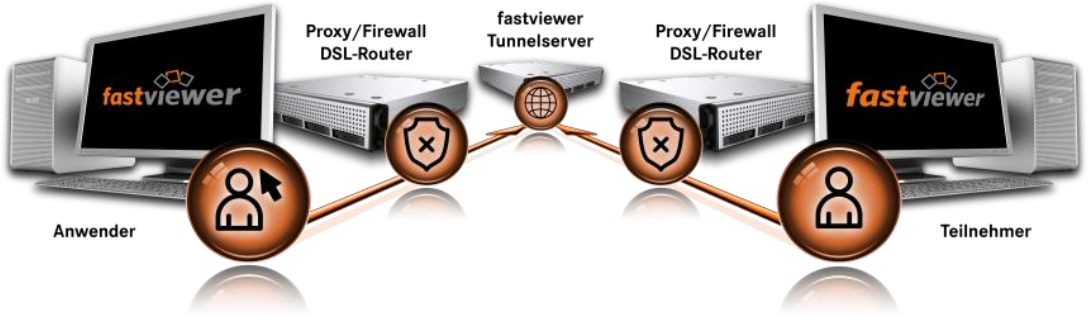
SICHERHEITSBESCHREIBUNG

Online-Meetings und Fernwartung. Einfach & sicher.

fastviewer

INHALTSVERZEICHNIS

ALLGEMEINE ARBEITSWEISE



Herzlich Willkommen zu unserer Sicherheitsbeschreibung

Die Sicherheit von Datenverbindungen nimmt einen immer größeren Stellenwert in unserer digitalen Welt ein. Bei FastViewer nehmen wir das Thema Sicherheit besonders ernst. Aus diesem Grund verlassen wir uns nicht nur auf Standard Protokolle, sondern haben z.B. unsere eigene Verschlüsselung innerhalb dieser Protokolle erstellt.
Auf den folgenden Seiten finden Sie einen Auszug aus unseren Sicherheitsdokumenten. Das Dokument richtet sich an Datenschützer, Sicherheitsbeauftragte sowie Personen, die sich für die Sicherheit von Daten interessieren. Ziel des Dokumentes ist es, einen umfassenden Einblick in das Sicherheitskonzept von FastViewer zu geben. Sollten Sie weiterführende Frage haben, stehen wir Ihnen gerne zu deren Beantwortung zur Verfügung.

Protokoll

Zur Kommunikation der FastViewer-Clients mit dem FastViewer-Server werden nur ausgehende Verbindungen benötigt. FastViewer verwendet dazu kein eigenes Protokoll, sondern bedient sich der folgenden Standard Protokolle des jeweiligen Betriebssystems (in der nachstehenden Reihenfolge):

- TCP (Port 5000)
- HTTPS Port 443)
- HTTP (Port 80)

Alle Einstellungen der SSL-Verbindung werden dabei vom Betriebssystem des FastViewer-
Clients bzw. des FastViewer-Servers vorgegeben.
Betreibt man einen eigenen FastViewer Server, so kann die Transport Layer Security durch eine Konfiguration des Betriebssystems vom Kunden selbst bestimmt werden.
Im Cloud Betrieb von FastViewer wird bei HTTPS als Protokoll TLS 1.2 mit der Cipher Suite
AES256CBC mit HMAC-SHA1 verwendet.

Bemerkenswert:
Das Protokoll ist unabhängig von der Verschlüsselung! Bedingt durch die im Folgenden vorgestellte Verschlüsselung sind selbst mit HTTP (Port 80) oder TCP (Port 5000) übertragenen Daten sicher Ende zu Ende verschlüsselt.

FastViewer benötigt nur einen Port für die Übermittlung der Daten. Stehen mehrere Ports zur Verfügung, so wird der höchste Port verwendet. Die andern Ports dienen dann als Fallback, sollte der ausgewählte Port ausfallen. Somit ist eine unterbrechungsfreie Übertagung – auch bei Ausfall eines Ports – möglich.

ALLGEMEINE ARBEITSWEISE

Verschlüsselung von Daten

Alle Nutzdaten (Bildschirminhalt, Dateien, Chat, VoIP, Video und Statusinformationen) werden durch eine 256-Bit-AES Ende-zu-Ende-Verschlüsselung geschützt. Der Sitzungs-Schlüssel wird bei jeder Sitzung neu ausgehandelt und liegt bedingt durch einen Austausch der Schlüsselpaare durch das RSA-Verfahren nur den Teilnehmern vor.
Somit ist gewährleistet, dass die während einer FastViewer Sitzung übertragenen Daten nur durch die an dieser Sitzung teilnehmenden FastViewer Teilnehmer entschlüsselt werden können. Der Server ist nicht im Besitz des Sitzungs-Schlüssels und kann die Daten folglich nicht entschlüsseln.

Bemerkenswert:
Oftmals wird unter einer 256-Bit-AES Ende-zu-Ende-Verschlüsselung lediglich das Protokoll HTTPS verstanden, bei welchem die übertragenen Daten lediglich zwischen dem Server und dem Teilnehmer Ende zu Ende verschlüsselt werden. Bei dieser Methode kann der Server die übertragenen Daten lesen!
FastViewer verschlüsselt die Daten vom Teilnehmer zum Teilnehmer ohne dass der Server die Daten mitlesen kann. Dies findet Anwendung bei Windows, OSX, iOS und Android Betriebssystemen.

Unterschied Moderator- / Teilnehmermodul

Das Moderatormodul von FastViewer dient dazu, Sitzungen zu planen und zu starten. Auch können über das Moderatormodul – sofern man die erforderlichen Berechtigungen besitzt – Verwaltungsfunktionen der Software vorgenommen werden.
Das Teilnehmermodul berechtigt lediglich zur Teilnahme an Sitzungen.

