EDV-Ingenieurbüro GmbH

Auftragsverarbeitung (AV) nach DS-GVO, Artikel 28

Ergänzung zum KSR-Softwarepflegevertrag

9605 – 28.04.2022

EDV-Ingenieurbüro GmbH

Inhalt

Hinweis: Die TeamViewer Sicherheitsinformationen können auch im Internet heruntergeladen werden:
https://dl.teamviewer.com/docs/de/TeamViewer-Security-Statement-de.pdf

1. Gegenstand des Auftrags

Dieses Dokument ist eine Ergänzung zum Softwarepflegevertrag, nachfolgend "Auftrag" genannt, zwischen der KSR EDV Ingenieurbüro GmbH (KSR) und dem Auftraggeber.

Der Auftrag umfasst folgende Leistungen:

- Bereitstellung von Programmupdates, die den dauerhaften Betrieb der gekauften / gemieteten Software sicherstellen.
- Unterstützung der Anwender via Telefon oder Fernwartung.

Der Auftrag über die Softwarepflege zielt allein auf die Supportleistung ab.
Wartung und Prüfung sind so organisiert und geregelt, dass Kunden-Daten angemessen geschützt sind. Die Schutzmaßnahmen werden im Kapitel Technische und Organisatorische Maßnahmen dargelegt.

Im Rahmen eines Supports ggf. übermittelte (pb-)Daten verlassen nicht das IT-System von KSR.

Hinweis zur Speicherung dieses Dokuments in VCS
Dieses Dokument kann vom Kunden seit der VCS-Version 2.50.77 über das Hilfemenü (Wichtige Dokumente) aufgerufen und gespeichert werden. Aktualisierungen werden mit VCS-Setups in das Programm übernommen. Siehe hierzu auch Anhang "Wichtige Dokumente …".

2. Dauer

Der Auftrag beginnt ab der Unterzeichnung der Bestellung durch den Verantwortlichen.
Die Dauer richtet sich nach den im Angebot bzw. in der Bestellung festgelegten Vereinbarungen.

3. Art und Zweck der vorgesehenen Verarbeitung von Daten

Zur Auftragserfüllung ist die Ansicht von personenbezogenen Daten beim Verantwortlichen nicht zu vermeiden.

Die nachfolgende Liste beschreibt typische Fälle, in denen unsere Mitarbeiter in Kontakt mit Daten des Verantwortlichen kommen.

3.1 Ansicht / Nutzung von Daten per Fernwartung

Zur Diagnose bzw. Behebung eines Anwenderproblems kann es erforderlich sein,

- sich die zugehörigen Daten im Programm des Verantwortlichen per Fernwartung anzuschauen oder telefonisch beschreiben zu lassen.
- per Fernwartung Listen zu erstellen oder sonstige Programmfunktionen auszuführen. Diese Listen, Protokolle, etc. können personenbezogene Daten enthalten.
- im betreffenden Programm Daten zu erfassen, zu ändern oder zu löschen. Soweit möglich, werden die Arbeiten anhand von Testdaten durchgeführt, die anschließend wieder gelöscht werden.
  Arbeiten mit echten Daten erfolgen generell in Absprache mit dem Verantwortlichen.

3.2 Ansicht / Nutzung von Daten bei KSR

Zur internen Klärung oder für spätere Rückfragen kann es erforderlich sein, Dateien mit personenbezogenen Daten an KSR zu übertragen. Das können z. B. sein:

- Screenshots (engl. für Bildschirmkopie, Bildschirmfoto) oder Videoaufzeichnungen von den zu klärenden Programmfunktionen
- Druckdateien von Listen, Belegen etc.
- Schnittstellen- oder Protokoll-Dateien

3.3 Programminstallation per Fernwartung

- Bei der Installation werden via Fernwartung neue Programmdateien auf das DV-System des Verantwortlichen übertragen.
  Hinweis: Bei einer Programminstallation werden keine personenbezogenen Daten übertragen oder verändert. Jede Datenübertragung bringt aber auch bei größter Sorgfalt ein Restrisiko für die vorhandenen Daten auf dem DV-System des Verantwortlichen mit sich.
- Vor der Installation kann es erforderlich sein, von bereits vorhandenen Daten eine temporäre Sicherheitskopie zu erstellen. Diese wird auf dem DV-System des Verantwortlichen gespeichert und nach der Installation wieder gelöscht.
- Um eine neue Installation zu testen, kann es erforderlich sein, im neu installierten Programm Daten anzuzeigen oder zu bearbeiten, Listen zu erstellen oder sonstige Programmfunktionen auszuführen. Soweit möglich, werden die Tests anhand von Testdaten durchgeführt, die anschließend wieder gelöscht werden.
  Tests mit echten Daten erfolgen generell in Absprache mit dem Verantwortlichen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

4. Art der Daten und Kategorien der betroffenen Personen

Je nachdem, welche KSR-Softwareprodukte bestellt und installiert wurden, können unsere Mitarbeiter mit folgenden personenbezogenen Daten in Kontakt kommen:

- IP-Adressen des Verantwortlichen.
- Jede Art von Daten, die sich auf dem gleichen DV-System befinden, auf dem die KSR-Softwareprodukte installiert sind.

Produkt	Art der Daten	Kategorien der betroffenen Personen
VIS = Vehicle Inhouse System VCS = Vehicle Calculation System VCS = Vehicle Trading System	• Adresse • Kontaktdaten • Geburtsdatum, -ort • Bankverbindung • Angaben zur berufl. Funktion, Status • Umsätze • Ansprechpartner • Fahrzeug-Zuordnung inkl. Kfz-Kennzeichen und Fahrzeugidentifikationsnummer • Zuständiger Kfz-Versicherer • Kauf- und Zahlungsverhalten • Geodaten	• Privatkunden des Verantwortlichen • Partner wie z. B. Gutachter • Ansprechpartner bei Kunden/ Lieferanten / Versicherungen / sonstigen Partnern des Verantwortlichen • Mitarbeiter des Verantwortlichen
TCS Time Calculation System TMT TCS Mobile Terminal	• Adresse • Kontaktdaten • Geburtsdatum • Geschlecht • Passbild • Ein-/Austrittsdatum • Personalart, Arbeitsgruppe/Abteilung • Lohnvorgabe, Sollstunden • Bewertungsfaktor • Infos zu Urlaub, Gleitzeit • Stempelzeiten • Fehlzeiten (Krankheit, Urlaub, Schulung, Gleitzeitausgleich)	• Mitarbeiter des Verantwortlichen
Sonstige Produkte, z. B. EKS, JPS2/APS2, Dashboard, MOW, RMA, AMG, Fzg-Scan, etc.	Alle anderen Produkte basieren auf VCS oder TCS und enthalten eine Teilmenge der oben aufgeführten personenbezogenen Daten.	Alle anderen Produkte basieren auf VCS oder TCS und betreffen einen Teil der oben aufgeführten Personenkategorien.

