Datenzugriff aus dem Internet

MF WebServer

Markus Friedrich Datentechnik

Copyright

Dipl.-Ing.
Markus Friedrich
- Datentechnik -
Bahnhofstr. 74
15732 Eichwalde bei Berlin

Tel: 030-6670 235 - 0
Fax: 030-6670 235 - 24
E-Mail: service@friedrich-datentechnik.de
Internet: www.friedrich-datentechnik.de

Inhalt

Vorstellung

Der MF WebServer, was ist das?

Der MF WebServer stellt Ihnen über das Internet Daten aus Ihren MF Programmen zur Verfügung. Hierzu fordert er vom Programm "MF Server" die Daten an, wandelt die Daten zu HTML-Dateien und stellt sie, vergleichbar einer Website, bereit.

Der Zugriff auf die Daten erfolgt über einen handelsüblichen Browser wie z.B. Microsoft Edge, Firefox, Google Chrome o.vgl. Als Endgeräte können PC´s, Smartphones und Tablets mit Android oder iOS oder sonstige Geräte mit Internet-Anschluss genutzt werden.

Wozu?

Mit dem MF WebServer haben Sie jederzeit und von überall Zugriff auf Ihre Firmendaten. Ihre Termine, Kundendaten, Materialpreise, Angebote u.a.m. können betrachtet und teilweise auch bearbeitet werden. Da es sich dabei um die Original-Daten des Firmenservers und nicht um Kopien handelt, können Sie jederzeit sehen, welche Termine Ihre Sekretärin für Sie eingetragen hat, ob die Abrechnung des Bauleiters fertiggestellt ist usw. Mit dem MF WebServer sind Sie immer und überall up-to-date.

Beispiel:

Bei der Nutzung von Adressdaten über Outlook muss ständig ein Datenabgleich vom Firmennetzwerk zu Outlook durchgeführt werden. Das ist lästig. Bei paralleler Eingabe von Daten in der Firma und am Mobilrechner entstehen Dubletten. Und wenn die Sekretärin um 18 Uhr ein Geschäftsessen einträgt, während Sie auf dem Smartphone für denselben Termin eine Partie Golf ins Outlook tippen, gerät die Welt schnell aus den Fugen. Über den MF WebServer wäre das nicht passiert.

Grundlagen

Hardware- und Softwarevoraussetzungen

Der MF WebServer kommuniziert mit dem MF Server und den Internet-Browsern über TCP/IP, benötigt also eine entsprechende Netzwerk-Topologie. Der MF WebServer muss über einen offenen Port mit den Clients kommunizieren können.
In der Programm-Voreinstellung nutzt der MF WebServer den Port 80 zur Kommunikation mit den Internet-Browsern.
Das alles hört sich zwar kryptisch an, ist aber in nahezu allen Standard-Windows-Netzwerken in dieser Form gewährleistet. Falls dennoch Schwierigkeiten auftreten, sind diese meist bei der Firewall bzw. Anti-Viren-Software zu suchen. Kontaktieren Sie in diesem Fall Ihren Netzwerkadministrator.

Alle weiteren Infos zu den Hardware- und Softwarevoraussetzungen entnehmen Sie bitte dem Installationshandbuch.

Software

Der MF WebServer bezieht alle Daten vom MF Server. Beide Programme müssen denselben Versionsstand besitzen. Der MF Server muss stets vor dem MF WebServer gestartet und nach dem MF WebServer beendet werden.

Netzwerkstruktur

Da der MF WebServer innerhalb des Firmennetzwerkes arbeitet und die Zugriffe von außerhalb, aus dem Internet, erfolgen, muss es einen Übergang vom Internet zum Firmennetzwerk geben. Der Fachbegriff hierfür lautet Gateway. Zusätzlich wird ein DSL-Modem benötigt, welches die digitalen Netzwerkdaten in analoge Telefonnetz-Signale umsetzt.