Sitzungsaufbau FastViewer Cloud

Zunächst bezieht das Moderatormodul über Port 80 eine redundant verteilte Liste aller zur Verfügung stehenden FastViewer Kommunikationsserver.
Hinweis: Der Abruf der Kommunikationsserverliste kann bei Einsatz der eigenen Serverlösung auch ausschließlich über HTTPS oder einem frei konfigurierbaren Port erfolgen.
Für weitere Details lesen Sie: Einsatz einer eigenen Server-Lösung auf Seite 17.

Nach Erhalt der Liste, ermittelt das FastViewer Moderatormodul den schnellsten Kommunikationsserver für diese Sitzung. Über das FastViewer Kundenportal kann übrigens konfiguriert werden, ob die Kommunikation über die weltweit verteilten, die europäischen oder ausschließlich die in Deutschland verfügbaren FastViewer-Kommunikationsserver laufen soll. Die für die jeweiligen Regionen bereitgestellten Server stellen eine 100%ige Ausfallsicherheit der FastViewer Cloud sicher.

Das Moderatormodul verbindet sich nun zum ausgewählten FastViewer Kommunikations-server. Über die hergestellte Verbindung wird eine 6-stellige Sitzungsnummer bezogen, welche für die Identifikation der korrekten Sitzung seitens des Teilnehmers genutzt wird. Diese Sitzungsnummer wird üblicherweise durch den Moderator per Telefon oder per E-Mail verschlüsselt an den Sitzungspartner übermittelt.

Fortsetzung Sitzungsaufbau FastViewer Cloud

Der Sitzungsteilnehmer muss die erhaltene Sitzungsnummer in das Teilnehmermodul eingeben (bzw. den Link in der E-Mail Einladung starten). Die Verbindung wird im Anschluss zu dem identifizierten FastViewer Server hergestellt, welcher die Sitzung für die angegebene Sitzungsnummer hosted.

Im Anschluss wird zwischen den Teilnehmern ein 256-Bit-AES-Schlüssel ausgehandelt, der für diese Sitzung verwendet wird. Der Austausch des Schlüssels erfolgt über das RSA-Verfahren.

Damit sichergestellt ist, dass weder am FastViewer Kommunikationsserver, noch an sonst einem Punkt der Verbindung mitgelesen werden kann, erfolgt die weitere Kommunikation ausschließlich über die 256-Bit-AES Ende-zu-Ende verschlüsselte Verbindung.
Dem FastViewer-Kommunikationsserver ist es NICHT möglich die Daten zu entschlüsseln, da er zu keinem Zeitpunkt im Besitz des 256-Bit-AES-Schlüssels ist!

Nachdem die sichere Ende-zu-Ende-Verbindung zwischen Moderatormodul und Teilnehmermodul aufgebaut wurde, erfolgt die Übertragung des Bildschirms in die jeweils gewünschte Richtung. Der Sitzungspartner kann die Steuerung jederzeit mit der Panik Taste unterbinden, bzw. die Verbindung per Mausklick sofort komplett trennen. Das Teilnehmermodul berechtigt lediglich zur Teilnahme an Sitzungen.

Anmerkung:
Die hier vorgestellte Sitzungsnummer hat nichts mit dem Sitzungsschlüssel zu tun. Sie stellt lediglich den Sitzungsraum dar und sorgt dafür, dass sich die Teilnehmer im gleichen Raum treffen.

VERSCHLÜSSELUNG

Verschlüsselung von Dateien

Alle Dateien, die über die Dateiablage von FastViewer eingestellt werden, bleiben während der Dauer der FastViewer-Sitzung 256-Bit-AES verschlüsselt auf dem FastViewer Server temporär zwischengespeichert.
Somit wird gewährleistet, dass jeder Teilnehmer die Dateien nur während der aktiven Sitzung herunterladen kann. Zusätzlich zur 256-Bit-AES-Verschlüsselung der Daten selbst (siehe „Verschlüsselung von Daten“ auf Seite 2) werden die Dateien noch als fragmentierte Pakete von 64 KB zwischengespeichert. Folglich ist nicht nur der Inhalt der Dateien, sondern auch deren Zusammensetzung kryptisch.

CRC Prüfung

Bei der Kompilierung der EXE-Files wird eine Prüfsumme in den Programmcode eingebaut. Wird die EXE über ein Tool geändert, ist das Programm aufgrund eines Prüfsummenfehlers nicht mehr verwendbar. Dies verhindert effektiv eine unerwünschte Veränderung am Programmcode und stellt gleichzeitig die Funktionstüchtigkeit aller definierten Sicherheitsfeatures sicher.

Redundanz - Lastverteilung

Das Moderatorenmodul sucht den schnellsten verfügbaren Kommunikationsserver, dieser wird für die folgende Sitzung verwendet. Eine Liste der verfügbaren Kommunikationsserver wird bei der eigenen Serverlösung im Moderator- sowie im Teilnehmermodul hinterlegt. Sollten mehrere eigene Server im Einsatz sein, oder die FastViewer-Cloud-Server verwendet werden, so prüft das Moderatorenmodul, welcher der Server die kürzeste Reaktionszeit auf die Anfrage hat. Dieser Server stellt die Sitzungsnummer bereit und dient als Kommunikationsserver der Sitzung. Somit ist eine gleichmäßige Auslastung der Server sichergestellt. Die Lastverteilung erfolgt automatisch.

