

Dokumentation: Call Recording (bis Version 22.2.16)

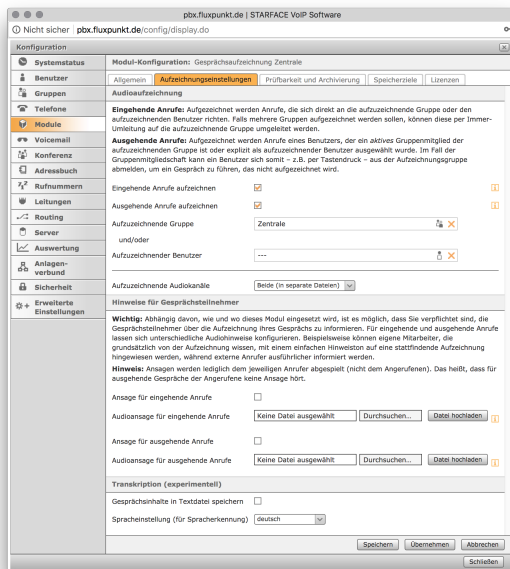
Allgemeines

Das Modul Gesprächsaufzeichnung ist grundsätzlich so entworfen, dass es mehrfach auf einer Anlage betrieben werden kann, das heißt: es können mehrere Modul-Konfigurationen angelegt werden. Alle Modulkonfigurationen teilen sich die integrierte Protokolldatenbank sowie das anlagenindividuelle Zertifikat und Schlüsselpaar für kryptografische Signaturen. Je Modul-Konfiguration können jedoch individuelle Speicherziele angegeben werden.

Bei der Ausführungsreihenfolge der Modul-Konfigurationen ist zu beachten, dass ein Gespräch, das bereits von einer Konfiguration aufgezeichnet wird, nicht erneut von einer anderen Konfiguration erfasst wird.

Aufzeichnungseinstellungen

Der Bereich Aufzeichnungseinstellungen behandelt die Konfiguration, welche Gespräche und welche Audiokanäle aufgezeichnet werden sollen sowie die optionale Wiedergabe von Aufzeichnungshinweisen.



Audioaufzeichnung

Eingehende Anrufe: Aufgezeichnet werden Anrufe, die sich *direkt an die aufzuzeichnende Gruppe* (Ziel ist eine Gruppenrufnummer) oder *den aufzuzeichnenden Benutzer* (Ziel ist die persönliche Rufnummer eines Benutzers) richten. Falls mehrere Gruppen aufgezeichnet werden sollen, können diese per Immer-Umleitung auf die aufzuzeichnende Gruppe umgeleitet werden.

Ausgehende Anrufe: Aufgezeichnet werden Anrufe eines Benutzers, der ein *aktives* Gruppenmitglied der aufzuzeichnenden Gruppe ist oder explizit als aufzuzeichnender Benutzer ausgewählt wurde. Im Fall der Gruppenmitgliedschaft kann ein Benutzer sich somit – z.B. per Tastendruck – aus der Aufzeichnungsgruppe abmelden, um ein Gespräch zu führen, das nicht aufgezeichnet werden soll.

Direktanrufe an aktive Gruppenmitglieder aufzeichnen: Eingehende Anrufe werden normalerweise nur aufgezeichnet, wenn sie direkt die aufzuzeichnende Gruppe oder den aufzuzeichnenden Benutzer zum Ziel haben. Bei Aktivierung der Einstellung "Direktanrufe an aktive Gruppenmitglieder aufzeichnen", werden zusätzlich Anrufe aufgezeichnet, die nicht an die aufzuzeichnende Gruppe oder den aufzuzeichnenden Benutzer gerichtet sind, sondern *direkt an die persönliche Durchwahl* eines Benutzers, der aber gleichzeitig *aktives* Mitglied in der aufzuzeichnenden Gruppe ist.

Das Modul prüft für jeden ein- und ausgehenden Anruf getrennt, ob die Aufzeichnungsvoraussetzungen vorliegen. Wenn ja, wird eine optionale Hinweisansage abgespielt und im Anschluss die Aufzeichnung automatisch gestartet.

