

Sicherheitsanforderung

Architektur Zugangs- und Transportnetz

Deutsche Telekom Gruppe

Version	2.1
Datum	01.12.2019
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.57	Dokumententyp Sicherheitsanforderung
Version 2.1	Stand 01.12.2019	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.12.2019 - 30.11.2024	Freigegeben von Stefan Pütz, Leiter SEC-NIS

Zusammenfassung

In diesem Dokument werden Sicherheitsanforderungen beschrieben, die für die Absicherung von IP-basierten Zugangs- und Transportnetzen umgesetzt werden müssen.

Copyright © 2019 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Allgemein	5
2.1.	Systemmanagement	5
2.2.	Signalisierungsprotokolle	6
3.	Zugangsnetz	9
3.1.	Spoofing-Schutz	11
4.	Multi Protocol Label Switching (MPLS)	13
4.1.	MPLS Layer-2 und -3 VPNs	13

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus den im Konzern gültigen Sicherheitsrichtlinien erstellt.

Die Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden. Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten.

2. Allgemein

Req 1	Das Produktivnetz und dessen Systeme müssen von Test- und Entwicklungssystemen vollständig getrennt werden.
-------	---

Das Produktivnetz und dessen Systeme müssen komplett von Test- und Entwicklungssystemen getrennt werden. Hierbei ist eine physische Trennung vorzuziehen. Eine logische Trennung ist nur zulässig, wenn die logische Trennung beider Systemarten nicht umgangen werden kann. Des Weiteren muss sichergestellt werden, dass eine sicherheitsrelevante Beeinträchtigung der Produktion durch Aktivitäten auf den Test- und Entwicklungssystemen ausgeschlossen wird.

Wenn eine Kommunikation zwischen Produktivsystemen und Test-/Entwicklungssystemen notwendig sein sollte, ist dies nur über eine geschützte Verbindung erlaubt. Dies bedeutet, dass die Kommunikation zwischen den Systemen über ein separates System, beispielsweise eine Firewall oder einen Router mit Access Control List, geführt werden muss. Dies ist notwendig, um möglichst restriktive Regeln für die Kommunikation umsetzen zu können.

Motivation: Bei Test- und Entwicklungssystemen kann nicht von einem hinreichend sicheren Systemzustand ausgegangen werden. Diese Systeme unterliegen typischerweise permanenten Veränderungen. Bei der Nutzung von Produktivsystemen oder -netzen für Test- und Entwicklungsaufgaben sowie bei einer ungesicherten Kommunikation zwischen den verschiedenen Systemarten kann möglicherweise unberechtigt aus der Test-/Entwicklungsumgebung heraus auf die Produktionsumgebung zugegriffen oder deren Stabilität und Verfügbarkeit beeinträchtigt werden. Ein weiterer Vorteil der vollständigen Separierung der Produktionsumgebung von Test- und Entwicklungssystemen ist die permanente Nutzbarkeit für Abnahmetests. So ist es auch während kritischer Phasen (sogenannten „Frozen Zones“) beispielsweise möglich Sicherheitsupdates schneller zu testen und bereitzustellen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit

ID: 3.57-1/2.1

Req 2	Der IPv4- und IPv6-Infrastrukturadressraum des Transportnetzes darf von Kundenanschlüssen und angeschlossenen Netzen nicht erreichbar sein.
-------	---

Der Infrastrukturadressraum des Transportnetzes wird für die Erreichbarkeit innerhalb des Netzes verwendet. Diese Adressen werden u.a. für die Übertragung des Signalisierungsverkehrs genutzt. Diese Adressen müssen nicht oder nur sehr eingeschränkt von außen, das heißt von Kundenanschlüssen oder angeschlossenen Netzen wie z. B. dem Internet erreichbar sein. Daher muss die Erreichbarkeit beschränkt werden. Hierfür gibt es verschiedene Lösungsansätze. Ein Ansatz ist beispielsweise die Verwendung Access Control Lists auf Routern zum Schutz des Infrastrukturadressraums (iACL).

