Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Datum: 10.03.2021

dDatabox

Dieses Dokument beschreibt den von Dataport angebotenen Dienst dDatabox in seiner Funktionsweise. Anschließend werden Fragen zum Datenschutz und zur Verwendung zum Datenaustausch mit hohem Schutzbedarf diskutiert.

INHALT

www.datenschutz-hamburg.de

E-Mail: mailbox@datenschutz.hamburg.de

Ludwig-Erhard-Str. 22 - 20459 Hamburg - Tel.: 040 - 4 28 54 - 40 40 - Fax: 040 - 4 28 54 – 40 00

Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden.

Der öffentliche PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 0932 579B 33C1 8C21 6C9D E77D 08DD BAE4 3377 5707).

Was ist dDatabox?

Die dDatabox wird von Dataport als Dienst zum Datenaustausch angeboten und kann von allen Organisationsbereichen als verantwortliche Stellen der Dataport-Trägerländer beauftragt werden. Mit der Hilfe von dDatabox können Daten in Form von Dateien in so genannten Datenräumen (Data Rooms) für eine kontrollierte Gruppe von Nutzern abgelegt und anschließend abgerufen werden. Eine Weitergabe an Nutzern außerhalb der Gruppe ist über einschränkbare Web-Links möglich. Externen Nutzern ist das Hinzufügen von Daten durch steuerbare Upload-Links ebenfalls möglich.

Der Dienst kann entweder über den Webbrowser (» kompatible Browsermatrix) als Webclient, durch verfügbare Plugins für Microsoft Windows Explorer und Outlook oder als App für mobile Endgeräte (verfügbar durch dSmartdesk) verwendet werden. Diese Plugins können über den SWK bezogen werden. Eine REST/JSON Schnittstelle für den programmatischen Zugriff stellt Dataport gemäß Herstellerdokumentation ausgewählten Projekten zur Verfügung.

dDatabox ist eine kommerzielle Softwarelösung von SSP Europe GmbH, die anderweitig als „Secure Data Space“ und „Dracoon“ vermarktet wird. Dataport stellt als Art. 28 DSG-VO Auftragsverarbeiter den Dienst für die Dataport-Trägerländer zur Verfügung. Es muss ein Verarbeitungsauftrag zwischen Dataport und dem Auftraggeber abgeschlossen werden.

Begriffsdefinitionen

In dDatabox existieren die Konzepte von Nutzern, Gruppen und Datenräumen. Im Folgenden sollen diese und weitere Begriffe mit einer Gültigkeit für dieses Dokument belegt werden, so dass eine einheitliche Definition entsteht und der Verständlichkeit dienlich ist.

Auftraggeber: Ist ein Kunde von Dataport, beispielsweise in Form einer Behörde und gehört in der Regel zum FHH Netz. Der Auftraggeber kann über einen Datenverarbeitungsvertrag mit Dataport den Dienst dDatabox nutzen.

Mandant: Wenn Kunden als Auftraggeber den Dienst beauftragen, erhalten sie Zugriff auf die von Dataport betriebene reguläre Instanz von dDatabbox, die sie sich mit allen anderen Auftraggebern teilen. Alternativ können Kunden einen eigenen Mandanten beauftragen. Hierfür wird eine unabhängige dDatabox Instanz mit eigener URL und Branding für den Auftraggeber eingerichtet. Diese Instanz ist nicht an das jeweilige Trägerland, sondern an den Kunden selbst gekoppelt. Die unterliegende Infrastruktur ist die gleiche wie alle anderen dDataboxen.

Nutzer: Eine Person, die dDatabox entsprechend ihrer Zugriffsberechtigungen verwenden kann. Dies geschieht in der Regel über eine Client-Software, wie beispielsweise einem Webbrowser, kann aber durch den Einsatz der REST/JSON Schnittstelle programmatisch ausgestaltet werden. Im Unterschied zu externen Nutzern werden normale Nutzer über die Nutzerverwaltung innerhalb des Dienstes organisiert. Eine Anbindung an Verzeichnisdienste wie LDAP ist nicht vorgesehen. » Verweis Nutzer, Nutzerrollen und Nutzergruppen

Data Space: Die übergeordnete Umgebung des Dienstes, in der Datenräume angelegt werden können. Hier werden globale Einstellungen sowie Nutzer und Gruppen verwaltet. Einen Data Space erhält der Auftraggeber durch Beauftragung von Dataport und kann anschließend diesen nach seinen Bedürfnissen gestalten.

Datenraum: Oberste Ebene der organisatorischen Struktur des Dienstes. Einem Datenraum können Nutzer zugewiesen und Berechtigungen erteilt werden. » Verweis Datenraum

Datenraumadministrator: Rolle eines Nutzers innerhalb eines Datenraumes auf der Seite des Auftraggebers mit umfangreichen Konfigurationsberechtigungen für diesen Raum. » Verweis Datenraumadministrator

Data Space Administrator: Nutzer auf der Seite des Auftraggebers mit Konfigurationsberechtigungen für den Data Space. » Verweis Data Space Administrator

TripleCrypt®: Ist ein optionaler Mechanismus für die Ende-zu-Ende-Verschlüsselung der Dateien und ihrer Übertragung. Hierbei handelt es sich um eine Nutzer-zu-Nutzer Verschlüsselung, so dass die Dateien für den Betreiber verschlüsselt im Datenraum vorliegen.

Passwort: Wird als Zeichenkettenkombination als ein Faktor für den Nutzerlogin gebildet. Eine Passwortrichtlinie wird in der Regel zur Bildung verwendet.

Passphrase: Eine Zeichenkettenkombination, die verwendet wird, um den privaten Teil eines asymmetrischen Schlüssels durch Verschlüsselung zu schützen. Eine Passwortrichtlinie gilt auf für die Passphrase.

Datei: dDatabox wurde für den Austausch von Daten auf Basis von Dateien konzipiert. Wurden entsprechende Berechtigungen gesetzt, können Nutzer beliebige Dateien durch einen Upload zum Dienst in einen Datenraum hinzufügen und anschließend wieder herunter geladen werden. Optional kann der Nutzer beim Upload die Verfügbarkeit der Datei durch ein Ablaufdatum einschränken.

Datenräume

Der Dienst ist in Datenräume strukturiert, die Dataport in der Dokumentation mit Aktenschränken vergleicht. Es können beliebig viele Datenräume im isolierten Data Space eines Auftraggebers erstellt und in Ebenen in einander verschachtelt werden. Zur Strukturierung innerhalb eines Datenraums ist die Organisation von Dateien in Ordnern vorgesehen. Datenräume können mit Quotas zur Speicherplatzbegrenzung versehen werden. Dies wirkt sich auch unterliegende Datenräume und Ordner aus.

Nach der Einrichtung des Raumes muss mindestens ein Nutzer mit der Rolle des Datenraumadministrators für diesen Raum festgelegt werden. Dieser Administrator richtet den Raum durch die Wahl möglicher Einstellungen nach den gegebenen Bedürfnissen ein. Anschließend können reguläre Nutzer dem Raum zugewiesen werden. Berechtigungen (Nutzungsrechte) können einzelnen Nutzern und Nutzergruppen zugewiesen werden. Berechtigungen des aktuellen Raumes können auf Unterräume optional vererbt werden. Für jeden Raum stehen folgende Berechtigungen für Nutzer und Nutzergruppen individuell zur Verfügung:

- Datenraumadministrator: generelle Verwaltungsberechtigung des vorliegenden Datenraumes
- Löschen von Dateien und Ordnern
- Editieren von Dateien und Ordnern
- Erstellen von Dateien und Ordnern

- Lesen von Dateien und Ordnern
- Download-Freigaben verwalten
- Upload-Freigaben verwalten
- Papierkorb leeren und versionierte Dateien endgültig löschen
- Wiederherstellung von Dateien aus dem Papierkorb
- Lesenden Zugriff auf den Papierkorb

Papierkorb

Bei der Erstellung eines Datenraumes wird ein Papierkorb für diesen Datenraum erstellt. Eine Aktivierung des Papierkorbs ist für einen Datenraum optional. Wurde der Papierkorb während des Erstellvorgangs des Datenraums aktiviert, kann er für diesen Datenraum nicht wieder deaktiviert werden. Gelöschte Dateien werden zunächst in den Papierkorb verschoben und können von dort wiederhergestellt oder ganz gelöscht werden. Zusätzlich kann ein Zeitraum in Tagen eingestellt werden, nach dessen Ablauf die Dateien im Papierkorb automatisch gelöscht werden. Der Papierkorb unterstützt eine optionale Versionierung von Dateien, so dass mehrere Dateien mit gleichem Dateinamen darin abgelegt werden können.

Nutzer, Nutzerrollen und Nutzergruppen

Nutzer werden vom Auftraggeber und insbesondere von Administratoren mit Nutzerverwaltungsrechten verwaltet. Ein Nutzer wird anhand einer E-Mail Adresse, seinem Namen und einem optionalen Ablaufdatum erstellt. Hieraus ergibt sich keine Bindung an die Zugehörigkeit an die Organisation des Auftraggebers. Lediglich eine E-Mail Adresse wird für die Identifikation benötigt. Es besteht keine Möglichkeit zur Integration von dDatabox mit Verzeichnisdiensten, wie LDAP.

