Anwendungsbeispiel Medienunternehmen

1) Beschreibung

Journalistenteams recherchieren und schreiben gemeinsam an einer Artikelserie (auch international vernetzt). Dabei müssen die beteiligten Personen vertrauliche Dokumente, Listen mit den persönlichen Daten von Ansprechpartnern oder O-Ton bzw. Bildmaterial austauschen. Zudem sollte jeder beteiligte Redakteur den jeweils aktuellen Stand der Artikel kennen, an denen er gerade mitarbeitet. Informanten brauchen einen abhörsicheren Kanal, um Kontakt aufnehmen zu können.

2) Anforderungen:

- Gemeinsame Arbeitsspeicher, um Dokumente auszutauschen (Artikelsortiert)
- die Vertraulichkeit muss in jedem Fall gewährleistet sein
- Foto/Audiodateien mit hoher Informationsmenge (viele 100 MB) sollen problemlos zu übermitteln sein
- Benachrichtigung in Echtzeit, sobald ein Journalist eine Aktualisierung vornimmt
- abhörsicherer Chat, um schnell Fragen klären zu können
- sicherer Zugriff vom PC aus, aber auch von mobilen Geräten wie Smartphone und Tablet
- Informanten brauchen von Anfang an einen sicheren Kanal zu ihren Ansprechpartnern
- gegebenenfalls sollte der Arbeitsbereich nach Beendigung des Projekt rückstandslos zu löschen sein
- geringe Kosten pro Datenraum.

3) Bereits vorhandene Lösungsoptionen:

a) eMail: Dies entspricht der üblichen Arbeitsweise, wobei Journalisten ihre E-Mail mehrheitlich verschlüsseln. Für jedes Projekt muss allerdings die Etablierung der Verschlüsselung geklärt werden, da es meist redaktionsexterne Teammitglieder gibt. Ein gemeinsamer Arbeitsbereich fehlt besonders bei kleineren oder mittleren Medienunternehmen; die Redaktion muss meist aufwendig koordinieren. Die Kontaktaufnahme von Informanten erfolgt meist telefonisch oder persönlich, damit sich diese „sicher“ fühlen.
Ergebnis: Anforderungen nicht komplett erfüllt.

b) SharePoint oder andere interne Plattformen: Bei großen Redaktionen ein gangbarer Weg. Schwierig bleibt der externe Zugang auf interne Systeme.
Ergebnis: Anforderungen nicht komplett erfüllt.

c) Öffentliche FileSharing-Dienste: Auf diese Dienste kann man einfach zugreifen und sie sind bequem zu bedienen. Leider können sie die von Journalisten benötigte Vertraulichkeit nicht liefern, denn der Service Provider kann prinzipiell auf alle Dokumente zugreifen.
Ergebnis: Anforderung nicht komplett erfüllt.

d) Datenraum-Dienste: Sie bieten ein hohes Maß an Sicherheit und erfüllen die meisten der genannten Anforderungen. Kosten und Verwaltungsaufwand jedoch sind ein Schwachpunkt bei diesen Diensten.
Ergebnis: Anforderungen weitgehend erfüllt, jedoch teuer und aufwendig.

4) Der Dienst iDGARD erfüllt alle Anforderungen:

Der Kommunikationsdienst erfüllte die Anforderungen bei vergleichsweise geringen Kosten. Die zugrundeliegende Basistechnologie Sealed Cloud (bereits in der EU und in den USA patentiert) verhindert zusätzlich, dass der Service Provider auf die Daten der jeweiligen Anwender zugreifen kann.
Ergebnis: Anforderungen erfüllt.

5) Konkreter Einsatz von iDGARD

Nach eingehender Prüfung entschied man sich für den Einsatz des Kommunikationsdienstes iDGARD. Die Registrierung dauerte nur zwei Minuten, danach war die Redaktion online und konnte die Redakteure als Mitarbeiter einladen: Für jedes Ressort wurde eine Privacy Box angelegt. Insgesamt steht ein Pool mit 100 GB Speicherplatz im Starter-Paket für alle Lizenzen zur Verfügung, innerhalb derer er bis zu 2.000 solcher Privacy Boxen anlegen kann.
Weiterer Speicher sowie Voll- und Gastlizenzen können bei Bedarf flexibel und individuell dazu gebucht und sofort genutzt werden.
Sind Funktionen wie Journal, Wasserzeichen oder Dokumente nur zur Ansicht notwendig, lässt sich jede Privacy Box ganz einfach und schnell in einen Datenraum umwandeln.
Die im jeweiligen Ressort arbeitenden Journalisten wurden vom Redakteur dann per Auswahl aus dem bereits automatisch erstellten iDGARD-Verzeichnis in die Privacy Box eingeladen – jeweils nur mit einem Klick. Freien oder externen Journalisten wies der Redakteur eine iDGARD-Gastlizenz zu, falls diese noch keine hatten. Dazu benötigte er nur die eMail-Adresse und die Handynummer des jeweiligen Journalisten.

Redaktionelle Integration der Privacy Boxen
Alle in dem Ressort tätigen Journalisten, interne wie externe, nutzten die für sie vorgesehenen Privacy Boxen, um Dateien und Nachrichten auszutauschen. Die Dateien wurden dabei in entsprechenden Verzeichnissen strukturiert und thematisch geordnet. Sie waren und sind für alle Teammitglieder sichtbar gespeichert. Diese können per Browser oder App jederzeit auf die Unterlagen des Ressorts zugreifen, sei es von ihrem PC, ihrem Smartphone oder Tablet aus. Jeder Mitarbeiter-Account ist abgetrennt, sodass die Redakteure ihre eigenen Boxen zu Artikeln anlegen konnten. Daher konnten die Redakteure auch vertraulichen Kontakt zu Informanten halten, eigene Recherchen durchführen oder Artikel entwickeln. Sie legten einfach eigene private Boxen, getrennt von der Ressort-Box an.

Zum Nachrichtenaustausch zwischen den Boxmitgliedern gibt es verschiedene Möglichkeiten:

a) iDGARD Chat: In Echtzeit Fragen klären oder schnell eine Diskussion führen – per Browser oder App
b) iDGARD Notizen: Nachrichten, die parallel zu den Dokumenten gespeichert wurden – zur Erläuterung oder mit Ergänzungen

Der Inhaber einer Privacy Box kann die darin enthaltenen Dokumente jederzeit lokal speichern und archivieren. Wenn man die Box löschen will, erfolgt dies bei iDGARD rückstandsfrei.

Sicherheitsmaßnahme im Bereich „Investigativer Journalismus“
Ein Mitarbeiter-Account lässt sich von der Redaktion aus verwalten, ohne dass der Administrator Einsicht in die dazugehörigen Boxen hat. Dies sichert Journalisten ab, wenn sie sich in einer Gefahrenzone befinden. Sollte sich ein Reporter plötzlich nicht mehr melden, kann die Redaktion als Sicherheitsmaßnahme ein neues Passwort für den Account anlegen. Im Falle eines verifizierten Fehlalarms gibt die Redaktion den Account einfach zurück.

Anonymer Kanal für Informanten
Informanten, die einen anonymen und sicheren Informationsaustausch wollen, können mit 1-Klick Kontakt aufnehmen. Dafür gibt es einen speziellen Button auf der Homepage der Redaktion. Ein eigens angelegter Kanal ermöglicht es Informanten, vorerst einmal anonym aufzutreten. Die Kontaktaufnahme kann selbst über die Verbindungsdaten nicht nachverfolgt werden.