Konzept „Sichere Dateiablage“

Inhaltsverzeichnis

Präambel

Dieses Dokument wurde vom AK-Internet im BEFG verfasst. Es wurde nach bestem Wissen zusammengestellt und wird laufend ergänzt.

IST-Situation - Problembeschreibung

Innerhalb des BEFG[1] gibt es oft den Wunsch, Dateien gemeinsam zu bearbeiten. Dies ist kein Problem, wenn sich die Mitarbeiter in einem gemeinsamen Netzwerk (LAN) befinden. Häufig ist dies aber nicht der Fall und die Distanzen betragen mehrere Kilometer.

Innerhalb einer Gemeinde kann es der Gemeinderat/Leitungskreis, ein Seelsorgekreis, ein Bauausschuss oder eine überregionale Gruppe sein, die gemeinsam Dateien bearbeiten. Diese Dateien enthalten nicht selten personenbezogene oder sensible Daten, die in vielen Fällen auf privaten Computern oder Laptops von Mitarbeitern gespeichert sind. Unbewusst werden sie jederzeit mitgenommen. Bei Verlust oder Diebstahl eines Endgerätes können diese Dateien schnell in unbefugte Hände gelangen, bei einem Defekt des Gerätes unwiederbringlich verloren gehen.

In einer kirchlichen Gemeinschaft ist der vertrauensvolle Umgang mit Menschen ein hohes Gut. Diese Menschen vertrauen uns. So wie wir mit unseren Mitmenschen und Geschwistern

1 Gemeint sind der Bund selbst, aber auch Gemeinden, Einrichtungen, Initiativen, Landesverbände und Vereine

umgehen, sollten wir auch mit ihren digitalen Daten umgehen. Ein leichtfertiger Umgang mit Daten kann auch das Vertrauen in die kirchliche Organisation in Frage stellen. Der vertrauensvolle Umgang mit sensiblen Daten sollte daher für eine kirchliche Organisation selbstverständlich sein.

Außerhalb eines gemeinsamen Netzwerkes müssen Dateien transportiert werden um sie allen Beteiligten zur Verfügung zu stellen. Hierzu gibt es unterschiedliche Möglichkeiten. Abhängig von der Sensibilität des Inhalts sind diese Verfahren technisch einfach umsetzbar, aber manchmal auch umständlich und zeitintensiv. Hierzu gehören z.B. der Postversand auf einem Datenträger (Ausdruck auf Papier, CD, DVD, USB-Stick) oder, sicherlich am häufigsten genutzt, der Versand per Email. Für sensible Daten, z.B. im Bereich Seelsorge, Mitgliederdaten, Finanzen oder strategische Dateien, sollte eine Verschlüsselung genutzt werden. Dies setzt aber technisches Wissen beim Sender und Empfänger voraus. Darüber hinaus haben viele Mailserver eine Dateiobergrenze von z.B. 10MB oder 20MB. Größere Dateien können daher nicht per Email versendet werden.

Die wenigsten Nutzer sind sich beim Versandt einer regulären E-Mail im Klaren darüber, dass diese im Internet eben so offen eingesehen werden kann wie beispielsweise eine Postkarte die auf dem Postweg versandt wird. Darüber hinaus erzeugt der Versand per Email mehrere Kopien der Daten. Neben dem Empfängerpostfach wird ebenfalls eine Kopie im ‚Gesendet‘-Ordner des Absenders abgelegt. Oft bleiben die Daten dort auf unbestimmte Zeit. Es ist nicht möglich diese zentral zu löschen.

Im Internet gibt es viele Anbieter von sog. Cloud-Diensten, die mit dem Vorteil einer sicheren zentralen Daten-Ablage werben. Der Austausch über einen Webserver oder Clouddienste, stellt auf den ersten Blick eine einfache Lösung für diese Anforderung dar.

Viele Anbieter (z.B. Dropbox, MS-OneDrive) betreiben ihre Systeme allerdings außerhalb der Europäischen Union (EU) und erfüllen damit nicht die Anforderungen bzgl. Datenschutz. Sowohl eine permanente Datenablage als auch ein temporärer Datenaustausch ist daher bei diesen Anbietern kritisch zu bewerten.
Bei Angeboten innerhalb der EU kann der Datenschutz anders bewertet werden. Dennoch liegen die Daten bei einem externen Dritten. Ein Einblick in die Unternehmensstruktur des Anbieters von außen ist oft nicht möglich. Dies bezieht sich auch auf die Vertraulichkeit der (uns unbekannten) Mitarbeiter.

