Security White Paper

Synappx™ Go und Synappx™ Meeting

www.sharp.de

SHARP
Be Original.

Inhalt

1. Einleitung

Übersicht

Synappx Go und Synappx Meeting und nicht Meetings sind Anwendungen und Services für die Zusammenarbeit, Produktivität und Analytik. Sie werden durch ein robustes Sicherheitssystem mit mehreren Ebenen geschützt, damit das System und seine Komponenten hinsichtlich Ihrer Daten oder Netzwerke keine Schwachstellen oder Zugriffsmöglichkeiten bieten. Durch eine Kombination von führenden Technologieanbietern wie Microsoft Azure, G Suite sowie bewährten Sicherheitsverfahren bleiben Ihre Daten während Ihrer Nutzung der Synappx-Services sicher und Sie maximieren gleichzeitig die Produktivität in Ihrem Büro. Die für Synappx geltenden Sicherheitsbestimmungen werden in diesem White Paper beschrieben.

Synappx Go

Synappx Go ist ein auf Mobiltelefone basierender Service, der die Nahfeld-Kommunikation (Near Field Communication; NFC) nutzt. Damit wird ein bequemes und zeitsparendes Scannen auf die auf das gewünschte Gerät sowie die Druckfreigabe oder das Drucken von Cloud-Dateien auf Sharp-Multifunktionsdruckern (Multifunction Printers; MFPs) in allen Büroräumen ermöglicht. Über Ihr Mobiltelefon und Ihre App können Sie auch Cloud-Inhalte auswählen und dank NFC einfach auf dem Sharp Display wiedergeben. Die Cloud Software und die Services von Synappx Go nutzen die Microsoft Azure Datenbank, die Geräteprovisionierung, den IoT-Hub und viele andere Services.

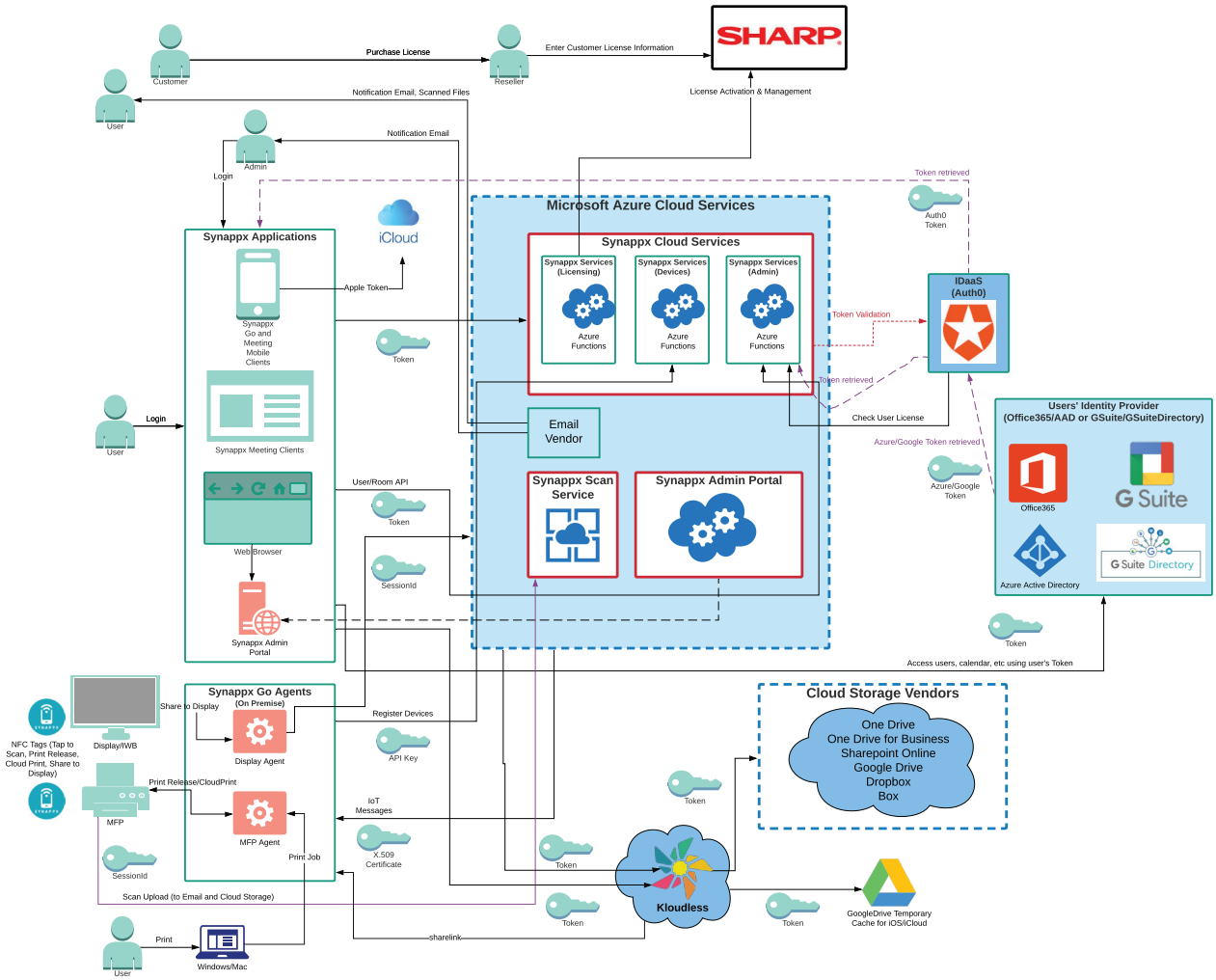
Synappx Meeting

Synappx Meeting nutzt die Azure-Cloud, Rich Clients sowie mobile und sprachgesteuerte * Technologien, damit die Benutzer ihre Meetings rechtzeitig beginnen und effektiver arbeiten können. Mit einem Klick auf eine Schaltfläche werden alle wichtigen Meeting-Komponenten verbunden. Ihr PC wird auf das Display des Sharp-Konferenzraums gespiegelt, die Web-Konferenz startet automatisch und Sie können auf die Meeting-Unterlagen zugreifen. Mit Sprachbefehlen* sparen Sie Zeit für gemeinsame Sitzungsaktionen. Die Cloud Software und die Services von Synappx Meeting nutzen die Microsoft Azure Datenbank, den Speicher, die Funktionen und viele andere Services.

* Die Sprachsteuerung ist momentan in Europa nicht verfügbar.

2. Überblick über die Architektur

Nachfolgend finden Sie einen Überblick über die Synappx-Plattform (bereitgestellt von Microsoft Azure) einschliesslich Synappx Go and Synappx Meeting:



3. Synappx Cloud Services

Synappx Meeting und Synappx Go nutzen die Cloud-Plattform-Services von Microsoft Azure als Grundlage für die Services der Synappx-Cloud. Microsoft Azure ist ein hochangesehener globaler Cloud-Service und bietet eine breite Vielzahl von Funktionen, die von der Produktfamilie von Sharp Synappx genutzt werden – dazu gehören auch die Datenbank Azure Cosmos, Speicher, zahlreiche IoT-Services, Key Vault, die Überwachung des Security Centres, Backup und vieles mehr.

