Technisches Beiblatt TeamViewer 12

TeamViewer wurde entwickelt, um einen Zugriff auf entfernte IT-Systeme ohne spezielle Firewall-Einstellungen zu ermöglichen. Wenn ein Internetzugang vorhanden ist, sollte der Zugriff auf TeamViewer in der Regel möglich sein. TeamViewer nutzt dabei ausgehende Verbindungen, die normalerweise nicht von Firewalls geblockt werden.

Allerdings kann es notwendig sein, dass bestimmte Firewall-Einstellungen eingerichtet werden müssen. Dies wäre beispielsweise der Fall bei sehr strikten Sicherheitsrichtlinien, bei denen alle unbekannten ausgehenden Verbindungen blockiert werden.

TCP/UDP 5938

TeamViewer bevorzugt den Aufbau ausgehender TCP- und UDP-Verbindungen über den **Port 5938** – dies ist der primäre Port, der von TeamViewer verwendet wird, mit dem Sie auch die beste Verbindungsqualität erreichen. Dieser Port sollte in Ihrer Firewall als Minimum freigegeben werden.

TCP Port 443

Falls TeamViewer keine Verbindung über den Port 5938 aufbauen kann, wird versucht, eine Verbindung über den **TCP Port 443** herzustellen. Allerdings ist die Verbindungsgeschwindigkeit dabei weniger optimiert als bei Nutzung des Ports 5938.

TCP Port 80

Falls TeamViewer keine Verbindung über Port 5938 oder 443 aufbauen kann, wird versucht, eine Verbindung über **Port 80** aufzubauen. Die Verbindungsgeschwindigkeit ist dabei ebenfalls weniger optimiert als bei Nutzung des Ports 5938.

Ziel IP-Adressen

Die TeamViewer-Software baut Verbindungen zu TeamViewer-MasterServern und -Routern rund um die Welt auf. Diese Server nutzen eine große Bandbreite von IP-Adressen, die sich regelmäßig verändern. Aus diesem Grund ist es nicht möglich, eine feste Liste von IP-Adressen für die Verbindungsserver bereitzustellen. Allerdings werden für alle IP-Adressen PTR-Einträge bereitgestellt, die auf *.teamviewer.com auflösen. Dies kann genutzt werden, um freizugebende IP-Adressen in Firewall oder Proxyserver einzuschränken.