Authentifizierung

Zur Authentifizierung eines Benutzers stehen in FastViewer unterschiedliche Möglichkeiten zur Verfügung, die auch in Kombination eingesetzt werden können.

AD-Authentifizierung.

Die Userverwaltung von FastViewer bietet die Möglichkeit AD-Gruppen, oder AD-Benutzer zu importieren. Somit können sowohl die Zugriffsrechte, als auch die Verwendung unterschiedlicher Profile zentral in ihrer AD konfiguriert werden.

AD-Anbindung.

Wir wissen wie sensibel die Daten des AD sind, deshalb importieren wir lediglich die SID der AD-Informationen in FastViewer und prüfen diese beim Programmstart gegen das Betriebs-system. Dabei verwenden wir die Standards ihrer Betriebssysteme. Es besteht also keine Not-wendigkeit, während der Laufzeit des Programmes auf ihre AD-Verwaltung zugreifen zu müssen.

Username und Passwort

Stellt ebenfalls eine Methode dar, mit der man sich an FastViewer anmelden kann. Diese Informationen werden in der Userverwaltung von FastViewer hinterlegt und stehen - auch außerhalb des firmeneigenen AD - zur Verfügung.

AD-Sperre

Unterbinden sie den Einsatz von FastViewer außerhalb ihrer Domäne oder schränken sie die Verwendung von FastViewer auf eine AD-Gruppe oder einen AD-User ein. Die AD-Sperre kann im Portal von FastViewer eingestellt werden und bedarf keiner zusätzlichen Userverwaltung.

Single-Sign on

Mit nur einem Klick in der Userverwaltung können auch nachträglich alle bereits verwendeten FastViewer Programme auf die Single Sign on Methode umgestellt werden.

Zwei Wege Authentifizierung

Beim Zugriff auf Remote Hosts spielt die Sicherheit eine besonders große Rolle. Aus diesem Grund haben wir eine 2 Wege Authentifizierung mittels SMS etabliert. Jeder Zugriff auf einen Remote Host (nach erfolgreicher Anmeldung am System selbst) muss zusätzlich durch die Eingabe eines SMS PIN an der FastViewer Anwendung bestätigt werden.
Damit sind Zugriffe auf ihr System nicht nur sicher, sondern können auch noch über ein vier Augen-Prinzip erfolgen.

NOCH MEHR SICHERHEIT

Revisionssichere Aufzeichnung

Auf Seiten des Teilnehmers als auch der des Moderators kann zu Nachweis-zwecken eine Videoaufzeichnung aktiviert werden, die auf Wunsch auch automatisch startet. Die Videodaten werden in einem eigenen Format als revisionssichere EXE-Datei abgelegt. Dies verhindert eine spätere Manipulation. Die Aufzeichnungs-Datei kann jederzeit eigenständig mittels eines integrierten Players abgespielt werden.

Anwendungssicherheit

Sichere Verbindungen alleine genügen nicht, auch der Übertragene Inhalt muss geschützt bzw. eingeschränkt werden können. Wir haben sehr viel Zeit investiert um ein Portal zu erstellen, über das sie FastViewer an die Vorgaben ihrer Datenschutzrichtlinien anpassen können.

FastViewer Cloud Server

Alle FastViewer Cloud-Server sind in Hochsicherheits-Rechenzentren aufgestellt. Dabei können Sie mit Hilfe Ihres persönlichen Kundenportals selbst bestimmen, ob Sie nur über die deutschen Server, Server in der Europäischen Union (EU) oder die weltweiten FastViewer Server kommunizieren wollen.

Sofern Ihnen das alles nicht ausreichend ist, können Sie auch Ihren eigenen FastViewer Server in einem Rechen-zentrum Ihrer Wahl, Ihrer DMZ oder in Ihrem Intranet betreiben. Alle Sitzungen werden dann über Ihren eigenen Server, unabhängig von den FastViewer Kommunikationsservern, abgewickelt.

Installationsfreie Nutzung

FastViewer ist eine für den Moderator, sowie für den Kunden eine installations-freie Anwendung. Nach einer FastViewer Sitzung werden die Programmodule rückstandsfrei beendet.

NOCH MEHR SICHERHEIT

Gerade beim einem unbeaufsichtigten Support muss die Sicherheit stimmen. Aus diesem Grund haben wir für unsere Remote-Lösung ein ausgeklügeltes Rechtesystem etabliert, das eng mit der Benutzerverwaltung zusammen arbeitet. Angefangen von einer automatisierten Installation inkl. Gruppenzuordnungen, bis hin zum zeitlich eingeschränkten Zugriff für Benutzergruppen bieten wir alles, was man für eine unbeaufsichtigte Remote-Support-Lösung benötigt.

Weitere Informationen finden Sie im Benutzerhandbuch der FastViewer User-Verwaltung.

Einmalige Fernwartung?

Bei Remote Hosts kann der Zustand nach einer FastViewer Sitzung frei definiert werden. Der Rechner kann gleich für die nächste Sitzung bereit stehen, oder erst nach einem manuellen
Vorgang wieder für einen Support bereit stehen.

Panik Taste

Durch eine fest definierte Taste, können die Fernsteuerung und die Bildschirm-freigabe sofort unterbrochen werden. Somit kann ein Anwender jederzeit eine Fernsteuerung beenden.