Die Synappx-Lösungen werden in sicheren Microsoft-Rechenzentren in Europa gehostet. Microsoft Azure Cloud und die Datenzentren werden durch die Sicherheitsrichtlinien von Microsoft geschützt. Jedes Datenzentrum bietet eine lokale Datenredundanz. Außerdem wird die gesamte Kommunikation zwischen den Anwendungen von Sharp Synappx und den Services der Synappx-Cloud (auf Microsoft Azure gehostet) über HTTPS (TLS v1.2, AES256) verschlüsselt und durch X.509-Zertifikate oder MQTT (von MFP und Display Agent genutzt) gesichert.

Der Zugriff auf alle Services der Synappx-Cloud durch Client-Anwendungen erfordert sichere Schlüssel, Zertifikate oder Authentifizierungs-Token. Nach dem Kauf von Synappx Service wird jedem Kunden ein eindeutiges Zertifikat für die Kommunikation zugewiesen. Dieses Zertifikat wird im Microsoft Key Vault gespeichert und garantiert einen sicheren Zugriff nur für diesen Kunden. Der Synappx-Azure-Datenbankzugriff ist auf IP-Adressen beschränkt, die in eine Whitelist auf sicheren Azure App Services eingetragen sind. Microsoft Key Vault wird für die Speicherung von SSL-Zertifikaten, X.509-Signaturzertifikaten, persönlichen Schlüsseln und weiteren Zertifikaten verwendet um die höchste Sicherheit zu gewährleisten. Der Zugriff auf Microsoft Azure Key Vault ist ausschließlich den Sharp-Servicemanagern und Systembenutzern vorbehalten, die über entsprechende Zugriffsberechtigungen verfügen.

Die kundenspezifischen Daten von Synappx Go und/oder Synappx Meeting, die in den sicheren Azure-Clouddatenbanken gespeichert werden, umfassen:

Synappx Meeting und Synappx Go

- Vorname, Nachname und E-Mail-Adresse des Benutzers (vom Administrator von Azure AD oder G Suite zu Synappx importiert)
- Vorname, Nachname und E-Mail-Adresse des Administrators (vom Administrator von Azure AD oder G Suite zu Synappx importiert)
- Namen, E-Mail-Adressen und Standorte der Workspaces (Meeting-Raum) vom Administrator von Microsoft Outlook oder dem G Suite Directory zu Synappx importiert.
- Manuell hinzugefügte Namen und Standorte der Workspaces
- Firmendomain-Aliasse von Azure AD und G Suite
- Nutzungsdaten der Anwendung zur Generierung von Berichten für den Administrator
- Synappx-Lizenzdaten (z. B. Ablaufdatum)
- Systemprotokolle

Speziell für Synappx Meeting:

- IP-Adresse und Port des Displays (falls von Admin konfiguriert)
- Optionale Konto-ID und Passwort des Displays (falls von Admin konfiguriert)
- Sendertyp, IP-Adresse und PIN des Castings (falls von Admin konfiguriert)
- Name des Meetings, tatsächliche Meeting-Dauer (Startzeit und Endzeit), Name des Meeting-Standorts, Name und E-Mail-Adresse des Teilnehmers

Speziell für Synappx Go:

- MFP-Informationen (Modellname, IP-Adresse, Seriennummer), abgerufen durch eine vom Administrator initiierte SNMP-Anfrage
- Informationen über den MFP-Agenten (Computername, Computerkennung, Versionsnummer, Update-Richtlinie, Datum der letzten Aktualisierung)
- Informationen über den Display-Agenten (Computername, Computerkennung, Versionsnummer, Update-Richtlinie, Datum der letzten Aktualisierung)
- Informationen über die NFC-Kennung (Kennungsnummer, Typ), die den vom Administrator konfigurierten Geräten zugewiesen sind

Die Daten in den Synappx-Datenbanken können nur von lizenzierten Kunden über die Synappx-Anwendungen und einer begrenzten Anzahl von Sharp-Mitarbeitern abgerufen werden, falls dies für Support-Zwecke erforderlich sein sollte.

Insgesamt beschränkt die Steuerung der Synappx-Clouddienste den Systemzugang auf ein Minimum an Mitarbeiter und gilt nur für Bereitstellungs- und Support-Zwecke. In den entsprechenden Abschnitten der Sharp-Sicherheitsrichtlinien finden Sie weitere Einzelheiten über dieses Thema.

Weitere Informationen über die Sicherheit von Microsoft Azure bezüglich der von den Synappx-Services genutzten Funktionen finden Sie über die folgenden Links:

- Übersicht: https://docs.microsoft.com/en-us/azure/security/security-white-papers
- Datenverschlüsselung im Ruhezustand: https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest
- Azure-Netzwerk-Sicherheit: https://docs.microsoft.com/en-us/azure/security/security-network-overview
- Azure-Funktionen und serverlose Plattform-Sicherheit: https://docs.microsoft.com/en-us/azure/security/abstract-serverless-platform-security
- Leitfaden zur Azure-Speichersicherheit: https://docs.microsoft.com/en-us/azure/security/security-storage-overview
- Sicherheitsmanagement in Azure: https://docs.microsoft.com/en-us/azure/security/azure-security-management
- Azure-Managementsteuerung: https://docs.microsoft.com/en-us/azure/governance/

4. Synappx Admin Portal

Die Administratoren (Admins) für Synappx Meeting und Synappx Go konfigurieren und verwalten das Synappx-System über die Webseiten des Synappx-Adminportals. Das Hinzufügen von Workspaces/Meeting-Räumen, Benutzern, Geräten, zusätzlichen Administratoren usw. erfolgt über diese sicheren Webseiten. Die Lizenzverwaltung erfolgt über das Admin-Portal und dort kann auch der Lizenz-Status abgerufen werden. Berichte helfen bei der Veranschaulichung der Synappx-Systemnutzung. Über diese Seiten kann bequem auf Downloads (für Synappx Go) zugegriffen werden und verschiedene Systemprotokolle stehen zum herunterladen bereit.

4.1 Zugriff und Anmeldung rollenbasierend (Für Admin Portal und Clients)

Der Zugriff auf das „Synappx Admin Portal“-System wird über mandantenbasierte und rollenbasierte Authentifizierungsprozesse gesteuert. Benutzer werden bei jedem Mandanten eingerichtet und mit einem bestimmten Kundenkonto und gemäß ihrer Benutzerrollen und Genehmigungen verbunden. Der eigentliche Administrator wird als Bestandteil des Auftragsvorgangs identifiziert. Nachdem sich der erste Administrator erfolgreich beim Synappx-Portal angemeldet hat, können weitere Administratoren hinzugefügt werden.

Nur Administratoren, die vom Kunden benannt oder zugewiesen wurden, können über das sichere Webportal auf ihr Konto zugreifen, es konfigurieren und lizenzieren, Benutzer und Workspaces des Synappx-Service verwalten, Berichte aufrufen usw. Jede Kommunikation mit dem Admin-Portal erfolgt über HTTPS/SSL (TLS1.2) Port 443, um die Daten bei der Übertragung zu schützen.

