# Beschreibung der Sicherheitsmaßnahmen am TK-System OmniPCX Office RCE bezüglich der Fernsteuerung von Rufumleitungen

August 2013

Bei dem TK-System OmniPCX Office RCE gibt es folgende Möglichkeiten, eine Rufumleitung aus der Ferne zu aktivieren bzw. zu deaktivieren:

1. Mit der Programmiersoftware OMC
2. Über das Leistungsmerkmal DISA-Transit
3. Durch das integrierte Voicemail-System
4. In Verbindung mit der Web-Applikation MyIC Web für Office
5. In Verbindung mit dem Extended Communication Server (ECS)
6. *Zusatzempfehlungen*

Standardmäßig sind alle Möglichkeiten bis auf den Punkt 1 inaktiv und müssen erst freigeschaltet werden. Nachfolgend werden diese Punkte im Einzelnen beschrieben.

**Generell kann, egal in welchem Software Release das System betrieben wird, keine externe Rufumleitung für eine Nebenstelle aktiviert werden.**
**Hierzu muss der jeweiligen Nebenstelle das Leistungsmerkmal „*Rufumleitung nach extern*“ freigegeben werden!**

**Eine Voicemail ist erst nach dem Ändern des Apparate-Passwortes von extern über das Voicemail-Menü erreichbar.**
**Standardmäßig werden die User bei der Erstinbetriebnahme bzw. nach dem Zurücksetzen des Passwortes zu einer Änderung aufgefordert.**

# 1. Mit der Programmiersoftware OMC

Die OmniPCX Office RCE ist im Werkszustand sofort fernwartungsfähig. Hierzu wird die Programmiersoftware OMC zusammen mit einem ISDN-Modem benötigt, sowie das Default-Installationspasswortes und die Anlagenrufnummer des jeweiligen Systems.

Diese Eigenschaft dient der Zugänglichkeit von extern nach dem Ur-Einschalten bzw. nach einem selbstständigen Zurücksetzen des Systems um eine Wiederinbetriebnahme bzw. eine Instandsetzung via Remote-Service zu gewährleisten.

Um nach der Inbetriebnahme diese Funktion zu schützen, sollte immer nach der Programmierung das Installationspasswort geändert werden und/oder der Remote-Zugang durch entsprechende Programmierung versteckt bzw. unzugänglich gemacht werden.

Ein Zugang mit der Programmiersoftware OMC ist auch dann gewährleistet, wenn das System via IP/VPN-Tunnel erreichbar ist. Hierzu werden dann zusätzlich zur OMC die IP-Adresse der CPU und das Installations-Passwort benötigt.

**Empfehlung:**
**Um das System gegen unbefugten Remote-Zugang über die Programmiersoftware OMC zu schützen, sollte immer das Installations-Passwort, wenn möglich in regelmäßigen Abständen, geändert werden.**

**Zusätzlich zum Installations-Passwort sollte auch zwingend das Passwort „SW-Herunterladen“ geändert werden. Dieses hat im Auslieferungszustand die gleiche Einstellung wie das Installations-Passwort, wird aber separat behandelt.**
**Über diesen Zugang könnte das System auf Default-Einstellung zurückgesetzt werden und wäre nun wieder mit dem Default-Passwort konfigurierbar.**

Mit dem Release 9.1 wurde die Policy der administrativen Passwörter als weiterführende Maßnahme dahingehend geändert, dass einfache Passwörter wie „00000000, 11111111, 12345678 usw. nicht mehr genutzt werden können und vom System als nicht-einstellbar abgewiesen werden (Das Operator-Passwort ist hiervon ausgeschlossen).

Das Passwort sollte ab dem Release 9.1 folgenden Kriterien entsprechen:

- Mindestens einen Großbuchstaben
- Mindestens einen Kleinbuchstaben
- Mindestens eine Ziffer
- Eine feste Länge von acht Charaktern

## 2. Über das Leistungsmerkmal DISA-Transit

Durch das Leistungsmerkmal DISA-Transit kann mit einem beliebigen Telefon via Remote-Einwahl ein Telefonat über eine Büronebenstelle (sofern diese die entsprechende Berechtigungen besitzt) geführt bzw. die Büronebenstelle auf ein beliebiges Ziel umgeleitet werden.

Dieses Leistungsmerkmal ist im Werkszustand deaktiviert und muss über eine entsprechende Programmierung aktiviert werden.