Für die aufzuzeichnenden Audiokanäle stehen folgende Optionen zur Verfügung:

- Anrufer
- Angerufener
- Beide (in eine Datei)
- Beide (in separate Dateien)

Inhalt

- [Allgemeines](#)
- [Aufzeichnungseinstellungen](#)
 - [Audioaufzeichnung](#)
 - [Hinweise für Gesprächsteilnehmer](#)
- [Prüfbarkeit und Archivierung](#)
- [Speicherziele](#)
 - [Windows-Share](#)
 - [SFTP](#)
 - [Microsoft OneDrive](#)
 - [Anlegen von Aufbewahrungsrichtlinien in Microsoft Office 365](#)
 - [Konfiguration von Aufbewahrungsrichtlinien](#)
 - [Benachrichtigung bei Speicherfehlern](#)
- [Bekannte Einschränkungen](#)
- [Hinweise zur Aufzeichnung nach dem WpHG \(Stand 03.01.2018\)](#)
- [Hinweise zur Konfiguration der App-Anmeldung an Microsoft Tenants](#)

i Bitte stellen Sie bei der Erstkonfiguration sicher, dass Sie das Modul-Loglevel mindestens auf Stufe "INFO" stellen. Das Modul gibt in diesem Loglevel Informationen zum Prüf-Zertifikat und der OneDrive-Anbindung aus.

! Sonderfall bei Gesprächen zwischen zwei STARFACE Benutzern

Bei Gesprächen *zwischen zwei STARFACE-Benutzern* wird in STARFACE Version 6.4.3 kein ausgehendes Gespräch (des Anrufers), sondern lediglich das eingehende Gespräch (des Angerufenen), an das Modulsystem signalisiert. Eine Aufzeichnung findet deshalb nur statt, wenn der angerufene Teilnehmer in einer Aufzeichnungsgruppe ist. Mit anderen Worten: Es ist nicht ausreichend, dass der anrufende STARFACE Benutzer Mitglied einer Aufzeichnungsgruppe ist.

Bei der Aufzeichnung beider Gesprächsteilnehmer in eine Datei, werden beide Teilnehmer als je ein Kanal einer Stereo-WAV-Datei gespeichert. Das Zusammenführen der Kanäle erfolgt unmittelbar nach Beendigung des Gesprächs, aber vor dem Signieren der Audiodaten.

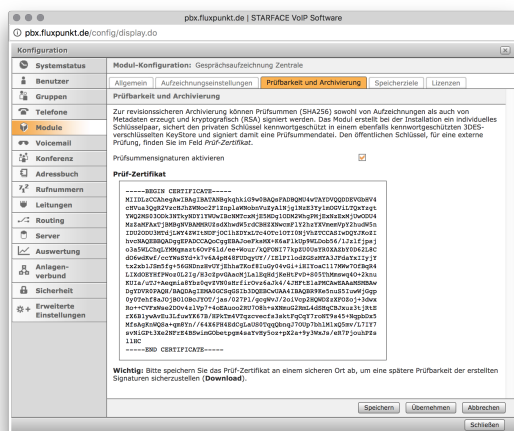
Hinweise für Gesprächsteilnehmer

Abhängig davon, wie und wo dieses Modul eingesetzt wird, ist es möglich, dass Sie verpflichtet sind, die Gesprächsteilnehmer über die Aufzeichnung ihres Gesprächs zu informieren. Für eingehende und ausgehende Anrufe lassen sich unterschiedliche Audiohinweise konfigurieren. Beispielsweise können eigene Mitarbeiter, die grundsätzlich von der Aufzeichnung wissen, mit einem einfachen Hinweiston auf eine stattfindende Aufzeichnung hingewiesen werden, während externe Anrufer ausführlicher informiert werden.

i Ansagen werden lediglich dem jeweiligen Anrufer abgespielt (nicht dem Angerufenen). Das heißt, dass für ausgehende Gespräche der Angerufene keine Ansage zu hören bekommt. Es wird davon ausgegangen, dass bei ausgehenden aufzuzeichnenden Anrufen, der Angerufene im Vorfeld über die Aufzeichnung informiert wurde.

Prüfbarkeit und Archivierung

Im Bereich Prüfbarkeit und Archivierung lassen sich Prüfsummensignaturen aktivieren um so spätere Nachweise der Unverändertheit und Integrität der protokollierten Metadaten und Audioaufzeichnungen zu erlauben.



