Anwendungsbeispiel Öffentliche Verwaltung / Kommunen: Datenschutz

1) Fallbeispiel

Öffentliche Verwaltungen arbeiten gemeinsam mit externen Ansprechpartnern wie z.B. Rechtsanwälten, Steuerberatern, Architekten, Behörden und Bürgern zusammen an verschiedenen Projekten.

Dabei müssen viele vertrauliche Dokumente ausgetauscht und bearbeitet werden. Ein Projekt kann bis zu mehrere Wochen oder Monate Zeit bis zu seinem Abschluss benötigen.

2) Anforderungen

- Gemeinsamer Arbeitsspeicher für Dateiaustausch
- hohe Sicherheit, die den Bedürfnissen der Geheimhaltung entspricht
- möglichst einfache Nutzung ohne Bedarf an Training
- Echtzeitbenachrichtigung bei Eingang neuer Dokumente an alle Mitglieder in einer Box
- sicherer Nachrichtenaustausch zwischen allen Projektbeteiligten
- Zugriff vom PC und auch von mobilen Geräten – Smartphone & Tablet – aus
- einfache Verwaltung – hinzufügen und entfernen von Teammitgliedern
- rückstandsfreies Löschen des Arbeitsbereichs nach Abschluss eines Projekts
- Virenschutz – direkt in der Cloud
- geringe Kosten je Datenraum (zum Schutz vor Weiterverbreitung von Dokumenten)
- optional: Zusätzliche Sicherheit durch 2-Faktor-Authentisierung (Login Card).

3) Betrachtete Lösungsoptionen

a) eMail: Nur mit Verschlüsselung akzeptabel – Verschlüsselungslösungen sind aber häufig Insellösungen und erfordern somit eine spezielle Schlüsselverwaltung. Ein gemeinsamer Arbeitsbereich für eine Öffentliche Verwaltung und ihre externen Partner fehlt.

b) SharePoint oder andere interne Plattform: Die meisten Anforderungen werden erfüllt. Externe Nutzer erhalten Zugriff auf interne Ressourcen – die sichere, meist aufwendige Abschottung von externen Nutzern ist notwendig.

c) Öffentliche FileSharing Dienste: Einfacher und bequemer Zugang sowie Nutzung. Erfüllen selten die Sicherheitsanforderungen von Öffentlichen Verwaltungen und deren Partnern. Außerdem haben Mitarbeiter des Service Providers prinzipiell Zugriff auf die Dokumente ihrer Nutzer.

d) Datenraumdienste: Bieten ein hohes Maß an Sicherheit und erfüllen viele der genannten Anforderungen. Allerdings sind diese Dienste meist sehr teuer und erfordern einen hohen Verwaltungsaufwand.

Ergebnis: Anforderungen nicht erfüllt.

4) Der Dienst iDGARD erfüllt alle diese Anforderungen

iDGARD erfüllt alle Anforderungen, die Öffentliche Verwaltungen/Kommunen anstreben und das bei sehr geringen Kosten, einfacher Nutzung und Verwaltung. iDGARD schließt durch die ihm zugrunde liegenden Sealed Cloud Technologie aus, dass Mitarbeiter des iDGARD-Betreibers auf Anwenderdaten zugreifen können. Die iDGARD Login Card (ein TAN-Generator im praktischen Scheckkartenformat) bietet bei Bedarf eine sichere 2-Faktor-Authetisierung auf allen Endgeräten ohne zusätzliche Lesegeräte.

5) Konkreter Einsatz von iDGARD

iDGARD Privacy Boxes als sichere Team-Arbeitsräume

Die Registrierung bei iDGARD dauert nur zwei Minuten. Anschließend kann man iDGARD sofort online nutzen und Mitarbeitern den Zugang einräumen. Der hauptverantwortliche Projektleiter legt 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 Mitglieder des Projektes werden vom Projektleiter per Auswahl aus dem iDGARD-Verzeichnis in die Privacy Box eingeladen – jeweils mit nur einem Klick.

Externen Ansprechpartnern (andere Behörden, Rechtsanwälte, Steuerberater, Architekten etc.) weist er eine iDGARD-Gastlizenz zu, falls diese noch keine haben. Dazu benötigt er lediglich die eMail-Adresse und Mobilrufnummer des jeweiligen Ansprechpartners.

Insbesondere in der Kommunikation mit Kunden, Partnern und Mandanten, bei denen nicht sicher ist, ob ein zuverlässiger Virenschutz besteht, kann iDGARD - Sealed Antivirus zusätzliche Sicherheit ohne Offenbarung von Daten gewährleisten.