Motivation: Wenn der Infrastrukturadressraum des Transportnetzes uneingeschränkt erreichbar ist, kann dies von Angreifern genutzt werden um Denial-of-Service-Angriffe gegen einzelne Systeme oder das komplette Netz durchzuführen. Des Weiteren können Dienste (Routing- und andere Signalisierungsprotokolle) im Netz hierüber erreichbar sein. Dies ermöglicht eine direkte Manipulation der Infrastruktur durch Dritte.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit

ID: 3.57-2/2.1

2.1. Systemmanagement

Req 3	Eine zuverlässige Übertragung von Signalisierungs- und Managementverkehr muss sichergestellt werden.
-------	--

Datenpakete, die zum Austausch von Signalisierungsinformationen und zum Management der verschiedenen Systeme in einem Netz genutzt werden, müssen bevorzugt übertragen werden. Um dies zu erreichen müssen entsprechende Pakete beispielsweise in einer ausreichend priorisierten Quality-of-Service-Klasse transportiert werden.

Motivation: Wenn Signalisierungs-, Management- und Nutzerverkehr in einem Netz gleich behandelt werden, kann dies bei einer Überlastsituation dazu führen, dass der Austausch von notwendigen Signalisierungsinformationen und der Zugriff auf Managementdienste nicht mehr möglich ist. Dies bedeutet auch, dass betroffene Systeme nicht mehr für Wartungs- und Endstöraufgaben erreicht werden können. Eine solche Situation kann zu einer Instabilität des Netzes bis hin zu einer Beeinträchtigung der Verfügbarkeit führen. Ein Angreifer kann dies ausnutzen, um mittels Denial-of-Service-Angriffen einen Ausfall des Netzes herbeizuführen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.57-3/2.1

Req 4	Falls ein Datenaustausch zwischen der Managementebene und den Ebenen für Nutz- und Signalisierungsverkehr notwendig ist, darf diese Kommunikation nur abgesichert erfolgen.
-------	---

Grundsätzlich muss der Managementverkehr von Signalisierungs- und Nutzverkehr separiert werden. Es kann allerdings die Notwendigkeit bestehen, Daten zwischen den verschiedenen Ebenen auszutauschen. Sollte dieses notwendig sein, darf der Austausch nur über gesicherte Verbindungen erfolgen. Eine Absicherung erfordert hierbei die bidirektionale Restriktion der zulässigen Kommunikationsbeziehungen auf notwendiger Absender und Empfänger. Alle nicht benötigten Kommunikationsbeziehungen müssen unterbunden werden.

Motivation: Wenn eine ungeschützte Kommunikation zwischen verschiedenen Netzebenen möglich ist, kann ein Angreifer dieses ausnutzen, um Managementdienste von Systemen anzugreifen. Ist ein solcher Angriff erfolgreich, hat dies meist eine komplette Kompromittierung des entsprechenden Systems zur Folge.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

ID: 3.57-4/2.1

Req 5	Nach erfolgreicher Authentifizierung auf einem Netzelement darf es nicht möglich sein, ohne erneute Authentifizierung auf andere Netzelemente oder Systeme zuzugreifen.
-------	---

Es darf nicht möglich sein, nach erfolgreicher Authentisierung auf einem Netzelement ohne weitere Authentisierung Zugang zum Management eines anderen Netzelements oder Systems zu erhalten. Daher muss eine erneute Authentisierung für die Anmeldung an einem anderen Netzelement erzwungen werden.

Motivation: Durch diese Maßnahme wird verhindert, dass ein Angreifer ein einmal kompromittiertes Netzelement nutzen kann, um darüber ohne weitere Authentisierung Zugang zu anderen Netzelementen oder Systemen zu erhalten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

ID: 3.57-5/2.1

2.2. Signalisierungsprotokolle

Req 6	Für interne Signalisierungsprotokolle, über die Weeginformationen ausgetauscht werden, muss eine gegenseitige Authentifizierung genutzt werden.
-------	---

Bei Signalisierungsprotokollen, wie Routing-Protokollen (IBGP, OSPF, IS-IS etc.) und andere Protokollen, über die Weeginformationen verteilt werden (LDP, RSVP etc.), muss eine Authentifizierung der Kommunikationspartner untereinander eingesetzt werden. Die zur Authentifizierung genutzten Daten müssen gegen Einsichtnahme und Manipulation mittels kryptographischer Verfahren geschützt werden. Hierbei ist ein möglichst sicheres Verfahren zu wählen.