Die einfachste Netzwerkstruktur mit Internetzugang über die Telefonbuchse sieht daher wie folgt aus:

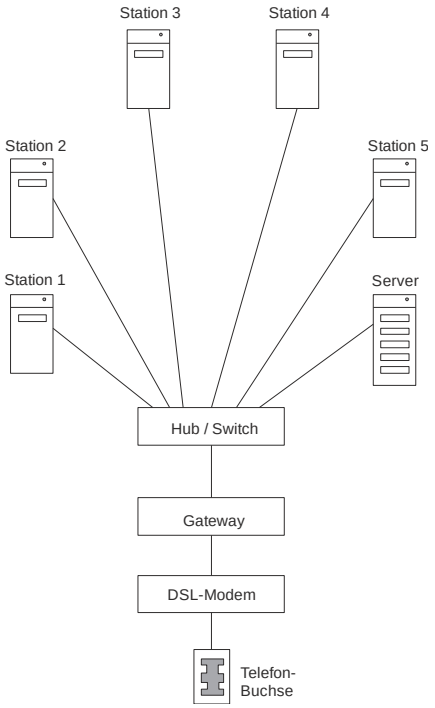


Bild 1: offene Netzwerkstruktur

Dieses Netzwerk wäre jedoch ein gefundenes Fressen für Viren, Würmer, Trojaner und alle anderen Schadsoftwaretypen aus dem Internet. Ohne jeglichen Schutz bietet es freien Zugang aus dem Internet (Telefonbuchse) zu den Arbeitsstationen und dem Server. Um dies zu vermeiden kann auf jeder Arbeitsstation und am Server eine Antiviren-Software installiert werden. Bei kleinen Netzwerken ist dies noch machbar, reduziert aber auch dort die Netzwerkgeschwindigkeit. In großen Netzwerken ist es sinnvoller die Viren direkt am Übergang zum Internet zu blockieren. Im obigen Beispiel wäre das zwischen Hub bzw. Switch und dem DSL-Modem.

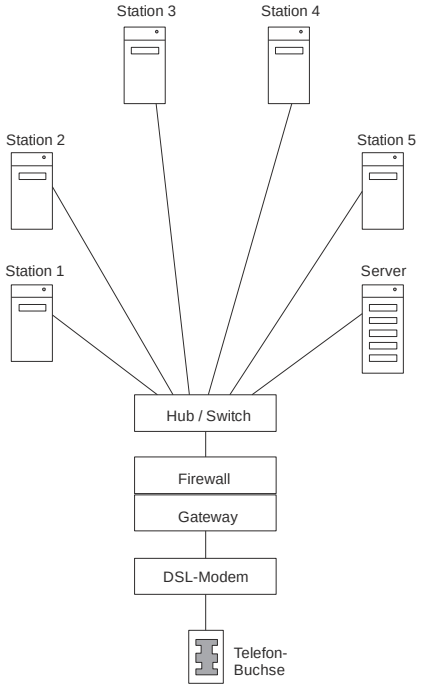


Bild 2: einfach geschützte Netzwerkstruktur

Die Firewall verhindert den unaufgeforderten Zugriff von Anfragen aus dem Internet auf das Firmennetzwerk. Durchgelassen werden nur Anfragen aus dem Firmennetz heraus und Anfragen in das Firmennetz hinein, wenn diese aus dem Firmennetz heraus angefordert werden. Zusätzlich können unterschiedliche Anfragetypen freigeschaltet oder blockiert werden. Diese sogenannten Freigaberegeln ermöglichen oder verbieten den Zugriff auf www-Seiten („normales Internet“), https-Seiten (sicheres Internet für Onlinebanking, Zahlungsverkehr…), ftp (Datenaustausch auf Dateibasis), E-Mail usw.
In professionellen Firewalls ermöglichen Content-Filter sogar das An- oder Abschalten von Inhalten wie Soziale Netzwerke, Erotik-Seiten, Nachrichtenseiten usw.