5. Technische und organisatorische Maßnahmen

Zum Schutz der personenbezogenen Daten des Verantwortlichen, die sich entweder bei KSR befinden oder auf die KSR-Mitarbeiter per Fernwartung Zugriff haben, trifft KSR standardmäßig die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen.

Hinweis: Die oben genannten Datensicherheitsmaßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

Maßnahmenziel	Maßnahmen
Vertraulichkeit (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die Unbefugten den Zutritt zu Räumen und Systemen mit personenbezogenen Daten verwehren* • Kein unbefugtes Betreten des KSR-Gebäudes oder des Server-Raums durch: - Alarmanlage mit Verbindung zu externem Wachdienst - Videoüberwachung - abgesicherte Gebäudeschächte, Sicherheitsschlösser - Durchgängig verschlossene Zugangstüren zu Gebäude und Server-Raum, Zugang zum Gebäude nur mit Transponder oder Schlüssel, Besucher müssen klingeln. - Zugang zum Serverraum nur nach Code-Eingabe. - Während der Geschäftszeiten durchgängig besetzter Empfang, Besucher-Einlass durch den Empfang entweder persönlich oder per elektronischem Türöffner. • Sichere Vergabe von Schlüsseln/Transpondern/Codes: - Transponderübergabe frühestens nach Ablauf der Probezeit - Schlüsselvergabe und Alarmanlagen-Code nur an langjährige Mitarbeiter und Geschäftsleitung, Aufbewahrung der restlichen Schlüssel im Tresor. - Schriftliche Belehrung/Information zur Aufbewahrung des Schlüssels/ Transponders mit sofortiger Informationspflicht bei Verlust. - Führen einer KSR-internen Schlüsselliste zur Dokumentation der verfügbaren Schlüssel/Transponder und der aktuellen Besitzer. • Reinigungsarbeiten erfolgen durch eine Gebäudereinigungsfirma, mit der eine Vereinbarung zur Verschwiegenheit besteht.
	Maßnahmen, die die unbefugte Nutzung der DV-Systeme bei KSR verhindern • Authentifizierung erforderlich an allen Rechnern mit Benutzername und Kennwort. • Passwortrichtlinie: mind. 8 Zeichen, Mischung aus Groß-/Kleinschreibung, Zahlen und Sonderzeichen (zentral geregelt über Active Directory). • Eindeutige Benutzerkennung für jeden Mitarbeiter und Berechtigungskonzept im Active Directory. • Anti-Viren-Software “Sophos Anti-Virus” • Hardware-Firewall inclusive Intrusion Detection System “Sophos UTM” • Software- und hardwarebasierte VPN-Technologien (Virtual Private Network) oder RemoteDesktop-Gateways für gesicherten Zugriff „von außen“ auf das KSR-Netzwerk (z.B. für Mitarbeiter in den Vertriebsbüros/im Home-Office).

Maßnahmenziel	Maßnahmen
Vertraulichkeit (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die bei und nach der Verarbeitung personenbezogener Daten die Vertraulichkeit sicherstellen* • Anzahl der Systemadministratoren auf das „Notwendigste“ reduziert (2 Personen mit Informatik-Ausbildung). • Verwaltung der Rechte nur durch Systemadministration oder Geschäftsleitung. • Restriktives, bedarfsorientiertes Berechtigungskonzepts nach Abteilungszu-gehörigkeit und Funktion im Active Directory. • Eigenes Fremddatenverzeichnis für Dateien von Kunden mit eingeschränktem Benutzerkreis. Nach Abschluss der Bearbeitung eines Kundenproblems werden die zugehörigen Dateikopien sofort gelöscht, sofern nicht mehr benötigt. • Zentrale Ausgabe und Rückgabe von mobilen Datenträgern (z. B. Notebooks, externe Platten), sachgerechte Formatierung gebrauchter Geräte sofort nach der Rückgabe. • mehrere elektrische Aktenvernichter zur Entsorgung gedruckter Screenshots oder Listen, handschriftlicher Aufschriebe und sonstiger Papiere mit vertraulichem Inhalt. • Professionelle Löschung/Vernichtung von alten oder defekten Datenträgern durch einen zertifizierten Entsorger.
Integrität (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die bei Transport und elektr. Übertragung personenbezogener Daten die Vertraulichkeit sicherstellen* • Verwendung von VPN-Tunneln oder RemoteDesktop-Gateways zur Übertragung von Daten zwischen der KSR-Zentrale und den Mitarbeitern in Vertriebsbüros, Home-Office oder bei Kunden. • Sichere Übertragung von Daten bei Fernwartungssitzungen durch: - Fernwartungsprogramme „TeamViewer““, der höchste Sicherheitsansprüche erfüllt (siehe Anlage). - KSRseitige Absicherung von Datenübertragungen an den Verantwortlichen durch Virenscanner, Firewall, unterbrechungsfreie Stromversorgung (USV). • Weitergabe von Datenträgern, Papieren, etc. nur durch eigene Mitarbeiter oder vertrauenswürdige Transporteure (z. B. Post) in sicherer Verpackung. Annahme und interne Verteilung aller Sendungen durch KSR-Zentrale.
	Maßnahmen, die die Verarbeitung personenbez. Daten nachvollziehbar machen **Hinweis:** Die Erfassung, Änderung oder Löschung von personenbezogenen Daten für den Verantwortlichen ist nicht Gegenstand des Auftrags. Sollte es zur Problemdiagnose erforderlich sein, einen einzelnen Datensatz temporär zu erfassen, zu ändern oder zu löschen gelten folgende Richtlinien: • Soweit möglich, werden Tests mit eigenen, erdachten Testdaten durchgeführt, die nach Testende sofort wieder gelöscht werden. • Tests mit echten Daten generell nur in Absprache mit dem Verantwortlichen. • Der Verantwortliche kann die Arbeiten und Tests jederzeit am Bildschirm beobachten oder unter Anleitung unserer Mitarbeiter selbst durchführen. • Unsere Mitarbeiter führen Tests und Arbeiten unter dem Benutzernamen „Support“ durch. In den KSR-Programmen wird dieser Name bei der Erfassung oder Änderung von Daten zusammen mit dem Datum am betreffenden Datensatz gespeichert und ermöglicht so die Unterscheidung von den eigenen Bearbeitungen des Verantwortlichen.