Motivation: Ein Angreifer kann Signalisierungsprotokolle angreifen, um Wegeentscheidungen im Netz zu manipulieren.

ren. Durch diese Manipulation kann Verkehr umgeleitet oder die Kommunikation gestört werden. Signalisierungsprotokolle und die dafür offenen Dienste auf einem Netzelement bringen zudem das Risiko von Denial-of-Service-Angriffen mit sich. Auch diese Angriffe können durch Nutzung einer gegenseitigen Authentifizierung der Kommunikationspartner bei entsprechenden Signalisierungsprotokolle verhindert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit

ID: 3.57-6/2.1

Req 7	Routing-Protokolle müssen auf Schnittstellen deaktiviert werden, auf denen der Versand und Empfang von Routing-Updates nicht erforderlich ist.
-------	--

Routing-Protokolle und somit der Versand von Routing Updates dürfen nur auf Schnittstellen zu anderen Netzelementen aktiviert sein, mit denen eine Nachbarschaftsbeziehung im Rahmen des entsprechenden Routing-Protokolls besteht. Auf allen anderen Schnittstellen ist das Routing-Protokoll zu deaktivieren.

Motivation: Ein Angreifer kann durch mitgeschnittene Routing Updates Informationen erhalten, die ihm Aufschluss über die Netzwerkarchitektur geben. Diese Informationen können für die Planung und Durchführung weiterer Angriffe genutzt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.57-7/2.1

Req 8	Für EBGp muss TTL-Security verwendet werden.
-------	--

EBGP-Pakete (External Border Gateway Protocol) werden mit einem TTL-Wert von 1 versendet, um sicherzustellen, dass sie nicht über einen Router hinweg übertragen werden. Durch die TTL-Security-Funktion wird erreicht, dass EBGp-Pakete mit einem möglichst hohen TTL-Wert versandt werden. Der TTL-Wert wird nach der Formel „255 – [maximale Anzahl notwendiger Hops]“ errechnet. Auf dem BGP-Nachbarn muss die Funktion mit dem gleichen TTL-Wert aktiviert werden. Nur so wird erreicht, dass BGP-Pakete mit einem kleineren als dem vordefinierten Wert verworfen werden. Die TTL-Security-Funktion wird nicht von allen Herstellern unterstützt.

Motivation: Ein ungeschützter BGP-Dienst kann von einem Angreifer übernommen werden. Ausserdem ist es möglich Denial-of-Service-Angriffe gegen erreichbare BGP-Ports und somit gegen den entsprechenden Router durchzuführen. Durch Umsetzung der Maßnahme werden Angriffe mit gefälschten BGP-Paketen aus Fremdnetzen weitestgehend unterbunden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit

ID: 3.57-8/2.1

Req 9	Falls Präfixe über ein Routing-Protokoll mit einem Kunden ausgetauscht werden, muss deren maximale Anzahl begrenzt werden.
-------	--

Wenn ein Router über Routing Updates neue Routen mitgeteilt bekommt, trägt er diese in seine Routing-Tabelle ein. Die Größe der Routing-Tabelle hat direkten Einfluss auf die Speicher- und CPU-Auslastung des Routers. Daher sollte abhängig von der verwendeten Hardware die maximale Anzahl der lernbaren Routen begrenzt werden.