Synappx Meeting und Synappx Go nutzen die Anmeldedaten von Microsoft 365 oder G Suite der Administratoren und Benutzer, um zu vermeiden, dass eigene Synappx-Anmeldeinformationen eingerichtet, verwaltet und geschützt werden müssen. Standardmäßig haben die Synappx-Services keinen Zugriff auf die Kundenpasswörter von Microsoft 365 oder Google G Suite. Das System nutzt Azure Active Directory oder G Suite Directory und verlässt sich auf Authentifizierungs-Token, um Administratoren und Benutzer (für den Client-Zugriff) zu erkennen. Die Benutzeridentität wird mit Ihrem Microsoft Azure AD (bei Microsoft-365-Konten) oder G Suite Directory (bei G-Suite-Konten) bestätigt und dies erfolgt durch einen sicheren Identitätspartner Auth0 (Informationen dazu weiter unten). Außerdem werden Benutzer-Passwörter niemals in den in Synappx- oder Auth0-Systemen gespeichert. Auf der Synappx-Plattform wird nur die E-Mail-Adresse und der Vor-/Nachname des Benutzers sicher gespeichert. Auf dem Synappx-System werden keine anderen persönlich identifizierbaren Informationen über den Benutzer gespeichert.

4.2 Auth0 (Identity Service Provider)

Bei den Synappx-Services arbeitet Sharp mit Auth0 (https://auth0.com/), um für Microsoft Azure AD und G Suite sichere Identitätsservices zu bieten. Auth0 hat laut eigenen Aussagen 21 Millionen Nutzer in 120.000 Anwendungen mit 2,5 Milliarden Anmeldungen pro Monat. Auth0 ist ein sehr angesehener Identitätsdienstleister.

Nachfolgend ist eine Übersicht über den Prozess:

1. Der Administrator oder Benutzer gibt die Anmeldedaten von Microsoft 365 oder G Suite über ein Fenster ein, wenn er sich beim Synappx-Adminportal oder einem beliebigen Synappx-Client anmeldet.

2. Auth0 delegiert die Authentifizierung des Benutzernamens und des Passworts über SSL/TLS 1.2 (Port 443) an Azure AD oder G Suite, die wiederum die Benutzername- und Passwort-Anmeldedaten validieren.

3. Auth0 kennt und speichert das Benutzer-Passwort nicht.

4. In Zusammenarbeit mit Azure AD oder G Suite wird ein sicherer JSON Web Token (JWT) zurück an den Browser (für den Zugang zum Synappx Admin Portal), mobile Geräte (bei Synappx Go und Synappx Meeting) und/oder an Windows-/Mac-Clients geschickt (bei Synappx Meeting).

5. Mit diesem Token kann die Anwendung Funktionen ausführen, ohne dass sich der Benutzer jedes Mal anmelden muss, wenn er die Anwendungen benutzen will (außer in Fällen, bei denen die Anmeldedaten geändert werden; z. B. das Passwort muss erneut eingegeben werden, Benutzer ist nicht mehr gültig, der Benutzer meldet sich aus der mobilen App ab oder ist 30 Tage inaktiv). Niemand kann den JWT-Token ohne den zugehörigen Geheimschlüssel manipulieren, der für die Anmeldung benutzt wird, und dieser Geheimschlüssel wird sicher in der Cloud gespeichert.

Es stehen mehrere Ebenen des Authentifizierungsschutzes zur Verfügung. Das mobile Gerät oder der Computer des Benutzers wird durch ein Passwort oder eine biometrische Anmeldung (z. B. Fingerabdruck oder Gesicht) geschützt. Benutzer-Passwörter sind den Synappx-Geräten nicht bekannt und werden nicht auf ihnen gespeichert, und die sicheren Token, die von Auth0 bereitgestellt werden, basieren auf sicheren Token und der Validierung durch Microsoft Azure oder G Suite.

Auth0 verfügt über zahlreiche Zertifizierungen für die Cloud-Sicherheit, wie etwa: ISO27001, ISO27018, SOC 2 Type II, HIPAA BAA, EU-US Privacy Shield Framework, Gold CSA STAR, DSGVO-Konformität und mehr. In den folgenden Auth0-Whitepapers finden Sie weitere Informationen über die Auth0-Sicherheitsbestimmungen:

- https://auth0.com/security/

- https://assets.ctfassets.net/kbkgmx9upatd/2KxmM5BICQ4GKgeIwA0sKu/bee69c73669bfdeb26ca8e43df65be27/Auth0_Platform_Operations.pdf

4.3 Gewähren der Privilegien für die Synappx-Anwendung

Um die Funktionen von Synappx Meeting und Synappx Go zu ermöglichen, muss der Administrator der Synappx-Anwendung die vom Benutzer ausgewählten Privilegien gewähren. Der erste Administrator, der sich beim System anmeldet, muss Admininstratorenrechte für Azure AD oder G Suite besitzen und im Namen der Organisation den geforderten Berechtigungen für Benutzer zustimmen, wenn auf die Synappx-Anwendungen/Services zugegriffen wird.

Die Berechtigungen und Gründe für Kunden von Microsoft 365 lauten:

Berechtigungen beantragt	Definition	Admin-Portal	Synappx Meeting	Synappx Go
Azure Active Directory Graph:				
User.Read	Erlaubt dem Benutzer, sich bei der App anzumelden, und gibt der App die Berechtigung, das Profil der angemeldeten Benutzer zu lesen. Außerdem wird der App dadurch gestattet, grundlegende Unternehmensinformationen von angemeldeten Benutzern zu lesen.	Ja	Ja	Ja
Directory.Read.All	Gestattet der App, Domain-Aliase von Azure AD zu lesen (für domainübergreifenden Support benötigt) und gestattet der App, Daten in Azure AD zu lesen, wie etwa Benutzer, Gruppen und Apps.	Ja	Nein	Nein
Microsoft Graph:				
Calendars.ReadWrite. Shared	Gestattet der App, Ereignisse in allen Kalendern zu erstellen, zu lesen, zu aktualisieren und zu löschen, bei denen der Benutzer eine Zugriffsberechtigung hat. Dies umfasst delegierte und geteilte Kalender.	Nein	Ja	Nein
Files.ReadWrite.All	Gestattet der App, alle Dateien zu lesen, zu erstellen, zu aktualisieren und zu löschen, auf die der angemeldete Benutzer zugreifen kann.	Nein	Ja	Nein
Group.Read.All	Gestattet der App die Auflistung von Gruppen und das Lesen ihrer Eigenschaften und aller Gruppenmitgliedschaften im Namen des angemeldeten Benutzers. Gestattet der App außerdem, Kalender, Gespräche, Dateien und andere Gruppeninhalte für alle Gruppen zu lesen, für die der Benutzer eine Zugriffsberechtigung besitzt.	Ja	Nein	Nein
User.Read.All	Gestattet der App, im Namen des angemeldeten Benutzers den vollständigen Satz von Profileigenschaften, Berichten und Managern anderer Benutzer in Ihrer Organisation zu lesen.	Ja	Ja	Nein
offline_access	Gestattet der App das Lesen und Aktualisieren von Benutzerdaten, selbst wenn sie die App derzeit nicht benutzen.	Ja	Ja	Ja
E-Mail	Gestattet der App das Lesen der primären E-Mail-Adresse Ihrer Benutzer.	Ja	Ja	Ja
openid	Gestattet den Benutzern die Anmeldung in der App mit ihren Firmen- oder Schulkonten und gestattet der App, grundlegende Profilinformationen des Benutzers aufzurufen.	Ja	Ja	Ja
profile	Erforderlich, um Profilinformationen des Benutzers von Azure AD abzurufen (z. B. Vor- und Nachname und die E-Mail-Adresse des Benutzers).	Ja	Ja	Ja