Auf den zweiten Blick gibt es bei der Ablage von Dateien auf einem zentralen Speicherort viele Fragestellungen, die zu beachten sind.

Hier ein kleine Auswahl:

- Wer hat beim Anbieter Zugriff auf die Daten?
- Wo liegen die Daten physisch und geografisch (z.B. in den USA?)
- Erfolgt eine Kopie (Sicherung) auf weitere Systeme? Wo stehen diese?
- Wie werden die Zugriffe verwaltet?
- Werden die Daten beim Löschen wirklich gelöscht oder nur ausgeblendet?

Konzept „Sichere Dateiablage“

- Wie ist der Schutzbedarf von sensiblen Daten (z.B. Mitgliederverzeichnissen, Dateien mit seelsorgerlichem Inhalt oder Finanzberichten) geregelt?
- Erfolgt der Zugriff über einen verschlüsselte Transportweg?

Vor dem Hintergrund dieser Fragen wird schnell deutlich, dass cloud-Dienste nicht geeignet sind, die vorhandenen Anforderungen zu erfüllen.

Anforderungen an eine Lösung

Die Liste der Anforderungen ist umfangreich:

- Die Dateien sollten zeitnah für die Empfänger verfügbar sein.
- Die Datenhoheit liegt beim Inhaber der Daten. (Gemeinde/Einrichtung/Landesverb.)
- Der Datenlagerort sollte sich in den Räumlichkeiten der Gemeinde/Einrichtung oder einem vertrauensvollen Ort befinden.
- Der Zugriff auf die Daten sollte ausschließlich über verschlüsselte Protokolle erfolgen, z.B. https, FTPS, SFTP oder WebDAVs
- Ein Zugriff auf die Daten darf nur durch berechtigte Personen möglich sein.
- Auch Dateien über 20MB (Obergrenze der meisten Mailserver) sollten ausgetauscht werden können.
- Die Handhabung sollte einfach sein.
- Die Dateien sollten von überall und von verschiedenen Endgeräten erreichbar sein.
- Die Lösung muss leicht umsetzbar und möglichst wartungsarm sein.
- Die Versorgung mit (Sicherheits-)Updates sollte gewährleistet und möglichst automatisiert sein.
- Verwendung von Standards (Keine 'selbstgestrickte‘ Lösung)
- Es sollten sich mehrere Personen mit der Lösung auskennen.
- Aufwand und Kosten sollten ‚zumutbar‘ sein.

Lösungsvorschläge

Variante 1: (empfohlen)
Der Handel bietet vorinstallierte NAS-Systeme an. Diese Systeme sind inzwischen auf einem hohen technischen Niveau, und werden daher auch in vielen Unternehmen im professionellen Umfeld eingesetzt. Einstiegsgeräte sind auch für Privatpersonen und Gemeinden erschwinglich. Diese Geräte bilden eine gute Basis für eine sichere Dateiablage.

Achtung:

Nur der Kauf und die Inbetriebnahme eines solchen Systems bietet noch keine sichere Dateiablage. Es ist notwendig eine Administrations- und Berechtigungsübersicht zu erstellen aus der die Zugriffsrechte hervorgehen.

Konzept „Sichere Dateiablage“

Variante 2:
Aufbau einer eigenen Hardware und Installation einer Cloud-Software (Own[2]-, Nextcloud[3], FreeNAS[4], OpenMediaVault[5] etc.)

Hinweis: Diese Variante erfordert tiefgehende IT-Fachkenntnisse um eine stabile und dauerhaft sichere Plattform zu betreiben. Sie sollte nur von erfahrenen IT-Experten in Betracht gezogen werden.

Wir empfehlen Variante 1 (NAS). Bekannte Hersteller solcher Systeme sind z.B. Synology oder QNAP. Grundsätzlich unterscheiden sich diese Hersteller nur in Details. Jeder Hersteller hat spezielle Vor- und Nachteile. Eine genauere Betrachtung und Bewertung der unterschiedlichen Details ist im Einzelfall sinnvoll.

Abhängig von der Ausstattung beträgt die einmalige Investition zwischen 300,- € und 700,- €. Die Lebensdauer dieser Geräte sollte mit 5 Jahren kalkuliert werden.

Kriterien für eine sichere Konfiguration

Im Folgenden sind Einstellungen beschrieben, die bei der Inbetriebnahme und der Konfiguration zu beachten sind. Die Geräte der bereits genannten Hersteller QNAP und Synology bieten diese Möglichkeiten. Andere Hersteller wurden nicht genauer betrachtet, es gibt aber sicherlich weitere vergleichbare Systeme.