Motivation: Eine zu große Routing-Tabelle kann zu einer kritischen Auslastung von System-Ressourcen wie dem Arbeitsspeicher und der CPU führen. Dies kann ein Angreifer gezielt nutzen, um mittels gefälschter Routen das Netzelement oder auch Teile des Netzes in seiner Verfügbarkeit zu beeinträchtigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.57-9/2.1

3. Zugangsnetz

Req 10	Falls die Echtheit eines Kundenendgerätes sichergestellt werden soll, muss ein standardisiertes Authentifizierungsverfahren genutzt werden.
--------	---

Es kann die Notwendigkeit bestehen, dass durch eine Authentifizierung die Echtheit von Endgeräten, die mit dem Zugangsnetz verbunden sind verifiziert werden muss. Hierdurch kann erreicht werden, dass sich nur bekannte und somit vertrauenswürdige Systeme mit dem Netz verbinden können. Dies ist meistens bei Systemen wie Netzelementen, die in nicht kontrollierbaren Umgebungen betrieben werden, oder auch bei Kundensystemen sinnvoll. Lösungen die hierfür in Frage kommen sind IKE/IPSec oder ggf. auch IEEE 802.1X (mit EAP) für eine Port-basierte Netzzugangskontrolle (PNAC).

Motivation: Netzelemente, die in unsicheren Umgebungen betrieben werden (z. B. Multifunktionsgehäuse im Außenbereich, kundenseitige Einrichtungen), unterliegen einer erhöhten Bedrohung durch Manipulationen oder unzulässigen Geräte austausch. Durch eine entsprechende Geräteauthentifizierung wird erreicht, dass nur vertrauenswürdige Systeme an das Netz angebunden werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

ID: 3.57-10/2.1

Req 11	Falls eine dynamische Vergabe von Adressen erfolgt, muss diese gegen Manipulationen geschützt werden.
--------	---

Wird eine dynamische Vergabe von IPv4- oder IPv6-Adressen wie beispielsweise DHCP genutzt, müssen entsprechende Systeme gegen die folgenden Szenarien geschützt werden:

- Manipulation der Adressvergabe mittels gefälschter Antwortpakete.
- Aufbrauchen des verfügbaren Adresspools.

Im Falle von DHCP muss ein Schutz gegen gefälschte Antwortpakete bzw. gegen einen gefälschten DHCP-Server durch die Funktion DHCP Snooping eingerichtet werden. Ein Schutz gegen das manipulative Allokieren des verfügbaren Adressraums ist z. B. die Beschränkung der maximalen Anzahl abrufbarer Adressen pro Anschluss, bzw. MAC-Adresse. Diese Maßnahme erfordert allerdings die Umsetzung einer weiteren Maßnahme, die gefälschte MAC-Adressen an einem Anschluss verhindert.

Motivation: Die automatische Vergabe von Adressen kann von einem Angreifer manipuliert werden. Eine Möglichkeit besteht darin, mittels gefälschter Antwortpakete Verkehr umzuleiten um so schutzbedürftige Daten mitschneiden zu können. Ein anderes Angriffsszenario ist das Aufbrauchen des verfügbaren Adresspools, wodurch für andere Systeme keine Adressen mehr verfügbar sind und diese in ihrer Funktionalität gestört werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.57-11/2.1

Req 12	Falls Signalisierungsprotokolle mit Kunden ausgetauscht werden, muss hierfür ein Rate Limit gesetzt werden.
--------	---

Signalisierungsprotokolle sind ein wichtiger Steuerungsmechanismus im Netz und werden beispielsweise für den Austausch von Routing- und Authentifizierungs-Daten auch mit Kunden ausgetauscht. Hieraus resultiert eine Bedrohung, da bei unzureichender Absicherung die Transportplattform beeinflusst werden kann. Daher muss ein Rate Limit für Signalisierungsprotokolle, die mit Kunden ausgetauscht werden, konfiguriert werden. Die entsprechenden Dimensionierung ist abhängig der verfügbaren Performanz der genutzten Netzelemente.