In Bild 2 wurden Firewall und Gateway zu einem Gerät zusammengefasst, was der heutzutage üblichen Bauform in einem Gerät entspricht. Für kleinere Netzwerke wird meist sogar noch ein 4-fach Hub und ein DSL-Modem eingebaut, so dass alle Funktionen vom Firmennetzwerk bis zur Telefonbuchse in einem Gerät vereint sind.

Unglücklicherweise kann eine Firewall nur starre Verbindungen von und zum Internet freischalten oder blockieren. Das Übertragen eines Virus von einer Homepage, die ein Anwender in bester Absicht geöffnet hat, kann eine Firewall nicht verhindern. Hierzu müssen die ein- und ausströmenden Daten auf Viren untersucht werden. Dies ist Aufgabe eines Viren-Scanners.

Bildlich gesprochen und auf eine mittelalterliche Burg zu Zeiten der Pest übertragen: Die Firewall ist der Burgwächter, der die Hängebrücke bedient. Der Antivirenscanner ist der Arzt, der den Besuchern auf die Zunge sieht und unter den Armen nach Beulen tastet.

Da eine geschlossene Hängebrücke zwar den sichersten Schutz vor der Pest bietet, andererseits aber den sichern Hungertod bedeutet, sind beide Schutzmaßnahmen erforderlich. In modernen, sogenannten „gemanagten Firewalls“ ist die Antivirensoftware mit eingebaut. Die zur Virenerkennung erforderlichen Viren-Vergleichsdaten (Viren-Signaturen) werden dabei regelmäßig und automatisch über das Internet in die gemanagte Firewall übertragen. Diese Arbeit übernimmt der Hersteller der Firewall, i.d.R. gegen eine monatliche oder jährliche Wartungsgebühr.

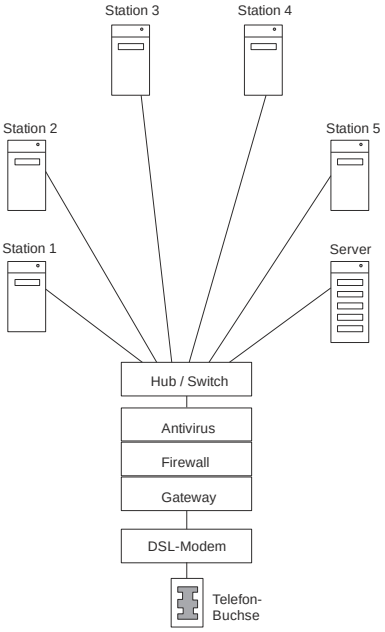


Bild 3: geschützte Netzwerkstruktur mit Virenabwehr

Die in Bild 1 bis 3 dargestellten Anbindungen eines Netzwerkes an das Internet nennt man hardware-basiert, da hierfür gesonderte Geräte existieren. Findet die Anbindung im Server statt, bestehen Firewall und Antivirenschutz aus Softwareprogrammen. Die Netzwerktopologie präsentiert sich damit folgendermaßen:

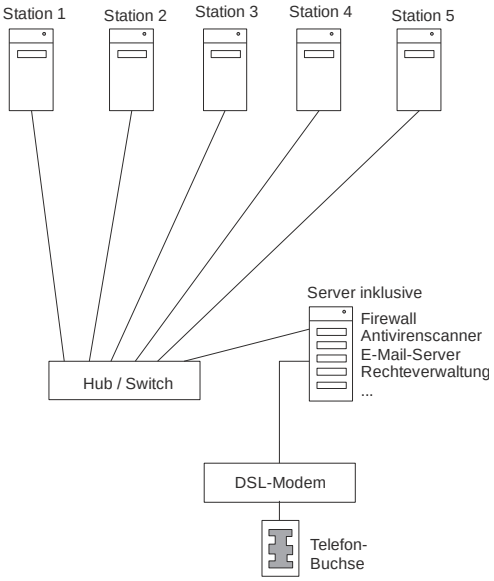


Bild 4: Netzwerkstruktur mit Netzwerkserver

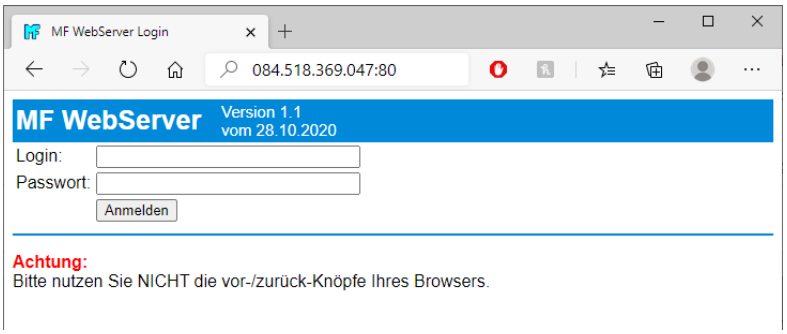
Die Netzwerkstruktur in Bild 4 ist nur für kleinere Netzwerke empfehlenswert, da der Server neben den internen Aufgaben (Druckerdienste, Speicherplatz zur Verfügung stellen, Programme bereitstellen, Nutzerverwaltung usw.) jetzt auch noch den gesamten Internetverkehr quasi nebenbei erledigen muss. Außerdem ist der Server der höchsten Infektionsgefahr durch Viren ausgesetzt. Dieser Gefahr muss durch intensives Virenscanning begegnet werden, was den Server stark ausbremst. Diese Nachteile können durch die Nutzung von zwei Servern kompensiert werden. Der erste Server bedient die Drucker, ist zentraler Datenspeicher und verwaltet die Programme. Ein zweiter Server regelt den Internetverkehr.

Netzwerkzugang

Der MF WebServer kann auf allen genannten Netzwerkstrukturen betrieben werden. Wichtig ist es dabei, einen passenden Netzwerkzugang einzurichten, mit dem Sie von außen auf den WebServer zugreifen können. Hierfür existieren vielfältige Varianten:

1. Das Firmennetzwerk besitzt eine statische Netzwerk-IP
   Zugang: Geben Sie in der Adresszeile des Internetbrowsers die Netzwerk-IP ein.
   Es öffnet sich der WebBrowser mit der Login-Seite.

   In diesem Beispiel hat das Firmennetzwerk die Netzwerk-IP 084.518.369.047
   Sollte ein weiterer Webserver, z.B. IIS von Microsoft, auf dem Server aktiv sein, müssen Sie die Programme über verschiedene Port-Nummern ansprechen. Falls der MF WebServer nicht auf dem Standard-www-Port 80 betrieben wird, muss die Portnummer an die IP-Nummer angehängt werden. Für Port 100 wäre die Eingabe: 084.518.369.047:100



2. Der Betreiber der aktiv gemanagten Firewall (z.B. Firma Octogate) stellt Ihnen eine Zugangsadresse zur Verfügung.

   Zugang: Geben Sie den Netzwerknamen in der Adresszeile des Internetbrowsers ein.
   Es öffnet sich der WebServer mit der Login-Seite.

3. DynDNS (Dynamische Netzwerkadresse)

   Eine feste IP-Adresse wie unter Punkt 1.) beschrieben ist eher die Ausnahme. Der „normale“ DSL- oder VDSL-Anschluss der Telekom hält eine Internet-Verbindung höchstens 24 Stunden lang aufrecht, führt spätestens dann eine Netztrennung durch und verbindet Sie anschließend mit einer neuen IP-Nummer. Auch bei der Neuanmeldung ohne vorherige Zwangstrennung erhalten Sie meist eine neue IP-Nummer, selbst wenn Sie sich am selben Tag das zweite oder dritte Mal ins Internet begeben. Dies gilt auch für Punkt 2.), nur dass dort der Lieferant des Gateways bei jedem Neuzugang zum Internet Ihre momentan gültige IP-Nummer gesendet bekommt und Sie deshalb jederzeit mit dem Firmennetzwerk verbinden kann.