Bei G-Suite-Kunden umfasst folgende Liste die erforderlichen API-Geltungsbereiche und den Grund für die einzelnen Punkte:

Angeforderte Google-API-Geltungsbereiche	Definition	Admin-Portal	Synappx Meeting	Synappx Go
https://www.googleapis.com/auth/admin.directory.domain.readonly	Gestattet der App, Domain-Informationen zu lesen, um eine domainübergreifende Funktion zu unterstützen.	Ja	Nein	Nein
https://www.googleapis.com/auth/admin.directory.group.readonly	Gestattet der App, Gruppe, Gruppenalias und Mitgliedsinformationen abzurufen, um Gruppen über das Admin-Portal hinzuzufügen.	Ja	Nein	Nein
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly	Gestattet der App, Kalender-Ressourcen abzurufen, um Workspaces über das Admin-Portal hinzuzufügen.	Ja	Nein	Nein
https://www.googleapis.com/auth/admin.directory.user.readonly	Gestattet der App, Benutzer oder Benutzer-Aliasse abzurufen, um Benutzer über das Admin-Portal hinzuzufügen.	Ja	Nein	Nein
https://www.googleapis.com/auth/calendar.readonly	Gestattet der App den ausschließlichen Lesezugriff auf Kalender.	Nein	Ja	Nein
https://www.googleapis.com/auth/calendar.events	Gestattet der App den Lese-/Schreibzugriff auf Ereignisse eines Kalenders und die Aktualisierung eines Kalenders (z. B. ein Verlängern der Meeting-Dauer).	Nein	Ja	Nein
https://www.googleapis.com/auth/drive	Gestattet der App den Zugriff auf autorisierte Google-Drive-Dateien (außer dem Anwendungsdaten-Ordner), um Dateien aufzulisten.	Nein	Ja	Nein
https://www.googleapis.com/auth/drive.file	Gestattet der App den Zugriff auf Dateien, die von der App zum Herunterladen und Hochladen erstellt oder geöffnet wurden. Die Dateiautorisierung wird pro Benutzer erteilt und widerrufen, wenn der Benutzer die Autorisierung der App widerruft.	Nein	Ja	Nein
https://www.googleapis.com/auth/userinfo.profile	Gestattet der App die Nutzung personenbezogener Daten, die der Benutzer öffentlich zur Verfügung gestellt hat, um den Benutzernamen und das Avatarbild zu erhalten.	Nein	Ja	Ja

4.4 Importieren der User oder Workspaces von Azure AD oder G Suite

Synappx Go lizenziert den Service auf Benutzerbasis, während Synappx Meeting auf Grundlage der Workspaces/Meeting-Räume lizenziert. Administratoren können Zeit sparen und Schreibfehler minimieren, indem sie Benutzer (bei Synappx Go) und Workspaces (z. B. Räume) direkt für beide Anwendungen aus Microsoft 365 (Azure AD) oder G Suite importieren. Es steht auch eine manuelle Eingabe von Workspaces zur Verfügung. Nur Benutzer in den unterstützten Domains und in Azure AD oder G Suite können als lizenzierte Synappx-Go-Benutzer hinzugefügt werden. Die Kommunikation mit Microsoft Azure und G Suite für den Benutzer- und/oder Workspace-Import erfolgt per HTTPS (Port 443).

4.5 Synappx Go Agent – Downloads

Der Synappx Go MFP und die Display Agents können von der Downloads-Seite des Synappx Admin Portal heruntergeladen werden. Die heruntergeladenen Agenten stehen nicht auf öffentlichen Websites zur Verfügung. Sie können nur von autorisierten Synappx-Administratoren heruntergeladen werden. Mit der ZIP-Datei, welche die benutzerspezifische Daten und die vom Kunden eingegebenen Daten enthält, um (für den MFP-Agenten) die automatische MFP-Erkennung über SNMP zu ermöglichen, ist eine verschlüsselte Konfigurationsdatei (SHA-256) gepackt. Weitere Einzelheiten über die agentenbezogene Sicherheit finden Sie im Abschnitt „Synappx Go Agents“.

4.6 Synappx – Berichte

Synappx Meeting und Synappx Go bieten Berichte, um den Administratoren die Benutzung und den Wert der Synappx-Anwendung näherzubringen. Die Daten, aus denen die Synappx-Berichte generiert werden, sind auf sicheren Microsoft-Servern gespeichert. Nachdem der Kunde den Service gekündigt hat, werden die Daten bis zu 45 Tage lang gespeichert (um ein Zeitfenster zu lassen, falls die Lizenz verlängert werden soll). Die benutzerspezifischen Daten in den Berichten stehen nur den Administratoren innerhalb des Unternehmens über die Berichtsseiten zur Verfügung. Anonymisiert zusammengefasste Daten über die Anwendungsnutzung durch den Kunden stehen für Sharp zur Verfügung, um im Laufe der Zeit Support und Produktverbesserungen anzubieten. Weitere Informationen hierzu finden Sie unter den Abschnitten, die sich mit den Themen Sharp-Unternehmenssicherheit, Sharp-Admin-Datenzugriff und Sharp-Datenschutzrichtlinie befassen.

4.7 Synappx – Unterstützte Domains

Bei Microsoft-365-Konten und G Suite sammelt Synappx Informationen zu den Domain-Aliases, die im Azure-AD- oder G-Suite-System des Kontos unterstützt werden. Bei Microsoft-365-Konten können Administratoren auf der Webseite der Admin-Einstellungen/unterstützen Domains nach der ersten Anmeldegenehmigung zusätzliche Domain-Aliase über die Azure-AD-Domain hinaus auswählen, unter der das Synappx-Konto erstellt wurde. So können Benutzer und Workspaces von ausgewählten Domains importiert werden, um sie mit den Synappx-Services zu nutzen.

4.8 Synappx – Systemprotokolle

Synappx Go und Synappx Meeting umfassen ein Systemprotokoll mit Informationen über Systemereignisse, die potentiell für Administratoren von Interesse sind. Dazu gehören Situation, die eine Administrator-Intervention erfordern könnten, um ein Problem zu beheben oder eine Fehlerbehebung durchzuführen. Die Administratoren können die Systemprotokolle zur weiteren Analyse als .CSV-Datei exportieren. Die Systemprotokolle werden vom Synappx-System 30 Tage lang gespeichert.

