THREAT MODELLING (BEDROHUNGSANALYSE)

UNTERNEHMENS- UND SECURITY-ZIELE

Unternehmensziel:

Die TV-Plattform erlaubt es den Kunden Live und Replay Fernsehsendungen im HD-Format anzuschauen.

Security-Ziele:

- Der Stream kann nicht kopiert oder aufgezeichnet werden.
- Nur Kunden des TV-Anbieters können die Inhalte schauen.
- Nach Ablauf einer Frist können die Inhalte nicht mehr wiedergeben werden.
- Zu üblichen Nutzungszeiten ist die Konsumation der Inhalte möglich

ALLGEMEINE INFORMATIONEN

Welche Funktionen stellt das System zu Verfügung?	Es werden TV-Inhalte zur Verfügung gestellt. Diese werden dem Konsumenten verschlüsselt übertragen. Das System ist auch für die Distribution der Entschlüsselungsinformationen verantwortlich.
Wer kann auf das System zugreifen?	Auf das System haben die Kunden des Anbieters Zugriff. Dabei wird beim Anbieter zwischen **Privatkunden** und **Businesskunden** unterschieden. Die **Administratoren**, welche beim Anbieter angestellt sind, haben ebenfalls Zugriff auf das System.
Was verarbeitet das System?	Es werden TV-Inhalte verarbeitet. Zu diesen Inhalten zählen Audio- und Videosignale. Es werden ausserdem Programminformationen und kryptografische Materialien verarbeitet.
Wie arbeitet das System?	Diese Frage wird in unserem Architektur Teil beantwortet.
Was für externe Abhängigkeiten hat das System?	Das TV-Signal wird von UPC und GibSolutions empfangen. Die Programminformationen werden von EPG.Best abgerufen. Als Internetanbieter fungiert Init7.
Welches Service-Level muss das System erfüllen?	Das System ist nur in der Schweiz verfügbar. Es soll nicht Hochverfügbar sein, jedoch soll es zu den üblichen Nutzungszeiten verfügbar sein. (16:00 Uhr – 01:00 Uhr)
Welche Security Requirements oder Security Controls wurden bereits definiert?	- Verfügbarkeit nur im internen Netzwerk möglich. - Externe Verbindungen nur mit HTTPS - Die Webapplikation darf nur gesichert kommunizieren (TLS 1.0 and 1.1) - Die Applikation unterstützt nur sichere Verschlüsselungen (AES mit Schlüssellänge ≥ 128 Bits, kein MD5).

VERMÖGENSWERTE DES SYSTEMS

Das zu untersuchende System beinhaltet folgende Vermögenswerte:

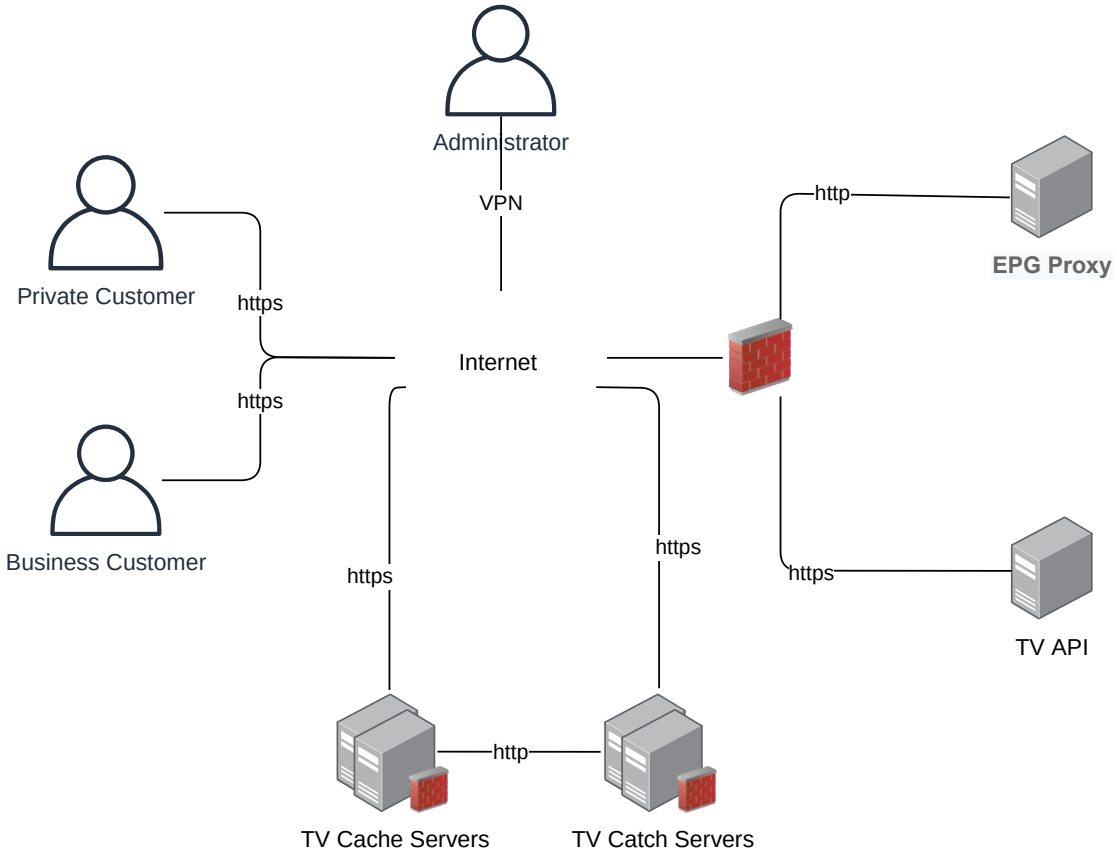
- **Serverseitige Systeme** (Integrität von Systemen und Daten)
- **Chunks und Keys** (Daten)
- **Stream- und Key-Austausch** (Prozesse)
- **Authentifizierungsprozess**
- **Anmeldedaten von Benutzern** (IP-Range)
- **Anmeldedaten des Administrators**
- **Logs**

