Sicherheitskonzept Connect4Video

Inhalt

1 Einführung

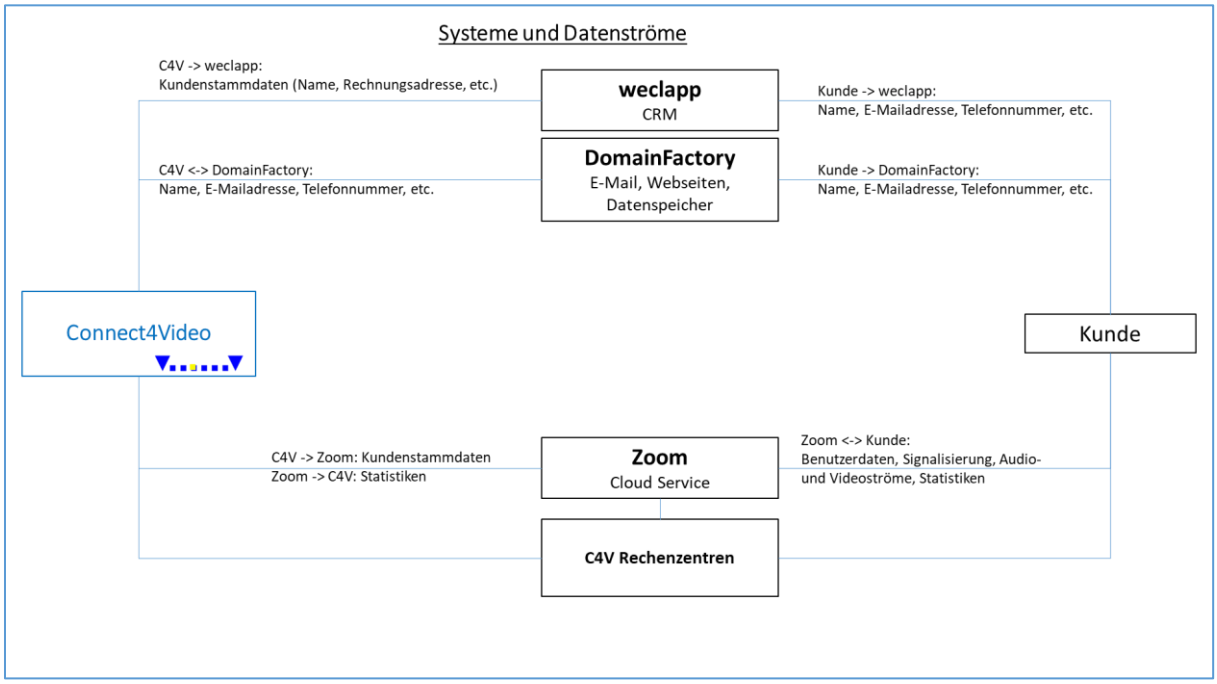
Connect4Video (C4V) bietet einen OTT-1 Dienst für Videokommunikation an.
Connect4Video betreibt kein öffentliches Telekommunikationsnetz.
Connect4Video ist nach §6 TKG bei der BNetzA gemeldet als Betreiber öffentlich zugänglicher Telekommunikationsdienste unter der Registriernummer 13/011. Daher führt C4V das vorliegende Sicherheitskonzept.

Connect4Video GmbH, Nibelungenstr. 28, 65428 Rüsselsheim
Tel: +49 6131 636 8760
E-Mail: info@connect4video.com
Amtsgericht Darmstadt, Registernummer: HRB 87548
Geschäftsführer: Michael Retagne, Jürgen Stierhof

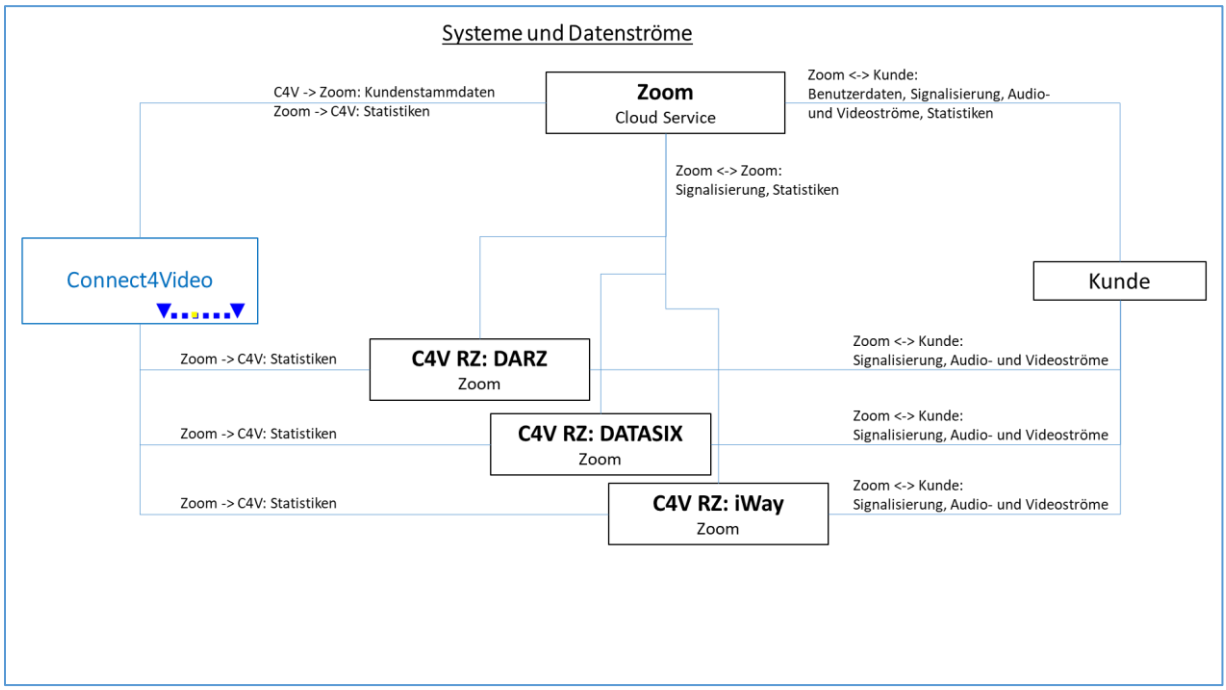
1.1 Sicherheitsbeauftragter

Sicherheitsbeauftragter ist:
Jürgen Stierhof
Tel: +49 6142 953 9522
E-Mail: juergen@connect4video.com

1.2 Übersichtspläne



Alle Verbindungen benutzen das Internet.
Die Anbindung der Mitarbeiter erfolgt über das Internet.



RZ: Rechenzentrum

1.3 Beschreibung des C4V Dienstes

C4V bietet Videokommunikationsdienste nur für Firmenkunden an (B2B).

Cloudbasierter Videokommunikationsdienst (Zoom):

C4V bietet den Clouddienst an als Reseller von Zoom (zoom.us).
C4V ist im Wesentlichen Reseller und führt lokale Vertriebs- und Marketingaktivitäten durch. Zoom bieten ihren Dienst in Deutschland auch über andere Vertriebspartner, d.h. ohne C4V, an.

