TLP : green

Ist SCION unangreifbar und unaufklärbar?

Explorative Arbeit

Masterthesis

Studiengang:	MAS Cyber Security
Autor*in:	Patrick Hager
Betreuer*in:	Jérôme Bueche
Auftraggeber*in:	VBS
Expert*in:	Hansjürg Wenger, Hans-Peter Käser
Datum:	10.03.2024

Berner Fachhochschule

Technik und Informatik
MAS Cyber Security

Abstract

Die Zahl der Cyberangriffe auf Unternehmen, kritische Infrastrukturen und Einzelpersonen wächst mit der zunehmenden Vernetzung in der digitalen Welt überproportional an. Kriminelle Gruppierungen haben meist monetäre Interessen. Aber auch Angriffe aus politischen Interessen, zu Spionage- und Sabotagezwecken sind Gefahren im Cyberraum. Die Hauptziele von Hackerangriffen sind Datendiebstahl, Datenmissbrauch, Datenmanipulation, Kontrolle über die IT-Infrastruktur und Informationsfluss.

Während sich ein Teil der Angriffe auf den Inhalt der Daten konzentriert, gibt es auch Angriffe auf die Kommunikationswege im Internet. Dazu gehören DDoS-Attacken, welche darauf zielen, IT-Systeme mit grossen Mengen von Anfragen innerhalb einer kurzen Zeit zu überfluten und lahmzulegen. Angriffsziele können zum Beispiel Webserver sein. Aber auch Komponenten in der Lieferkette eines Unternehmens, einer Organisation oder eines Staates können von Attacken betroffen sein. Ein solcher Angriff kann direkte oder indirekte finanzielle Konsequenzen haben und dem Image schaden.
Auch Meldungen zu 'BGP-Hijacking' sind oft in den Medien zu lesen. Bei diesen Angriffen handelt es sich um Attacken und Übernahmen von Kommunikationspfaden im Internet. Dabei geht es bei solchen Angriffen darum, an Informationen aus den Datenströmen zu gelangen. Oft stecken politisch motivierte Akteure hinter solchen Angriffen. Es können auch wirtschaftliche Schäden daraus entstehen.

SCION (Scalability, Control and Isolation on Next-Generation Networks) ist eine neue Internetarchitektur, welche zum Ziel hat, die Kommunikationswege im Internet sicherer zu machen und Angriffe wie DDoS und BGP-Hijacking zu verhindern. Diese Architektur wurde grösstenteils von einer Forschungsgruppe der ETH Zürich entwickelt und wird immer noch weiter ausgebaut. Der Vorteil dieser Architektur besteht darin, dass sie die bestehende Internetarchitektur nicht ersetzt, sondern darauf aufbaut und ergänzt. Mit SCION sind die Transportpfade, über welche die Daten gesendet werden, definiert und kryptografisch abgesichert. Die erste praktische Anwendung dieser Architektur ist das Swiss Secure Finance Network (SSFN), welches dem Schweizer Finanzplatz eine sicheres Kommunikationsnetzwerk bietet und Daten direkt zwischen zwei Finanzinstituten sicher austauschen lässt. Eine weitere Anwendung ist der HIN Vertrauensraum. Dieser befindet sich im Aufbau und hat zum Ziel, die verschiedenen Akteure des Schweizer Gesundheits- und Sozialwesens einfach und sicher zusammenzuführen.
SCION schützt die Integrität der Kommunikationswege zwischen allen Teilnehmern in einer Domäne mit kryptografischen Methoden und stellt mit einer gut ausgelegten Netzwerktopologie eine hohe Verfügbarkeit sicher. Jedoch ist die Kommunikation in SCION ohne Zusatzmassnahmen nicht anonym. Jeder Teilnehmer des Netzwerks hat die Möglichkeit, die Kommunikation der anderen Teilnehmer zu verfolgen. Die Nutzdaten sind in SCION nicht verschlüsselt. Eine Verschlüsselung der Nutzdaten muss auf einem höheren Layer im OSI-Modell (4-7) zusätzlich erfolgen, z.B. durch einen VPN-Tunnel.

In einem Bereich des Kommando Cyber im VBS gibt es Bestrebungen, SCION als eine Komponente für eine sichere Kommunikation über öffentliche Netze zu Nutzen. Dabei soll SCION als Ergänzung zur bestehenden einsatzkritischen Kommunikationsplattform vom Kommando Cyber, zur Erschliessung kleiner Bürostandorte und temporären Arbeitsplätzen genutzt werden. Während der Bau neuer Glasfaserleitungen ein langwieriger und kostenintensiver Prozess ist, bietet SCION die Möglichkeit, neue Standorte über die Netze öffentlicher Internet Service Provider schnell, flexibel und trotzdem sicher zu erschliessen.

Diese Arbeit befasst sich mit Möglichkeiten und Risiken der Erschliessung neuer Standorte über SCION. Die Architektur soll dafür ausgelegt sein, dass sensible Daten, bis Stufe geheim, über das Netz versendet werden können. Zur Erschliessung kleiner Standorte mit dem Netzwerk vom Kommando Cyber über die Netzwerkinfrastruktur öffentlicher Internet Service Provider (ISP) werden drei Anwendungsfälle betrachtet.

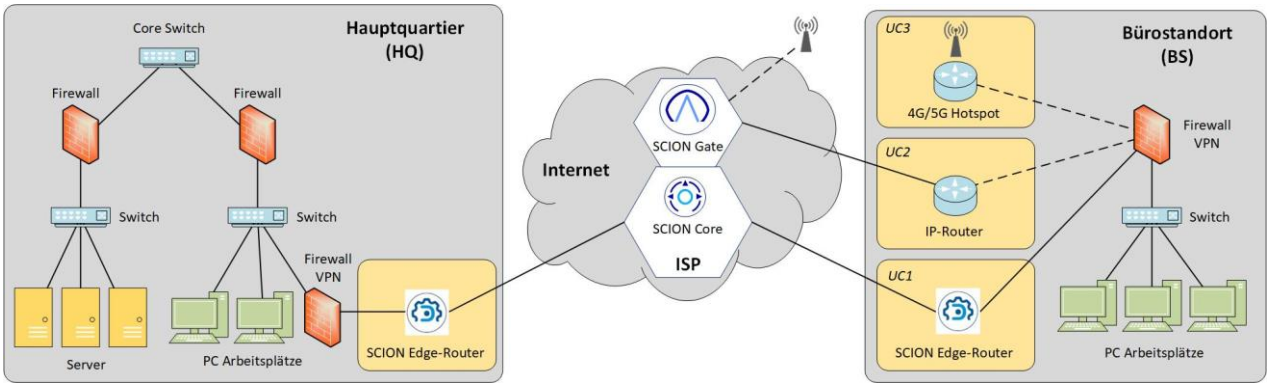

Abbildung 1: Netzwerkaufbau der Anwendungsfälle (UC)

- Bei Anwendungsfall 1 (UC1) (vgl.Abbildung 1) werden sowohl im Hauptquartier wie auch am Bürostandort SCION Edge-Router installiert, welche kryptografisch die Integrität der Kommunikationspfade über das öffentliche Netz des Internet Service Providers (ISP) sicherstellen.
- In Anwendungsfall 2 (UC2) kommt am Bürostandort ein konventioneller IP-Router zum Einsatz. Die Integrität des Kommunikationswegs wird in diesem Fall erst zwischen SCION Gate im Netzwerk des Internet Service Providers (ISP) und dem SCION Edge-Router des Hauptquartiers durch kryptografische Massnahmen sichergestellt. Die Strecke zwischen IP-Router vom Bürostandort bis zum SCION Gate bleibt kryptografisch ungeschützt und ist somit weiterhin den bekannten Gefahren im Internet ausgesetzt.
- Bei Anwendungsfall 3 (UC3) kommt anstelle eines kabelgebundenen IP-Routers ein 4G/5G Hotspot zum Einsatz, welcher die Verbindung zwischen Bürostandort und ISP über die Luftschnittstelle des Mobilfunknetzes sicherstellt. Auch hier ist die Pfadintegrität erst ab dem SCION Gate in Richtung Hauptquartier kryptografisch geschützt.

Der Einsatz von SCION über ein öffentliches Netz wird für Anwendungsfall UC1 als eine mögliche Ergänzung zu eigenen Glasfaser- oder Kupferleitungen erachtet. Dabei erfolgen die Verbindungen immer von einem SCION Edge-Router über den SCION Core. Die Pfadintegrität ist über den gesamten Weg im Netzwerk des ISP kryptografisch gesichert. Die zwei weiteren Anwendungsfälle UC2 und UC3, welche eine Verbindung zum SCION Netzwerk mit einem konventionellen IP-Router oder einem 4G/5G Hotspot zu einem SCION Gate herstellen, sind für die betrachteten Einsatzzwecke nicht zu empfehlen. Mit der Entwicklung eines portablen SCION Edge-Routers können die Risiken für diese beiden Anwendungsfälle verringert werden. Das Ziel ist es, dass sämtliche Verbindungsvarianten immer von einem SCION Edge-Router über den SCION Core erfolgen. Somit ist sichergestellt, dass der Kommunikationspfad über die gesamte Strecke im öffentlichen Netzwerk des ISP integritätsgeschützt ist.

Inhaltsverzeichnis

1 Einleitung

Das Internet ist das grösste und meistgenutzte Kommunikationsmittel der heutigen Zeit. Sicherheitslücken sind eine ernsthafte Bedrohung für staatliche Organisationen, Unternehmen und Privatanwender. Kriminelle Gruppen und staatlich unterstützte Organisationen führen immer wieder Angriffe auf Internetinfrastruktur aus, um sich einen wirtschaftlichen, politischen oder militärischen Vorteil zu verschaffen [1]. Meldungen wie 'BGP-Hijacking' und 'DDoS Angriff' gehören heute zum Alltag im Internet.

Das Border Gateway Protokoll (BGP) ist ein fundamentales Internet-Routingprotokoll zum Austausch von Datenpaketen zwischen unabhängigen Autonomen Systemen (AS) [2, S. 83–85]. Während der Entwicklung des BGP-Protokolls Anfang der 1990er Jahre war die Sicherheit und Verwundbarkeit im Internet noch kein grosses Thema. Jeder Internet Service Provider (ISP) besitzt für sein Netzwerk ein oder mehrere AS. Zur Verhinderung von Konflikten mit öffentlichen Internetprotokoll-Adressen (IP), werden IP-Adressen von Internetregistrierungsstellen verwaltet, welche jedem AS eindeutige IP-Adressbereiche zuweisen. BGP-Nachrichten sind unverschlüsselt. Die Authentizität des Absenders kann kryptografisch nicht verifiziert werden [2, S. 103]. Fehlkonfigurationen oder bewusste Manipulation der Routingpfade eines AS können Datenpakete fehlleiten [2, S. 103]. Bei böswilliger Absicht können Datenpakete von Teilen oder eines ganzen AS-Netzwerks umgeleitet, eingesehen und manipuliert werden. In diesem Fall handelt es sich um BGP-Hijacking.
Das Problem der mangelnden Sicherheitsmechanismen in den Kernprotokollen des Internets wurde früh erkannt. Ende der 1990er und zu Beginn der 2000er Jahre wurde an Sicherheitsverbesserungen der Protokolle geforscht. Mit Border Gateway Protocol Security (BGPsec) und Resource Public Key Infrastructure (RPKI) entstand die Grundidee, IP-Adressbereiche und AS-Nummern kryptografisch zu zertifizieren und BGP-Nachrichten zu authentifizieren. Die Standardisierung von BGPsec und RPKI wurde erst in den Jahren 2012 und 2017 vollzogen und deren Einsatz nahm in den letzten Jahren erheblich zu. Jedoch zeigte sich aus einer detaillierten Analyse des Protokolls, dass BGPsec nur geringe Sicherheitsvorteile bietet, auch wenn alle AS das Protokoll konsequent umsetzen und nutzen. Bei einem teilweisen Einsatz von BGPsec, d.h. wenn nicht alle AS das Protokoll verwenden, kann es Instabilitäten im Routing verursachen. Zudem können mit Downgrade-Angriffen AS dazu gebracht werden, dass gefälschte Standard-BGP-Nachrichten akzeptiert werden, obschon mit BGPsec ein gesicherter Pfad existiert. Auch bei einer weltweit konsequenten Umsetzung von BGPsec besteht das Problem, dass nur sehr wenige Organisationen an der Spitze der RPKI-Hierarchie stehen. Diese haben die Macht, Zertifikate zu erstellen oder zu widerrufen und so die Möglichkeit, Teile des Internets vom Rest der Welt zu trennen. Die ständigen Änderungen der Routingpfade im Internet führen zu einer grossen Anzahl an BGP-Update Nachrichten. Dies erfordert bereits eine hohe Rechenleistung der BGP-Infrastruktur. Mit BGPsec wird aufgrund der zusätzlichen kryptografischen Operationen noch erheblich mehr an Rechenleistung bei der BGP-Infrastruktur notwendig [1, S. 5-6].

Das Ziel eines Distributed Denial of Service Angriffs (DDoS) ist es, ein System mit einer grossen Zahl von Anfragen verschiedener Hosts zu überfluten, bis dieses die Anfragen nicht mehr verarbeiten kann und der Dienst nicht mehr zur Verfügung steht. Dies kann zum Beispiel ein Webserver eines Webshops sein, welcher während der Dauer des Angriffs reguläre Anfragen nicht mehr verarbeiten kann.

Beide Angriffsarten lassen sich mit der bestehenden Internetarchitektur und BGP nur schwer verhindern.

Mit SCION (Scalability, Control and Isolation on Next-Generation Networks), einer neuen Internetarchitektur, lassen sich viele der Probleme von BGP minimieren oder verhindern. Im Jahr 2012 startete eine Forschungsgruppe der ETH Zürich mit dem Ziel, das Internet sicherer zu machen. Während etablierte sichere Internetprotokolle wie Transport Layer Security (TLS) oder Virtual Private Network (VPN) im OSI-Modell zwischen Layer 4 bis 7 funktionieren, verfolgt SCION das Ziel, die Kommunikationspfade auf Layer 1 bis 3 durch Skalierbarkeit, Kontrolle und Isolation zu schützen [3, S. 7–8]. SCION ist ein Inter-Domain Routingprotokoll, mit Fokus auf die Kontrolle und Sicherheit der Kommunikationspfade.

«*Im Unterschied zu einer herkömmlichen Internet-Infrastruktur wird ein Datenpaket in SCION nicht nur mit der Empfangsadresse versehen, sondern es enthält bereits beim Abschicken die ganze Route, die es auf dem Weg durchs Internet einschlagen soll. In SCION machen Datenpakete deshalb keine Umwege – wie sie im heutigen Internet oft vorkommen – und vertrauliche Daten geraten auch nicht auf unerwartete Abwege*» [4].

Jedoch ist wichtig zu wissen, dass SCION keine Ende-zu-Ende Verschlüsselung bietet und auch keine intra-AS Routingprobleme löst. Das Hauptziel von SCION ist es, eine hochverfügbare und effiziente Zustellung von Datenpaketen zwischen Domänen (AS) durch integritätsgeschützte Kommunikationswege zu ermöglichen [5].

2 Ausgangslage

Das Kommando Cyber betreibt in der Schweiz ein hochsicheres Netzwerk für die eigene Informatikinfrastruktur als Backbone für den Datentransport im VBS. Es gibt Bestrebungen, neue Standorte in der Schweiz mit bis zu 10 Arbeitsplätzen oder einsatzbezogene temporäre Büros zu erschliessen. Allerdings ist die Erschliessung eines neuen Standortes mit dem Transportnetz ein zeit- und kostenintensiver Prozess. Deshalb werden Alternativen gesucht, mit welchen zukünftig solche Standorte schneller und kostengünstiger, aber trotzdem sicher angebunden werden können.

Im Rahmen einer Studie mittels Proof of Concept (PoC) soll untersucht werden, ob die SCION-Technologie den Anforderungen vom Kommando Cyber in Bezug auf Leistung, Flexibilität, Integrität, Verfügbarkeit und Sicherheit genügt.

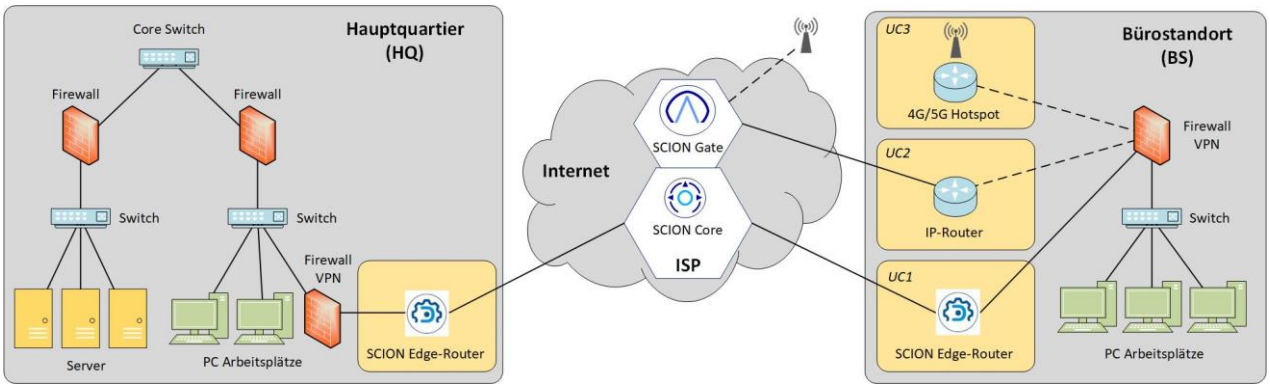

Abbildung 2: Laboraufbau (PoC)

Das Schema in Abbildung 2 gibt eine Übersicht über den Laboraufbau des PoC. Die Erschliessung eines Bürostandorts kann über eine der drei dargestellten Anwendungsfälle sog. Use Cases (UC) erfolgen welche in Tabelle 1 beschrieben sind.

Variante	Anwendung	Funktion
UC1	Permanenter Bürostandort mit bis zu 10 Arbeitsplätzen über SCION Edge Router	Der SCION Edge ist eine Appliance auf einem kabelgebundenen Router und dient als Zugangspunkt zum isolierten Internetverkehr zwischen Unternehmensstandorten in einer bestimmten SCION Isolation Domain (ISD) [6]. Dieser kann entweder vom Unternehmen selbst betrieben, oder vom ISP als Managed Service in Anspruch genommen werden [7].
UC2	Mobile temporäre Arbeitsplätze mit kabelgebundenen Internetrouter via SCION Gate	Das SCION Gate dient zur Anbindung von Aussen-stellen, Partnerorganisationen und Mitarbeitenden im Home-Office ins ISD-Ökosystem. Es ist ein Gateway im Netzwerk eines ISP welches externe Benutzer an Remote-Arbeitsplätzen in das SCION-Netzwerk einbindet [6]. Die Datenpakete werden in einem IP-in-SCION Tunnel gekapselt und übermittelt.
UC3	Mobile temporäre Arbeitsplätze über 4G/5G Hotspot via SCION Gate	Gleich wie UC2, jedoch erfolgt die Verbindung der Aussenstelle über einen 4G/5G Hotspot anstatt eines kabelgebundenen IP-Routers.

Tabelle 1: SCION PoC Anwendungsfälle

2.1 Ziele

Die vorliegende Arbeit befasst sich mit möglichen Angriffsvektoren auf die SCION-Infrastruktur (vgl. Tabelle 1). Dabei werden SCION Edge-Router, SCION Gate und SCION Core betrachtet. Zudem wird untersucht, ob die Kommunikationswege des SCION Protokolls und die SCION Infrastruktur mit konventionellen Methoden aus dem Internet unsichtbar sind und ob es Möglichkeiten gibt, die Pfade sichtbar und angreifbar zu machen. Weiter werden Aspekte des Betriebs der SCION Infrastruktur wie Verfügbarkeit und Sicherheit untersucht. Daraus soll ein Vorschlag für einen Aufbau einer SCION Architektur für das Kommando Cyber erarbeitet werden.

Nr.	Beschreibung	Resultat
1	Eruieren möglicher Angriffsvektoren auf die SCION Infrastruktur aus UC1	Die Angriffsvektoren sind bekannt, beschrieben und bewertet
2	Eruieren möglicher Angriffsvektoren auf die SCION Infrastruktur aus UC2	Die Angriffsvektoren sind bekannt, beschrieben und bewertet
3	Eruieren möglicher Angriffsvektoren auf die SCION Infrastruktur aus UC3	Die Angriffsvektoren sind bekannt, beschrieben und bewertet
4	Untersuchung der Sicherheit der Kommunikationswege im Internet in UC1	Aufzeigen der Sichtbarkeit der Routinginformationen und Metadaten in SCION-Paketen
5	Untersuchung der Sicherheit der Kommunikationswege im Internet in UC2	Aufzeigen der Sichtbarkeit der Routinginformationen und Metadaten in SCION-Paketen

Nr.	Beschreibung	Resultat
6	Untersuchung der Sicherheit der Kommunikationswege im Internet in UC3	Aufzeigen der Sichtbarkeit der Routinginformationen und Metadaten in SCION-Paketen
7	Die SCION-Architektur muss folgende Anforderungen erfüllen: • Datenpakete dürfen die Schweiz nicht verlassen • Die Infrastruktur darf aus dem Internet nicht sichtbar sein • Die SCION Dienste müssen redundant sein	Vorschlag einer SCION-Architektur mit Aufbau einer Trust Root Configuration (TRC) und redundanten Kommunikationskanälen

Tabelle 2: Projektziele

Erkenntnisse aus den Labortests und aus Diskussionen mit Experten sollen in die in die Arbeit einfliessen und für den Aufbau einer möglichen SCION Architektur für das Kommando Cyber berücksichtigt werden. Dabei werden Gespräche mit Experten der Firma Anapaya, der ETH Zürich, von armasuisse W+T und weiteren Bereichen der Bundesverwaltung, internen Experten vom Kommando Cyber, sowie den Betreibern des Swiss Secure Finance Networks (SSFN), bestehend aus dem Finanzdienstleister SIX und der Schweizerischen Nationalbank (SNB) geführt.