   Ohne feste IP oder gemanagtes Gateway gelangen Sie daher nicht direkt an Ihr Netzwerk, da Sie dessen Adresse aus der Ferne nicht ermitteln können. In dieser Situation ist DynDNS die Lösung. DynDNS tritt an die Stelle eines gemanagten Gateways wie unter 2.) beschrieben. Aufgrund der fehlenden Gateway-Hardware muss jedoch der Internet-Router (z.B. FritzBox, siehe nächstes Kapitel) passend konfiguriert werden oder ein Zusatzprogramm im Firmennetzwerk laufen, um stets die aktuelle IP-Nummer an DynDNS zu melden. DynDNS setzt diese IP auf einen stets gleichlautenden www-Namen um, unter dem Sie Ihr Firmennetzwerk erreichen.

Einrichtung einer FritzBox

Portweiterleitung intern einrichten (Stand: Fritz!OS 07.12)

Melden Sie sich am Server-PC im Webbrowser an der FritzBox an (typ. Eingabe „fritz.box“). Gehen Sie im Menü zu „Internet“> „Freigaben“> „Portfreigaben“ wählen dort den Button am unteren Bildschirm „Gerät für Freigabe hinzufügen“. Wählen Sie hier das richtige Gerät (den Server-PC) aus der Liste. Unterhalb der Überschrift „Freigaben“ wählen Sie den Punkt „Portfreigabe“ an und wählen bei „Anwendung“ den Eintrag „http-Server“. Für die Eingabe „von bis“ wählen Sie z.B. den Port 80. Für den externen geben Sie den Port entsprechend der WebServer-Konfiguration ein (Menü Server > IP-Adresse und Port). Anschließend schließen Sie die Dialogbox mit Ok und speichern die Änderungen auf der Seite mit dem Klick auf Ok.

MyFritz!-Konto für externen Zugriff einrichten

Um von unterwegs Zugriff auf Ihr Netzwerk zu erhalten, benötigen Sie einen „Durchgang“. Diesen können Sie mit Hilfe eines MyFritz-Kontos einrichten. Wenn Sie über fritz.box im Browser eingeloggt sind, gehen Sie im Menü „Internet“ zu „MyFritz!-Konto“ und richten Sie ein MyFritz!-Konto und einen Benutzer ein. Anschließend erhalten Sie eine E-Mail an die Mailadresse des MyFritz-Kontos mit Bestätigungslink. Bestätigen Sie diesen und laden Sie die Seite neu. Die MyFritz-Adresse können Sie anschließend testen, indem Sie mit einem Mobilgerät den Code mit der Endung .myfritz.net und Port, welchen Sie vorhin bei der Portweiterleitung festgelegt haben (z.B. Port 80) im Browser eingeben. Beachten Sie, dass sich das Gerät dabei nicht im gleichen WLAN befinden sollte. Wenn alles geklappt hat, wird die Login-Maske für den WebServer dargestellt.

Tipp1: Diese URL kann als Haupt-URL für MF mobil verwendet werden.

Tipp2: Die interne URL des WebServers kann als alternative URL eingegeben werden.

Tipps und Tricks

1. Das Einrichten des Netzwerkes und des Internetzuganges sollten Sie Ihrem Netzwerktechniker überlassen, denn spätestens jetzt beginnt es normalerweise kompliziert zu werden, da die Technik nur so von Fachbegriffen durchsetzt ist.
2. VPN (Virtual Private Network).
   Über ein virtuelles, privates Netzwerk haben Sie einen sicheren, geschützten Zugang zum Firmennetzwerk. Dafür ist der Installationsaufwand ein wenig höher, da Sie ein zusätzliches Programm, den VPN-Client, auf dem Smartphone, Laptop oder vgl. installieren müssen. Auf Fremdrechnern, z.B. dem Internet-Terminal am Flughafen, ist kein über VPN gesicherter Zugriff möglich. Bezüglich Installation siehe Punkt 1.
3. Große Netzwerke können den MF WebServer in die DMZ (De-Militarisierte Zone) des Gateways einbinden. Damit kann der MF WebServer vom Internet angesprochen werden, ohne dass Datenpakete in den internen Teil Ihres Netzwerkes gelangen. Energiesparend, ausreichend schnell und sicher ist dies, wenn Sie den MF WebServer auf einen Netbook mit Antiviren-Software installieren.
4. Auf der Internetseite *www.wieistmeineip.de* können Sie die eigene IP-Nummer und die Qualität des Internetzuganges ermitteln.