Der Firmenkunde kauft personalisierte Zugänge zum Dienst und legt die Nutzer des Dienstes innerhalb seiner Organisation fest.
Der Dienst stellt virtuelle Konferenzräume zur Verfügung, d.h. jeder Nutzer hat einen persönlichen virtuellen Konferenzraum.
Kunden kaufen den Dienst zur Kommunikation innerhalb der eigenen Organisation bzw. Gruppe.
Die Kommunikation mit Externen kann unterbunden werden:

- Die Nutzergruppe eines Kunden verwendet ein virtuelles Segment des Dienstes, das von den virtuellen Segmenten anderer Kunden strikt getrennt ist.
- Nutzer eines Kunden können nicht ohne Weiteres von Externen kontaktiert werden. Selbst durch das Herunterladen der entsprechenden App kann ein Externer nicht beliebige Nutzer kontaktieren.
- Sofern gewünscht, trifft man sich in virtuellen Räumen, die entweder der einen Partei oder der anderen Partei zugeordnet sind. Dabei muß die jeweilige Partei der jeweiligen anderen Partei erlauben, die virtuellen Räume zu betreten. Dies geschieht durch Mitteilen der (vom Raum-Admin änderbaren) Raumnummer, Mitteilen des (vom Raum-Admin änderbaren) Passwortes, etc. Es besteht hier ein Zugriffsschutz. Externe müssen sich authentifizieren.

Das Hauptmerkmal des Dienstes ist Kommunikation innerhalb von Benutzergruppen und mit Externen. Es erfolgt keine Zusammenschaltung von Netzen.

Zoom betreibt den Dienst, den C4V weiterverkauft. C4V vermarktet den Dienst von Zoom unter dem Markennamen easymeet24.
Mitarbeiter von C4V haben Zugang zu Daten der C4V Kunden, aber haben keinen Zugriff auf die Technik des Zoom Dienstes.
C4V hostet in angemieteten Rechenzentren lokale Server (virtuell oder physikalisch), die in den Dienst von Zoom eingebunden sind. Auf den Servern läuft Software von Zoom. Mitarbeiter von C4V haben Zugang zu diesen Servern.
Die Zoom Systeme verarbeiten und speichern personenbezogene Daten.

Angebundene Systeme:

Für Kundenbestandsdatenverwaltung und Buchhaltung wird der Clouddienst von weclapp verwendet.

E-Mail, Webseiten und Datenspeicherung werden gehostet bei DomainFactory.

Für die Steuerberatung und die Buchhaltung ist das Steuerbüro Stephan beauftragt.

Rechtsberatung macht das Anwaltsbüro Kolb.

Die Telefonanlage ist von sipgate in der Cloud.

Manche Systeme werden realisiert im Rahmen des Kontingents der ZengerConsult GmbH (Nibelungenstr. 28, 65428 Rüsselsheim), siehe dazu die Angaben bei den Teilsystemen. Aus Gründen der Transparenz wird der hinter der ZengerConsult stehende Auftragnehmer angegeben. Die ZengerConsult ist als deutsche Firma dem BDSG und der EU-DSGVO verpflichtet und als Mehrheitsgesellschafter der C4V ausreichend sensibilisiert für die Belange des Datenschutzes und des Fernmeldegeheimnisses.

1.4 Störfallmanagement

Die erste Verteidigungslinie ist ein widerstandsfähiges Systemdesign. Es wird Wert gelegt auf Absicherung der Systemzugänge, auf geeignete Vergabe von Zugriffsrechten und deren Dokumentation und regelmäßige Überprüfung.

Störfälle werden regelmäßig durch die Kooperation von Mitarbeitern in den Bereichen Technik und Kundenbetreuung bearbeitet. Im Allgemeinen arbeiten umso mehr Personen an einem Vorfall, je schwererwiegend er ist.

Normalerweise nehmen Störfälle in Phase eins ihren Anfang. Diese Phase dauert an, bis das aktuelle Problem unter Kontrolle ist. In Phase zwei arbeiten wir daran, das System in den normalen Betriebszustand zurückzuversetzen. Häufig ist die Kundenkommunikation in Phase zwei besonders wichtig. In Phase drei ziehen wir Schlüsse aus dem Vorfall und ergreifen langfristige Maßnahmen für die zukünftige Sicherheit.

Bei schwerwiegenden oder komplexen Vorfällen müssen Spezialisten der Zulieferer hinzugezogen werden.

Bei allen Vorfällen ist unser Ziel die schnelle Problemlösung. Dabei sorgen wir dafür, dass unsere Kunden stets zufrieden bleiben und dass das Netzwerk sicher ist. Zudem konzentrieren wir unsere Arbeiten auf den Störfall und minimieren die Auswirkungen auf den Rest des Unternehmens.

1.5 Mitteilungsverfahren bei Sicherheitsverletzungen

Werden Beeinträchtigungen festgestellt, die im Sinne des §109 (5) TKG einzuordnen sind, so wird der Mitarbeiter, der die Beeinträchtigung festgestellt hat, unverzüglich den Operations Manager informieren, der unverzüglich den Geschäftsführer informieren wird und eine entsprechende Meldung an die BNetzA abgeben wird.

1.6 Allgemeines

Kunden werden vor Vertragsabschluss in den AGBs und der Datenschutzerklärung der C4V über Erhebung und Speicherung personenbezogener Daten informiert. Zustimmung ist Voraussetzung für einen Vertragsabschluss und nachfolgende Datenverarbeitung.

2 Sicherheitsteilsysteme

2.1 Überblick

Das Gesamtsystem wird in folgende Sicherheitsteilsysteme aufgeteilt.
Alle Teilsysteme verarbeiten und speichern personenbezogene Daten unterschiedlicher Art in unterschiedlicher Art und Weise.

Zoom Infrastruktur
C4V ist Zoom Partner und Reseller des Dienstes, den Zoom betreibt. C4V hat keinen operativen Zugriff auf Technik und Systeme, die Zoom betreibt, um den Dienst anzubieten.
Ausnahme: Zoom Server, die C4V in DACH betreibt, bilden hier ein eigenes Sicherheitsteilsystem.

C4V Rechenzentrum DARZ
Teile der Videodienste von C4V werden auf Servern in angemieteten Rechenzentren betrieben.

C4V Rechenzentrum DATASIX
Teile der Videodienste von C4V werden auf Servern in angemieteten Rechenzentren betrieben.

C4V Rechenzentrum iWay
Teile der Videodienste von C4V werden auf Servern in angemieteten Rechenzentren betrieben.

CRM
Als Kundendatenverwaltungssystem (CRM), für Buchhaltung und als Ticketsystem wird das Cloud-CRM-System von weclapp eingesetzt.

E-Mail Server
Als E-Mail Server wird gehostetes Microsoft Exchange bei DomainFactory eingesetzt.

Webseiten- und Domainhosting
Webseiten werden bei DomainFactory gehostet. Domains werden bei DomainFactory verwaltet.

Online-Terminvergabe
Über den Dienst eTermin können Kunden online Termine mit C4V vereinbaren.

Datenspeicherung
Ein Datenspeicherungsserver wird bei DomainFactory gehostet.

Wiki
Für ein internes Wiki wird die cloudbasierte Softare Confluence von Atlassian verwendet.

Personal
Das Personal umfasst die Firmeninhaber, den Geschäftsführer, freie Mitarbeiter sowie Geschäftspartner.

Steuerberatung und Buchhaltung
Für die Buchhaltung ist das Steuerbüro Stephan beauftragt.

Rechtsberatung
Rechtsberatung macht das Anwaltsbüro Kolb.

Telefonanlage
Die Telefonanlage ist von sipgate in der Cloud.

2.2 Sicherheitsteilsystem im Detail: Zoom

C4V ist Zoom Partner und Reseller des Videokommunikationsdienstes, den Zoom betreibt.
(www.zoom.us, Zoom Video Communications, Inc., 55 Almaden Blvd, Suite 600, San Jose, CA 95113, USA)

C4V hat mit Zoom einen Auftragsverarbeitungsvertrag und die EU Standardvertragsklauseln abgeschlossen.

Zoom verarbeitet personenbezogene Daten und Verkehrsdaten.
C4V hat keinen operativen Zugriff auf Technik und Systeme, die Zoom betreibt, um den Dienst anzubieten.
C4V hat lediglich Zugriff auf ausgewählte Verkehrsdaten, um Fehler zu untersuchen und die Qualität der Verbindungen sicherstellen zu können (Zoom Backend). C4V kann diese Daten nur sehen, aber nicht bearbeiten oder löschen.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz des Fernmeldegeheimnisses
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Gewährleistung eines ordnungsgemäßen Betriebes des Dienstes.