ANALYSE UND ZERSETZUNG DES SYSTEMS

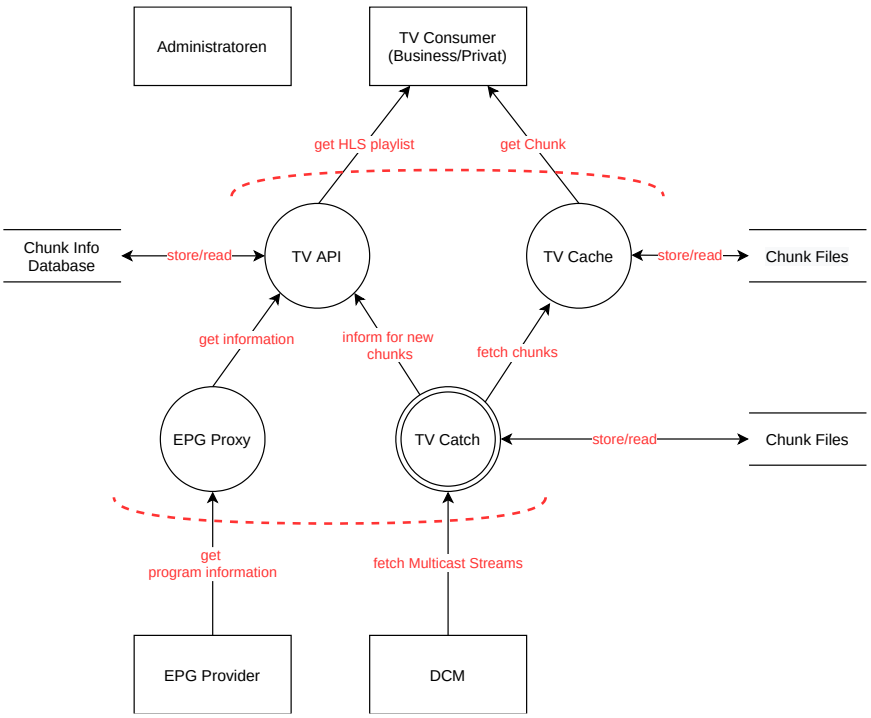
Das System existiert bereits in einem unverschlüsselten Zustand. Wir wollen die Sicherheitslücken des IST-Zustands ermitteln, damit wir auch Verbesserungen der Bestehenden Infrastruktur ermitteln können. In einem zweiten Schritt haben wir noch die von uns erschaffene Architektur analysiert und zersetzt.

IST-ZUSTAND

Den IST-Zustand haben wir mit Informationen aus dem GitLab des bestehenden Codes und Mitarbeitern des TV-Anbieters ermittelt. Der momentane Netzwerkaufbau haben wir in der untenstehenden Grafik visuell dargestellt. Die Cache und Catch Server stehen direkt im Internet und werden jeweils mit einer IPTables Firewall geschützt. Es existieren jeweils mehrere Catch und Cache Server. Die TV API und der EPG Proxy Server werden durch eine virtuelle Firewall mit dem Internet verbunden. Die Benutzer greifen über https auf die TV API und die Cache Server zu.

