IAITested

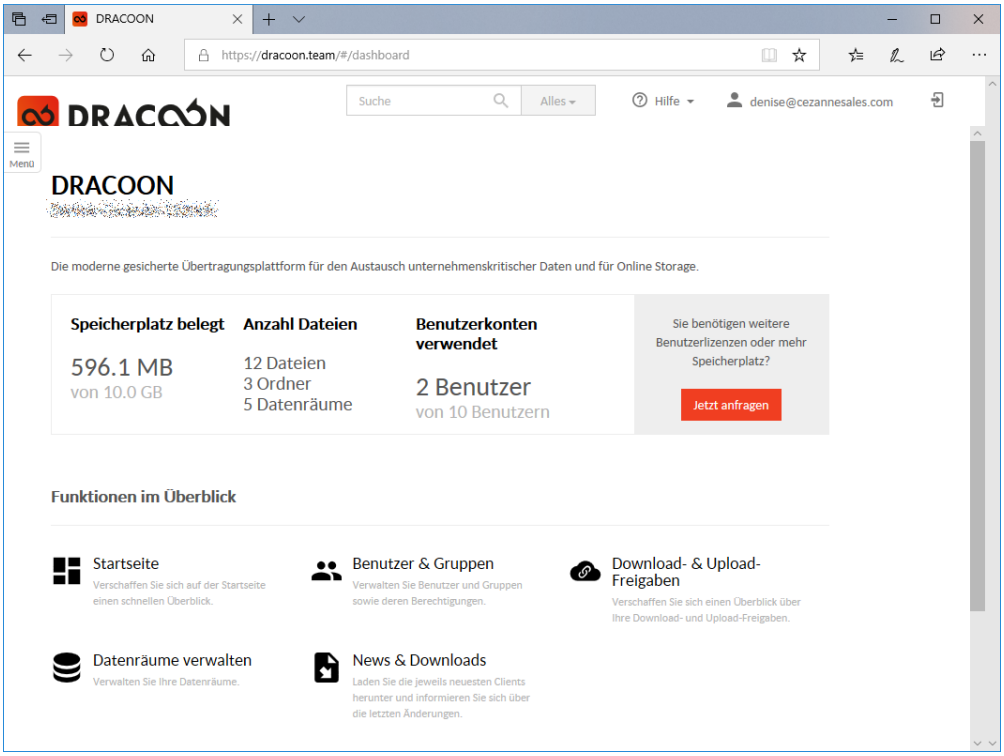
Im Test: Die Enterprise Cloud von DRACOON

Leistungsfähiger Cloudspeicher für den professionellen Einsatz

Autor: Dr. Götz Güttich

DRACOON bietet einen sicheren Cloudspeicher für Unternehmen an. Bei der Lösung des deutschen Anbieters werden die Daten client-seitig verschlüsselt, das bedeutet, dass sämtliche Daten überall sicher „verwahrt“ werden. Somit kann nicht einmal DRACOON als Hersteller auf gespeicherte Kundendaten zugreifen. Wir haben im Testlabor die Funktionalitäten des Produkts unter die Lupe genommen.

Der Cloudspeicher von DRACOON wurde speziell auf die Anforderungen von Unternehmen zugeschnitten. Deswegen gibt es nicht nur die Option, sämtliche Daten hochsicher zu verschlüsseln, sondern das System bietet auch ein komplett eigenes Branding mit eigener URL und einem eigenen Design an.