2.2 Einschränkungen

Zum Zeitpunkt der Durchführung dieser Arbeit stand das Labor für den PoC nicht bereit. Aus diesem Grund wurde auf das SCION Labor vom Cyber-Defence Campus von armasuisse Wissenschaft und Technologie (armasuisse W+T) ausgewichen. Der Laboraufbau im Cyber-Defence Campus entspricht nicht eins zu eins dem Aufbau des PoC in UC1 (vgl. Kapitel 5.3.6.1). Der Unterschied besteht darin, dass der Datenverkehr im Labor vom Cyber-Defence Campus durch zwei ISD (inter-ISD) geroutet wird und dann das SCION-Netzwerk ins Internet verlässt. Zudem existieren im Laboraufbau keine Firewalls als VPN-Endknoten, welche die IP-Adressen der kommunizierenden Endsysteme im privaten Netz vom Internet verbergen. Trotzdem kann mit dem Testaufbau in Abbildung 11 die Kommunikation innerhalb der ISD zwischen SCION Edge-Router und SCION Core mitgeschnitten und ausgewertet werden.

Mit der zur Verfügung stehenden SCION-Infrastruktur im Labor vom Cyber-Defence Campus kann UC2 nicht getestet werden. Deshalb richtet sich der Fokus im Labor auf die Fälle 1 und 4 (vgl. Tabelle 2). Die anderen Fälle werden theoretisch betrachtet.

2.3 Abgrenzung

SCION bietet viele Möglichkeiten zum Aufbau einer Architektur. Die vorliegende Arbeit betrachtet nur Aspekte, welche für die vorliegenden Anwendungsfälle des PoC von Nutzen sind.

Der Fokus dieser Arbeit liegt auf UC1 und UC2 (s. Abbildung 2). UC3 wird nur am Rande betrachtet, da dies gemäss Aussagen von Anapaya zusätzliche Schwachstellenanalysen in der Mobilfunkübertragung erfordert, welche den Rahmen der vorliegenden Arbeit sprengen würde.

SCION bietet keine Verschlüsselung der Nutzdaten (Payload). Die Verschlüsselung des Inhalts von Nachrichten wird in dieser Arbeit nicht betrachtet und es wird auf bestehende Lösungen in der Bundesverwaltung verwiesen.

3 Grundsätzliches

Zum Verständnis der beschriebenen Technologien und Modelle in dieser Arbeit, werden in diesem Kapitel das Border Gateway Protokoll (BGP) und das OSI-Referenzmodell kurz erklärt.

3.1 Border Gateway Protokoll (BGP)

Das Internet ist ein weltweites Netzwerk, welches aus vielen Netzen besteht. Jeder klassische ISP besitzt ein oder mehrere autonome Netzwerke (AS), welche über BGP-Edge-Router Daten mit anderen AS austauschen. Wie in Kapitel 1 erwähnt, ist das Border Gateway Protokoll eine Grundlage für die heutige Internetkommunikation. BGP ist ein Routingprotokoll, welches unterschiedliche AS miteinander verbindet und für das Routing der Daten über die AS-Grenzen im Internet sorgt [8].

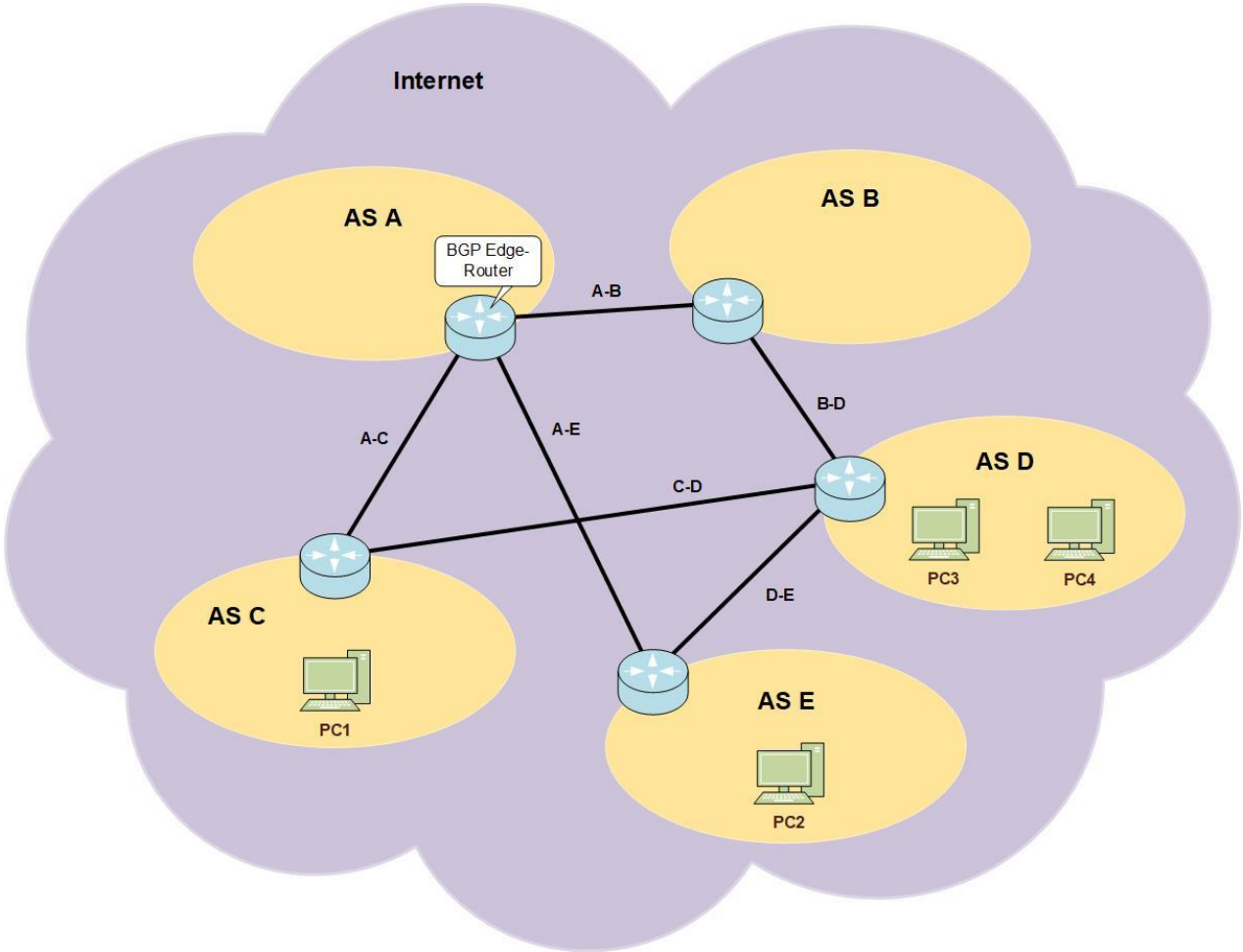

Abbildung 3: BGP-Netzwerk

BGP ist ein Pfadvektor-basiertes Protokoll. Die BGP-Edge-Router tauschen untereinander Routinginformationen aus, so dass jeder Router weiss über welche Pfade, sog. Hops, ein anderes AS zu erreichen ist. Dabei spielen Metriken wie Kosten und Pfadlänge eine Rolle, über welche ein Datenpaket vom Quell-AS zum Ziel-AS gelangt. Kommuniziert z.B. PC1 mit PC2, können die Datenpakete von AS C entweder über den Pfad A-C und A-E, oder von C-D und D-E zu AS E an PC2 geschickt werden (vgl. Abbildung 3). Welchen Pfad die Datenpakete nehmen, hängt von den definierten Metriken ab, welche in den Edge-Routern

hinterlegt sind. Das Quell-AS hat nur die Pfadkontrolle über den ersten Hop. Fällt eine Verbindung zwischen zwei AS aus, werden die Datenpakete über eine alternative Route vom Quell-AS zum Ziel-AS weitergeleitet. Ein Datenpaket nimmt immer den günstigsten und kürzesten Pfad. Bei einer Kommunikation innerhalb eines AS, wie z.B. zwischen PC3 und PC4 verlassen die Datenpakete das Netzwerk von AS D nicht, sondern werden über ein internes Routingprotokoll im eigenen Netzwerk weitergeleitet.
BGP ist für maximale Skalierbarkeit und hohe Zuverlässigkeit optimiert. Die Konfiguration ist aufwendig und Veränderungen von Verbindungswegen konvergieren mit BGP relativ langsam. Die aktuell verwendete Version des Protokolls ist BGPv4.

3.2 OSI-Referenzmodell

Zu Beginn der 1970er Jahre entstanden viele herstellerspezifische Datennetzwerke mit eigenen Protokollen, welche zum Datenaustausch mit Systemen anderer Hersteller inkompatibel waren. Die Unternehmen, welche diese Systeme und Netzwerke einsetzten, wollten jedoch immer häufiger und grössere Mengen an Daten mit Systemen anderer Herstellern austauschen und nicht an einzelne Hersteller gebunden sein. Um diesem Umstand entgegenzuwirken, schaffte die International Standardisation Organisation (ISO) das OSI-Referenzmodell (OSI: Open System Interconnect). Dieses Modell unterteilt die Datenkommunikation in 7 Abstraktionsebenen (vgl. Abbildung 4) [9].

Schicht 7	**Anwendungsschicht**	**(Application Layer)**
Schicht 6	**Darstellungsschicht**	**(Presentation Layer)**
Schicht 5	**Sitzungsschicht**	**(Session Layer)**
Schicht 4	**Transportschicht**	**(Transport Layer)**
Schicht 3	**Netzwerkschicht**	**(Network Layer)**
Schicht 2	**Datensicherungsschicht**	**(Data Link Layer)**
Schicht 1	**Physikalische Schicht**	**(Physical Layer)**

Abbildung 4: OSI-Referenzmodell [9]

Mit Hilfe des OSI-Modells wird jedes Problem der Kommunikation in einem System in verschiedene Teilprobleme aufgeteilt und abstrahiert. Jeder Schicht sind spezifische Teile einer Datenkommunikation zugeordnet. Alle Kommunikationssysteme werden nach denselben Regeln unterteilt und funktionieren auf allen Stufen identisch wie andere Systeme auf der Gegenseite.

Jede Schicht im OSI-Modell bearbeitet auf der Sendeseite ein Teilproblem einer Kommunikation und übergibt die nächste Aufgabe der darunterliegenden Ebene (vgl. Abbildung 5). Auf der Empfangsseite bearbeitet das System das Teilproblem auf derselben Schicht und übergibt für die Abarbeitung der Kommunikation an die nächsthöhere Schicht.

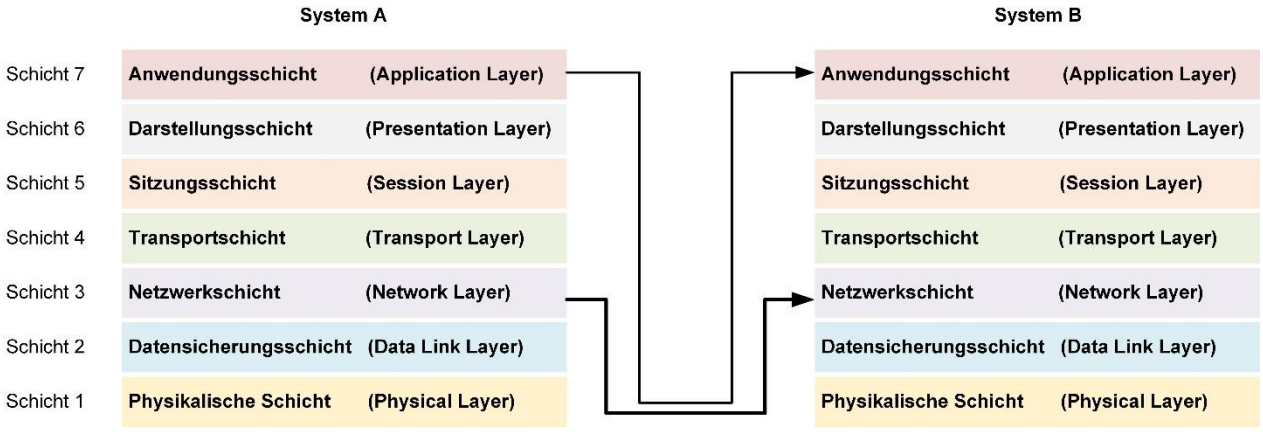

Abbildung 5: Funktion OSI-Modell

Mit dem OSI-Modell als Basis kann eine herstellerübergreifende Kommunikation gewährleistet werden.

4 SCION im Überblick

Damit Entscheidungen und Schlussfolgerungen in dieser Arbeit nachvollzogen werden können, ist das Verständnis der Grundprinzipien der SCION-Internetarchitektur erforderlich. Diese sind im Kapitel 4 beschrieben.

Das Ziel von SCION ist es, Datenpakete sicher, kontrolliert und effizient zwischen Domänen im Internet (AS) zu übertragen, ohne dass dabei die Kommunikationspfade manipuliert werden können [5].

Das SCION Protokoll ist in drei Ebenen unterteilt (vgl. Tabelle 3):

Ebene	Funktion
Isolation Domain (ISD)	• Gruppierung unabhängiger Autonomer Systeme (AS) in ISDs mit gemeinsamem Vertrauensbereich, welcher in der Trust Root Configuration (TRC) hierarchisch definiert wird (vgl. Abbildung 6)
Control Plane (CP)	• Verantwortlich für 'Routing und Discovering' von Pfadsegmenten • Zwei Routingebenen, inter-ISD für das Routing zwischen ISDs und intra-ISD für das Routing innerhalb einer ISD (vgl. Abbildung 6) • Pfadinformationen sind kryptografisch integritätsgeschützt • Pfadsegmente sind in der Pfaddatenbank der ISD registriert
Data Plane (DP)	• Transport von Datenpaketen auf definierten Pfaden • Kombiniert Pfadsegmente zu End-to-End Pfaden • Datenpaket beinhaltet Pfadinformationen und Payload • Weiterleitung ist kryptografisch integritätsgeschützt • SCION Router leitet Pakete anhand der AS-Pfadinformationen im Header weiter

Tabelle 3: Funktionsbereiche SCION Protokoll [10]

4.1 Isolation Domain (ISD)

Eine ISD ist eine logische Gruppierung von AS, welche eine Einheit unabhängiger Routingebenen bildet (Abbildung 6). Eine ISD besteht aus Core AS und non Core AS. Sie kann in sich isoliert sein, oder Verbindungen zu anderen ISDs haben. Die Core AS bilden die Trust Root Configuration (TRC) (vgl. Abbildung 6, AS A und AS B), welcher alle AS einer ISD vertrauen und von welcher sie die Zertifikate erhalten (s. Kapitel 4.2.1). Die Core AS verwalten die Konnektivität zu anderen ISDs und bilden den Vertrauensbereich für alle AS in der eigenen ISD. Ein AS kann auch Mitglied von mehreren ISDs sein (vgl. Abbildung 6, AS N und AS P) [5].

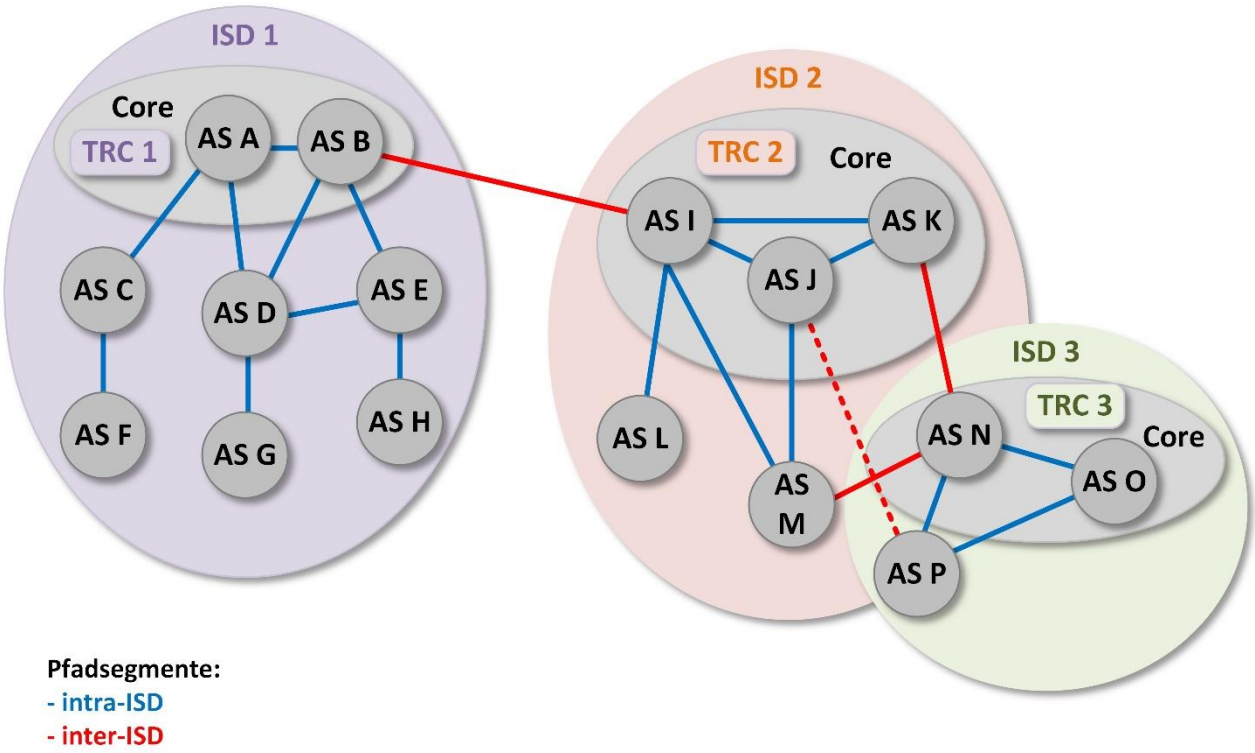

Abbildung 6: SCION Isolation Domain [10]

«*ISDs dienen den folgenden Zwecken:*

- *Sie ermöglichen SCION die Unterstützung von Vertrauensheterogenität, da jede ISD ihre Vertrauenswurzeln (TRC) unabhängig definieren kann.*
- *Sie bieten Transparenz für Vertrauensbeziehungen*
- *Sie isolieren den Routing-Prozess innerhalb einer ISD von externen Einflüssen wie Angriffen und Fehlkonfigurationen*
- *Sie verbessern die Skalierbarkeit des Routing-Protokolls, indem sie dieses in einen intra- und einen inter-ISD Teil trennen*» [5]

SCION Core Betreiber sind (meistens) ISP, welche nebst den herkömmlichen Internetservices SCION-Dienste mit ihren autonomen Netzwerken (AS) anbieten [11].

4.2 Control Plane (CP)

Die Control Plane (CP) ist für die Erkennung von Pfadsegmenten und deren Bereitstellung für die Endpunkte in einer ISD verantwortlich. Als Kontrollebene beinhaltet sie die Control Plane Public Key Infrastructure (CP-PKI), welche das kryptografische Material einer ISD ausstellt und verwaltet. Die CP-PKI bildet die Grundlage für die Authentifizierungsverfahren in SCION. Sie dient zum Authentifizieren und Verifizieren von Pfadinformationen in einer ISD [12].

4.2.1 Trust Root Configuration (TRC)

Das Vertrauensverhältnis einer ISD ist über die TRC hierarchisch definiert. Jede ISD besitzt eine eigene TRC. Diese wird von den Core AS gebildet, welche die öffentlichen Schlüssel (Public Keys) für die ISD ausstellen, verwalten und für die Richtlinien (Policies) zuständig sind. Die TRC ist verantwortlich für die Sammlung von X.509 v3 Zertifikaten in der ISD. Jede Version der TRC muss von den dafür bestimmten (Quorum-) AS signiert werden, so dass Aktualisierungen gegenüber Vorgängerversionen validiert werden können [10].

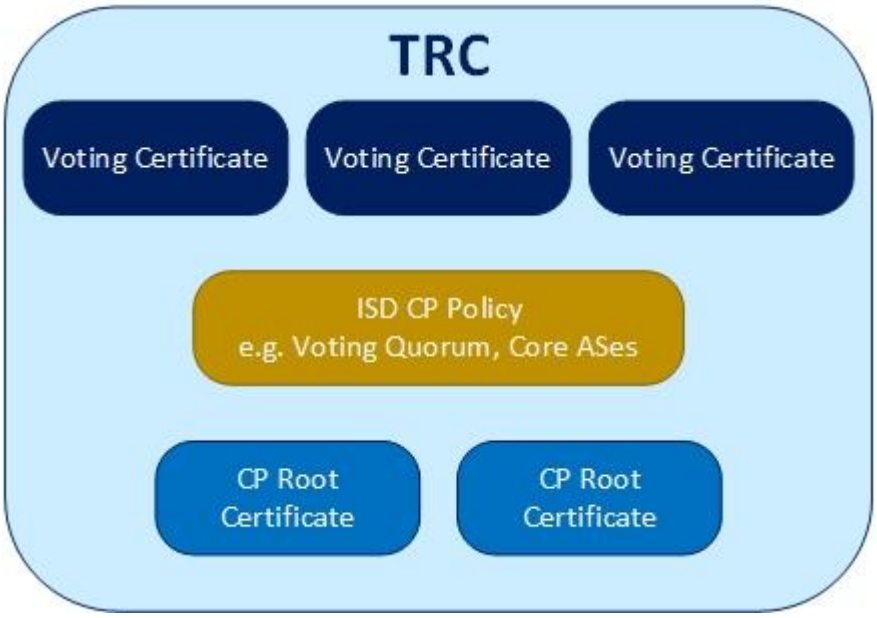

Abbildung 7: Trust Root Configuration (TRC) [10]

Wie am Anfang des Kapitels 4.2 erwähnt, beinhaltet die TRC die CP-PKI und stellt die Public Keys für die Authentifizierung von SCION Routingpfaden in der ISD zur Verfügung. Jedes AS signiert seine Pfade mit seinem privaten Schlüssel aus dem CP-Root Zertifikat. Die anderen AS in der ISD verifizieren die Signatur mit dem öffentlichen Schlüssel des publizierenden AS [12].