Gefährdungen:
Da der Dienst von Zoom betrieben wird und C4V keinen operativen Zugriff auf Technik und Systeme hat, sind folgende Gefährdungen für C4V relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Benutzerverhalten

Sicherheitsanforderungen:

- Verarbeitung, Nutzung, Verwendungszweck personenbezogener Daten sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.

Schutzmaßnahmen:
Da der Dienst von Zoom betrieben wird und C4V keinen operativen Zugriff auf Technik und Systeme hat, liegen folgende Schutzziele ausserhalb des Einflusses von C4V. Der entsprechende Schutz obliegt dem Betreiber des Dienstes, Zoom Video Communications, Inc.

- Schutz des Fermeldegeheimnisses.
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können.
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer.
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.

Zoom betreibt den Dienst in weltweit verteilten, redundanten Rechenzentren. Zoom hat adäquate Sicherheitsmaßnahmen implentiert (Details siehe hier: https://support.zoom.us/hc/en-us/articles/201362063-Security-White-Paper).
Zoom erfüllt SSAE16 SOC 2. Zoom erfüllt die Anforderungen der EU-DSGVO (https://zoom.us/privacy-and-legal).

Die Nutzer des Dienstes haben einen personalisierten Zugang und einen personalisierten virtuellen Konferenzraum. Beides ist passwortgeschützt.
Meetings sind verschlüsselt mit AES-256-GCM.

Die Zugriffsberechtigungen auf das Zoom Backend werden von der C4V-Firmenführung vergeben. Die Zugänge sind personalisiert. Es gibt keine allgemeinen Zugänge, die von mehreren Personen benutzt werden.

Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Der Zugriff auf das Zoom Backend erfolgt über das Internet. Alle Verbindungen sind verschlüsselt (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256).

Bewertung:
Es besteht ein Restrisiko eines Ausfalles des Dienstes. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere angesichts des redundanten Aufbaues der Zoom Infrastruktur.
Es besteht ein Restrisiko eines unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.3 Sicherheitsteilsystem im Detail: Rechenzentrum DARZ

Teile des Zoom Dienstes können auf lokalen Servern abgebildet werden. Dafür läßt C4V im Rechenzentrum DARZ virtuelle Maschinen hosten.
(www.da-rz.de, DARZ GmbH, Julius-Reiber-Str. 11, 64293 Darmstadt)
DARZ ist eine deutsche Firma und dem BDSG und der EU-DSGVO verpflichtet.

Im DARZ sind Meeting Connectoren (MC), Virtual Room Connectoren (VRC) und Recording Connectoren (RC) installiert auf virtuellen Maschinen (VM) auf der VMware Umgebung des DARZ.
Es werden personenbezogene Daten (z.B. IP Adressen) verarbeitet und gespeichert. Es werden Mediendaten der Meetings verarbeitet aber nicht gespeichert.

Schutzziele:
Relevante Schutzziele sind:

- Schutz des Fernmeldegeheimnisses
- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.

Gefährdungen:
Folgende Gefährdungen sind relevant:

- Technische Störungen, Ausfälle
- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
DARZ ist ISO 27001 zertifiziert.

Die VMs haben öffentliche IP Adressen, sind aber durch lokale Linux-Firewalls auf den VMs gesichert. Die Firewall ist entsprechend der Herstellervorgaben so restriktiv wie möglich konfiguriert. Nicht nötige Ports sind geschlossen.

C4V hat in insgesamt drei Rechenzentren Zoom Server aufgebaut. So wird eine Redundanz erreicht, d.h. bei einem Ausfall der Komponenten in einem Rechenzentren wird der Betrieb des Dienstes über die anderen Rechenzentren weitergeführt.
Zudem wird die Infrastruktur laufend überwacht, um bei Störungen schnell reagieren zu können.

Die VMware Umgebung ist über eine Weboberfläche erreichbar. Die Verbindung ist verschlüsselt (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256).
Gängige Konfigurationsparameter sind über eine Weboberfläche erreichbar. Die Verbindung ist verschlüsselt (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384).
Die Weboberfläche der Anwendung hat ein vom Aussteller selbst signiertes Sicherheitszertifikat. Dies ist hier kein Problem, denn der Zugriff auf die Weboberfläche wird nur von C4V verwendet, nicht von Kunden, und erfolgt mit der IP Adresse, nicht über einen Domainnamen.

Die Zoom Server werden sowohl bzgl. der Zoom Anwendung als auch bzgl. des Betriebssystems (Linux) regelmäßig gepflegt. Softwareupdates werden eingespielt, wenn sie zur Verfügung stehen, die

Verwendung sinnvoll ist und der Einspielaufwand in vernünftigem Verhältnis zu den erreichbaren Verbesserungen steht.
Die Regelmäßigkeit wird mit Hilfe von automatisierten Erinnerungen erreicht.

Die Zugriffsberechtigungen auf die VMs werden von der C4V-Firmenführung vergeben. Die VPN-Zugänge sind personalisiert.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Die gesamte Installation ist dokumentiert. Die Dokumentation wird laufend aktualisiert.

In den Systemlogs der Server werden zur Fehlersuche personenbezogene Daten (IP Adressen) gespeichert. Die Logs werden von C4V regelmäßig, spätestens nach 6 Monaten, gelöscht. Die Löschfristen werden mit Hilfe von automatisierten Erinnerungen eingehalten.
Es werden keine Gesprächsinhalte gespeichert.
Es ist keine technische Möglichkeit vorgesehen, Nachrichteninhalte mitzuhören.

Bewertung:
Es besteht ein Restrisiko des Ausfalles infolge von z.B. Witterungseinflüssen auf das RZ, DDoS-Attacken oder Fehlbedienung. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere infolge der angewendeten RZ-Redundanz.
Es besteht ein Restrisiko des unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.4 Sicherheitsteilsystem im Detail: Rechenzentrum DATASIX

Im Rechenzentrum DATASIX sind Teile der Videodienste von C4V gehostet.
(www.datasix.at, DATASIX Rechenzentrumsbetriebs GmbH, Hofmühlgasse 3-5, 1060 Wien, Austria)
DATASIX ist eine österreichische Firma und der EU-DSGVO verpflichtet.

Im DATASIX sind Meeting Connectoren (MC), Virtual Room Connectoren (VRC) und Recording Connectoren (RC) installiert (virtualisiert auf physikalischen Servern der C4V).
Es werden personenbezogene Daten (z.B. IP Adressen) verarbeitet und gespeichert. Es werden Mediendaten der Meetings verarbeitet aber nicht gespeichert.

Schutzziele:
Relevante Schutzziele sind:

- Schutz des Fernmeldegeheimnisses
- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.

Gefährdungen:
Folgende Gefährdungen sind relevant:

- Technische Störungen, Ausfälle
- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
DATASIX ist ISO27001 zertifiziert.
Für die gemieteten Racks hat das RZ zur Sicherheit entsprechende Zutrittsregelungen implementiert.

Die VMs haben öffentliche IP Adressen, sind aber durch lokale Linux-Firewalls auf den VMs gesichert.
Die Firewall ist entsprechend der Herstellervorgaben so restriktiv wie möglich konfiguriert. Nicht nötige Ports sind geschlossen.
Der Zugriff auf die VM-Umgebung erfolgt teilweise über VPN (128bit verschlüsselt) und teilweise über https (ebenfalls 128bit verschlüsselt) und verwendet starke Passwörter.