Rollen

Innerhalb von dDatabox existieren mehrere Rollen, die administrative Berechtigungen gestatten. Einzelne Nutzer und Nutzergruppen können mit einer solchen Rolle ausgestattet werden. Folgende Rollen sieht der Dienst vor:

- Konfigurations Manager: Festlegung globaler Systemeinstellungen
- Benutzer Manager: globale Benutzerverwaltung durch Anlegen, Bearbeiten und Löschen von Benutzern
- Gruppen Manager: Nutzergruppenverwaltung durch Anlegen, Bearbeiten und Löschen von Gruppen sowie dem Zuweisen von Nutzern zu Gruppen
- Data Room Manager: Datenräume anlegen, umbenennen und löschen sowie Speicherplatzbeschränkungen festlegen

- Protokoll Auditor: erlaubt Einsicht in das Systemprotokoll des Dienstes

Nutzergruppen

Es können beliebig viele Nutzergruppen durch Berechtigte in Form des Gruppen Managers erstellt werden. Diesen Nutzergruppen werden anschließend Nutzer als Gruppenmitglieder zugewiesen. Nutzergruppen haben zwei verschiedene Funktionen:

- Sie sind ein Mittel, um globale Berechtigungen durch Rollen zu erteilen.
    - Beispielsweise kann die Gruppe „Raum Manager“ die Rolle „Data Room Manager“ erhalten und somit allen Mitgliedern die Verwaltung von Datenräumen gestatten.

- Sie können einem oder mehreren Räumen zugewiesen werden und innerhalb dieser Räume ihren Mitgliedern die zur Verfügung stehenden Rechte eines Datenraumes gestatten (» Verweis Datenraum)
    - Die Gruppe „Referat A“ kann für Datenraum 1 allerdings andere Rechte zugewiesen bekommen als für Datenraum 2. Sie ermöglicht nur einer Sammlung von Nutzern für den jeweiligen Raum definierte Berechtigungen zuzuweisen.

Nutzer

Nutzer sind in der Regel normale Anwender des Dienstes auf der Seite des Auftraggebers. In folgendem sollen spezielle Nutzer hervorgehoben werden, die durch den Dienst festgelegte Berechtigungen durch die bestehenden Berechtigungsrollen erhalten:

Data Space Administrator
Wenn die dDatabox für einen Kunden durch Dataport eingerichtet und der Data Space erstellt wird, erfolgt auch die Erstellung eines initialen Nutzers, welches dem Kunden übergeben wird. Der Nutzer ist zu Beginn der Data Space Administrator und erhält alle verfügbaren Rollen und damit alle administrativen Berechtigungen auf dem Dienst. Diese Form des Administrators ist nicht auf einen Nutzer beschränkt und auch nicht auf diesen initialen Nutzer festgelegt. Alle administrativen Rollen können beliebigen anderen Nutzern zugewiesen werden und auch wieder von einem jeden Nutzer entfernt werden. Damit kann der initial erste angelegt Nutzer auch von der Funktion des Data Space Administrators entbunden werden.

Ein Data Space Administrator erhält nicht automatisch Zugriff auf jeden beliebigen Datenraum und die darin enthaltenen Daten. Ein Nutzer mit allen administrativen Rollen muss dennoch einem jeden Datenraum als Nutzer zugewiesen werden, um darauf zugreifen zu können.

Systemweite administrative Berechtigungen werden als technisches Verfahrensmanagement durch Dataport wahrgenommen. Die Verantwortung liegt hierfür bei Dataport. Es wird innerhalb von dDatabox ein spezielles Administratorkonto verwendet, welches bei Dataport durch 3 Personen in dieser Funktion Unterstützung findet. Für die Administration der involvierten Systeme wird eine 2-Faktor-Authentisierung verwendet.

Datenraumadministrator
Der Datenraumadministrator ist regelhaft ein Mitarbeiter des Auftraggebers und hat alle verfügbaren Berechtigungsrollen für den jeweiligen Datenraum inne. Der Administrator richtet den Raum entsprechend den Anforderungen des Auftraggebers ein und muss beispielsweise über die Verwendung von TripleCrypt® entscheiden, bevor eine erste Datei in dem Datenraum abgelegt wird. Durch das Hinzufügen von Nutzern wird der Datenraum für die Verwendung freigegeben.

Die Rolle des Datenraumadministrators befindet sich wie alle weiteren Rollen im Verantwortungsbereich des Auftraggebers. Es handelt sich bei diesem Nutzer um ein normales Nutzerkonto mit der zusätzlichen Rolle des Administrators für einen oder mehrere Datenräume, der für die betreffenden Datenräume mit folgenden Berechtigungen zur Verwaltung ausgestattet ist:

- Anlegen, Umbenennen und Löschen von untergeordneten Datenräumen innerhalb des jeweiligen Datenraums
- Festlegung von Speicherplatzbeschränkungen für untergeordnete Datenräume
- Hinzufügen und Entfernen von Nutzern zu bzw. aus dem Datenraum. Nutzer sind zuvor von einem Administrator mit dem Berechtigungen zur Nutzerverwaltung anzulegen.
- Vergabe von Berechtigungen innerhalb des jeweiligen Datenraums inklusive Ernennung von weiteren Datenraumadministratoren
- Aktivierung von TripleCrypt® für den Datenraum.
- Protokoll Auditor Berechtigungen

Datenraumnutzer
Die normale Benutzerrolle zur Verwendung von dDatabox im Verantwortungsbereich des Auftraggebers. Rollen werden global und Datenraumberechtigungen werden durch Gruppen oder Direktzuweisung innerhalb von Datenräumen einem Nutzer zuge-

wiesen. Bei der Erstellung eines Nutzers oder eines Datenraums besteht keine Vorselektierung von Rollen und Berechtigungen, so dass jede einzelne Berechtigung durch den Administrator aktiviert werden muss. Jedoch kann sich eine Vorauswahl durch die mögliche Vererbung von Berechtigungen aus dem darüber liegenden Datenraum eine Vorauswahl ergeben.

Download-Freigabe-Empfänger
Um für externe Nutzer außerhalb des FHH-Netzes Dateien bereitstellen zu können, muss kein dediziertes Nutzerkonto angelegt werden. Eine Download-Freigabe für einzelne Dateien, Ordner oder ganze Datenräume kann durch Datenraumnutzer erstellt und als eindeutige Adresse (URL) versendet werden. Über diese Adresse erhält eine externe Person Zugriff auf die jeweiligen Dateien. Optional kann eine Download-Freigabe durch ein Freigabekennwort geschützt werden. Durch Festlegen eines Ablaufdatums kann die Freigabe zeitlich begrenzt werden.

Bei aktivierter TripleCrypt®-Verschlüsselung des Datenraums ist nur die Freigabe einzelner Dateien möglich. In diesem Fall ist die Verwendung eines Freigabepasswortes in Form einer Passphrase obligatorisch und die Ende-zu-Ende-Verschlüsselung bleibt intakt. Das Freigabekennwort ermöglicht externen Nutzern die Verwendung der zugrundeliegenden asymmetrischen Verschlüsselung der Dateischlüssel, da durch den freigebenden Nutzer für diese Freigabe ein neues asymmetrisches Schlüsselpaar erzeugt wird. Die auszutauschende Datei wird erst auf dem Client (Browser) des externen Nutzers dechiffriert.

Über die Verwaltung von Freigaben können Nutzer des Datenraumes die Anzahl der bisherigen Downloads einer Dateifreigabe ermitteln. Eine maximale Anzahl von möglichen Downloads lässt sich zur Einschränkung einer Freigabe einstellen.

Upload-Konto
Für einen bidirektionalen Dateiaustausch mit externen Nutzern ist neben der Download-Freigabe auch eine Dateianfrage (Upload-Freigabe) durch das Erzeugen eines zweckbestimmten Links möglich. Der Empfänger des Links erhält die Möglichkeit, Dateien dem Datenraum hinzuzufügen. Einschränkende Optionen durch Passwortabfrage, Ablaufdatum der Freigabe und Speicherplatzbegrenzung für den Upload stehen dem einrichtenden Nutzer zur Verfügung.

Protokoll Auditor
Nutzer mit dieser Rolle erhalten innerhalb der webbrowserbasierten dDatabox-Anwendung Lesezugriff auf die Protokolldaten. Diese beziehen sich entweder auf den ganzen Data Space, so dass alle Interaktionen in allen Datenräumen aufgelistet wer-

den, oder aber nur auf die Protokollierung innerhalb eines Datenraumes. Hierbei entscheidet die Berechtigung durch die administrative Rolle des Data Spaces oder die Aktivierung der Protokollierung innerhalb eines Datenraumes zusammen mit der Berechtigung des Nutzers auf die Möglichkeit zur Einsichtnahme.