Maßnahmenziel	Maßnahmen
Integrität (Art. 32, Abs.1 b DS-GVO)	**Hinweis:** Manche Software-Probleme lassen sich unter dem Benutzernamen „Support“ nicht nachvollziehen. In diesem Fall müssen die Tests unter dem Benutzernamen des Mitarbeiters durchgeführt werden, der das Problem gemeldet hat. Nachdem sich dieser mit seinem Benutzernamen angemeldet hat, kann er die Tests entweder unter Anleitung von KSR selbst durchführen oder am Bildschirm beobachten.
Verfügbarkeit & Belastbarkeit (Art. 32, Abs.1 b DS-GVO)	*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.* **Hinweis:** Die Erfassung, Änderung oder Löschung von personenbezogenen Daten für den Verantwortlichen ist nicht Gegenstand des Softwarepflegevertrags. Daraus folgt, dass keine Original-Daten des Verantwortlichen bei KSR gespeichert sind. Folgende technische Maßnahmen dienen generell der ständigen Verfügbarkeit aller Daten bei KSR: • Feuer- und Rauchmeldeanlagen, generelles Rauchverbot innerhalb des Gebäudes • Unterbrechungsfreie Stromversorgung (USV) • Spezielle Schutzmaßnahmen für den Serverraum: - Alarmmeldung bei unberechtigtem Zutritt zum Serverraum - Klimaanlage, Feuerlöscher - Geräte zur Überwachung von Temperatur und Feuchtigkeit • Hohe Ausfallsicherheit der Server durch redundante Datenspeicher (RAID) • automatisierte tägliche Sicherung der Server • mindestens 1x jährlich Recovery-Test (Datenwiederherstellung) • Datensicherungen werden an einem sicheren Ort außerhalb des KSR-Gebäudes aufbewahrt.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32, Abs. 1 d DS-GVO).	*Maßnahmen, die sicherstellen, dass keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers erfolgt.* • Die zu erbringenden Leistungen werden praktisch ausschließlich per Fernwartung oder telefonisch erbracht. Dabei sind unsere Mitarbeiter in direktem Kontakt mit dem Verantwortlichen, so dass schon dadurch eine Auftragskontrolle gegeben ist. • Das eingesetzte Fernwartungsprogramm „TeamViewer“ und „ISLLight“ ist so konzipiert, dass Sicherheit und Kontrollierbarkeit einer Fernwartungssitzung oberste Priorität haben. Konkret bedeutet dies: - Eine Fernwartungssitzung ist nur möglich in Absprache mit dem Verantwortlichen, da dieser einen bestimmten Code eingeben muss. Dieser Code wird für jede Sitzung neu vergeben. - Jede Fernwartungssitzung kann vom Verantwortlichen am Bildschirm des gewarteten Rechners beobachtet werden. - Der Verantwortliche kann jederzeit wieder die Steuerung übernehmen. - Eine Fernwartungssitzung kann vom Verantwortlichen jederzeit abgebrochen werden.

6. Berichtigung, Einschränkung und Löschung von Daten

Es erfolgt keine Berichtigung, Einschränkung oder Löschung von Daten des Verantwortlichen durch KSR. Deshalb ist für die Wahrung der Rechte der Betroffenen bzgl. Berichtigung, Einschränkung und Löschung von Daten in den zu wartenden DV-Systemen der Verantwortliche zuständig. Falls zur Auftragserfüllung temporär Datenkopien von Betroffenen bei KSR vorliegen, wird KSR den Verantwortlichen bei der Wahrung der Rechte des Betroffenen bzgl. dieser Kopien unterstützen und die nötigen Maßnahmen treffen.

7. Qualitätssicherung und sonstige Pflichten von KSR

KSR verpflichtet sich, die ihr zugänglichen oder überlassenen Daten ausschließlich im Rahmen des zugrunde liegenden Softwarepflegevertrags und der damit verbundenen Weisungen des Verantwortlichen zu nutzen.

7.1 Weisungsberechtigte Person bei KSR

Folgende Person ist zur Erteilung und Entgegennahme von Weisungen befugt:

Geschäftsführer Peter Ringhut. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage von KSR sowie im Kapitel "Kontakt" dieses Dokuments angegeben.

7.2 Datenschutzbeauftrager bei KSR

Die einschlägigen datenschutzrechtlichen Vorschriften sind der KSR bekannt und deren Einhaltung wird überwacht.
Ein betrieblicher Datenschutzbeauftragter ist bestellt und der Meldebehörde bekannt.
Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage von KSR sowie im Kapitel "Kontakt" dieses Dokuments angegeben.

7.3 Geheimhaltungspflicht der KSR-Mitarbeiter

Alle Mitarbeiter der KSR sind schriftlich auf das Datengeheimnis verpflichtet und wurden mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht.

8. Unterauftragsverhältnisse

(1) KSR zieht zur Erbringung von Softwarepflege-Leistungen keine Subunternehmen heran.

(2) Bei fremd vergebenen Nebenleistungen (z. B. Datenträgerentsorgung, Netzwerkwartung, etc.) trifft KSR zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen angemessene und gesetzeskonforme vertragliche Vereinbarungen und ergreift entsprechende Kontrollmaßnahmen.

9. Kontrollrechte des Verantwortlichen

(1) KSR verpflichtet sich, dem Verantwortlichen eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen, z. B. durch den Einsatz von Technologien, mit denen der Verantwortliche die durchgeführten Arbeiten auf einem Monitor verfolgen kann.

(2) Wenn der Verantwortliche die Tätigkeiten nicht via Monitor beobachten möchte oder kann, kann er von KSR die Erstellung und Überlassung einer Videoaufzeichnung der durchgeführten Arbeiten verlangen. Die Aufzeichnung erfolgt nur bei ausdrücklicher Aufforderung.