Bei einem Virenscan müssen die Daten grundsätzlich in entschlüsselter Form vorliegen. Daher kann der Zugriff bei herkömmlichen Systemen durch den Betreiber nicht zuverlässig ausgeschlossen werden. Durch iDGARDs patentierte Sealed Cloud Technologie ist ein Virenscan in der Sealed Cloud möglich ohne die Sicherheit einzuschränken.

Alle Teammitglieder, intern und extern, nutzen die Privacy Box zum sicheren Austausch von Dokumenten und Nachrichten. Die Dokumente werden dabei in entsprechenden Verzeichnissen strukturiert und somit thematisch geordnet für alle Teammitglieder sichtbar gespeichert. Alle Teammitglieder haben per Browser oder App jederzeit Zugriff auf alle Unterlagen zum Projekt – von Ihrem PC oder auch vom Smartphone & Tablet aus.

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

Zum Nachrichtenaustausch zw. den Projektmitgliedern verwendet man verschiedene Methoden:

a) iDGARD Chat für den Austausch in Echtzeit, d.h. sofortige Diskussion online möglich.
b) iDGARD Notizen für Nachrichten, die für eine Nachverfolgung der Diskussion parallel zu den jeweiligen Dokumenten gespeichert werden.

Zum Abschluss des Projekts werden alle Dokumente und Nachrichten lokal vom Projektleiter gespeichert und archiviert. Der Projektarbeitsraum/Privacy Box kann gelöscht werden. Dies erfolgt bei iDGARD rückstandsfrei.

Beispiel: Für ein Projekt mit 5 Mitarbeitern der Behörde und 10 externen Projektpartnern werden folgende iDGARD-Lizenzen benötigt: 5 Volllizenzen und 10 Gastlizenzen.
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 sowohl von internen Mitarbeitern als auch von externen Projektpartnern produktiv genutzt wird.

iDGARD
by UNISCON - a member of TÜV SÜD

Virtuelle Datenräume und Teamarbeit

komfortabel und produktiv bei höchster Compliance

Versiegelter **Austausch von Dokumenten**
(statt limitierter FTP-Lösungen)

Versiegelte **Datenräume**
(statt typischer File Sharing Dienste / klassischer Datenraumdienste)

Versiegelter **Austausch von Nachrichten**
(statt unverschlüsselter eMail)

Versiegelter **Chat**
(statt typischer Chat Dienste)

Sicherer, **mobiler Zugriff** auf Unterlagen und Nachrichten
(statt Dropbox)

Sichere **Terminabstimmung**
(statt Doodle)

Versiegelte **Machine-to-machine** Datenräume
(statt VPN-Vermaschung und Öffnung der Netze)

Gefördert durch das
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

- Versiegelte Verarbeitung – ohne Betreiberzugriff (patentiert)
- einzigartiger Schutz von Inhalten & Verbindungsinformationen – zertifiziert
- vom TÜV-IT mit der höchsten Schutzklasse für Clouds bewertet.

Für Berufs- und Dienstgeheimnisträger (§ 203 Abs. 2 StGB, § 353b Abs. 1 StGB) zulässig – z.B. Ärzte, Anwälte, Wirtschaftsprüfer, Amtsträger

Kontakt:
Uniscon – The Web Privacy Company
Agnes-Pockels-Bogen 1, 80992 München
www.idgard.de | contact@idgard.de
Telefon: 089 / 4161 5988 100

Virtuelle Datenräume und Teamarbeit

Key Facts

Systeme & Integration:

- Komfortabel über AD_LDAP mit SSO einsetzbar
- produktive Clients für ab Windows 7 (MAC Roadmap)
- sichere Apps für iOS, Android, Windows, Blackberry
- optionale Integration von CRM, Web-konferenz-Systemen, u.a.

Vorteile:

- Optimierung der Unternehmens-kommunikation
- nachhaltige Kundenbindung und Wettbewerbsvorteile
- Schutz vor Industriespionage und Ihrer Metadaten

Sicherheit:

- Automatisches AES-256 Schlüssel-management
- Architektur kommt ohne Schlüssel-speicher im System aus
- Einzelverschlüsselung der Dateien / versiegeltes Backup
- kein Zugriff durch Administratoren und Betreiber
- Unterstützung multipler Schnittstel-len & Protokolle zur Authentifizie-rung
- Online Anti-Virus-Scan

Datenschutz & Compliance :

- Höchste Klassifizierung im Trusted Cloud Datenschutz Profil (III für Be-rufs- und Dienstgeheimnisträger)
- versiegelte Cloud – im Rahmen der Trusted Cloud Ausschreibung vom BMWi gefördert
- Server Standort ausschließlich in Deutschland
- Schutz von PDF-Dokumenten vor un-erwünschter Weiterverbreitung: Do-kumente nur zur Ansicht, dynami-sches Wasserzeichen, Anti-Virus-Schutz, revisionssicheres Journal, Screen-Scraper Schutz