Erklärung zum Verschlüsselungsverfahren und zur Datensicherheit beim Einsatz von FastViewer

Zunächst bezieht das Mastermodul über http von **mehreren redundanten Webservern** die Liste der aktiv verfügbaren FastViewer-Kommunikationsserver.

Das Mastermodul sucht sich den schnellsten Kommunikationsserver, dieser wird für die aktuelle Sitzung verwendet. Dadurch wird eine **100%ige Ausfallsicherheit** gewährleistet. Derzeit sind für unser Unternehmen mehr als **20 Kommunikationsserver** in **4 Rechenzentren** weltweit im Einsatz.

Das Mastermodul verbindet sich nun zum ausgewählten FastViewer-Kommunikationsserver. Dies geschieht über den **Port 5000** (TCP), **Port 443** (HTTPS) oder **Port 80** (HTTP) bzw. über einen evtl. **vorhandenen Proxyserver**. Über diese Verbindung wird die **5-stellige Sitzungsnummer** bezogen. Diese wird üblicherweise per Telefon oder E-Mail an den Sitzungspartner übermittelt.

Nun gibt der Sitzungspartner die erhaltene Sitzungsnummer in das Kundenmodul ein. Das Kundenmodul bezieht ebenfalls die Liste der aktiv verfügbaren FastViewer-Kommunikationsserver. Das Kundenmodul verbindet sich über den **Port 5000** (TCP), **Port 443** (HTTPS) oder **Port 80** (HTTP) bzw. über einen evtl. vorhandenen **Proxyserver** zum FastViewer-Kommunikationsserver.

Der Server tauscht die IP-Adressen der beiden Clients zwischen den beiden Modulen aus. Danach versucht das Kundenmodul sich direkt auf die IP-Adresse des Mastermoduls **auf Port 5001** zu verbinden. Dadurch erfolgt eine evtl. LAN interne Kommunikation direkt.
Bei Erfolg wird der weitere Datentransfer über diese **Direktverbindung** getätigt, bei Fehlschlag erfolgt der Datentransfer über den FastViewer-Kommunikationsserver, welcher die Pakete zwischen den beiden Modulen weiterleitet.

Nun handeln sich Mastermodul und Kundenmodul einen **256-Bit-AES-Schlüssel (verwendet den Rjindael-Algorithmus)** aus. 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 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! Siehe auch TÜV Zertifikat vom Oktober 2007.

Anschließend erfolgt die Übertragung des Bildschirmes in die jeweils gewünschte Richtung. Der Sitzungspartner kann die Steuerung jederzeit mit der **Taste F11** unterbinden, bzw. die Verbindung per Mausklick sofort komplett trennen.

Sicherheitsfeatures der Remote Edition

Bei der **Remote Edition** von FastViewer ist ein besonders intensiver Schutz nötig, dieser wird durch eine **3-fache Sicherheit** gewährleistet:

- Nachdem der installierte Remote Client ausschließlich eine ausgehende Verbindung benötigt ist ein möglicher Fernzugriff von außen nicht ersichtlich. **Keine Hacker Angriffe möglich, da kein Port eingehend geöffnet wird**.
- FastViewer arbeitet wie eine EC Karte mit Pin. Einloggen ist **nur** dann möglich wenn man die zum Client passende **FastViewer EXE Datei** hat und den **richtigen Login** kennt.
- Durch die **Windows-Anmeldung** ist **ein zusätzlicher Schutz** vorhanden um die lokale Sicherheit zu gewährleisten.

Bleiben Sie unabhängig durch eine eigene Serverlösung

Eine weitere Möglichkeit besteht in der Verwendung einer **eigenen Serverlösung**. Diese Lösung kann **komplett unabhängig von unserer IT-Infrastruktur** eingesetzt werden. Alle Sessions werden über Ihren **eigenen Server**, unabhängig von den FastViewer-Kommunikationsservern, abgewickelt. Diese Variante verwendet die **gleichen Sicherheitsstandards** wie bereits beschrieben. **Die Ausfallsicherheit** kann durch **mehrere, redundante Systeme** gewährleistet werden.

Über den Rijndael-Algorithmus

Im Jahr 2000 wurde durch das National Institute of Standards and Technology der Rijndael-Algorithmus als offizieller Standard festgelegt, der so genannte Advanced Encryption Standard (AES). In dem dreijährigen Auswahlprozess wurden 15 potentielle Kandidaten mit eingebunden. Während des Wettbewerbs wurden die Verschlüsselungsformeln der einzelnen Kandidaten öffentlich gemacht, damit diese auch durch die Mitbewerber öffentlich getestet (attackiert) werden konnten. Der Rijndael Algorithmus wurde von den Finalisten als „beste Kombination aus Sicherheit, Performance und Effektivität“ ausgewählt. (Quelle: www.nist.gov)

Christian Wolf
CTO - Geschäftsführer

Steffen Fürsch
CEO - Geschäftsführer

Neumarkt i.d. OPf. im Oktober 2007