   Die nachfolgenden Schritte, selbst die Konfiguration des MF WebServers, kann auch ein durchschnittlich geübter Computeranwender vornehmen.

Einrichtung

Installation

Der MF WebServer wird zusammen mit dem Hauptprogramm (MF Dach plus CS, MF Dach plus miniServer, MF Handwerk plus CS, MF Handwerk miniServer) installiert, besitzt also keine eigene Installationsroutinen.
Bitte beachten Sie vor der Installation das gesonderte Handbuch „Installation“. Dieses beinhaltet das Kapitel „Netzwerk-Installation“ und Hinweise zur „Client-Server“-Umgebung. Diese Hinweise bitte genauestens beachten!

UNBEDINGT BEACHTEN: Auf dem Serverrechner muss die Windows-eigene Firewall abgeschaltet sein. Firewalls von Drittanbietern (Norton, McAfee…) sind entweder ebenfalls abzuschalten oder für die verwendeten IP-Adressen und Ports zu öffnen.

Programmstart

Sobald das Hauptprogramm MF Dach… bzw. MF Handwerk… installiert wurde, können Sie die Programme MF Server und MF WebServer von Hand starten. Klicken Sie hierzu im Programmordner zunächst doppelt auf das Programm MF_Server.exe und konfigurieren Sie dieses (siehe Handbuch MF_Server). Anschließend starten Sie das Programm MF_WebServer.exe und konfigurieren dieses wie nachfolgend beschrieben.

Nach Abschluss der Konfigurationen testen Sie die Funktion an einem Netzwerkrechner. Starten Sie dort einen Internet-Browser und geben Sie in dessen Adresszeile die IP-Nummer des MF_WebServers ein. Falls der Login-Bildschirm erscheint, hat alles funktioniert. Bei Bedarf können Sie Verknüpfungen der Programme MF_Server.exe und MF_WebServer.exe (Reihenfolge beachten → Aufruf über Batch-Datei) in den Autostart-Ordner packen und die Arbeiten damit abschließen.

Konfiguration

Die Konfiguration sowohl des MF_WebServers als auch der Nutzerprofile erfolgt innerhalb des MF WebServers. Eine Konfiguration auf Client-Seite, also im Browser des Anwenders, ist weder nötig noch möglich.

Für eine erfolgreiche Inbetriebnahme des MF WebServers arbeiten Sie die nachfolgenden Einträge des Konfiguration-Menüs von oben nach unten ab.

Menü Konfiguration

Kennwort

Das Kennwort gilt ausschließlich für die Zugriffsteuerung der Konfiguration des MF WebServers, nicht für die Zugriffe per Internet-Browser oder den Programmstart des MF WebServer.

Achtung: Legen Sie nur dann ein Kennwort fest, wenn dies notwendig ist!

Sobald ein Kennwort eingetragen wurde, kann der MF WebServer nur noch nach Eingabe dieses Kennwortes umkonfiguriert werden. Sowohl die Änderung der Gruppenrechte und der Anwender erfordern fortan die Eingabe des Kennworts.