Auch bei keiner Aktivierung der Protokollierung in einem Datenraum werden bei allen Nutzerinteraktionen in diesem Datenraum Protokolleinträge erzeugt und in der systemweiten Übersicht des Dienstes für administrative Nutzer mit der Rolle Protokoll Auditor angezeigt. Ein ausschließen von Einträgen für bestimmte Räume oder Nutzer ist nicht möglich.

Sitzungen

Vor der Verwendung von dDatabox muss sich ein Nutzer zunächst mit Nutzername und Passwort anmelden. Anmeldungsvorgänge werden überwacht und drei fehlgeschlagene Anmeldungsversuche führen zu einer temporären Sperrung von 5 Minuten. Bei der Verwendung des Webclients wird bei jeder Interaktion mit dem Dienst ein Session Token aufgefrischt, der nach 120 Minuten Inaktivität abläuft und anschließend ein erneutes Anmelden erforderlich macht.

Für die Nutzung von dDatabox steht für alle der Webclient zur Verfügung, der den gänzlichen Funktionsumfang abbildet. Zusätzlich kann durch Dataport ein Plugin für den Microsoft Windows Explorer installiert werden, um eine ähnliche Handhabung wie im lokalen Dateimanager für die Ordner und Dateien in einem Datenraum zu erreichen. Für Microsoft Outlook kann ein Add-In verwendet werden, um leichter Links für Download-Freigaben und Upload-Konten im Datenraum per E-Mail versenden zu können. Dataport stellt zudem Client-Anwendungen für mobile Endgeräte für iOS und Android zur Verfügung; auch unter dSmartDesk.

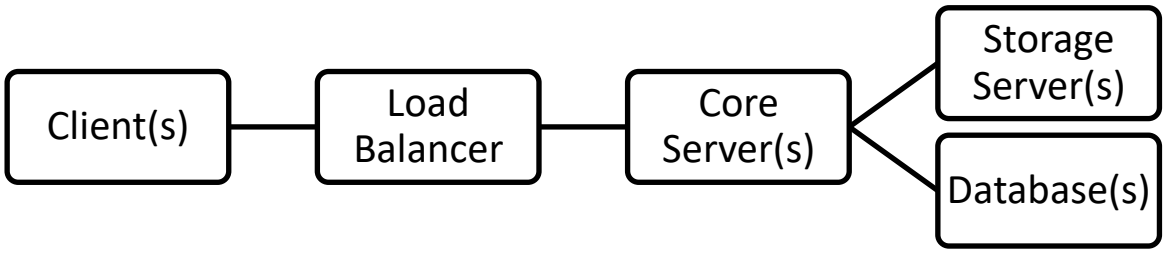
Ein externer Nutzer, der ein Empfänger einer Download-Freigabe oder Upload-Freigabe ist, wird nach dem Aufruf des zugehörigen Links zur Eingabe des Freigabepasswortes aufgefordert. Anschließend hat dieser externe Nutzer die Möglichkeit auf einer minimalen Webseite die vorgegebene Download- oder Upload-Funktion durchzuführen.

Absicherung von Nutzerkonten

Ein Nutzerkonto besteht aus Nutzername und Passwort. Es existiert eine Passwortrichtlinie, die eine Mindestzeichenlänge von 8 Zeichen, Groß- und Kleinschreibung und mindestens ein Sonderzeichen vorschreibt. Dataport gibt in der Dokumentation an, Login-Passwörter unter Einbeziehung von Salting, Peppering und Iterations mit bcrypt-Funktionen zu hashen und anschließend zu speichern.

Infrastruktur

Die Architektur von dDatabox besteht aus einem oder mehreren Servern, die über einen Load Balancer als ein Dienst nach außen hin angesprochen werden. Die Server können abhängig von ihrer Last skaliert werden und sind an weitere Datenbank- und Storage-Server angebunden. Letztere persistieren die Metadaten von Nutzern und Daten sowie die eigentlich abgelegten Daten in einem Datenraum.



Abfrageverlauf eines Nutzers von links nach rechts. Einheiten mit (s) können als mehrfache Instanzen vorkommen.

Mandantentrennung

Für alle Auftraggeber innerhalb einer Mandanten-Instanz des Dienstes wird eine gemeinsame Installation des Dienstes verwendet. Eine Trennung der Daten unterschiedlicher Auftraggeber erfolgt über applikationsgesteuerte Logik. Es werden alle Metadaten in der gleichen Datenbank über einen Auftraggeber-Identifikationsbezeichner, als ID bezeichnet, geführt. Eine Trennung und damit eine Entscheidung über Zugriffsrechte löst man über die Vergabe und Zuordnung von Nutzern über verschiedene IDs innerhalb der Datenbank. Es findet also eine Trennung durch Software-Logik innerhalb der Anwendung statt.

Diese Auftraggeber-ID wird zur Speicherung der eigentlichen Dateien im Dateisystem durch Aufteilung in Unterordnern verwendet.

Der Auftraggeber kann Dataport zur Erstellung eines eigenen Mandanten veranlassen. Damit wird eine dedizierte Instanz des Dienstes zur Verfügung gestellt, deren Datentrennung von anderen Kunden Dataports über die Ebene der Anwendungslogik hinaus reicht. Allerdings wird diese Instanz auf der gleichen Infrastruktur betrieben.

Für den Einsatz von dDatabox kann Art. 26 der DSG-VO angewendet werden. Zum einen besteht eine gemeinsame Verantwortlichkeit von Auftraggeber und Dataport als Dienstleister. Die Verantwortlichkeiten und die daraus resultierenden Aufgaben lassen sich gut trennen und werden im Abschnitt Verantwortlichkeitsverteilung aufgeführt.

Eine gemeinsame Verantwortlichkeit der verschiedenen Auftraggeber untereinander schließt Dataport jedoch aus, da die Trennung auf Logikebene zu keinem Zeitpunkt eine Berührung der Nutzer verschiedener Data Spaces erlaubt.

Stetige Verschlüsselung

Transportverschlüsselung

Bei der Verwendung von dDatabox findet eine erzwungene Transportverschlüsselung in Form von TLS 1.2 und höher statt. Nach Angaben von Dataport wird diese Verschlüsselung auf einem, dem Dienst vorgeschalteten Application Layer Gateway in Form eines Apache Webservers terminiert.

Datenverschlüsselung auf dem Storage-Server

Alle in Datenräumen abgelegten Daten werden in einem mit AES-256 verschlüsselten Dateisystem auf den dDatabox-Servern gespeichert. Dies dient laut Dataport dem Schutz bei einem unwahrscheinlichen Fall eines Einbruchs im Rechenzentrum mit Zugriff auf die Hardware, so dass keine schnell brauchbaren Daten erbeutet werden können. Die angewendete Verschlüsselung entspricht den Standardmaßnahmen der von Dataport genutzten RZ² Rechenzentren. Bei der Auswahl geeigneter Algorithmen und Produkte wurde auf die Anforderungen (M 2.162, M 2.163, M 2.164, M 2.165) des Grundschutzkatalogs aus dem Jahr 2016 eingegangen.

Neben dem Storage-Server werden auch Meta-Daten in einer Datenbank mit AES-256 verschlüsselt. Dafür wird der eingebaute Krypto-Mechanismus der eingesetzten Datenbank verwendet. Snapshots und Backups der Datenbank werden verschlüsselt angefertigt. Die Schlüsselverwaltung für die Datenbank findet über das Datenbankmanagementsystem und der Speicherung des Master Keys auf einem externen USB-Stick statt. Dieser Stick wird für das initiale Starten der Datenbank benötigt.

Die eingesetzten Verschlüsselungen von Dateisystemen als auch der verwendeten Datenbanken entsprechen dem Standardverfahren in den RZ² Rechenzentren und bedürfen keine Sonderbehandlung. Diese dafür verwendeten Master Keys werden vom technischen Verfahrensmanagement verschlüsselt abgelegt und aufbewahrt.

Eine Abgrenzung vom Standardverfahren und ein zusätzlicher Gewinn an Sicherheit kann durch TripleCrypt® erreicht werden.

Optionale Verschlüsselung durch TripleCrypt®

Für einen Datenraum kann der Datenraumadministrator die Verwendung von TripleCrypt® einrichten. Diese Funktion muss zuvor für die gänzliche dDatabox Umgebung des Auftraggebers aktiviert werden. Anschließend kann für neue Datenräume, die nach der Aktivierung erstellt wurden, jeweils dieser Schutz angeschaltet werden. Unterräume erhalten automatisch ein aktiviertes TripleCrypt®, wenn in ihrem übergeordneten Datenraum dies angeschaltet wurde.

Vor der erstmaligen Verwendung des Datenraumes wird für jeden Nutzer des Raumes ein asymmetrisches RSA-2048Bit Schlüsselpaar generiert. Der Nutzer wird dazu aufgefordert, eine Passphrase zu wählen, mit dem der private Teil des asymmetrischen Schlüssels mittels PBKDF2 und AES-256 chiffriert wird.

