

Anwendungsbeispiel Industrie: Sichere Team Workspaces (Secure Data Rooms) und Übermittlung von sensiblen Daten und großen Dateien

1) Beschreibung

Firmeninterne Mitarbeiter (z.B. Einkauf, Marketing & Kommunikation, Qualitätsmanagement) arbeiten im Team mit externen Partnern wie Designern, Ingenieurdienstleistern, Zulieferern und Patentanwälten. Sie stellen vertrauliche Informationen (z.B. im Rahmen von Neuentwicklungen, Machbarkeitsanalysen, Ausschreibungen, Qualitätsmanagement) zur Verfügung und arbeiten gemeinsam an Dokumenten (z.B. CAD-Dateien, ARIS-Dateien). Es handelt sich dabei um sowohl hochsensible als auch große Dateien, die sicher ausgetauscht und bearbeitet werden müssen. Ein Projekt kann über mehrere Wochen dauern bis zu seinem Abschluss.

2) Anforderungen

- Gemeinsamer Arbeitsspeicher für Dateiaustausch
- hohe Sicherheit, die den Bedürfnissen der Geheimhaltung entspricht
- möglichst einfache Nutzung ohne Bedarf an Training
- Echtzeitbenachrichtigung à Meldung neuer Dokumente an alle Projektmitglieder
- sicherer und verschlüsselter Nachrichtenaustausch ohne kompliziertes Schlüsselmanagement
- Zugriff von PC und mobilen Geräten – Smartphone & Tablet – aus
- einfache Verwaltung – hinzufügen und entfernen von Projektmitgliedern
- rückstandsfreies Löschen des Arbeitsbereichs nach Abschluss eines Projekts und vorherigen Backups
- geringe Kosten je Datenraum (zusätzliche Features zum Schutz vor Weiterverbreitung)
- optional: Zusätzliche Sicherheit bei der Anmeldung durch 2-Faktor-Authentisierung.

3) Bisherige Alternativen, die die Anforderungen nur unzureichend erfüllen

- a) eMail: Dies entspricht der bisherigen Arbeitsweise. Dokumente werden per E-Mail ausgetauscht und jeweils lokal gehalten. Leider muss für jedes Projekt erneut die Etablierung von E-Mail-Verschlüsselung geklärt werden, die oftmals nicht firmenübergreifend vorhanden ist. Ein gemeinsamer Teambereich fehlt.
- b) SharePoint oder andere interne Plattform: Hier werden die meisten Anforderungen erfüllt. Es hat sich jedoch als schwierig erwiesen, externen Nutzern den Zugriff auf interne Systeme zu gewähren. Oft ist es auch aufwendig, die Zugriffsrechte externer Nutzer detailliert zu steuern.
- c) Öffentliche FileSharing Dienste: Diese Dienste bieten einfachen und bequemen Zugang sowie Nutzung. Leider erfüllen sie zumeist nicht die Sicherheitsanforderungen von Unternehmen. Wichtige Dokumente dürfen nicht auf Systemen gespeichert werden, wenn der Service Provider prinzipiell auf die Dokumente Zugriff hat.
- d) Datenraumdienste: Diese Dienste bieten ein hohes Maß an Sicherheit und erfüllen viele der genannten Anforderungen. Die Dienste sind jedoch sehr teuer und erfordern zumeist einen höheren Verwaltungsaufwand. Die Anforderungen werden weitgehend erfüllt, die Dienste sind jedoch teuer und aufwendig.

4) Die Lösung: iDGARD erfüllt alle Ihre Anforderungen

Der Dienst iDGARD erfüllt alle diese Anforderungen bei sehr geringen Kosten, einfacher Nutzung und Verwaltung. iDGARD schließt durch die zugrunde liegenden Sealed Cloud Technologie aus, dass Mitarbeiter des iDGARD-Betreibers auf Anwenderdaten zugreifen können. Die iDGARD Login Card (TAN-Generator im Scheckkartenformat) erhöht bei Bedarf noch zusätzlich die Sicherheit bei der Anmeldung mit 2-Faktor-Authentisierung auf allen Endgeräten ohne Bedarf zusätzlicher Lesegeräte.