4.3 AS-Rollen in einer TRC

Ein AS kann in einer SCION ISD mehrere der in den Kapiteln 4.3.1 bis 4.3.4 beschriebenen Rollen haben.

4.3.1 Core Member

Die Core Member (Core AS) sind AS, welche die Netzwerkverbindungen zu anderen Providern und zu ihren Kunden innerhalb einer ISD ermöglichen. Diese bieten Ihre Dienstleistungen im Sinne eines klassischen ISP an [12]. Sämtliche Pfadsegmente, intra- oder inter-ISD starten von den Core Member aus.

4.3.2 Voting Member

Die Aufgabe der Voting Member ist das Erstellen und Aktualisieren der TRC. Dabei existieren zwei unterschiedliche TRC-Update-Schlüssel. Die Regular-TRC-Updates werden über Online-Keys automatisch verteilt. Diese beinhalten unsensible Informationen wie z.B. Verlängerung der Gültigkeitsdauer. Sensitive-TRC-Updates kommen eher selten vor und können nur manuell über Offline-Keys verteilt werden. Mit diesen können Voting Member, Voting Quorum oder die Root Zertifikate angepasst werden. Die Keys der Root Zertifikate müssen sicher aufbewahrt werden. Die Anzahl AS eines Voting Quorums sollte immer grösser als 1 sein, um böswillige TRC-Aktualisierungen zu verhindern [12].

4.3.3 Issuing Member

Die Issuing Member, oder auch Certificate Authorities (CA) sind für die Ausstellung der AS-Zertifikate innerhalb einer ISD verantwortlich. Die AS-Zertifikate dienen der Authentifizierung der Netzwerkteilnehmer und der Verifizierung der Routingpfad- und Netzwerkinformationen. Soll ein neues AS als Mitglied in eine ISD aufgenommen werden, muss dieses zur Ausstellung eines AS-Zertifikats einen Zulassungsprozess durchlaufen [12].

4.3.4 Authoritative Member

Authoritative Member AS besitzen immer die aktuellen TRCs. Von denen erfolgen die Ankündigungen einer TRC-Aktualisierung. Aus Verfügbarkeitsgründen muss ein authoritatives Mitglied auch ein Core AS sein [12].

4.4 Data Plane (DP)

Die Data Plane (DP) ist verantwortlich für die Paketweiterleitung über den ausgewählten Pfad. Die SCION-Border-Router leiten die Pakete anhand dem AS-Level-Pfad an das nächste AS weiter, ohne die Zieladresse zu prüfen oder die Inter-Domain-Weiterleitungstabelle abzufragen. Erst der Border-Router vom Ziel-AS prüft die Zieladresse und leitet die Datenpakete an den lokalen Endpunkt weiter [13].

4.5 ISD-AS Nummerierung

Zur Identifizierung besitzen sämtliche SCION AS eine global eindeutige ISD-AS Nummer. In Tabelle 4 sind die Wertebereiche der ISD-Nummer und der AS-Nummer aufgeführt.

ISD-Nummer	AS-Nummer	Wertebereich
Bereich von 0 bis 2^{16}-1	Global eindeutige Nummer:	0 bis 2^{48}-1
Speziell reservierte Werte wie 0 für Wildcard ISD	• entweder AS-Nummer aus der BGP-Welt	0 bis 2^{32}-1
Öffentliche ISD-Nummer muss eindeutig sein	• oder AS-Nummer aus dem SCION Universum	2^{32} bis 2^{48}-1

Tabelle 4: Wertebereich SCION ISD-AS Nummerierung

Wie sich die ISD-AS-Nummer zusammensetzt, ist in Abbildung 8 illustriert. Existiert für ein AS bereits eine AS-Nummer aus der BGP-Welt, behält dieses auch im SCION-Universum seine Nummer. Falls für ein Netz eines SCION-Teilnehmers ein neues AS erstellt wird, erhält dieses eine AS-Nummer aus dem SCION-Universum nach IPv6 Notation (vgl. Tabelle 4) [10].

Abbildung 8: Beispiel SCION ISD-AS Nummerierung [10]

Wie im Beispiel in Abbildung 8 ersichtlich ist, besitzt die Swiss Isolation Domain die ISD-Nummer 64. Die Swiss ISD besteht aus mehreren Schweizer ISPs und wird laufend grösser. Eine Auflistung der teilnehmenden Parteien ist unter folgendem Link ersichtlich https://www.scion.org/scion [14].

5 Angriffsvektoren

Dieses Kapitel befasst sich mit den möglichen Schwachstellen im PoC, welche zusammen mit Experten aus verschiedenen Bereichen der Bundesverwaltung gefunden wurden.

5.1 Terminologie

Ein Angriffsvektor bezeichnet jedes Mittel, mit welchem ein Angriff auf eine IT-Umgebung erfolgen kann. Eine Angriffsfläche bezeichnet die Verwundbarkeit, die diese Vektoren schaffen. Sämtliche Punkte, über welche Daten in oder aus einer Anwendung oder einem Netzwerk gelangen können, sind potenzielle Angriffsvektoren. Identitäten, Netzwerke, E-Mails, Lieferketten und externe Datenquellen wie Wechselmedien und Cloud-Systeme können von einem böswilligen Akteur als Kanäle dienen, um an sensible Daten zu gelangen und diese zu gefährden. Auch jede Systemaktualisierung und Systemfreigabe kann neue Angriffsvektoren schaffen [15].

5.2 Angriffsmodell

Um im betrachteten PoC einen Angriff starten zu können, muss eine angreifende Person über Insiderwissen zum privaten SCION-Netzwerk verfügen. Die SCION-Infrastruktur ist ausserhalb der SCION-ISD, d.h. vom Internet nicht sichtbar. Deshalb muss sich die Infrastruktur für einen Angriff im Fall von UC1 innerhalb der ISD befinden. Bei UC2 und UC3 sind konventionelle Attacken auf die Internetinfrastruktur oder die Kommunikationswege zwischen IP-Router oder 4G/5G Hostspot bis zum SCION Gate möglich.

Ein passiver Angriff kann durch Mitlesen des Datenverkehrs (Packet Sniffing) in der ISD erfolgen (vgl. Kapitel 5.3.6.1). Auch aktive Angriffe auf das SCION-Protokoll (Protocol Injection) sind mit dieser Methode theoretisch möglich.

Die eingesetzte Hardware, Software und das Betriebssystem, auf welchem die SCION-Dienste laufen, birgt Gefahren durch Schwachstellen, welche durch Infizierung von SCION-Hosts und -Gateways ausgenutzt werden könnten.
Eine Infizierung mit Schadsoftware kann auch über das Netzwerkmanagement der SCION-Infrastruktur erfolgen.

Eine angreifende Partei kann versuchen, sich als legitimes SCION-AS auszuweisen (AS Spoofing oder Route-Hijacking). Dabei wären auch DDoS-Attacken auf die SCION-Infrastruktur möglich.

Sowohl Hersteller von SCION-Netzwerkinfrastruktur als auch externe Betreiber von SCION-Diensten müssen als potenzielle Quellen betrachtet werden, von welchen Angriffe erfolgen können.

Die Hardware aus den konventionellen IP-Netzen wie Internet-Router oder 4G/5G Hotspots kann Schwachstellen aufweisen und als Angriffspunkt benutzt werden.

5.3 Angriffsvektoren im PoC

Wie jedes IT-System birgt auch SCION im betrachteten PoC potenzielle Risiken für Cyberangriffe. Durch Kenntnis der potenziellen Angriffsvektoren und Einhaltung von Vorgaben und Empfehlungen, bzw. schliessen von Sicherheitslücken, kann die Angriffsfläche auf ein System minimiert werden. Als Leitfaden zur Cybersicherheit können 'best practices' z.B. vom Bundesamt für Sicherheit in der Informationstechnik (BSI) oder vom National Institute of Standards and Technology (NIST) zu Hilfe genommen werden.

In Abbildung 9 sind die Angriffsvektoren aufgeführt, welche in der SCION-Architektur für den PoC ermittelt wurden. Auf eine Analyse der Angriffsvektoren im privaten Netz hinter den Firewalls wird verzichtet, da der Fokus dieser Arbeit auf der SCION-Architektur liegt. Diese können nach 'best practices' Methoden zum Schutz von privaten IP-Netzwerken ermittelt und die dafür notwendigen Massnahmen umgesetzt werden.
Die Angriffsvektoren des SCION Edge-Routers im Hauptquartier sind dieselben wie am Bürostandort. Aus diesem Grund wird auf diese nicht separat eingegangen.

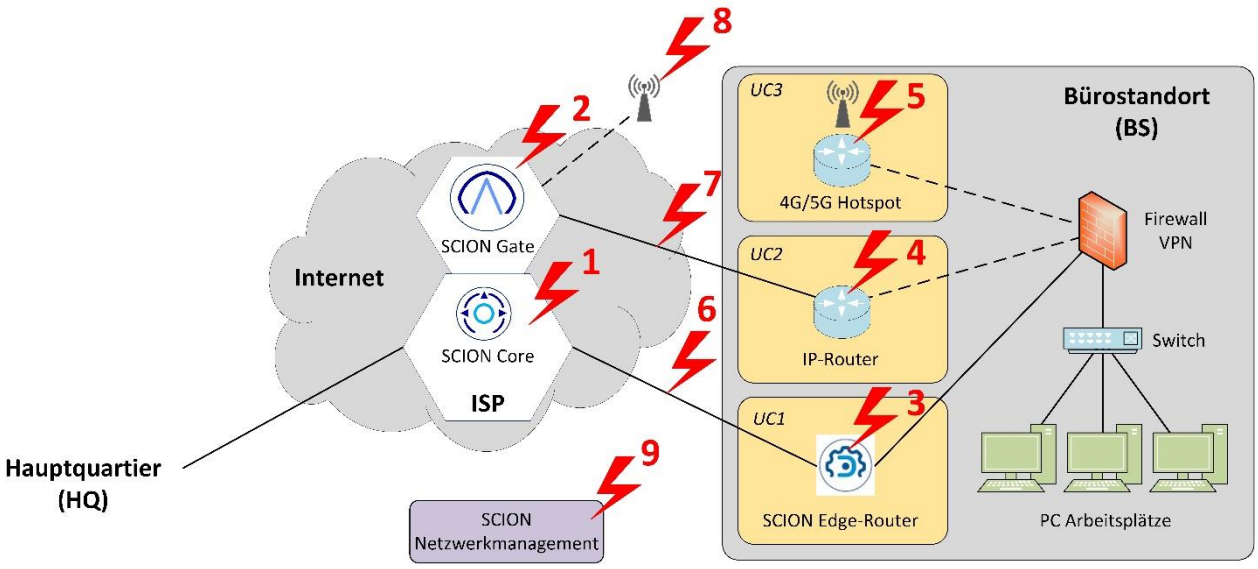

Abbildung 9: Angriffsvektoren im PoC

Aus Erfahrungswerten und Diskussionen mit Experten vom Kdo Cy und armasuisse W+T ergeben sich folgende Angriffsvektoren der verschiedenen Komponenten und Kommunikationspfaden in der SCION-Architektur (vgl. Abbildung 9). In Tabelle 5 sind die potenziellen Angriffsvektoren aufgelistet. Diese sind in Kapitel 5.3.1 bis 5.3.9 beschrieben. Die Schutzmassnahmen der SCION-Infrastruktur (Nr. 1-5 in Tabelle 5) werden in Kapitel 7 behandelt.

Nr.	Komponente/Pfad	Angriffsvektor
1	SCION Core	• Hardware/Firmware • Betriebssystem • PKI
2	SCION Gate	• Hardware/Firmware • Betriebssystem • PKI
3	SCION Edge Router	• Hardware/Firmware • Betriebssystem • PKI
4	IP-Router	• Hardware/Firmware • Betriebssystem
5	Mobile IP-Router	• Hardware • Firmware/Betriebssystem
6	Verbindung SCION Edge – SCION Edge	• Mitlesen oder modifizieren des Netzwerkverkehrs WAN-seitig (‘packet sniffing und packet spoofing’) (vgl. Kapitel 5.3.6)
7	Verbindung IP-Router – SCION Gate	• Mitlesen oder modifizieren des Netzwerkverkehrs WAN-seitig (‘packet sniffing und packet spoofing’) • Kryptografisch ungeschützter Pfad zwischen IP-Router bis zum SCION Gate (vgl. Kapitel 5.3.7)
8	Verbindung Mobile IP-Router – SCION Gate	• Mitlesen oder modifizieren des Netzwerkverkehrs WAN-seitig über die Luftschnittstelle (‘packet sniffing und packet spoofing’) • Kryptografisch ungeschützter Pfad zwischen IP-Router bis zum SCION Gate (vgl. Kapitel 5.3.8)
9	SCION Netzwerkmanagement	• Manipulation oder Fehlkonfigurationen der Routingpfade • Einschleusen manipulierter Software/Firmware

Tabelle 5: Angriffsvektoren in der SCION-Architektur

5.3.1 SCION Hardware und Firmware

Die SCION Services können sowohl auf dedizierter Hardware als auch in virtuellen Umgebungen installiert werden. Veraltete Hardware oder Firmware können Schwachstellen haben, welche für Cyberangriffe ausgenutzt werden können. Wie in Tabelle 5 ersichtlich ist, gelten diese Angriffspunkte für SCION Core, Edge, und Gate.

5.3.2 Betriebssystem

Die SCION Services laufen auf einem Linux-basierten Betriebssystem, entweder Ubuntu oder RedHat. Gemäss Empfehlungen der SCION Architecture wird empfohlen Ubuntu einzusetzen [16]. Wie jedes Betriebssystem, birgt auch dieses Risiken für Cyberangriffe durch Schwachstellen. Daher muss das Betriebssystem auf einem aktuellen Stand gehalten werden. Werden Sicherheitslücken im Betriebssystem entdeckt, müssen diese geschlossen werden. Die Dringlichkeit hängt von der Kritikalität der Sicherheitslücke und der Verfügbarkeit der Bugfixes ab. Dies gilt für alle SCION-Netzwerkkomponenten wie Core, Edge und Gate.

5.3.3 SCION Public Key Infrastruktur (PKI)

Die SCION-PKI ist ein zentraler Faktor der gesamten SCION Vertrauensstruktur. Je nach Hierarchiestufe in der TRC kann eine Kompromittierung des kryptografischen Materials einen grösseren oder kleineren Schaden in der Vertrauensstellung einer ISD bewirken. Ein kompromittierter privater Schlüssel eines Member AS beschränkt sich auf die Pfade, welche von oder zu diesem AS führen. Eine Kompromittierung eines Core- oder Voting-AS hat Auswirkungen auf die gesamte ISD oder über die Grenzen der ISD hinaus.
Nebst der Vertrauensstellung kann ein Angriff auf die PKI einer der Core Member auch die Verfügbarkeit der SCION Dienste beeinträchtigen.

5.3.4 IP-Router

Wie bei den SCION-Netzwerkkomponenten ist wichtig, dass die Hardware und Firmware eines IP-Routers und dessen Betriebssystem auf einem aktuellen Stand sind. Ein Kompromittieren der SCION-Routingpfade in der ISD durch einen konventionellen IP-Router ist zwar eher unwahrscheinlich. Wird der Router sowohl für Internetzugriffe wie auch für die Konnektivität zu einem SCION-Netzwerk über den SCION Gate verwendet (UC2), könnte dieser als Einfallstor für kriminelle Aktivitäten innerhalb einer ISD missbraucht werden. Ein Einschleusen z.B. von Ransomware wäre möglich. Weiter könnten auch die Pfade des Internetrouters bis zum SCION Gate manipuliert werden, da diese bis dort nicht durch kryptografische Massnahmen gesichert sind.

5.3.5 4G/5G Hotspot

Beim Einsatz eines 4G/5G Hotspot (UC3) existieren Hardware-, Firmware- und Betriebssystem-seitig dieselben Gefahren wie beim kabelgebundenen Internetrouter. Zusätzlich eröffnet sich über die Luftschnittstelle eine weitere Möglichkeit für einen Angriff.

5.3.6 Verbindung SCION Edge – SCION Edge (UC1)

Die beiden privaten IP-Netze vom Hauptquartier (HQ) und Bürostandort (BS) sind IP-mässig durch einen VPN-Tunnel in der SCION ISD verbunden und die Kommunikation darin verschlüsselt (vgl. Abbildung 10). Die SCION Edge Router übernehmen die Funktion der Gateways (SIG) zwischen den privaten Netzen von Hauptquartier (HQ) und Bürostandort (BS) in das SCION Netz der ISD. SCION bildet das Overlay-Netzwerk über die beiden VPN-Endpunkte. Die Verbindung zwischen den beiden SCION Edge Routern ist in der ISD kryptografisch geschützt. Für eine angreifende Person ist es kaum möglich, die Routingpfade umzuleiten oder eine Man-in-the-Middle Attacke in einer SCION ISD zu machen. Dazu wäre eine Mehrfachkompromittierung der PKI notwendig. Ein Angriff auf die Routingpfade würde schnell bemerkt und es würde keine Kommunikation zwischen den betroffenen Pfaden stattfinden.

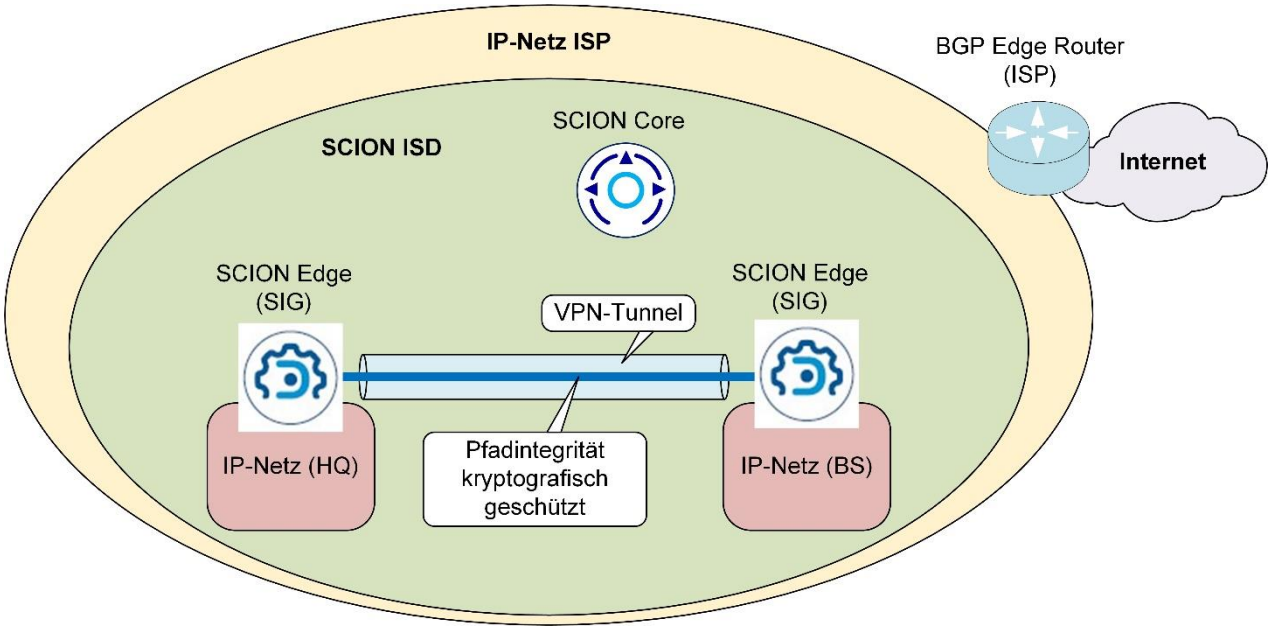

Abbildung 10: Verbindung SCION Edge - SCION Edge (UC1)

WAN-seitig lässt sich ‘Packet Sniffing’ nicht verhindern. Allerdings ist dafür physischer Zugang zu einer Internetleitung zwischen den WAN-Schnittstellen von zwei SCION-Routern (Edge und/oder Core) notwendig. Damit der Datenverkehr zwischen zwei SCION-Routern mitgelesen werden kann, ist die Installation eines Network Test Access Point (TAP) in der Leitung erforderlich. Die Installation eines TAPs in einer aktiven Leitung führt immer zu einem Kommunikationsunterbruch. Ein installierter TAP in einer aktiven Verbindung ist jedoch kaum erkennbar. Der nachfolgende Abschnitt (5.3.6.1 - 5.3.6.3) befasst sich mit der Sichtbarkeit und Anonymität der Kommunikation von UC1 in einer ISD.