Anschließend wird der öffentliche Schlüssel zusammen mit dem verschlüsselten privaten Schlüssel in die dDatabox geladen und dort in einer Datenbank abgelegt. Der Dienst nimmt damit dem Nutzer eine notwendige Synchronisierung der Schlüssel mit seinen weiteren verwendeten Clients und Geräten ab.

Bei der Erstellung der Passphrase für den privaten Schlüssel wird nicht vom Dienst geprüft, ob die gewählte Zeichenkette sich vom Login-Passwort des dDatabox-Nutzerkontos unterscheidet. Da die Passwörter unterschiedlich behandelt werden und Dienst oder Dienstleister zu keiner Zeit Informationen zur Passphrase des privaten Schlüssels eines Nutzers erlangen („Zero-Knowledge-Policy“), kann keine Überprüfung auf Gleichheit seitens des Dienstes stattfinden. Eine geeignete Passwortrichtlinie und deren Einhaltung muss auf Seite des Auftraggebers etabliert sein.

Aus diesem Grund kann bei Verlust der Passphrase auch kein Zurücksetzen dessen erfolgen. Vielmehr kann ein neues Schlüsselpaar erzeugt werden und in allen genutzten Datenräumen erneut bereitgestellt werden. In diesem Fall muss der Nutzer für jeden Datenraum von den entsprechenden Datenraumadministratoren mit seinem neuen Schlüsselpaar erneut autorisiert werden. Ist der Nutzer im Falle eines Verlustes der Passphrase der einzige Nutzer eines Datenraums, werden die verschlüsselten Daten als verloren angesehen, da ohne die Kenntnis der Passphrase die Verschlüsselung der Daten ohne erheblichen Aufwand nicht rückgängig gemacht werden kann.

Passwortrichtlinie

Der Dienst setzt folgende Anforderungen an Passwörter um:

- Mindestlänge von 8 Zeichen
- Buchstaben und Ziffern
- Groß- und Kleinbuchstaben müssen enthalten sein
- Mindestens 1 Sonderzeichen muss enthalten sein

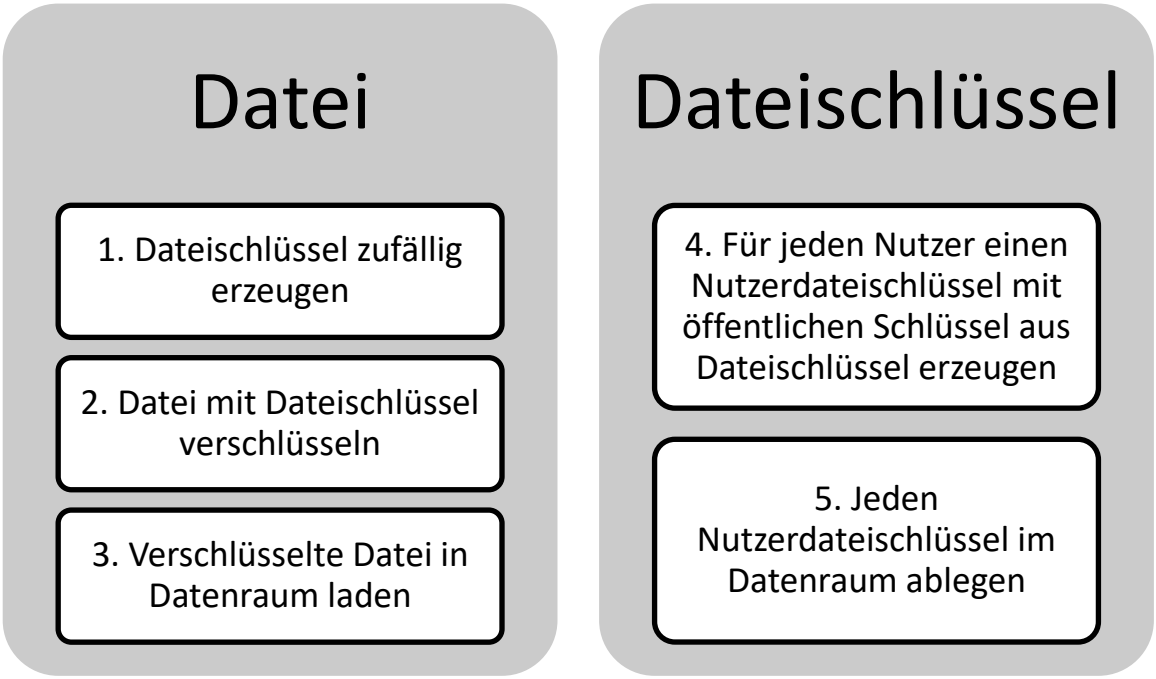
Rescue Key

Um im Falle eines Verlustes der Passphrase aller Teilnehmer eines Datenraums dennoch an die Daten zu gelangen, kann optional ein Rettungsschlüssel (auch „System-Notfallkennwort“ genannt) eingerichtet werden. Solch ein Rettungsschlüssel wird bei der Aktivierung von TripleCrypt® vom Data Space Administrator erstellt und kann dann beim Einrichten eines Datenraums vom Datenraumadministrator für den jeweiligen Raum eingetragen werden. Alternativ kann der Datenraumadministrator für einen Raum einen individuellen Rettungsschlüssel einrichten. In beiden Fällen empfiehlt Dataport eine sichere Aufbewahrung der Passphrase des Rettungsschlüssels beispielsweise in einem Tresor. Dataport selbst handhabt die eigene Schlüsselverwaltung nach zentralen Richtlinien.

Die Funktionsweise des Rettungsschlüssels ist identisch zu den normalen Schlüsseln. Auch hier wird ein asymmetrisches Schlüsselpaar erzeugt und für jede dem Datenraum hinzugefügte Datei wird zusätzlich ein Dateischlüssel für den Rettungsschlüssel erstellt. Der Datenraumadministrator hat durch diesen Schlüssel die Möglichkeit, auf die Daten eines Raumes zuzugreifen, für die er ohne Rettungsschlüssel bei entsprechender Rechtevergabe keinen Zugriff hätte. In den Richtlinien zur Nutzung von dDatabox sollte der Auftraggeber seine Nutzer darauf hinweisen, keine Rettungsschlüssel für Daten mit hohem Schutzbedarf in den Datenraum einzutragen, um Zugriff durch Dritte zu unterbinden.

Bereitstellen einer verschlüsselten Datei

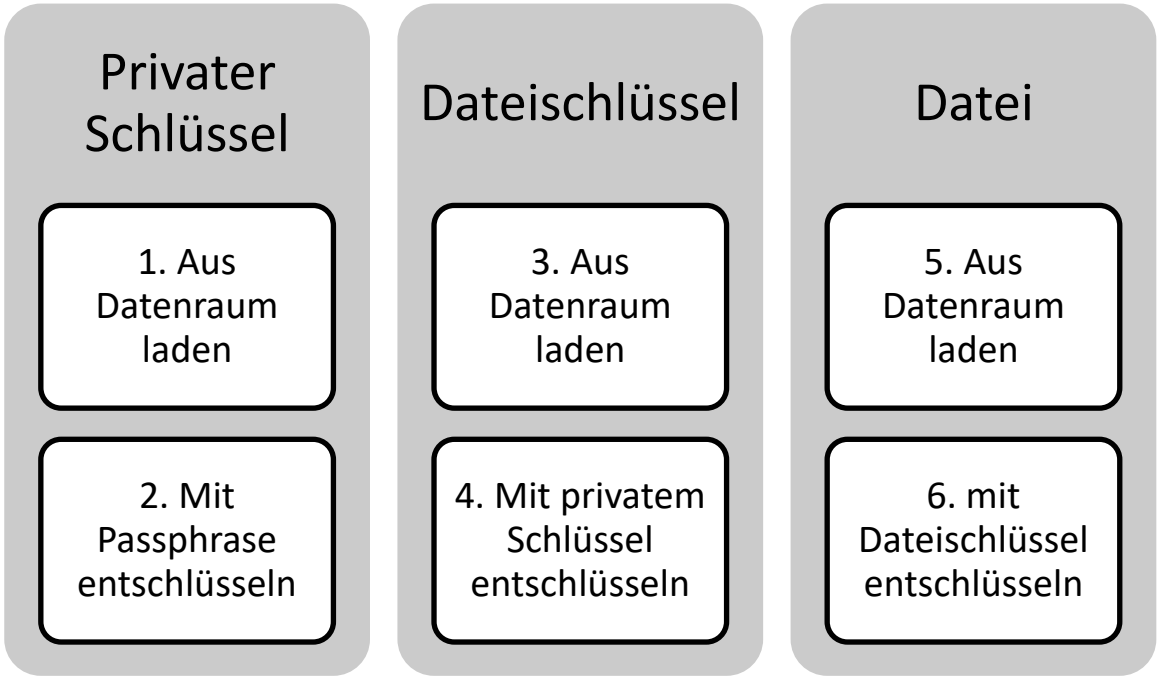
Der Datenraum mit aktiviertem TripleCrypt® wird von den Nutzern Alice, Bob und Carola genutzt. Wenn Alice eine Datei im Datenraum bereitstellt, wird zunächst ein zufälliger symmetrischer AES-256 Schlüssel erzeugt, der als Dateischlüssel bezeichnet wird. Mit ihm wird die Datei verschlüsselt und in den Datenraum übertragen. Anschließend werden die öffentlichen Schlüssel von Alice, Bob und Carola aus dem Datenraum geladen. Vom Dateischlüssel wird nun für jeden Nutzer des Datenraums eine individuelle Version durch Verschlüsselung mit dem öffentlichen Schlüssel des jeweiligen Nutzers erzeugt. Diese Version wird als Nutzerdateischlüssel bezeichnet und anschließend ebenfalls im Datenraum gesichert. Die Bereitstellung der Datei im Datenraum ist nun abgeschlossen. Der ursprüngliche Dateischlüssel wird in seiner unverschlüsselten Form nicht an den Dienst übertragen und vom Client nach der Bereitstellung entfernt.



