GovIX Betriebsvereinbarung

§ 1 Allgemeines

GovIX steht für "**Gov**ernment **I**nternet e**X**change" und stellt eine gemeinsame, komplementäre und verteilte Peering-Infrastruktur für den österreichischen Behördenbereich dar. In der Implementierung ist GovIX als dediziertes, österreichweites VLAN auf der ACOnet Infrastruktur realisiert und steht somit an allen ACOnet-PoPs zur Verfügung.

Es gelten für alle GovIX Teilnehmer zunächst die Grundsätze für die Teilnahme am ACOnet. ACOnet fungiert als Betreiber der zentralen Switching-Infrastruktur. Aufgrund der Reichweite des GovIX-VLANs in die Betriebsbereiche der Teilnehmer hinein ist ein gemeinsames Betriebskonzept und -verständnis erforderlich, das in der vorliegenden Betriebsvereinbarung definiert wird.

Neben dem eigentlichen GovIX-VLAN zählen auch noch der Routing-Layer, insbesondere die GovIX BGP Route-Server, sowie dedizierte Anycast-Instanzen von Domain Name Servern zur GovIX Infrastruktur. Diese Services werden vom ACOnet-Betreiber in Kooperation mit Betriebspartnern erbracht. Weitere Services, die von GovIX Teilnehmern gegenseitig angeboten und erbracht werden, sind nicht Bestandteil dieser Betriebsvereinbarung.

§ 2 Technische Voraussetzungen

Die Routing-Technologie des GovIX basiert auf dem Routing-Protokoll BGP. Jeder Teilnehmer betreibt entweder selbst mindestens einen BGP-Router oder bedient sich dafür eines Access-Providers. Für die Teilnahme ist je Teilnehmerrolle[1] jeweils eine unterschiedliche Autonomous System (AS) Number notwendig. Diese kann eine global eindeutige, vom Access-Provider für den Teilnehmer zur Verfügung gestellte oder eine durch ACOnet vergebene private AS-Number sein. Um den Konfigurationsaufwand für die Teilnehmer gering zu halten und die Betriebssicherheit sicher zu stellen, müssen die von den GovIX-Betreibern zur Verfügung gestellten redundanten Instanzen von BGP Route-Reflektoren verwendet werden. Das BGP-Peering erfolgt ausschließlich über diesen Mechanismus multilateral zwischen den Teilnehmern.

Die GovIX-Infrastrukturadressen (insbesondere Anschlussadressen der Teilnehmer-Router sowie der zentralen Route-Reflektoren am GovIX) sind offizielle IP-Adressen, welche durch die GovIX-Betreiber zugewiesen werden. Dieser Adressbereich darf nicht außerhalb des GovIX Betriebsbereiches als erreichbar angekündigt werden.

In der Regel kommunizieren die teilnehmenden Organisationen auch am GovIX unter Verwendung ihrer bereits im Internet genutzten IP-Adressen. Unter Umständen kann für den Teilnehmer eine Änderung des eingesetzten Routing-Protokolls oder auch eine Umstellung auf einen anderen IP-Adressbereich nötig sein. Die Überprüfung und Abklärung erfolgt durch die GovIX-Betreiber.

Die Identifikation eines Teilnehmers ist durch seine eindeutig zugewiesenen Adress-Bereiche (IPv4 oder IPv6 Prefixe) gegeben. Die Ankündigung von privaten IP-Adressen (RFC1918, RFC 4193) ist nicht zulässig.

Der Teilnehmer darf nur Adressbereiche via BGP ankündigen, die laut RIPE-Datenbank seinem AS zugeordnet sind.

[1] Primärteilnehmer, Sekundärteilnehmer, Peering-Partner, Access-Provider

§ 3 Anschlussmöglichkeiten

An Ethernet-basierten Internet Exchange Points (IXPs) gilt üblicherweise die Regel, dass pro Teilnehmer-Anschlussport an der Peering-Infrastruktur nur genau ein Peering-Router angeschlossen werden darf – es darf nur eine Ethernet MAC-Adresse sichtbar sein. Diese Regel dient der Betriebssicherheit und deren Sicherstellung durch den Betreiber und wird üblicherweise unterstützt und forciert durch automatische Port-Security, die bei einer Verletzung der Regel den jeweiligen Port automatisch abschaltet. Dies würde im Falle des GovIX allerdings eine größere Hürde darstellen, da fast alle Teilnehmer dann zusätzliche, dedizierte Zubringungen an die Infrastruktur oder geeignete Multiplexer installieren müssten. Es sind somit folgende Anschlussarten an die GovIX Infrastruktur vorgesehen (in der Reihenfolge der Präferenz durch die GovIX-Betreiber):