5.3.6.1 Testaufbau

Das Mitlesen von Netzwerkverkehr, das sog. 'Packet Sniffing' in Kombination mit Traffic Analyse ist oft Teil der Vorbereitungsarbeiten eines Cyberangriffs. Diese Methode wird verwendet, um an Informationen über Kommunikationsverbindungen, Meta- und Nutzdaten zu gelangen. Da diese Methode einen Eingriff in die Kommunikation zwischen zwei Hosts, z.B. Router erfordert, wird diese mehrheitlich von staatlichen Akteuren angewendet. Für kriminelle Organisationen ist diese Methode eher schwierig umzusetzen, da dies ein physischer Eingriff auf die Infrastruktur eines ISP erfordert.

Um den Netzwerkverkehr innerhalb einer ISD (intra-ISD) oder zwischen zwei ISD (inter-ISD) abhören zu können, muss ein TAP zwischen zwei aktiven Netzwerkkomponenten (Router oder Switch) dazwischengeschaltet werden. Beim passiven Abhören wird mit den Monitoringports des TAP der eingehende und ausgehende Netzwerkverkehr zwischen den beiden Netzwerkgeräten auf ein Analysesystem weitergeleitet und aufgezeichnet. Dabei wird der Datenverkehr nicht beeinträchtigt, da keine Manipulationen an den Routingpfaden oder der Nutzdaten erfolgen.

Für den Abgriff des Netzwerkverkehrs in UC1, ist in der Verbindung zwischen der WAN-Schnittstelle des SCION Edge Routers und SCION Core ein TAP in den Kommunikationspfad dazwischengeschaltet (vgl. Abbildung 11). Mit PC2 wird der Netzwerkverkehr aufgezeichnet.

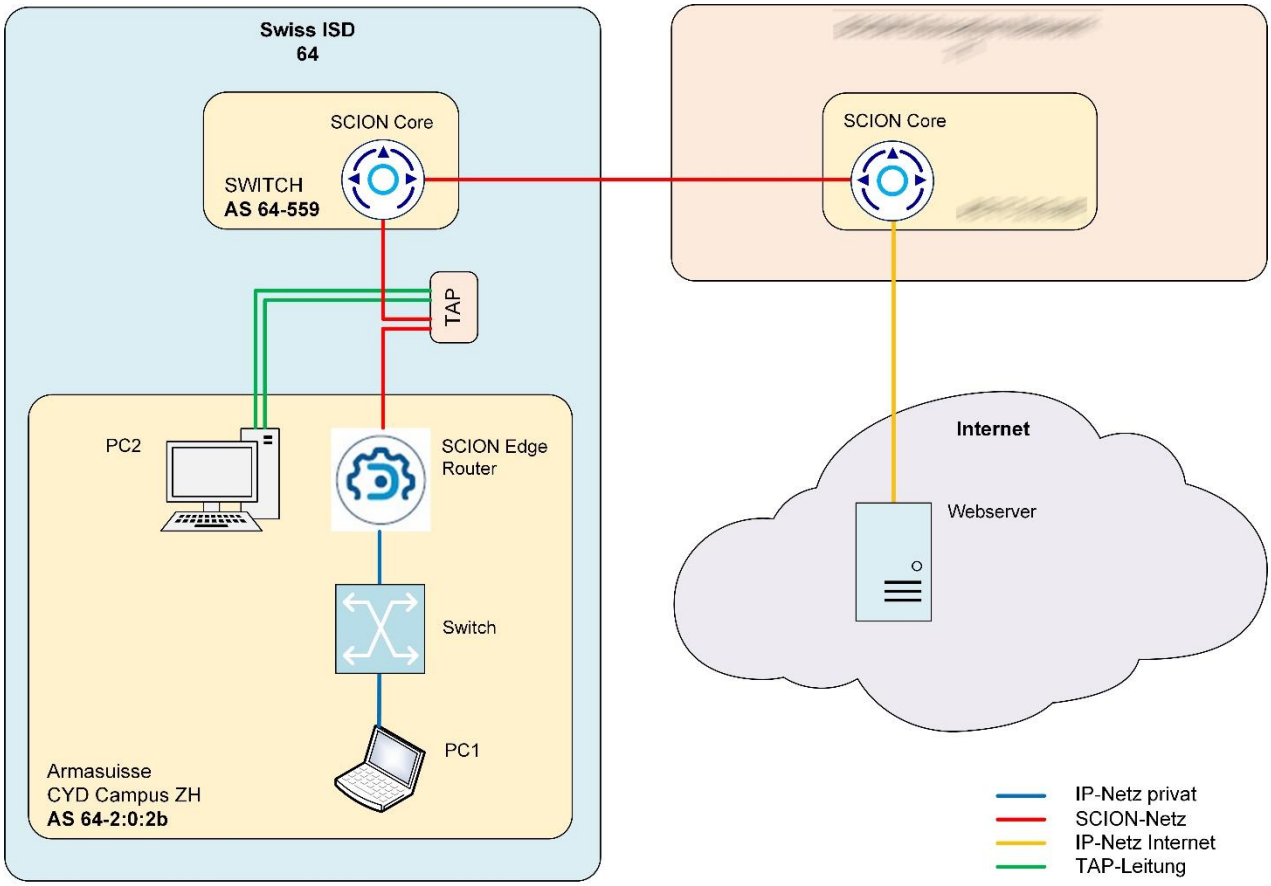

Abbildung 11: Testaufbau UC1

PC1 wird als Last zum Generieren von Netzwerkverkehr verwendet. Der Datenverkehr zwischen PC1 und dem Webserver im Internet wird durch das SCION-Netz von ISD 64 und ISD [redacted] geroutet, bevor dieser aus AS [redacted] ins Internet zum Webserver gelangt.

5.3.6.2 Testvorgehen

Zur Durchführung des Tests ist es sinnvoll, eine Kommunikation zwischen den beiden Endsystemen PC1 und Webserver aufzubauen, über welche viele Datenpakete gesendet werden. Dies vereinfacht die Suche der ausgetauschten Datenpakete in der nachfolgenden Analyse zwischen Sender und Empfänger. Dazu eignet sich z.B. ein Internet Speedcheck.

Zum Generieren der Last wird mit PC1 (private IP-Adresse 192.168.111.12) die Webseite www.speedcheck.org aufgerufen. Die private IP-Adresse ist für die Analyse im Hexdump relevant (vgl. Kapitel 5.3.6.3).

Durch die aufgerufene Applikation auf dem Webserver werden Datenpakete zwischen Webserver und PC1 ausgetauscht, welche mit PC2 aufgezeichnet werden. Nebst den Angaben der durchschnittlichen Latenzzeit, der Up- und Downloadgeschwindigkeit, sind auch Informationen zum ISP wie IP-Adresse und Providername ersichtlich (vgl. Abbildung 12).

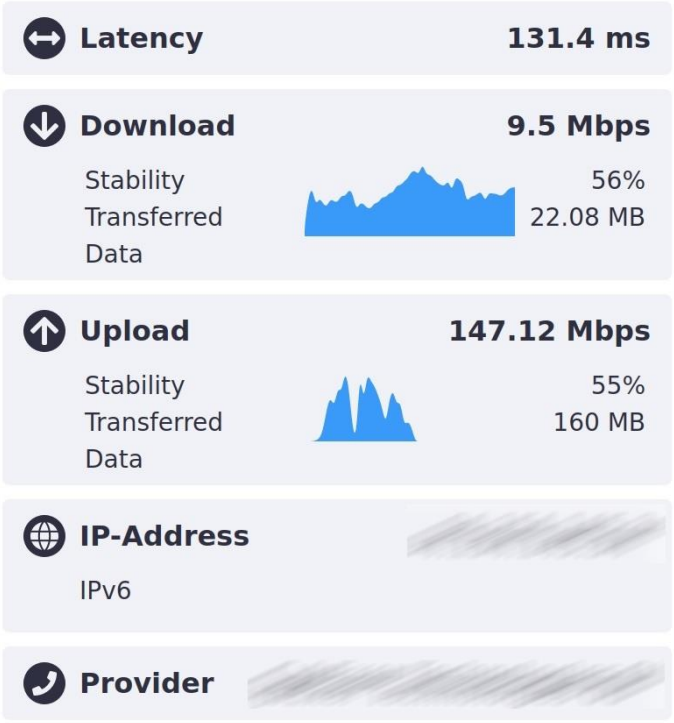

Abbildung 12: Antwort Webserver (UC1)

Der Dienst «*whois*» von RIPE liefert weitere Informationen zum ISP, welcher die Schnittstelle zwischen SCION-Welt und Internet bildet (vgl. Abbildung 13).

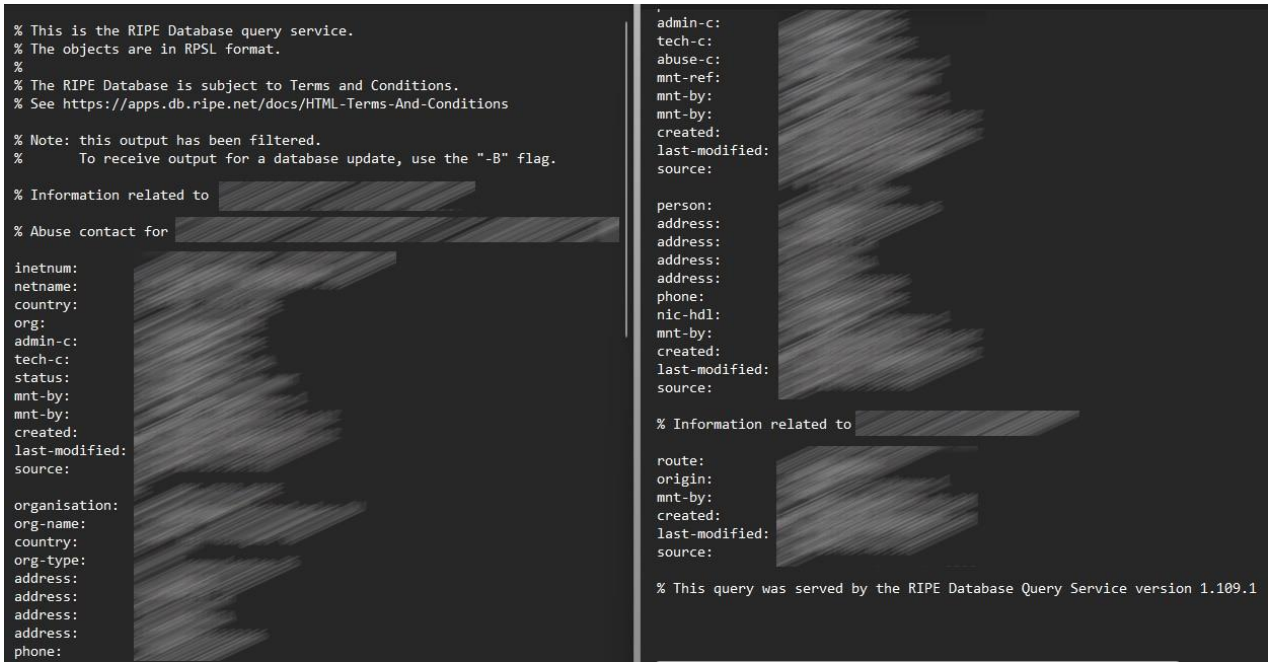

Abbildung 13: Resultat «*whois*» (UC1)

Mit dieser Information und den Ergebnissen aus den Aufzeichnungen in Kapitel 5.3.6.2 ist sichergestellt, dass der generierte Datenverkehr zwischen PC1 und dem Webserver durch das SCION-Netz ins Internet geroutet wird.

5.3.6.3 Testresultat

Um den aufgezeichneten Datenverkehr in Wireshark öffnen zu können, muss das SCION Plugin *scion.lua* installiert werden.

Eine genaue Beschreibung von SCION und Wireshark ist unter folgendem Link ersichtlich: https://docs.scion.org/en/latest/dev/wireshark.html [17].

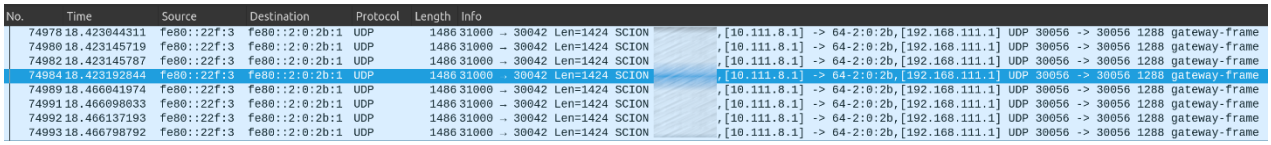

Abbildung 14: Wireshark Paketlistenansicht (UC1)

Der Datenaustausch zwischen den beiden Endsystemen PC1 und Webserver erfolgt über SCION-IP Gateways (SIG). SIG tunneln IP-Pakete durch das SCION Netzwerk. Ein Ingress SIG kapselt IP-Pakete in ein SCION-Paket und sendet dieses an ein Egress SIG. Der SCION Edge Router sendet das Datenpaket gemäss den konfigurierten Routingpfade an den SCION Edge-Router der Gegenstelle durch das SCION Netzwerk. Das Ziel-SIG entkapselt das SCION-Paket und sendet die IP-Pakete an die IP-Adresse des Zielsystems im lokalen Netzwerk [18] (vgl. Abbildung 15). Im Fall von UC1 wird das gekapselte IP-Paket durch das Ziel-SIG entkapselt und über das Internet zum Webserver geschickt.

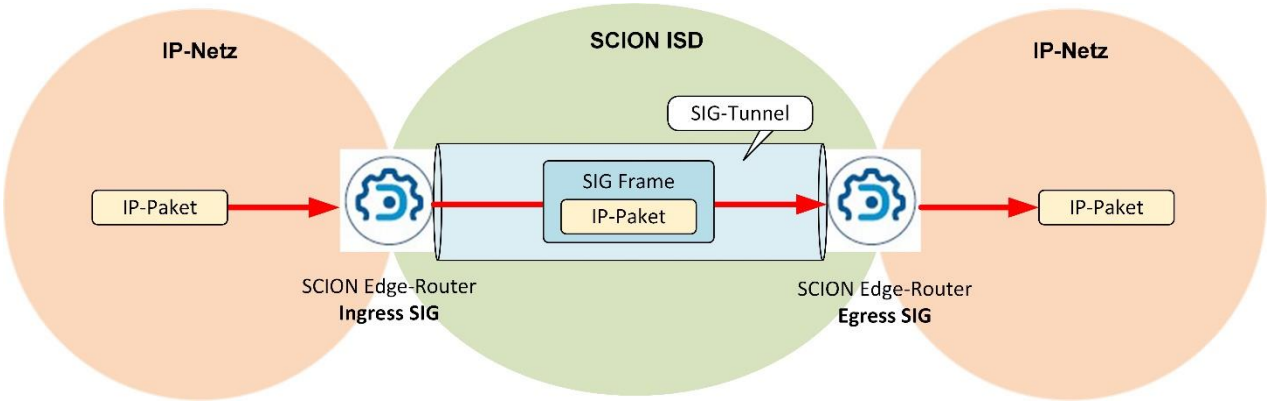

Abbildung 15: IP-Paket durch Ingress- und Egress-SIG

Ein SIG-Frame kann mehrere IP-Pakete enthalten. Ein einzelnes IP-Paket kann auch in mehrere SIG-Frames aufgeteilt sein. Jedes SIG-Frame besitzt eine Sequenznummer. Das Ziel-SIG nutzt die Sequenznummer, um die darin enthaltenen IP-Pakete wieder zusammenzusetzen. SIG-Frames werden über das User Datagram Protocol (UDP) übertragen (vgl. Abbildung 14).

In der Paketlistenansicht (Abbildung 14) sind die beiden ISD und die IP-Adressen der SCION Edge-Router ersichtlich. Die SCION Edge-Router übernehmen im vorliegenden Anwendungsfall auch die Funktion des SIG.

In der Paketdetailansicht (Abbildung 16) ist ein SIG-Frame aus der aufgezeichneten Kommunikation im SCION-Protokoll ersichtlich.

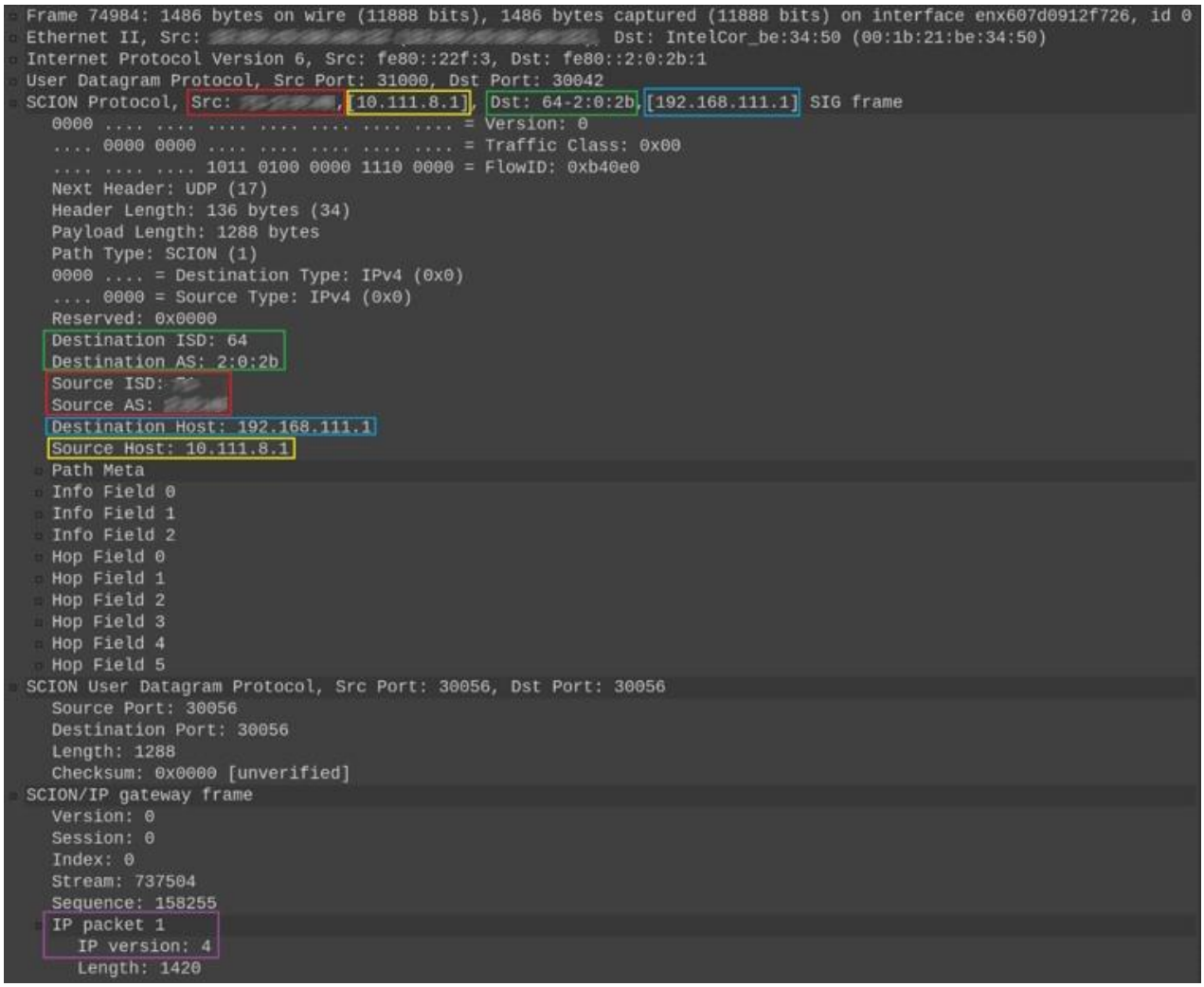

Abbildung 16: Wireshark Paketdetailansicht (UC1)

Im Laboraufbau bilden die beiden SCION Edge-Router (src) 10.111.8.1 und (dst) 192.168.111.1 eine logische Verbindung miteinander. Über diese wird der Datenverkehr der beiden Endsysteme PC1 und Webserver geroutet (vgl. Abbildung 16) [19]. Die Datenpakete werden als SIG-Frames in UDP-Pakete gepackt und als Stream gesendet. Gemäss Tabelle in der SCION Gateway Dokumentation [18] bezeichnet der Port 30056 die ‘underlay data-plane’. Im SCION Protokoll sind Informationen zu Quell- und Ziel-ISD, AS und die IP-Adressen der beiden Edge-Router zu finden.

Wird im Hexdump nach den IP-Adressen der kommunizierenden Endsysteme Webserver (src) und PC1 (dst) gesucht, sind diese im eingekapselten IPv4-Paket vom SIG-Frame im Hexadezimalformat auffindbar (vgl. Abbildung 17).

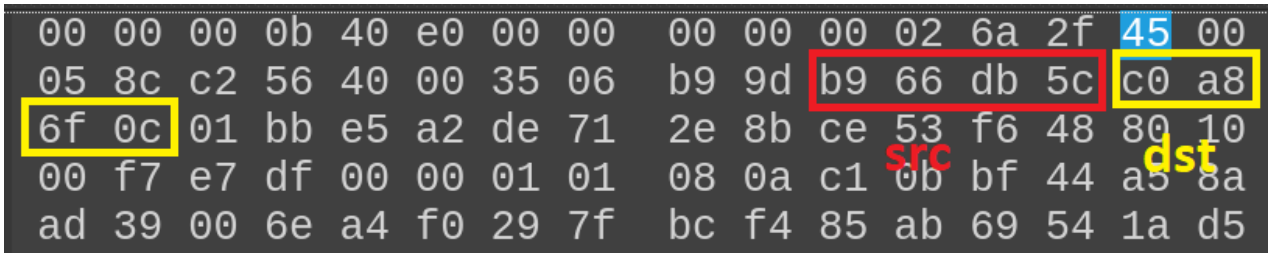

Abbildung 17: Auszug hexdump (UC1)

Umgewandelt vom Hexadezimal- ins Dezimalformat, ergeben sich folgende IP-Adressen:

Webserver (src): b9:66:db:5c -> 185.102.219.92
PC1 (dst): c0:a8:6f:0c -> 192.168.111.12

Dieser Test zeigt, dass mit 'Packet Sniffing' ohne entsprechende Massnahmen im SCION-Protokoll Rückschlüsse bis auf die Endsysteme gemacht werden können. Unverschlüsselte Nachrichten sind Klartext lesbar.
Wird der Kommunikationskanal zwischen zwei privaten Netzen durch einen VPN-Tunnel verschlüsselt (vgl. Abbildung 10), lassen sich zwar keine Rückschlüsse auf die Endgeräte in den privaten Netzen machen. Jedoch sind die IP-Adressen der beiden VPN-Knoten und die verschlüsselte Kommunikation sichtbar.