Von links nach rechts: Prozess des Hinzufügens einer Datei in einen Datenraum.

Abrufen einer verschlüsselten Datei

Carola möchte die Datei von Alice aus dem TripleCrypt® gesicherten Datenraum auf ihr Gerät laden und den Inhalt lesen. Zunächst entnimmt Carolas Client ihren verschlüsselten privaten Schlüssel dem Datenraum. Carola entschlüsselt diesen mit der Eingabe ihrer Passphrase. Dann kann Carolas Nutzerdateischlüssel für die gewünschte Datei aus dem Datenraum laden und mit Hilfe ihres privaten Schlüssels zum Dateischlüssel entschlüsseln. Mit diesem kann nun die Datei aus dem Datenraum geladen und lokal entschlüsselt werden. Nun ist es Carola möglich, die Datei zu öffnen und den Inhalt zu lesen.



Von links nach rechts: Prozess des Abrufens einer Datei aus einem Datenraum.

Protokollierung

Einträge für die Protokollierung werden aus zwei Quellen erzeugt. Zum einen dienen die Standard-Log-Einträge der Systemkomponenten Datenbank, Apache Webserver und Tomcat Applikationsserver einer Systemprotokollierung, die auf Anfrage und im Fehlerfall von Dataport ausgewertet werden. Auftraggeber erhalten keinen Zugriff. Alle administrativen Tätigkeiten werden protokolliert und regelmäßigen Revisionen unterzogen. Zusätzlich protokolliert Dataport übergreifend über alle dDatabox Instanzen und Mandanten alle Login-Fehlversuche. Diese Systemprotokolle werden für 30 Tage gespeichert.

Als zweite Quelle dient die dDatabox-Anwendung selbst und protokolliert alle Zugriffe auf Daten. Diese Protokolleinträge werden in die Datenbank geschrieben und optional in einem dritten System hinterlegt, wie beispielsweise einem angeschlossenen Syslog-Dienst. Während die Datenbankadministratoren von Dataport diese Einträge ungefiltert einsehen können, unterstützt die dDatabox-Anwendung die Einsicht für Nutzer des Dienstes mit der Berechtigung „Log Auditor“ in für ihnen zugewiesenen Datenräumen bzw. im Falle der administrativen Rolle für den gesamten Data Space. Der Verantwortungsbereich für die Überprüfung dieser Protokolleinträge innerhalb der Anwendung liegt beim Auftraggeber.

Protokolleinträge werden laut Dataport revisionssicher für eine Speicherdauer von 90 Tagen aufbewahrt. Da die Einträge in einer Datenbank gesammelt werden, sind sie für Nutzer auf Seite des Auftraggebers nicht veränderbar. Die Speicherdauer ist für gesonderte Mandanten-Instanzen abweichend von der des Basismandanten auf Wunsch des Auftraggebers anpassbar.

Protokolleinträge auf System- als auch Anwendungsebene weisen keine Nutzerdaten in Form von IP-Adressen auf.

Löschen

Ein festlegbares Ablaufdatum für Nutzer, Dateien und Freigaben verhindert einen regulären Zugriff von Nutzern außerhalb eines Fristzeitraumes. Bei Austausch des Datenträgers kommt ein Dataport-weites Löschkonzept durch mehrmaliges Beschreiben mit Zufallsdaten oder Vernichtung des Datenträgers gemäß den Empfehlungen des BSI zur Anwendung. Es gelten die etablierten Löschkonzepte und Richtlinien der Dataport Rechenzentren RZ².

Die Protokollierung erzeugt weitere Transparenz im Löschprozess.

Schutzbedarf

Dataport betreibt den Dienst auf eigener Infrastruktur im Bereich „Shared Basis“ im Sicherheitsbereich „Standardsicherheit“. Der Dienst selbst wird von Dataport mit einem Schutzbedarf „Hoch“ betrieben. Im Einzelnen sind die Schutzziele mit folgendem Schutzbedarf festgelegt:

- Verfügbarkeit: normal
- Vertraulichkeit: hoch
- Integrität: hoch

Der Dienst wird zusammen mit anderer Software in einer Umgebung betrieben, die einige Empfehlungen des BSI Grundschutzes mit hohem und sehr hohem Schutzbedarf nachkommt. Die Dokumentation des Dienstes datiert auf 2017 und enthält keine Betrachtungen auf DSGVO Niveau. Der Umgang mit den Gewährleistungszielen des Datenschutzes kann mit folgenden Maßnahmen interpretiert werden:

- Verfügbarkeit
  - Der Dienst wird in den Dataport RZ² Rechenzentren betrieben und unterliegt den SLAs der Dienste der „Shared Basis“ Umgebung.

- Datenminimierung
  - Die erzeugten Metadaten dienen nur dem Ziel des verschlüsselten Dateiaustausches mit internen und externen Nutzern. Lediglich in der Protokollierung werden Interaktionen eines Nutzers mit dem Dienst gespeichert.
- Integrität
  - Eine unberechtigte Manipulation der Daten wird durch den Einsatz einer Ende-zu-Ende-Verschlüsselung erschwert.
  - Es findet keine Datensicherung innerhalb des Dienstes statt.
- Vertraulichkeit
  - Anwendbarkeit einer Ende-zu-Ende-Verschlüsselung durch TripleCrypt®
- Nichtverkettung
  - Der Betreiber wertet Protokolleinträge nur aus Gründen der Fehlerbeseitigung aus.
- Transparenz
  - Protokolleinsicht durch Log Auditor Nutzerrolle auf Seite des Auftraggebers
- Intervenierbarkeit
  - Der Dienst verfolgt das Konzept des Datenaustausches. Der Auftraggeber ist insbesondere bei Einsatz von TripleCrypt® alleiniger Entscheider, wer auf die Daten Zugriff erhält und wie lange diese zur Verfügung stehen.

Nach der für den Betrieb des Dienstes durchgeführten Sicherheits- und Risikoanalyse kommt Dataport zu folgenden Maßnahmen zur Reduktion der identifizierten Risiken:

- Die gespeicherten Daten auf dem Server sind immer verschlüsselt. Es wird stets eine Transportverschlüsselung verwendet. Alle Sicherheitsvorkehrungen der von Dataport genutzten Rechenzentren, deren Infrastruktur einen hohen Schutzbedarf auch für Basisdienste bietet, gelten auch für dDatabox. Die Verschlüsselung auf dem Client (Ende-zu-Ende-Verschlüsselung) ist optional und muss vom Auftraggeber aktiviert werden.
- Transparenz: durch Protokollierung auf zwei Ebenen erlangt der Auftraggeber durch Prüfmöglichkeit über alle Interaktionen mit seinen Datenräumen innerhalb der Anwendung.
- Mandantentrennung auf technischer Basis im Application Server (erfüllt M 2.549); Empfohlene Trennung auf beispielsweise der Ebene des File-Services oder Datenbank findet nicht statt. (SYS.1.8.A15)
- Rechte- und Rollenkonzept für Dataport als auch Nutzer des Auftraggebers
- Schulung vor Programmnutzung durch Dokumentation und sicherheitsrelevanten Hinweisen (M 3.4)
- Das zugrunde liegende Produkt Secure Data Space von SSP Europe GmbH ist sicherheitsüberprüft. Der Hersteller listet auf seiner Webseite folgende Zertifizierungen mit Prüfbericht:

  - Anforderungskatalog Cloud Computing (C5) des BSI geprüft durch PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (2019)
  - ISO/IEC 27001:2013-Zertifikat geprüft durch TÜV Rheinland (2020)
  - IDW PS 951 geprüft durch PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (2019)
- Zweckbindung: der Dienst erfüllt die Funktion des sicheren Dateiaustauschs für den Auftraggeber und bringt keine weitere Funktionalität mit sich, die dem Betreiber gestattet, anderweitig die Daten zu verwenden.

Dataport bietet dDatabox für Daten mit hohem Schutzbedarf an, in dem der Dienst in einer normalen „Shared Basis" betrieben wird und sich von anderen Diensten in dieser Umgebung nur durch das optionale TripleCrypt® absichern lässt.