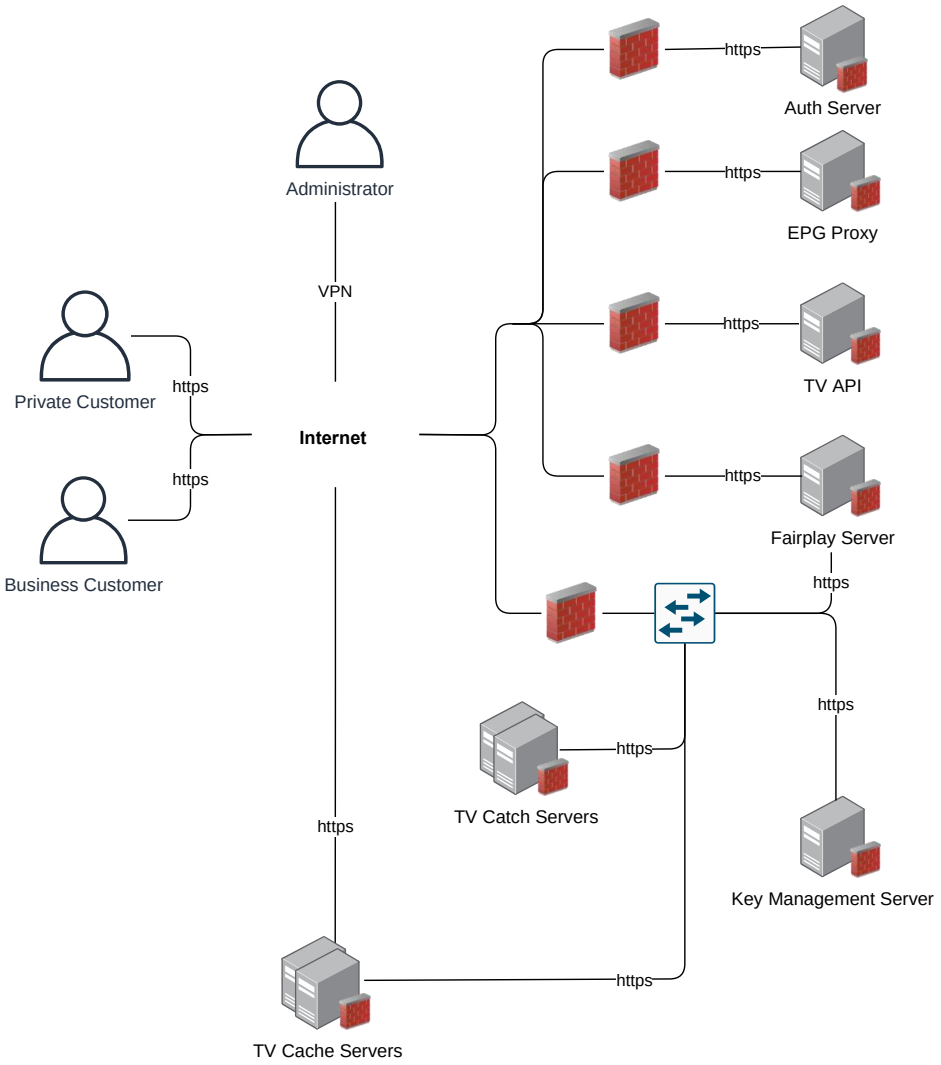


Das Data-Flow-Diagramm konnten wir mithilfe von Informationen aus einer bestehenden Architekturgrafik und der Analyse des Codes erstellen. In dieser Konfiguration ist es dem TV-Konsumenten mit jedem Gerät und Software möglich, den TV-Stream zu schauen. Wie in der Grafik ersichtlich ist, greift er dazu auf die TV API und die Cache Server zu. Diese werden mit Informationen von den Catch Servern und dem EPG Proxy versorgt. Die TV-Inhalte werden von den Multicast Streams der DCM Server geholt. Die Administratoren haben auf alle Services und Server Zugriff. Mit den roten gestrichelten Linien haben wir den vertrauenswürdigen Bereich markiert. Diesen haben wir so gewählt, da diese Bereiche komplett vom TV-Anbieter verwaltetet werden. Sowohl die Server, das Netzwerk und die Software werden vom Anbieter zur Verfügung gestellt.

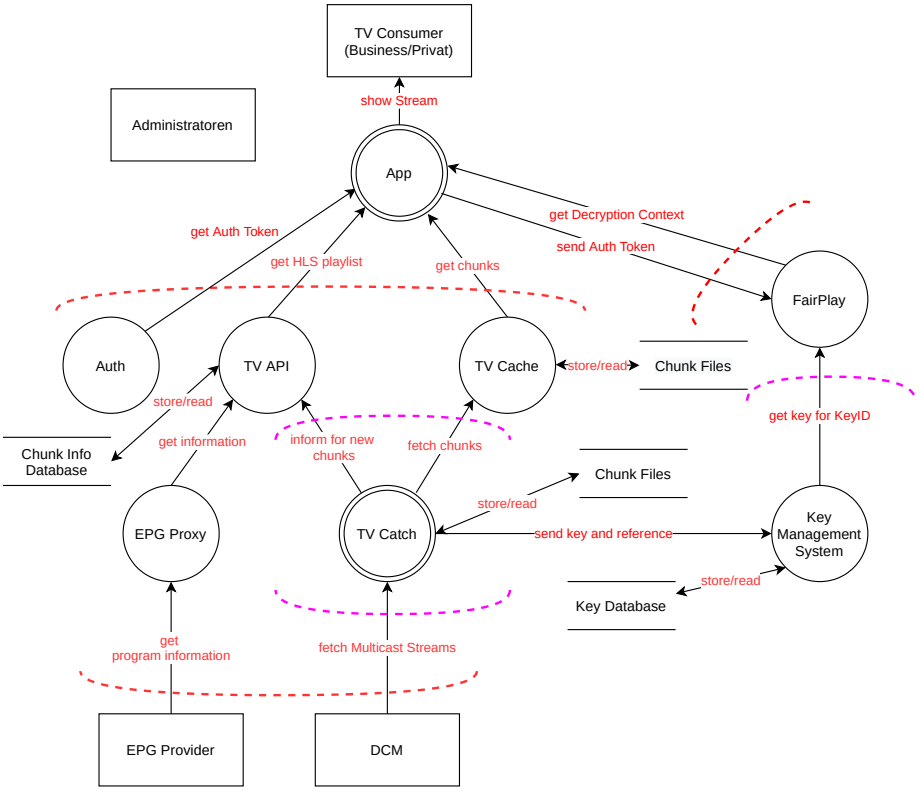


SOLL-ZUSTAND

Im Soll-Zustand haben wir unsere zusätzlichen Server für die neue Architektur eingebunden und auch Anpassungen für die Sicherheit des IST-Zustands integriert. Zu den wichtigsten Änderungen gehört die Umstellung der gesamten Netzwerkverkehrs auf https. Ausserdem ist es nicht notwendig, dass die Catch Server aus dem Internet erreichbar sind. Diese würden wir deshalb zusammen mit dem Key Management Server in ein separiertes Netzwerk nehmen, welches den Zugriff von aussen nicht zulässt. Wie in der untenstehenden Grafik ersichtlich ist, hätten zusätzlich der FairPlay Server und auch die Cache Server Zugriff in dieses abgeschottete Netzwerk. Diese Server sind auf die Kommunikation mit den Catch Server oder dem Key Management Server angewiesen. Eine weitere Änderung ist, dass alle Server mit der IPTables Firewall abgesichert werden sollen.



Im Datenflussdiagramm der neuen Lösung, haben wir die zusätzlichen Services integriert. Dazu gehören der Auth Server, welcher die Authentifizierungstokens ausstellt und die gesamte Key Management Infrastruktur. Eine Neuerung ist ebenfalls, dass der Stream nur noch mit der App vom TV Anbieter angeschaut werden können. Mit der violetten gestrichelten Linie haben wir einen tiefer liegenden Vertrauensbereich geschaffen. Diese Datenflüsse finden im abgeschotteten Netzwerk statt und haben nur mit dem Schlüsselaustausch zu tun.