Benutzerverwaltung

Jede Personen, die Zugang haben soll, muss eine eigene Berechtigung erhalten. Je nach Bedarf können die Berechtigungen (Lesen/Ändern/Kein Zugriff) unterschiedlich vergeben werden. Um Fehler bei der Inbetriebnahme zu vermeiden, wird empfohlen vor der Einrichtung eine Übersicht zu erstellen, aus der die eingerichteten Ordner sowie die Schreib- und Leseberechtigungen für die vorgesehenen Benutzer hervorgehen.

Ein Administratorkonto dient der Einrichtung der Benutzerkonten und sollte keinen Zugriff auf die eingerichteten Ordner haben. Es wird empfohlen das Passwort des Administrators im 4-Augen-Prinzip zu vergeben. Mindestens eine Passworthälfte sollte im Besitz einer Person aus der Leitung sein. (z.B. Mitglied des Gemeinderates) Die beiden Passworthälften können für den Notfall in zugeklebten Umschlägen an getrennten Orten sicher verwahrt werden.

Verwendete Protokolle

Das System ist so zu konfigurieren, dass ausschließlich eine verschlüsselte Kommunikation möglich ist. Dies bezieht sich auf die Weboberfläche (https), als auch auf die Einbindung als Netzlaufwerk (webdavs) die für einzelne Benutzer sinnvoll ist.
Hierzu gehören https, WebDAVs, SFTP oder FTPS. Der Zugriff über unsichere Protokolle (z.B. webdav, http oder FTP) sollte nicht ermöglicht werden.

2 https://owncloud.org/
3 https://nextcloud.com/
4 https://www.freenas.org/
5 https://www.openmediavault.org/

Verfasser:
Arbeitskreis Internet im BEFG
Fragen? support@ak-internet.de

Konzept „Sichere Dateiablage“

SSL-Zertifikat

Für einen verschlüsselten Zugriff wird ein SSL-Zertifikat benötigt. Dieses kann selbst generiert werden. Dieser Vorgang ist für Laien allerdings schwierig. Darüber hinaus entsteht hierdurch der Nachteil, dass diese sog. „selbstsignierten“ Zertifikate eine Warnmeldung beim Aufruf im Browser erzeugen.
Kommerzielle NAS unterstützen das Einbinden von Zertifikaten. Die genannten Hersteller unterstützen die Zertifikate von „Let‘sEncrypt“. Diese Zertifikate bieten eine ausreichende Absicherung und sind kostenlos.

Aufstellort

Das System sollte nicht allgemein zugänglich sein. Idealerweise steht es in einem abgeschlossenen Raum (z.B. EDV-Raum, Gemeindebüro, abgeschlossener Raum oder Schrank). Der Aufstellort sollte so gewählt sein, dass das Gerät nicht durch ein Fenster sichtbar ist, nicht in der Nähe von wasserführenden Leitungen steht und ausreichend belüftet ist. Grundsätzlich ist es auch möglich, dass das NAS bei einer Person aus der Leitung (z.B. Gemeindeleiter oder Pastor) zu Hause steht. Hierbei ist jedoch verstärkt darauf zu achten, dass der Zugriff durch Unbefugte (z.B. Kinder oder Gäste) nicht möglich ist.

Datensicherung

Die Systeme bieten die Möglichkeit , regelmäßig (z.B. täglich) automatisch Sicherungen durchzuführen. Dies kann auf einem direkt angeschlossenen Sicherungsmedium oder auf einem weiteren System erfolgen. Hierbei gelten dieselben Anforderungen an den Aufstellort wie beim (Haupt-)System selbst.

Virenscan

Viele Hersteller ermöglichen einen täglichen automatischen Virenscan. Diese Funktion sollte genutzt werden. Hierfür werden von den Herstellern auch kostenlose Virenscanner angeboten.

Anbindung/Erreichbarkeit über das Internet

Um ein System aus dem Internet erreichen zu können, muss die sog. IP-Adresse des Anschlusses bekannt sein. Diese Adresse bekommt der Router, in der Regel jede Nacht, automatisch von einem Provider neu zugewiesen. Durch die tägliche Änderung ist ein Zugriff über diese Adresse praktisch nicht realisierbar, da diese Adresse jeden Tag allen Nutzern bekanntgegeben werden müsste. Mit Hilfe von DynDNS-Diensten kann dieses Problem gelöst werden. Es ist auch möglich den Aufruf über eine Sub-Domain (z.B. http://cloud.efg-musterstadt.de) zu realisieren.