Zoom Dienst:
C4V hat in insgesamt drei Rechenzentren Zoom MCs und VRCs aufgebaut. So wird eine Redundanz erreicht, d.h. bei einem Ausfall der Komponenten in einem Rechenzentren wird der Betrieb des Dienstes über die anderen Rechenzentren weitergeführt.
Abhängig von der Art der Anwendung kann der Admin-Zugriff auf die VMs über das Internet erfolgen. Gängige Konfigurationsparameter sind über eine Weboberfläche erreichbar. Die Verbindung ist verschlüsselt (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384).
Die Weboberfläche der Anwendung hat ein vom Aussteller selbst signiertes Sicherheitszertifikat. Dies ist hier kein Problem, denn der Zugriff auf die Weboberfläche wird nur von C4V verwendet, nicht von Kunden, und erfolgt mit der IP Adresse, nicht über einen Domainnamen.

Die Zoom Server werden sowohl bzgl. der Zoom Anwendung als auch bzgl. des Betriebssystems (Linux) regelmäßig gepflegt. Softwareupdates werden eingespielt, wenn sie zur Verfügung stehen, die

Verwendung sinnvoll ist und der Einspielaufwand in vernünftigem Verhältnis zu den erreichbaren Verbesserungen steht. Die Regelmäßigkeit wird mit Hilfe von automatisierten Erinnerungen erreicht.

Firewall (OPNsense):
Diese Firewall wird für die VM-Umgebung verwendet und damit für Firewall Traversal Dienst (GnuGK) und für Infrastrukturüberwachung (Zabbix, Graylog).
Der Firewall Server ist eine Einzelinstallationen ohne Redundanz. Die schnelle Wiederherstellung der Funktion im Fehlerfalle wird unterstützt durch:

- Regelmäßiges Backup der VM, das eine zügige Wiederherstellung erlaubt
- Dokumentation der Konfiguration.

Die Server werden sowohl bzgl. der Anwendung als auch bzgl. des Betriebssystems (Linux) regelmäßig gepflegt. Softwareupdates werden eingespielt, wenn sie zur Verfügung stehen, die Verwendung sinnvoll ist und der Einspielaufwand in vernünftigem Verhältnis zu den erreichbaren Verbesserungen steht. Die Regelmäßigkeit wird mit Hilfe von automatisierten Erinnerungen erreicht.
Es wird kein Virenschutzprogramm verwendet. Auf den Servern werden nur vom Hersteller freigegebene Anwendungen oder OS-Updates aus geprüften Repositories installiert.

Infrastrukturüberwachung (Zabbix, Graylog):
Zabbix ist ein Netzwerk-Monitoringsystem. Es dient der Überwachung der IT-Infrastruktur in den RZ. Dazu werden auf den zu überwachenden Servern Zabbix-Agents installiert, die mit dem Zabbix-Server kommunizieren. Bei Störungen schickt der Zabbix-Server E-Mails an mehrere Mitarbeiter.
Der Zabbix Server ist eine Einzelinstallationen ohne Redundanz. Die schnelle Wiederherstellung der Funktion im Fehlerfalle wird unterstützt durch:

- Regelmäßiges Backup der VM, das eine zügige Wiederherstellung erlaubt
- Dokumentation der Konfiguration.

Graylog ist ein Log-Management-System zum Sammeln, Speichern und Analysieren von Logs. Es dient der Analyse und graphischen Darstellung von Logdaten, die von Zabbix importiert werden.
Der Graylog Server ist eine Einzelinstallationen ohne Redundanz. Die schnelle Wiederherstellung der Funktion im Fehlerfalle wird unterstützt durch:

- Regelmäßiges Backup der VM, das eine zügige Wiederherstellung erlaubt
- Dokumentation der Konfiguration.

Der Zugriff erfolgt über eine Weboberfläche und ist SHA-256 verschlüsselt. Die Weboberfläche der Anwendung hat ein C4V-Sicherheitszertifikat.

Die Server werden sowohl bzgl. der Anwendung als auch bzgl. des Betriebssystems (Linux) regelmäßig gepflegt. Softwareupdates werden eingespielt, wenn sie zur Verfügung stehen, die Verwendung sinnvoll ist und der Einspielaufwand in vernünftigem Verhältnis zu den erreichbaren Verbesserungen steht. Die Regelmäßigkeit wird mit Hilfe von automatisierten Erinnerungen erreicht.
Es wird kein Virenschutzprogramm verwendet. Auf den Servern werden nur vom Hersteller freigegebene Anwendungen oder OS-Updates aus geprüften Repositories installiert.

Generell:
Zugriffsberechtigungen werden von der C4V-Firmenführung vergeben.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Die gesamte Installation ist dokumentiert. Die Dokumentation wird laufend aktualisiert.

In den Systemlogs der Server werden zur Fehlersuche personenbezogene Daten (IP Adressen) gespeichert. Die Logs werden von C4V regelmäßig, spätestens nach 6 Monaten, gelöscht. Die Löschfristen werden mit Hilfe von automatisierten Erinnerungen eingehalten.
Es werden keine Gesprächsinhalte gespeichert.
Es ist keine technische Möglichkeit vorgesehen, Nachrichteninhalte mitzuhören.

Bewertung:
Es besteht ein Restrisiko des Ausfalles infolge von z.B. Witterungseinflüssen auf das RZ, DDoS-Attacken oder Fehlbedienung. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere infolge der angewendeten RZ-Redundanz.
Es besteht ein Restrisiko des Ausfalles der Komponenten, die nicht mehrfach vorhanden sind. Dieses Restrisiko ist überschaubar und akzeptabel, da der Dienst für die Kunden nicht überlebensnotwendig ist (alternative Kommunikationsmöglichkeiten aus dem Produktportfolio von C4V stehen zur Verfügung) und die Auswirkungen eines Ausfalles vorübergehend hingenommen werden können.
Zudem wird die Infrastruktur laufend überwacht, um bei Störungen schnell reagieren zu können.
Es besteht ein Restrisiko des unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.5 Sicherheitsteilsystem im Detail: Rechenzentrum iWay

Teile des Zoom Dienstes können auf lokalen Servern abgebildet werden. Dafür läßt C4V im Rechenzentrum iWay (www.iway.ch, iWay AG, Badenerstrasse 569, 8048 Zürich, Schweiz) physikalische Maschinen hosten.

Die Europäische Kommission hat die Angemessenheit des Datenschutzniveaus in der Schweiz festgestellt. Die Schweiz wird auf der entsprechenden Liste der sicheren Drittstaaten aufgeführt.

Bei iWay sind Meeting Connectoren (MC) und Recording Connectoren (RC) installiert (virtualisiert auf physikalischen Servern der C4V).
Es werden personenbezogene Daten (z.B. IP Adressen) verarbeitet und gespeichert. Es werden Mediendaten der Meetings verarbeitet aber nicht gespeichert.

Schutzziele:
Relevante Schutzziele sind:

- Schutz des Fernmeldegeheimnisses
- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.

Gefährdungen:
Folgende Gefährdungen sind relevant:

- Technische Störungen, Ausfälle
- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Die VMs haben öffentliche IP Adressen, sind aber durch lokale Linux-Firewalls auf den VMs gesichert.
Der Server ist durch eine Firewall des RZ-Betreibers gesichert. Der Zugriff auf die VM-Umgebung erfolgt über https, ist 128bit verschlüsselt und verwendet starke Passwörter.
Die Firewalls sind entsprechend der Herstellervorgaben so restriktiv wie möglich konfiguriert. Nicht nötige Ports sind geschlossen.
C4V hat keinen Zugriff auf die Firewall des RZ, nur das Personal des Rechenzentrums. Konfigurationsänderungen werden nur ausgeführt, wenn diese von entsprechend bekannten E-Mailadressen angefordert werden.
Der gemietete Rackspace ist nur zugänglich für das RZ-Personal. Das RZ hat zur Sicherheit entsprechende Zutrittsregelungen implementiert. Der Zutritt in die Räume erfolgt durch eine Vereinzelungsanlage mit biometrischer Zutrittskontrolle. Alle Räume sind einbruchgesichert und videoüberwacht.