Threat Agents (Bedrohungsakteure)

Agents	Ziel
Script Kiddies	Sie wollen prüfen, ob sie in der Lage sind das System zu hacken. Ihr einziges Ziel ist Spass.
Mitarbeiter	Ehemalige Mitarbeiter möchten sich rächen oder das System sabotieren, da sie ihren Job verloren haben. Oder sie wollen Profit machen. Ziel: finanzieller Gewinn oder Sabotage.
Cyber Criminal	Sie wollen Malware ins System einschleusen und an User verbreiten. Oder sie möchten Daten verschlüsseln. Ziel: finanzieller Gewinn.
Konkurrenz	Sie wollen das System sabotieren, dem Image schaden und dadurch Kunden zum Wechsel des Anbieters bewegen. Ziel: finanzieller Gewinn und Imageschaden

Unwahrscheinliche Bedrohungsakteure sind: Staaten (keine Motivation), Hacktivisten (keine politische Motivation).

THREATS (BEDROHUNGEN)

Anhand der STRIDE-Methode wurde für jede Kategorie unseres Systems aufgelistet, was schiefgehen kann.

Nr.	Element	Kat.	Beschreibung	Nutzen für Angreifer	Req	Realistisch
T1	TV Konsument	S	Angreifer kann Stream über VPN Technologie an weitere Personen weitergeben.	Unbefugte Personen können den Stream schauen.	R15, R38	Ja
T2		R	Angreifer kann Stream über VPN Technologie an weitere Personen weitergeben.	Unbefugte Personen können den Stream schauen.	-	Nein
T3	DCM	S	Ausgeben als Provider	Kann System mit gefälschten Streams füllen	R10	Nein
T4		R	Ausgeben als Provider	Kann System mit gefälschten Streams füllen	-	Nein
T5	EPG Provider	S	Ausgeben als EPG Proxy (IP)	Angreifer kann EPG Daten erhalten ohne zu bezahlen	R15	Nein
T6		R	Ausgeben als EPG Proxy (IP)	Angreifer kann EPG Daten erhalten ohne zu bezahlen	-	Nein
T7	Get Auth Token	T	Token ersetzen/kaputt machen	Kunde kann kein verschlüsseltes TV schauen (DoS)	R13, R14	Nein
T8		I	Angreifer beschafft sich ein Token.	Angreifer kann verschlüsseltes TV schauen.	R13, R14, R21, R30, R33	Ja
T9		D	DoS auf Auth Server Kommunikation	Kunden können sich nicht mehr authentifizieren.	R3, R4, R5, R6, R11,	Nein
T10	Get HLS Playlist	T	Anpassen der Pfade zu Chunk Files und Keys. Übernahme des Streams	Kunde bekommt falschen Stream. Kunde kann beeinflusst werden. Mediashop Attack	R13, R14	Nein
T11		I	Angreifer ergaunert sich eine oder mehrere Playlisten.	Er kann dadurch die Pfade zu den Chunk-Dateien ermitteln. Ausserdem erhält er Informationen über den Schlüsselwechsel.	R10, R13, R14, R20, R21, R28	Ja
T12		D	DoS auf TV API-Kommunikation	Kunden können kein TV schauen	R5	Nein
T13	Get Chunk	T	Chunks können manipuliert werden.	Kunden können kein TV schauen	R13, R14	Nein
T14		I	Chunks könnten abgegriffen werden.	Dadurch könnte der Angreifer die Chunk Inhalte schauen.	R13, R14, R20,	Ja

					R21, R28	
T15		D	DoS auf Cache-Kommunikation	Kunden können keine Chunks mehr abrufen und können kein TV mehr schauen	R5	Nein
T16	Get Decryption Context	T	Modifizieren des Decryption Context	Kunden können kein verschlüsseltes TV schauen	R13, R14, R18	Nein
T17		I	Decryption Context könnte von einem Angreifer mitgehört werden.	Der Angreifer hätte so Zugriff auf einen oder mehrere Entschlüsselungsschlüssel.	R13, R14, R21, R28, R29, R31, R32	Ja
T18		D	DoS auf Key-Kommunikation	Kunden können keine Schlüssel mehr abrufen und können kein verschlüsseltes TV mehr schauen	R5	Nein
T19	Store/read chunks	T	Chunks können manipuliert werden.	Kunden können kein TV schauen, falsche Informationen bekommen	R13, R14, R18	Nein
T20		I	-			Nein
T21		D	DoS auf Storage	Für einige Sender können Kunden keine Chunks mehr abrufen und kein TV mehr schauen	R5, R18	Nein
T22	Fetch chunks	T	Chunks können manipuliert werden.	Kunden können kein TV schauen, falsche Informationen bekommen	R13, R14, R18	Nein
T23		I	Chunks werden bei der Übertragung mitgeschnitten.	Anreifer kommt an die Chunks und kann die Videostreams schauen	R13, R14, R18, R20, R28	Nein
T24		D	DoS auf Cache/Catch-Kommunikation	Für einige Sender können Kunden keine Chunks mehr abrufen und kein TV mehr schauen	R5, R18	Nein
T25	Inform for new Chunks	T	Chunks können manipuliert werden.	Kunden können kein TV schauen, falsche Informationen bekommen	R12, R13, R14, R28	Nein
T26		I	Angreifer kann sich Informationen über neue Chunks holen	Angreifer kann sich selbst eine Playlist zusammenbauen	R13, R14, R18, R20	Nein
T27		D	DoS auf TV-Spray, verhindern der Kommunikation von catch zu TV API	Für einige Sender können Kunden keine Chunks mehr abrufen und kein TV mehr schauen	R5, R18	Nein