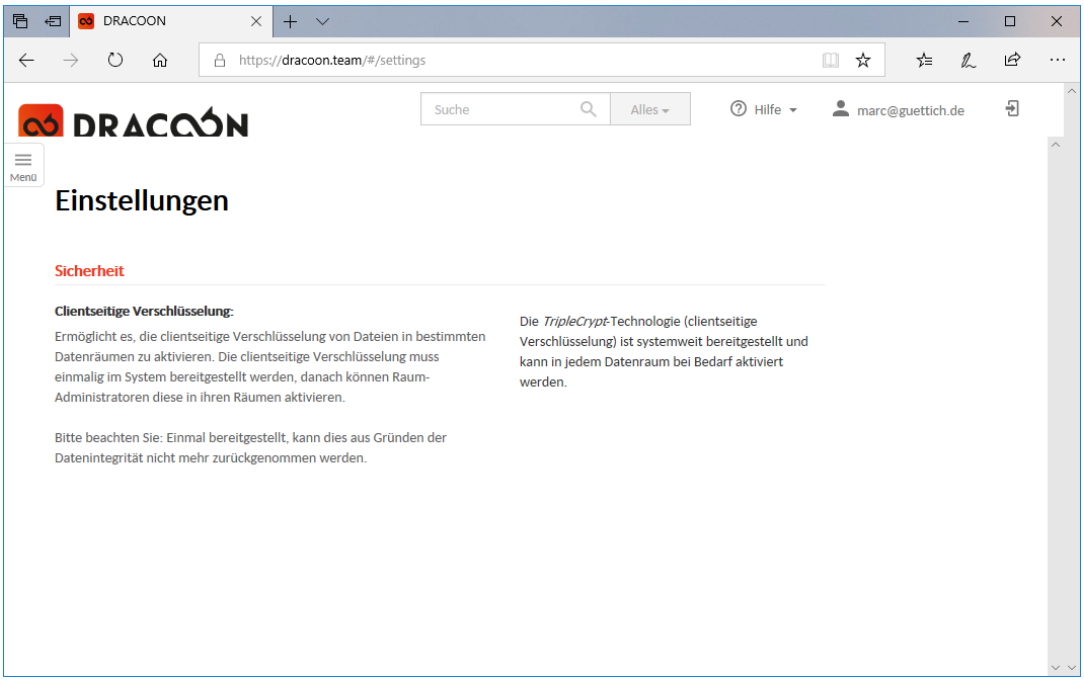
Nach dem Login haben die Benutzer Zugriff auf alle Funktionen der Enterprise Cloud

Zum Leistungsumfang gehören außerdem umfassende Administrationsfunktionen, die eine Vielzahl von Anwendungsszenarien abdecken. So lassen sich beispielsweise sogenannte Datenräume einrichten, auf die nur bestimmte Anwender Zugriff haben. Innerhalb dieser Räume ist es auch möglich, den Benutzern wiederum nur bestimmte Rechte zuzugestehen und Datenräume innerhalb von Datenräumen zu erzeugen. In der Praxis könnte man so beispielsweise dem Anwender „Andreas“, der in der Buchhaltung arbeitet, im Datenraum „Buchhaltung“ volle Schreib- und Leserechte auf alle Dateien (oder untergeordneten Datenräume) geben, ihm gleichzeitig im Datenraum der IT-Abteilung aber nur Leserechte auf den Sub-Datenraum „Rechnungen“ einräumen.

Interessant ist vor allem, dass die DRACOON-Lösung ohne zentralen Administrator auskommt. Der Anwender, der das Konto anlegt und die ersten Datenräume erzeugt, hat zwar zu Beginn Zugriff auf alle Daten, die im Cloudspeicher vorhanden sind, er kann aber andere User zu Administratoren der einzelnen Datenräume ernennen. Sobald diese Administratorrechte in ihren Datenräumen erlangt haben, besteht die Möglichkeit, dem ersten Administrator die Rechte zum Zugriff auf diese Datenräume zu entziehen und so dafür zu sorgen, dass immer nur die Mitarbeiter die Daten einsehen und modifizieren können, die das auch wirklich müssen, um ihre Arbeit zu erledigen. Diese Funktionalität vermeidet, dass die IT-Abteilung immer auf alles zugreifen kann, was im Unternehmen verfügbar ist. Insbesondere bei der Bearbeitung von besonders sensiblen Daten wie Löhnen, Gehältern, Personal- oder auch Gesundheitsdaten spielt dies eine große Rolle.

Verfügbare Benutzerrollen

Konkret unterscheidet DRACOON zwischen fünf verschiedenen Verwaltungsrollen, die vergeben beziehungsweise Benutzern zugewiesen werden können. Beispielsweise darf der „Konfigurationsmanager“ die Systemeinstellungen ändern, während der „Benutzermanager“ die Möglichkeit hat, weitere Benutzer anzulegen.