5) Konkreter Einsatz von iDGARD

iDGARD Privacy Boxes als sichere Team-Arbeitsräume

iDGARD – sichere Kommunikation und Datenaustausch

1. Sicherer mobiler Aktenkoffer

Jederzeit Zugriff auf Ihre Daten – mobil mit speziellen Apps oder per Browser



2. Alternative zu FTP- & Filesharing-Diensten

Große Dateien sicher versenden – automatisches Schlüsselmanagement – leicht verständlich

3. Projekt- & Team-Arbeits-Räume

Firmenübergreifender Dokumenten- und Datenaustausch, Nachrichten & Chats



4. iDGARD Datenräume

Schutz vor unerwünschter Weiterverbreitung (z.B. Wasserzeichen, Journal,...) für PDFs

Die Registrierung eines Unternehmens bei iDGARD dauert nur zwei Minuten. Anschließend kann man iDGARD sofort online nutzen und Mitarbeitern den Zugang (Volllizenz) einräumen.

Der hauptverantwortliche Projektleiter legt dann innerhalb von Sekunden eine Privacy Box für das Projekt an. 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 kann 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 internen und externen Mitglieder des Projekts werden vom Projektleiter per Auswahl aus dem iDGARD-Verzeichnis in die Box eingeladen – jeweils mit nur einem Klick. Externen Partnern (z.B. Zulieferer und Dienstleister) weist er eine iDGARD-Gastlizenz zu. Dazu benötigt er lediglich deren eMail-Adresse und Mobilrufnummer zur Übermittlung des Passwortes.

Alle Projektmitglieder, intern und extern, nutzen diese Privacy Box zum Austausch von wichtigen Dokumenten und Nachrichten. Die Dateien werden dabei in entsprechenden Verzeichnissen strukturiert, thematisch geordnet und für alle Teammitglieder sichtbar gespeichert.

Alle Projektmitarbeiter haben so per Browser oder App jederzeit Zugriff auf alle Unterlagen zum Projekt – von Ihrem PC oder auch vom Smartphone & Tablet aus.

Ist ein wichtiger Kollege krank, im Urlaub oder die Zuständigkeit für ein Projekt ändert sich, kann eine projektspezifische Box an einen Kollegen übergeben werden. Wechselt ein Mitarbeiter, kann der gesamte Account inkl. der enthaltenen Boxen an seinen Nachfolger übertragen werden.

Zum Nachrichtenaustausch zwischen Projektmitgliedern verwendet man verschiedene Methoden:

1. iDGARD Chat für den Austausch in Echtzeit, d.h. sofortige Diskussion online möglich.
2. iDGARD Notizen für Nachrichten, die für eine Nachverfolgung der Diskussion parallel zu den jeweiligen Dokumenten gespeichert werden.
3. eMail steht natürlich weiterhin zur Verfügung.

Nach Abschluss des Projekts wird der Inhalt der gesamten Privacy Box lokal archiviert – und anschließend gelöscht. Dies erledigt iDGARD rückstandsfrei.

Für ein Projekt mit 3 internen Mitarbeitern und 6 externen Partnern werden folgende iDGARD-Lizenzen benötigt:
3 Volllizenz und 6 Gastlizenz

Jeder Nutzer kann parallel in beliebig vielen Boxen arbeiten, zu welchen er eingeladen wurde.

Generell zeigt sich, dass iDGARD intuitiv ohne Training und ohne Softwareinstallation von den internen Mitarbeitern als auch von den externen Ansprechpartnern produktiv genutzt wird.

Kontakt:

Unicon – The Web Privacy Company
Agnes-Pockels-Bogen 1, 80992 München

www.idgard.de | contact@idgard.de
Telefon: 089 / 4161 5988 100