5.3.7 Verbindung IP-Router – SCION Gate (UC2)

Die Kommunikation zwischen einem IP-Router und SCION Gate erfolgt über das herkömmliche IP-Protokoll im Netzwerk eines ISPs. Dieser Teil des Kommunikationspfads ist kryptografisch ungeschützt. Hier wäre z.B. eine Man-in-the-Middle Attacke möglich. Ist die öffentliche IP-Adresse des IP-Routers bekannt, kann dieser ohne Gegenmassnahmen durch gezielte volumetrische Angriffe lahmgelegt werden, was zu einem Ausfall der Kommunikation führen kann. Auch 'Packet Sniffing' lässt sich nicht verhindern.

Im folgenden Abschnitt wird die Verbindung zwischen einem IP-Router eines privaten Netzwerks und dem SCION Gate betrachtet, welcher in diesem Fall auch die Funktion des SIG übernimmt (vgl. UC2). Die Verbindung zwischen den beiden privaten IP-Netzen des Hauptquartiers (HQ) und des Bürostandorts (BS) ist durch einen VPN-Tunnel verschlüsselt (vgl. Abbildung 18).

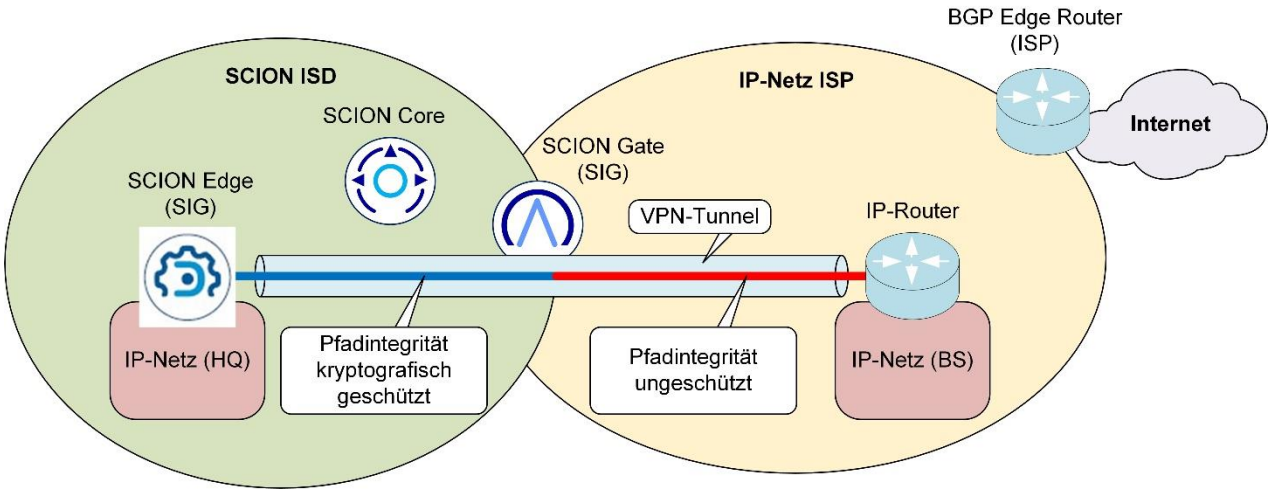

Abbildung 18: Verbindung IP-Router - SCION Gate (UC2)

Während in UC1 das SIG bereits die Schnittstelle zwischen dem privaten Netz am Bürostandort (BS) und der WAN-Schnittstelle des SCION Edge-Routers zum SCION-Netzwerk bildet, werden die IP-Pakete in UC2 erst im SCION Gate beim ISP in SCION Pakete gekapselt. Zwischen SCION Gate und SCION Edge in der ISD sind die Pfade kryptografisch geschützt. Für die Absender eines IP-Pakets aus den privaten Netzen des Hauptquartiers (HQ) und des Bürostandorts (BS) sind die Routingpfade im IP-Netz eines ISP jedoch unbekannt. Auf dieser Strecke können die definierten Richtlinien der TRC nicht überprüft und umgesetzt werden. Es ist möglich, dass eine geografische Eingrenzung der Kommunikationswege im IP-Netz des ISP nicht eingehalten wird. Auf diesem Teil der Verbindung sind die Daten und die Verbindung den Risiken der IP-Welt ausgesetzt.

5.3.8 Verbindung Mobile IP-Router – SCION Gate (UC3)

Die Kommunikation zwischen Mobile IP-Router und SCION Gate erfolgt wie die kabelgebundene Verbindung im Kapitel 5.3.7 über das konventionelle IP-Protokoll eines ISPs. Deshalb weist diese Art der Verbindung dieselben Schwachstellen auf wie die kabelgebundene Verbindung. Zusätzlich bildet die Luftschnittstelle der Mobilfunkverbindung weitere Möglichkeiten für Cyberattacken. Diese sind nicht Bestandteil dieser Arbeit und müssen zusätzlich betrachtet werden.

5.3.9 SCION Netzwerkmanagement

Ein Angriff auf das Netzwerkmanagement kann grosse Auswirkungen auf die gesamte SCION-Infrastruktur in einer ISD haben. Durch Installieren von manipulierter Software und Firmware, sowie Manipulation der Routingpfade, haben Angreifende die Möglichkeit, in die ISD einzudringen oder diese lahmzulegen.
Die Verwaltung und Überwachung der SCION-Infrastruktur durch einen externen IT-Dienstleister bergen weitere Risiken. Eine kompromittierte IT-Infrastruktur des Dienstleisters kann ein Einfallstor für einen Cyberangriff auf die SCION-Infrastruktur sein.

6 Informationssicherheit

Die Ziele der Informationssicherheit sind der Schutz von Geschäftsgeheimnissen, Kunden- und Personendaten, Zugriffs- und Zutrittsschutz, Schutz vor Elementarschäden wie Wasser und Feuer und weiteren Gefahren. Die Risiken der Informationssicherheit für ein Unternehmen sind unterschiedlich und müssen individuell erkannt, betrachtet und beurteilt werden. Manche Risiken werden bewusst in Kauf genommen, andere müssen auf ein akzeptables Mass reduziert werden. Das CIA-Prinzip ist ein etabliertes Modell und eine Orientierungshilfe, um sich mit den Schutzzielen der Informationssicherheit auseinanderzusetzen. Dabei werden die Vertraulichkeit (Confidentiality), die Integrität (Integrity) und die Verfügbarkeit (Availability) der Daten, der Systeme und der Kommunikation betrachtet. In einer digital vernetzen Welt hat der Schutz der Informationen, der Systeme und der Kommunikation einen hohen Stellenwert für ein Unternehmen.

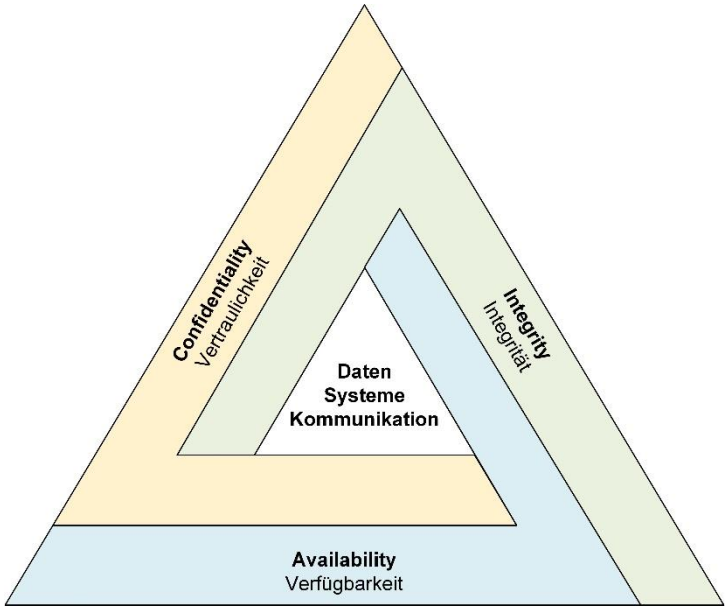

Abbildung 19: CIA-Prinzip

SCION hat zum Ziel, die Kommunikation in einer digital vernetzten Welt besser zu kontrollieren und zu schützen. Der Fokus liegt auf dem Schutz vor Angriffen auf OSI-Layer 1-3. Zum Schutz des Informationsinhalts sind zusätzliche Massnahmen auf einem höheren OSI-Layer (4-7) notwendig, z.B. durch VPN, TLS, etc.

Aus den Diskussionen mit Experten von Armasuisse W+T, Kdo Cy und den gewonnenen Erkenntnissen in Kapitel 5 werden die SCION-Kommunikationswege und die Infrastruktur nach dem CIA-Prinzip betrachtet und beurteilt. Der Fokus liegt auf der WAN-Umgebung der Anwendungsfälle UC1-UC3.

6.1 Vertraulichkeit (Confidentiality)

Die Vertraulichkeit in der Kommunikation im Internet bezieht sich sowohl auf den Inhalt einer Nachricht und den Kommunikationsweg als auch auf die Anforderungen zum Verbergen von sensitiven Netzwerktopologien im Betrieb. Nur autorisierte Teilnehmer dürfen im Kommunikationspfad sein und auf die Daten Zugriff haben. Standardmässig stellt die SCION-Architektur keine vertraulichen Kommunikationskanäle oder Netzwerktopologien zur Verfügung.

In einer SCION ISD teilen alle AS ihre Pfade über den Beaconing-Prozess und dem 'Path Advertising' den anderen AS mit [10]. Sämtliche Pfade in einer ISD sind für alle AS sichtbar. Die Kommunikation zwischen einem Absender und einem Empfänger können mit gezielten Methoden (vgl. Kapitel 5.3.6) mitgelesen werden. Ohne weitere Massnahmen sind die Kommunikationswege in SCION somit nicht vertraulich.

Mit 'hidden path communication' bietet SCION eine Möglichkeit, bestimmte Pfadsegmente nur autorisierten AS mitzuteilen [20]. Um diese verdeckt zu halten, müssen die Pfadinformationen 'out-of-band' ausgetauscht werden. Nur autorisierte AS erhalten diese Informationen. Für alle anderen AS in der ISD sind diese Pfade unsichtbar.
Mit 'hidden path communication' lässt sich ein Mitlesen der Kommunikation mit einem TAP jedoch nicht verhindern. Wird ein TAP an der richtigen Stelle im Kommunikationspfad eingesetzt, lassen sich sowohl in UC1, als auch in UC2 und UC3 Pfadinformationen und Metadaten herausfinden.

Die Sicherstellung der Vertraulichkeit vom Inhalt einer Nachricht muss über zusätzliche Massnahmen in OSI-Layer 4-7, z.B. durch Verschlüsselung über ein VPN oder TLS erfolgen.

6.2 Integrität (Integrity)

Integrität in der Informationssicherheit bedeutet die Sicherstellung der Korrektheit und Unversehrtheit der Daten. Mit kryptographischen Methoden stellt SCION die Integrität und Authentizität des Kommunikationsweges sicher. Die Pfadsegmente sind eindeutig zuzuordnen und abgesichert. Um einen Angriff erfolgreich durchführen zu können, müssten mehrere Komponenten in der SCION-PKI kompromittiert werden.

6.3 Verfügbarkeit (Availability)

Die Bedeutung von Verfügbarkeit in der Informationssicherheit heisst sowohl die Möglichkeit des Zugriffs auf Daten wie auch die Verfügbarkeit von Systemen und Kommunikationswegen. Eines der Ziele von SCION ist die Sicherstellung der Verfügbarkeit der Kommunikationswege. Verteilte volumetrische Attacken auf OSI-Layer 3 lassen sich mit SCION grösstenteils verhindern. Eine DDoS-Attacke in einer ISD auf die SCION-Infrastruktur ist eher unwahrscheinlich.

Die Verfügbarkeit hängt auch von der Topologie eines Netzwerks ab. SCION-Infrastrukturkomponenten wie Edge, Gate oder Core können technisch bedingt ausfallen. Deswegen empfiehlt es sich, wichtige Pfade redundant aufzubauen. Für die ISD wichtigen Core-Komponenten sollte nebst Hardware- und Pfadredundanz auch eine geografische Trennung erfolgen, so dass bei einem Ereignis wie Wasser oder Feuer nicht die komplette ISD in Mitleidenschaft gezogen wird.

Um die Abhängigkeit von einzelnen ISP zu minimieren, ist die Erschliessung mit mindestens zwei Providern als Core-AS zu empfehlen. So kann verhindert werden, dass ein Ausfall eines Core-AS eines ISPs Auswirkungen auf die gesamte ISD hat.

6.4 Anonymität

Nebst den drei Pfeilern des CIA-Prinzips spielt auch die Anonymität in der Kommunikation eine wichtige Rolle. In einer SCION ISD teilen sämtliche AS ihre Pfade über den Path-Advertising-Prozess. Somit sind jedem AS die Wege zu einem anderen AS bekannt. Wie bereits in Kapitel 6.1 erwähnt, existiert mit 'hidden path' in SCION eine Möglichkeit, dass einzelne AS bestimmte Pfadsegmente nicht im Path-Advertising-Prozess melden und somit nur für autorisierte AS bekannt sind. Da jedoch wie im IP-Protokoll auch in SCION

zum Versenden und Empfangen von Datenpaketen ein Sender und ein Empfänger definiert werden muss, ist eine absolute Anonymität nicht gegeben. Kann der Kommunikationskanal eines 'hidden path' (vgl. Kapitel 5.3.6) mitgelesen werden, können auch hier Metadaten und die Kommunikation analysiert werden.

Mit HORNET (High-speed Onion Routing at the Network Layer), einem in der Praxis noch unerprobten Protokoll der ETH Zürich und dem University College London, könnte die Anonymität mit SCION gewährt werden. Dabei kennen sich Sender und Empfänger im SCION-Netzwerk nicht [21]. Die Funktionsweise ist vergleichbar mit dem TOR-Netzwerk.

6.5 Risiken

In Tabelle 6 sind bekannte Angriffstechniken aufgelistet, welche im OSI-Modell in Schicht 1-3 angewendet werden. Die Angriffstechniken sind nach CIA zugeordnet und zeigen, auf welchen der drei Bereiche ein Angriff zielt. Die Techniken sind gemäss den Schutzzielen von SCION beurteilt und werden für die Risikoeinschätzung der Kommunikationspfade von UC1-UC3 verwendet.

	Angriffstechnik	Beurteilung
Confidentiality	Packet Sniffing (OSI Layer 1)	Ein passives Mitlesen (Packet Sniffing) der SCION-Kommunikation wird kaum erkannt. SCION-Headerinformationen über kommunizierende ISD, AS und IP-Adressen von SIG sind sichtbar. Werden die Nutzdaten nicht mit einem Protokoll auf OSI Layer 4 oder höher verschlüsselt, sind diese im Klartext einsehbar (vgl. Kapitel 5.3.6).
Integrity	Man-in-the-Middle (MITM) (OSI Layer 2)	Die Pfadsegmente von jedem AS sind in SCION kryptografisch integritätsgeschützt. Deshalb sind MITM-Attacken zur Manipulation des Routings kaum möglich und würden schnell erkannt. Für eine erfolgreiche MITM-Attacke wäre eine mehrfache Kompromittierung der SCION-PKI notwendig.
	Route-Hijacking (Prefix-Hijacking) (OSI Layer 3)	Route-Hijacking ist in SCION nicht möglich, da jeder Pfad kryptografisch integritätsgeschützt ist und der Sender den Pfad zum Empfänger bestimmt. Eine Änderung im Pfad würde bemerkt und die Kommunikation verworfen.
	AS Spoofing (OSI Layer 3)	AS Spoofing ist mit SCION schwer durchzuführen. Dazu müsste ein gültiges AS-Zertifikat zum Generieren von gültigen 'Path-Segment Construction Beacons' (PCB) und 'Hop Field' Informationen (HF) vorhanden sein. Die Pfadinformationen werden jedoch unverschlüsselt übertragen und können von Dritten mitgelesen werden.

	Angriffstechnik	Beurteilung
Availability	DDoS (OSI Layer 3)	Durch Separierung von Control- und Dataplane ist es schwierig, einen netzwerkbasierten, verteilten, Angriff (volumetrisch) auf einen SCION-Knoten durchzuführen. Wegen der Vertrauensstellung innerhalb einer ISD zwischen den AS und ISD-übergreifend könnte ein Angriff nur innerhalb der TRC erfolgen. Botnetze und Command-and-Control-Server müssten sich innerhalb der ISD befinden. Zudem bietet SCION mit 'multi-path' die Möglichkeit, die Kommunikation über verschiedene Pfade zu leiten. Als optionale Zusatzmassnahme kann eine DDoS-geschütze Mindestbandbreite zwischen zwei Netzwerken reserviert werden. Einige Protokollbasierte Angriffe wie z.B. SYN Flooding können mit SCION auch verhindert werden. Angriffe wie z.B. applikationsbasierte Angriffe auf OSI-Layer 7 kann SCION jedoch nicht verhindern [22].

Tabelle 6: Beurteilung von Angriffstechniken mit SCION

6.5.1 Risikoskalierung

Die Skalierung in Tabelle 7 und Tabelle 8 wird für die Beurteilung der Risiken in Kapitel 6.5.2 bis 6.5.6 verwendet.

	Schadensausmass	
1	niedrig	Eintritt des Risikos hat nur geringe Konsequenzen
2	mittel	Bei Eintritt des Risikos sind die Konsequenzen leicht beherrschbar
3	hoch	Eintritt des Risikos benötigt Zeit, um die Konsequenzen zu beheben
4	sehr hoch	Erhebliche Konsequenzen bei Eintritt des Risikos und Möglichkeit eines langfristigen Schadens
5	kritisch	Grosse Konsequenzen und mögliche permanente Schäden

Tabelle 7: Skalierung Schadensausmass

	Eintrittswahrscheinlichkeit	
1	unmöglich	Fall tritt nie ein
2	unwahrscheinlich	Eher unwahrscheinlich, dass Risiko eintritt
3	möglich	Das Risiko kann, muss aber nicht eintreten
4	wahrscheinlich	Risiko kann mit erhöhter Wahrscheinlichkeit eintreten
5	sehr wahrscheinlich	Hohe Wahrscheinlichkeit, dass Risiko eintritt

Tabelle 8: Skalierung Eintrittswahrscheinlichkeit

6.5.2 Packet Sniffing

Durch Mitlesen von SCION Netzwerkverkehr, auch wenn die Nutzdaten darin verschlüsselt werden, kann dies Angreifenden Informationen zur Netzwerktopologie liefern. Durch Traffic Analysen lassen sich Metadaten wie Zeit, Headerinformationen über verwendete Protokolle, Ports, Routingpfade und IP-Adressen sowie Muster im Datenverkehr herausfinden.

	Packet Sniffing	Schadens-ausmass	Eintrittswahr-scheinlichkeit
UC1	Packet Sniffing im Umfeld der ICT-Infrastruktur eines ISP wird als eher schwierig erachtet, da zur Installation der dafür benötigten Infrastruktur Zutritt zu Gebäuden und der physische Zugriff auf die ICT-Infrastruktur eines ISP oder den SCION Edge-Routern im Hauptquartier (HQ) oder des Bürostandorts (BS) erforderlich ist. Dies ist nur einem eingeschränkten Personenkreis möglich. Ein Abgriff eines Kommunikationskanals müsste gezielt auf einer Leitung für SCION-Netzwerkverkehr erfolgen.	3	2
UC2	Für UC2 gelten dieselben Bedingungen wie bei UC1. Allerdings ist die Strecke zwischen IP-Router und SCION Gate kryptografisch ungeschützt. Die Transportpfade im Netzwerk eines ISP sind für den Absender einer Nachricht bis zum SCION Gate unbekannt. Dies könnte von einer angreifenden Person ausgenutzt werden. Allerdings ist auch hier der Zutritt zu Gebäuden und der physische Zugriff auf die ICT-Infrastruktur eines ISP erforderlich. Wahrscheinlicher ist es, dass ein Abgreifen des Netzwerkverkehrs beim der WAN-Schnittstelle der IP-Routers erfolgt.	3	3
UC3	Die Risiken, welche für UC2 gelten, haben auch für UC3 Gültigkeit. Zusätzlich kann der Netzwerkverkehr über die Luftschnittstelle zwischen Mobilfunk IP-Router und einer Mobilfunkantenne mitgehört werden.	3	3

Tabelle 9: Risikobeurteilung Packet Sniffing

6.5.3 Man-In-The-Middle

Eine MITM-Attacke hat das Ziel, die Kontrolle des Datenverkehrs zwischen zwei oder mehreren Netzwerkteilnehmern zu erlangen. Eine solcher Angriff erfordert physischen oder logischen Zugriff auf die Kommunikation von zwei Netzwerkpartnern [23].