Die client-seitige Verschlüsselung muss in den Einstellungen explizit aktiviert werden

Die „Datenraumadministratoren“ wiederum verwalten die Rechte und Benutzer innerhalb der Datenräume, während die „Datenraum-User“, je nach den ihnen zugewiesenen Rechten, Daten hochladen, löschen und versenden können. Das gleiche gilt für die Erstellung von Down- und Upload-Links. Die letztgenannten Rechte haben alle Administratorkonten sowieso. Darüber hinaus können externe Benutzer via Down- und Upload-Freigaben temporär auf Datenräume zugreifen.

Verschlüsselung und Zugriffsoptionen

Insgesamt unterscheidet DRACOON zwischen der Verschlüsselung auf dem Client, auf dem Server und während des Transports. Während der Server und der Transport immer verschlüsselt sind, muss die client-seitige Verschlüsselung manuell aktiviert werden. Um DSGVO-konform zu agieren, sollten personenbezogene Daten übrigens immer client-seitig verschlüsselt sein.

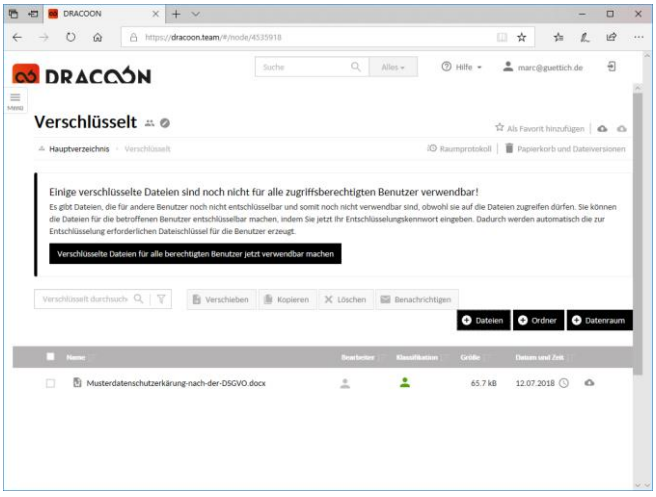
Der Zugriff auf den Cloudspeicher ist auf eine Vielzahl unterschiedlicher Wege möglich. Neben der Web-Anwendung, die via Internet zur sicheren Steuerung der Lösung dient und die auch den Up- und Download von Dateien ermöglicht, stehen Clients für die Desktop-Betriebssysteme MacOS (ab Version 10.8.3) und Windows (ab Windows 7) sowie die mobilen Betriebssysteme Android (seit Version 4.1) und iOS (ab Version 9.3) in Form einer eigenen App zur Verfügung. Darüber hinaus können die IT-Verantwortlichen DRACOON in ihre Active Directory-Umgebung integrieren und ein JSON/REST-API unterstützt die Anbindung von Drittlösungen wie SharePoint und ähnlichem.

Weitere Funktionen

Neben den bereits genannten Features bietet DRACOON auch ein Outlook-Add-In an, mit dem sich die Zustellung von Mail-Anhängen absichern lässt. Ebenfalls von Interesse sind die Dateiversionierung und das Reporting-Tool, darauf gehen wir später im Detail noch genauer ein.

Der Test

Für unseren Test verwendeten wir die kostenlose Free-Variante von DRACOON, die alle Funktionen (außer den Branding-Features) umfasst, zeitlich nicht beschränkt ist und als einzige Einschränkung das Speicherplatzvolumen auf – für ein Gratisangebot recht großzügige – zehn GByte und die Nutzerzahl auf zehn beschränkt. Um dieses Angebot zu nutzen, muss man als Anwender lediglich auf der Website des Herstellers unter https://www.dracoon.com/free einen Account anlegen, anschließend kann man sofort loslegen.