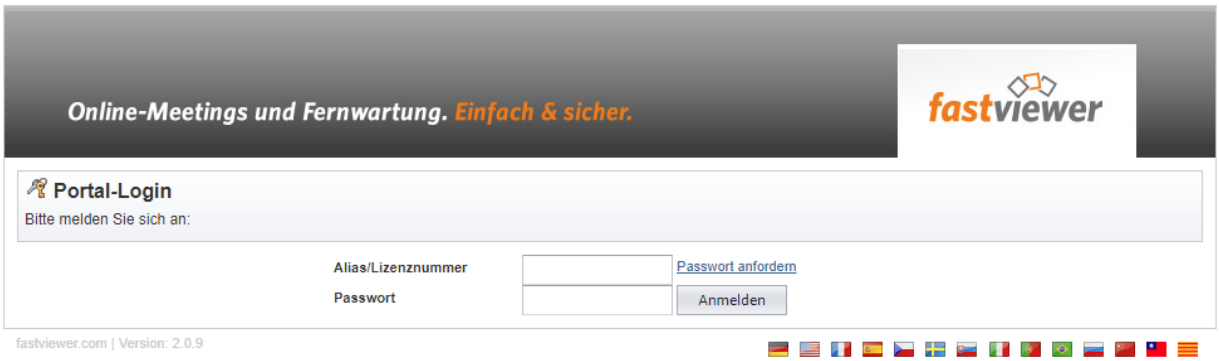
Fernwartung unterbrochen?

Mit FastViewer können sie selbst bestimmen, in welchen Zustand der ferngewartete Rechner gehen soll, wenn eine Fernsteuerung unerwartet abbricht. Somit ist gewährleistet, dass kein Rechner ungeschützt bleibt (z.B. offene Sitzung).

Volle Kontrolle

Bei der Freigabe der Bildschirm-übertragung entscheidet immer der Anwender, welche Inhalte er freigeben möchte.

SICHERHEITSFEATURES KUNDENPORTAL

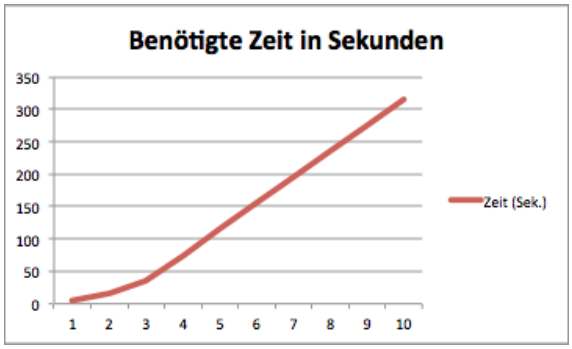


Das FastViewer Kundenportal dient als Konfigurationsplattform der FastViewer Lösung. Hier können Anpassungen bezüglich der Sicherheit, des Funktionsumfangs oder des Erscheinungsbilds der Software vorgenommen werden. Der Zugang zum FastViewer Kundenportal ist durch eine 10-stellige Lizenznummer sowie ein individuelles Passwort geschützt. Nur dem jeweils berechtigten Lizenzinhaber ist somit der Zugriff auf das Kundenportal und damit auf die FastViewer Module möglich. Die Kommunikation mit dem Kundenportal erfolgt immer über HTTPS (Port 443).

Sollte der Lizenzinhaber sein individuelles Passwort vergessen haben, so kann dies über die Startseite des Portals abgerufen werden. Der Versand erfolgt ausschließlich an die im Portal hinterlegte Email-Adresse, die bei Lizenzausstellung vom Lizenzinhaber gewählt wurde.
Sichere Verbindungen alleine genügen nicht, auch der übertragene Inhalt muss geschützt bzw. eingeschränkt werden können. Wir haben sehr viel Zeit investiert um ein Portal zu erstellen, über das sie FastViewer an die Vorgaben ihrer Datenschutzrichtlinien anpassen können:

Schutz gegen Brute-Force

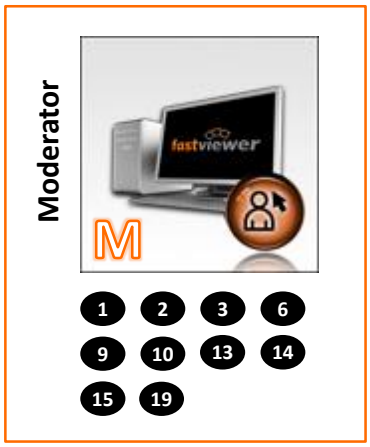
Der Zugriff zu den Portaleinstellungen von FastViewer ist passwortgeschützt. Um Brute-Force-Attacken abzuwenden, wird ein Delay eingesetzt, der sich bei jeder fehlerhaften Anmeldung erhöht. Man benötigt für 10 Versuche bereits über 5 Minuten.



Black- & Whitelist

Durch die Black- & White-List kann man festgelegen, welche Applikationen übertragen werden dürfen bzw. welche Applikationen von der Übertragung explizit ausgeschlossen werden sollen.

SICHERHEITSFEATURES MODULE



1 Videoaufzeichnung

Das Moderator- sowie das Teilnehmermodul ermöglichen unabhängig voneinander die Aufzeichnung der aktiven Sitzung. Dabei wird das Video in einem eigenem Format gespeichert inklusive des eigenen FastViewer-Players. Für die jeweilige Gegenseite ist immer ersichtlich, wenn eine Videoaufzeichnung stattfindet.

2 Protokollierung

Während einer Sitzung werden in einem Online-Log Informationen zur durchgeführten Session gespeichert. Hierzu gehören der FastViewer-Benutzername, die verwendete Sitzungsnummer, Anzahl der Teilnehmer, FastViewer-Versionsnummer, Windows-Anmeldename, Hostnamen, IP-Adressen, Freitextpositionen sowie Zeitstempel. Optional und über das Kundenportal einstellbar kann zusätzlich die übertragene Applikation geloggt werden. Die Protokolle können über das Kundenportal oder bei Einsatz einer eigener Serverlösung über ein eigenes Tool ausgewertet und exportiert werden.