C4V hat in insgesamt drei Rechenzentren Zoom MCs und VRCs aufgebaut. So wird eine Redundanz erreicht, d.h. bei einem Ausfall der Komponenten in einem Rechenzentren wird der Betrieb des Dienstes über die anderen Rechenzentren weitergeführt.
Zudem wird die Infrastruktur laufend überwacht, um bei Störungen schnell reagieren zu können.

Der Admin-Zugriff auf die VMs erfolgt über das Internet. Gängige Konfigurationsparameter sind über eine Weboberfläche erreichbar. Die Verbindung ist verschlüsselt (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384).
Die Weboberfläche der Anwendung hat ein vom Aussteller selbst signiertes Sicherheitszertifikat. Dies ist hier kein Problem, denn der Zugriff auf die Weboberfläche wird nur von C4V verwendet, nicht von Kunden, und erfolgt mit der IP Adresse, nicht über einen Domainnamen.

Die Zoom Server werden sowohl bzgl. der Zoom Anwendung als auch bzgl. des Betriebssystems (Linux) regelmäßig gepflegt. Softwareupdates werden eingespielt, wenn sie zur Verfügung stehen, die Verwendung sinnvoll ist und der Einspielaufwand in vernünftigem Verhältnis zu den erreichbaren Verbesserungen steht.
Die Regelmäßigkeit wird mit Hilfe von automatisierten Erinnerungen erreicht.

Die Zugriffsberechtigungen werden von der C4V-Firmenführung vergeben.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Die gesamte Installation ist dokumentiert. Die Dokumentation wird laufend aktualisiert.

In den Systemlogs der Server werden zur Fehlersuche personenbezogene Daten (IP Adressen) gespeichert. Die Logs werden von C4V regelmäßig, spätestens nach 6 Monaten, gelöscht. Die Löschfristen werden mit Hilfe von automatisierten Erinnerungen eingehalten.
Es werden keine Gesprächsinhalte gespeichert.
Es ist keine technische Möglichkeit vorgesehen, Nachrichteninhalte mitzuhören.

Bewertung:
Es besteht ein Restrisiko des Ausfalles infolge von z.B. Witterungseinflüssen auf das RZ, DDoS-Attacken oder Fehlbedienung. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere infolge der angewendeten RZ-Redundanz.
Es besteht ein Restrisiko des unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.6 Sicherheitsteilsystem im Detail: Buchhaltung, CRM

Buchhaltung, Kundenbestandsdatenverwaltung (CRM) und das Supportticketsystem werden mit dem Programm von weclapp durchgeführt.
Weclapp hostet das System in eigener Verantwortung (SaaS) und stellt Benutzern wie C4V einen Fernzugriff zur Verfügung.
Weclapp ist eine deutsche Firma und dem BDSG und der EU-DSGVO verpflichtet.
(www.weclapp.com/de/, weclapp SE, Neue Mainzer Straße 66 – 68, 60311 Frankfurt am Main)
Weclapp ist ISO 27001 und GoBD zertifiziert.

C4V bietet Videokommunikationsdienste nur für Firmenkunden an (B2B).
Es werden personenbezogene Daten (Kundenbestandsdaten) verarbeitet und gespeichert.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Gewährleistung eines ordnungsgemäßen Betriebes des Dienstes.

Folgende Schutzziele sind bedeutungslos:

- Schutz des Fernmeldegeheimnisses.
  Begründung: Das Buchhaltungssystem ist kein Fernmeldesystem.

Gefährdungen:
Da das Buchhaltungssystem ein gehostetes Cloudsystem ist, sind folgende Gefährdungen für C4V relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Benutzerverhalten

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Protokollierung der Veränderungen der Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Da das Buchhaltungssystem ein gehostetes Cloudsystem ist, werden diverse Sicherheitsanforderungen vom Anbieter weclapp erfüllt.
Bei den oben letztgenannten Schutzzielen (Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können, Gewährleistung eines ordnungsgemäßen Betriebes der Dienste) ist zu beachten, daß diese Schutzziele relevant für das Buchhaltungssystem sind, aber das Buchhaltungssystem nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.

Eine Backupregelung ist eingeführt. Weclapp macht regelmäßig Backups, die die Datensicherung im Falle einer versehentlichen Löschung oder eines technischen Problems gewährleisten.

Kunden werden vor Vertragsabschluss in den AGBs und der Datenschutzerklärung der C4V über Erhebung und Speicherung personenbezogener Daten informiert. Zustimmung ist Voraussetzung für einen Vertragsabschluss und nachfolgende Datenverarbeitung.

Löschungsfristen sind definiert und werden mit Hilfe von automatisierten Erinnerungen eingehalten.

Die Zugriffsberechtigungen für Benutzer werden von der C4V-Firmenführung vergeben. Die Zugänge sind personalisiert. Es gibt keine allgemeinen Zugänge, die von mehreren Personen benutzt werden.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Der Zugriff auf das Buchhaltungssystem erfolgt über das Internet. Alle Verbindungen sind verschlüsselt (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384).
Zugriffe und Aktivitäten werden im Buchhaltungssystem protokolliert.

Bewertung:
Es besteht ein Restrisiko eines Ausfalles bzw. Datenverlustes des Buchhaltungssystem. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da das Buchhaltungssystem nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.
Es besteht ein Restrisiko eines unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.7 Sicherheitsteilsystem im Detail: E-Mail Server

Als E-Mail Server wird gehostetes Microsoft Exchange bei DomainFactory eingesetzt. DomainFactory hostet die E-Mail Server in eigener Verantwortung und stellt Benutzern wie C4V einen Fernzugriff zur Verfügung.
DomainFactory ist eine deutsche Firma und dem BDSG und der EU-DSGVO verpflichtet.
(www.df.eu, domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning)

Es werden personenbezogene Daten (Name, E-Mailadresse, Telefonnummer etc.) verarbeitet und gespeichert.

Das Serverhosting wird abgewickelt im Rahmen des Kontingents der ZengerConsult GmbH. Die ZengerConsult ist als deutsche Firma dem BDSG und der EU-DSGVO verpflichtet und als Mehrheitsgesellschafter der C4V ausreichend sensibilisiert für die Belange des Datenschutzes und des Fernmeldegeheimnisses.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz des Fernmeldegeheimnisses
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Gewährleistung eines ordnungsgemäßen Betriebes des Dienstes.

Gefährdungen:
Da das E-Mail System ein gehostetes Cloudsystem ist, sind folgende Gefährdungen für C4V relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Benutzerverhalten

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Da das E-Mail System ein gehostetes Cloudsystem ist, werden diverse Sicherheitsanforderungen vom Anbieter domainfactory erfüllt.
Bei den oben letztgenannten Schutzzielen (Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können, Gewährleistung eines ordnungsgemäßen Betriebes der Dienste) ist zu beachten, daß diese Schutzziele relevant für den E-Mail Server sind, aber der E-Mail Server nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.

Eine Backupregelung ist eingeführt. DomainFactory macht regelmäßig Backups, die die Datensicherung im Falle einer versehentlichen Löschung oder eines technischen Problems gewährleisten.

Kunden werden vor Vertragsabschluss in den AGBs und der Datenschutzerklärung der C4V über Erhebung und Speicherung personenbezogener Daten informiert. Zustimmung ist Voraussetzung für einen Vertragsabschluss und nachfolgende Datenverarbeitung.

Löschungsfristen sind definiert und werden mit Hilfe von automatisierten Erinnerungen eingehalten.

Die Zugriffsberechtigungen für Benutzer und für Administratoren werden von der C4V-Firmenführung vergeben. Die Zugänge sind personalisiert. Es gibt keine allgemeinen Zugänge, die von mehreren Personen benutzt werden.

Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Der Zugriff auf das E-Mail System erfolgt über das Internet per Outlook-App. Alle Verbindungen sind verschlüsselt (TLS 1.2; Microsoft RPC Encryption).
Mitarbeiter sind angehalten, nicht den Webmail-Zugang zu verwenden (da verschlüsselt nur mit TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA).
Bei Zugriff auf das E-Mail System über IMAP oder POP3 sind die Mitarbeiter angehalten, verschlüsselte Zugriffsarten zu verwenden.

Alle Mitarbeiter haben in ihrem E-Mail-Client ein Zertifikat hinterlegt. E-Mails werden standardmäßig signiert verschickt.
E-Mail-Verschlüsselung ist möglich, allerdings immer abhängig vom Empfänger. Eine durchgehende, einfach zu bedienende Lösung ist auf dem Markt nicht verfügbar. Die Mitarbeiter sind angehalten, wo möglich die E-Mails verschlüsselt zu verschicken.

Bewertung:
Es besteht ein Restrisiko eines Ausfalles bzw. Datenverlustes des E-Mail-Systems. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da das E-Mail-System nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.
Es besteht ein Restrisiko eines unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.8 Sicherheitsteilsystem im Detail: Webseiten- und Domainhosting

Die Webseiten www.connect4video.com und www.easymeet24.com sind bei DomainFactory gehostet. DomainFactory betreibt Webserver in eigener Verantwortung und stellt Benutzern wie C4V einen Fernzugriff zur Verfügung.
Domains (connect4video.com, easymeet24.com, deren Subdomains sowie andere relevante domains) werden bei DomainFactory verwaltet.
DomainFactory ist eine deutsche Firma und dem BDSG und der EU-DSGVO verpflichtet.
(www.df.eu, domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning)

Es werden personenbezogene Daten (IP Adressen) verarbeitet.

Das Webseiten- und Domainhosting wird abgewickelt im Rahmen des Kontingents der ZengerConsult GmbH. Die ZengerConsult ist als deutsche Firma dem BDSG und der EU-DSGVO verpflichtet und als Mehrheitsgesellschafter der C4V ausreichend sensibilisiert für die Belange des Datenschutzes und des Fernmeldegeheimnisses.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz des Fernmeldegeheimnisses
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.

Gefährdungen:
Da das Webseiten- und Domainhosting ausgelagert ist, sind folgende Gefährdungen für C4V relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Fehler bei der Webseitenprogrammierung oder Domainenverwaltung
- Benutzerverhalten

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Da das Webseiten- und Domainhosting ausgelagert ist, werden diverse Sicherheitsanforderungen vom Anbieter DomainFactory erfüllt.
Bei den oben letztgenannten Schutzzielen (Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können, Gewährleistung eines ordnungsgemäßen Betriebes der Dienste) ist zu beachten, daß diese Schutzziele relevant für das Webseiten- und Domainhosting sind, aber das Webseiten- und Domainhosting nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.

Webseitenbenutzer werden in der Datenschutzerklärung der C4V, die sich auf der Webseite befindet, über Erhebung und Speicherung personenbezogener Daten informiert.

Es werden keine personenbezogenen Daten gespeichert. Es gibt für den Admin allgemeine Benutzungsstatisitiken ohne Angaben zu den Besuchern. Weder der Hoster DomainFactory noch die Webseitensoftware Joomla liefern dem Admin Statistiken mit personenbezogenen Daten.

Die Webseiten sind verschlüsselt (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256).

Die Zugriffsberechtigungen für Webseitenprogrammierung und Domainverwaltung werden von der C4V-Firmenführung vergeben. Die Zugänge sind personalisiert. Es gibt keine allgemeinen Zugänge, die von mehreren Personen benutzt werden.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Der Webmaster pflegt die eingesetzte Softwarelösung und spielt Softwareupdates ein, wenn sie zur Verfügung stehen, die Verwendung sinnvoll ist und der Einspielaufwand in vernünftigem Verhältnis zu den erreichbaren Verbesserungen steht.
Der Webmaster sorgt für angemessene Backups.

Bewertung:
Es besteht ein Restrisiko eines Ausfalles des Webseiten- und Domainhostings. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da das Webseiten- und Domainhosting nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.
Es besteht ein Restrisiko eines unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.9 Sicherheitsteilsystem im Detail: Online-Terminvergabe

Über den Dienst eTermin können Kunden online Termine mit C4V vereinbaren. Die Webseite https://www.etermin.net/C4V wird von eTermin betrieben.

eTermin GmbH ist eine Firma in der Schweiz und der EU-DSGVO verpflichtet.
(www.etermin.net, eTermin GmbH, Wiesengrund 8, 8304 Wallisellen, Schweiz)

Es werden personenbezogene Daten (IP Adresse, Name, E-Mailadresse) verarbeitet.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz des Fernmeldegeheimnisses
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.

Gefährdungen:
Da die Webseite von eTermin betrieben wird, sind folgende Gefährdungen für C4V relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Benutzerverhalten

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Da die Webseite von eTermin betrieben wird, werden diverse Sicherheitsanforderungen vom Anbieter eTermin erfüllt.
Bei den oben letztgenannten Schutzzielen (Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können, Gewährleistung eines ordnungsgemäßen Betriebes der Dienste) ist zu beachten, daß diese Schutzziele relevant für die Online-Terminvergabe sind, aber die Online-Terminvergabe nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.

Webseitenbenutzer werden mit einem eingeblendeten Disclaimer und in der Datenschutzerklärung der C4V, die auf der Webseite verlinkt ist, über Erhebung und Speicherung personenbezogener Daten informiert.

Die Webseite ist verschlüsselt (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS 1.2).

eTermin synchronisiert die Termine über ein Outlook-Plugin mit dem lokalen Outlook des Nutzers. Die Verbindung ist mit einem private/public API Schlüssel gesichert.

Die Zugriffsberechtigungen für die Webseitenprogrammierung werden von der C4V-Firmenführung vergeben. Die Zugänge sind personalisiert. Es gibt keine allgemeinen Zugänge, die von mehreren Personen benutzt werden.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Der Webmaster pflegt die eingesetzte Softwarelösung.

Bewertung:
Es besteht ein Restrisiko eines Ausfalles der Online-Terminvergabe. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da die Online-Terminvergabe nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.
Es besteht ein Restrisiko eines unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.10 Sicherheitsteilsystem im Detail: Datenspeicherung

Ein Datenspeicherungsserver wird bei DomainFactory gehostet. Für den Server verwendet C4V in Eigenverantwortung die Software Nextcloud.
DomainFactory ist eine deutsche Firma und dem BDSG und der EU-DSGVO verpflichtet.
(www.df.eu, domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning)

Es werden personenbezogene Daten (Name, E-Mailadresse, Telefonnummer etc.) gespeichert.

Die Datenspeicherung wird abgewickelt im Rahmen des Kontingents der ZengerConsult GmbH. Die ZengerConsult ist als deutsche Firma dem BDSG und der EU-DSGVO verpflichtet und als Mehrheitsgesellschafter der C4V ausreichend sensibilisiert für die Belange des Datenschutzes und des Fernmeldegeheimnisses.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Gewährleistung eines ordnungsgemäßen Betriebes des Dienstes.

Folgende Schutzziele sind bedeutungslos:

- Schutz des Fernmeldegeheimnisses.
  Begründung: Das DV-System ist kein Fernmeldesystem.

Gefährdungen:
Folgende Gefährdungen sind relevant:

- Technische Störungen, Ausfälle
- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe
- Benutzerverhalten

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Bei den oben letztgenannten Schutzzielen (Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können, Gewährleistung eines ordnungsgemäßen Betriebes der Dienste) ist zu beachten, daß diese Schutzziele relevant für die Datenspeicherung sind, aber die Datenspeicherung nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.