Motivation: Die Ressourcen (z. B. CPU, Speicher) eines Systems sind begrenzt. Dieses kann versehentlich ausgenutzt werden oder auch durch gezielte Angriffe dazu führen, dass die Systemverfügbarkeit negativ beeinflusst wird. In die-

sem Fall werden massenhaft erzeugte Signalisierungspakte genutzt, um eine hohe Last auf dem betroffenen System zu erzeugen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.57-12/2.1

Req 13	Bei Ethernet-basierten Kundenanschlüssen muss die maximale Anzahl erlernbarer MAC-Adressen auf Netzseite begrenzt werden.
--------	---

Wenn die Notwendigkeit besteht, dass auf Netzseite MAC-Adressen von Kundenendgeräten gelernt werden müssen, ist es notwendig, dass die maximale Adresse pro Kunde begrenzt wird. Anschlüsse bei denen MAC-Adressen gelernt werden müssen sind z. B. Ethernet-basierte und VPLS-/Layer-2-VPN-Kundenanschlüsse. Die maximale Anzahl zu lernender MAC-Adressen ist abhängig vom Einzelfall sowie der eingesetzten Hardware und kann daher nicht verbindlich vorgegeben werden.

Motivation: Ein Angreifer kann mittels gefälschter Pakete mit einer hohen Anzahl verschiedener MAC-Adressen ggf. die vorhandenen Ressourcen überbuchen, so dass Systeme in ihrer Funktionalität und somit Verfügbarkeit beeinträchtigt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.57-13/2.1

Req 14	VLAN-Tags, die von Kundenanschlüssen oder externen Netzen stammen, dürfen nicht für die Verkehrssteuerung genutzt werden.
--------	---

VLAN-Tags sind frei manipulierbar und somit als nicht vertrauenswürdig einzustufen, wenn sie auf Kundenseite vergeben werden. Daher müssen VLAN-Tags an der Netzgrenze entsprechend behandelt werden. Abhängig vom Nutzungsmodell sind folgende Vorgehensweisen möglich:

- Bei einem Layer-2 VPN-Dienst sendet der Kunde Pakete mit VLAN-Tag (C-Tag). Dieses C-Tag darf netzintern nicht ausgewertet werden, sondern der Verkehr muss transparent zu einem anderen Kundenstandort durch geleitet werden. Das heißt, dass netzintern der Verkehr gekapselt transportiert werden muss. Dies kann z. B. mittels eines zusätzlichen, an der Netzgrenze vergebenen, Provider-Tag (P-Tag) erreicht werden.
- Wird von einem Kunden kein Verkehr mit VLAN-Tag erwartet, so müssen Pakete mit VLAN-Tag verworfen werden.

Sollte abweichende von dieser Anforderung doch VLAN-Tags von Kundenseite für die netzintern Verkehrssteuerung genutzt, muss am Netzeingang geprüft werden, ob das VLAN-Tag für diesen Kunden korrekt ist und kein Mehrfach-Tagging (Q-in-Q) vorliegt.

Motivation: Mittels manipulierter VLAN-Tags kann ein Angreifer möglicherweise aus seinem erlaubten Kommunikationskanal ausbrechen, um so andere Systeme im Netz oder um Systeme von anderen Kunden erreichen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.57-14/2.1

Req 15	QoS-Werten in Paketen, die von Kundenanschlüssen oder externen Netzen stammen, darf nicht vertraut werden.
--------	--

Quality-of-Service (QoS) wird im Netz zum Priorisieren von Verkehrsströmen genutzt. Dies wird netzintern für eine vorrangige Übertragung von Signalisierungs- und Managementverkehr genutzt. Ausserdem werden mittels dieser Technik verschiedene Verkehrsklassen für Kunden realisiert. Daher ist es notwendig, dass die hierfür genutzten Parameter

in Paketen (TOS-Bit) oder Frames (p-Bits) auf vertrauenswürdigen Systemen vergeben werden. Dies bedeutet, dass entsprechende Werte, in Paketen oder Frames, die von Kundenanschlüssen oder aus angeschlossenen Netzen Dritter stammen, nicht vertraut werden darf. Auf Netzelementen an den Netzkanten müssen diese Werte überschrieben und auf eigene Werte geändert werden.

