Projektauftrag

VoIP Secure

Auftraggeber	Netstream AG, CFO Dominik
Projektleiter	Grassi Giuliano
Autor	Grassi Giuliano
Klassifizierung	Vertraulich
Status	Zur Prüfung

Änderungsverzeichnis

Datum	Version	Änderung	Autor
10.11.2013	0.1	Ausgangslage,Ziele, Lösungsbeschreibung, Stategie, Gesetz	Grassi G.
25.11.2013	0.2	Risiken, Nutzwertanalyse, Organisation	Grassi G.
30.11.2013	1.0	Abschluss	Grassi G.

Inhaltsverzeichnis

1 Ausgangslage

Hinter netvoip.ch steht ein Voice over IP Service welcher durch die Netstream AG in Dübendorf angeboten wird. Mit einem VoIP Angebot kann man nicht nur telefonieren, sondern auch noch diverse Zusatzdienste wie Faxbox, Combox, Halten, Wartefunktion, Weiterleitung, Konferenzschaltung, Umschaltung etc. verwenden. Für Private bestehen Prepaid sowie Abo Angebote. Für Firmen, welche eine Telefonanlage benötigen, bestehen zudem Virtual PBX (private branch exchange) oder Hosted PBX Angebote.

Die VoIP Infrastruktur basiert auf einer Software namens Porta, welche als Proxy den RTP Verkehr überträgt, sowie die Funktionalität, Kundenmanagement und Billing übernimmt.
Momentan wird eine Voice-Session zwischen den beteiligten Knotenpunkten über SIP (Session Initiation Protocol) aufgebaut und der kontinuierliche Voice Stream über RTP (Real-Time Transport Protocol) übertragen. Befindet sich ein Angreifer im gleichen Netz, kann der gesamte Datenverkehr mit entsprechender Software (z.B. Wireshark) mitgeschnitten werden. Nach Art. 13 Abs. 1 der Bundesverfassung haben alle *Anspruch auf Achtung ihres Privat- und Familienlebens, Ihrer Wohung sowie ihres Brief-, Post- und Fernmeldeverkehrs*. Bei der jetzigen Umsetzung sind Private sowie Firmenkunden selber verantwortlich die Telefongespräche mittels geeigneten Massnahmen abzusichern.

Seit dem Maintainance Release 23 im Jahr 2011 der Porta Software, besteht eine TLS (Transport Layer Security) Unterstützung, duadurch kann die Initiierung einer Session zwischen zwei Knoten durch Zertifikate (Authorisation) geschützt werden. Dieser Schutz ist notwendig um den Schlüsselaustausch zwischen den Knoten nicht im Klartext zu übertragen. Die von der Netstream AG verkauften VoIP Telefone haben einen SRTP Support, dieser ist notwendig um die Sprachdaten mit den zuvor ausgetauschten Schlüsseln zu sichern um die Integrität und Vertraulichkeit des Telefongesprächs zu gewährleisten. Jedoch haben Schweizer Provider das gezielte Abhören von einzelnen Telefonleitungen, mittels richterlichen Beschluss, zu Gewährleisten.

2 Ziele

Systemziele

Nr.	Kategorie	Beschreibung	Messgrösse	Priorität
1	Initialisierung *SIP over TLS (Transport Layer Security) einführen*	*Die Sicherung des Initialisierungsprozesses (SIP) für den Schlüsselaustausch bei Projektabschluss*	*Von heute Klartext-Übertragung auf neu verschlüsselt*	*M1*
2	Schlüsselaustausch PKI für TLS (Public Key Infrastructure)	Die von TLS benötigten Zertifikate pro Kunden ausstellen können bei Vertragsabschluss. Als Certificate Authority eine Puplic Key Infrastructure für netvoiop.ch Firmenkunden aufbauen.	VeriSign defined: Digital Certificates Class 3-5	M1
3	Sprachdaten SRTP (Secure Real-Time Transport Protocoll)	SRTP als Sprachdatenübertragungsprotokoll für gesicherte wie ungesicherte Leitungen einrichten	Sesson Boarder Controller terminiert neu den SRTP Stream	M1
4	REST PortaAPI	WebService Calls für PortaAPI um Customer auf Secure umzustellen/einzurichten bei Optionsauswahl.	Erfolgreiche Umstellung eines Customers (alle Lines)	M2
5	Customeradministration User Interface	Im User Management Interface kann der Kunde die Option „Secure“ für seinen Customer ab- bzw bestellen	Fehlerfreie Anzeige des Secure Status für den Customers	M3
6	Billing Vertrag erstellen	Ein Vertrag VOIP_SECURE wird dem Kunde bei Bestellung der Option hinzugefügt und entsprechend verrechnet.	Zuordnung der Option für ein erfolgreiches Billing	M2

