Sparkasse Oberhessen

Kundenleitfaden

Fernwartung mit der Software TeamViewer

TeamViewer – was ist das?

Das Programm TeamViewer erlaubt es, die aktuellen Bildschirminhalte zweier über das Internet verbundener PCs in Echtzeit zu übertragen (sog. Desktop-Sharing).
Nach Start des Programms und Austausch der Partner-ID und des Kennwortes sieht Ihr Berater zunächst den Inhalt Ihres Bildschirms.
Zusätzlich können Sie Ihrem Berater zudem den Fernzugriff auf Ihren Rechner erlauben.

Bitte stellen Sie vor Nutzung des TeamViewer sicher, dass Sie alle Anwendungen und Daten schließen, die Ihr Sparkassenberater nicht sehen soll.

Die im Rahmen der Fernwartung anfallenden Daten werden in der Sparkasse zu Dokumentationszwecken in einem Video aufgezeichnet und 3 Monate aufbewahrt.
Eine anderweitige Nutzung der Daten erfolgt nicht.

Voraussetzungen für die Nutzung von TeamViewer

- Teamviewer-Software
- eine Telefonverbindung mit Ihrem Berater
- eine aktive Verbindung zum Internet

Sicherheit des TeamViewers

Zahlreiche Mechanismen sorgen dafür, dass der TeamViewer ohne Sicherheitsbedenken eingesetzt werden kann.

OPDV-Freigabe

Für Kreditinstitute ist ein verantwortungsvoller Umgang mit IT-Anwendungen zwingend notwendig. Die eingesetzten Programme müssen gewährleisten, dass Finanz-transaktionen und vertrauliche Informationen sicher und nachvollziehbar be- und verarbeitet werden. Dazu werden die eingesetzten Programme einer Prüfung nach OPDV-Richtlinien unterzogen.

Zufällige Partner-ID und Kennwort für den Verbindungsaufbau

Damit eine Verbindung zwischen zwei PCs aufgebaut werden kann, muss eine Partner-ID und Kennwort eingeben werden, die der Kunde dem Electronic Banking Berater via Telefon mitteilt. Die Partner-ID und das Kennwort stellen sicher, dass die richtigen Partner miteinander verbunden sind.

Die Nummern werden zufällig erzeugt und gelten nur für eine Sitzung.

Sitzungsverschlüsselung verhindert das Abhören einer Sitzung

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 auch bei https/SSL eingesetzt und gilt nach heutigem Standard der Technik als vollständig sicher. Da der Private Key niemals den Clientrechner verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Rechner im Internet den Datenstrom nicht entziffern können. Das gilt somit auch für die TeamViewer Routingserver.

Beendigung jederzeit mit nur einem Klick möglich

Durch Klicken auf das Schließen-Symbol „X“ des TeamViewer-Fensters kann die Sitzung von beiden Seiten jederzeit beendet werden.

Die TeamViewer-Software ist signiert

Als zusätzliche Sicherheitsfunktion werden alle unsere Programme mittels VeriSign Code Signing signiert. Dadurch ist der Herausgeber der Software immer zuverlässig identifizierbar.