T28	Get Information from EPG Proxy	T	EPG kann manipuliert werden.	Replay kann unmöglich werden, falsche Programminformationen beim Kunden	R13, R14, R10	Nein
T29		I	EPG könnte vom Angreifer abgegriffen werden.	EPG könnte ohne Bezahlung abgerufen werden.	R13, R14, R18, R28	Nein
T30		D	DoS auf EPG Proxy	Kein direkter Effekt	R5	Nein
T31	Send key and reference	T	Senden falscher Keys.	Kunden können kein verschlüsseltes TV schauen	R12, R13, R14, R18, R28	Nein
T32		I	Key und KeyID könnten von einem Angreifer mitgehört werden.	Der Angreifer hätte so Zugriff auf einen oder mehrere Entschlüsselungsschlüssel.	R13, R14, R18, R29, R31, R32	Ja
T33		D	Verhindern des senden der Key-Informationen	Für einige Sender können Kunden keine Keys beziehen und bis repariert kein TV schauen	R1, R5, R18	Nein
T34	Store/read Key	T	Senden falscher Keys.	Kunden können kein verschlüsseltes TV schauen	R12, R28	Nein
T35		I	-	-	-	Nein
T36		D	Verhindern des Zugriffs auf die Key-Datenbank	Kunden können keine Schlüssel mehr abrufen und können kein verschlüsseltes TV mehr schauen	R3, R5	Nein
T37	Get key for KeyID	T	Senden falscher Keys.	Kunden können kein verschlüsseltes TV schauen	R12, R13, R14, R18, R28	Nein
T38		I	Key und KeyID könnten von einem Angreifer mitgehört werden.	Der Angreifer hätte so Zugriff auf einen oder mehrere Entschlüsselungsschlüssel.	R13, R14, R18, R29, R31, R32	Ja
T39		D	Verhindern der Kommunikation mit dem Key Server	Kunden können keine Schlüssel mehr abrufen und können kein verschlüsseltes TV mehr schauen	R5, R18	Nein
T40	Fetch Multicast Stream	T	Sende gefälschten MC-Stream	Kunden erhalten falsche Informationen.	R12, R18	Nein
T41		I	TV-Multicast könnte von Angreifer abgegriffen werden.	Angreifer kann kostenlos TV schauen.	R10	Nein

T42		D	DoS auf Multicast Stream Kommunikation. Ausfall beim Provider	Es können keine Chunk Files mehr generiert werden. Dadurch gibt es kein Live TV und keine Aufzeichnung zu diesem Zeitpunkt	R2, R5	Ja
T43	Get program information	T	Bereitstellen von gefälschten EPG Daten	Replay kann unmöglich werden, falsche Programminformationen beim Kunden	R13, R14	Nein
T44		I	EPG könnte vom Angreifer abgegriffen werden.	EPG könnte ohne Bezahlung abgerufen werden.	R13, R14, R18, R28	Nein
T45		D	DoS auf Kommunikation zum EPG Provider oder Ausfall des EPG Providers	Es können keine Programminformationen mehr zur Verfügung gestellt werden. Keine grosse Auswirkung	R2, R5	Ja
T46	Chunk Files	T	Chunks können manipuliert werden.	Kunden können kein TV schauen, falsche Informationen bekommen	R12, R13, R14, R18, R16, R17, R35	Nein
T47		R	Chunks können manipuliert werden.	Kunden können kein TV schauen, falsche Informationen bekommen	R39, R40	Nein
T48		I	Angreifer kann Chunks auslesen.	Der Angreifer kann sich einen Stream zusammenbauen.	R11, R12, R15, R16, R17, R19, R20	Nein
T49		D	Ausfall der Disks	Es ist nicht möglich TV zu schauen.	R7	Nein
T50	Key Database	T	Anpassen der Keys oder KeyIDs.	Kunden können kein verschlüsseltes TV schauen	R12, R16, R17, R18	Nein
T51		R	Unbemerktes anpassen der Keys oder KeyIDs.	Angreifer kann TV-Wiedergabe verunmöglichen.	R39, R40, R41	Nein
T52		I	Key und Key ID können ausgelesen werden	Angreifer kann verschlüsseltes TV schauen	R11, R12, R15, R16, R17, R18, R19, R34, R35, R36	Ja

T53		D	Ausfall der Datenbank oder erhöhtes Anfrageaufkommen	Der Zugriff auf die Datenbank ist nicht mehr möglich. Die Schlüssel können nicht mehr gespeichert werden und es kommt zu einem Ausfall beim Recording.	R1, R7, R18	Nein
T54	Auth Server	S	Durch IP-Spoofing kann man ein Token erhalten	Der Angreifer hat dadurch Zugriff auf das TV System und kann die Inhalte konsumieren, obwohl er kein Kunde ist.	R10	Nein
T55		T	Code anpassen und Authentifizierung aushebeln oder verschärfen.	Jeder kann konsumieren oder keiner kann konsumieren.	R5, R8, R9, R11, R12, R16, R17, R18	Nein
T56		R	Angreifer kann unbemerkt ein Token fälschen oder den Code verändern.	Er kann auf alles zugreifen oder machen was er will.	R39, R40, R42	Nein
T57		I	Signierungsschlüssel kann geklaut werden.	Ein Angreifer kann sich selbst Tokens ausstellen.	R11, R12, R16, R17, R18, R19, R29, R34, R35, R36	Ja
T58		D	DoS auf Auth Server/Software	Kunden können sich nicht mehr authentifizieren.	R3, R4, R5, R6	Ja
T59		E	Broken Access Control oder fehlerhafte Algorithmen könnten dazu führen, dass sich ein Angreifer ein Access Token generieren kann, obwohl er keine Berechtigung dazu hat.	Der Angreifer hat dadurch Zugriff auf das TV System und kann die Inhalte konsumieren, obwohl er kein Kunde ist.	R5, R8, R9	Nein
T60	TV API	S	Gestohlenes Catch-Token IP Spoofing	Möglichkeit Chunk/Sender und EPG Daten zu modifizieren Zugriff auf Streams ohne Kunde zu sein	R10, R21, R20	Nein
T61		T	Modifizieren der Chunk-Informationen und Key Referenzen	Flasche Streams bereitstellen, Streams löschen, Verschlüsselung aufheben, Verschlüsselung erzwingen.	R5, R8, R9, R11, R12, R16, R17	Nein