	Man-In-The-Middle (MITM)	Schadens-ausmass	Eintrittswahr-scheinlichkeit
UC1	Für eine Man-In-The-Middle Attacke wäre eine Mehrfachkompro-mittierung der SCION PKI notwendig. Dies hätte Auswirkungen auf die gesamte Vertrauensstellung einer TRC. Ohne gültiges AS-Zertifikat ist eine MITM-Attacke auf die SCION-Infrastruktur nicht möglich.	5	2
UC2		5	2
UC3		5	2

Tabelle 10: Risikobeurteilung Man-In-The-Middle

6.5.4 Route-Hijacking

Beim Route-Hijacking übernimmt ein fremder Router im Internet den Transport von Daten zum Zielpunkt. Die Gründe dafür sind vielfältig. Die Absichten dahinter können politisch motiviert, aber auch kriminell Natur sein. Manchmal sind es auch Fehlkonfigurationen ohne böswillige Absichten, welche eine Abweichung von der effizientesten Route zur Folge haben [24].

	Route-Hijacking	Schadens-ausmass	Eintrittswahr-scheinlichkeit
UC1	Für ein erfolgreiches Route-Hijacking müsste eine angreifende Person im Besitz des kryptografischen Schlüsselmaterials einer TRC sein. Ohne gültiges Schlüsselmaterial ist in einer ISD keine Änderung von Pfadinformationen möglich. Eine Übernahme eines ganzen oder von Teilen eines Netzwerks eines AS hätte jedoch erhebliche Folgen in einer ISD.	5	2
UC2		5	2
UC3		5	2

Tabelle 11: Risikobeurteilung Route-Hijacking

6.5.5 AS Spoofing

Beim AS Spoofing wird versucht, die Identität eines vertrauenswürdigen AS zu übernehmen. Durch die Übernahme der Identität weist sich das schadhafte AS gegenüber der Gegenstelle als vertrauenswürdig aus.

	AS Spoofing	Schadens-ausmass	Eintrittswahr-scheinlichkeit
UC1	AS Spoofing ist mit SCION kaum möglich, da eine angreifende Person im Besitz des kryptografischen Schlüsselmaterials eines AS sein müsste. Dafür wäre eine Mehrfachkompromittierung der SCION PKI notwendig. Das Schadensausmass wäre hoch, da die angreifende Person sich als autorisierter und authentifizierter Netzwerkteilnehmer ausgeben könnte.	5	2
UC2		5	2
UC3		5	2

Tabelle 12: Risikobeurteilung AS Spoofing

6.5.6 DDoS-Attacke

Mit DDoS-Attacken wird versucht, mit einer grossen Anzahl von Anfragen vieler Systeme ein Zielsystem lahmzulegen. Während der Zeit eines laufenden Angriffs kann das Zielsystem keine weiteren, legitimen Anfragen bearbeiten. Es besteht auch die Gefahr, dass das Zielsystem in einen unsicheren Zustand gebracht wird. Dieser könnte ausgenutzt werden, um ins System einzudringen und dieses zu manipulieren, oder mit Schadsoftware zu infizieren.

	DDoS	Schadens-ausmass	Eintrittswahr-scheinlichkeit
UC1	DDoS-Attacken in SCION können nur innerhalb einer ISD durchgeführt werden. Systeme, welche sich nicht innerhalb der ISD befinden, können nicht über die SCION-Infrastruktur kommunizieren. SCION bietet mit einer Bandbreitenreservierung die Möglichkeit an, bei einer hohen Auslastung eine Restbandbreite für wichtige Dienste freizuhalten. Da bei UC2 und UC3 der Kommunikationspfad zwischen IP-Router und SCION Gate kryptografisch ungeschützt ist, können mit gezielten Angriffen der IP-Router, resp. Mobile IP-Router lahmgelegt werden. Nebst einem Ausfall der Kommunikation zwischen IP-Router und SCION Gate, könnten durch die Überlastung der IP-Router auch Schwachstellen zum Infizieren oder Manipulieren der Geräte ausgenutzt werden.	4	2
UC2		5	3
UC3		5	4

Tabelle 13: Risikobeurteilung DDoS-Attacke

Das Risiko für DDoS-Attacken in SCION ist geringer als in IP-Netzwerken. Deshalb wird die Eintrittswahrscheinlichkeit etwas niedriger beurteilt. Allerdings besteht bei UC2 und UC3 ein Restrisiko für DDoS-Angriffe auf die SCION-Infrastruktur im IP-Netz des ISP.

6.5.7 Risikobeurteilung

Aus den in den Kapiteln 6.5.2 - 6.5.6 ermittelten Angriffstechniken auf OSI-Layer 1-3 geht hervor, dass die grössten Risiken in UC2 und UC3 bei DDoS-Attacken bestehen (vgl. Abbildung 20). Der Schaden, welcher aus einer kompromittierten CP-PKI entstehen kann, ist zwar unwahrscheinlich, wird aber als kritisch eingestuft. Mit einer kompromittierten CP-PKI wären Man-in-The-Middle Angriffe, Route-Hijacking und AS Spoofing möglich.

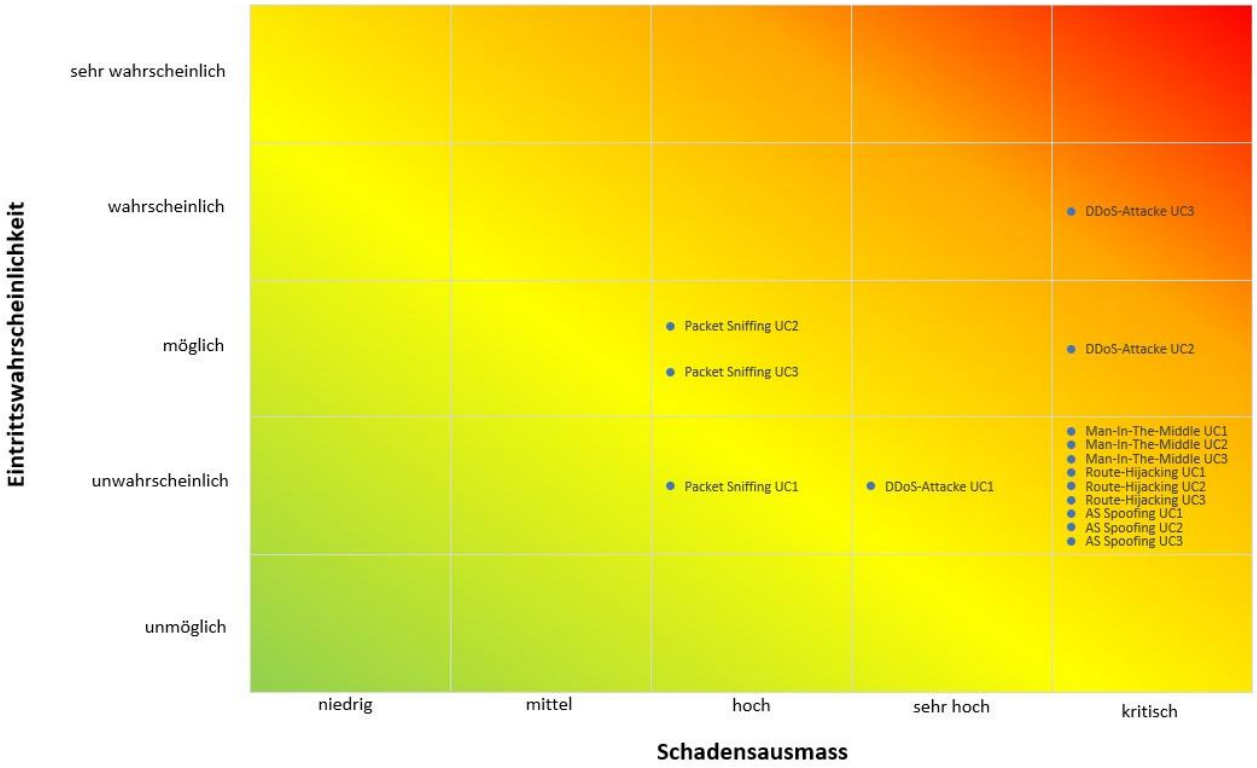

Abbildung 20: Risikomatrix

Während DDoS-Attacken bei UC1 als unwahrscheinlich eingeschätzt werden, ist die Wahrscheinlichkeit für UC2 und UC3 höher, da der Kommunikationskanal bis zum SCION Gate allen Gefahren aus der IP-Welt ausgesetzt ist. Für UC3 weist die Luftschnittstelle ein weiteres Gefahrenpotential für Cyberangriffe aus. Ein Mitlesen der Daten ist hier ohne physikalischen Eingriff in den Kommunikationskanal möglich. Da dies in der vorliegenden Arbeit nicht weiter analysiert wird, wird das Risiko für diesen Anwendungsfall am höchsten eingestuft.

7 Schutzmassnahmen der SCION-Infrastruktur

Damit die in Kapitel 5 aufgeführten Angriffsvektoren (1-5) in der SCION-Infrastruktur minimiert werden können, sollten die in Tabelle 14 aufgeführten Schutzmassnahmen beachtet und umgesetzt werden. Mit diesen lassen sich die Risiken eines Angriffs oder die Kompromittierung der SCION-Infrastruktur reduzieren.

Angriffsvektor	Schutzmassnahmen
SCION Hardware/Firmware	• Sicherung des Zugangs zum System durch Zutritts- und Zugriffsschutz • Deaktivieren nicht benutzter physischer Schnittstellen (USB, Netzwerk, Seriell, etc.) • Änderung von Standardpasswörtern durch starke, komplexe Passwörter • Passwortschutz von BIOS/UEFI • Deaktivierung nicht benötigter Komponenten in BIOS/UEFI • Definieren der Boot-Reihenfolge, Ausschalten nicht benötigter Boot-Komponenten • Regelmässige Aktualisierung der Firmware • Deaktivierung nicht benötigter Benutzerprofile • Dedizierte Hardware für SCION-Dienste
Betriebssystem (Linux Server)	Härtung des Betriebssystems durch folgende Massnahmen: • Deaktivierung nicht benötigter Dienste und Applikationen • Regelmässige Aktualisierung mit den neusten Patches und Sicherheitsupdates • Konfiguration von personalisiertem Zugriff (User Access) Aktivierung Zweifaktorautorisierung (falls möglich) • Sicherer SSH Zugriff durch Authentisierung mit Zertifikat Anstelle eines Passworts • Implementation einer starken Passwort Policy • Dateisystemverschlüsselung (z.B. LUKS) • Partitionierung für Logfiles, Home, temporäre Dateien • Deaktivierung von ‘root login’ • Evtl. Änderung des SSH Defaultports (Port 22) • Installation einer Antivirussoftware/Virenscanner • Autorisierung: Serverdienste müssen unter eigenem, nicht privilegiertem Account laufen • Installation von AppArmor • Persistenz zur Steuerung von Deamons (systemd) • Härtung des Netzwerkstacks • Konfiguration des Loggings, z.B. *syslog-ng* • Integritätsprüfung von Paketen der Linux Distribution • Beachtung von Herstellervorgaben (gem. [16])

Angriffsvektor	Schutzmassnahmen
CP-PKI	• Einsatz eines Hardware Security Module (HSM) für die Verwaltung des privaten Schlüsselmaterials • HSM-Aufbau georedundant • Physischer Zutritts- und Zugriffsschutz • Zugriff nur vom lokalen Netz, kein Fernzugriff
IP-Router	• Hardware, Firmware und Betriebssystem auf aktuellem Stand halten
Mobile IP-Router	• Hardware, Firmware und Betriebssystem auf aktuellem Stand halten
Verbindung SCION Edge – SCION Edge (UC1)	• Physischer Schutz. Zutritt zu Gebäude, Raum und Rack nur für berechtigte Personen. Zugang zu LAN und WAN-Schnittstellen der SCION Edge-Router muss gesichert sein • Protokollierung des Zutritts
Verbindung IP-Router – SCION Gate (UC2)	• Physischer Schutz. Zutritt zu Gebäude, Raum und Rack zu SCION GATE nur für berechtigte Personen. Zugang zu LAN und WAN-Schnittstellen von SCION Gate muss gesichert sein • Protokollierung des Zutritts • Physischer Schutz von IP-Router (abschliessbares Rack)
Verbindung Mobile IP-Router – SCION Gate (UC3)	• Physischer Schutz. Zutritt zu Gebäude, Raum und Rack zu SCION Gate nur für berechtigte Personen. Zugang zu LAN und WAN-Schnittstellen von SCION Gate muss gesichert sein • Protokollierung des Zutritts • Physischer Schutz von IP-Router (abschliessbares Rack) -> Signalstärke der Mobilfunkverbindung muss beachtet werden
SCION Netzwerkmanagement	• Zugriff nur für autorisiertes Personal • Persönliche Benutzer-Accounts • Regelmässige Audits der Core AS • Out-of-Band Management über kryptografisch gesicherte und verschlüsselte Pfade

Tabelle 14: Schutzmassnahmen SCION-Infrastruktur [25]

Um zu verhindern, dass Schwachstellen aus der BGP- und IP-Welt auch in SCION ausgenutzt werden können, sollten die SCION-Dienste auf dedizierter Hardware laufen.

8 Technologienvergleich

Neben SCION existieren auf dem Telekommunikationsmarkt weitere Technologien für WAN-Dienste, welche je nach Anwendungsgebiet ihre Vorzüge und Nachteile haben. In diesem Kapitel werden Software Defined Wide Area Network (SD-WAN) und Multiprotocol Label Switching (MPLS) SCION gegenübergestellt.

8.1 Software Defined Wide Area Network (SD-WAN)

Die globale Vernetzung von Unternehmen und Rechenzentren verlangt nach flexiblen, offenen und Cloud-basierten WAN-Technologien anstelle von teuren, fixen Leitungen oder proprietärer Hardware. Deswegen wurde SD-WAN entwickelt, um über geografische Grenzen und grosse Distanzen eine Kommunikation zwischen verschiedenen Netzwerkendpunkten zu ermöglichen [26].

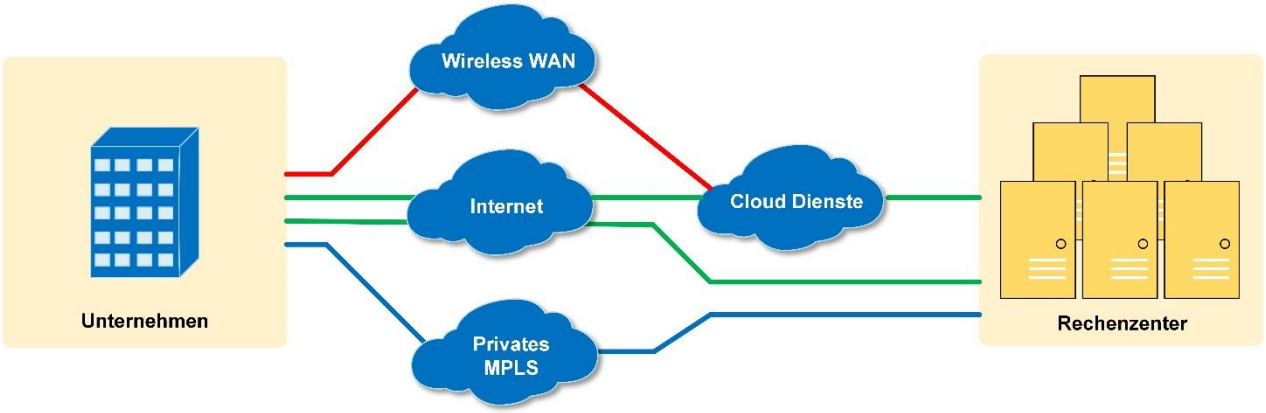

Abbildung 21: SD-WAN Netzwerk [26]

SD-WAN eignet sich für Unternehmen mit zentralen Unternehmensnetzwerken und vielen Zweigstellen oder zwischen Rechenzentren, welche geografisch getrennt sind. Mit SD-WAN lässt sich ein Netzwerk gut skalieren. Anpassungen im Netzwerk können schnell umgesetzt werden.

8.2 Multiprotocol Label Switching (MPLS)

MPLS wird verwendet, um zwei Firmenstandorte zu verbinden. Datentechnisch kann MPLS wie eine Punkt-zu-Punkt Verbindung betrachtet werden. Auf diese Weise können Firmen eine einzelne Netzwerkverbindung für verschiedene Dienste nutzen. Die Funktion ist ähnlich wie bei Ethernet-Switches und -Routern und befindet sich im OSI-Modell zwischen Schicht 2 und 3. Die Datenpakete der unterschiedlichen Quellen werden in MPLS mit Etiketten, sog. Labels versehen, mit welchen sich der Datenverkehr priorisieren lässt. Somit können zeitkritische Anwendungen wie Sprach- und Videodaten höher priorisiert werden als anderer Netzwerkverkehr [26].

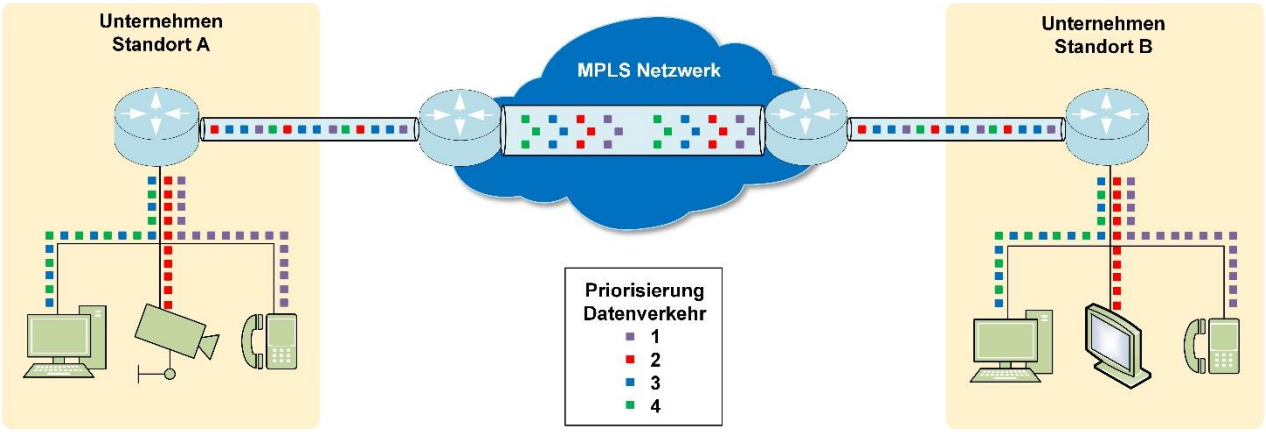

Abbildung 22: MPLS Netzwerk [26]

MPLS-Verbindungen sind sehr zuverlässig. Allerdings sind Änderungen im Netzwerk aufwendig und unflexibel. Die Kosten zur Erschliessung neuer Standorte sind relativ hoch, da für die Verbindung eigene Leitungen gebaut oder bei einem ISP gemietet werden müssen. Je nach Bandbreitenbedarf lassen sich die Leitungen mit Diensten anderer Unternehmen teilen, was die Betriebskosten etwas senkt.

8.3 Vor- und Nachteile der Technologien

Tabelle 15 und Tabelle 16 geben einen Überblick über die Vor- und Nachteile der jeweiligen Technologie.

Vorteile	
SCION	• **Pfadkontrolle:** Absender und Empfänger kennen den gesamten Übertragungspfad durch Schutz der Pfadintegrität durch kryptografische Methoden. • **Flexibel:** Erschliessung an beliebigen Standorten über Internetverbindungen lokaler ISP. • **Sicherheit:** Schutz gegen DDoS-Attacken und BGP-Hijacking, da aus dem legacy Internet unsichtbar.
SD-WAN	• **Kosten:** Keine hohen Kosten für Routing-Hardware und keine Herstellerbindung • **Keine geografischen Beschränkungen:** Erschliessung an beliebigen Standorten über das Internet. • **Betrieb:** Vereinfachung des Betriebs durch Zero-Touch-Provisionierung und Cloud-basiertes Netzwerkmanagement.
MPLS	• **Hohe Leistung:** Durch vordefinierte Netzwerkpfade entfällt das Routing, was die Datenübertragung schnell macht. Durch die Kennzeichnung der Pakete kann zeitkritischer Netzwerkverkehr priorisiert werden. • **Pfadkontrolle:** Die Netzwerkpfade sind durch die vorgegebenen Verbindungen definiert. • **Verlässlichkeit:** Zuverlässige Zustellung von Paketen und hohe Qualität für zeitkritische Protokolle.

Tabelle 15: Technologie Vorteile

Nachteile	
SCION	• **Bandbreite:** Zurzeit ist SCION auf eine maximale Bandbreite von ca. 10 Gbit/s begrenzt. Es existiert noch keine dezidierte Hardware, welche höhere Übertragungsraten zulässt. • **Kosten:** Durch die zusätzlich erforderliche PKI sind die Kosten höher als eine konventionelle Breitband-Internetverbindung • **Verbreitung:** Aktuell bieten weltweit nur wenige ISP SCION-Dienste an. • **Komplexität:** Aufbau und Betrieb der PKI-Infrastruktur sind zeit- und kostenintensiv.
SD-WAN	• **Sicherheit:** SD-WAN bietet selbst keine Sicherheit. Jede Zweigstelle ist mit dem Internet verbunden und somit anfällig für Cyberangriffe. Die Gewährleistung der Sicherheit muss über Zusatzmassnahmen erfolgen. • **Fehleranfälligkeit:** Jitter und Paketverluste können vorkommen. • **Keine Pfadkontrolle:** Ausser dem ersten Hop einer Netzwerk-verbindung sind die Pfade nicht vordefiniert.
MPLS	• **Kosten:** Die Bandbreitenkosten sind höher als bei einer konventionellen Breitband-Internetverbindung • **Flexibilität:** Nur für Punkt-zu-Punkt Verbindungen. Cloud-Anwendungen und Dienste wie ‘Software-as-a-Service’ (SaaS) sind nicht direkt möglich.