Eine Backupregelung ist eingeführt. DomainFactory macht regelmäßig Backups, die die Datensicherung im Falle einer versehentlichen Löschung oder eines technischen Problems gewährleisten.

Der Zugriff auf die Datenspeicherung erfolgt über das Internet. Zugang kann über einen Webbrowser oder eine App für PCs erfolgen. Alle Verbindungen sind verschlüsselt (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256).
Die Weboberfläche hat ein vom Aussteller selbst signiertes Sicherheitszertifikat. Dies ist hier kein Problem, denn die Weboberfläche wird über eine Subdomain erreicht. Das Risiko, daß diese Subdomain umgeleitet wird, ist gering und damit akzeptabel.

Die Zugriffsberechtigungen auf die Datenspeicherung werden von der C4V-Firmenführung vergeben. Die Zugänge sind personalisiert. Es gibt keine allgemeinen Zugänge, die von mehreren Personen benutzt werden.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Bewertung:
Es besteht ein Restrisiko eines Ausfalles der Datenspeicherung. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da die Datenspeicherung nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.
Es besteht ein Restrisiko eines unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.11 Sicherheitsteilsystem im Detail: Wiki

Für ein internes Wiki wird die cloudbasierte Software Confluence von Atlassian (www.atlassian.com, Level 6, 341 George Street, Sydney, NSW 2000, Australia) verwendet.

C4V hat mit Atlassian einen Auftragsverarbeitungsvertrag und Standardvertragsklauseln abgeschlossen.

Es werden keine personenbezogenen Daten von externen Personen gespeichert. Das Wiki wird nur von C4V-Personal verwendet. Das Wiki dient dazu, die Produktdokumentation der Hersteller zu ergänzen und interne Prozesse zu unterstützen.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Gewährleistung eines ordnungsgemäßen Betriebes des Dienstes.

Folgende Schutzziele sind bedeutungslos:

- Schutz des Fernmeldegeheimnisses.
  Begründung: Das Wiki ist kein Fernmeldesystem.

Gefährdungen:
Folgende Gefährdungen sind relevant:

- Technische Störungen, Ausfälle
- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe
- Benutzerverhalten

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Da das Wiki ein gehostetes Cloudsystem ist, werden diverse Sicherheitsanforderungen vom Anbieter Atlassian erfüllt.
Bei den oben letztgenannten Schutzzielen (Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können, Gewährleistung eines ordnungsgemäßen Betriebes der Dienste) ist zu beachten, daß diese Schutzziele relevant für das Wiki sind, aber das Wiki nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.

Eine Backupregelung ist eingeführt. Atlassian macht regelmäßig Backups, die die Datensicherung im Falle einer versehentlichen Löschung oder eines technischen Problems gewährleisten.

Der Zugriff auf das Wiki erfolgt über das Internet. Zugang kann über einen Webbrowser oder eine App erfolgen. Alle Verbindungen sind verschlüsselt (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256).

Die Zugriffsberechtigungen auf das Wiki werden von der C4V-Firmenführung vergeben. Die Zugänge sind personalisiert. Es gibt keine allgemeinen Zugänge, die von mehreren Personen benutzt werden.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Bewertung:
Es besteht ein Restrisiko eines Ausfalles des Wikis. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da das Wiki nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.
Es besteht ein Restrisiko eines unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.12 Sicherheitsteilsystem im Detail: Personal

Das Personal umfasst Firmeninhaber, Geschäftsführer, Angestellte, freie Mitarbeiter sowie Geschäftspartner.
In unterschiedlicher Art und Weise verarbeitet das Personal personenbezogene Daten der Kunden.

Schutzziele:
Relevante Schutzziele sind:

- Schutz des Fernmeldegeheimnisses
- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können.
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer.
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.

Gefährdungen:
Folgende Gefährdungen sind relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Alle Mitarbeiter arbeiten im Homeoffice. Die Firma stellt Computer und Telefone zur Verfügung.
Die Mitarbeiter der C4V sind dahingehend sensibilisiert, daß bei allen C4V-Belangen der Datenschutz und das Telekommunikationsgesetz zu beachten und einzuhalten sind.
Dies bezieht sich besonders auf die Belange von Heimarbeitsplätzen (sichere WLANs, eventuelle Datenbackups, generelle Vorsicht bei potentiell verseuchten E-Mails, aktuelle Virenscanner, Zutritt zu Büroräumen, automatische Sperre der Rechner bei Inaktivität, usw.).
Die Mitarbeiter der C4V sind angewiesen, starke Passwörter zu verwenden, Zugangsdaten sicher aufzubewahren und nicht weiterzugeben.
Die Mitarbeiter der C4V sind auf einen Kodex für ethisches und rechtskonformes Verhalten verpflichtet.
C4V hat Sicherheitsrichtlinien erlassen und an die Mitarbeiter kommuniziert, die u.a. auf die besonderen Belange des Datenschutzes und des Fernmeldegeheimnisses hinweisen und an die Wahrung des Datenschutzes nach BDSG, an die Wahrung des Fernmeldegeheimnisses nach §88 TKG sowie an die strafrechtlichen Vorschriften nach §42 und §43 BDSG und §206 StGB erinnern.
Die Mitarbeiter der C4V haben eine Verpflichtungserklärung unterschrieben zur Wahrung der Vertraulichkeit personenbezogener Daten nach Art. 5 Abs. 1 f, Art. 32 Abs. 4 DSGVO, einschl. eines entsprechenden Merkblatts zur Verpflichtungserklärung (Texte der Art. 5, Art. 32 Abs. 4, Art. 83 Abs. 4 DSGVO, der §§ 42, 43 BDSG sowie der §§ 202a-d, 203 StGB).

Zugriffsberechtigungen auf Systeme werden von der C4V-Firmenführung vergeben.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Bewertung:
Es besteht ein Restrisiko, daß durch persönliches Fehlverhalten die Schutzziele verletzt werden.
Dieses Risiko ist überschaubar und akzeptabel, denn das Personal ist sorgfältig ausgewählt und hat viele Jahre Erfahrung im IT- und TK-Bereich und so entsprechendes Bewußtsein der besonderen Belange des Datenschutzes und des Fernmeldegeheimnisses.

Die Belange des Datenschutzes, der IT-Sicherheit und des Fernmeldegeheimnisses werden in der täglichen Arbeit regelmäßig thematisiert und in Erinnerung gerufen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.13 Sicherheitsteilsystem im Detail: Steuerberatung und Buchhaltung

Mit der Steuerberatung und der Buchhaltung ist das Steuerbüro Stephan beauftragt.
Das Steuerbüro Stephan ist eine deutsche Firma und dem BDSG und der EU-DSGVO verpflichtet.
(www.steuerbuero-stephan.de, Stephan Steuerberatungsgesellschaft mbH, Hans-Sachs-Str. 100, 65428 Rüsselsheim)

Es werden personenbezogene Daten (Name, Adresse etc.) verarbeitet und gespeichert.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer.

Folgende Schutzziele sind nicht relevant:

- Schutz des Fernmeldegeheimnisses
  Begründung: Steuerberatung ist kein Fernmeldesystem.
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
  Begründung: Steuerberatung ist kein operativer Teil des Dienstes für die C4V Kunden.
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.
  Begründung: Steuerberatung ist kein operativer Teil des Dienstes für die C4V Kunden.

Gefährdungen:
Folgende Gefährdungen sind relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Das Steuerbüro Stephan ist aufgrund der Natur seines Geschäftes ausreichend sensibilisiert für die Belange des Datenschutzes und des Fernmeldegeheimnisses. Auskünfte werden nur gegenüber den Finanzbehörden und den persönlich bekannten Mitarbeitern der C4V erteilt.