Motivation: Wenn ein Angreifer die QoS-Klasse von Paketen manipulieren kann, ist es ggf. möglich Verkehr aufzuwerten und so Leistungen in Anspruch zu nehmen die nicht seinem Vertrag entsprechen oder um den Transport von Daten anderer Kunden und der Transportplattform zu beeinflussen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.57-15/2.1

3.1. Spoofing-Schutz

Req 16	Gefälschte ARP-Pakete müssen erkannt und verworfen werden.
--------	--

Auf einem Netzelement oder auf einem separaten System im Netz muss ein Schutz vorhanden sein, durch den gefälschte ARP-Pakete erkannt werden. Die hierbei zu bevorzugenden Maßnahme ist der Einsatz von ARP Inspection für die Überwachung des ARP Cache und –Verkehrs und somit zum Erkennen von ARP-Spoofing-Angriffen. Weitere, zum Teil ergänzende Maßnahmen sind das Deaktivieren von Proxy ARP und Gratuitous ARP, sowie die Nutzung von statischen ARP-Einträgen.

Motivation: Ein Angreifer kann ARP Spoofing-Angriffe u.a. zur Vorbereitung von Man-in-the-Middle-Angriffen auf Systeme, die sich im gleichen Netz wie der Angreifer befinden, nutzen. Hierfür sendet er gefälschte ARP-Pakete an die Systeme im Netz, wodurch jeglicher Verkehr, der an das Ursprungssystem gesendet werden soll, über das System des Angreifers umgeleitet wird.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.57-16/2.1

Req 17	Frames von Kundenanschlüssen mit gleicher MAC-Absender- und -Zieladresse müssen verworfen werden.
--------	---

Einen Erkennung und Filterung von Frames mit gefälschten MAC-Adressen ist aufwändig und nur bedingt möglich. Daher müssen zumindest Frames die eine ungültige MAC-Absender- und -Zieladressen-Kombination enthalten, erkannt und verworfen werden. Dies sind Frames bei denen die MAC-Absender- und -Zieladresse gleich sind. Ein Netzelement muss einen solchen Frame als ungültig erkennen und verwerfen. Eine weitere Verarbeitung ist nicht erlaubt.

Motivation: Ein Angreifer kann manipulierte Frames mit gleicher MAC-Absender- und -Zieladresse nutzen, um anfällige Systeme in seiner Verfügbarkeit zu beeinträchtigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.57-17/2.1

Req 18	Frames mit gleicher MAC-Absenderadresse von unterschiedlichen Kundenanschlüssen am selben Netzelement müssen verworfen werden.
--------	--

Netzelemente speichern die MAC-Absenderadressen erstmalig weitergeleiteter Frames in einer Tabelle um nachfolgende Frames schneller verarbeiten zu können. Wenn eine MAC-Adresse an einem Kundenanschluss erkannt und in der MAC-Adressentabelle des Netzelementes gespeichert wurde, müssen Frames mit der gleichen MAC-Absenderadresse von einem anderen Kundenanschluss verworfen werden.

Motivation: Ein Angreifer kann einen Frame mit einer gefälschten MAC-Absenderadresse des Opfers senden. Ein Netz-

element, welches dies nicht erkennt, überschreibt die bestehende MAC-Adresse in der MAC-Adresstabelle mit der Portnummer des Anschlusses des Angreifers. Solange das Opfer keinen neuen Frame sendet, empfängt der Angreifer die Daten des Opfers.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.57-18/2.1

Req 19	Pakete mit gefälschter IPv4- oder v6-Absenderadresse müssen erkannt und verworfen werden.
--------	---

Auf Routern an Netzgrenzen, d. h. beispielsweise Übergängen zu Fremdnetzen und Netzelemente zu Kundenanschlüssen, muss ein Schutz gegen Pakete mit gefälschten IPv4- oder v6-Absenderadressen vorhanden sein, um entsprechende Pakete zu erkennen und zu verworfen. Mögliche Lösungen sind:

- Aktivierung der Funktion Unicast RPF (Unicast Reverse Path).
- Access Control List durch die Pakete erkannt und verworfen werden, die aus einem externen Netz stammen und eine IP-Absenderadresse aus dem internen Netz haben.