5. Clients für Windows und Apple Mac für Synappx Meeting

Synappx Meeting hilft bei der Verbindung des Displays im Meeting-Raum, dem Starten einer Web-Konferenz und der Steuerung von Anwendungen durch einfache Sprachbefehle*. Es wird eine breite Palette von Sicherheitsmerkmalen bereitgestellt, unter anderem:

- Der gesamte Client-Zugriff von Synappx Meeting auf Cloud-Ressourcen erfolgt über HTTPS (Port 443)
  - Azure (ruft Informationen über den Meeting-Raum von Synappx Admin ab)
  - Auth0 (Übertragung der Benutzerauthentifizierung auf Azure AD)
  - Azure AD (Benutzerauthentifizierung mit dem Microsoft-365-Konto) oder G Suite (Benutzerauthentifizierung mit dem G-Suite-Konto)
  - Microsoft Graph APIs (ruft Meeting-Informationen und Dateien für ein Meeting von Microsoft Office 365 ab) oder Google API Scopes (ruft Meeting-Informationen und Dateien für ein Meeting von G Suite ab)
  - Amazon Web Services für Warteschlangenzugriff für Sprachbefehle*

- Zugriff auf das lokale Display
  - Ermöglicht die Steuerung von interaktiven Anzeigesystemen BIG PAD per Sprachsteuerung*. Das Protokoll ist Telnet (Port 10008)

- Der Benutzer authentifiziert sich bei der ersten Nutzung der Synappx-App mit Microsoft-365- oder G-Suite-Passwörtern, und wenn es Änderungen an den Anmeldedaten (z. B. eine Aktualisierung des Passworts) gibt oder die App 3 Tage lang nicht benutzt wird, erfolgt eine Abmeldung von der Client-App.

- Die Benutzerpasswörter werden nicht auf dem mobilen Gerät gespeichert; stattdessen wird nach der Benutzerpasswort-Authentifizierung mit dem Azure-AD- oder G-Suite-System über eine Partner-Auth0 ein sicherer JWT-Token bereitgestellt.
  - Der Token für den Benutzerzugriff wird auf dem lokalen Computer gespeichert
  - ID/Passwort für Proxy werden auf dem lokalen Speicher gespeichert. (verschlüsselt mit AES128)

* Die Sprachsteuerung ist momentan in Europa nicht verfügbar.

6. Synappx Go und Synappx Meeting Mobile

Mit der zunehmenden Nutzung mobiler Geräte im Geschäftsleben werden Smartphones inzwischen häufig verwendet, um auf Unternehmensinhalte zuzugreifen und sie freizugeben. Benutzer erwarten intuitive mobile Dienste, mit denen sie ihre Arbeit schneller erledigen können. Mit der mobilen App „Synappx Go" können die Benutzer zu häufig genutzten Zielen scannen, auf einem beliebigen mit Synappx Go konfigurierten Gerät eine Druckfreigabe erteilen oder unterstützte Cloud-Dateien drucken sowie Cloud-Dateien mit konfigurierten Sharp-Displays teilen. Mit der mobilen App „Synappx Meeting" können die Benutzer Ihr Meeting beginnen, Web-Konferenzen starten und schnell auf Dokumente zugreifen. Hier sind einige Sicherheitsmerkmale, die mit den mobilen Clients verbunden sind:

Synappx Meeting und Synappx Go:

- Ein mobiles Gerät erfordert die Eingabe von Benutzerpasswörtern oder einer biometrischen Authentifizierung (z. B. Fingerabdruck, Gesichtserkennung) für den App-Zugriff.

- Die Benutzer authentifizieren sich bei der ersten Nutzung der Synappx-App mit Microsoft-365- oder G-Suite-Anmeldedaten, und wenn es Änderungen an den Anmeldedaten (z. B. eine Aktualisierung des Passworts) gibt oder die App 30 Tage lang oder länger nicht benutzt wird, erfolgt eine Abmeldung von der mobilen App.
  Nutzungen:
  - Auth0 (Übertragung der Benutzerauthentifizierung auf Azure AD)
  - Azure AD (Benutzerauthentifizierung mit dem Microsoft-365-Konto) oder G Suite (Benutzerauthentifizierung mit dem G-Suite-Konto)
- Die Benutzerpasswörter werden nicht auf dem mobilen Gerät gespeichert; stattdessen wird nach der Benutzerpasswort-Authentifizierung mit dem Azure-AD- oder G-Suite-System über eine Partner-Auth0 ein sicherer JWT-Token bereitgestellt.

- Der gesamte Zugriff auf das System wird mit TLS v1.2 AES256 (Port 443) verschlüsselt

Speziell für Synappx Go:

- Der mobile Benutzerzugriff wird zentral über das Synappx Admin Portal gesteuert. Admins können eine Benutzerlizenz jederzeit entfernen, um die folgende Nutzung der mobilen Funktionen von Synappx Go zu sperren.

- Die Benutzer werden aufgefordert, den Zugriff auf ihre mobile Kontaktliste zu gewähren, um das Scannen an E-Mail-Ziele zu ermöglichen, ohne dass Sie die Benutzer-E-Mails des Ziels erneut eingeben müssen. Dies spart Zeit und minimiert Schreibfehler.

- Für einen Scan in einen Ordner eines Cloudspeichers, das Drucken ausgewählter Cloud-Dateien oder das Teilen von Cloud-Dateien mit Sharp-Displays können die Benutzer Synappx Go so konfigurieren, um auf Dateien von unterstützten Cloudspeicher-Sites zuzugreifen (One Drive for Business, One Drive, SharePoint Online, Dropbox, Box oder Google Drive). Bei der iOS-App sind die iCloud und die lokalen Dateien bereits konfiguriert.

  - Bei favorisierten Speicherorten können die Benutzer ihren Benutzernamen und ihr Passwort eingeben, die mit den Cloudspeicher validiert werden. Nach der Validierung wird ein sicherer Token bereitgestellt und in Synappx Go Mobile gespeichert, damit der Benutzer diese Anmeldedaten nicht erneut eingeben muss, außer sie sind nicht mehr gültig (z. B. Passwort-Änderung, Konto-Deaktivierung usw.)
  - Sharp- und Komponenten-Lieferanten haben keinen Zugriff auf die Passwörter der Cloudspeicher des Benutzers.
  - Für jeden Cloudspeicher-Service wird der Benutzer aufgefordert, der Synappx-App ausgewählte Berechtigungen zu erteilen, damit auf die Dateien, die der Benutzer auf ein Display herunterladen und bearbeiten möchte, zugegriffen werden kann und dass diese aktualisiert werden können. Hinweis: Der Synappx-Go-Service verfügt über keine Funktion, um Dateien oder Ordner aus einer Cloudspeicher zu löschen.
  - Hinweis: Sharp ist eine Partnerschaft mit einem Anbieter von Drittanbietern, Kloudless (Kloudless.com) eingegangen, um effiziente Verbindungen von Synappx Go mit mehreren Anbietern von Cloud-Speichern zu unterstützen. Kloudless hat keinen Zugriff auf Benutzerpasswörter. Seine sichere Datenbank umfasst Benutzer-E-Mail-Adressen von Synappx Go. Kloudless speichert die geringstmögliche Anzahl von Datei-/ Ordner-Metadaten (z. B. Dateiname und ID, Änderungsdatum), um die Ansicht kürzlich modifizierter Daten aus der Cloud zu nutzen. Kloudless speichert keine Benutzer-Dateiinhalte.