3 Benutzerverwaltung

Das Moderatormodul kann durch die Benutzerverwaltung vor unberechtigtem Zugriff geschützt werden. Durch die LDAP-Importfunktion können AD-Gruppen und Benutzer komfortabel die Berechtigung zur Nutzung von FastViewer erhalten. Somit können sowohl die Zugriffsrechte, als auch die Verwendung unterschiedlicher Profile zentral in ihrer AD konfiguriert werden.

Wir wissen wie sensibel die Daten des AD sind, deshalb importieren wir lediglich die SID der AD-Informationen in FastViewer und prüfen diese beim Programmstart gegen das Betriebssystem. Dabei verwenden wir die Standards ihrer Betriebssysteme.

Es besteht also keine Notwendigkeit, während der Laufzeit des Programmes auf ihre AD-Verwaltung zugreifen und Anpassungen vornehmen zu müssen.

4 Pause-Funktion

Die aktive Session kann durch den Präsentator jederzeit pausiert werden. Dabei wird die Bildübertragung eingefroren.

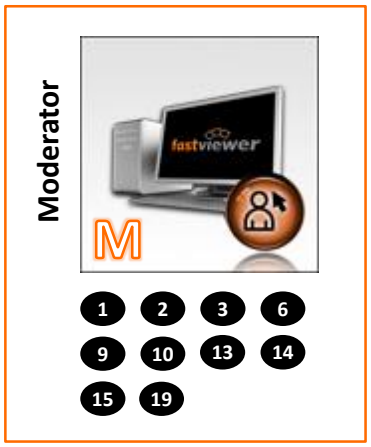
5 Schutzfunktionen

Der User behält jederzeit die Kontrolle über die Fernwartung. Die Steuerungsrechte können durch betätigen der Panik Taste dem Supporter entzogen werden. Der User hat jederzeit die Möglichkeit einen Dateizugriff oder die gesamte Sitzung abzubrechen.

6 Active Directory-Benutzer-Sperre

Mit dieser Funktion wird ein aus einem vorhandenen Active Directory importierter Domain-Schlüssel (Domain SID oder Domain Gruppen SID) für die Nutzung von FastViewer zugelassen. Nutzer außerhalb der Domäne/Gruppe können die Module nicht starten. Alternativ kann die FastViewer Benutzerverwaltung verwendet werden, um Zugriffsrechte auf Benutzer- oder Gruppen-Ebene zu vergeben.

SICHERHEITSFEATURES MODULE



7 Black- & Whitelist

Es kann im Kundenportal eine Black- & White-List konfiguriert werden, um gezielt Anwendungen verfügbar zu machen oder einen Zugriff zu sperren. Diese Einstellung kann in der aktiven Sitzung nicht mehr verändert werden.

8 Applikationswahl

Bevor der entfernte Desktop übertragen wird, bekommt der Präsentator die Möglichkeit, gezielt zu übertragende Anwendungen auszuwählen. Ebenso verfahren Sie mit dem Desktop und der Taskleiste oder neu gestarteten Applikationen. Natürlich besteht auch die Möglichkeit, den gesamten Desktop freizugeben.

9 Konfiguration der Funktionen

Über das Kundenportal sind alle Features konfigurierbar. Dies ermöglicht eine individuelle Gestaltung des Zusammenspiels aller Sicherheitsfeatures. Es ist hier z. B. möglich,, den Dateitransfer sowie die Dateiablage zu unterbinden. Außerdem kann eine Steuerung des Clients unterbunden werden.

10 Sitzung beenden

Der Kunde ist jederzeit in der Lage, die Sitzung zu beenden. Dies geschieht durch einen Klick auf die Schließen-Schaltfläche in der FastViewer Sidebar. Außerdem hat der Kunde die Möglichkeit per Druck der „F11-Taste“ (Panik-Taste), auf seiner Tastatur, die Fernsteuerung zu unterbrechen. So kann der Kunde aktiv Veränderungen an seinem System verhindern und den Zugriff beenden.

11 Dateitransfer

Wird in einer aktiven Session per Dateitransfer auf das entfernte System zugegriffen, treten mehrere Sicherheitshürden in Kraft. Der „supportete“ Kunde muss dem Dateitransfer zustimmen. Wird die Freigabe nicht erteilt, kann kein Zugriff auf das Dateisystem durchgeführt werden. Natürlich kann ein bereits freigegebener Dateitransfer / Dateisystemzugriff jederzeit abgebrochen werden.

Secure Advisor (Remote Zugriff)

Bei FastViewer Secure Advisor ist ein besonders intensiver Schutz nötig. Da der Remote-Client ausschließlich eine ausgehende Verbindung benötigt, werden durch FastViewer keine eingehenden Ports geöffnet. Somit sind keine Hacker-Angriffe möglich. Durch die Windows-Anmeldung ist ein zusätzlicher Schutz vorhanden um die lokale Sicherheit zu gewährleisten.

12 Ausgehende Verbindung

Der Remote-Client ist aufgrund einer reinen ausgehenden Verbindung unsichtbar für Angriffe von Außen.

13 Zugriffsbeschränkung

Der Zugang ist ausschließlich durch Eingabe eines Benutzernamens und des dazugehörigen Passwortes möglich (über die FastViewer-Benutzerverwaltung).

14 Sicher wie eine EC-Karte

FastViewer arbeitet wie eine EC-Karte mit PIN. Einloggen ist nur dann möglich, wenn man die zum Client passende FastViewer EXE-Datei besitzt und den richtigen Login kennt.