Im Falle von Peering-Routern dürfen nur gefälschte Pakete gefiltert werden, die an Infrastrukturadressen des Backbones gerichtet ist. Transitverkehr darf nicht reglementiert werden.

An Netzübergängen an denen eine Firewall zum Einsatz kommt, auf der eine IP Spoofing-Schutz realisiert ist, kann auf die Umsetzung dieser Maßnahme auf dem Router verzichtet werden.

Motivation: Ein Angreifer kann Pakete mit einer gefälschten IP-Absenderadresse nutzen, um bei Angriffen seine eigentliche IP-Absenderadresse zu verschleiern und um Systeme zu erreichen, für die seine IP-Absenderadresse gesperrt ist.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.57-19/2.1

4. Multi Protocol Label Switching (MPLS)

Req 20 Die innere Struktur des MPLS-Transportnetzes darf von außen nicht sichtbar sein.

Die innere Struktur des MPLS-Transportnetzes darf von außen nicht sichtbar sein. Das bedeutet, dass die Label Switch Router (LSR) des Transportnetzes bei einem Trace Route von einem Kundenanschluss oder aus Fremdnetzen nicht als Hop erscheinen dürfen. Das Transportnetz wird im Pfad somit nur mit zwei Hops (ingress und egress LER) dargestellt. Dies kann durch eine Konfiguration auf den entsprechenden Routern erreicht werden. Hierbei wird die Propagierung des TTL-Feldes des IP-Paketes in das vorangestellte MPLS-Label unterdrückt.

Motivation: Durch Umsetzung der Maßnahme wird die Informationsgewinnung durch einen Angreifer erschwert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit

ID: 3.57-20/2.1

4.1. MPLS Layer-2 und -3 VPNs

Req 21 Die Anbindung eines Kunden-Routers an den MPLS Edge Router muss über eine separate Verbindung erfolgen.

Um eine Separierung von VPNs zu gewährleisten, muss für jeden Anschluss eines Kunden-Routers (CE) an einen Label Edge Router (LER) eine separate Anbindung genutzt werden. Die Anbindung kann entweder physisch oder logisch getrennt erfolgen. Wird im Falle der logischen Trennung ein Switch genutzt, muss darauf geachtet werden, dass für jede CE-/LER-Anbindung ein separates VLAN genutzt wird.

Motivation: Falls mehrere Kunden-Router sich eine gemeinsame Layer-2-Infrastruktur für LER-Anschluss teilen, können ggf. von einem VPN-Kunden gefälschte Pakete eingespielt werden, um so Zugang zu einem VPN eines anderen Kunden am selben LER zu erhalten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit

ID: 3.57-21/2.1

Req 22 Kunden-VPNs müssen vollständig voneinander und vom zugrundeliegenden Transportnetz separiert werden.

Mittels Layer-2- und Layer-3-VPNs können virtuelle Netze für Kunden auf einem MPLS-basierten Transportnetz realisiert werden. Hierbei kann jeder Kunde seine eigenen IP-Adressstruktur nutzen ohne andere Kunden zu beeinflussen. Bei der Implementierung solcher VPN-Lösungen muss sichergestellt werden, dass der Verkehr und die IP-Adressstruktur der verschiedenen Kunden voneinander und von der genutzten Transportplattform separiert werden.

Motivation: Es muss sichergestellt werden, dass Kunden nicht aus ihrem VPN ausbrechen können. Ist die Überwindung der VPN-Grenzen möglich, kann ein Angreifer eventuell Pakete in fremde Kunden-VPNs einspeisen oder Systeme des Transportnetzes erreichen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit

ID: 3.57-22/2.1

Req 23 Falls in einem Kunden-VPN ein eigenes Routing genutzt wird, muss dieses vollständig vom Routing anderer VPNs und der Transportplattform getrennt werden.

Da jeder VPN-Kunde seinen eigenen IP-Adressraum innerhalb seines VPNs nutzen kann, besteht die Möglichkeit, dass mehrere Kunden gleiche IP-Adressen verwenden. Daher ist neben der strikten Separierung des VPN-Verkehrs auch die Nutzung einer unabhängigen Routing-Instanz pro Kunden-VPN notwendig.