Speziell für Synappx Meeting:

- Mobile Apps stehen jedem Benutzer des Service zur Verfügung (keine Lizenz erforderlich); der Benutzer muss allerdings in der gleichen Kunden-Domain ein validierter Nutzer in Azure AD oder G Suite sein.
- Von Synappx Admin wird auf Azure-Meeting-Raumdaten zugegriffen
- Microsoft Graph API erhält von Microsoft Office 365 Meeting-Informationen und Dateien für das Meeting. Google-API-Geltungsbereiche erhalten von G Suite Informationen und Dateien für das Meeting.

7. Synappx Go – NFC-Tags

Synappx Go nutzt spezielle von Sharp oder autorisierten Vertriebspartnern bereitgestellte und/oder in ausgewählte MFP-Modelle eingebettete NFC-Tags. Die Tags enthalten eine eindeutige Identifikation und sind nur mit einem Lesezugriff ausgestattet (sie können nicht umprogrammiert werden). Jeder Tag kann gleichzeitig immer nur einem Gerät zugeordnet sein. Nach der Konfiguration auf einem Gerät (z.B. MFP oder Display-PC) durch den Administrator über die Synappx Go-Mobilanwendung, kann der Benutzer auf die NFC Taste im App drücken. Das Tag und die mobile Anwendung identifizieren zusammen die Benutzeridentität und das mit dem Tag vebundene Gerät. Sie können somit Scannen, einen Druckauftrag freigeben, Cloud-Dateien drucken oder die Cloud-Datei auf einem Display wiedergeben.

8. Synappx Go MFP Agent

Der Synappx Go MFP Agent (inklusive Druckfreigabe-Software) ist eine Vor-Ort-Komponente des Synappx-Go-Systems, die auf einem Kunden-PC oder Kunden-Server installiert ist, um die Kommunikation zwischen Synappx-Go-fähigen MFPs und der Synappx Go Cloud zu erleichtern. Es ermöglicht mobile und NFC-basierte Anwendungen im Zusammenhang mit Sharp MFPs. Mit Synappx Go müssen Sie nicht mehr das Bedienpanel des MFPs kennen, um Druckaufträge freizugeben, ausgewählte Cloud-Dateien zu drucken oder Dateien an bevorzugte Scan-Ziele zu senden. Die Benutzer sparen Zeit beim Scannen und sicheren Drucken und außerdem wird das Risiko verringert, dass unbefugt auf die Druckaufträge des Benutzers zugegriffen wird.

Der MFP-Agent von Synappx Go wird benötigt, um Scan- und Druckaufträge auszulösen. Eine der wichtigsten Funktionen des Agenten ist der Aufbau eines sicheren Kommunikationskanals zur Synappx-Cloud. Der Agent verbindet sich mit der Cloud, um die Datenkommunikationen zu registrieren und abzusichern und um Nachrichten an den Agenten und die unterstützten MFPs zu senden und von ihnen zu erhalten. Jeder Agent verfügt über eine einzigartige Kennung und diese wird vom Cloud-System von Synappx Go zur Erkennung genutzt, an welchen Agenten Nachrichten geschickt werden sollen. Die Agenten warten auf Nachrichten, indem sie ihr eindeutige Kennung abonnieren, und die Cloud-Dienste versenden eine Nachricht durch eine Veröffentlichung bei von dieser Kennung.

8.1 MFP-Agent – Installation

Zur Installation des MFP Agents wird das benutzerdefinierte Installationspaket vom Admin-Portal von Synappx Go heruntergeladen, zusammen mit einer für den Kunden einzigartigen Konfigurationsdatei. Die Inhalte der Konfigurationsdatei werden über Verschlüsselungsalgorithmen gesichert. Dieses Installationspaket des MFP Agents steht nicht über eine öffentliche Website zur Verfügung und ist an das spezifische Kundenkonto gebunden. Bei den meisten Kundeninstallationen wird pro Kundenstandort ein MFP Agent installiert, der maximal 50 bis 100 MFPs unterstützt (je nach Anzahl der Benutzer und Druckaufträge), welche die Druck- und Scanfunktionen von Synappx Go nutzen können. Kunden, die mehr als 100 MFPs unterstützen möchten, müssen einen oder mehrere zusätzliche MFP-Agenten installieren.

Nach der Installation sendet der MFP-Agent zur Registrierung seine einzigartige Kennung zusammen mit Agenten-Sicherheitsanmeldedaten an die Synappx Go Cloud, um sich im Geräteverzeichnis zu registrieren. Die im Geräteverzeichnis gespeicherten Informationen umfassen Daten wie beispielsweise die Gerätekennung, den Standort, die Mandantenkennung und bei MFPs den mit dem MFP verbundenen MFP-Agenten.

8.2 MFP-Agent – Kommunikation

Die gesamte Kommunikation zwischen dem Synappx Go MFP Agent und der Synappx Go Cloud nutzt entweder HTTPS (Port 443) oder X.509 Client-Sicherheit über MQTT. HTTPS wird bei Erstinstallation-Kommunikationen zwischen dem Synappx Go MFP Agent und der Synappx Go Cloud, genutzt – sowie zum Senden der MFP-Informationen und aller Fehlerinformationen.

- Die privaten X.509-Agentenschlüssel verlassen niemals das System, auf dem der Agent installiert ist und werden daher niemals durch eine Übermittlung über das Internet gefährdet.

- Alle X.509-Agentenzertifikate werden mit den Signierungszertifikaten des Kunden unterzeichnet. Agenten erhalten nur eine Erlaubnis zur automatischen Registrierung, wenn das X.509-Zertifikat von seinem zugehörigen Kunden unterzeichnet wird, der das Zertifikat unterzeichnet.

Die Cloud-Services von Synappx Go verwalten eigene Signierungszertifikate für jeden Kunden von Synappx Go. Dies garantiert, dass Agenten nur innerhalb ihres verbundenen Mandanten-Verzeichnisses bereitgestellt werden.

Nach der automatischen Bereitstellung des Agenten für die Synappx Go Cloud inklusive der X.509-Zertifizierungen, erfolgt die Kommunikation zwischen dem Agenten und der Cloud über sichere MQTT-Verbindungen. Es werden Sharp Synappx Go X.509-RootCA-signierte Zertifikate genutzt. Die RootCA-unterzeichneten Zertifikate stellen ein zusätzliches Zertifizierungsniveau zur Verfügung, das beglaubigt, dass es sich um den Zertifikatsinhaber handelt. Die Verwendung von X.509-Zertifikaten bietet die höchste Sicherheit bei der Geräteauthentifizierung, denn der private Schlüssel eines jeden Agenten-Geräts verlässt niemals das Gerät und wird daher unmöglich gefährdet. Das Root-CA-Signierungszertifikat von Synappx Go Agent wird vom Synappx Go Tenant Provisioning Service generiert und im Azure Key Vault gespeichert.

- Vorteile von MQTT- und X.509-Zertifikaten sind unter anderem, dass sich die Agenten nur bei ihrem eigenen einzigartigen Gerätekennung anmelden dürfen; das bedeutet, dass Synappx-Go-Agenten NUR Nachrichten an ihre jeweilige Gerätekennung erhalten. Der Agent kann keine Inhalte von einem anderen Endpunkt erhalten.