(3) KSR erklärt sich damit einverstanden, dass der Verantwortliche jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz sowie die Einhaltung der vorliegenden Ergänzung zum Auftrag im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften. Je nach Aufwand behält sich KSR vor, einen Vergütungsanspruch geltend zu machen.

10. Mitteilung bei Verstößen durch KSR

(1) KSR unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Verletzungen von Datenschutzbestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen.

Insbesondere bei Verdacht auf eine Verletzung des Schutzes personenbezogener Daten gem. Art. 33, 34 EU-DSGVO (meldepflichtige Datenpanne) ist der Verantwortliche unverzüglich zu benachrichtigen. Soweit den Verantwortlichen Pflichten nach Art. 33, 34 EU-DSGVO treffen, unterstützt KSR ihn hierbei.

KSR unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten:

Art. 32 Sicherheit der Verarbeitung

Art. 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Art. 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

Art. 35 Datenschutz-Folgenabschätzung

Art. 36 Vorherige Konsultation mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten seitens KSR zurückzuführen sind, kann KSR eine Vergütung beanspruchen.

11. Umfang der Weisungsbefugnisse des Verantwortlichen

(1) Der Verantwortliche hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren zu einer einzelnen Softwarepflege-Leistung zu erteilen. Weisungen können schriftlich, telefonisch oder per E-Mail/Online-Support-Anfrage erteilt werden.
Bei unüblichen Weisungen kann KSR verlangen, dass diese Weisungen schriftlich erteilt werden.

(2) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Verantwortlichen entstehen, bleiben unberührt.

(3) Der Verantwortliche informiert die KSR unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Wartung und Pflege durch KSR feststellt.

(4) Ist KSR der Ansicht, dass eine Weisung des Verantwortlichen gegen die Datenschutzvorschriften verstößt, wird sie den Verantwortlichen unverzüglich darauf hinweisen.

12. Datenträger-Rückgabe und Daten-Löschung bei Auftragsende

(1) Nach Abschluss jeder Softwarepflege-Leistung werden die dabei erzeugten Dateikopien oder Ausdrucke standardmäßig sofort gelöscht bzw. vernichtet.

(2) Sollte es für spätere Rückfragen oder aus Gewährleistungsgründen erforderlich sein, Dateien bzw. Ausdrucke länger bei KSR aufzubewahren, erfolgt die Löschung bzw. Vernichtung spätestens bei Beendigung des Auftragsverhältnisses.

(3) Datenträger des Verantwortlichen werden in Absprache mit dem Verantwortlichen entweder zurückgegeben oder datenschutzgerecht gelöscht und vernichtet.

Anhang

Glossar

Glossar und Abkürzungsverzeichnis	
Begriff	**Beschreibung**
Auftragsverarbeitung	Die Auftragsverarbeitung ist die zielgerichtete Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragsverarbeiter gemäß den Weisungen des für die Datenverarbeitung Verantwortlichen auf Grundlage eines Vertrages.
Verantwortlicher/ Auftragsverarbeiter	Art. 28 DS-GVO: Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
Anonymisierung *)	Bei der Anonymisierung werden personenbezogene Daten verändert, so dass diese Daten nicht mehr einer bestimmten Person zugeordnet werden können.
Pseudonymisierung *)	Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym ersetzt, so dass die Feststellung der Identität der Person ausgeschlossen oder wesentlich erschwert wird.
Löschen *)	Beim Löschen werden Daten unwiederbringlich entfernt, so dass sie nicht wiederhergestellt werden können. Dies betrifft alle Daten, auch personenbezogene.

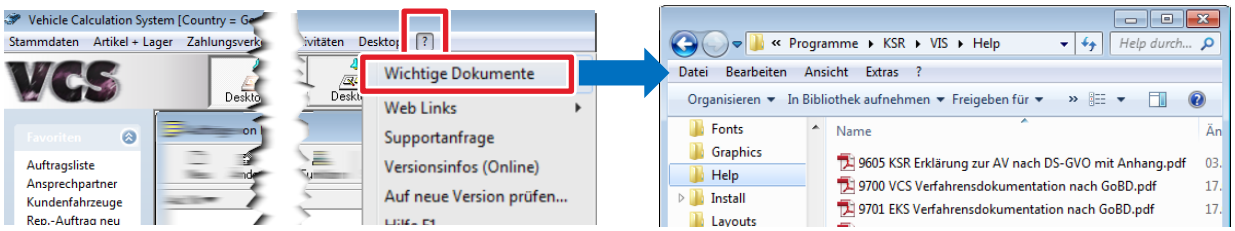
Legende: *) Dieser Begriff wird hier zum besseren Verständnis und zur Abgrenzung genannt. In diesem Dokument wird darauf nicht weiter eingegangen.

Wichtige Dokumente zu DS-GVO und GoBD über den Menüpunkt "Hilfe" öffnen

Bereits seit der VCS-Version 2.50.48 können Sie die VCS-Verfahrensdokumentation nach GoBD direkt in VCS öffnen. Zu den GoBD-Dokumenten kamen nach und nach die Dokumente von BDSG und seit Mai 2018 Dokumente der DS-GVO.

Mit dem Anwachsen der Themen und der Dokumentenzahl wurde nun der Zugang zu diesen Dokumenten vereinheitlicht und Sie haben problemlos Zugriff auf wesentliche Informationen. Die darin enthaltenen Dokumente werden fortlaufend gepflegt und ergänzt.

Öffnen Sie über den Menüpunkt "Hilfe? → Wichtige Dokumente" das Verzeichnis "Help" von VCS/VIS/VES im Windows Explorer. Alle wichtigen Dateien zu GoBD, DS-GVO u. a. wichtigen Themen sind hier zu finden. Doppelklicken Sie die Datei, die Sie öffnen möchten.



Bitte beachten Sie: Studieren Sie diese Dokumente aufmerksam und erkundigen Sie sich jederzeit bei uns, wenn Sie Fragen haben oder zu einem Punkt vertiefte Informationen wünschen.