! Bitte speichern Sie das im Modul angezeigte Prüf-Zertifikat ab. Es enthält keine geheimen Informationen, ist jedoch für eine spätere Integritätsprüfung unerlässlich! Ohne das Zertifikat kann nicht sichergestellt werden, dass die Prüfsummen der Meta- und Audiodaten vom Modul selbst erzeugt wurden. Es wird empfohlen, das generierte Zertifikat zeitnah von einer vertrauenswürdigen CA digital signieren zu lassen.

Das Modul erstellt bei der Erstinstallation ein individuelles 2048-Bit RSA-Schlüsselpaar (privater und öffentlicher Schlüssel). Der private Schlüssel wird mit einem geheimen, kundenindividuellen Passwort verschlüsselt und in einem kennwortgeschützten und 3DES-verschlüsselten KeyStore abgelegt. Der private Schlüssel steht ausschließlich modulintern zur Verfügung.

Nach einer Aufzeichnung wird innerhalb des Moduls eine Prüfsummendatei erstellt, die die SHA256-Prüfsummen der Meta- und aller Audiodateien enthält. Die Prüfsummendatei ist formatkompatibel zu shasum (Digest-SHA).

Liegen alle Meta- und Audiodaten sowie die Prüfsummendatei in einem Verzeichnis ist die Integrität mittels `shasum -a 256 <Prüfsummendatei>` nachprüfbar.

Anschließend wird noch eine base64-kodierte und SHA256-basierte RSA-Signatur (basierend auf dem individuellen privaten Schlüssel) der Prüfsummendatei erzeugt und in einer Datei mit dem Namen `<Prüfsummendatei>.SHA256withRSA.sig` gespeichert.

Diese Signatur stellt sicher, dass die angegebenen Prüfsummen innerhalb des Moduls berechnet und nicht nachträglich geändert wurden.

Für die Signaturprüfung wird der öffentliche Schlüssel des RSA-Schlüsselpaares benötigt. Dieser ist innerhalb des Prüfzertifikats, das in der Modulkonfiguration angezeigt und im Modul-Log bei jedem Start ausgegeben wird, kodiert.

Das Prüf-Zertifikat ist von und für den Inhaber "Fluxpunkt Gesprächsaufzeichnung <Modul-ID>" ausgestellt und hat eine Gültigkeitsdauer von 100 Jahren ab Zeitpunkt der Generierung.

Die Echtheit des Zertifikats kann über das Modullog verifiziert werden. Dort werden alle Zertifikatsdetails bei jedem Start abgebildet.

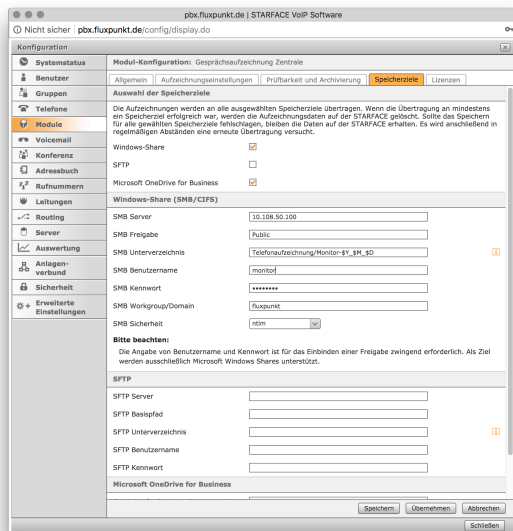
Die vollständige Prüfung einer Aufzeichnung besteht nun aus

1. dem Vergleich der in der Prüfsummendatei hinterlegten Prüfsummen mit den Prüfsummen der Audio- und Metadatendateien
2. dem Prüfen der Signatur der Prüfsummendatei mit dem öffentlichen Schlüssel des Prüf-Zertifikats.

Hierfür steht Ihnen als Beispielimplementierung unser Prüf-Skript [verify.sh](#) zur Verfügung.

Speicherziele

Im Bereich Speicherziele lassen sich Uploads auf SMB-Freigabe n, SFTP-Server und Microsoft OneDrive aktivieren. Es ist möglich mehrere unterschiedliche Speicherziele zu aktivieren, so dass die Aufzeichnungsdaten an mehreren Orten gespeichert werden.