15 Windowsanmeldung

Ein zusätzlicher Schutz ist durch die vorgeschaltete Windowsanmeldung des Clients gegeben (es gelten die jeweiligen Windows Sicherheitseinstellungen).

16 Diensteinstellungen

Der Dienst muss durch den Anwender aktiv geschaltet werden, um Zugriff zu gewähren (konfigurierbar).

17 Zugriffs-Timeout

Beim Zugriff auf einen Remote-Client bestimmt dieser Timeout die zur Verfügung stehende Zeit zur Interaktion des Teilnehmers.
Über das FastViewer-Kundenportal kann konfiguriert werden, ob nach Ablauf dieser Zeit der Zugriff auf den Remote-Client gewährt oder verweigert werden soll. Auch die Länge des Timeouts ist hierbei anpassbar.

18 Zwei-Wege- Authentifizierung

Beim Zugriff auf Remote-Clients spielt die Sicherheit eine besonders große Rolle. Aus diesem Grund haben wir eine Zwei-Wege-Authentifizierung mittels SMS etabliert, die für zusätzliche Sicherheit aktiviert werden kann.

Jeder Zugriff auf einen Remote-Client (nach erfolgreicher Anmeldung am System selbst) muss zusätzlich durch die Eingabe eines SMS-PIN an der FastViewer Anwendung bestätigt werden. Zugriffe auf ihr System sind dadurch nicht nur sicher, sondern können auch noch über ein Vier-Augen-Prinzip erfolgen.

19 Weitere Authentifizierungsmechanismen

Die Verwendung der Smartcard-Authentifizierung ermöglicht es, die Teilnehmer direkt und sicher zu authentisieren. Hierzu identifiziert und authentisiert sich der jeweilige Benutzer durch seine Smartcard und erhält anschließend Zugriff und Berechtigung zum Starten des Moderator-/Teilnehmer-Moduls.

Dieser Authentifizierungsmechanismus ist stark von der jeweiligen Kunden-IT-Infrastruktur und vom Kunden verwendeten Smartcard-Lösung abhängig und wird generell als Kundenprojekt-spezifische Lösung umgesetzt. Sollten weitere oder andere Maßnahmen zur Zugangsprüfung notwendig sein, setzen Sie sich bitte hierzu mit uns in Verbindung, um eine Lösung gemäß Ihrer Anforderungen zu besprechen.

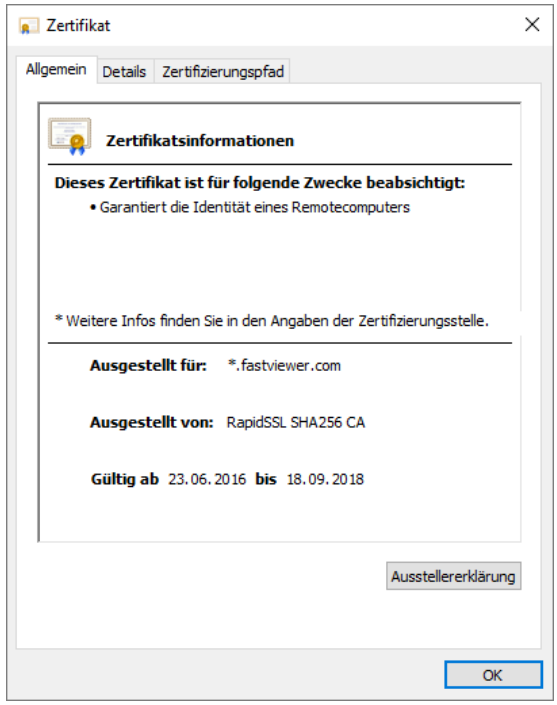
EINGESETZTE ZERTIFIKATE (SSL)

Abfrage Serverzertifikat

Standardmäßig findet die FastViewer Kommunikation über TCP 5000, alternativ über HTTPS 443 oder HTTP 80 statt. Kunden, die eine eigene Serverlösung von FastViewer im Einsatz haben, können selbst entscheiden welche Ports für die Kommunikation verwendet werden. Ein Betrieb von FastViewer rein über HTTPS bietet hier eine erweiterte Sicherheit, da hier durch das übliche SSL Verschlüsselungs-verfahren die „Echtheit“ des / der Tunnelserver(s) verifiziert werden kann. Der Kommunikationsserver benötigt für einen Betrieb über HTTPS eine IP Adresse und ein SSL Zertifikat. In der FastViewer Verbindung kann der Betrachter überprüfen über welches Protokoll er mit dem Tunnelserver verbunden ist. Es gibt die Möglichkeit auf einem Proxyserver / Firewall nur gültige HTTPS Verbindungen zu-zulassen, somit kommt nur dann eine Verbindung zu Stande wenn am Tunnelserver gültige SSL Zertifikate eingespielt sind. Über den Internet Explorer kann man ganz einfach durch den Aufruf das SSL Zertifikat überprüfen.
z.B. https://tunnel200.fastviewer.com -> Rechte Maustaste Eigenschaften -> Zertifikate

Authentifizierung

Ein SSL Server-Zertifikat garantiert neben der verschlüsselten Übertragung von Daten die Identität des jeweiligen Kommunikationsservers. Es dient dazu, dass sich die Teilnehmer hinsichtlich der Vertrauenswürdigkeit des Kommunikationsservers sicher sein können.



HTTPS

HTTPS dient zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser im World Wide Web.