Legende: Priorität: M=Muss /1=hoch, 2=mittel, 3=tief

Vorgehensziele

Nr	Kategorie	Beschreibung	Messgrösse	Priorität
1	Solve TLS Bug	TLS implementation von Porta weist bekannte Bugs aus welche behoben werden müssen	*Fehlerfreie Verschlüsselung*	*M3*
2	Key Exchange	Die SIP Clients müssen konfiguriert werden, damit ein Schlüsselaustausch und RSTP signalisiert wird	SIP signalisiert Schlüsselaustausch	M2
3	PortaAPI	Applikation sowie Datenbank Layer durch IT-Architekt analysieren und anpassen	WebService Call setzt Customers Account auf Secure und fügt den VOIP_Secure Vertrag hinzu. Löst Support Auftrag für die Konfiguration des Kunden aus	M2
4	User Interface	WebApplication Erweiterungen Designen und implementieren	Kunde kann Option bestellen und Zertifikate erzeugen/managen	M
5	Support	Die SMC Abteilung erstellt Benutzeranleitungen, erfasst mögliche Supportanfragen und deren Prozesse vor Einführung, welche für den Kunden aufbearbeitet werden zur Selbsthilfe.	Abteilung verfügt über aktualisierte Bestellformulare und Prozessbeschreibungen. Anzahl Supportanfragen	H
6	Marketing	Promotion des Services	Anzahl Neukunden	H
7	Pricing	Preis pro Leitung und Aufschaltgebühren definieren	Konkurrenzpreis von Sfr. 4.-- pro Monat/Leitung bzw. Sfr. 40.-- (Flatrate für Firmenkunden) als Referenz	

Rahmenbedingungen

Datenschutzrichtlinien:	Nach Art. 13 Abs. 1 der Bundesverfassung haben alle *Anspruch auf Achtung ihres Privat- und Familienlebens, Ihrer Wohung sowie ihres Brief-, Post- und Fernmeldeverkehrs*
Kostendach:	Die einmaligen Kosten betragen Fr. 360'000 Die wiederkehrenden Kosten betragen Fr. 60'000/Jahr Diese Kosten dürfen um max 10% überschritten werden.
Ressourcen:	Gem. Kap. 9 Organisation
Verfügbarkeit:	Die vollständige Verschlüsselung ist nur möglich, wenn beide Knoten die SRTP Technologie beherschen. Von VoIP zu Festnetz können keine gesicherten Telefonate geführt werden.
Lieferanten	Vertraulich
Technologien	SRTP, TLS, SIP, JAX-RS, PHP 5.0
Organisation:	Projektorganisation

Abrenzung

Vertragsmodalitäten des Artikels sind nicht Bestandteil dieses Berichts.

3 Lösungsbeschreibung

Um die Integrität und Vertraulichkeit der ausgetauschten Schlüssel zu gewährleisten wird die Initialisierung zwischen zwei beteiligten Knoten mittels SIP over TLS und entsprechenden Zertifikaten gesichert.

SIP	TLS	TCP	IP	Ethernet/FDDI

Nach dem TCP Handshake authentifizieren sich die Enpunkte über TLS mittels Zertifikaten und können somit den folgenden Verkehr mit den ausgetauschten Schlüsseln absichern. Daher sind die über SIP ausgetauschten Schlüssel für SRTP mit TLS gesichert. Um den Sprachverkehr bei einem Richterlichen Beschluss zu entschlüsseln, wird der SRTP Stream über den Session Boarder Controller terminiert. Durch die höheren Lizenzkosten des SBC verteuert sich der Betrieb pro Leitung.

Nach erfolgreicher Konfiguration der VoIP-Infrastruktur kann sich das Marketing mit der Promotionskampagne beginnen.

Das netvoip.ch Kundenportal sowie das Registrierungsformular wird um die Funktion Secure erweitert. Bei Aktivierung werden alle Rufnummern des Kunden umgeschaltet sowie Kontakt mit dem Kunden aufgenommen. Der Kunden soll durch das SMC mittels Anleitungen oder Email Kontakt instruiert werden. Die Zertifikate soll der Kunde über die WebApp beziehen können.