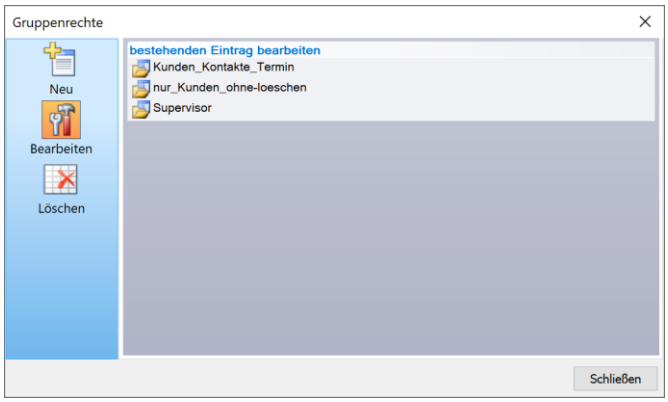
Nach Eingabe eines Kennwortes und Bestätigung mit OK erscheint die Dialogbox ein zweites Mal und fordert die erneute Eingabe zur Bestätigung. Geben Sie das Kennwort erneut ein und beenden Sie den Vorgang mit OK.

Gruppenrechte

Hier legen Sie fest, welche Daten für welche Anwender-Gruppen sichtbar bzw. bearbeitbar sein sollen.

Typischerweise legen Sie ein Gruppenrecht für den Chef bzw. Netzwerbetreuer an, in dem alle Daten sichtbar und bearbeitbar sind. Ergänzend schaffen Sie sich Gruppenrechte, in denen nur diejenigen Daten sicht- oder bearbeitbar sind, die für sonstige Gruppen von Anwendern von Interesse sind (typ. Mitarbeiter, Bauleiter, Büro etc.).

In der hier sichtbaren Konfiguration sind drei Gruppenrechte eingerichtet. Diese heißen Kunden_Kontakte_Termine, nur_Kunden_ohne-loeschen und Supervisor.



Klicken Sie oben links auf "Neu" um ein zusätzliches Gruppenrecht einzurichten.

Mit "Bearbeiten", gefolgt von der Anwahl eines Gruppenrechtes, können Sie die Gruppenrechte ändern.

Der Knopf "Löschen" entfernt das anschließend anzuklickende Gruppenrecht aus der Liste, vorausgesetzt dieses wird bei keinem Anwender mehr eingesetzt.

Die Einstellung innerhalb eines Gruppenrechts listet diverse Rubriken von Kontakten über Dokumententypen bis hin zur Zeiterfassung auf. Grundsätzlich sind alle Zugriffsrechte ausgeschaltet, um sicherzugehen, dass nicht versehentlich alle Angebote mit Preisen auf dem Mitarbeiterhandy landen. Daher schalten Sie nach und nach Rechte frei und schauen Sie ggf. das "Ergebnis" über den Internetbrowser oder ein Mobilgerät an.

Die Zuordnung eines Gruppenrechtes zu einem Anwender erfolgt im Menü Anwender. Dort kann Anwendern über ein Drop-Down-Menü eines der obigen Gruppenrechte zugewiesen werden.

Anwender

Hinterlegen Sie hier alle Nutzer, welche den über den MF Webserver über das Internet auf die Daten zugreifen dürfen bzw. sollen. Geben Sie diesen Nutzern zusätzlich zum echten Namen einen Anwendernamen und tragen Sie für diesen ein Passwort, die Nutzungsrechte u.a.m. ein.

Klicken Sie zunächst auf "Neu", gefolgt von „Hier klicken, um neuen Eintrag zu erstellen“ um einen zusätzlichen Anwender anzulegen. Es folgt eine listenförmige Dialogbox zur Eingabe von Bezeichnung, Passwort, Nutzerrechten usw. Klicken Sie in die rechte Seite der Tabelle, um die daraufhin erscheinenden Felder zu wählen. Sollte Ihnen die Bedeutung der Felder unklar sein, gibt Ihnen der Hilfetext am unteren Rand Hilfestellung.

Menü Server

IP-Adresse und Port

Im obersten Feld tragen Sie die Netzwerkadresse und den http-Port des WebServers ein. Die typische http-Port-Nr ist die 80.