Syntax

Syntaktisch ist HTTPS identisch mit dem Schema für HTTP, die zusätzliche Verschlüsselung der Daten geschieht mittels SSL/TLS: Unter Verwendung des TLS-Handshake-Protokolls findet zunächst eine geschützte Identifikation und Authentifizierung der Kommunikationspartner statt. Anschließend wird mit Hilfe asymmetrischer Verschlüsselung oder des Diffie-Hellman-Schlüsselaustauschs ein gemeinsamer symmetrischer Sitzungsschlüssel ausgetauscht. Dieser wird schließlich zur Verschlüsselung der Nutzdaten verwendet.

EXTERNE ZERTIFIKATE

FIDUCIA

Wenn es um Geld geht, ist der bestmögliche Sicherheitsstandard gerade gut genug. Unsere Lösung hat die sicherheitstechnische Prüfung der Fiducia IT erfolgreich durchlaufen. Hierbei wurde die Unbedenklichkeit der Installation einer Fremdanwendung auf dem „agree Windows 7 Bank-arbeitsplatz“ im Fiducia & GAD Umfeld verifiziert. Die Fiducia IT betreut als Provider den Datenverkehr von 1.120 Volks- und Raiffeisenbanken sowie Privatbanken.

FIDUCIA GAD
ZUKUNFTSERFAHREN

OPDV

Auch die OPDV-Richtlinien der Sparkassen-Finanzgruppe legen für den IT-Bereich höchste Sicherheitsstandards fest. (Freigabe 1/2015). Die OPDV-Prüfung beleuchtet die Ordnungs-mäßigkeit, Funktion, Wirtschaftlichkeit sowie die Sicherheit der Software. Getestet wurde vor allem der Schutz vor Manipulation. Die OPDV-Freigabe bestätigt ein weiteres Mal: FastViewer steht für höchste Sicherheit!

BISG

Der dt. Bundesfachverband der IT-Sachverständigen und Gutachter (BISG) zeichnet FastViewer mit dem begehrten Qualitätssiegel aus und beschreibt die Leistung des Produktes mit „sehr gut“. Die Tester lobten v.a. die schlanke Architektur, installationsfrei Benutzung, hervorragende Bedienbarkeit und sehr gute Stabilität.

Die Prüfer lobten, dass die Bedienung für den Nutzer übersichtlich gestaltet ist und so lange Eingewöhnungs-phasen verhindert würden. Rundum ein sehr gutes Produkt. Auch im Bereich der Verbindungsarten bietet FastViewer alle Möglichkeiten, wie etwa HTTP(S)-Client für Tunnel-verbindungen (auch hinter Firewalls), gesicherte Direktverbindungen (verschlüsselt) oder Direktverbindung.

Da FastViewer niemals als Server agiert, wird es zusätzlich modernen Sicherheits-richtlinien gerecht, ohne dabei auf eine ausgewogene Leistungsperfomance ver-zichten zu müssen. Hier der ab-schließende Kommentar des Bundesfach-verbandes:

„Zusammenfassend ist FastViewer ein Produkt, welches durch seine Flexibilität und Benutzer-freundlichkeit besticht“.

TECHNISCHE & ORGANISATORISCHE MAßNAHMEN

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)

a) Zutrittskontrolle
Ein unbefugter Zutritt zu Datenverarbeitungs-anlagen ist zu verhindern.

Die Zutrittskontrolle wird durch eine dokumentierte und überwachte Schlüsselvergabe gewährleistet. Der Serverraum von FastViewer kann nur von zutrittsberechtigten Personen betreten werden. Die Schließanlage der dort vorhandenen Tür schützt vor unbefugtem Zutritt durch fremde oder dritte Personen.

b) Zugangskontrolle
Eine unbefugte Systemnutzung ist zu verhindern.

Der Zugang zu den Räumen der Datenverarbeitungsanlagen ist geschützt und sämtliche Anlagen bzw. IT-Systeme mit stetig wechselnden Passwörtern versehen. Alle Rechnersysteme werden durch das IT-Personal in der Form eingerichtet, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine persönliche Anmeldung mit Benutzerkennung und Passwort erforderlich. Nach der Erstellung/Vergabe ist das Passwort vom jeweiligen Benutzer zu ändern, dies besteht aus Klein-/Großbuchstaben, sowie Ziffern. Durch die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen erfolgt in der Regel personenbezogen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Kennungen und Passwörter weiterzugeben. Die jeweiligen Passwörter werden im Abstand von 30 Tagen geändert. Sollte ein User, etc. dies nicht tun, wird er vom System dazu gezwungen.

c) Zugriffskontrolle / Benutzerkontrolle
Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.

Personenbezogene Daten können nur auf Grundlage der nach dem „need to know“ Prinzip vergebenen Berechtigungen verändert werden. Hierzu wird ein dokumentiertes Berechtigungskonzept etabliert. Mitarbeiter sind in Gruppen eingeteilt, die unterschiedliche Zugangsberechtigungen zu den Datensätzen haben. Dies wird mittels einer Windows Serverstruktur in Verbindung mit „Active Directory“ gewährleistet.

d) Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.

Im FastViewer System ist gewährleistet, dass Daten die zu unterschiedlichen Zwecken erhoben wurden auch getrennt voneinander verarbeitet werden können.

e) Pseudonymisierung und Verschlüsselung (Zugangs- / Weitergabe- / Übertragungs-kontrolle) personenbezogener Daten (Art. 32 Abs. 1 lit a, 25 Abs. 1 EU-DS-GVO)

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Alle Backups (Veeam) werden mit einer 256 Bit AES Verschlüsselung versehen.

