

DocRAID stellt auf der conhIT erstmalig sicheres und einfaches File-Sharing und E-Mail-Verschlüsselung für den Gesundheitssektor vor

Berlin, 24.4.2016

DocRAID, der Anbieter sicherer Cloud-Storages im RAID-Verbund, stellt auf dem Cetus Security-Pavillon der conhIT erstmalig sein sicheres und einfaches File-Sharing und Email Verschlüsselung für den Gesundheitssektor vor.

DocRAID holt den Nutzer dort ab, wo er bereits arbeitet: im WWW Explorer, im Dateimanager oder in Outlook.

Verschlüsselung von Anhängen oder ganzen Nachrichten, Abrufkontrolle, Ablaufdaten von E-Mails und Zugriff-Alerts sind die wichtigsten Features der DocRAID Email Verschlüsselung. Der sichere und einfach nutzbare Austausch von Dateien, z.B. für Tumorkonferenzen, für den Bildungsbereich, für die Vorstands- und Geschäftsführerkommunikation sind wichtige Anwendungsbereiche im Gesundheitssektor. Datenräume werden per WebDAV als Laufwerk angebunden.

Das Plugin für Microsoft Outlook funktioniert mit jedem E-Mail-Provider und setzt auf der Empfängerseite anders als etwa PGP keine zusätzliche Software voraus. Bei jeder versandten Mail kann einzeln ausgewählt werden, ob der Anhang oder die gesamte E-Mail mit DocRAID verschlüsselt werden soll oder nicht. Wird die Verschlüsselung von DocRAID genutzt, wird die E-Mail statt an den Empfänger an einen DocRAID-Server geschickt. Von DocRAID erhält der Empfänger eine E-Mail mit einem Link, der zu dem geschützten Inhalt führt.

Usability als Voraussetzung für Security

Erst kürzlich veröffentlichte Bitkom Zahlen zum Anwender-Verhalten bei E-Mail-Verschlüsselung. Ernüchternde 15 Prozent der Nutzer verschlüsseln in Deutschland ihre E-Mails. Mehr als die Hälfte aller Befragten verzichteten auf E-Mail-Verschlüsselung, weil die Kommunikationspartner keine Verschlüsselung einsetzen und jeder vierte befand die bisherigen Lösungen für schlicht zu aufwendig.

Dies ist der Punkt, bei dem DocRAID ansetzt. Security muss benutzerfreundlich sein und muss die bisherige Arbeitsweise unterstützen um akzeptiert zu werden. Damit dies gelingt, sind bei der DocRAID E-Mail-Verschlüsselung mehrere Usability-Features umgesetzt worden. Zunächst kann bei jeder E-Mail ausgewählt werden, ob die gesamte E-Mail oder nur der Anhang verschlüsselt werden soll. Im letzteren Fall wird auch nur der Anhang auf einem DocRAID-Server gespeichert, während der Body der E-Mail an den Empfänger weitergeleitet wird. Der verschlüsselte Anhang kann dann über den Link statt über das E-Mail-Programm des Empfängers

aufgerufen und abgespeichert werden.

The screenshot shows the DocRAID email protection settings interface. At the top, it says "DocRAID® email protection for professionals". On the left, there is a green DocRAID logo with the text "16.01.0703" below it and a link "www.docraid.com" at the bottom. The main settings area is titled "Verschlüsselung" and "Server". It includes a "Schutzniveau" indicator with two green squares. Under "Verschlüsselung", there are three radio button options: "die gesamte EMail, inkl. Anhang verschlüsseln", "nur den Anhang verschlüsseln" (which is selected), and "nicht verschlüsseln". Below this, it states "Der Inhalt dieser Mail ist verfügbar bis:" followed by a date selector set to "Freitag, 29. Januar 2016". There are four checkboxes: "Code-Protect: Empfänger erhält Code zum Abruf" (unchecked), "Benachrichtige mich, wenn die Email abgerufen wird" (checked), "Unverschlüsselte Kopie lokal speichern" (checked), and "Dieses Menü beim nächsten Senden anzeigen" (checked). An "Email-Adresse:" field contains "hoffmann@docraid.com". At the bottom, there is a "Daten speichern" button.

Ferner bestehen für Empfänger, wie auch für den Sender die Möglichkeit, die gesamte E-Mail im Mail-Programm unverschlüsselt abzuspeichern, um sie archivierbar und durchsuchbar zu halten. Auf Sender-Seite reicht eine einmalige Einstellung und alle über DocRAID gesendeten E-Mails sind weiterhin im Ordner "Gesendet" als unverschlüsselte Kopie erhalten. Auf Empfängerseite besteht die Möglichkeit über den mitgeschickten Link nicht nur den Anhang, sondern die gesamte E-Mail im Original wahlweise als msg-, txt- oder html-Datei herunterzuladen und mit dem entsprechenden Mail-Programm zu öffnen.