Die SMC Abteilung wird über das neue Angebot instruiert und definiert entsprechende Ablaufprozesse für Neukkunden, Changes sowie Problemfällen mit der Konfiguration.

4 Strategiebezug und Umsetzung von Vorgaben

Strategiebezug:

- State of the Art Technologien verwenden und innovative Angebote
- Die Freiwillige Transparenz zur Netzneutralität passt zum erzeugten Images durch das Secure Package

Umsetzung von Vorgaben:

- BSI (Bundesamt für Sicherheit in der Informationstechnik) Baustein VoIP im Detail Massnahme 5.134 und 5.135 (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b04/b04007.html;jsessionid=89251713DE398FE43B012575E34DC54A.2_cid294)

5 Rechtliche Grundlagen

„Das FMG definiert einen Fernmeldedienst als die fernmeldetechnische Übertragung von Informationen für Dritte . Weil VoIP unter diese Definition fällt, sind die Bestimmungen des FMG und der Fernmeldeverordnung (FDV) auch auf VoIP-Dienste anwendbar. Schlussfolgerung aus der Rechtsgrundlagenanalyse für unser Projekt und sicherzustellende Punkte sind:

„ 1. die Leitweglenkung der Notrufe an die Alarmzentralen der zuständigen Dienste sowie die Standortidentifikation der Anrufenden sicherstellen

...

2. Pflicht zur Einhaltung des Fernmeldegeheimnisses und zur Sicherstellung der Überwachung des Fernmeldeverkehrs im Rahmen der anwendbaren Vorschriften“

Quellenangabe: Dr. Widmer & Partner, Rechsanwälte, Bern / 12.9.2005, https://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CFoQFjAC&url=http%3A%2F%2Fwww.widmerpartners-lawyers.ch%2FNR%2Frdonlyres%2F33AA70FD-42B2-4240-80E2-2BBEC27375D7%2F0%2Fvoipregulationde.pdf&ei=FsV8UqPDPOWw7Qbl8oDoBA&usg=AFQjCNEwjBkuHaKpD2zNdA4hOazPDxPNAw&sig2=lO7tUxhQIARtp6MDLnye0g&bvm=bv.56146854,d.ZGU *(8.11.2013)*

6 Mittelbedarf

Kosten	CHF	Ertrag	CHF/Monat
Entwicklungskosten	100,000	Geschäftskunden	120,000
Testing	50,000	Private Abo	20,000
Proj. Mngmt	30,000	Private Prepaid	9,800
Infrastruktur	15,000		
Marketing	150,000		
Sonstige	15,000		
Einmalige Kosten Total	**360,000**	**Ertrag/Monat**	**149,800**
Lizenzen	30,000		
Betrieb/ Unterhalt	30,000		
Wiederkehrende Kosten Total/Jahr	**60,000**		
		Gewinn/Monat	**144,800**

Sachmittel

Sofware	Session Boarder Controller Lizenz von XY
Netzwerk	TLS benötigt mehr Ressourcen
Räume	Meetingraum
IT-Infrasturkur	VoIP-Testlabor

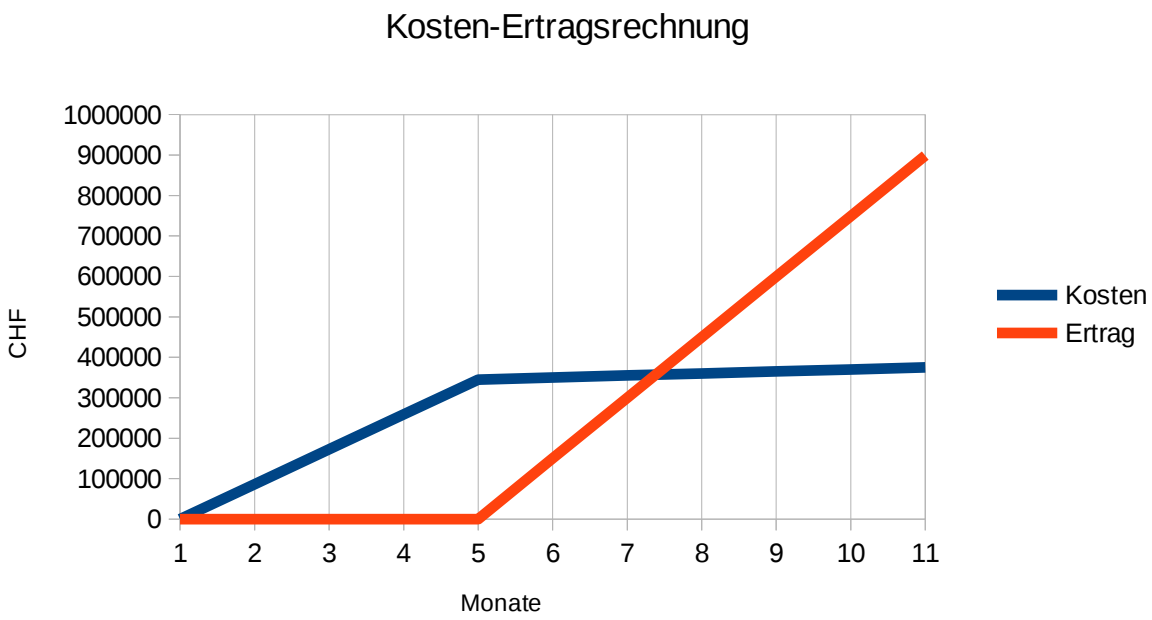
(Dies ist eine zusammengefasste Berechnung, die Details der einzelnen Kostenpunkte können bei Bedarf nachgereicht werden)

