Connect - Whitepaper zur Infrastruktur

Grundlagen

MediFox Connect ist eine Webanwendung, welche den Zugriff auf bestimmte Daten und Funktionen innerhalb von MediFox stationär erlaubt.

Durch die Bereitstellung einer Webanwendung ist dieser Zugriff prinzipiell über jedes webfähige Endgerät (PC, Tablet, Smartphone etc.) möglich. Man benötigt lediglich eine Browseranwendung (z.B. Google Chrome, Safari, Firefox, Microsoft Edge) und einen Netzwerkzugang auf den entsprechenden Webserver in der Infrastruktur des Kunden. Eine Installation weiterer Software auf dem Endgerät ist nicht nötig.

Das übliche Nutzungsszenario für MediFox Connect wird i.d.R. ein Fernzugriff auf Daten und Funktionen über das Internet sein. Der Nutzer ist also räumlich von der jeweiligen Einrichtung getrennt. Die Webanwendung muss daher im öffentlichen Netzwerk verfügbar gemacht werden. Durch diesen Umstand werden die folgenden Aspekte relevant:

Zugriffsmöglichkeit

Lokale Einrichtungsnetzwerke werden durch Router und Firewalls vom öffentlichen Internet abgeschottet. Der MediFox-Server ist bisher üblicherweise nur im internen Einrichtungsnetzwerk erreichbar. Durch den Einsatz von MediFox Connect muss nun der Webserver, der die Connect Anwendung bereitstellt, über das Internet erreichbar sein. Im Rechenzentrumsbetrieb, d.h. der MediFox-Server steht physisch nicht in einer Einrichtung, trifft dies ebenfalls prinzipiell zu.

Dazu ist folgendes nötig:

- Die öffentliche IP-Adresse des Routers in der Einrichtung muss durch einen verfügbaren, einmaligen DNS-Namen (z.B. "medifox.allegrocare.de") im Internet bekannt gemacht werden. Ein solcher DNS-Name kann über einen Hosting-Provider (z.B. STRATO oder 1&1) erworben werden. Hierbei ist zusätzlich zu beachten, dass (je nach gebuchtem Internetzugang) die IP Adresse entweder fest (statisch) oder veränderlich (dynamisch) ist.
    - Eine **statische** IP-Adresse wird einmalig beim Hosting-Provider dem DNS-Namen zugeordnet
    - Eine **dynamische** IP-Adresse muss immer nach Änderung (häufig täglich) beim Hosting-Provider dem DNS-Namen zugeordnet werden. Dieser Vorgang geschieht automatisch durch eine entsprechende Konfiguration im Router in der Einrichtung. Der Hosting-Provider muss hierbei sogenanntes "DynDNS" unterstützen.
- Eine Verbindung vom Endgerät durch die Firewall der Einrichtung zum Connect-Server muss ermöglicht werden.
    - Szenario 1: MediFox Connect soll von **verschiedenen Personengruppen** (Mitarbeiter, Ärzte, Bewerber) genutzt werden, die normalerweise keinen Zugriff von außen auf die MediFox-Installation haben. Daher muss ein entsprechender Port auf der öffentlichen IP-Adresse in der Firewall freigeschaltet und der internen MediFox Connect-Serveradresse zugeordnet werden (z.B. per NAT).
    - Szenario 2: MediFox Connect soll lediglich von **eigenen Mitarbeitern** genutzt werden, denen ein gesicherter Zugang (VPN) in das interne Netz verfügbar gemacht werden kann.

Sicherheitsaspekte

Der MediFox Connect-Webserver muss vom Internet aus erreichbar sein. Daraus ergeben sich erhöhte Anforderungen an die Sicherheit. Hierbei gilt es zum einen, den Transportweg der übertragenen Daten abzusichern und zum anderen die eigene Infrastruktur vor Angriffen zu schützen.