Verantwortungsverteilung

Dataport tritt als Auftragsverarbeiter mit dDatabox auf. Hieraus ergeben sich unterschiedliche Verantwortungsbereiche, die sich sowohl beim Auftraggeber als auch bei Dataport befinden. Der Verantwortliche des Auftraggebers wird vor der Nutzung des Dienstes über Sicherheitsweise und mit Anleitungsdokumenten informiert.

Verantwortungsbereiche des Auftraggebers

- Laut Kundenhinweis seitens Dataport hat der Benutzer aktuelle Browserversionen und aktuelle Betriebssysteme einzusetzen.
- Die Form und Art der in der dDatabox ausgetauschten Daten. Die Datenschutzbedingungen des jeweiligen Landes sind zu beachten und mit dem Datenschützer die Rahmenbedingungen zu klären. Dataport unterstützt bei Bedarf bei der Klärung.
- Obwohl die Dateien eines unverschlüsselten Datenraumes nach dem Hochladen von Dataport nach Viren geprüft werden, kann dieser Schutz nicht für verschlüsselte Datenräume erfolgen. Für einen Virenschutz der ausgetauschten Daten auf Clientgeräten hat der Auftraggeber zu sorgen.
- Die Software auf Clientgeräten stellt laut Dataport das größte Angriffspotential dar. Die Verwaltung und Absicherung liegt beim Auftraggeber. Es wird der Einsatz von zentral verwalteten Geräten empfohlen.
- Der Dienst dDatabox erfüllt keine Funktion der Datensicherung. Bei versehentlichem Löschen oder unerwartetem Hardware- bzw. Datenträgerdefekt ist der Auftraggeber für eine Sicherungskopie der Dateien zuständig.
- Die regelmäßige Prüfung und Kontrolle der Auftraggeber-Protokolleinträge durch den Datenraumadministrator ist durchzuführen. Die Protokolle enthalten

personenbezogene Daten und sind entsprechend datenschutzrechtlich zu behandeln. Die Nutzer des Dienstes sind vom Verantwortlichen des Auftraggebers zuvor darüber zu informieren.
- Die Aktivierung von TripleCrypt® für Datenräume obliegt dem Auftraggeber. Die Handhabung und die sichere Aufbewahrung von Schlüsseln und Rettungsschlüsseln obliegen dem Auftraggeber.
- Die Nutzerverwaltung und granulare Zugriffsberechtigung wird durch den Auftraggeber gesteuert. Die Verwendung eines Ablaufdatums für Benutzer, Freigaben und Dateien kann die Sicherheit erhöhen.
- Erstellung und Einhalten von internen Passwortrichtlinien, die das Verwenden eines identischen Passworts für Nutzer-Login und Passphrase für die Verschlüsselung verbietet. Zusätzlich sollte das Erstellen und der Umgang mit Rettungsschlüsseln und Freigabepasswörtern geregelt werden.

Verantwortungsbereich Dataport

- Kontinuierlicher und selbstständiger Betrieb des Dienstes dDatabox wird durch Dataport gewährleistet. Eine Bereitstellung der Infrastruktur ist mit einer Verfügbarkeit von 95% bei einem 24/7 Betrieb vorgesehen.
- Durchführen von Aktualisierungen der Software des Dienstes. Der Hersteller ist laut Dataport in regem Kontakt mit der Community und liefert zügig Lösungen beim Auftreten von Problemen. Dataport spielt die aktuellste Version der dDatabox Software zeitnah ein.
- In Abhängigkeit vom festgelegten Schutzbedarf trifft Dataport Schutzmaßnahmen im Sinne des BSI Grundschutzhandbuches. Diese Maßnahmen sind auf dem Stand der Technik zu halten. Dafür wurde ein Sicherheitskonzept erstellt, welches auch Veränderungen und Migrationen innerhalb des Systems beinhaltet.
- Integration der Dataport Mitarbeiter durch regelmäßige Schulungen und Sensibilisierung für Sicherheitsrichtlinien.
- Regelmäßige Kontrollen zur Aufrechterhaltung der Informationssicherheit
- Ausschöpfen von Möglichkeiten zum Schutz des Dienstes vor Angriffen von außen, beispielsweise Bruteforce-Login-Versuchen oder Denial of Service.

Außerordentliche Zugriffsszenarien

Um außer der Regel auf Daten zugreifen zu können, benötigt ein Angreifer neben Direktzugriff auf das Dateisystem und dem Schlüssel zur Entschlüsselung der Daten auch Zugriff auf die Datenbank, um einer Zuordnung der Daten zu einem Mandanten

und Datenraum herstellen zu können. Die Daten werden im Dateisystem in einer Ordnerstruktur durch Auftraggeber-ID und Nummerierungen abgelegt. Aus der im Dateisystem vorliegenden Auftraggeber-ID kann ohne Zugriff auf die Datenbank keine Zugehörigkeit zu einem Auftraggeber generiert werden.

Im Falle eines fehlerhaften Verhaltens der Software wäre ein Zugriff auf Daten oder Protokolleinträge fremder Nutzer denkbar. In diesem Szenario ist der Einsatz einer Ende-zu-Ende-Verschlüsselung ein Schutz vor dem Verlust der Vertraulichkeit. Ein Datenverlust kann durch mögliche Schreibzugriffe durch Dritte nicht ausgeschlossen werden. Eine Backup-Funktionalität innerhalb des Dienstes ist durch Dataport nicht vorgesehen.

Abschließende Betrachtungen

Nach der Beschreibung des Dienstes sollen einige Aspekte des Dienstes auf Datensicherheit und Datenschutzkriterien diskutiert werden:

Mandantentrennung

Die Mandantentrennung auf Anwendungsebene ist laut nach BSI Grundschutz Kompendium ausreichend, wenn auch Vorschläge wie isolierte Dateispeicherung in dedizierten Dateisystemen oder File-Services nicht beachtet oder nicht beschrieben werden. Die Berechtigungsfreigabe für Mandanten gilt als abgeschlossen. Mit ihr soll verhindert werden, dass beispielsweise Nutzer von Mandant A Zugriffsrechte auf Datenräume von Mandant B erhalten. Diese basiert auf der Annahme der korrekten Funktion der Mandantentrennung durch die fehlerfreie Funktion der Logik des Anwendungsservers. Im Falle eines Fehlers und der damit vorstellbaren Vermischung von Zugriffsberechtigungen auf fremde Ordner wirkt die optionale Ende-zu-Ende-Verschlüsselung als ausreichender Schutz für die Gewährleistung der Vertraulichkeit.

Transparenz

Die Protokollierung schafft eine notwendige Transparenz für Auftraggeber des Dienstes und bringt für den Anwender eine Revisionssicherheit. In wie weit das Manipulieren von Protokolleinträgen durch Dataport Administratoren mit Zugriff auf Protokollsystemen und Datenbank innerhalb von Dataport auffällt, kann nur durch eine regelmäßige Überprüfung der internen Protokollierung geschehen. Dies gilt aber für jeden Dienst, der in den RZ² Rechenzentren betrieben wird.

Anhand der Protokollierung von Interaktionen in Datenräumen können Nutzer mit der administrativen Rolle des „Log Auditor“ Rückschlüsse über die Daten in diesen Datenräumen erlangen, auch wenn sie keine Zugriffsberechtigung für diese Datenräume besitzen.

Mangelnde Übersicht an Zugriffsrechten

Da Datenraumberechtigungen über Gruppen als auch direkt an Nutzer vergeben werden können, sind mehrschichtige Zugriffsberechtigungen möglich. Eine direkte Auflistung aller Nutzer mit Berechtigungen auf einen Datenraum bietet die vorliegende Version des Dienstes nicht. Neben der Liste der Nutzer mit Direktzugriff müsste jede einzelne zugewiesene Nutzergruppe überprüft werden.

Hier liegt ein Gefahrenpotential für eine unbeabsichtigte Freigabe an unbefugte Nutzer innerhalb der Organisation des Auftraggebers. Die Verwendung von dDatabox erfordert ein stark ausgeprägtes Konzept in der Nutzer- und Gruppenverwaltung und eine hohe Disziplin, dies auch einzuhalten.

Datenaustausch

Die Freigabesteuerung für externe Nutzer ist durch Passwortvergabe und Einschränkung auf Downloadanzahl und Zeitraum ausreichend gesichert, wenn der Verantwortliche für die Übermittlung von Adresse und Passwort an den externen Nutzer nicht den gleichen Kommunikationskanal (zBsp. E-Mail) verwendet. Eine 2-Faktor-Authentisierung bei Freigaben ist ohne Nutzerkonto für externe Nutzer nicht möglich. Für die Verwendung des Dienstes für Daten mit hohem Schutzbedarf sollte gemäß BSI Grundschutzkompendium (ORP.4.A21) eine solche Authentisierung realisiert werden. In der vorliegenden Version unterstützt der Dienst dies nicht. Laut Aussage Dataports ist eine Implementierung nicht für die nahe Zukunft geplant. Das zusätzliche Schlüsselpasswort von TripleCrypt® stellt per Definition zwar keinen zweiten Faktor einer 2-Faktor-Authentisierung dar ist bei eine Beurteilung der Angemessenheit der getroffenen Schutzmaßnahmen jedoch zu berücksichtigen. Ergänzend sollte insbesondere für externe Nutzer geprüft werden, ob im konkteten Anwendungsfall sich aus anderen Regelungen etwa der eIDAS-Verordnung eine rechtliche Vorgabe besteht, eine 2-Faktor-Authentisierung zu nutzen.