8.3 MFP-Agent – Anforderungen

Der Synappx Go Agent wurde mit folgenden Anforderungen von der Azure-Cloud entworfen:

- Ehe sich ein Gerät mit der Azure-Cloud verbinden kann, MUSS das Gerät registriert werden
- Ehe ein Gerät registriert werden kann, MUSS das Gerät (von einem Kunden-Administrator) bereitgestellt werden
- Ehe ein Gerät bereitgestellt werden kann, MUSS das Gerät (über das System) über Sicherheitszertifikate verfügen

8.4 MFP-Agent – Geräteerkennung

Um die Sammlung von MFP-Informationen zu automatisieren (erforderlich, um die MFP-Services von Synappx Go zu konfigurieren), besitzt der MFP-Agent die Funktion, MFPs mit SNMP-Erkennung zu finden. Die Erkennung wird nach der Installation des ersten Agenten automatisch initiiert. Der Administrator gibt für die Suche den Anfang und das Ende des IP-Bereichs über das Admin-Portal ein und kann zudem bei Bedarf über Port 443 eine erneute Suche durchführen (auch vom Administrator über die Admin-Konsole initiiert). Bei diesem Vorgang werden folgende Informationen über den MFP gesammelt und an die Synappx Go Cloud gesendet:

- Kennung des MFP Agent, die vom System erstellte MFP-Kennung (z. B. Sharp MX-C301W 63004882), Hersteller, Modellname, Seriennummer, Gerätename (falls eingestellt), Standort (falls eingestellt), Netzwerk-IP-Adresse

8.5 MFP-Agent – Druckfreigabe und Scannen von Dokumenten

Ein Admin oder Benutzer kann einen Sharp-Druckertreiber konfigurieren, um auf einen Synappx Go Agent/Druckfreigabe-PC oder Server zu verweisen. Wenn Aufträge an den Treiber der Druckfreigabe gesendet werden, werden lizenzierte Druckdateien des Benutzers von Synappx Go User für jeden Benutzer automatisch in einem Ordner auf dem Agent-PC/Agent-Server gespeichert, um vom Benutzer auf jedem mit einer Synappx-Kennung konfigurierten MFP freigegeben zu werden.

- Die auf dem Server gespeicherten Druckdateien (im Format .PRN) werden nach 24 Stunden automatisch gelöscht.
- Die .PRN-Dateien können nur von autorisierten Administratoren abgerufen werden, die über einen normalen PC-/Server-Passwortschutz auf den Computer zugreifen können.

Die Auswirkungen auf das Kundennetzwerk beziehen sich auf die Verwendung des Scan- und Druckeinsatzes des Benutzers von Synappx Go. Zu den geschätzten Auswirkungen zählen:

- Scannen zu den beliebtesten Zielen (pro Benutzer) – geschätzt durchschnittlich 1 MB pro Scan (kann variieren)
- Sicheres Drucken (pro Benutzer pro Druckauftrag) – geschätzt durchschnittlich 1,2 MB pro Druckauftrag (kann variieren)
- Drucken einer Cloud-Datei (pro Benutzer pro Druckauftrag) – geschätzt durchschnittlich 1,2 MB pro Druckauftrag (kann variieren)

9.Synappx Go Display Agent

Der Synappx Go Display Agent ist eine Vor-Ort-Komponente des Synappx-Go-Systems, die auf einem Kunden-Display-PC oder Server installiert ist, und die Kommunikation zwischen Synappx-Go-fähigen PCs und der Synappx Go Cloud ermöglicht - dies erlaubt das mobile Teilen und das NFC-Teilen auf Sharp-Displays. Synappx Go ermöglicht dem Benutzer die einfache einmalige Einrichtung von Verbindungen zu allen beliebten Cloudspeicher und das Auffinden der übergreifenden Datei(en), um sie auf Sharp-Displays zu teilen und/oder zu bearbeiten (bei den meisten Cloudspeicher) – alles über das mobile Gerät und mit einem einfachen NFC-Tippen, um die Dateien herunterzuladen. Die Benutzer sparen Zeit, die sie besser für die Zusammenarbeit rund um den Dateiinhalt nutzen können, und außerdem wird das Risiko verringert, dass andere Teilnehmer des Meetings die Namen von sensiblen Dateien sehen, die sich ebenfalls in den Cloud-Ordnern befinden. Zudem können Dateien (in den meisten Fällen) von mehreren Benutzern auf dem gleichen Display-PC heruntergeladen und bearbeitet werden, um den Dateiinhalt gemeinsam zu editieren und zu vergleichen.

9.1 Display-Agent – Installation

Um „Share to Display“-Anwendungen zu ermöglichen, muss der Synappx Display Agent auf einem Windows PC oder einem Server installiert werden. Eine wichtige Funktionen des Agenten ist der Aufbau eines sicheren Kommunikationskanals zur Synappx-Cloud.

- Der Agent verbindet sich mit der Cloud, um die Datenkommunikationen zu registrieren und abzusichern und um Nachrichten an den Agenten zu senden und von ihnen zu erhalten. Jeder Agent verfügt über eine einzigartige Kennung und diese wird vom Cloud-System von Synappx Go zur Erkennung genutzt, welchen Agenten Nachrichten geschickt werden sollen.
- Die Agenten warten auf Nachrichten, indem sie ihr eindeutiges Kennung abonnieren, und die Cloud-Dienste versenden Nachrichten durch eine Veröffentlichung bei diesem Kennung.

Zur Installation des Display Agent wird das benutzerdefinierte Installationspaket vom Admin-Portal von Synappx Go heruntergeladen, zusammen mit einer für den Kunden einzigartigen Konfigurationsdatei. Dieses Display-Installationspaket steht nicht über eine öffentliche Website zur Verfügung und ist an das spezifische Kundenkonto gebunden. Nach der Installation sendet der Display-Agent zur Registrierung seine einzigartige Kennung zusammen mit Agenten-Sicherheitsanmeldedaten an die Synappx Go Cloud, um sich im Geräteverzeichnis zu registrieren. Zu den Informationen, die in der Geräteregistrierung gespeichert werden, gehören Daten wie PC-/Servername, eindeutige PC-/Server-Kennung und Mandantenkennung.

9.2 Display-Agent – Kommunikation

Die gesamte Kommunikation zwischen dem Synappx Go Display Agent und der Synappx Go Cloud nutzt entweder HTTPS (Port 443) oder X.509 Client-Sicherheit über MQTT. HTTPS wird bei Erstinstallation-Kommunikationen zwischen dem Synappx Go Display Agent und der Synappx Go Cloud, genutzt – sowie zum Senden von Fehlerinformationen.

- Informieren Sie sich im obigen Abschnitt des MFP Agent über X509 und andere Kommunikationsdetails. Der Display Agent hat die gleichen Sicherheitsfunktionen wir der hier beschriebene MFP Agent.

9.3 Display Agent – Teilen von Inhalten

Für den Display Agent sind die folgenden zusätzlichen Sicherheitsfunktionen für „Share to Display“ implementiert:

- Sobald der Benutzer die gewünschten Cloudspeicher über sein mobiles Gerät konfiguriert hat (z. B. SharePoint Online, Dropbox), werden die sicheren Benutzer-Token vorübergehend mit einem sicheren Synappx-Cloud-Cache geteilt, wenn der Benutzer auf die „Share to Display“-Funktion zugreift. Auf den Cache kann nur mit sicheren Schlüsseln zugegriffen werden. Das Benutzer-Token wird kurze Zeit nach der Benutzung aus der Sharp-Synappx-Cloud entfernt und das Benutzer-Token wird niemals auf die Display Agents heruntergeladen.