T62		R	Angreifer kann unbemerkt den Code/Daten verändern.	Er kann unbemerkt falsche Streams verbreiten. (Mediashop Attack)	R39, R40, R41	Nein
T63		I	Kann Meta-Information über Chunks und Keys auslesen.	Angreifer kann sich seine Playlist selbst zusammenstellen.	R8, R9, R10, R11, R12, R15, R16, R17, R19, R20, R21, R35, R36	
T64		D	DoS auf TV API Server/ Software	Kunden können keine Playlists mehr herunterladen und können nicht mehr auf die TV-Inhalte zugreifen.	R3, R4, R5, R6	Ja
T65		E	Broken Access Control SSH Zugriff mit Brute Force/Exploit im SSH Server	Möglichkeit Chunk/Sender und EPG Daten zu modifizieren oder das System zu übernehmen	R5, R8, R11, R12	Nein
T66	TV Cache	S	Mit einer Man-in-the-Middle Attacke könnte sich ein Angreifer sich als Catch Server ausgeben.	Der Angreifer kann so den Inhalt des Streams anpassen und so Werbung oder andere Inhalte verbreiten.	R5, R18	Nein
T67		T	Chunks können manipuliert werden.	Kunden können kein TV schauen, falsche Informationen bekommen	R5, R8, R9, R12, R16, R17	Nein
T68		R	Angreifer kann unbemerkt die Config/Chunks verändern.	Er kann auf alles zugreifen oder machen was er will.	R39, R40, R41	Nein
T69		I	Chunk Dateien können abgerufen werden.	Der Angreifer kann TV Streams schauen.	R11, R12, R15, R16, R17, R19, R20, R21	Ja
T70		D	DoS auf TV Cache Server/ Software	Es gibt mehrere Cache Server. Wenn es einen Ausfall gibt, hat dies keine Auswirkungen. Die Cacheserver laufen redundant. Falls jedoch zwei Server mit den gleichen Inhalten ausfallen, gibt es einen Ausfall bei einem Teil der Sender.	R3, R4, R5, R6	Ja

T71		E	Mit einer Brute-Force Attacke könnte sich ein Angreifer Zugriff auf den Server verschaffen. Da keine Zugriffssteuerung existiert, kann ein Angreifer auf alle Chunks zugreifen.	Er könnte die TV-Inhalte ohne Erlaubnis konsumieren, wenn die Namen der Chunks herausfindet. Er könnte sich Adminrechte verschaffen und den Server zweckentfremden. (Cryptomining, Datenzugriff)	R5, R11, R12, R20, R21	Nein
T72	TV Catch	S	Gestohlener SSH Zugriff Man-in-the-Middle zu Key Server	Er könnte sich Adminrechte verschaffen und den Server zweckentfremden. (Cryptomining, Datenzugriff) und kann die aufgezeichneten Chunks bearbeiten. Der Angreifer kommt an das Key-Material.	R10, R16, R17, R18, R22	Nein
T73		T	Manipulation des Key-Generators, damit dieser einfache oder bekannte Keys generiert.	Der Angreifer könnte so einfach an die Schlüssel kommen. Kunden können je nach Anpassung kein TV schauen	R5, R8, R9, R11, R12, R16, R17, R18	Nein
T74		R	Angreifer kann unbemerkt die Config/Chunks verändern. Angreifer kann unbemerkt Key stehlen.	Er kann auf alles zugreifen oder machen was er will.	R39, R40, R41	Nein
T75		I	Die Schlüssel des Key Generators könnten abgegriffen werden. Chunk Dateien können abgerufen werden.	Mit den Schlüsseln und den Referenzen kann der Angreifer die Streams entschlüsseln. Der Angreifer kann an die Chunks kommen.	R11, R12, R15, R16, R17, R18, R19, R20, R21, R22, R32, R33	Nein
T76		D	DoS auf TV Catch Server/ Software	Die Catch Server laufen nicht redundant, deshalb kommt es zu einem Teilausfall bei den Sendern. Es gibt ausserdem beim Recording eine Lücke.	R3, R4, R5, R6, R18	Nein
T77		E	Mit einer Brute-Force Attacke könnte sich ein Angreifer Zugriff auf den Server verschaffen.	Er könnte sich Adminrechte verschaffen und den Server zweckentfremden. (Cryptomining, Datenzugriff, Datenlöschung)	R5, R11, R12, R18	Nein
T78	EPG Proxy	S	Gestohlener SSH Zugriff	Er könnte sich Adminrechte verschaffen und den Server	R5, R11, R15,	Nein

