



Sicherheitshighlights von BeckmanConnect

Überblick

In diesem Dokument werden die Datenschutzfunktionen der Remote-Verwaltungslösung BeckmanConnect hervorgehoben. Diese Lösung wurde entwickelt, um unserem Wartungs- und Support-Team zu ermöglichen, die Beckman Coulter-Geräte in Ihrem Labor über eine sichere Fernverbindung in Echtzeit zu warten. Das vorliegende Dokument ist für den IT-Administrator für Geräte-PCs und Netzwerkinfrastruktur Ihrer Einrichtung vorgesehen. Die Durchsicht des Dokuments ist Teil des Genehmigungsprozesses für BeckmanConnect.

Die Remote-Verwaltungsplattform von Beckman Coulter wird von der TeamViewer GmbH – einem weltweit führenden Unternehmen für sichere(n) Online-Zusammenarbeit und Remote-Support – unterhalten. Als anerkannter Anbieter von cloudbasierten Technologien ist die TeamViewer GmbH führend im Bereich der Entwicklung von Fernwartungssoftware. Sie ist mit einem 5-Sterne-Qualitätssiegel des Bundesverbands der IT-Sachverständigen und Gutachter ausgezeichnet. TeamViewer ist der bevorzugte Anbieter für viele Bereiche, in denen mit sensiblen Daten umgegangen wird, darunter Einrichtungen des Gesundheitswesens, Regierungseinrichtungen und Einrichtungen im Finanzsektor.¹

BeckmanConnect stellt unter Einhaltung regionaler Datenschutzbeschränkungen (z. B. HIPAA und DSGVO²) Fernzugriff bereit. Im Speziellen dient TeamViewer als eine Art Verbindungsglied zwischen zwei Endpunkten, ohne jedoch irgendwelche identifizierenden Informationen zu speichern.

Technische Zusammenfassung

TeamViewer stellt eine Plattform zum sicheren Teilen von Bildschirmen und Dateien über Fernzugriff bereit. Dadurch wird den Experten des Wartungs- und Support-Teams von Beckman Coulter ermöglicht, sich über Fernzugriff mit den Beckman Coulter-Geräten in den Einrichtungen ihrer Kunden zu verbinden. Der gesamte Datenverkehr über TeamViewer ist über RSA-Verschlüsselung (Public/Private Key Exchange) und AES (256 Bit) Sitzungsverschlüsselung geschützt. Zusätzlich ist die Plattform konfiguriert, um „Man-in-the-Middle“-Angriffe sowie „Brute-Force“-Angriffe zu verhindern. Weitere Informationen erhalten sie hier in den TeamViewer [Sicherheitsinformationen](#).¹



Abbildung 1. Durch Zwei-Faktor-Authentifizierung, vertrauenswürdige Geräte und die Verwendung von Whitelists wird sichergestellt, dass der Fernzugriff auf die Beckman Coulter-Geräte in Ihrem Labor nur autorisierten Support-Mitarbeitern von Beckman Coulter möglich ist.

¹ TeamViewer Sicherheitsinformationen, <https://dl.tvcdn.de/docs/de/TeamViewer-Security-Statement-de.pdf>

² TeamViewers Verpflichtung auf Datenschutz, <https://content.teamviewer.com/de/dsgvo/>

Sicherheitsmaßnahmen

Zur Nutzung von TeamViewer ist eine Internetverbindung notwendig. Bevor Sie das erste Mal den PC eines Beckman Coulter-Geräte mit dem Netzwerk verbinden, sollten Sie das Dokument „Anforderungen bei der Vernetzung des PC eines Beckman Coulter-Geräts“ gelesen und sichergestellt haben, dass der Geräte-PC sicher ist. Vor der Aktivierung der Fernsupport-Funktionen sind das gründliche Durchlesen unserer IT-Anforderungen, sowie die Zustimmung zu den Dienstleistungsbedingungen erforderlich.