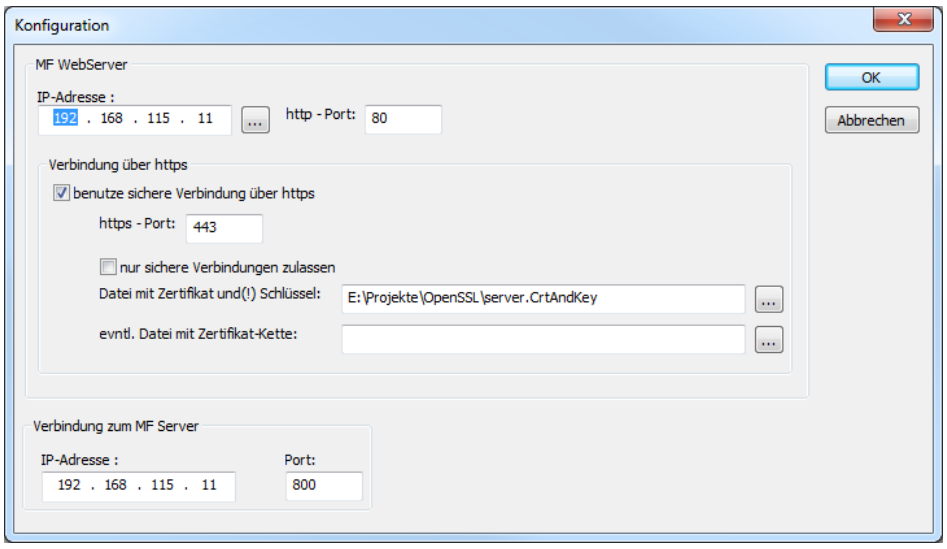
Für den Fall, dass Sie die Verbindung nicht über den ungesicherten http-Port aufbauen möchten, steht Ihnen auch ein sicherer https-Zugang zur Verfügung. Voraussetzung hierfür ist jedoch ein Sicherheitszertifikat, welches entweder selbst signiert oder von einem Sicherheitsdienstleister (Verisign, Let´s Encrypt…) bezogen werden kann.
Doch Vorsicht: selbst erzeugte Zertifikate werden nicht von allen Browsern akzeptiert und gekaufte Zertifikate kosten jährliche Gebühren.

Falls dennoch gewünscht, kann der https-Zugang mit dem Häkchen vor „benutze sichere Verbindung über https“ aktiviert werden. Die Port-Nr sollte mit 443, dem Standard-https-Port, belegt werden. Falls ausschließlich über https kommuniziert werden soll, muss auch das Häkchen bei „nur sichere Verbindung zulassen“ gesetzt werden. Die beiden Felder mit den Pfad- und Dateinamen der Zertifikate müssen sich auf die Pfade am Server-Rechner beziehen. Nur das obere ist ein Pflichtfeld.

Bitte beachten: Es gibt nur eine Zertifikatdatei! Diese muss das Zertifikat und den Key gemeinsam beinhalten. Eventuell müssen hierfür die server.crt und server.key zusammengefasst werden. In der CMD-Zeile geben Sie hierfür sinngemäß den Befehl `copy server.crt + server.key server.crtandkey`

Im letzten Feld tragen Sie die IP-Nr. und die Port-Nr. des MF_Servers ein.

Sollte deren IP-Adresse identisch sein, muss zumindest die Port-Nummer verschieden sein. In diesem Fall muss der WebServer im lokalen Netzwerk bzw. bei Nutzung einer statischen IP samt seiner Port-Nr. aufgerufen werden (Doppelpunkt beachten!). Die Eingabe in der Adresszeile des Browsers müsste im nachfolgenden Fall lauten: 192.168.115.124:80



Achten Sie darauf, dass die IP-Adresse und die Port-Nr. nicht dem Microsoft IIS oder Internetgeräten wie Web-Kameras, Telefonanlagen o.vgl. kollidieren.