				zweckentfremden. (Cryptomining, Datenzugriff)	R16, R17	
T79		T	Bereitstellen von gefälschten EPG Daten oder keinen Daten	Replay kann unmöglich werden, falsche Programminformationen beim Kunden	R5, R8, R9, R11, R12, R16, R17, R18	Nein
T80		R	Angreifer kann unbemerkt die Config/EPG Daten verändern.	Er kann auf die Programm Informationen zugreifen.	R39, R40, R41	Nein
T81		I	EPG könnte vom Angreifer abgegriffen werden.	EPG könnte ohne Bezahlung abgerufen werden.	R8, R9, R11, R12, R15, R16, R17, R35	Nein
T82		D	EPG Proxy nicht verfügbar	TV API kann EPG nicht laden. Keine direkte Auswirkung.	R5	Nein
T83		E	Mit einer Brute-Force Attacke könnte sich ein Angreifer Zugriff auf den Server verschaffen.	Er könnte sich Adminrechte verschaffen und den Server zweckentfremden. (Cryptomining, Datenzugriff)	R5, R11, R12	Ja
T84	Key Management System	S	Gestohlenes Token	Manipulation Key-Material möglich	R18	
T85		T	Löschung oder Verteilung der Keys kann manipuliert werden.	Ein Angreifer könnte sich so die Keys beschaffen oder auch die Löschung verhindern. Damit könnte er alle Chunks entschlüsseln. Er kann aber auch Wiedergabe verschlüsselter Kanäle verhindern	R5, R8, R9, R11, R12, R16, R17, R18	Nein
T86		R	Angreifer kann unbemerkt den Code/Config anpassen.	Er kann den Betrieb beeinträchtigen.	R39, R40, R41	Nein
T87		I	Schlüssel und Key Referenzen könnten abgegriffen werden	Der Angreifer könnte alle Streams entschlüsseln.	R8, R9, R11 R12, R15, R16, R17, R18, R19, R32, R33, R34,	Ja

					R35, R36	
T88		D	DoS auf Key Management Server/ Software	Wenn das Key Management System ausfällt, können keine Schlüssel mehr abgerufen werden. Dadurch können keine verschlüsselte TV-Inhalte mehr konsumiert werden.	R3, R4, R5, R6, R18	Nein
T89		E	Mit einer Brute-Force Attacke könnte sich ein Angreifer Zugriff auf den Server verschaffen.	Ein Angreifer kann verschlüsselte Streams entschlüsseln. Er könnte sich Adminrechte verschaffen und den Server zweckentfremden. (Cryptomining, Datenzugriff)	R5, R8, R11, R12, R18	Nein
T90	FairPlay	S	Durch die Fälschung des Authentifizierungstokens kann sich jemand die Inhalte anschauen, ohne dass er dazu berechtigt ist.	Er kann sich die TV-Inhalte anschauen, ohne dass er dafür ein Kunde sein muss.	R5, R8	Ja
T91		T	Keys können beliebig ausgegeben oder die Ausgabe komplett verhindert werde	Ein Angreifer könnte sich so die Keys beschaffen oder auch die Löschung verhindern. Damit könnte er alle Chunks entschlüsseln. Er kann aber auch Wiedergabe verschlüsselter Kanäle verhindern.	R5, R8, R9, R11, R12, R16, R17, R18	Nein
T92		R	Angreifer kann unbemerkt die Config/Code verändern.	Er kann den Betrieb beeinträchtigen.	R39, R40, R41	Nein
T93		I	Angreifer kann sich die Authentifizierung für den Keyserver holen.	Der Angreifer könnte alle Streams entschlüsseln.	R8, R9, R11, R12, R15, R16, R17, R19, R32, R33, R34, R35, R36	Ja
T94		D	FairPlay Server nicht verfügbar	Kunden, welche auf FairPlay angewiesen sind (Apple) können kein verschlüsseltes TV schauen.	R3, R4, R5, R6	Ja
T95		E	Broken Access Control Mit einer Brute-Force Attacke könnte sich ein Angreifer Zugriff auf den Server verschaffen.	Ein Angreifer kann verschlüsselte Streams entschlüsseln.	R5, R8, R11, R12	Nein

				Er könnte sich Adminrechte verschaffen und den Server zweckentfremden. (Cryptomining, Datenzugriff)		
T96	Administratoren	S	Man-in-the-Middle / Social Hacking / Phishing	Die Kennwörter für die Server können so herausgefunden werden. Mit diesen Informationen ist der Zugriff auf das gesamte System möglich. Ausserdem könnte sich jemand als Chef oder System ausgeben und beim Administrator Informationen holen. (Phising, Social Hacking)	R13, R14, R16, R17, R19	Ja
T97		R	Social Hacking/ Phishing	Kann mit den Zugriffsdaten Streams stehlen und den Betrieb beeinträchtigen.	R39, R40, R41, R43	Nein
T98	App	S	App mit ähnlichen Namen im App Store aufschalten	Gewisse Benutzer könnten das falsche App herunterladen.	R23, R26	Ja
T99		T	Manipulation des Apps durch Updates	Defektes App oder Kontrolle übernehmen.	R23, R25	Nein
T100		R	Ein Entwickler kann bösartigen Code veröffentlichen.	Er kann dadurch den Betrieb beeinträchtigen oder Kunden angreifen.	R9, R42	Nein
T101		I	Angreifer kann an Schlüssel und Streams kommen.	Angreifer kann Streams aufzeichnen.	R3, R27, R37	Ja
T102		D	App store dazu bringen, App zu löschen (Copyright claim?)	Kunden können App nicht erhalten	R24	Nein
T103		E	Root Rechte auf dem Gerät holen.	Dadurch kann der Angreifer auf Daten vom App und DRM System zugreifen. Mögliche Entschlüsselung	R27	Ja
T104	Show Stream	T	Man-in-the-Middle	Kann App mit gefälschten Streams füllen (Schnauz auf Fernseher)	R13, R14	Nein
T105		I	Abfilmen des Displays	Angreifer kann Stream aufzeichnen.	-	Ja
T106	Send Auth Token	T	Der Angreifer könnte sich so ein unendliches Auth Token generieren. Oder eine andere IP-Adresse angeben.	Nutzer können Streams schauen, die sie nicht dürfen oder können gewisse verschlüsselte Streams nicht schauen.	R13, R14, R29, R30	Ja
T107		I	Der Angreifer kann sich ein Token ergaunern.	Dadurch kann der Angreifer unerlaubt Streams abrufen.	R13, R14, R30	Ja
T108		D	Kommunikation mit Tokens kann überlastet werden.	Kein Kunde kann sich mehr authentifizieren.	R3, R4, R5,	Nein