- dedizierter physischer Teilnehmer-Anschluss (IXP Standard)
- dedizierter VLAN-basierter Teilnehmer-Anschluss (Teilnehmer erhält GovIX als VLAN 701 auf bestehendem Ethernet/802.1Q Trunk aufgeschaltet)
- mehrfach genutzter physischer Dienstleister-Anschluss zum Anschluss mehrerer Teilnehmer
- mehrfach genutzter VLAN-basierter Dienstleister-Anschluss zum Anschluss mehrerer Teilnehmer

§ 4 Gewährleistung der Betriebssicherheit

Um die Betriebssicherheit am GovIX zu gewährleisten, ist eine symmetrische Routing- und Forwarding-Situation notwendig. Aus diesem Grund ist jeder Teilnehmer bzw. dessen Access-Provider verpflichtet, die von ihm am GovIX angekündigten Teilnehmer-Prefixes/Netzbereiche den GovIX-Betreibern bekanntzugeben. Es dürfen ausgehend nur Pakete mit einer Quelladresse aus diesen Netzbereichen über den GovIX übertragen werden. GovIX-Infrastrukturadressbereiche dürfen nicht über externe Routingprotokolle angekündigt werden. Am GovIX-VLAN ist nur BGP als Routingprotokoll erlaubt. Über den GovIX gelernte Prefixes dürfen – außer vom jeweiligen Eigentümer der Prefixes bzw. dessen Access-Provider – nicht über das GovIX-Teilnehmerumfeld hinaus angekündigt werden.

Betreiberverpflichtungen:

- Der **Betreiber** konfiguriert das GovIX-VLAN (701) mit dediziertem Rapid Spanning Tree Protokoll (IEEE 802.1w) mit primary und secondary Root-Bridge innerhalb der eigenen Infrastruktur.
- Der **Betreiber** konfiguriert die Teilnehmer- und Access-Provider-Anschlüsse mit geeigneten Port-Security Parametern (insbesondere: Spanning Tree Protokoll Root Guard, MAC-Address Limit, Broadcast Storm Filterung).

Der Betreiber übernimmt keinerlei Verantwortung für Konfigurationsfehler außerhalb seiner eigenen Infrastruktur. Ausfälle von Teilnehmer- oder Access-Provider-Anschlüssen oder Beeinträchtigungen der gemeinsamen Infrastruktur, die auf Konfigurationsfehler durch Teilnehmer oder Access-Provider zurückzuführen sind, sind vom Verursacher zu verantworten.

Teilnehmerverpflichtungen:

Jeder **Teilnehmer** stellt sicher, dass das GovIX-VLAN in seinem Netzwerk schleifenfrei bleibt.
Eine Weitergabe des GovIX-VLAN seitens des Teilnehmers an Dritte ist nur in Absprache mit den Betreibern zulässig.

Verpflichtungen des Access-Providers:

Jeder Access-Provider achtet darauf, dass jeder durch ihn angeschlossene Teilnehmer o.g. Voraussetzung einhält und dass das GovIX VLAN innerhalb seiner Providerinfrastruktur schleifenfrei bleibt.

§ 5 Wartungsfenster und Betriebsunterbrechungen

Inbetriebnahmen, Wartungsarbeiten und Außerbetriebnahmen, Teilnehmer- oder, Betreiber-seitig bzw. seitens eines Access-Providers, welche ausschließlich die GovIX-Infrastruktur betreffen, sind mit einer – in der Regel einwöchigen Vorlaufzeit – über die GovIX-Info Mailingliste an alle GovIX-Teilnehmer anzukündigen. Wartungen, die die darunterliegende ACOnet-Infrastruktur betreffen, werden über die ACOnet-Info Mailingliste ausgesandt.

Der Betreiber ist verpflichtet, mehrere Teilnehmer betreffende Störungen im GovIX via GovIX-Info Maillingliste und nach Behebung der Störung bzw. Ermittlung der Gründe, diese auch via GovIX-Info Maillingliste bekannt zu geben.

Betriebliche Anomalien und ungeplante Ausfälle oder Funktionsbeeinträchtigungen sind im Anlassfall an die GovIX-NOC Betreibermailbox zu melden.

§ 6 Empfehlungen seitens der Betreiber

Zur Erzielung einer bestmöglichen Ausfallsicherheit wird den Teilnehmern ein Doppel-Anschluss (Primary/Backup) unter Berücksichtigung der vorhandenen Backbone-Redundanzen empfohlen.

Um die im Rahmen des GovIX betriebene Domain Name Server Infrastruktur optimal nutzen zu können, wird den Teilnehmern empfohlen, den vom österreichischen Government CERT angebotenen Secondary Domain Name Service (GovDNS) in Anspruch zu nehmen.