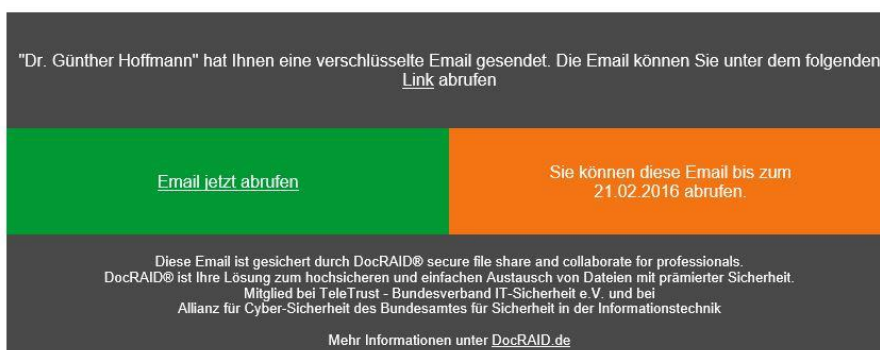
Zusätzliche Features über Verschlüsselung hinaus für Compliance und Datenschützer

Während PGP oder S/MIME nur die Verschlüsselung gewährleisten, bietet eine Server-basierte Lösung einen größeren Funktionsumfang. So können auf DocRAID-Servern zum Download stehende Anhänge und E-Mails auch mit einem Verfallsdatum versehen werden, innerhalb dessen sie abgerufen werden müssen. Andernfalls werden sie automatisch gelöscht. Auch wird protokolliert, wann wer welchen Anhang abgerufen hat. Alert-Funktionen für den Sender der E-Mail bei Abruf sind ebenfalls einstellbar. Das inzwischen fast obsolet gewordene Prinzip der Empfangsbestätigung wird dadurch wirkungsvoll ersetzt. Ob und wann Anhang oder E-Mail abgerufen wurden, kann zweifelsfrei dokumentiert werden, ohne dass die Empfänger-Seite dies explizit bestätigen muss. Natürlich können alle Einstellungen, wie Ablaufdatum oder Alert-Funktion auch nachträglich nach Versenden der E-Mail noch geändert werden. Ein fälschlich gesendeter Anhang kann solange noch rückwirkend gelöscht werden, wie er nicht abgerufen wurde.

Da der Server des eigentlichen E-Mail-Providers faktisch umgangen wird, fällt auch die Größenbegrenzung des E-Mail-Providers weg. Anhänge in beliebiger Größe können an beliebige Empfänger verschickt werden.

Codesperre und restriktiver Zugriff gegen Man-in-the-Middle-Attacken

Eine Lösung, die nur vom Sender allein installiert und bedient werden kann und keine Anforderungen an den Empfänger stellt hat sicherheitstechnisch Vor- und Nachteile. Zu den Vorteilen gehört zweifelsohne, dass ein Sender nicht darauf angewiesen ist, dass der Empfänger die gleiche oder überhaupt irgendeine Form der Verschlüsselung benutzt. Dies schafft Akzeptanz und Akzeptanz führt im Ergebnis zu Sicherheit, denn Mechanismen, die Mitarbeiter in gewohnten Abläufen zu stark beeinträchtigen werden in der Praxis einfach umgangen.



Zu den Nachteilen gehört, dass man sich angreifbarer gegenüber Man-in-the-Middle-Attacken macht. Um dem vorzubeugen sind von DocRAID für das Outlook-Plugin weitere Features hinzugefügt worden. Zum einen gibt es die sogenannte Codesperre. Hier kann der Absender dem Anhang oder der gesamten E-Mail eine Codesperre hinzufügen. Der Empfänger erhält wie gewohnt den Link, muss sich dann aber zunächst an eine E-Mail-Adresse seiner Wahl eine PIN schicken lassen, mit der er die online hinterlegten Informationen abrufen kann. In der Praxis muss ein Angreifer bei einer Man-in-the-Middle-Attacke also Zugriff auf zwei verschiedene E-Mail-Postfächer erlangen. Außerdem wird auch bei einer Codesperre jeder Abruf und auch die Anforderung der PIN protokolliert, so dass ein Man-in-the-Middle-Angriff kaum unbemerkt bleiben würde. Zusätzlich kann der Abruf der online bei DocRAID hinterlegten Daten auf bestimmte Personengruppen beschränkt werden.

Verfügbarkeit

DocRAID für den Gesundheitssektor ist ab sofort verfügbar und setzt im off-premise Betrieb keine Installation voraus. DocRAID im Kundenrechenzentrum wird als on-premise Version angeboten. Das Plugin für Microsoft Outlook kann mit den üblichen Windows Verfahren ausgerollt werden.

Über DocRAID®:

DocRAID® wurde mehrfach ausgezeichnet, u.a. mit dem Bayer Grants4Apps Award; IKT Innovativ Sonderpreis 2013 von SAP, Siemens, Empolis; Bundesministerium für Wirtschaft und Technologie (BMWi); nominiert für den TeleTrust-Innovationspreis.

DocRAID ist Mitglied bei TeleTrust Bundesverband IT-Sicherheit e.V. und Träger des Qualitätszeichens ITSMIG ("IT Security made in Germany") unter der Trägerschaft des BMI und des BMWi.

Weitere Informationen:

DocRAID® file sync, share, collaborate with maximum data privacy

ContentPro AG

Dr. Günther Hoffmann

Gewerbezentrum am Südkreuz

Wilhelm-Kabus-Str. 21-35

10829 Berlin

Tel.: 030 609898 061

Email: press@docraid.com

WWW: <http://www.docraid.com>

Pressemeldungen:

https://secure.docraid.com/command=dir_list&sid=060D96140ADA6C27A1618B414DDF1441C0D65936FCA48780DEDBE655D77FF63A@LKCBBQECOPDIIBBJLBCKBCPHE&dirname=News/Presse%20Freigabe%20D

Bildquellen:

https://secure.docraid.com/command=dir_list&sid=060D96140ADA6C27A1618B414DDF1441C0D65936FCA48780DEDBE655D77FF63A@LKCBBQECOPDIIBBJLBCKBCPHE&dirname=News/Presse%20Freigabe%20D