Windows-Share

Geben Sie den Server der Ziel-Netzwerkfreigabe ausschließlich als Hostnamen oder IP-Adresse an. Es wird keine Protokollangabe oder Ähnliches benötigt (und auch nicht unterstützt).

Der Benutzername erfordert keine Domänenangabe (hierfür gibt es ein eigenes Feld). Der eingetragene Benutzer benötigt für die angegebene Freigabe Lese-/Schreibrechte und das Recht, Verzeichnisse /Dateien neu zu erstellen.

Der Freigabename darf keine Unterverzeichnisangaben enthalten.

Im Feld SMB Unterverzeichnis können statische und dynamische Verzeichnisangaben (getrennt durch "/>) enthalten sein. Beispiel einer statischen Angabe wäre die Verzeichnisstruktur "Aufzeichnung/Starface". Dynamische Verzeichnisangaben bestehen aus einer Zusammensetzung Variablen mit optional statischen Namensanteilen, z.B. "Record-\$Y_\$M_\$D_\$h_\$m_\$s". Nicht existierende Verzeichnisse werden erstellt.

Folgende Platzhalter können in den variablen Namensbestandteilen verwendet werden:

- \$Y = Jahr
- \$M = Monat
- \$D = Tag
- \$h = Stunde
- \$m = Minute
- \$s = Sekunde

Die variablen Bestandteile werden durch den Zeitstempel vom Beginn der Aufzeichnung ersetzt. Durch dynamische Unterverzeichnisse kann nicht nur chronologisch archiviert werden, sondern auch verhindert werden, dass sich zu viele Audiodateien in einem Verzeichnis ansammeln, was zu serverseitigen Performanceproblemen führen kann.

Das Feld "SMB Sicherheit" ist derzeit ein Platzhalter und wird noch nicht aktiv berücksichtigt.

SFTP

Geben Sie hier den SFTP-Server als Hostnamen oder IP-Adresse an. Es wird keine weitere Protokollangabe oder Ähnliches benötigt (und auch nicht unterstützt).

Das SFTP-Verzeichnis sollte relativ zum Home-Verzeichnis des SFTP-Benutzers angegeben werden. Bitte verwenden Sie ausschließlich ASCII-Zeichen ohne Sonderzeichen für die Verzeichnisangabe. Die von STARFACE verwendete SFTP-Bibliothek hat in manchen Fällen Probleme mit verschachtelten Verzeichnissen. Falls es beim Upload zu Problemen kommt, versuchen Sie bitte die Angabe nur eines Verzeichnisses oder der Angabe eines Punktes ("."), um das Home-Verzeichnis des SSH-Benutzers auszuwählen. Modulseitig werden innerhalb der Verzeichnisangabe die selben variablen Namensbestandteile unterstützt, wie für Windows-Shares.

Microsoft OneDrive



GermanCloud vs. InternationalCloud

Kunden der Microsoft GermanCloud (Office 365 Deutschland oder OneDrive Plan Deutschland; spezieller und etwas teurerer Tarif für erhöhte Datenschutzanforderungen) müssen in der Modulkonfiguration zwingend die Option GermanCloud aktivieren und den danach neu generierten

Authorisierungs-Link verwenden (erkennbar am Ziel-Host `login.microsoftonline.de`). Für Kunden der internationalen Cloud muß die Option deaktiviert werden (der generierte Link enthält dann `login.microsoftonline.com`).

Es ist weder möglich, sich mit Zugangsdaten der internationalen Cloud an der GermanCloud anzumelden, noch umgekehrt.

Falls es beim Gewähren der Zugriffsrechte Probleme gibt, versuchen Sie bitte die Anmeldung mit einem administrativen Office 365-Konto.



Hinweis

Wir empfehlen, für das Modul Gesprächsaufzeichnung einen separaten Office 365-Benutzer zu verwenden. Auf diese Weise läßt sich die konfigurierte Aufbewahrungsrichtlinie gezielt nur auf Dateien dieses Benutzers anwenden, ohne dass alle übrigen Inhalte der Aufbewahrungsrichtlinie unterliegen.

Wenn Sie Microsoft OneDrive als Speicherziel verwenden möchten, klicken Sie im Modulkonfigurations-Tab "Speicherziele" auf den Button "Gesprächsaufzeichnung für OneDrive-Nutzung autorisieren". Kopieren Sie den angezeigten Link und öffnen diesen mit einem Webbrowser Ihrer Wahl. Sie werden auf eine Microsoft-Anmeldeseite umgeleitet und zur Eingabe Ihrer Office 365/OneDrive-Zugangsdaten aufgefordert.