Verschlüsselung

Die vorhandene Verschlüsselung erzeugt drei Angriffsvektoren, um an den geschützten Inhalt zu gelangen:

1. Ein Angreifer, beispielsweise ein Dataport Administrator mit Zugriff zum im Server eingebundenen Dateisystem, kann die mit AES-256 verschlüsselte Datei durch Bruteforce dechiffrieren. Der Aufwand bis zur erfolgreichen Entschlüsselung ist vom eingesetzten Kryptoverfahren abhängig. AES-256 ist im Jahr 2020 Stand der Technik.
2. Ein Angreifer kann den Dateischlüssel, also den aus Angriff 1 verwendeten AES-256 Schlüssel, durch Bruteforce dechiffrieren. Dafür muss das angewendete Kryptoverfahren RSA-2048Bit überwunden werden. Auch dieses entspricht dem Stand der Technik für das Jahr 2020.
3. Ein Angreifer kann den privaten Schüssel eines Nutzers dechiffrieren. Dies ist ein Angriff auf die Passphrase des Nutzers. Das eingesetzte Kryptoverfahren mit PBKDF2 / AES-256 ist Stand der Technik im Jahr 2020. Ein erfolgreicher Angriff ist von der Einhaltung und Wirksamkeit einer Passwortrichtlinie abhängig.

Das Verschlüsselungskonzept des Dienstes wird ausreichend dargestellt, wenn auch Details über alle eingesetzten Cypher Suites und verwendeten Betriebsmodi nicht in der Dokumentation enthalten sind. Die vermittelten Angaben entsprechen den Anforderungen des BSI nach dem Stand der Technik.

Der Schwachpunkt der Aufbewahrung des privaten Schlüssels innerhalb des Dienstes lässt sich mit starker symmetrischer Verschlüsselung begegnen, mit der der Schlüssel vor dem Transport an den dDatabox Server chiffriert wird. Der private Schlüssel wird laut „Zero-Knowledge-Policy“ nur von der Client-Anwendung lokal mittels Passwort dechiffriert. Der verwendete Algorithmus entspricht dem Stand der Technik. (🔗 NIST: Recommendation for Password-Based Key Derivation)

Die Aktivierung von TripleCrypt® ist für den Auftraggeber bei der Verarbeitung von Daten mit hohem Schutzbedarf zu erzwingen, da hierbei ein mögliches Einwirken durch lesenden oder manipulativen Zugriff auf den Inhalt seitens des Dienstleisters oder Dritter erheblich erschwert wird. Ein Angreifer innerhalb des Dataport „Shared Basis“ Systems könnte lediglich Dateien gänzlich entfernen oder diese durch neue Dateien ersetzen, da die hierfür benötigten Schlüssel konzeptbedingt nutzbar auf dem Server vorliegen. Diese zusätzliche Verschlüsselung wirkt sich zudem positiv auf die Auswirkungen bei einem Logikfehler seitens des Anwendungsservers und auf die Anforderungen eines Löschvorgangs aus, da es den Inhalt von Dateien bei fälschlichem Zugriff oder bei Rekonstruktion von gelöschten Daten erschwert.

Da der Dienst keine generelle Option zum Erzwingen einer Ende-zu-Ende-Verschlüsselung bietet, könnte dies durch eine Organisation in Unterräume mit aktivierter Verschlüsselung ab dem Datenraum in höchster Ebene erzwungen werden.

Verarbeitung von Daten mit hohem Schutzbedarf

Ohne den Einsatz von TripleCrypt® erfüllt dDatabox die Anforderungen an die Verarbeitung von Daten mit hohem Schutzbedarf nicht. Ob eine Zwei-Faktoren-Authentisierung zusätzlich zur Verschlüsselung mit TripleCrypt® erforderlich ist, muss vom Verantwortlichen geprüft werden. Die fehlende Übersicht an Zugriffsberechtigungen innerhalb des Dienstes erfordert einen gewissenhaften und disziplinierten Umgang durch die Nutzer.

Verwendung des Dienstes und Alternativen

Wenn innerhalb des Dataport-Netzes Daten mit Schutzbedarf höher als normal ausgetauscht werden sollen, bietet Dataport eine E-Mail-Verschlüsselung für Microsoft Outlook als „RMS Schutz“ an. Diese Lösung ist für Anwender einfach zu nutzen, wenn sie sich im Rahmen der inhärenten Einschränkungen bewegen. Zu beachten ist die Größenbegrenzung der Anhänge einer E-Mail und die Einschränkung auf eine Kommunikation innerhalb des Dataport-Netzes, da der „RMS Schutz“ kein verbreiteter, E-Mail-Anbieter-übergreifender Standard ist.

Für einen Dateiaustausch mit einer Ende-zu-Ende-Verschlüsselung mit einem nicht zum Dataport-Netz gehörenden Kommunikationspartner können das Verfahren dDatabox und der Austausch von per Passwort verschlüsselten Zip-Archiven verglichen werden. In beiden Verfahren werden die ausgetauschten Dateien mit AES-256 verschlüsselt. Beim Versand des Zip-Archivs über das Internet (beispielsweise durch E-Mail, Instant-Messaging oder Sharing-Dienst) sind oftmals mehrere Dienstleister an der Übertragung beteiligt. Eine Verletzung der Vertraulichkeit der ausgetauschten Daten durch Dienstleister können sowohl der Austausch passwortgeschützter Zip-Archive als auch dDatabox durch die Verschlüsselung erschweren. Ein Unterbinden von Brute-Force-Angriffen auf das Passwort des Zip-Archives oder der im Datenraum abgelegten Datei ist in beiden Fällen aber nicht möglich.

In der Verwendung bringt dDatabox eine höhere Komplexität mit sich, da Nutzer, Gruppen und Berechtigungen auf der Seite des Verantwortlichen verwaltet werden müssen. In allen weiteren zu betrachtenden Aspekten bietet dDatabox einen ähnlichen oder größeren Schutz für Integrität und Vertraulichkeit seitens involvierter Dienstleister und möglicher Dritter:

Nutzbarkeit im Alltag
Die Nutzung der dDatabox Datei-Upload-Freigabe durch externe Anwender erfordert ein geringeres Maß an fachkundigem Wissen. Im Vergleich wird für den Umgang mit einem passwortgeschützten Zip-Archiv oftmals die Installation einer Zusatzsoftware benötigt. Das weit verbreitete Betriebssystem Microsoft Windows 10 stellt Anwendern eine integrierte Zip-Funktion zur Verfügung, die keine passwortgeschützten Zip-Archive unterstützt.

Passwörter
Für den Datenaustausch unter Verwendung von dDatabox für interne Nutzer kommen zwei Passwörter (Login-Passwort und Passphrase) zur Verwendung. Die Einhaltung der vorgegebenen Passwortrichtlinie wird vom Dienst erzwungen. Bei der Übermittlung eines Zip-Archives kann ebenfalls ein zweites Passwort eine Verwendung finden, da beispielsweise bei der Nutzung von E-Mail oder Instant-Messaging ein Passwort zur Nutzerkontenauthentifizierung üblich ist. Eine Passwortrichtlinie kann als technische Schutzmaßnahme bei der Erstellung eines Zip-Archives in der Regel durch Software nicht erzwungen werden.

Passwortaustausch
Durch dDatabox erfolgt explizit ein Hinweis, das Passwort dem externen Empfänger auf einem anderen Kommunikationsweg wie den Freigabe-Link mitzuteilen.

Verschlüsselungsstärke
Der Zip-Standard existiert seit 1989 und wurde über die Zeit durch die gestiegenen Anforderungen weiterentwickelt. Dies trifft auch auf den Verschlüsselungsalgorithmus zu, der in mehreren Iterationen verbessert wurde. 31 Jahre nach der ersten Veröffentlichung sieht der Zip-Standard zwei Verschlüsselungsmethoden vor: AES-256 und ZipCrypto. Die zweitgenannte Methode ist die ältere der beiden und erfüllt die Anforderungen an einen starken kryptografischen Algorithmus nicht. Jedoch ist ZipCrypto noch immer im Standard enthalten und wird von den gängigen Programmen zur Zip-Archiv-Erstellung unterstützt. Vielmehr verzichten diese Programme oftmals auf einen Hinweis der ungenügenden Stärke und geben (im Fall des beliebten Programmes „7-Zip“) ZipCrypto als Voreinstellung zur Verschlüsselung vor.