Historie der Ablagestruktur

ab VCS-Version	Dokument-kategorie	Inhalt	Erläuterung	Versions-news
2.50.90	GoBD und DS-GVO	Menüpunkt "Wichtige Dokumente" öffnet direkt den Windows-Explorer mit den aktuellen PDF-Dokumenten von GoBD und DS-GVO	Alle Dokumentkategorien werden über das Kontextmenü der Hilfe --> Wichtige Dokumente geöffnet	9213
2.50.77	GoBD und BDSG	VCS GoBD-Dokumente und Auftragsdatenverarbeitung sind über das "Hilfe ?-Menü" erreichbar	Für jede Dokumentkategorie gibt es ein eigenes Verzeichnis im Kontextmenü der Hilfe	9209
2.50.48	GoBD	GoBD: Verfahrensdokumentation direkt aus VCS aufrufbar	Über Stammdaten ist das PDF aufrufbar	9207

Bitte beachten Sie: Ab der VCS Version 2.50.74 ist der Ordner "Wichtige Dokumente" verfügbar. Ab der VCS Version 2.50.91 wird über den Ordner "Wichtige Dokumente" das Verzeichnis im Windows Explorer geöffnet, in dem die Dokumente gespeichert sind.

Änderungs- und Versionshistorie

Version	Datum	Erläuterung	geändert durch
1.7	28.04.2022	▪ Kapitel Kontakt überarbeitet	KSR EDV GmbH / GRE
---	10.08.2021	Kapitel 5 um das Produkt Fahrzeug-Scan erweitert Im Jahr 2021 wurde keine Überarbeitung des Dokuments veröffentlicht	KSR EDV GmbH / GRE
1.6	09.07.2020	▪ Kapitel "Mitteilung bei Verstößen durch den KSR" überarbeitet	KSR EDV GmbH / GRE
1.5	05.02.2020	▪ Titel des Dokuments geändert, "Erklärung" entfällt ▪ "Erklärung" ersetzt im gesamten Dokument ▪ Den Satz "Eine Erhebung oder Verarbeitung von Daten für den Verantwortlichen ist nicht Gegenstand des Auftrags." gelöscht ▪ Hinweis von Kapitel 5 vor die Tabelle gestellt ▪ Auszug aus der Datenschutzgrundverordnung (DS-GVO) entfällt komplett ▪ Neuer Anhang: "Wichtige Dokumente zu DS-GVO und GoBD über den Menüpunkt "Hilfe" öffnen" neu ▪ Versionshistorie in den Anhang verschoben	KSR EDV GmbH / GRE
1.4	26.07.2019	▪ Kapitel 1: Hinweis zur Speicherung dieses Dokuments in VCS	KSR EDV GmbH / GRE
1.3	15.07.2019	▪ Kapitel 5 - Vertraulichkeit geändert, da ab sofort externe Gebäudereinigungsfirma ▪ Kapitel 7 in Unterkapitel unterteilt ▪ Glossar angepasst	KSR EDV GmbH / GRE
1.2	02.04.2019	▪ Layoutanpassungen ▪ Anhang 2 "islonline Security Statement" entfällt komplett ▪ Glossar neu	KSR EDV GmbH / GRE
1.1	03.05.2018	▪ Umbenennung des Titels ▪ Layoutanpassungen	KSR EDV GmbH / GRE
1.0	30.03.2018	Freigabe des Dokuments	KSR EDV GmbH / AST

Kontakt

KSR EDV-Ingenieurbüro GmbH
Adenauerstraße 13/1
D-89233 Neu-Ulm

Sie erreichen uns **telefonisch** unter
+49 (0) 731 / 20 555 - 0

Per **Fax** unter
+49 (0) 731 / 20 555 - 450

Öffnungszeiten

Montag - Donnerstag	08.00 bis 18.00 Uhr
Freitag	08.00 bis 16.30 Uhr

Geschäftsleitung
Peter Ringhut Dipl.-Ing. Elektrotechnik (FH) Techn. Informatik

Direkt per **E-Mail**
info@ksredv.de

Datenschutzbeauftragter (DSB)
datenschutz@ksredv.de

TeamViewer Sicherheitsinformationen

Zielgruppe

Dieses Dokument richtet sich an professionelle Netzwerkadministratoren. Die Informationen in diesem Dokument sind technischer Art und sehr detailliert. Anhand dieser Informationen können sich IT-Profis bereits vor dem Einsatz von TeamViewer ein fundiertes Bild von der Softwaresicherheit machen. Gerne können Sie dieses Dokument auch Ihren Kunden weiterleiten, um eventuelle Sicherheitsbedenken auszuräumen.

Falls Sie sich selbst nicht zur Zielgruppe zählen, helfen Ihnen vielleicht dennoch die Softfacts im Abschnitt „Das Unternehmen / die Software“, um sich ein subjektives Bild zu machen.

Das Unternehmen / die Software

Über uns

Die TeamViewer GmbH wurde 2005 gegründet und hat Ihren Sitz im süddeutschen Göppingen (Nähe Stuttgart) mit weiteren Niederlassungen in Australien und den USA. Wir beschäftigen uns ausschließlich mit Entwicklung und Vertrieb von sicheren Systemen für die webbasierte Zusammenarbeit und Kommunikation. Ein rasanter Start und schnelles Wachstum haben zu über 200 Millionen Installationen der TeamViewer Software und Nutzern in fast allen Ländern der Erde geführt. Die Software ist in mehr als 30 Sprachen verfügbar.

Die Entwicklung findet ausschließlich in Deutschland statt. Auch Vertrieb und Support werden von Deutschland aus geleistet.

Unser Sicherheitsverständnis

TeamViewer wird weltweit millionenfach für den spontanen Support über das Internet, den Zugriff auf unbeaufsichtigte Server (z. B. Serverfernwartung) und für Online Meetings eingesetzt. Je nach Konfiguration von TeamViewer bedeutet dies, dass der entfernte Computer gesteuert werden kann, als säße man direkt davor. Ist der am entfernten Computer angemeldete Benutzer Windows-, Mac- oder Linux-Administrator, so erhält man also Administrator-Rechte am Computer.

Es ist offensichtlich, dass solch mächtige Funktionalität über das an und für sich unsichere Internet gegen verschiedenste Arten von Angriffen abgesichert werden muss. Tatsächlich dominiert das Thema Sicherheit bei uns alle anderen Entwicklungsziele – um den Zugriff auf Ihre Computer sicher zu gestalten und selbstverständlich auch um unsere ureigensten Interessen zu wahren: Denn nur einer sicheren Lösung vertrauen weltweit Millionen Anwender und nur eine sichere Lösung sichert langfristig unseren Unternehmenserfolg.