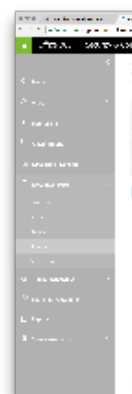
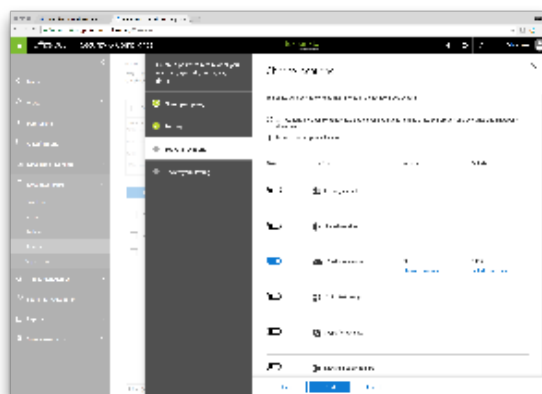
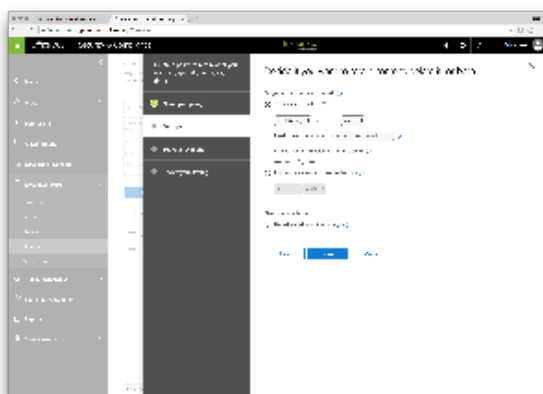
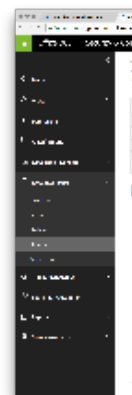
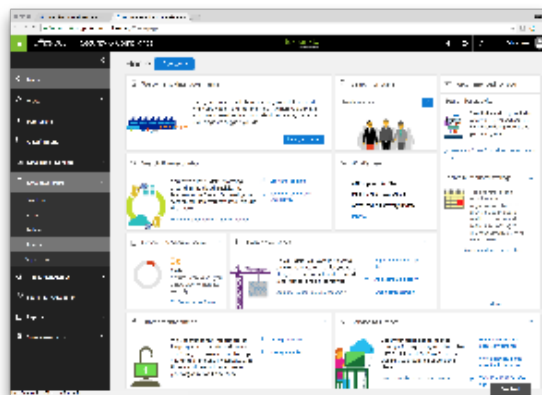
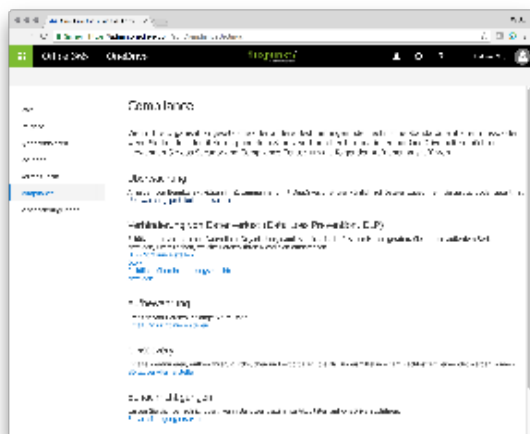
Anschließend haben Sie die Möglichkeit, dem Modul Gesprächsaufzeichnung Zugriff auf Ihr OneDrive-Verzeichnis zu geben. Wenn Sie den Zugriff bestätigen, werden Sie auf eine inhaltlose Seite umgeleitet. In der Browseradresszeile finden Sie einen Parameter `code=<OneDrive_Authorisierungscode>`. Kopieren Sie den Authorisierungscode (ausschließlich den Code ohne irgendeine weiteren Parameter) in das Feld "OneDrive for Business Authorisierungscode" innerhalb der Modulkonfiguration.