- Wenn ein Benutzer eine Datei/mehrere Dateien über die Synappx-Go-Anwendung aus seiner Cloudspeicher für den Download auf den Display PC auswählt, generiert die Synappx Cloud eine Download-URL mit einer Sitzungskennung, um die ausgewählte(n) Benutzer-Datei(en) anzurufen. Die Dateien werden automatisch auf dem Display Agent PC geöffnet, um sie anzusehen und/oder zu bearbeiten (für die meisten Cloudspeicher). Die Dateien werden auf dem Display PC in einem temporären Ordner gespeichert.

    - Dateien, die über den Synappx-Go-Service zur Ansicht oder Bearbeitung heruntergeladen werden können, sind auf folgende Formate beschränkt:
        - Einfacher Text, Microsoft-Office-Dateien (Word, PowerPoint, Excel, OneNote), PDF, Bilddateien (JPEG, TIFF, GIF, BMP, PNG) und Videodateien (MP4, AVI, WMV, MOV)
        - Hinweis: Ausführbare Dateien oder Script-Dateien werden nicht unterstützt und können über diesen Service nicht heruntergeladen werden.

    - Dateien, die über den Synappx-Go-Service nur zur Ansicht heruntergeladen werden können, sind auf folgende Formate beschränkt:
        - Für iOS-, iCloud- und Local-Files-Speicher: gleiche Dateiliste wie oben
        - Für auf Google Drive gespeicherte G-Suite-Dateien: Google Docs, Google Slides, Google Sheets, Google Drawing, Google Jamboard
        - Hinweis: Ausführbare Dateien oder Script-Dateien werden nicht unterstützt und können über diesen Service nicht heruntergeladen werden.

    - Wenn der Benutzer eine editierbare Datei speichern möchte, nachdem er Änderungen auf dem Display PC vorgenommen hat, wird sie wieder am gleichen Speicherort des Cloud-Ordners gespeichert, von dem sie heruntergeladen wurde, entweder als neue Version und/oder mit einem angehängten Dateinamen (entsprechend den Richtlinien der jeweiligen Cloudspeicher).

    - Wenn ein Benutzer eine editierbare Datei wieder in der Cloud speichert oder eine Datei ohne zu speichern schließt, wird sie aus dem temporären Ordner des Display PCs entfernt.

    - Mehrere Benutzer mit Synappx-Go-Lizenzen/-Apps können jeweils Cloud-Dateien zum gleichen Display Agent herunterladen, um sie anzusehen, zu kopieren und editierbare Inhalte einzufügen und Dateien zu vergleichen, bevor diese wieder auf der jeweiligen Cloud gespeichert werden.

10. Unternehmenssicherheit

Sharp bietet ein zuverlässiges Programm zur Informationssicherheit, um die Vertraulichkeit, Integrität und Verfügbarkeit aller verarbeiteten und/oder auf den Geschäftssystemen von Sharp gespeicherten Informationsgüter zu schützen. Das Management von Sharp ist sich der sich rasch entwickelnden und wachsenden Risiken bewusst, die mit dem Schutz der Informationsgüter von Sharp und unserer geschätzten Geschäftspartner verbunden sind, und erforscht, prüft und investiert regelmäßig in prozedurale und technische Gegenmaßnahmen, um die Zuverlässigkeit und Sicherheit zu gewährleisten. Ein Team von engagierten Fachleuten bewertet ständig das Geschäftsumfeld und nutzt dazu ihre fachliche Expertise, um die Informationssicherheit von Sharp zu erhöhen und ständig zu verbessern. Zusätzlich zu diesen internen Bemühungen nutzt Sharp strategische Partnerschaften mit branchenführenden Dienstleistungsanbietern, um unsere implementierten Informationssicherheitsprogramme zu testen, zu überwachen und zu prüfen.

11. Sharp-Administrator – Datenzugriff

Die IT oder der Support von Sharp muss vielleicht gelegentlich auf Ihre Daten zugreifen, um Support bei technischen Problemen zu gewährleisten. Die Zugriffsberechtigungen für diese Arten von Problemen werden auf erforderliche minimale Berechtigung beschränkt, um Ihr Problem zu lösen. Die Administratoren von Sharp erhalten sorgfältige und rollenbasierte Berechtigungen, um die Datensicherheit für den Kunden aufrechtzuerhalten:

- Die Möglichkeit, Informationen über das Kundenkonto einzusehen und zu aktualisieren, wie etwa den Kontostatus und die E-Mail-Adresse, aber keine Kundendateien
- Die Möglichkeit, den Dateibaum und die Dateinamen einzusehen, aber sie können die eigentlichen Dateien nicht aufrufen oder herunterladen
- Die Benutzer, Administratoren und Händler von Synappx haben ausschließlich zweckmäßigen Zugriff auf die Dateien, solange dies durch ihre Befugnisse gewährleistet wird. Die Systemverwaltung wird streng kontrolliert und auf das autorisierte Personal von Sharp beschränkt. Sharp-Administratoren können nur auf Informationen zugreifen, die für den Betrieb des Systems entscheidend sind. Die Benutzer des Systems können zu keinem Zeitpunkt direkt auf die Datenbank oder andere Systemkomponenten zugreifen.
- Hinweis: Die Daten im Zusammenhang mit Ihren Synappx-Services werden 45 Tage nach dem Ablauf eines Abonnements gelöscht.

12. Sharp-Datenschutzrichtlinie

Bitte lesen Sie die Synappx-Nutzungsbedingungen und die Synappx-Datenschutzrichtlinie unter:

- www.sharp.de/synappx/datenschutz
- www.sharp.de/synappx/nutzungsbedingungen

13. Zusammenfassung

Der Übergang zu cloudbasierten, mobilen Kollaborations- und Meeting-Services bietet für die Unternehmen eine wirtschaftliche Möglichkeit, ihre zunehmend mobilen Mitarbeiter zu unterstützen. Wenn man kollaborative, reaktionsfähige Büroumgebungen schaffen möchte, ist der Einsatz von Cloud- und Mobiltechnologie keine Frage des „ob“, sondern des „wann“.

Organisationen, die Cloud-basierte Dienste nutzen, schöpfen ihre vorhandenen Technologie-Investitionen voll aus – dazu gehören Computer, mobile Geräte, interaktive Monitore und MFPs. In Kombination mit den auf Abonnements basierenden Synappx-Services bedeutet die Eliminierung von Kapitalausgaben für interne IT-Ressourcen noch niedrigere Gesamtbetriebskosten. Dennoch kämpfen einige Entscheidungsträger damit, was eine Cloud-Implementierung mit sich bringt, um Komfort mit Zugänglichkeit und Sicherheit ins Gleichgewicht zu bringen. Die Sharp Synappx Services unterstützen Sie dabei, diese Barrieren zu beseitigen, mit einer sicherheitsorientierten Architektur und einer Hardware-/Software-Synergie, die agile Arbeitsgruppen ermöglicht, die schnell auf Geschäftsanforderungen reagieren kann.

www.sharp.de

SHARP
Be Original.