Tabelle 16: Technologie Nachteile

9 Empfehlungen

Die untersuchten Anwendungsfälle in Kapitel 5.3.6 bis 5.3.8 zeigen, dass der Einsatz von SCION in einem einsatzkritischen Umfeld nicht für alle betrachteten Anwendungsfälle gleich gut geeignet ist. In einer bestehenden legacy IP-Infrastruktur für UC1 wird SCION als eine mögliche Alternative zu eigenen Glasfaser- und Kupferleitungen erachtet, da sich der Edge-Router als SIG in unmittelbarer Nähe zum privaten IP-Netz befindet. Der Einsatz von SCION für UC2 und UC3 wird als risikoreicher eingestuft, da die Kommunikationswege im Netz des ISP bis zum SCION Gate kryptografisch ungeschützt sind und sich der Pfad vom Absender bis zum SCION Gate nicht definieren und kontrollieren lässt. Aus diesem Grund wird eine Verbindung über SCION Gate nicht empfohlen. Es ist immer eine Verbindung über einen SCION Core zu bevorzugen.

Falls sich eine Implementierung des SCION-Protokolls in Zukunft in den Betriebssystemen durchsetzen wird, werden die Lösungen mit SIG hinfällig. Die Absendersysteme werden beim Versenden von Nachrichten den Pfad selbst definieren und die Empfangssysteme werden den Kommunikationsweg auf Authentizität überprüfen können. Dann werden die Kommunikationspfade mit SCION kryptografisch Ende-zu-Ende geschützt sein.

Die CP-PKI ist ein Kernelement von SCION. Aus diesem Grund ist eine sorgfältige Planung der PKI-Architektur wichtig. Aspekte wie Resilienz und Systemredundanz haben einen Einfluss auf die Ausfallsicherheit einer TRC. Für den Aufbau einer CP-PKI Architektur muss definiert sein, welche Organisationen welche Rollen in der TRC haben.

Aus den Gesprächen mit Experten der SNB und SIX und den Erfahrungen im produktiven Umfeld des SSFN wird diese TRC als Orientierungshilfe für den Vorschlag einer TRC für das Kommando Cyber genommen (vgl. Kapitel 9.6) [27] [1].

9.1 Portabler SCION Edge-Router (UC2)

Momentan ist der Einsatz eines SCION Edge-Routers noch an den Formfaktor von 19'' Racks gebunden. Solange das SCION-Protokoll nicht in den Endsystemen implementiert ist und diese das SCION-Protokoll nicht nativ beherrschen, sind Entwicklungen von Zwischenlösungen für UC2 und UC3 notwendig. Um SCION bei temporären Einsätzen mit einzelnen Endsystemen oder im Homeoffice einzusetzen, ohne den Risiken über den Weg eins SCION Gates ausgesetzt zu sein, kann die Entwicklung eines portablen SCION-Routers in Erwägung gezogen werden. Neben der WAN-Schnittstelle kann dieser z. B. auch LAN-Schnittstellen haben und im privaten Netz die Funktion eines Netzwerkswitches übernehmen. Zusätzlich kann in einem portablen SCION-Router auch die Funktion eines VPN-Endpunktes implementiert werden. So würde sich eine Anwendung für UC2 umsetzen lassen.

9.2 Analyse der Luftschnittstelle 4G/5G Hotspot (UC3)

Für UC3 ist zu prüfen, ob eine Verbindung von einem SCION Edge-Router über einen 4G/5G Hotspot hergestellt werden kann (vgl. Abbildung 23). Bei dieser Option müssen die Risiken, welche für die Datenübertragung über die Luftschnittstelle bestehen, ermittelt und überprüft werden.

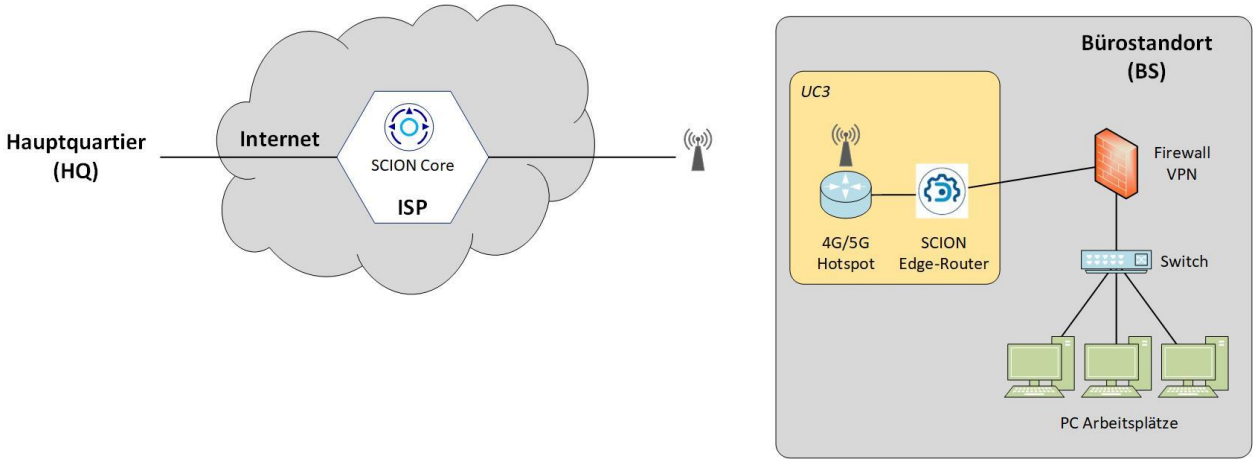

Abbildung 23: Verbindung 4G/5G Hotspot - SCION Core

Falls sich die Datenübertragung über die Luftschnittstelle als unkritisch erweist, kann ein 4G/5G-fähiger SCION-Hotspot entwickelt werden.

9.3 Verhinderung Internetzugriff

Das bestehende Netzwerk vom Kommando Cyber ist vom Internet isoliert. Mit einer eigenen ISD kann mit SCION ein privates Netz gebaut werden, welches die Internetarchitektur der ISP für den Datentransport zwischen Hauptquartier (HQ) und Bürostandort (BS) verwendet, jedoch ausserhalb der ISD und vom konventionellen Internet (BGP) nicht erreichbar ist.

Eine Internetkonnektivität der Endsysteme aus dem privaten IP-Netz vom Hauptquartier (HQ) und Bürostandort (BS) muss verhindert werden. Dies lässt sich über die Konfiguration der SCION Edge-Router steuern, welche nur SCION-Traffic innerhalb der ISD zulassen und den Internetverkehr blockieren.

9.4 Vorschlag ISD

Das Kommando Cyber betreibt ein eigenes Glasfasernetz. Deshalb ist es naheliegend, in SCION eine eigene ISD zu bilden. Dadurch besteht die Kontrolle über den Datenverkehr, welcher die Schweiz geografisch nicht verlassen darf. Jeder Standort bildet mit seinen Edge-Routern ein eigenes AS.

Falls zukünftig weitere Bereiche im VBS SCION-Dienste nutzen sollten, kann dafür dieselbe physische Infrastruktur für die CP-PKI benutzt werden. Die Netze sollten jedoch logisch in unterschiedliche ISD aufgeteilt sein. Dies hätte den Vorteil, dass Skaleneffekte genutzt und Betriebskosten gesenkt werden können.

9.5 Vorschlag Netzwerktopologie

Die Erschliessung wichtiger Bürostandorte (BS), aber mindestens das Hauptquartier (HQ), soll mit physischer Redundanz aufgebaut werden. Das heisst, pro Standort zwei Edge-Router mit zwei physisch getrennten Internetleitungen, einer Leitung pro ISP.

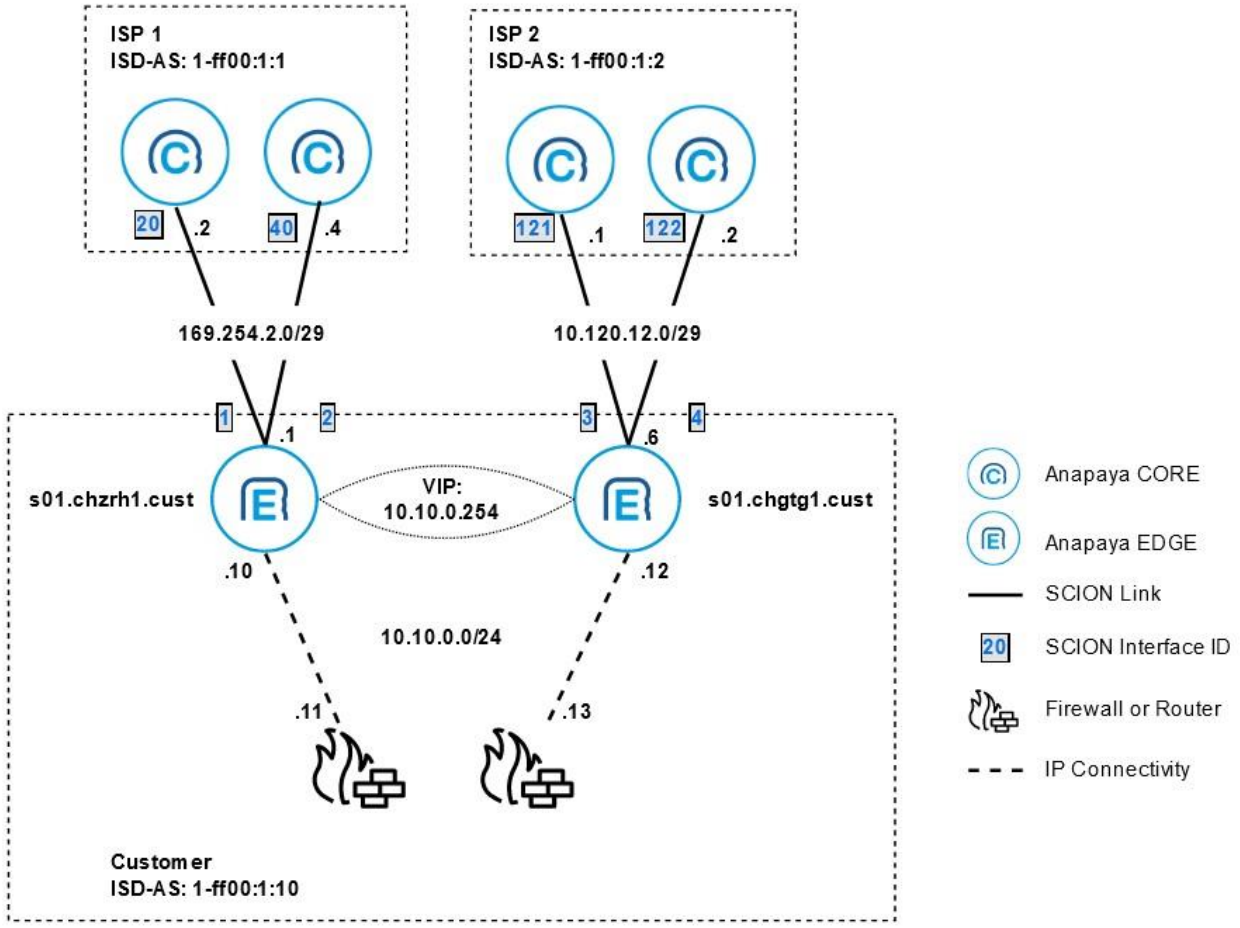

Abbildung 24: Redundantes Edge Setup [28]

Gemäss Designvorschlag von Anapaya (vgl. Abbildung 24) werden aus Redundanzgründen zwei Edge-Router pro Standort eingesetzt. Die Links zwischen Edge-Router zum Core-Router können entweder als statische oder dynamische Redundanz konfiguriert werden. Dieses Setup hat den Vorteil, dass die Appliances automatisch die Pfadinformationen untereinander austauschen und so Provider-Uplink-Redundanz besteht. In dieser Konfiguration bilden die Edge-Router einen Cluster und verwenden dafür das Virtual Router Redundancy Protocol (VRRP). Statische Redundanz wird empfohlen, wenn das Firmennetzwerk kein dynamisches Routingprotokoll für die Edge-Router zur Verfügung stellt. In dieser Topologie wird der ausgehende Datenverkehr nur über einen Edge-Router geleitet. Der zweite Edge-Router dient als Rückfallebene. Eingehender Datenverkehr vom SCION-Netzwerk kann über beide Edge-Router erfolgen [28].

9.6 Vorschlag TRC

9.6.1 Core AS

Aus Verfügbarkeitsgründen sollen für die Core AS zwei oder mehr ISP definiert werden. Ein Ausfall eines Core AS wirkt sich dadurch nicht auf die Verfügbarkeit der gesamten TRC resp. ISD aus.

9.6.2 Voting AS

Die Voting Member (Voting AS) bestimmen, welche Teilnehmer (Member AS) in die ISD aufgenommen werden. Für das Kommando Cyber soll eine eigene ISD erstellt und dieses als alleiniges Voting AS in der TRC definiert werden. Dies entspricht zwar nicht den Empfehlungen von Anapaya, da dies das Vertrauenskonstrukt einer TRC in Frage stellt. Ein Ausfall eines alleinigen Voting AS hätte zur Folge, dass das Vertrauenskonstrukt der TRC zusammenfällt. Da die Hoheit der ISD jedoch nur für das Kommando Cyber als alleiniger Nutzer der Domäne erstellt werden soll, wird diese Variante weiterverfolgt. Aus den Diskussionen mit SNB und SIX (SSFN) und deren Erfahrungen sollte eine TRC mit nur einem Voting AS möglich sein.

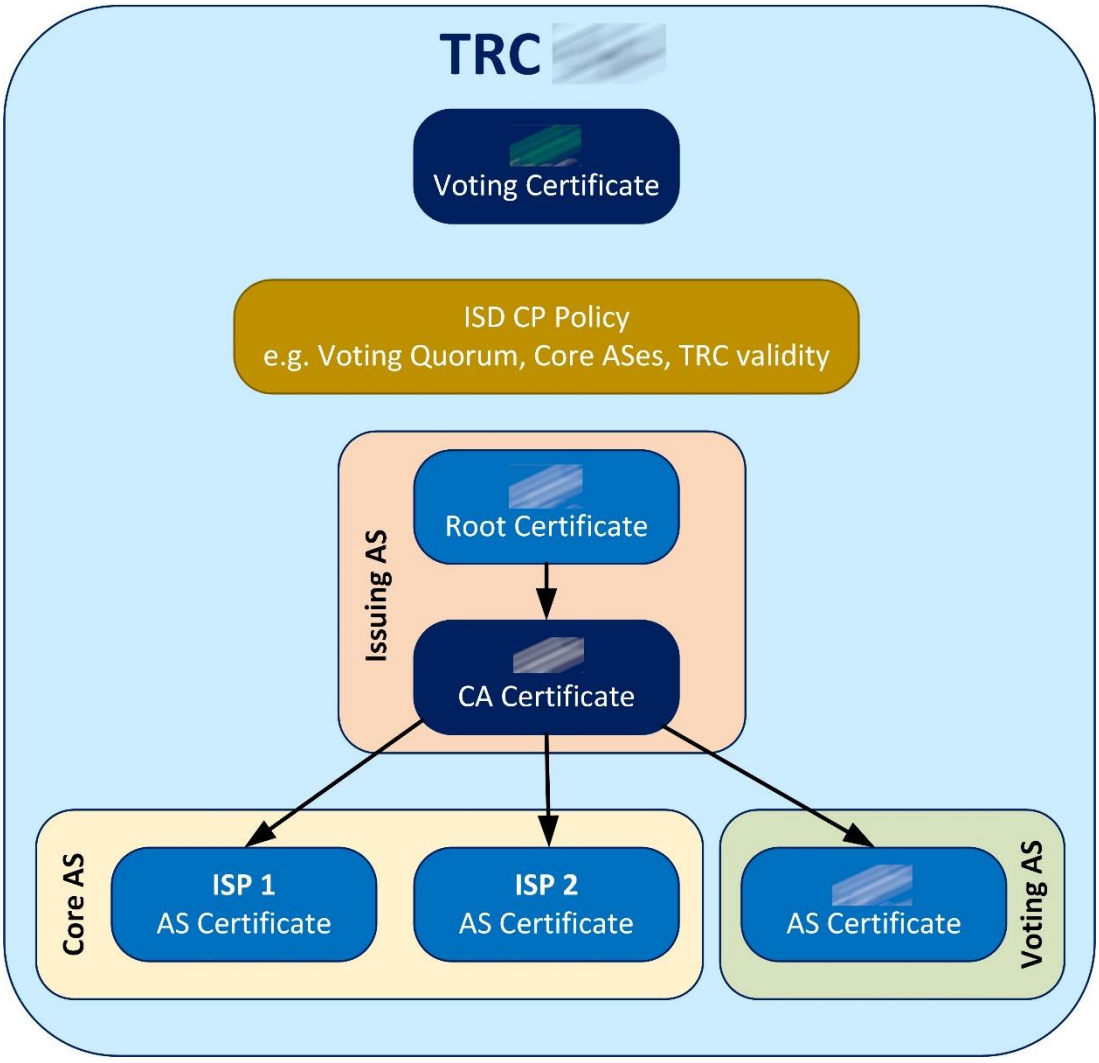

Abbildung 25: TRC-Vorschlag

9.6.3 Issuing AS

Die Issuing Member (Issuing AS) bilden die Certificate Authority (CA) einer TRC. Diese stellen die AS-Zertifikate für sämtliche AS in der ISD aus. Der Betrieb einer CA stellt ein Unternehmen vor neue Herausforderungen und erfordert spezifisches Wissen. Aus diesem Grund kann nicht abschliessend gesagt werden, dass das Kommando Cyber eine eigene CA betreiben, oder die Dienstleistung von Partnern in der Bundesverwaltung beziehen soll.
Dieser Vorschlag einer TRC für das Kommando Cyber dient als Leitfaden und ist nicht abschliessend. Es sind weitere Sicherheitsanalysen von internen Experten und grundlegende Entscheidungen zum Aufbau und Betrieb der CP-PKI notwendig.

9.7 Weiteres Vorgehen

Zum Test der Eignung und der Einführung von SCION im Kommando Cyber sind weitere Schritte notwendig. Diese sind in folgende Arbeitspakete aufgeteilt:

AP Nr.	Beschreibung
1	Planung und Aufbau SCION CP-PKI
2	Planung und Aufbau PoC UC1 im Labor vom Cyber-Defence Campus für Last- und Redundanztest: • 10 Zeroclients virtuell an BS • 5 Zeroclients virtuell im HQ • Videokonferenzserver virtuell im HQ • Server virtuell für Officeanwendungen im HQ • 2 SCION Edge Router im HQ • 1 SCION Edge Router im BS
3	Pilotbetrieb (UC1) mit einem Bürostandort • 10 Arbeitsplätze (BS) • 5 Arbeitsplätze (HQ)
4	• Pentest SCION-Protokoll
5	• Schulung Betriebspersonal SCION-Infrastruktur
6	• Entwicklung portabler SCION Edge-Router (UC2)
7	• Schwachstellen- und Risikoanalyse Luftschnittstelle (UC3) • Test SCION Edge-Router über 4G/5G Hotspot (UC3)

Tabelle 17: Arbeitspakete

Da während des Pilotbetriebs (AP Nr.3) noch keine eigene CP-PKI zur Verfügung steht, soll als Zwischenlösung die CP-PKI aus dem Labor vom Cyber-Defence Campus genommen werden.

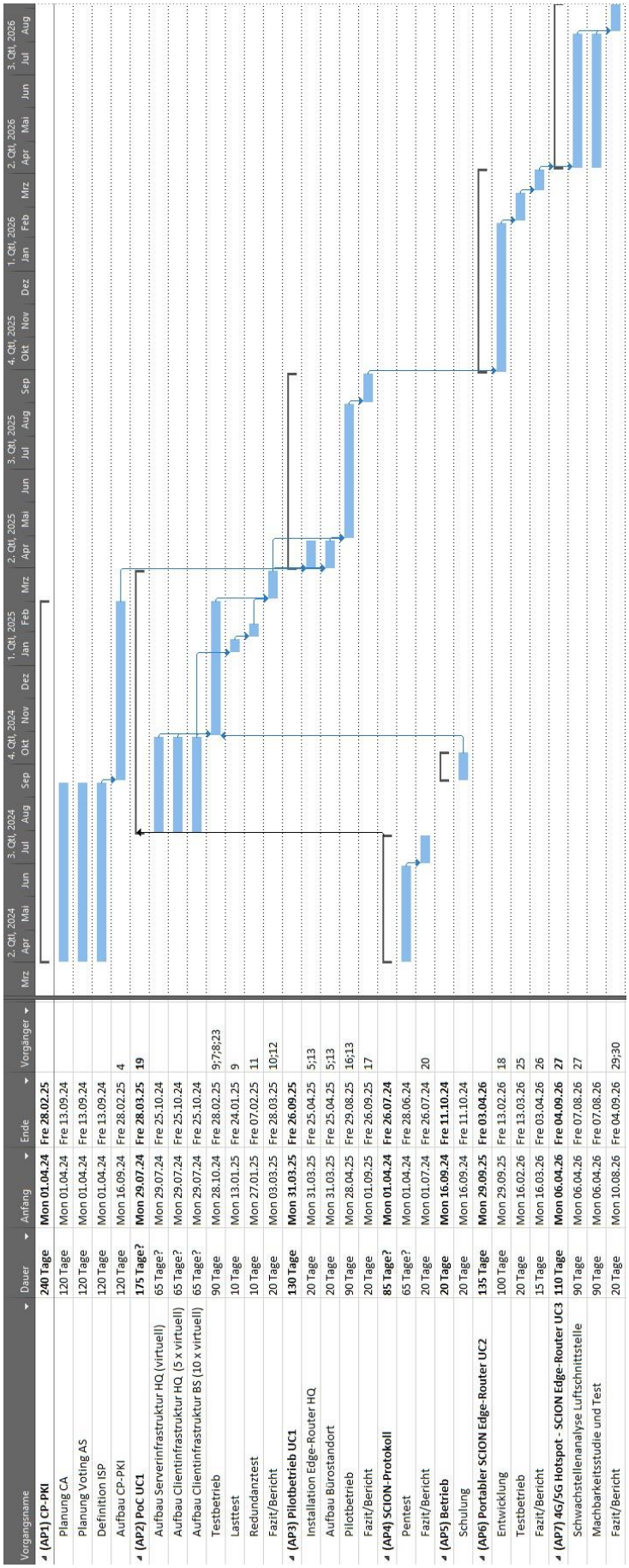

Abbildung 26: Planung Arbeitspakete

Die CP-PKI ist das Kernelement in SCION. Eine gute Planung und Umsetzung ist die Grundlage für einen sicheren und erfolgreichen Betrieb von SCION.