Das Feld "OneDrive for Business Unterverzeichnis" unterstützt die selbe Syntax, wie Unterverzeichnisse bei Windows-Shares. Es können hier verschachtelte Angaben und variable Namensbestandteile verwendet werden.

Sollte der Upload auf OneDrive fehlschlagen, prüfen Sie bitte den eingegebenen Authorisierungscode. Schlägt der Upload immer noch fehl, führen Sie die beschriebene OneDrive-Anmeldeprozedur erneut durch.

Anlegen von Aufbewahrungsrichtlinien in Microsoft Office 365

Konfiguration von Aufbewahrungsrichtlinien



Benachrichtigung bei Speicherfehlern

Wenn Sie über Probleme beim Upload Ihrer Gesprächsaufzeichnungen informiert werden möchten, geben Sie bitte eine Emailadresse für Benachrichtigungen an. Der erfolgreiche Emailversand setzt voraus, dass die STARFACE-Emailkonfiguration korrekt durchgeführt wurde.

Für jeden Uploadversuch, bei dem mindestens eine Datei nicht korrekt hochgeladen werden konnte, wird eine Email versendet. Da die Dateien in diesem Fall auf der STARFACE verbleiben und beim nächsten Uploadversuch erneut erfasst werden, kann es in kurzen Intervallen zu sehr vielen Emails kommen.

Bekannte Einschränkungen



Maximale Größe einer Aufzeichnung

Die Länge eines Telefongesprächs darf im WAV-Format nicht mehr als 2GB (entspricht einem Gespräch von etwa 33h) beanspruchen, ansonsten schlägt die Aufzeichnung für dieses Gespräch fehl.



Dringende Empfehlung: Email-Benachrichtigung

Wir empfehlen dringend, die Emailbenachrichtigung bei Speicherfehlern zu aktivieren. Sollte es Call Recording nicht möglich sein, Aufzeichnungen in das gewählte Speicherziel hochzuladen, so verbleiben diese auf Ihrer STARFACE. Hierdurch kann der verfügbare Festplattenplatz Ihrer Installation vollständig aufgebraucht werden und das System zum Stillstand bringen.



STARFACE Backups / STARFACE Redundanzmodul

Während einer Gesprächsaufzeichnung darf kein STARFACE Backup-Vorgang ausgeführt werden, da ansonsten das Ziel-Laufwerk für die Aufzeichnung in das Backup mit aufgenommen wird (betrifft STARFACE 6.4.2.x) oder laufende Aufzeichnungsprozesse gestört bzw. unterbrochen werden, wodurch aufgezeichnete Teilnehmer nicht mehr angerufen werden können (betrifft auch andere STARFACE Versionen). Bitte planen Sie die Backup-Zeit so, dass währenddessen keine Gesprächsaufzeichnung stattfindet.

Da das STARFACE Redundanzmodul technisch ebenfalls Backupprozesse auslöst, gilt die genannte Einschränkung ebenfalls für das STARFACE Redundanzmodul. Dieses ist nicht kompatibel mit dem Modul Gesprächsaufzeichnung!

Wenn nicht ausgeschlossen werden kann, dass während eines Backups aufzuzeichnende Gespräche stattfinden, müssen STARFACE Backups deaktiviert und eine STARFACE-VM-Edition eingesetzt werden, die es erlaubt externe Backups der VM durchzuführen (Snapshot-basierte Backups), die für die auszuführende Anwendung (das STARFACE-System) transparent sind.

Das STARFACE-Default-Backup kann derzeit nur über die Ausführung des folgenden SQL-Statements innerhalb der STARFACE-Datenbank deaktiviert werden (bitte wenden Sie sich hierfür an Ihren zuständigen STARFACE Partner):

```
UPDATE backup_schedules SET type = 'MANUAL' WHERE id = 0;
```



Bitte beachten Sie, dass die Gesprächsaufzeichnung eine STARFACE Appliance oder VM mit ausreichend freiem Speicherplatz und eine SSD mit hohen Schreibraten erfordert!

Parallele Aufzeichnungen stellen erhöhte Anforderungen an die Ressourcen Ihrer Anlage, so dass die von STARFACE für Appliances angegebenen Werte für die maximale Anzahl Gespräche/User bei Aufzeichnungen nicht erreicht werden.