TECHNISCHE & ORGANISATORISCHE MAßNAHMEN

2. Integrität (Art. 32 Abs. 1 lit. b EU-DS-GVO)

a) Weitergabekontrolle / Übertragungskontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

Personenbezogene Daten aus dem IT-System sind vor unbefugtem kopieren auf Datenträgern geschützt. Grundsätzlich werden bei FastViewer keine Daten auf Datenträger gespielt und außerhalb der Firma verwendet. Sollte ein Mitarbeiter über eine VPN-Verbindung von unterwegs aus arbeiten, ist der Zugang durch eine Firewall und dementsprechende Antiviren-, Antispy- und Antihackersoftware geschützt. Einmal von Seiten der Server aus aber auch von den User Computern her, durch die Installation dementsprechender Software.

b) Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Feststellung, ob und von wem personen-bezogene Daten in Datenverarbeitungs. systeme eingegeben, verändert oder entfernt worden sind.

Im FastViewer IT-System wird jegliche Veränderung, Löschung oder Bearbeitung von Daten und Datensätzen gespeichert, sofern es das System zulässt. Hierbei ist jederzeit nachvollziehbar, welcher User, zu welchem Zeitpunkt welche Veränderung, etc. vorgenommen hat.

3. Verfügbarkeit und Belastbarkeit / Wiederherstell-barkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

Es kommen skalierbare Server-Systeme auf Basis von Microsoft Hyper-V zum Einsatz, die sich je nach Belastung anpassen lassen. Die Server werden täglich komplett gesichert. Die verwendeten Geräte können jederzeit über die Softwarelösung FastViewer ferngewartet sowie administriert werden. Die hierfür verwendeten Kommunikationsserver befinden sich in Hochsicherheits-Rechenzentren. Für die Verbindungen selbst wird eine der hochwertigsten verfügbaren Verschlüsselung eingesetzt, um einen entsprechenden Sicherheitsstandard zu gewährleisten. (256 Bit-AES)

Alle wichtigen Systeme unterliegen einer permanenten Überwachung durch Monitoringsoftware des Herstellers Paessler. Sollten kritische Werte erreicht werden, betreffend der Verfügbarkeit oder der Leistungsfähigkeit der Netzwerke/der eingesetzten Geräte, so werden die betreuenden Administratoren umgehend per E-Mail/SMS benachrichtigt. Die gezielte Überwachung von Systemkomponenten und -prozessen hilft, Systemengpässe, Überlastungen und Ausfälle zu vermeiden. Durch die Funktionsvielfalt der Monitoringsysteme von Paessler ist es möglich, 24 Stunden täglich den gesamten Status des Netzwerks sowie der einzelnen Geräte zu überwachen und zu dokumentieren. Der Monitoring Report regelmäßig von einem entsprechend befugten Administrator ausgewertet.

TECHNISCHE & ORGANISATORISCHE MAßNAHMEN

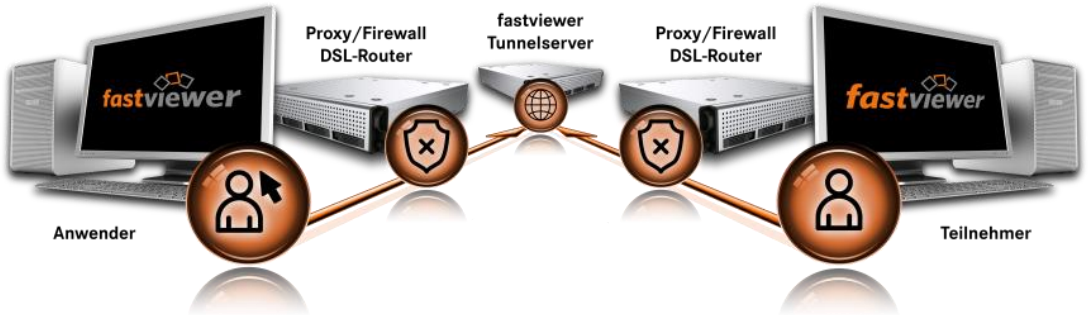
4. Einführung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 EU-DS-GVO); inkl. Datenschutz-Management, Incident-Response-Management, Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DS-GVO)

Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers.

Es bestehen schriftliche Verträge zwischen Auftraggeber und Auftragnehmern.
Der Auftraggeber erteilt dem Auftragnehmer die Weisungen in Schriftform. Der Auftragnehmer hat ausreichende betriebsinterne Anweisungen aufgrund des Auftrags und der damit verbundenen Weisungen des Auftraggebers.

Ausreichende Maßnahmen zur Einhaltung des Datenschutzes durch einen möglichen Unterauftragnehmer können auch durch den Auftraggeber geprüft werden.
Ein Datenschutzmanagementsystem unter Wahrung der Grundsätze des PDCA-Zyklus nebst schriftlicher Niederlegung, wird etabliert.



Hinweis: Einsatz einer eigenen Server-Lösung

Das HTTP-Protokoll wird verwendet um die zur Verfügung stehenden Server beim Modulstart abzufragen. Bei Einsatz einer eigenen FastViewer Serverlösung kann dieser Abruf mithilfe von HTTPS statt HTTP durchgeführt und die Portnummer zudem frei gewählt werden. (z.B. HTTPS 321). Wird HTTPS konfiguriert, empfiehlt FastViewer die Verwendung von TLS 1.2 für maximale Sicherheit. Somit ist es möglich die verwendeten Protokolle und damit die Voraussetzung der zu öffnenden Ports einzuschränken und eigene Sicherheitsstandards zu garantieren.

Eine Beschreibung der einzelnen Konfigurationsschritte finden Sie im Handbuch der FastViewer Serverlösung (Kapitel 6.5 Einrichtungsschritte zur ausschließlichen Verwendung von HTTPS) welches in Ihrem persönlichen Portal unter "Dokumente" abliegt:
https://portal.FastViewer.com/