Die Arbeitspakete (vgl. Abbildung 26) sind so gewählt, dass bei einem negativen Ergebnis eines der Pakete, die Folgerbeiten abgebrochen und das Projekt gestoppt werden kann.

9.8 Ausblick

SCION baut mit der TRC auf eine Vertrauensbasis von verschiedenen AS. Dazu gehört auch das Vertrauen zu den ISPs. Eine Erweiterung einer ISD über die Schweizergrenzen erfordert Vertrauen zu ausländischen ISPs. Obschon mit dem SCION-Protokoll die Kontrolle der Routingpfade besteht, kann der Datentransfer mit SCION durch autoritäre Regime führen, welche den Internetverkehr kontrollieren und zensieren. Dabei besteht die Möglichkeit, dass Traffic-Analysen gemacht werden. Obschon die Nutzdaten heute grösstenteils verschlüsselt sind, wird im Datenverkehr nach Mustern gesucht. Auch Metadaten wie IP-Adresse des Senders sowie des Empfängers und Uhrzeit liefern Informationen über eine Kommunikation. Ohne Zusatzmassnahmen ist mit SCION keine Anonymisierung der Routingpfade möglich. Ist dies gefordert, muss dies auf einer anderen Schicht im OSI-Modell erfolgen (s. Kapitel 10.3).

10 Fazit

10.1 Angreifbarkeit

Werden die Schutzmassnahmen für die SCION-Infrastruktur beachtet und konsequent umgesetzt, ist ein Cyberangriff auf die Kommunikationspfade in SCION schwierig. Durch die TRC als Vertrauenskonstrukt einer ISD und der Trennung zwischen Control- und Dataplane müsste eine Mehrfachkompromittierung der SCION CP-PKI erfolgen, dass ein Angriff erfolgreich wäre. Für einen Einsatz wie in UC1 vorgesehen, wird SCION als eine mögliche Variante erachtet. Wird jedoch maximale Sicherheit für die Kommunikationspfade auch für UC2 und UC3 gefordert, müssen die Restrisiken der letzten Meile (vgl. Kapitel 5.3.7) auf ein akzeptables Minimum reduziert werden.

10.2 Aufklärbarkeit

Innerhalb einer ISD sind jedem AS die Pfade der anderen AS bekannt. Auch inter-ISD Informationen sind im SCION Header ersichtlich. Wie im Kapitel 5.3.6 aufgezeigt, sind Informationen zu ISD, AS, IP-Adressen von Edge-Routern und Quell- und Zieladressen von Endsystemen im SCION Underlay ersichtlich. SCION schützt die Integrität in der Kommunikation. Auch die Verfügbarkeit der Kommunikationspfade kann über das Design der SCION-Netzwerkarchitektur sichergestellt werden. Das SCION-Protokoll bietet ohne Zusatzmassnahmen wie ‘hidden path’ oder ‘HORNET’ keine Anonymität in den Kommunikationspfaden und ist mit den entsprechenden Möglichkeiten aufklärbar.

10.3 Anonymität

Die Kommunikationspfade in SCION sind nicht anonym. Jeder Teilnehmer einer ISD kann die Kommunikation zwischen zwei AS mitverfolgen. Wie in Kapitel 5.3.6 beschrieben können bei einem Mittschnitt von Kommunikationsdaten Headerinformationen aus dem SCION- und IP-Protokoll und weitere Metadaten gewonnen werden.

Ein interessanter Ansatz zur Anonymisierung von Internetdatenverkehr liefert HOPR [29]. HOPR ist ein Protokoll, welches vom gleichnamigen Startup entwickelt wurde. Eine Kombination aus einem weltumspannenden Netzwerk von SCION-Knoten und HOPR würden die Kommunikationswege im Internet sicherer und anonymer machen.

10.4 Cybersicherheit

SCION ist nicht das Allerheilmittel, um sämtliche Cyberangriffe verhindern zu können. Aber etwas, was Cyberattacken auf OSI-Layer 1-3 schwieriger macht. Mit SCION kann kein Route-Hijacking mehr gemacht werden, da die Datenpfade kryptografisch abgesichert sind. DDoS-Attacken sind mit SCION immer noch möglich, aber die Durchführung wird schwieriger. Dafür müssten sich sämtliche Systeme in derselben ISD befinden, in welcher der Angriff stattfinden soll. Ein solches Vorhaben würde bei den ISPs vermutlich schnell entdeckt und es könnten Gegenmassnahmen getroffen werden. Ein grösserer Schaden oder längere Systemausfälle könnten wahrscheinlich verhindert werden.

SCION eignet sich für Maschine-zu-Maschine Kommunikation, welche keine menschliche Interaktion erfordert. Auch verteilte private Netze, welche das Internet als Transportnetz nutzen und die Sicherheit der Kommunikationswege eine hohe Wichtigkeit hat, können von SCION profitieren.

Wenn jedoch ein Clientsystem, z.B. im Homeoffice auch eine Verbindung ins Internet hat, ist der Mensch die grösste Schwachstelle im System. Auf einem höheren Layer (4-7) im OSI-Modell verhindert SCION keine Cyberangriffe. Diese müssen mit anderen technischen Methoden überwacht und verhindert werden. Die Sensibilisierung der Menschen im Umgang mit Cyberrisiken bleibt weiterhin bestehen.

Da die SCION Infrastruktur aus Netzwerkkomponenten besteht, welche auf einem Linux-basierten Betriebssystem läuft, muss diese auch gepflegt werden. Werden Schwachstellen im Linux-Kernel, in der SCION-Appliance oder auch in Applikationen bekannt, welche SCION-Dienste nutzen, müssen diese so schnell wie möglich behoben werden. Auch hier birgt der Mensch durch Nachlässigkeit die grösste Gefahr.

10.5 Wirtschaftliche Risiken

Je spezifischer (kleiner) eine ISD definiert wird, umso weniger wird diese bei einem ISP skalieren. Dadurch werden die Betriebskosten höher, was Auswirkungen auf den Preis für den Kunden hat. Deshalb muss eine Erschliessung von Bürostandorten technologieneutral betrachtet werden. Es existieren weitere Lösungen auf dem Markt, wie MPLS, Mietleitungen, Darkfiber oder SD-WAN mit all ihren Vor- und Nachteilen. Diese sollen verglichen und gegeneinander abgewogen werden. Schlussendlich soll die beste Lösung für die spezifische Anwendung gewählt werden.

Zurzeit ist die Standardisierung von SCION in der Internet Engineering Task Force (IETF) am Laufen. Falls sich SCION als neuer Internetstandard durchsetzen wird, werden weitere Netzwerkausrüster den SCION-Stack in ihrer Hardware implementieren und das Angebot an SCION-fähiger Netzwerkausrüstung wird sich auf dem Telekommarkt vergrössern. Sollte dies jedoch nicht der Fall sein, sind die dafür aufgewendeten finanziellen Mittel verloren.

11 Persönliche Erfahrungen

Um SCION vollständig zu verstehen, reich die Zeit von einem halben Jahr für eine Masterthesis nicht aus. Allein der Aufbau einer PKI ist ein komplexes und umfangreiches Gebiet, welches genügend Inhalt für eine Masterthesis liefert.
Es muss bekannt sein, für welches Einsatzgebiet SCION verwendet werden soll. Die Netzwerkarchitektur kann sich je nach Anwendung erheblich unterscheiden. Ob zum Beispiel eine ISD einzig mit Schweizer ISPs gebildet wird, oder ob grenzüberschreitende Kommunikation notwendig ist, welche auch über ausländische Provider erfolgt.

Aus den Gesprächen mit Experten anderer Firmen und Bereichen der Bundesverwaltung merkt man, dass das Bedürfnis für ein sichereres Internet vorhanden ist. Jeder Kontakt mit Gleichgesinnten öffnet wieder neue Kontakte zu anderen Personen, welche sich mit dem Thema SCION auseinandersetzen.

Als während dem Verlauf der Masterthesis bekannt wurde, dass das Labor für den PoC nicht rechtzeitig bereit ist, war gut, dass ein Plan B vorhanden war. Es konnten zwar nicht alle drei Anwendungsfälle im Labor getestet werden. Zudem unterscheidet sich der im Labor getestete Anwendungsfall UC1 in Teilen vom Aufbau des PoC. Aber aus den Expertengesprächen und den persönlichen Erfahrungen aus den Labortests konnten die theoretischen Schlüsse zu den Anwendungsfällen UC2 und UC3 gemacht werden.

Das SCION Labor vom Cyber-Defence Campus umfasst vier physische Standorte mit je einem Edge-Router. Diese werden aktuell noch von Anapaya betrieben. Aufgrund der Komplexität der Konfiguration eines SCION Edge-Routers wurden von mir keine Änderungen am Routing vorgenommen. Aus den Expertengesprächen kam heraus, dass an der Bedienung und dem Management von SCION-Komponenten für die Marktreife noch gearbeitet werden muss. Dies wird sich hoffentlich in den nächsten Jahren ändern, sobald Hardwarehersteller dedizierte SCION-Hardware entwickeln und auf den Markt bringen.

12 Abbildungsverzeichnis

13 Tabellenverzeichnis

14 Abkürzungen

armasuisse W+T ..... *armasuisse Wissenschaft und Technologie*
AS ..... *Autonomous System*
BGP ..... *Border Gateway Protocol*
BGPsec ..... *Border Gateway Protocol Security*
BGPv4 ..... *Border Gateway Protocol Version 4*
BIOS ..... *Basic Input/Output System*
BS ..... *Bürostandort*
BSI ..... *Bundesamt für Sicherheit in der Informationstechnik*
CA ..... *Certification Authority, Certificate Authority*
CIA ..... *Confidentiality, Integrity, Avaliability*
CP ..... *Control Plane*
CP-PKI ..... *Control Plane Public Key Infrastructure*
DDoS ..... *Distributed Denial of Service*
DP ..... *Data Plane*
HF ..... *Hop Field*
HORNET ..... *High-speed Onion Routing at the Network Layer*
HQ ..... *Hauptquartier*
HSM ..... *Hardware Security Module*
IETF ..... *Internet Engineering Task Force*
IP z ..... *Internet Protocol*
IPv6 ..... *Internet Protocol Version 6*
ISD ..... *Isolation Domain*
ISO ..... *International Standardisation Organisation*
ISP ..... *Internet Service Provider*
Kdo Cy ..... *Kommando Cyber*
LAN ..... *Local Area Network*
MITM ..... *Man-in-the-Middle*
MPLS ..... *Multiprotocol Label Switching*
NIST ..... *National Institute of Standards and Technology*
OSI ..... *Open System Interconnect*
PCB ..... *Path-Segment Construction Beacons*
PKI ..... *Public Key Infrastructure*
PoC ..... *Proof of Concept*
RIPE ..... *Réseaux IP Européen*
RPKI ..... *Resource Public Key Infrastructure*
SCION ..... *Scalability, Control and Isolation on Next-Generation Networks*
SD-WAN ..... *Software Defined Wide Area Network*
SIG ..... *SCION-IP Gateway*
SNB ..... *Schweizerische Nationalbank*
SSFN ..... *Swiss Secure Finance Network*
SSH ..... *Secure Shell*
TAP ..... *Test Access Point*
TLS ..... *Transport Layer Security*
TOR ..... *The Onion Router*
TRC ..... *Trust Root Configuration, Trust Root Configuration*
UC ..... *Use Case*
UDP ..... *User Datagram Protocol*
UEFI ..... *Unified Extensible Firmware Interface*
VPN ..... *Virtual Private Network*
VRRP ..... *Virtual Router Redundancy Protocol*
WAN ..... *Wide Area Network*

15 Glossar

armasuisse W+T:

armasuisse Wissenschaft und Technologie ist das Technologiezentrum des VBS und bietet Forschungsdienstleistungen in Wissenschaft, Technologie, Innovation, Erprobung, Robotik, Cyber, Sensorik, Ballistik, Forschung, Simulation, Munition, Explosives und Weltraum an.
https://ch.linkedin.com/showcase/armasuisse-w-t

Kdo Cy:

«Der Auftrag des Kommandos Cyber (Kdo Cy) innerhalb der Armee ist der Schutz der IKT-Infrastruktur der Schweizer Armee gegen Cyberangriffe. Das militärische Kommando steht unter der Führung von Divisionär Simon Müller. Es übernimmt den Status eines Bundesamtes von der Führungsunterstützungsbasis, die Ende 2023 aufgelöst wurde. Die Stelle verantwortet – im gesamten Aufgabenspektrum der Armee – permanent die operationellen Fähigkeiten in den Bereichen Eigenschutz im Cyber- und elektromagnetischen Raum (CER), Lageverständnis und vernetzte Führung, robuste und sichere Datenbearbeitung sowie Aktionen im CER.

Das Kommando Cyber überwacht die Lage im CER im Alltag, bei Einsätzen und in Krisensituationen. Es sorgt dafür, dass die Armee ihre Mittel zur richtigen Zeit und am richtigen Ort, mit einem Wissens- und Entscheidvorsprung einsetzen kann, um eine optimale Wirkung zu erzielen.»

(Medienmitteilung 28.12.2023)
https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-99573.html

16 Literaturverzeichnis

[1] L. Chuat, M. Legner, D. Basin, D. Hausheer, S. Hitz, und A. Perrig, *The Complete Guide to SCION*. in Information Security and Cryptography. Cham: Springer, 2022. [Online]. Verfügbar unter: https://link.springer.com/book/10.1007/978-3-031-05288-0

[2] L. Keller und S. Gilgen, „Inter Domain Routing“, in *Communication Systems III*, B. Stiller, T. Bocek, F. Hecht, C. Morariu, P. Racz, A. Vancea, und M. Waldburger, Hrsg., in Technical Report. , Zürich: Department of Informatics (IFI), 2009, S. 83–106. Zugegriffen: 15. November 2023. [Online]. Verfügbar unter: https://files.ifi.uzh.ch/hkunz/techreports/TR-2009/ifi-2009.03.pdf#page=83

[3] J. Gessner, „Leveraging Application Layer Path-Awareness with SCION“, S. 93 p., 2021, doi: 10.3929/ETHZ-B-000512601.

[4] „Snapshot“. Zugegriffen: 15. November 2023. [Online]. Verfügbar unter: https://ethz.ch/staffnet/de/news-und-veranstaltungen/intern-aktuell/archiv/2022/01/das-sichere-internet-scion-erreicht-den-arbeitsalltag.html

[5] Anapaya, „SCION Overview — SCION documentation“. Zugegriffen: 3. Dezember 2023. [Online]. Verfügbar unter: https://scion.docs.anapaya.net/en/latest/overview.html

[6] Sunrise Communications AG, „SCION – secure connectivity at multiple locations | Sunrise Business“. Zugegriffen: 2. Dezember 2023. [Online]. Verfügbar unter: https://sunrise.ch/business/de/grossunternehmen/internet-networking/business-wan/scion

[7] E. Faverio, „Müssen wir als Institution, den SCION Edge Router selbst betreiben?“, HIN Support. Zugegriffen: 2. Dezember 2023. [Online]. Verfügbar unter: https://support.hin.ch/de/scion/muessen-wir-als-institution-den-scion-edge-router-selbst-betreiben/

[8] A. Donner und S. Luber, „Was ist das Border Gateway Protocol (BGP)?“, IP-Insider. Zugegriffen: 28. Februar 2024. [Online]. Verfügbar unter: https://www.ip-insider.de/was-ist-das-border-gateway-protocol-bgp-a-804823/

[9] A. Moning und R. Lanz, „Netzwerk-Technologien (Skript CAS Networking & Security)“, 2017.

[10] S. Hitz und H. Züllig, „Anapaya Schulungsunterlagen ICT Warrior Academy“, Juli 2023.

[11] InfoGuard AG, „HIN | InfoGuard - HVR Managed SCION Edge | MSSP“. Zugegriffen: 2. Dezember 2023. [Online]. Verfügbar unter: https://www.infoguard.ch/de/hvr-managed-scion-edge

[12] „SCION Control-Plane PKI“. Zugegriffen: 18. Dezember 2023. [Online]. Verfügbar unter: https://www.ietf.org/id/draft-dekater-scion-pki-04.html

[13] C. de Kater, N. Rustignoli, und A. Perrig, „SCION Overview“, Internet Engineering Task Force, Internet Draft draft-dekater-panrg-scion-overview-03, März 2023. Zugegriffen: 3. Dezember 2023. [Online]. Verfügbar unter: https://datatracker.ietf.org/doc/draft-dekater-panrg-scion-overview-03

[14] „SCION | SCION Association“. Zugegriffen: 22. Dezember 2023. [Online]. Verfügbar unter: https://www.scion.org/scion

[15] „Angriffsvektor versus Angriffsfläche“, Trend Micro. Zugegriffen: 19. Januar 2024. [Online]. Verfügbar unter: https://www.trendmicro.com/de_de/devops/23/b/angriffsvektor-versus-angriffsflache.html

[16] „SCION Internet Architecture“. Zugegriffen: 31. Dezember 2023. [Online]. Verfügbar unter: https://scion-architecture.net/pages/faq/

[17] „Wireshark — SCION documentation“. Zugegriffen: 25. Dezember 2023. [Online]. Verfügbar unter: https://docs.scion.org/en/latest/dev/wireshark.html

[18] „SCION-IP Gateway — SCION documentation“. Zugegriffen: 25. Dezember 2023. [Online]. Verfügbar unter: https://scion.docs.anapaya.net/en/latest/sig.html

[19] *What is Underlay Network and Overlay Network?*, (10. Mai 2022). Zugegriffen: 29. Dezember 2023. [Online Video]. Verfügbar unter: https://www.youtube.com/watch?v=AbImMmhP6kY

[20] „Hidden Paths — SCION documentation“. Zugegriffen: 29. Dezember 2023. [Online]. Verfügbar unter: https://scion.docs.anapaya.net/en/latest/hidden-paths.html#security

[21] C. Chen, D. E. Asoni, D. Barrera, G. Danezis, und A. Perrig, „HORNET: High-speed Onion Routing at the Network Layer“, in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver Colorado USA: ACM, Okt. 2015, S. 1441–1454. doi: 10.1145/2810103.2813628.

[22] M. Blarer, „SCION – Allheilmittel gegen DDoS-Angriffe?“, Oneconsult AG. Zugegriffen: 6. Januar 2024. [Online]. Verfügbar unter: https://www.oneconsult.com/de/blog/scion-allheilmittel-gegen-ddos-angriffe/

[23] „Man-in-the-Middle-Angriff“, *Wikipedia*. 5. Januar 2024. Zugegriffen: 26. Januar 2024. [Online]. Verfügbar unter: https://de.wikipedia.org/w/index.php?title=Man-in-the-Middle-Angriff&oldid=240862245

[24] „Wie funktioniert BGP-Hijacking und warum ist es gefährlich? | Computer Weekly“, ComputerWeekly.de. Zugegriffen: 26. Januar 2024. [Online]. Verfügbar unter: https://www.computerweekly.com/de/tipp/Wie-funktioniert-BGP-Hijacking-und-warum-ist-es-gefaehrlich

[25] R. Inversini, „Linux Hardening (Skript CAS Security Incident Management)“, 2022.

[26] „SD WAN vs. MPLS: Vor- und Nachteile | FS Community“, Knowledge. Zugegriffen: 1. März 2024. [Online]. Verfügbar unter: https://community.fs.com/de/article/sd-wan-vs-mpls-pros-and-cons.html

[27] A. Maurer, „Security Benchmark and Forensics Framework“, 2021.

[28] „Anapaya EDGE — Anapaya Knowledge Base documentation“. Zugegriffen: 28. Januar 2024. [Online]. Verfügbar unter: https://docs.anapaya.net/en/latest/deployment-examples/edge/

[29] H. Association, „HOPR Newsletter | Substack“. Zugegriffen: 30. Januar 2024. [Online]. Verfügbar unter: https://hopr.substack.com/embed

17 Selbständigkeitserklärung

Ich bestätige, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der im Literaturverzeichnis angegebenen Quellen und Hilfsmittel angefertigt habe. Sämtliche Textstellen, die nicht von mir stammen, sind als Zitate gekennzeichnet und mit dem genauen Hinweis auf ihre Herkunft versehen.

Ort, Datum:

Unterschrift: Hager Patrick K0EXVM

Digital unterschrieben von Hager Patrick K0EXVM
Datum: 2024.03.10 20:48:47 +01'00'

18 Anhang

18.1 Fotos Labor UC1


ZRH-CYD-SW3
LAN