Wir empfehlen Enterprise/Platinum-Appliances oder VM-Editionen mit SSD-Storage und mindestens 8 GB RAM zu verwenden. Können die Aufzeichnungsdaten nicht schnell genug auf das Storage-System geschrieben werden, so kommt es zu Gesprächsaussetzern!

Hinweise zur Aufzeichnung nach dem WpHG (Stand 03.01.2018)

Wertpapierdienstleistungsunternehmen müssen Neu- und Altkunden sowie eigene Mitarbeiter und beauftragten Personen *vorab* in geeigneter Weise über die Aufzeichnung von Telefongesprächen informieren. Hat ein Wertpapierdienstleistungsunternehmen seine Kunden nicht vorab über die Aufzeichnung der Telefongespräche oder der elektronischen Kommunikation informiert oder hat der Kunde einer Aufzeichnung widersprochen, darf das Wertpapierdienstleistungsunternehmen für den Kunden keine telefonisch oder mittels elektronischer Kommunikation veranlassten Wertpapierdienstleistungen erbringen, wenn sich diese auf die Annahme, Übermittlung und Ausführung von Kundenaufträgen beziehen.

Es bietet sich daher an, Kunden im Rahmen einer gesonderten Mitteilung im Vorfeld, am Besten schriftlich, über die Aufzeichnungspflicht nach dem Wertpapierhandelsgesetz zu unterrichten.

Auf Anfrage des Kunden sind diesem, die ihn betreffenden und gespeicherten Aufzeichnungen, während der Aufbewahrungsdauer, zur Verfügung zu stellen. Nach Ablauf der geforderten Aufbewahrungsdauer sind die Aufzeichnungen zu löschen.

Quellen

- Wertpapierhandelsgesetz (WpHG)
- Verordnung (EU) Nr. 600/2014
- Verordnung (EU) Nr. 596/2014
- Delegierte Verordnung (EU) 2017/565
- MiFID II - Richtlinie (EU) 2014/65

Richtlinie 2014/65/EU Neufassung - MiFID II

Delegierte Verordnung (EU) vom 25.04.2016

2. FiMaNoG (Zweites Finanzmarktnovellierungsgesetz)

Hinweise zur Konfiguration der App-Anmeldung an Microsoft Tenants



Informationen zur rechtssicheren Umsetzung geltender Gesetze

Bitte haben Sie dafür Verständnis, dass wir keine Rechtsberatung anbieten dürfen. Bei Fragen zur rechtssicheren Umsetzung gesetzlicher Anforderungen im konkreten Fall wenden Sie sich bitte an eine zur Rechtsberatung berechnete Person Ihres Vertrauens.

1. Im Azure Portal (<https://portal.azure.com/>): "App-Registrierungen" -> "+ Neue Registrierung"
2. Name der App eintragen und bei "Unterstützte Kontentypen" den Punkt "Konten in einem beliebigen Organisationsverzeichnis (beliebiges Azure AD-Verzeichnis – mehrinstanzenfähig)" auswählen und auf "Registrieren" klicken.
3. In der linken Spalte auf "API-Berechtigungen" und dort auf "+ Berechtigungen hinzufügen" und dort "Microsoft Graph" -> "Anwendungsberechtigungen" auswählen. In der angezeigten Liste müssen folgende Berechtigungen ausgewählt werden und anschließend auf "Berechtigungen hinzufügen" klicken:
 - Files.ReadWrite.All
4. Anschließend auf "Administratorenzustimmung für '...' erteilen" klicken und den Dialog bestätigen.
5. In der Tabelle sollte jetzt bei allen Berechtigungen in der Spalte "Status" ein grüner Hacken sein.
6. In der linken Spalte auf "Zertifikate & Geheimnisse" und dort auf "+ Neuer geheimer Clientschlüssel" klicken. "Beschreibung" und "Gültig bis" nach belieben setzen (max. 2 Jahre möglich) und anschließend auf Hinzufügen klicken.
7. In der Spalte "Wert" steht nun das "Anwendungs Geheimnis". Dieses sollte gesichert werden, da es später nicht mehr einsehbar ist.
8. In der linken Spalte auf "Übersicht" klicken. Dort findet man die Werte für "Anwendungs-ID" und "Verzeichnis-ID"
9. "Anwendungs-ID", "Anwendungs Geheimnis" und "Verzeichnis-ID" im Modul eintragen.