bei einer *hosted RPKI* werden die RPKI-Objekte von einem RIR verwaltet. Bei *delegated RPKI* werden die Zertifizierungsstellen lokal, z. B. beim ISP aufgebaut.

Die für Deutschland zuständige regionale Internet-Registrierungsstelle RIPE NCC bietet über das Mitgliederportal (LIR-Portal) an, ein Ressourcenzertifikat zu erstellen und dieses beim RIPE NCC zu verwalten. Der Vorteil dieses gehosteten Systems ist die Auslagerung regelmäßiger Verwaltungsaufgaben, wie die Erneuerung von Zertifikaten. Nachteilig ist hingegen, dass z. B. die privaten Schlüssel beim RIPE NCC verbleiben.

Inzwischen ist diese Dienstleistung auch für Organisationen verfügbar, die zwar nicht Mitglied beim RIPE NCC sind aber dennoch sogenannte Provider-unabhängige IP-Adressen aus dem Zuständigkeitsbereich des RIPE NCC besitzen.[3]

Alternativ zum gehosteten System kann auch eine eigene Zertifizierungsstelle betrieben werden. Die Anbindung an das RIPE NCC ist derzeit noch im Testbetrieb.[4]

2.2 Route Origin Authorisation

Eine *Route Origin Authorisation* (ROA) ist ein kryptografisch signiertes Objekt, das Aussagen über die Gültigkeit von Annoncierungen ermöglicht. Es gibt Auskunft darüber, welches autonome System autorisiert ist, ein bestimmtes IP-Präfix zu annoncieren. Eine ROA enthält dafür die folgenden Informationen:

1. das autorisierte AS
2. das IP-Präfix, das von diesem AS annonciert werden darf
3. die maximale Länge des Präfixes

Wird keine maximale Länge angegeben, so darf ausschließlich das angegebene IP-Präfix annonciert werden. Eine Annoncierung von Sub-Präfixen ist dann nicht erlaubt. Es sollte auf alle mögliche AS-Präfix-Kombinationen geachtet werden, da es sonst zu ungewollten Effekten kommen kann [Detect].

Zu einer Annoncierung lässt sich über ROAs der Status dieser Annoncierung ermitteln. Folgende Zustände sind möglich:

Status	Bedeutung
NOT FOUND oder UNKNOWN	Es existiert keine ROA zu dieser Annoncierung.
VALID	Es existiert eine passende ROA zu dieser Annoncierung.
INVALID	Es existiert eine oder mehrere ROAs, die die Annoncierung abdecken, aber keines der ROAs stimmt mit dem Origin AS oder der Präfix-Länge in der Annoncierung überein.

Tabelle 1: Mögliche Status von Annoncierungen

1 Regional Internet Registry
2 Local Internet Registry
3 http://www.ripe.net/lir-services/resource-management/certification/resource-certification-rpki-for-provider-independent-end-users
4 http://www.ripe.net/lir-services/resource-management/certification/using-the-rpki-system

3 Einrichten von RPKI

Im Folgenden wird die Einrichtung von RPKI über das gehostete System beschrieben. Nachdem Sie die Schritte für ihre IP-Präfixe durchgeführt haben, können Dritte Annoncierungen dieser Präfixe auf ihre Richtigkeit hin überprüfen.

Zur Verdeutlichung wird bei der Einrichtung folgendes fiktives Beispiel[5] verwendet: Dem autonomen System AS65536 sind die IP-Präfixe 172.16.128.0/18 und 172.16.224.0/21 zugeordnet. Das IP-Präfix 172.16.128.0/18 wird zusammenhängend annonciert. Es ist nicht geplant, das Präfix in kleineren Blöcken zu annoncieren. Das Präfix 172.16.224.0/21 hingegen wird als /21 und als /22 annonciert. Eine Annoncierung als /24 soll ebenfalls möglich sein:

IP-Präfix	Annoncierung als
172.16.224.0/21	/21, /22, /24
172.16.128.0/18	/18

Tabelle 2: IP-Präfixe des AS65536

3.1 Benutzerrechte zuweisen

Zunächst muss einem Benutzer das Recht zur Einrichtung von RPKI zugewiesen werden:

1. Einloggen ins LIR-Portal unter https://lirportal.ripe.net.
2. Im Menü *MyLIR* den Unterpunkt *Manage Users* auswählen.
3. Die Benutzerrechte durch einen Klick auf *Edit* neben dem Benutzerkonto bearbeiten.
4. Auswählen von *Access and use Resource Certification (RPKI) [CERTIFICATION]*.
5. Veränderungen speichern.