Typischerweise wird die Separierung des Routings für ein VPN durch die Konfiguration von „Route Targets“ für das VRF (Virtual Routing and Forwarding) erreicht. Mittels „Route Targets“ wird definiert, welche Routen auf einem LER in ein VRF eines Kunden-VPNs importiert oder exportiert werden.

Motivation: Die Routing-Instanzen der verschiedenen Kunden-VPNs müssen komplett voneinander getrennt sein, da sonst eine unerlaubte Erreichbarkeit von Systemen zwischen Kunden-VPNs möglich wäre. Die größte Bedrohung für die Separierung der VPNs geht in diesem Fall von einer Fehlkonfiguration der Netzelemente aus.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit

ID: 3.57-23/2.1

Req 24	Die Komponenten des MPLS-Transportnetzes dürfen nicht aus Kunden-VPNs erreichbar sein.
--------	--

Das MPLS-Transportnetz stellt die Transportleistung von Daten für die angeschlossenen Kunden zur Verfügung. Für einen Kunden ist das MPLS-Transportnetz, an dem die CE seiner Lokationen angeschlossen werden, nicht sichtbar. Um die Transportleistung in Anspruch nehmen zu können, genügt es, dass maximal die IP-Adressen zwischen den CE und LER für den Anschluss seines VPNs an das MPLS-Transportnetz sichtbar sind. Eine Erreichbarkeit von IP-Adressen des Kernnetzes ist nicht notwendig.

Motivation: Eine direkte Erreichbarkeit des MPLS-Transportnetzes von einem Kunden-VPN aus, stellt ein erhöhtes Angriffsrisiko dar.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit

ID: 3.57-24/2.1

Req 25	Layer-2- und Layer-3-Signalisierungsverkehr von Kunden darf keinen Einfluss auf das Transportnetz haben.
--------	--

Ein Dienstmerkmal von Layer-2- und Layer-3-VPNs ist der Austausch von Signalisierungsprotokollen mit dem Kunden. Dieses wird für die Verbreitung von Routing-Informationen zwischen Kundenlokationen oder zum Austausch von Wegeentscheidungen für den Transport im VPN genutzt. Dabei ist sicher zu stellen, dass die verwendeten Signalisierungsprotokolle keinen Einfluss auf das Transportnetz haben.

Motivation: Eine Auswertung der Signalisierungsprotokolle durch die Transportplattform kann von einem Angreifer gezielt ausgenutzt werden, um die Plattform in Ihrer Verfügbarkeit zu beeinträchtigen oder um ggf. Verkehr zu beeinflussen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.57-25/2.1

Req 26	Es muss sichergestellt werden, dass Targeted-LDP-Pakete nur von vertrauenswürdigen Absendersystemen akzeptiert werden.
--------	--

Targeted-LDP-Pakete (LDP = Label Distribution Protocol) werden zwischen Routern ausgetauscht, die nicht direkt miteinander verbunden sind, um darüber beispielsweise Layer-2 VPNs aufzubauen. Da solche Pakete über mehrere Hops hinweg versendet werden können, muss sichergestellt werden, dass diese nur von vertrauenswürdigen Absendern akzeptiert werden.

Eine Option um dies zu erreichen ist es die Akzeptanz von Targeted-LDP-Paketen auf konfigurierte Nachbarn zu be-

schränken. Dies wird allerdings nur von einigen Router-Herstellern unterstützt. Eine weitere Möglichkeit ist die Nutzung von Filterlisten, um Targeted-LDP-Pakete nur von autorisierten IP-Absenderadressen zu zulassen.

Motivation: Das Akzeptieren von allen Targeted-LDP-Anfragen auf einem Zielsystem ermöglicht einem Angreifer, falsche Informationen an ein Zielsystem zu senden und damit die Stabilität einzelner VPNs oder auch der Plattform zu gefährden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.57-26/2.1