BeckmanConnect ist konfiguriert, um auf Anhieb maximale Sicherheit zu gewährleisten:

- Die Kontrolle der TeamViewer-Verbindung mittels „Whitelisting“ wird eingesetzt, um den Zugriff auf die Geräte durch Quellen, die sich außerhalb des Wartungs- und Support-Netzwerks von Beckman Coulter befinden, zu verhindern.
- Anfragen nach einer ausgehenden TeamViewer-Verbindung sowie die Meeting-Funktion innerhalb des Client sind deaktiviert.
- Zur Herstellung aller Verbindungssitzungen ist die Bereitstellung eines individuellen Verbindungspassworts durch den Benutzer notwendig. Das Passwort ändert sich bei jeder neuen Sitzung, um nicht autorisierte Verbindungen zu verhindern.
- Nach der erfolgreichen Authentifizierung einer sicheren Sitzung über TeamViewer müssen Benutzer jegliche Anfragen nach Ansicht des Bildschirms, Fern-Kontrolle und Austausch von Dateien manuell über den TeamViewer-Client genehmigen. Verbindungsanfragen und Dateiübertragung werden für Auditzwecke auf sicheren Servern von TeamViewer gespeichert.
- Hinweis: Die Dateiübertragung ist derzeit nicht für Geräte-Controller-PCs aktiviert, die persönliche Gesundheitsdaten enthalten (Navios EX, DxFLEX, Data Innovations Instrument Manager, Aquios CL, CellMekSPS, Navios). Wenn diese Funktion in einer zukünftigen Version aktiviert ist, müssen Benutzer ein Update herunterladen und die neue Funktion während der Installation autorisieren, bevor sie aktiviert wird.
- Der Zugriff auf das TeamViewer-Verwaltungsportal von Beckman Coulter ist durch einen Benutzernamen und ein Passwort beschränkt. Der Zugriff ist auf Beckman Coulter-Mitarbeiter beschränkt, die eine Schulung über die Datenschutzrichtlinien, die in dem Land des Firmensitzes des Kunden Anwendung finden, absolviert haben.

Firewall-Anforderungen

BeckmanConnect ist so gestaltet, dass eine sichere Fernverbindung ohne die Notwendigkeit spezieller Firewall-Konfigurationen ermöglicht wird. In bestimmten Situationen kann eine Firewall eingerichtet sein, um unbekannte ausgehende Verbindungen zu blockieren. In solchen Fällen muss die Firewall so konfiguriert sein, dass sie die Verbindung ermöglicht.

BeckmanConnect verwendet Anschluss 443 zur Herstellung einer ausgehenden TCP-Verbindung. Anschluss 443 wird für die Client-Software für Folgendes benötigt:

- Automatische Aktualisierungen
- Festlegen erforderlicher Einstellungen von Gruppenrichtlinien aus Sicherheitsgründen
- Zulassen von Fernverbindungen mit den Wartungs- und Support-Mitarbeitern von Beckman Coulter

HINWEIS: Ohne ausgehenden Zugriff auf Anschluss 443 ist eine ordnungsgemäße Funktion des Service nicht möglich.

BeckmanConnect stellt Verbindungen zu sicheren Servern auf der ganzen Welt her. Diese Server verwenden eine Reihe unterschiedlicher IP-Adressen, die sich mit der Zeit ändern können. Alle von BeckmanConnect verwendeten IP-Adressen führen zu einer Domain mit den Endungen ***.teamviewer.com** oder ***.beckman.com**. Nutzen Sie diese Informationen, um die Ziel-IP-Adressen, die Sie durch Ihre Firewall oder Ihren Proxy-Server zulassen, einzuschränken.

Da der Dienst BeckmanConnect nur ausgehende Datenverbindungen durch eine Firewall veranlasst, ist es ausreichend, eingehende Verbindungen zu blockieren und nur ausgehende TCP-Verbindungen über den Anschluss 443 zu Domains mit den Endungen ***.teamviewer.com** ***.beckman.com** zu gestatten.

Zusammenfassung

BeckmanConnect ist ein sicheres System, das den Wartungs- und Support-Mitarbeitern von Beckman Coulter für Wartungszwecke den Fernzugriff auf bestimmte Geräte gestattet. Die Ende-zu-Ende-Verbindung ist verschlüsselt und es werden Maßnahmen unternommen, um Kunden zu schützen und sicherzustellen, dass nur geschulten Beckman Coulter-Mitarbeitern der Zugriff gestattet wird.

Erfahren Sie mehr und stellen Sie noch heute eine Verbindung her :

connect@beckman.com



© 2021 Beckman Coulter Life Sciences. All rights reserved. Beckman Coulter, the stylized logo, and the Beckman Coulter product and service marks mentioned herein are trademarks or registered trademarks of Beckman Coulter, Inc. in the United States and other countries.

For Beckman Coulter's worldwide office locations and phone numbers, please visit Contact Us at beckman.com

MULTI-648302.20