Eine bebilderte Anleitung in englischer Sprache ist auf der Webseite des RIPE NCC verfügbar.[6]

3.2 Route Origin Authorisations einrichten

Derjenige Benutzer, dem das Recht *CERTIFICATION* zugewiesen wurde, kann nun unter der URL https://certification.ripe.net für die IP-Präfixe Route Origin Authorisations einrichten.

Wenn RPKI das erste Mal eingerichtet wird, muss eine Certificate Authority erstellt werden. Dazu müssen die AGB des RIPE NCC akzeptiert werden:

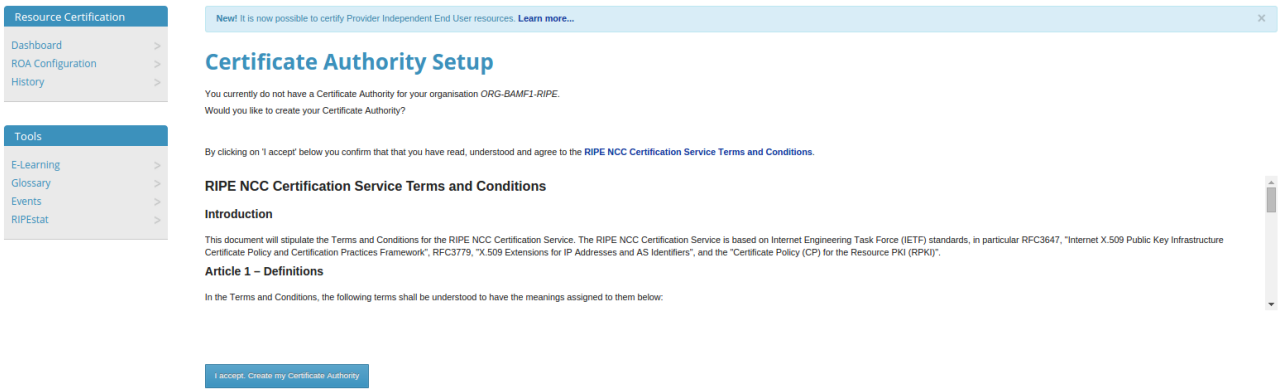

Abbildung 1: Einrichten der Certification Authority

Anschießend kann man sich für die ausgewählten IP-Präfixe passende ROAs vorschlagen lassen:

5 In dem Beispiel werden IP-Adressen aus einem reservierten Bereich für private Netzwerke verwendet.
6 http://www.ripe.net/lir-services/resource-management/certification/how-to-enable-resource-certification-in-the-lir-portal