Löschungsfristen sind definiert und werden mit Hilfe von automatisierten Erinnerungen eingehalten.

Bewertung:
Es besteht ein Restrisiko eines Ausfalles bzw. Datenverlustes des Steuerbüros, z.B. durch außergewöhnliche Witterungseinflüsse vor Ort. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da die Steuerberatung nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.
Es besteht ein Restrisiko eines unbefugten Zuganges zum Steuerbüro, z.B. durch Einbruch. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.14 Sicherheitsteilsystem im Detail: Rechtsberatung

Rechtsberatung macht das Anwaltsbüro Kolb.
Das Anwaltsbüro Kolb ist eine deutsche Firma und dem BDSG und der EU-DSGVO verpflichtet.
(www.kolb-blickhan-partner.de, Rechtsanwälte Kolb, Blickhan & Partner mbB, Rheinstraße 20, 64283 Darmstadt)

Es werden personenbezogene Daten (Name, Adresse etc.) verarbeitet und gespeichert.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer.

Folgende Schutzziele sind nicht relevant:

- Schutz des Fernmeldegeheimnisses
  Begründung: Rechtsberatung ist kein Fernmeldesystem.
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
  Begründung: Rechtsberatung ist kein Fernmeldedienst.
- Gewährleistung eines ordnungsgemäßen Betriebes der Dienste.
  Begründung: Rechtsberatung ist kein Fernmeldedienst.
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
  Begründung: Das Anwaltsbüro hat generell keinen Zugriff auf TK- und DV-Systeme

Gefährdungen:
Folgende Gefährdungen sind relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Das Anwaltsbüro Kolb ist aufgrund der Natur seines Geschäftes ausreichend sensibilisiert für die Belange des Datenschutzes und des Fernmeldegeheimnisses. Auskünfte werden nur in Absprache mit und gegenüber den persönlich bekannten Mitarbeitern der C4V erteilt.

Löschungsfristen sind definiert und werden mit Hilfe von automatisierten Erinnerungen eingehalten.

Bewertung:
Es besteht ein Restrisiko eines Ausfalles bzw. Datenverlustes des Anwaltsbüros, z.B. durch außergewöhnliche Witterungseinflüsse vor Ort. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da die Rechtsberatung kein operativer Teil des Dienstes für die C4V Kunden ist.
Es besteht ein Restrisiko eines unbefugten Zuganges zum Anwaltsbüro, z.B. durch Einbruch. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

2.15 Sicherheitsteilsystem im Detail: Telefonanlage

Als Telefonanlage wird ein cloudbasierter Dienst von sipgate verwendet.
Sipgate ist eine deutsche Firma und dem BDSG und der EU-DSGVO verpflichtet.
(www.sipgate.de, sipgate GmbH, Gladbacher Straße 74, 40219 Düsseldorf)

Es werden personenbezogene Daten (Telefonnummern) verarbeitet und gespeichert.

Schutzziele:
Relevante Schutzziele sind:

- Schutz personenbezogener Daten
- Sicherheit vor unerlaubten Zugriffen auf TK- und DV-Systeme
- Schutz des Fernmeldegeheimnisses
- Reduzierung der Auswirkung von Sicherheitsverletzungen auf Nutzer
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können
- Gewährleistung eines ordnungsgemäßen Betriebes des Dienstes.

Gefährdungen:
Da die Telefonanlage ein gehostetes Cloudsystem ist, sind folgende Gefährdungen für C4V relevant:

- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Benutzerverhalten

Sicherheitsanforderungen:

- Erhebung und Speicherung personenbezogener Daten erfolgt nur gesetzkonform oder nach Einwilligung des Betroffenen.
- Löschungsfristen sind gesetzeskonform zu gestalten und einzuhalten.
- Verarbeitung, Nutzung, Verwendungszweck sind gesetzeskonform zu gestalten.
- Zugriffsberechtigungen sind nur Berechtigten zu erlauben.
- Schutz gespeicherter personenbezogener Daten ist zu gewährleisten.
- Schutz personenbezogener Daten vor Zerstörung und Verlust ist zu gewährleisten.

Schutzmaßnahmen:
Da die Telefonanlage ein gehostetes Cloudsystem ist, werden diverse Sicherheitsanforderungen vom Anbieter sipgate erfüllt. Die sipgate GmbH arbeitet ausschließlich mit nach ISO 27001 zertifizierten Rechenzentren zusammen.
Bei den oben letztgenannten Schutzzielen (Schutz vor Störungen, die zu erheblichen Beeinträchtigungen führen können, Gewährleistung eines ordnungsgemäßen Betriebes der Dienste) ist zu beachten, daß diese Schutzziele relevant für die Telefonie sind, aber die Telefonanlage nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.

Löschungsfristen sind definiert und werden von sipgate eingehalten.

Die Zugriffsberechtigungen für Benutzer und für Administratoren werden von der C4V-Firmenführung vergeben. Die Zugänge sind personalisiert. Es gibt keine allgemeinen Zugänge, die von mehreren Personen benutzt werden.
Zugriffsberechtigungen auf Systeme werden dokumentiert. Dies dient der Prozesse bei Ein- und Freistellung von Mitarbeitern sowie des Notfallmanagements im Falle des Verlustes der Zugangsdaten.

Der Zugriff auf die Konfiguration der Telefonanlage erfolgt über das Internet. Alle Verbindungen sind verschlüsselt (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384).

Bewertung:
Es besteht ein Restrisiko eines Ausfalles der Telefonanlage. Dieses Restrisiko ist überschaubar und akzeptabel, insbesondere da die Telefonanlage nicht operativer Teil des Dienstes ist, den die Kunden von C4V verwenden.
Es besteht ein Restrisiko eines unbefugten Zuganges. Dies ist überschaubar und akzeptabel angesichts der verwendeten Sicherheitsmaßnahmen.
Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.

3 Bewertung des Gesamtsystems

Das Gesamtsystem wird gebildet aus den zusammenwirkenden Sicherheitsteilsystemen.

Es bleibt ein Restrisiko, daß Schutzziele verletzt werden oder die Verfügbarkeit des Dienstes nicht sichergestellt ist.
Dieses Restrisiko besteht im Wesentlichen aus außergewöhnlichen Witterungseinflüßen auf Sicherheitsteilsysteme, aus persönlichem Fehlverhalten von Mitarbeitern und daraus, daß der ganze Dienst und die Kommunikation zwischen den Sicherheitsteilsystemen über das öffentliche Internet läuft.

Dieses Restrisiko ist überschaubar und akzeptabel, denn:

- Der Hauptteil des Dienstes ist redundant aufgebaut durch die Verwendung geographisch getrennter Rechenzentren.
- Die Infrastruktur wird laufend überwacht, um bei Störungen schnell reagieren zu können.
- Mit Hilfe eines eigenen Notfallkonzeptes ist es C4V möglich, im Falle eines Totalausfalls eines Dienstes den Kunden schnell vorübergehend Kapazitäten des anderen Dienstes zur Verfügung zu stellen.
- Zugänge zu datenverarbeitenden Systemen werden abgesichert mit Passwörtern, Verschlüsselung bzw. Zutrittskontrollen. Zutritts- und Zugriffsrechte werden sorgfältig vergeben und dokumentiert.
- Mitarbeiter werden sorgfältig ausgewählt und entsprechend sensibilisiert für die Belange des Datenschutzes und des Fernmeldegeheimnisses.

Die Aktualität des Sicherheitskonzeptes und die Wirksamkeit der Schutzmaßnahmen werden regelmäßig geprüft. Bei Bedarf werden entsprechende Änderungen vorgenommen.
Die Regelmäßigkeit wird mit Hilfe von automatisierten Erinnerungen sichergestellt.

Daher folgt:
Die Sicherheitsanforderungen sind erfüllt, die Schutzziele erreicht.