Externes Expertengutachten

Unsere Software TeamViewer wurde durch den Bundesverband der IT-Sach-verständigen und Gutachter e.V. (BISG e.V.) mit dem Qualitätssiegel mit fünf Sternen (Maximalwert) ausgezeichnet. Die unabhängigen Sachverständigen des BISG e.V. prüfen Produkte qualifizierter Hersteller auf Qualitäts-, Sicherheits- und Serviceeigenschaften.

Referenzen

Zum aktuellen Zeitpunkt ist TeamViewer auf über 200.000.000 Computern im Einsatz. Internationale Top-Unternehmen aus allen Branchen (inklusive hochsensibler Bereiche wie Banken, Finanzwirtschaft, Gesundheitswesen und Regierungswesen) setzen TeamViewer erfolgreich ein.

Wir laden Sie herzlich ein, unsere Referenzen-Seite im Internet aufzurufen und sich so vorab bereits einen Eindruck von der Akzeptanz unserer Lösung zu verschaffen. Sicher werden Sie zustimmen, dass die meisten dieser Unternehmen vermutlich ähnliche Sicherheits- und Verfügbarkeitsanforderungen hatten, bevor Sie sich schließlich nach intensiver Prüfung für TeamViewer entschieden haben. Damit Sie sich dennoch selbst einen Eindruck verschaffen können, finden Sie im Folgenden technische Details.

TeamViewer-Sitzung

Verbindungsaufbau und Verbindungsarten

TeamViewer ermittelt beim Aufbau einer Verbindung die optimale Verbindungsart. Nach dem Handshake über unsere Master-Server findet in 70% der Fälle (auch hinter Standard-Gateways, NAT und Firewalls) eine Direktverbindung über UDP oder TCP statt. Die restlichen Verbindungen werden über unser hochredundantes Router-Netzwerk via TCP oder http-Tunneling geleitet. Sie müssen also keinerlei Ports öffnen, um mit TeamViewer arbeiten zu können!

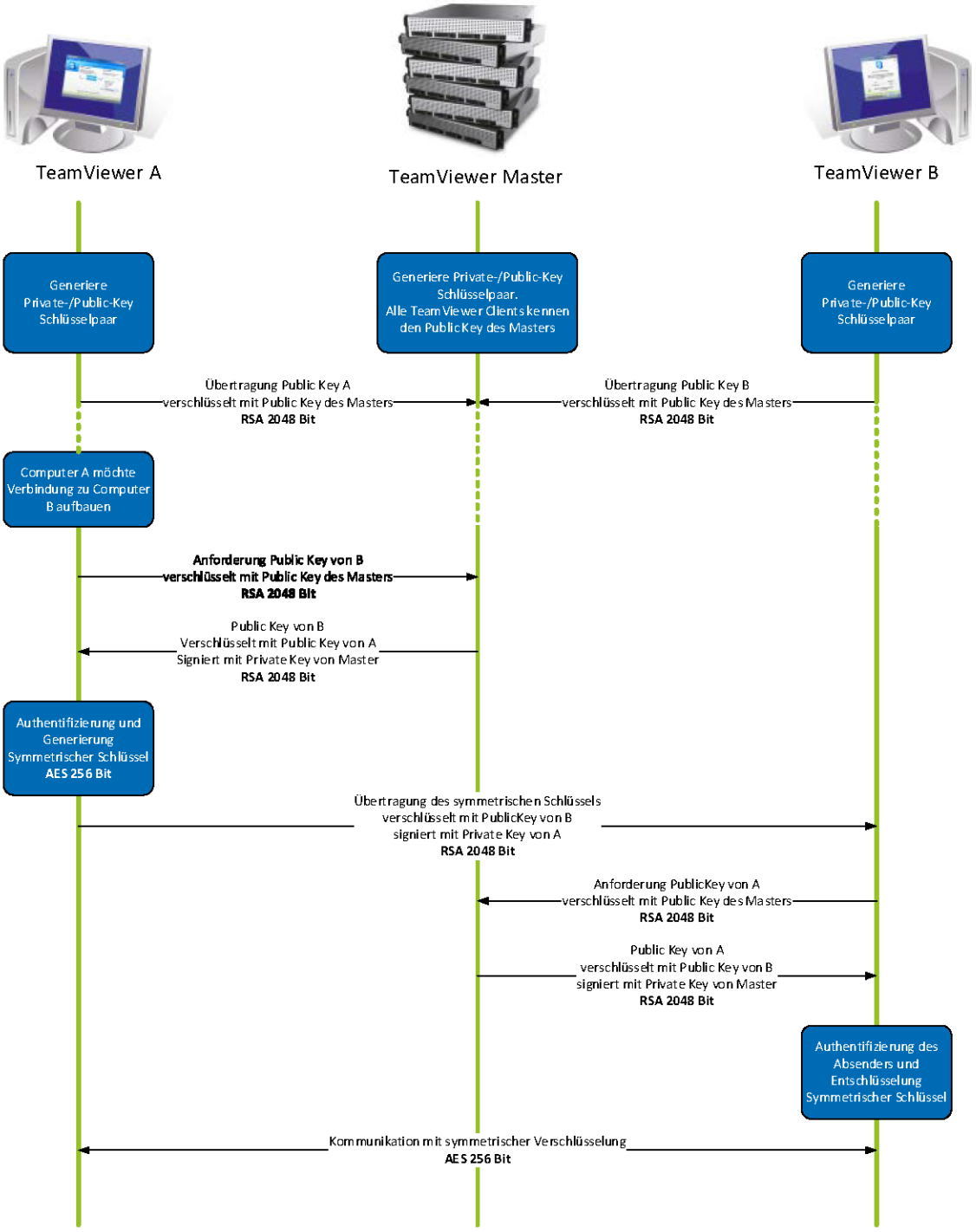
Wie später im Abschnitt „Verschlüsselung und Authentifizierung“ beschrieben, können auch wir als Betreiber der Routingserver den verschlüsselten Datenverkehr nicht einsehen.

Verschlüsselung und Authentifizierung

TeamViewer-Verbindungen laufen über komplett gesicherte Datenkanäle, die mit einem 2048 Bit RSA Public-/Private Key Exchange aufgebaut und mit 256 Bit AES verschlüsselt sind. Diese Technik wird in vergleichbarer Form auch bei https/SSL eingesetzt und gilt nach heutigem Stand der Technik als vollständig sicher. Da der Private Key niemals den Clientcomputer verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Computer im Internet den Datenstrom nicht entziffern können, das gilt somit auch für die TeamViewer Routingserver.