Um dieses Leistungsmerkmal zu nutzen, werden folgende Informationen benötigt:

- Anlagenrufnummer
- DISA-Transit Rufnummer
- DISA-Transit Passwort (optional zu programmieren)
- Rufnummer der Büronebenstellen
- Passwort der Büronebenstelle
- Kennziffer für Rufumleitung, wenn eine Rufumleitung aktiviert werden soll

**Empfehlung:**
**Dieses Leistungsmerkmal sollte immer mit DISA-Transit Passwort eingerichtet werden. Desweiteren sollten die Passwörter der Büronebenstellen in regelmäßigen Abständen geändert werden.**

## 3. Durch das integrierte Voicemail-System

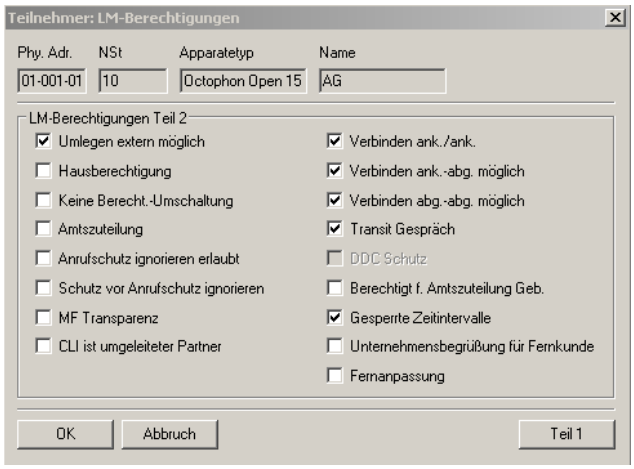
Über das integrierte Voicemail-System kann mit einem beliebigen Telefon via Einwahl eine Büronebenstelle (sofern diese die entsprechende Berechtigungen besitzt), auf ein beliebiges Ziel umgeleitet werden.
Eine Rufumleitung kann im „*Persönlichen-Optionsmenü*“ (Ziffer 9) über den Menüpunkt „*Konfiguration Ihres Assistent*“ (Ziffer 2) und über den Menüpunkt „*Änderung der Anrufweiterleitung*“ (Ziffer 7) aktiviert werden.

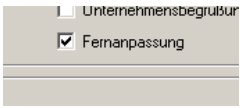
Hierzu gibt es werksseitig mehrere Verhinderungen:

Das „*Persönliche-Optionsmenü*“ (Ziffer 9) wurde für Anrufe von extern auf das Voicemail-System ab folgenden Anlagensoftwareständen deaktiviert:

- R310 060.001
- R410 065.001
- R510 059.001
- R610 047.001
- R710 069.001
- R800 030.002
- R810 045.003
- R820 026.007
- R900 033.002
- R910 021.001

Diese Option kann pro Teilnehmer durch Setzen eines Flags im Menüpunkt „*Teilnehmer-Basisstationenliste/Details/LM-Berechtigungen/Teil 2 – **Fernanpassung***“ wieder aktiviert werden:




**Hinweis:**
**Zum Ändern dieser Einstellung wird mindestens die Konfigurationssoftware „OMC 800 21.1b“ benötigt!**

Der Menüpunkt „*Konfiguration Ihres Assistent*“ (Ziffer 2) im Persönlichen-Optionsmenü wurde ab folgenden Anlagensoftwareständen steuerbar gemacht:

- R410 064.001
- R510 058.001
- R610 031.001
- R700 026.001
- R710 022.001
- R800 030.002
- R810 045.003
- R820 026.007
- R900 033.002
- R910 021.001

Dieser Menüpunkt kann systemweit unter „*System Verschiedenes/Speicher Lesen-Schreiben/Sonstige symbolische Adressen*“ über folgende CM-Adresse gesteuert werden:

Adresse = **PerAssAlwd** (Personal Assistant Allowed)
Default-Wert = **00**

Mögliche Werte = **00 – Menüpunkt einstellbar aber inaktiv**
**01 – Menüpunkt einstellbar und aktiv**

Der Menüpunkt „***Änderung der Anrufweiterleitung***“ (Ziffer 7) im Persönlichen-Optionsmenü wurde ab folgenden Anlagensoftwareständen deaktiviert:

- R710 028.001
- R800 030.002
- R810 045.003
- R820 026.007
- R900 033.002
- R910 021.001

Dieser Menüpunkt kann systemweit unter „*System Verschiedenes/Speicher Lesen-Schreiben/Sonstige symbolische Adressen*“ über folgende CM-Adresse wieder aktiviert werden:

Adresse = **DivRemCust** (Diversion Remote Customization)
Default-Wert = **00**

Mögliche Werte = **00 – Menüpunkt inaktiv**
**01 – Menüpunkt aktiv**

Um diese Leistungsmerkmale zu nutzen, werden folgende Informationen benötigt:

- Anlagenrufnummer
- Rufnummer des Voicemail-Systems
- Rufnummer der Büronebenstellen
- Passwort der Büronebenstelle

**Empfehlung:**
**Die Passwörter der Büronebenstellen sollten in regelmäßigen Abständen geändert werden.**

**Weiterführende Maßnahmen:**

Folgende Schutzmechanismen wurden im Zuge dieser Änderungen zusätzlich implementiert:

Die Policy der Benutzer-Passwörter wurde darauf hingehend geändert, dass einfache Passwörter wie „0000...., 1111...., 1234.... usw. nicht benutzt werden können und vom System als nicht-einstellbar abgewiesen werden.

Diese Änderung wurde ab folgenden Anlagensoftwareständen eingeführt:

- R410 064.001
- R510 058.001
- R610 047.001
- R710 052.007
- R800 030.002
- R810 045.003
- R820 026.007
- R900 033.002
- R910 021.001

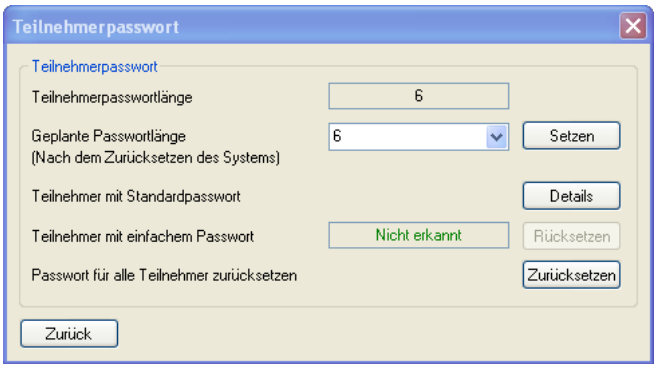
Ab dem **Release 8.2** können die Benutzer-Passwörter von 4-Stellen auf 6-Stellen ein- bzw. umgestellt werden. Standardmäßig startet das System mit einer 6-Stellen-Passworteinstellung.

**Hinweis:**
**Ein von < R8.2 migriertes System behält die 4-stellige Passworteinstellung. Es wird aber dann bei jeder Anmeldung mit der OMC ein Hinweis hierzu eingeblendet.**

Ab dem Release 9.1 gibt es in der OMC einen Menüpunkt, mit dem der Status der Teilnehmer-Passwörter ermittelt werden kann.

Über dieses Menü können folgende Aktionen durchgeführt werden:

- Die aktuell eingestellte Teilnehmerpasswortlänge kann ermittelt werden
- Die Teilnehmerpasswortlänge kann umgestellt werden (Reset erforderlich)
- Alle Teilnehmer, die ein noch unverändertes Passwort besitzen, können ermittelt werden
- Alle Teilnehmer, die ein einfaches Passwort besitzen (z. B. durch eine migrierte Datenbank), können ermittelt werden
- Alle Teilnehmer-Passwörter können zurückgesetzt werden




Dieser Menüpunkt wird unter „*System Verschiedenes/Passwort/Teilnehmerpasswort*“ erreicht.

Eine Falscheingabe der Passwörter zur Authentifizierung über das Voicemail-System wird gezählt. Die Anzahl der Fehlversuche ist einstellbar. Nach dem Überschreiten der Fehlversuche wird das Passwort für den externen Zugriff gesperrt und kann nur über die Vermittlung, den Administrator oder durch einen lokalen Zugriff des jeweiligen Benutzers auf das Voicemail-System wieder zurückgesetzt werden.