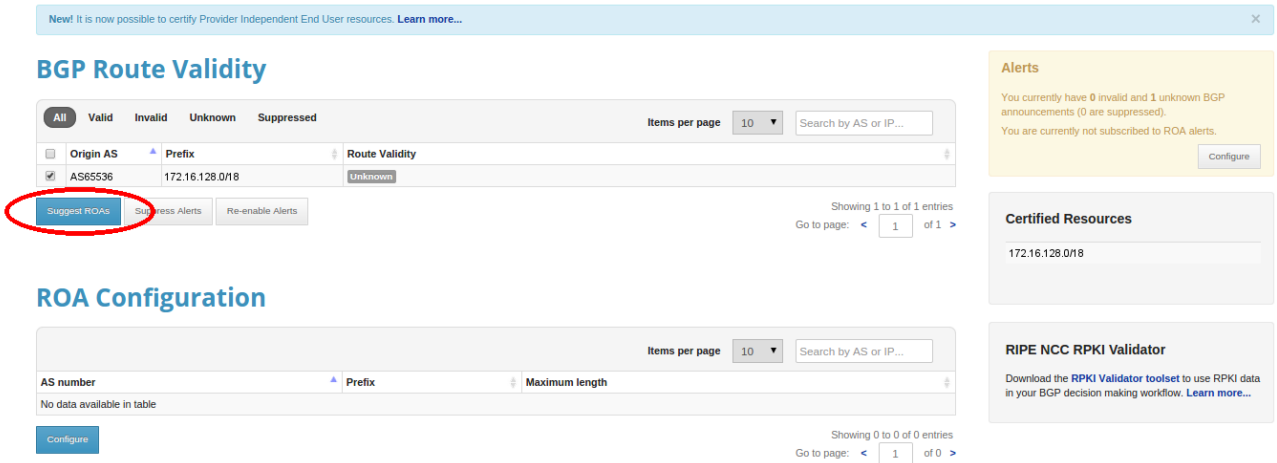

Abbildung 2: Vorschläge für ROAs generieren

Die vorgeschlagenen ROAs basieren auf den in der RIPE IRR Datenbank eingetragenen Route-Objekten und den tatsächlichen Routinginformationen. Es ist unbedingt erforderlich, die vorgeschlagenen ROAs auf Plausibilität zu prüfen und mögliche zukünftige Anforderungen zu berücksichtigen. Unter *BGP Route Validity* wird für jede vorgeschlagene ROA angezeigt, wie diese ROA den Status einer Annoncierung verändern würde:

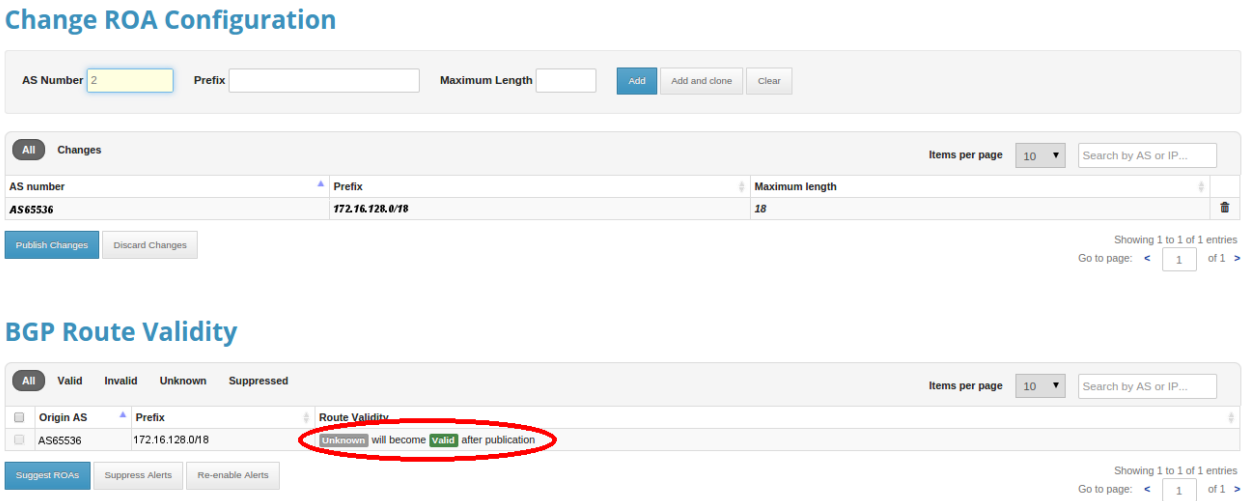

Abbildung 3: Status der vorgeschlagenen ROAs prüfen

Wenn die vorgeschlagenen ROAs in Ordnung sind bzw. an die Bedürfnisse angepasst wurden, müssen die Änderungen noch publiziert werden:

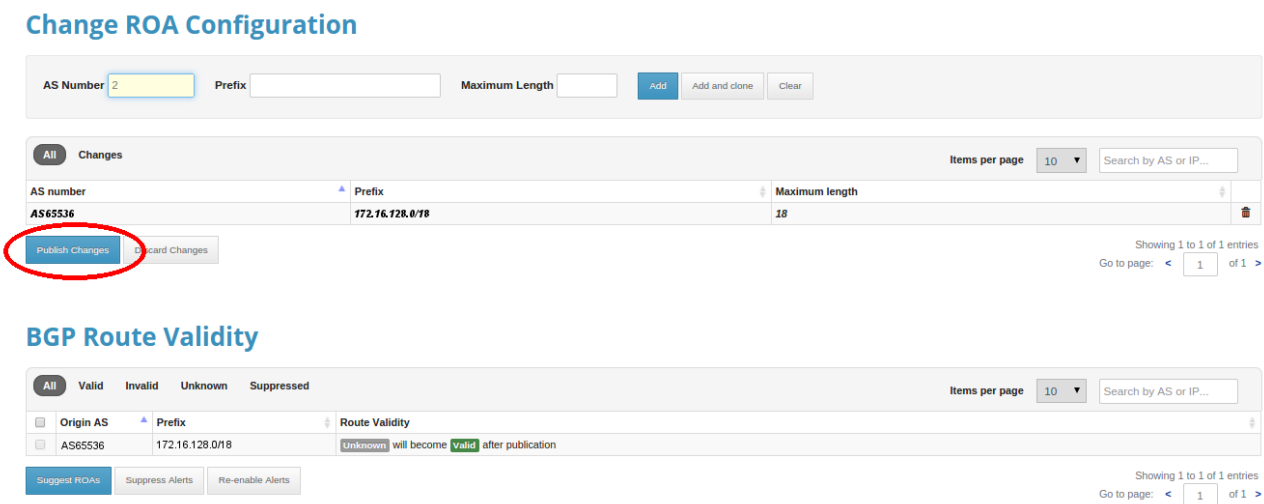

Abbildung 4: Publizieren der erzeugten ROAs

3.3 Gültigkeit der ROAs überprüfen

Nachdem die Einrichtung abgeschlossen ist, führt die URL https://certification.ripe.net direkt zum sogenannten *RPKI Dashboard*, wo sich die Gültigkeit von ROAs überprüfen lässt:

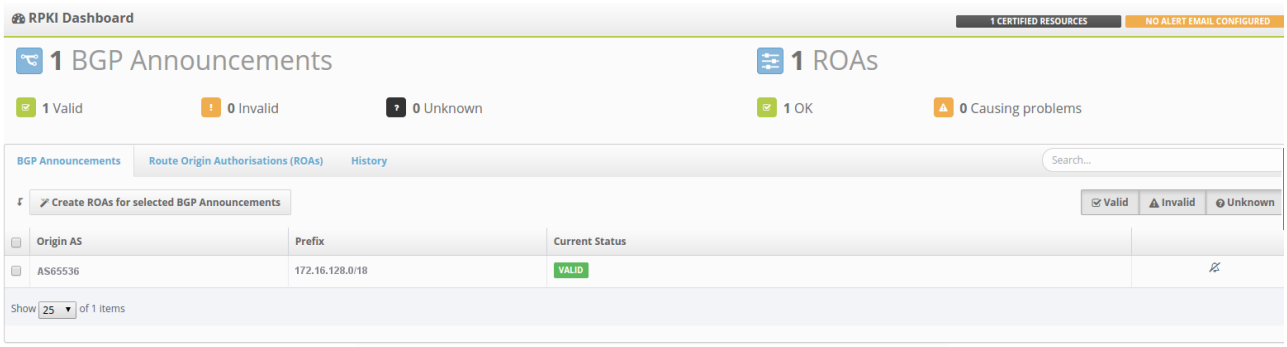

Abbildung 5: Statusanzeige im RPKI Dashboard

Dort lässt sich auch eine E-Mail-Alarmierung einrichten, die darüber benachrichtigt, wenn Annoncierungen mit dem Status INVALID oder UNKNOWN zu sehen sind:

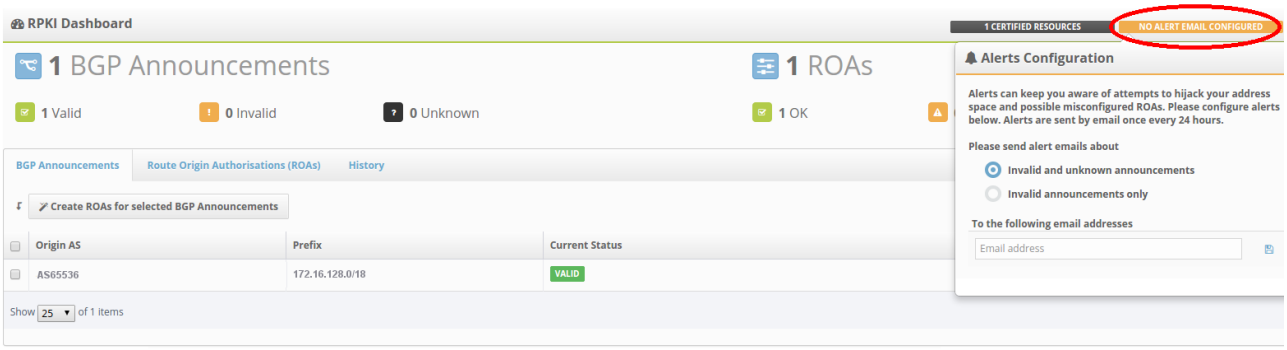

Abbildung 6: Einrichten eines E-Mail-Alarms

3.4 Stolperfallen bei der Einrichtung

Die häufigste Ursache für Annoncierungen, die als INVALID gekennzeichnet werden, ist eine Überschreitung der maximalen Präfix-Länge [NIST-RPKI]. Dies kann durch eine fehlerhafte Erstellung von ROAs bedingt sein.

Wenn im obigen Beispiel in der ROA für das Präfix 172.16.224.0/21 keine gesonderte Maximallänge festgelegt worden wäre, dann wären die Annoncierungen der /22 INVALID und nur die Annoncierung des /21 VALID.

Insbesondere wenn die Annoncierung des gesamten Präfixes durch ein anderes autonomes System erfolgt als die Annoncierung des Subpräfix – etwa bei einer Delegation von IP-Adressen – kann es schnell zu unbeabsichtigten Fehlern kommen.

4 Pro und Contra

RPKI ermöglicht bereits jetzt die zuverlässige Erkennung von Prefix-Hijacking und wird langfristig gesehen diese Art von Angriffen verhindern können. Dennoch gibt es Kritik an RPKI.

Das Widerrufen von Zertifikaten ermöglicht das Ergebnis der BGP-Validierung zu manipulieren. Dabei ist es unerheblich, ob der Widerruf versehentlich durch einen Fehler bei der Zertifizierungsstelle oder gezielt durch eine Kompromittierung oder dem Einfluss einer staatlichen Stelle bedingt ist. Es gibt derzeit zwei Vorschläge, die diese Bedenken adressieren, indem sie ungewollte Änderungen verhindern [Suspenders] oder zumindest erkennbar machen [Consent].

Trotz der Bedenken wurde der Bedarf an RPKI bereits von vielen AS-Betreibern erkannt. So sind beispielsweise Präfixe der Deutschen Telekom, Facebook, 1&1 und das BSI durch ROAs gesichert. Einige Provider validieren bereits jetzt die Annoncierungen auf Basis von ROAs.

5 Quellen

[Consent] E. Heilman, D. Cooper, L. Reyzin, S. Goldberg, From the Consent of the Routed: Improving the Transparency of the RPKI, 2014, http://dx.doi.org/10.1145/2619239.2626293

[Detect] M. Wählisch, O. Maennel, T. Schmidt, Towards detecting BGP route hijacking using the RPKI, 2012, http://dl.acm.org/citation.cfm?doid=2377677.2377702

[NIST-RPKI] NIST, Global Prefix/Origin Validation using RPKI, https://rpki-monitor.antd.nist.gov/

[RFC6480] M. Lepinski, S. Kent, An Infrastructure to Support Secure Internet Routing, 2012, http://tools.ietf.org/html/rfc6480

[Suspenders] S. Kent, D. Mandelberg, Suspenders: A Fail-safe Mechanism for the RPKI, https://tools.ietf.org/html/draft-kent-sidr-suspenders

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.