Jeder TeamViewer Client hat bereits den Public-Key unseres Masterclusters implementiert und kann so Nachrichten an den Mastercluster verschlüsseln bzw. dessen Signatur überprüfen. Die Public-Key-Infrastruktur verhindert effektiv „Man-in-the-middle-Attacken“. Das Kennwort wird trotz Verschlüsselung niemals direkt, sondern im Challenge-Response Verfahren übertragen und ist nur auf den lokalen Computern gespeichert.

Bei der Authentifizierung wird das Kennwort aufgrund der Verwendung des Secure Remote Password Protokolls (SRP) niemals direkt übertragen und es wird lediglich ein Passwort-Verifier auf dem lokalen Computer gespeichert.



TeamViewer-Verschlüsselung und Authentifizierung

Validierung von TeamViewer IDs

Die TeamViewer IDs werden direkt von TeamViewer automatisch anhand von diversen Hardware- und Softwaremerkmalen generiert. Die TeamViewer Server kontrollieren diese ID bei Verbindungen auf ihre Gültigkeit.

Brute-Force Schutz

Wenn Interessenten uns zur TeamViewer-Sicherheit befragen, spielt das Thema Verschlüsselung eine große Rolle. Verständlicherweise ist die Möglichkeit, dass Dritte eine Verbindung einsehen oder die TeamViewer-Zugangsdaten abgegriffen werden können, gefürchtet. In der Praxis sind es dann aber oft ganz primitive Angriffe, die am gefährlichsten sind.

Im Kontext der Computersicherheit ist ein Brute-Force Angriff meist der Versuch, ein Kennwort, welches den Zugriff auf eine Ressource schützt, durch Ausprobieren zu erraten. Mit der steigenden Rechenleistung handelsüblicher Computer wird der Zeitaufwand für das Ausprobieren auch längerer Kennwörter immer weiter reduziert.

Zur Abwehr von Brute-Force Angriffen erhöht TeamViewer exponentiell die Wartezeit zwischen Verbindungsversuchen. Für 24 Versuche werden so bereits 17 Stunden benötigt. Die Wartezeit für Verbindungsversuche wird erst nach der erfolgreichen Kennwort-Eingabe zurückgesetzt.

TeamViewer bietet seinen Kunden nicht nur Schutz vor Angriffen eines bestimmten Computers, sondern auch vor sogenannten Botnetz-Angriffen, bei denen versucht wird, von mehreren Computern aus auf eine spezielle TeamViewer ID zuzugreifen.

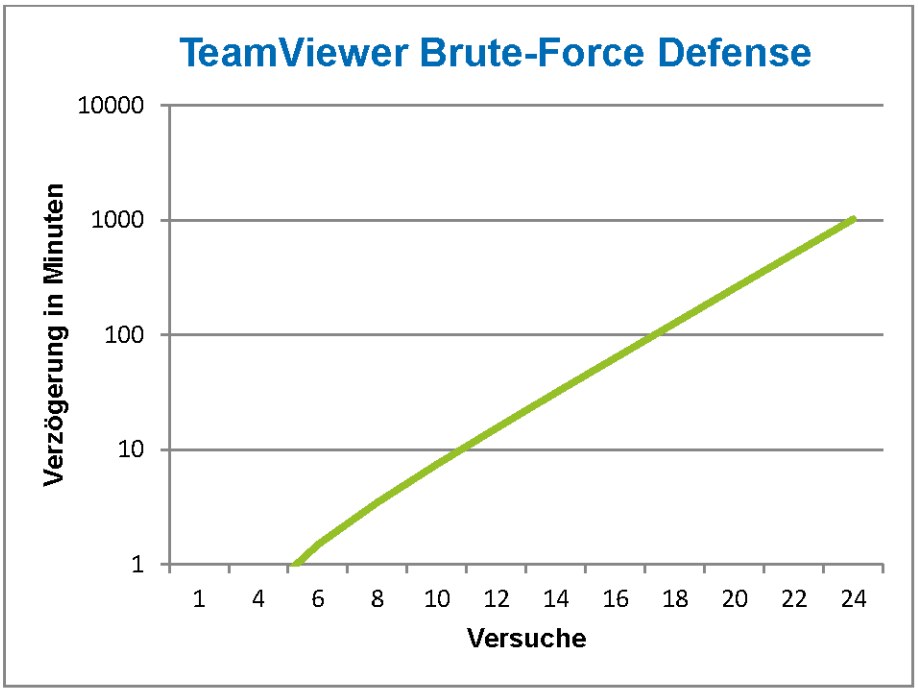


Diagramm: Benötigte Zeit für die Anzahl von Versuchen bei einem Brute-Force Angriff

Code Signing

Als zusätzliche Sicherheitsfunktion werden alle unsere Programme mittels VeriSign Code Signing signiert. Dadurch ist der Herausgeber der Software immer zuverlässig identifizierbar. Wird die Software nachträglich verändert, wird die digitale Signatur automatisch ungültig.

Datacenter & Backbone

Diese beiden Themen betreffen sowohl die Verfügbarkeit als auch die Sicherheit von TeamViewer. Die zentralen TeamViewer Server befinden sich innerhalb der Europäischen Union, in nach ISO 27001 zertifizierten Rechenzentren mit multiredundanter Carrier-Anbindung und redundanter Stromversorgung. Es wird ausschließlich Markenhardware eingesetzt.

Personenbezogene Zutrittsüberwachung, Videokameras, Bewegungsmelder, 24/7-Überwachung und Vor-Ort-Sicherheitspersonal gewährleisten, dass nur autorisiertes Personal Zugang zum Rechenzentrum hat und garantieren die bestmögliche Sicherheit für Hardware und Daten. An dem Single-Point-of-Entry zum Rechenzentrum findet eine ausführliche Personenüberprüfung und
-identifikation statt.