Anzahl der Dienstleister
Bei Betrieb von dDatabox müssen die Anwender genau einem Dienstleister (in Form von Dataport) vertrauen. Beim Versand von Zip-Archiven per E-Mail oder einigen Instant Messenger Diensten sind oftmals mehrere Dienstleister mit Zugriff auf das Zip-Archiv an der Übertragung beteiligt.

Angriff durch Ersetzen und Löschen
Der Betreiber von dDatabox kann durch Kenntnis der öffentlichen Schlüssel jederzeit die vorliegenden Dateien durch andere ersetzen. Dafür wird ein neuer symmetrischer Schlüssel erzeugt und mit den öffentlichen Schlüsseln aller Teilnehmer eines Datenraumes verschlüsselt. Diese Manipulation ist nur von dem Teilnehmer, der die Dokumente dem Datenraum hinzufügte, durch einen Vergleich feststellbar. Zip-Archive verhalten sich als Container ähnlich. Die Namen der im Zip-Archiv enthaltenen Dateien können auch ohne Passwort aufgelistet werden. Einzelne Dateien können aus dem Zip-Archiv ohne die Eingabe des Passwortes gelöscht werden. Auch können neue Dateien ohne Passwortschutz dem Archiv hinzugefügt werden. Extrahiert ein Empfänger anschließend den Inhalt des manipulierten Zip-Archives, wird das verwendete Zip-Programm nach dem Passwort für nicht manipulierte Dateien fragen und die ersetzten

Dateien ohne Passwortschutz entpacken. Dies geschieht in der Regel ohne einen Hinweis für den Anwender.

Fehlerbehebung und Aktualität der Software
Werden Fehler in der Software entdeckt, bessert der Hersteller oft in kurzen Zeiträumen durch Software-Updates nach. Dataport verspricht als Dienstleister in engem Kontakt zum Hersteller von dDatabox zu stehen und diese Updates zeitnah einzuspielen. Durch die heterogene Natur an Programmen für Zip-Unterstützung kann oftmals keine aktuelle Software-Version garantiert werden, da zum einen Einzelanwendungen den Nutzer nicht über eine nötige Aktualisierung hinweisen oder die Bibliothek, die eine Zip-Funktionalität zur Verfügung stellt, durch den Entwickler der Hauptanwendung nicht aktualisiert wird.

Transparente Nutzung
Ist bei großen Datenmengen die Übermittlung per E-Mail ungeeignet, können Dateien durch den Upload zu Online-Speicherdiensten oder durch Peer-to-Peer Verfahren dem Empfänger angeboten werden. Hierfür wird ein Download-Link erzeugt, der bei Aufruf die Dateiübertragung für den Empfänger startet. Die Protokollierung von dDatabox erlaubt eine Kontrolle der Interaktionen in einem Datenraum. Das Abfragen eines Download-Passwortes und der möglichen Sperrung der Download-Freigabe durch Ablauf eines Zeitraums oder einer festgelegten Anzahl von durchgeführten Downloads ermöglicht eine weitere Varianten zur Verwendung, die bei regulärem Austausch von Zip-Archiven durch E-Mail oder Instant Messaging nicht vorgesehen sind.

Der Dienst dDatabox stellt eine Möglichkeit für Austausch von Dateien mit substantiellen Schutzbedarf dar und bietet wirksame Maßnahmen zur Reduzierung der Risiken von Verlust an Vertraulichkeit und Integrität. Verantwortliche müssen sich der Einschränkung des Fehlens einer Zwei-Faktoren-Authentisierung bei hohem Schutzbedarf verdeutlichen. Für den Austausch großer Datenmengen und insbesondere mit externen Teilnehmern findet sich mit dDatabox im Softwarekatalog von Dataport ein geeignetes Werkzeug welches der Verwendung von passwortgeschützten Zip-Dateien oder der transportverschlüsselten E-Mail-Kommunikation vorzuziehen ist.

Die Nutzung einer Ende-zu-Ende-Verschlüsselung durch PGP per E-Mail oder Instant Messaging ist vom Dienstanbieter unabhängig und bietet die geringsten Einschränkungen für ein hohes Schutzniveau. PGP erfordert die Installation und Einrichtung zusätzlicher Software und die Kompatibilität der eingesetzten E-Mail- oder Messenger-Programme. Das Verfahren bringt leider im Alltag eine unvermeidbare Komplexität für jeden einzelnen Anwender mit sich und ist daher selten bei Kommunikationspartnern verfügbar. Kann PGP nicht eingesetzt werden, findet sich Softwarekatalog von Dataport mit dDatabox eine sichere Lösung für den Dateiaustausch.

Anlagen

Browsermatrix für Kompatibilität mit Webclient

Dataport gibt in den rechtlichen Bedingungen zur Nutzung des Dienstes folgende Unterstützung an:

„Der Benutzer hat die aktuellste Browserversion und das aktuellste Betriebssystem einzusetzen. Ab 01.07.2020 kann bei Benutzung des Web-Clients ausschließlich für die aktuellen Versionen von Microsoft Edge, Chrome, Firefox oder Safari Support geleistet werden. Bei Verwendung des Internet Explorers wird im Fehlerfall nur dann unterstützt, wenn dieser auch in anderen Browsern auftritt."

https://www.ddatabox.de/fileadmin/user_upload/kampagnenseiten/ddatabox/ddatabox-auftrag.pdf

Der Hersteller listet die Browseranforderungen auf der dracoon Webseite:
https://support.dracoon.com/hc/de/articles/360010786380-Systemanforderungen

Protokollierung von Ereignissen

Aus der dDatabox Dokumentation zur Protokollierung:

Es wird weder auf Serverebene noch Anwendungsebene die anfragende IP-Adresse protokolliert. Die IP-Adresse wird im TCP-Traffic nicht an die Anwendungsserver übermittelt, da der NetScaler als Netzwerkkomponente mit der öffentlichen IP-Adresse als TCP-Full Proxy fungiert.

Folgende Ereignisse werden in der aktuellen Version protokolliert:

group_name	**name**
Authentication	User Logon
Authentication	User Logon AD
Authentication	User Logoff
Authentication	User Logoff Everywhere
Authentication	User Token expired

Node	Node Create
Node	Node Delete
Node	Node Move
Node	Node Copy
Node	Node Download
Node	Node Zip Download
Node	Node Set Meta Status
Node	Node Set Attribute
Node	Node Change Attribute
Node	Node Delete Attribute
Node	Data Room Keypair Create
Node	Data Room Rescue KeyPair Download
Share	Download Share Create
Share	Download Share Delete
Share	Download Share Utilize
Share	Upload Share Create
Share	Upload Share Delete
Share	Upload Share File Create
Recycle Bin	Permanently Delete
Recycle Bin	Restore
User	User Create
User	User Delete
User	User Grant Data Space Admin
User	User Revoke Data Space Admin
User	User Grant User Manage
User	User Revoke User Manage
User	User Add Permission

User	User Remove Permission
User	User Change Permission
User	User Set Meta Data
User	User Change Meta Data
User	User Delete Meta Data
User	User Change Meta Status
User	User Reset Meta Data
Group	Group Create
Group	Group Delete
Group	Group Set Meta Data
Group	Group Change Meta Data
Group	Group Delete Meta Data
Group	Group Add Permission
Group	Group Change Permission
Group	Group Remove Permission
Group	Group User Add
Group	Group User Remove
Global	Global Encryption Activate
Global	Data Space KeyPair Create
Global	Data Space KeyPair Download
Global	Global Status Set
Global	Global Config Set
Global	Global Config Change
Global	Global Config Delete
Global	Global Config Password Reset
User	Password Invalidate
User	User Keypair Create

User	User Keypair Delete
Global	Global Config Create
Global	Global Config Delete
User	Client Authorization Create
User	Client Authorization Delete
Global	Client Definition Create
Global	Client Definition Delete
Share	Download Share Change
Share	Upload Account Change

In den Server Log Files speichert Dataport die Informationen, die der Browser des Nutzers durch die Funktionsweise von HTTP übermittelt. Diese protokollierten Daten werden von Dataport für folgende Zwecke verwendet:

- Zur technischen Administration und zur Bereitstellung der Website.
  - Ausschließlich im gesetzlich vorgesehenen Rahmen,
  - zur Abwehr von Angriffsversuchen auf Webserver,
  - zur Missbrauchserkennung und Störungsbeseitigung,
  - zur Weitergabe bzw. Auskunftserteilung gegenüber staatlichen Stellen,
  - zur Weitergabe bzw. Auskunftserteilung gegenüber Inhabern von Urheber- und Leistungsschutzrechten.

Verlaufsdaten werden automatisch nach 6 Monaten gelöscht, Protokolldaten (Logdateien) werden automatisch nach 30 Tagen gelöscht.

Weiterführende Dokumentation

- Hersteller Dokumentation
- Dataport Wiki zu dDatabox

- Dataport Produktseite zu dDatabox
- Hersteller Whitepaper zum Thema Sicherheit
- Herstellerseite zur Zertifizierung