- **Transportsicherheit**:
    - Die Übertragung der Daten sollte grundsätzlich über **TLS** (Transport Layer Security) abgesichert werden. Das bedeutet, dass die MediFox Connect Webanwendung per HTTPS verfügbar gemacht wird. Zur Schaffung einer Vertrauensstellung zwischen dem Browser des Anwenders und dem MediFox Connect Webserver sollte ein offizielles Zertifikat bei einer vertrauenswürdigen Zertifizierungsstelle (z.B. Comodo, Swiss Sign) erworben und verwendet werden.
    - Zusätzlich kann (im Falle von oben geschildertem Szenario 2) die Verbindung vom Browser zum MediFox Connect Server über ein **VPN** abgesichert werden. Dies bedingt allerdings einen höheren Konfigurationsaufwand, und schließt "anonyme" Nutzergruppen (z.B. Bewerber) aus.
- **Schutz der eigenen Infrastruktur**
    - Zum Schutz der internen Infrastruktur sollte der MediFox Connect-Webserver idealerweise innerhalb des Netzwerkes in einer sogenannten **demilitarisierten Zone (DMZ)** platziert werden. Der MediFox Connect Webserver (der vom Internet aus erreichbar ist) wird damit von der restlichen Netzwerk-Infrastruktur getrennt.
    - Es sollten immer die neuesten Sicherheitsupdates des Betriebssystems auf dem MediFox Connect Webserver installiert sein.

Mögliche Szenarien zur Einrichtung

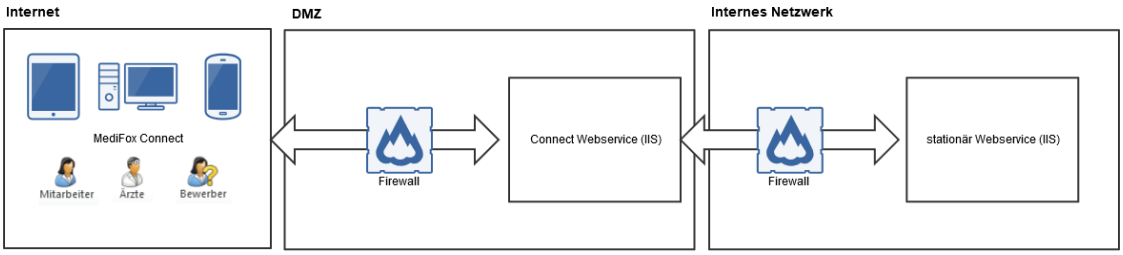
Aufgrund der geschilderten Aspekte ergeben sich die folgenden typischen Szenarien zur Einrichtung von MediFox Connect:

Szenario 1a: Der MediFox Connect Webservice befindet sich im Netzwerk des Kunden in einer DMZ und ist damit vom internen Netzwerk getrennt. Der Zugriff vom MediFox Connect Webservice auf den Stationär Webservice wird durch eine zusätzliche Firewall geleitet. Dieses Szenario ist das bevorzugte.

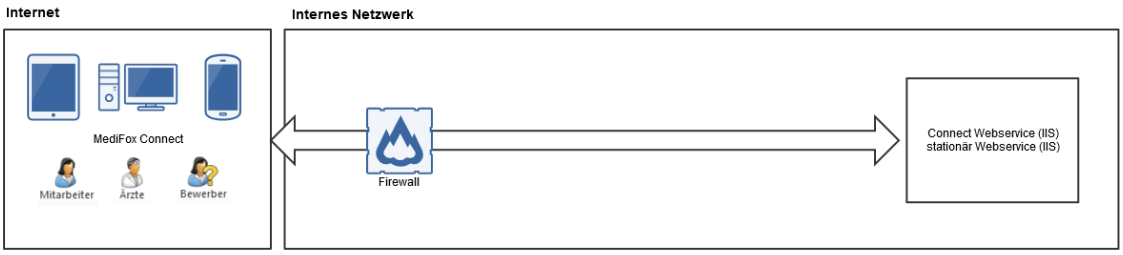
Szenario 1b (Testszenario): Der MediFox Connect Webservice wird gemeinsam mit dem MediFox stationär Webservice auf dem selben Rechner bzw. im selben Netzwerk installiert. **Technisch gesehen ist diese Art der Einrichtung zwar möglich, darf jedoch nur zu Testzwecken entsprechend eingerichtet werden, da dies eine deutlich unsicherere Konstellation darstellt.**

Szenario 2: Der MediFox Connect Webservice wird gemeinsam mit dem MediFox stationär Webservice auf dem selben Rechner bzw. im selben Netzwerk installiert. Der Zugriff vom Internet aus ist nur über ein VPN möglich. Dies schränkt jedoch die Benutzergruppen auf Mitarbeiter und ggf. Ärzte (sofern ein VPN-Zugriff besteht) ein.

Szenario 1a (bevorzugt)



Szenario 1b (Testszenario)



Szenario 2