TeamViewer-Konto

Die TeamViewer-Konten werden auf dedizierten TeamViewer Servern gehostet. Weitere Informationen zur Zutrittskontrolle entnehmen Sie bitte dem Abschnitt „Datacenter & Backbone“. Für Autorisierung und Passwortverschlüsselung wird das Secure Remote Password Protokoll (SRP), ein erweitertes passwortbasiertes Authentisierung- und Schlüsseleinigungsverfahren (PAKE) verwendet. Dadurch wird verhindert, dass ein Eindringling oder Man-In-The-Middle ausreichend Informationen erhält, um ein Passwort durch Brute-Force Angriffe zu erraten. Somit kann selbst mit schwachen Passwörtern eine hohe Sicherheit gewährleistet werden. Sensible Daten des TeamViewer-Kontos, z. B. Anmeldeinformationen für Cloud-Speicherdienste, werden mit AES/RSA 2048Bit verschlüsselt gespeichert.

Management Console

Die TeamViewer Management Console ist eine webbasierte Plattform, die dem Benutzermanagement, der Verbindungsprotokollierung und der Verwaltung der Computer & Kontakte dient. Sie wird in einem nach ISO-27001 zertifizierten Rechenzentrum gehostet. Die Datenübertragung wird durch das Verschlüsselungsprotokoll SSL (Secure Sockets Layer) verschlüsselt, dem Standard für sichere Internetverbindungen. Sensible Daten werden außerdem mit AES/RSA 2048 Bit verschlüsselt gespeichert. Für Autorisierung und Passwortverschlüsselung wird das Secure Remote Password Protokoll (SRP), ein erweitertes passwortbasiertes, gängiges und stabiles Authentisierung- und Schlüsseleinigungserfahren (PAKE) verwendet. Entsprechend der Datenschutzrichtlinie der Europäischen Union verbleiben die Daten innerhalb der EU.

Einstellungen per Richtlinie

Nutzer können aus der TeamViewer Management Console heraus Richtlinien für TeamViewer-Einstellungen an Ihnen zugewiesenen Geräten festlegen, anwenden und erzwingen. Richtlinien für Einstellungen erhalten eine digitale Signatur von dem Account, mit dem die Richtlinien erstellt wurden. So ist sichergestellt, dass das Konto, welches dem Gerät eine Richtlinie zuweisen darf, auch das Konto ist, dem das Gerät zugewiesen wurde.

Anwendungssicherheit in TeamViewer

Black- & Whitelist

Insbesondere wenn Sie TeamViewer auf Computern installieren, die unbeaufsichtigt gewartet werden sollen (also TeamViewer als Windows-Systemdienst installieren), kann es für Sie von Interesse sein, zusätzlich zu allen Sicherheitsmechanismen den Zugriff auf diese Computer nur für bestimmte Clients zu erlauben.

Über die Whitelist-Funktion können Sie explizit angeben, welche TeamViewer IDs und/oder TeamViewer-Konten sich auf einen Computer verbinden dürfen, über die Blacklist-Funktion können Sie bestimmte TeamViewer IDs und TeamViewer-Konten sperren. Eine zentrale Whitelist ist als Teil der “Einstellungen per Richtlinie” (beschrieben im gleichnamigen Abschnitt) verfügbar.

Chat- und Video-Verschlüsselung

Chatverläufe sind mit Ihrem TeamViewer-Konto verknüpft. Sie werden daher, wie im Abschnitt „TeamViewer-Konto“ beschrieben, mit AES/RSA 2048 Bit verschlüsselt und gespeichert. Alle Nachrichten und Video-Daten sind mit AES (256 Bit) Ende-zu-Ende verschlüsselt.

Kein Stealth-Mode

Es gibt keine TeamViewer-Funktion, die es ermöglicht, TeamViewer komplett unsichtbar im Hintergrund laufen zu lassen. Über ein Icon im Infobereich (System Tray) ist TeamViewer auch dann sichtbar, wenn die Applikation als Windows-Systemdienst im Hintergrund läuft.

Nach dem Aufbau einer Verbindung ist immer ein kleines Control-Panel sichtbar – zur versteckten Überwachung von Computern oder Mitarbeitern ist TeamViewer daher bewusst ungeeignet.

Kennwort-Schutz

Für den spontanen Kunden-Support generiert TeamViewer (TeamViewer QuickSupport) ein Sitzungskennwort (Einmal-Kennwort). Teilt Ihr Kunde Ihnen dieses Kennwort mit, so können Sie sich durch Eingabe von ID und Kennwort auf den Kundencomputer aufschalten. Wird TeamViewer auf Kundenseite neu gestartet, wird ein neues Sitzungskennwort generiert, sodass Sie die Computer Ihrer Kunden nur erreichen können, wenn Sie explizit dazu eingeladen werden.

Beim Einsatz zur unbeaufsichtigten Fernwartung (z. B. von Servern) vergeben Sie ein individuelles festes Kennwort, das den Zugriff auf den Computer schützt.

Ein- und ausgehende Zugriffskontrolle

Sie können die Verbindungsmöglichkeiten von TeamViewer individuell konfigurieren. So können Sie beispielsweise Computer so einrichten, dass keine ein- oder ausgehenden Verbindungen (Fernsteuerung oder Meeting) möglich sind.

Die Beschränkung der Funktionalität auf die wirklich benötigten Funktionen bringt immer auch eine Beschränkung der möglichen Angriffspunkte mit sich.

Zwei-Faktor-Authentifizierung

Mit der Zwei-Faktor Authentifizierung unterstützt TeamViewer Unternehmen dabei, Ihre HIPAA und PCI-Anforderungen zu erfüllen. Die Zwei-Faktor-Authentifizierung bietet eine zusätzliche Sicherheitsebene zum Schutz vor unbefugtem Zugriff auf das TeamViewer-Konto. Zusätzlich zu seinem Passwort muss der User einen Code eingeben, um sich zu authentifizieren. Der Code wird mit einem zeitbasierten TOTP (time-based one-time password) Algorithmus erzeugt, dadurch hat der Code nur eine kurze, zeitlich begrenzte Gültigkeit.

Durch die Zwei-Faktor-Authentifizierung und die eingeschränkte Zugriffskontrolle mittels Whitelisting erfüllt TeamViewer alle notwendigen Kriterien für HIPAA und PCI Zertifizierungen.

Weitere Fragen?

Bei weiteren Fragen zum Thema Sicherheit freuen wir uns jederzeit über Ihren Anruf unter der Rufnummer +49 (0) 7161 60692 50, bzw. Ihre E-Mail: support@teamviewer.com.

Kontakt

TeamViewer GmbH
Jahnstr. 30
D-73037 Göppingen
service@teamviewer.com