7 Wirtschaftlichkeit

Nutzwertanalyse

Thema	Gewicht in %	Produkt 1 Punkte	Produkt 1 Total Punkte	Produkt 2 Punkte	Produkt 2 Total Punkte
Produkt					
Techologie/Standards	30	2	0.6	4	1.2
Kosten	5	4	0.2	1	0.05
Betrieb	5	3	0.15	3	0.15
Referenzen	10	1	0.1	4	0.4
			0		0
Vendor			0		0
SLA, SLA Org.	15	2	0.3	4	0.6
Referenzen	15	1	0.15	2	0.3
Geographisch	5	5	0.25	2	0.1
Marktführerschaft	10	1	0.1	4	0.4
Kosten	5	4	0.2	1	0.05
Total	**100**	**23**	**2.05**	**25**	**3.25**

Wirtschaftlichkeitsanalyse



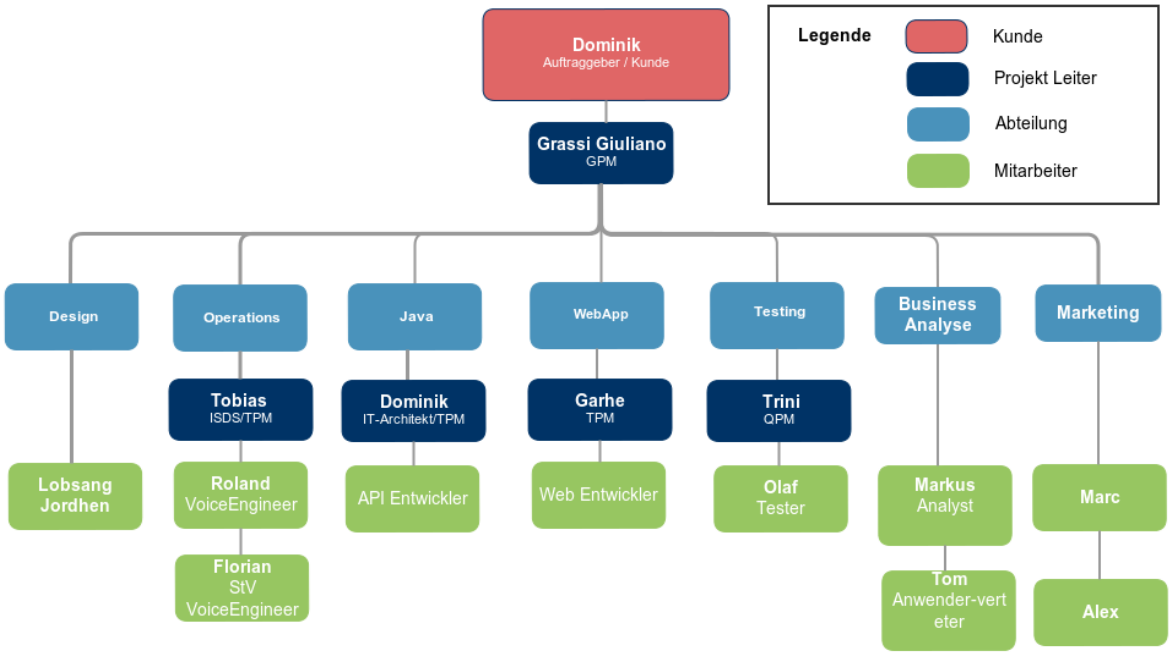
8 Planung

Meilensteine und Termine

Meilensteine	Geplant
Projektfreigabe	*Mo.13.01.2014*
ProjektLeiter Information	Mo. 20.01.2014
Kickoff Projektstart	Do. 23.01.2014
Anforderungsanalyse Operations	Do. 30.01.2014
VoIP-Secure Testumgebung	Do. 13.02.2014
Milestone: Abnahme VoIP Secure Testumgebung	Do. 20.02.2014
JavaDev PortaAPI Erweiterungen Marketing Kampagne erstellen	Do. 6.03.2014
Tested PortaAPI	Do. 20.03.2014
Milestone PortaAPI Erweiterung	Do.20.03.2014
WebDev NetVoip Portal Erweiterungen	Do. 3.04.2014
Tested NetVoip Portal Erweiterungen	Do. 17.04.2014
Milestone Netvoip Portal Erweiterungen	Do. 17.04.2014
Launch on Preview	Do. 24.04.2014
Test Umstellung für alle Abotypen+Bugfixing	Do. 8.05.2013
Milestone VoIP Secure Feature Abnahme	Do. 8.05.2013

9 Organisation

Rolle in der Projektorganisation	Name	Kürzel	Funktion/Vertretene Organisationseinheit
Auftraggeber	Dominik	chdbrdo0	GL (CTO)
Gesamtprojektleitung	Giuliano Grassi	chdgrgi0	Software Engineer
Gesamtprojektleitung	Giuliano Grassi	chdgrgi0	Software Engineer
ISDS-Verantwortlicher	Tobias	chdmema0	Leader Development
Fachspezialist Operations	Roland	chdkaro0	Voice Engineer
Fachspezialist Geschäftsprozessverantwortlicher	Markus	chdmame0	Leader Development