Diese Änderung wurde ab folgenden Anlagensoftwareständen eingeführt:

- R310 060.001
- R410 064.001
- R510 058.001
- R610 033.001
- R700 026.001
- R710 022.007
- R800 030.002
- R810 045.003
- R820 026.007
- R900 033.002
- R910 021.001

Die Anzahl der Fehlversuche kann systemweit unter „*System Verschiedenes/Speicher Lesen-Schreiben/Symbolische Fehlersuchadressen*“ über folgende CM-Adresse eingestellt werden:

Adresse = **VMUMaxTry**
Default-Wert = **03**

Mögliche Werte = **00** - **FF**

Bei der Fernabfrage einer Sprachnachricht über das Voicemail-System kann über die Ziffer 3 ein Rückruf zum jeweiligen Anrufer veranlasst werden. Der Menüpunkt kann deaktiviert werden.

Diese Änderung wurde ab folgenden Anlagensoftwareständen eingeführt:

- R510 064.001
- R610 052.001
- R710 097.001
- R820 045.001
- R900 037.001
- R910 021.001

Dieser Menüpunkt kann systemweit unter „*System Verschiedenes/Speicher Lesen-Schreiben/Sonstige symbolische Adressen*“ über folgende CM-Adresse deaktiviert werden:

Adresse = **CallCorres**
Default-Wert = **01**

Mögliche Werte = **00 – Menüpunkt inaktiv**
**01 – Menüpunkt aktiv**

## 4. In Verbindung mit der Web-Applikation MyIC Web für Office

Mit dem Release 8.1 wurde die Applikation MyIC Web für Office eingeführt. Mit diesem Feature kann die Büronebenstelle sehr einfach auf ein beliebiges Ziel umgeleitet werden.
Der Zugriff auf diese Web-Oberfläche kann so konfiguriert werden, dass diese von überall aus dem Internet mit einem Browser erreicht werden kann.

Um diese Leistungsmerkmale zu nutzen, werden folgende Informationen benötigt:

- Öffentliche Internetadresse (URL) der Firma
- Umgeleitete Portnummer
- Rufnummer der Büronebenstellen
- Passwort der Büronebenstelle

**Empfehlung:**
**Bei der Nutzung von MyIC Web für Office über das Internet sollten die Benutzer-Passwörter auf 6-stellig eingestellt sein. Desweiteren sollte der Umgang mit dem jeweiligen Benutzer-Passwort hierbei sehr sensibel behandelt werden.**

## 5. In Verbindung mit dem Extended Communication Server (ECS)

Wird die OmniPCX Office RCE zusammen mit einem Extended Communication Server betrieben, können auf dem ECS eigerichtete Benutzer, die einer Nebenstelle zugeordnet wurden, über einen Browser-Zugriff auf das Virtuelle Büro eine Rufumleitung für die jeweils zugeordnete Nebenstelle aktivieren.

Um dieses Leistungsmerkmal zu nutzen, werden folgende Informationen benötigt:

- Öffentliche Internetadresse (URL) des ECS
- Benutzer-Name
- Benutzer-Passwort

# 6. Zusatzempfehlungen

- **In den häufigsten Fällen wird zum Einleiten der Rufumleitung das Apparate-Passwort benötigt. Deswegen wird generell empfohlen, das System mindestens im Release 8.2 zu betreiben um auf 6-stellige Apparate-Passwörter umschalten zu können.**

- Das System kann in den Nachtzeiten und am Wochenende via Zeitsteuerung oder auch manuell in den **„Eingeschränkten Modus“** gesetzt werden. Dadurch können die Teilnehmerberechtigungen und auch die öffentliche Einwahl verändert werden (Nachtschaltung)

- Die Sprachspeicherports sollten nur entsprechend der **benötigten** Berechtigungen eingestellt werden

- Es sollten Rufnummern-Sperrtabellen verwendet werden

- In der Regel wird die Ziffer „0“ für eine Amtsholung verwendet. Die Bündelberechtigung sollte hierzu auf „National“ beschränkt werden. Für „Internationale Gespräche“ kann ein zusätzliches Bündel mit einer aufwändigeren Amtsholung wie z. B. „*#*“ eingerichtet werden.

- Sollte ein Service-Techniker das Unternehmen verlassen, so nimmt er möglicherweise auch sämtliche Einwahl-Daten der Kunden mit. Diese sollten dann zur Sicherheit geändert werden.

- Apparate-Passwörter sollten nicht sichtbar im Büro notiert werden (z.B. mit Notizzetteln unter dem Telefon usw.). Dadurch wird das Passwort fremden Personen ersichtlich.

- Beim Verlassen des Arbeitsplatzes sollte das Telefon abgesperrt werden um das Einleiten einer Rufumleitung von fremden Personen zu verhindern.

*---ENDE DES DOKUMENTS---*