Port-Freigaben im Router

Für die verschlüsselte Weboberfläche muss das System über einen definierten Port (üblich ist 443) aus dem Internet erreichbar sein. Diese Einstellung lässt sich in den üblichen Routern vornehmen.
Für „Let‘sEncrypt“ muss das NAS über Port 80 erreichbar sein. Sonst ist keine Verlängerung des Zertifikates möglich. Dies kann auch nur temporär erfolgen.

Verfasser:
Arbeitskreis Internet im BEFG
Fragen? support@ak-internet.de

Konzept „Sichere Dateiablage“

Für die Nutzung von WebDAV muss zusätzlich ein weiterer Port (z.B. 5001 oder 5006) freigegeben werden.

Zugriff auf die Daten

Über eine Benutzerverwaltung können die unterschiedlichen Berechtigungen konfiguriert werden. Es gibt unterschiedliche Zugriffsmöglichkeiten:

Zugriff mit einem Benutzerkonto
Benutzer können sich am System (über einen Browser) mit ihren Zugangsdaten anmelden.
Administratoren können jedem Benutzer, je nach Bedarf, Lese bzw. Schreibberechtigungen für die eingerichteten Freigabeordner zuweisen.
Benutzer können Freigabelinks erstellen. Abhängig vom Hersteller des NAS ist es möglich für einen Ordner gleichzeitig mehrere Freigabelinks zu erzeugen. z.B. einer mit Uploadfunktion und einer ohne.
Freigabelinks sollten nur mit gesichertem Zugriff (SSL) eingerichtet werden.

Ein Administrator kann die Freigabelinks aller Mitarbeiter einsehen und verwalten.

Benutzer mit Adminrechten können zusätzlich Einstellungen vornehmen und Benutzer verwalten.

Mitarbeiter die ein Benutzerkonto erhalten sollen, müssen auf den vertrauensvollen Umgang hingewiesen werden. Die Anzahl er Benutzer sollte möglichst gering sein

Zugriff über einen Freigabelink
Dieser Zugriff wird von einem Benutzer eingerichtet und ermöglicht Externen den Zugriff auf einzelne Dateien sowie Ordnern (mit Unterordnern!). Freigabelinks sollten zeitlich begrenzt werden. Je nach Anforderung sind Uploads für Externe möglich.

Berechtigungen im Überblick:			
Funktion	**1. Benutzerkonto**	**2. Freigabelink** (zeitlich begrenzt, mit Passwortschutz)	**3. Freigabelink mit Upload** (zeitlich begrenzt mit Passwortschutz)
Dateien herunterladen	*	*	*
Dateien hochladen	*	-	*
Dateien durch Hochladen zur Verfügung stellen	*	-	*(1)
eigene Freigabelinks erstellen	*	-	-
Zugriffsmöglichkeiten			
Einbindung als Netzlaufwerk (WebDAVs)	*	-	-
Mobile App (Android, IOS)	*	-	-

Verfasser:
Arbeitskreis Internet im BEFG
Fragen? support@ak-internet.de

Konzept „Sichere Dateiablage“

(1) Es besteht grundsätzlich das Risiko, dass ein Externer, dem ein Freigabelink mit Uploadfuntkion erteilt wurde, die Plattform temporär für eigene Zwecke nutzt, oder den Link weiterleitet und so z.B. das als 'Sharing-Plattform' zweckentfremdet. Dieses würde aber protokolliert werden.

Updates

Viele Systeme prüfen selbstständig ob neue Updates vorliegen. Ist dies der Fall, erhält ein Administrator bei der Anmeldung an der Weboberfläche einen entsprechenden Hinweis.

Hardwarebeispiele

Folgende Geräte können aus praktischer Erfahrung empfohlen werden (Modelle aus 2018):

Synology DS-220+ **QNAP TS-251+**

Die Geräte sind sehr ähnlich, unterscheiden sich aber in Kleinigkeiten. Der Hersteller Synology hat einige Details etwas eleganter gelöst, daher ist dieser Hersteller von uns derzeit empfohlen.
Der Preis liegt bei beiden Geräten bei ca. 300,- bzw. 500,-€ (ohne Festplatten). Abhängig von der Größe der Festplatten liegt der Gesamtpreis bei ca. 600,- € bis 700,- €. Damit sind diese Geräte nicht für jede Gemeinde erschwinglich.

Verfasser:
Arbeitskreis Internet im BEFG
Fragen? support@ak-internet.de