Projektleiter Java Development IT-Architekt	Dominik	chdmedo0	Leader Software Development
Projektleiter Web Development	Neirouz	chdgane0	Leader Web Development
Qualitäts- und Risikomanager Testingverantwortlicher	Trini	chdngtr0	ProjektManager
Web Developper	Alexander	chdboal0	WebEntwickler
Java Developper	Julian	chdhaju0	JavaEntwickler
Tester	Olaf	chdanol0	ProjektLeiter
Marketing	Marc	chomma0	Werbefachmann
Marketing	Alex	chnial0	Werbefachmann
Anwendervertreter	Tom	Tom.x@xy.ch	Firmenkunde
Designer	Lobsang	chlojo0	Designer



10 Risiken

Nr.	Risikobeschreibung	EW	AG	RZ	Massnahmen	Verantw.	Termin
1	*Voice Engineer fällt aus*	*2N*	*3H*	*6*	*Stellvertretung einbinden*	*OP*	
2	PortaBilling TLS Implementation nicht verwendbar	2M	2M	4	Prototype erstellen	OP	Vor init
3	Sicherheitslücke SW (Fernmeldegeheimniss)	2M	2M	4	Standardisierte Komponenten verwenden	DEV	
4	Interfaces Porta Billing ändert unerwartet	1N	3H	3	Vorabklärungen mit Porta führen	CTO	Vor Init
5	Mehr Kunden Live als was System designed ist	2M	1N	2	Daily Reporting/trends Auswertungen erstellen	CUC/ Marketing/ DEV	Vor live
6	Voice Stream Qualität fällt unter Schwellwert	1H	2M	2	VoIP Network Priorisierung überprüfen	OP	Vor Test
7	PortaBilling TLS Implementation nicht verwendbar	2M	2M	4	Prototype erstellen	OP	Vor init

Legende:
EW=Eintretenswahrscheinlichkeit: 1 Niedrig / 2 Mittel / 3 Hoch;
AG=Auswirkungsgrad(Schadenausmass): 1 Gering / 2 Mittel / 3 Gross,
RZ=Risikozahl (EW*AG)

Eintretens-wahrscheinlich-keit	Hoch			
	Mittel	5	3,2,7	1
	Niedrig		6	4
Risiko Matrix		Niedrig	Mittel	Hoch
		Auswirkungsgrad		

11 Konsequenzen

Bei Projektfreigabe

- Resourcen werden blockiert

- Lizenzvertragsverhandlungen müssen geführt werden

Wenn Projekt nicht oder zu einem späteren Zeitpunkt frei gegeben wird

- Marktanteilverluste

- Gewinnverluste