					R6, R7	
T109	Chunk Info Database	T	Chunk Metadaten könnten verändert werden.	Dadurch ist die Konsumation von TV Streams nicht mehr möglich oder kann beeinflusst werden. (Mediashop Attack)	R11, R12, R15, R16, R17, R18, R19, R35, R36	Nein
T110		R	Unbemerktes anpassen der Chunk- oder EPG-Informationen.	Angreifer kann falsche Informationen verbreiten.	R39, R40, R41	Nein
T111		I	Chunk Metadaten können abgerufen werden.	Der Angreifer kann sich selbst eine Playlist zusammenstellen.	R8, R9, R11, R12, R15, R16, R17, R19, R20, R21, R35, R36	Nein
T112		D	Datenbank nicht verfügbar	Kunden können keine Playlists mehr herunterladen und können nicht mehr auf die TV-Inhalte zugreifen.	R3, R4, R5, R6	Ja

MITIGATION (SCHADENSBEGRENZUNG)

Nachfolgend werden die Massnahmen beschrieben, die die obengenannten Bedrohungen abschwächen bzw. die Ausnutzung von diesen schwierig machen.

Nr.	Beschreibung
R1	Der Key Generator muss die Keys so lange behalten, bis sie erfolgreich an den Key Server gesendet wurden.
R2	Redundanz schaffen, indem mehrere Anbieter für den gleichen Dienst verwendet werden.
R3	Mehrere Instanzen des Systems für Hochverfügbarkeit/Redundanz aufschalten.
R4	Einsatz von selbstheilenden Systemen mit Orchestrierung. (Benötigt ausserdem den Einsatz von Health Checks)
R5	Verwendung von Monitoring und Alarmierung.
R6	Einsatz von Metric collection und Autoscaling.
R7	Einsatz von redundanten Speichersystemen. (RAID, Ceph, Object-Storage, Datenbank-Cluster)
R8	Für Algorithmen und bekannte Implementierung wird auf bewährte Bibliotheken zurückgegriffen. (Keine Fehler durch eigenen Code)
R9	Durchführen von Code- und Konfig-Reviews. (automatisiert und manuell)
R10	Kontrolle des kompletten Kommunikationswegs, um Netzwerk-Spoofing zu verhindern.
R11	Limitierung der Anzahl Loginversuche pro Zeiteinheit.
R12	Einsatz einer Firewall (White- und Blacklisting, Portsperrung) Nur Ports und Verbindungen freigeben, welche auch verwendet werden.
R13	Einsatz von http Public Key Pinning, um Man-in-the-Middle Attacken zu verhindern.
R14	Kommunikation findet nur per TLS statt.
R15	Aktivierung verstärkter Authentifizierung (Benutzername/Passwort, Kennwortrichtlinien, Token, 2FA)
R16	Sensibilisierung der Administratoren auf Phishing und Social Hacking.
R17	Administratoren gezielt auswählen. Soviel wie nötig, so wenig wie möglich.
R18	Abgeschottetes Netzwerk ohne Zugriff von aussen (nur per Jump Host)
R19	Externer Zugriff von Administratoren nur mit 2-Faktor Authentifizierung zulassen.
R20	Chunk Dateien müssen verschlüsselt werden.
R21	Zugriff auf die Ressourcen und Server nur im Init7 Kundennetzwerk zulassen.
R22	Gespeicherte Keys werden nach Rotation gelöscht.
R23	Apps signieren.
R24	App auch auf Website anbieten.
R25	Apps nur aus offiziellem Store unterstützen.
R26	Apps regelmässig im Store überprüfen und Nachahmer den Storebetreibern melden.
R27	Root-Rechte/Jailbreak auf den Endgeräten erkennen und Betrieb der App verweigern.
R28	Datenübertragung muss authentifiziert sein.
R29	Schlüssel werden periodisch rotiert.
R30	Quelladresse im Request Header mit Inhalt des JWT Tokens abgleichen.
R31	Schlüsselaustausch findet nur verschlüsselt statt.
R32	Es werden pro TV-Sender verschiedene Keys verwendet.
R33	Key oder Token hat nur eine begrenzte Lebensdauer.

R34	Keys verschlüsselt in der Datenbank speichern.
R35	Für die Dienste und die Datenzugriffe werden nur Serviceuser mit begrenzten Zugriffsrechten verwendet.
R36	Verhindern von SQL-Injection durch die Verwendung von Prepared Statements.
R37	Einsatz von DRM-Lösungen, welche für die jeweiligen Endgeräte vorgesehen sind.
R38	Einschränken der Anzahl gleichzeitige Sessions/Logins.
R39	Es gibt keine geteilten Administratoren Logins, sondern nur personalisierte Logins.
R40	Zentralisierte (Applikations-)Log-Collection, kein bearbeiten der Admins.
R41	Datenbankadministratoren dürfen keinen Admin-Zugriff auf dem System haben.
R42	Arbeit mit Versionsverwaltung (Bsp. Git) und Continous Deployment.
R43	Ablauf der Administratoren Kennwörter nach einer gewissen Dauer.