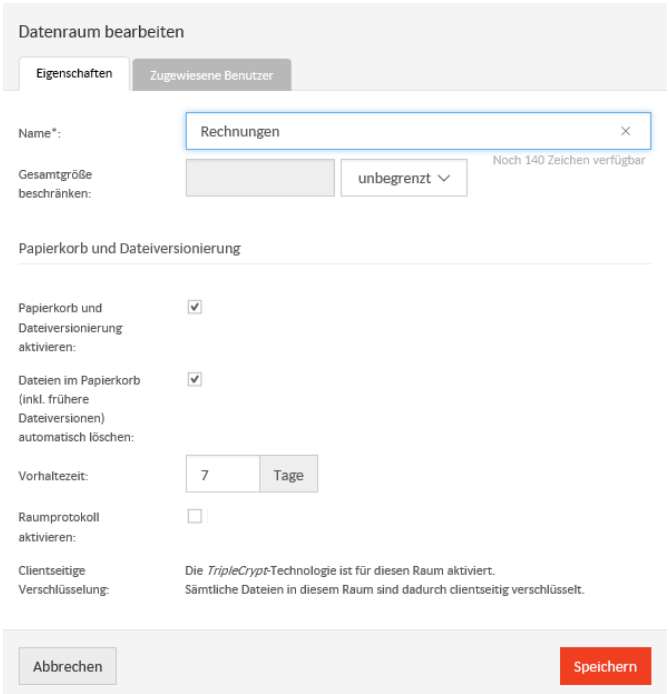
Client-seitig verschlüsselte Daten sind nur dann nutzbar, wenn das Entschlüsselungskennwort eingegeben wird

Neben dem Gratisangebot hat DRACOON auch noch diverse kostenpflichtige Enterprise-Varianten im Angebot: Bei der „Cloud-Unternehmenslösung“ werden die Daten in zertifizierten DRACOON-Rechenzentren mit unbegrenztem Datenvolumen gespeichert. Diese Variante greift ab 50 Usern. Bei der „Hybrid-Lösung“, die ebenfalls ab 50 Benutzern verfügbar ist, wird DRACOON aus der Cloud betrieben. Die Dateien speichert das System in diesem Fall im eigenen Rechenzentrum des Kunden. Die „On-Premises-Version“ hingegen ermöglicht ab 100 Usern die Installation und den Betrieb der DRACOON-Lösung im eigenen Rechenzentrum des Kunden. Nachdem wir unseren Account eingerichtet hatten, legten wir erst einmal diverse Benutzerkonten an, erzeugten Datenräume, vergaben Rechte und überprüften, ob sich das System im Betrieb so verhielt, wie erwartet.

Anschließend installierten wir auf diversen Rechnern unter Windows 10 den Windows-Client und nutzten diesen, um damit automatisch den Cloudspeicher zwischen diesen Clients zu synchronisieren. Danach verwendeten wir Smartphones unter Android 7 und 8, um mit Hilfe des Android-Clients mobil auf unsere Daten zuzugreifen. Unter iOS nutzten wir zu diesem Zweck diverse iPads. Außerdem nahmen wir auch noch die Funktionalität des Outlook-Add-Ins und des Reporting-Tools unter die Lupe.

Der Test-Account

Um sich einen DRACOON-Account zuzulegen, müssen die Anwender lediglich auf der oben genannten Webseite ihren Namen und ihre E-Mail-Adresse angeben. Danach erhalten sie eine Mail, die die URL auf den DRACOON Server, den Benutzernamen (das ist die E-Mail-Adresse) und das Initialpasswort sowie einen Link zur Dokumentation enthält.

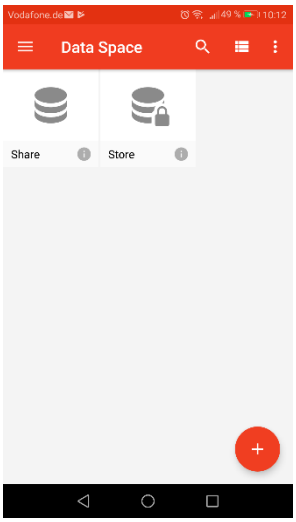


Bei den Einstellungen zu den Datenräumen lässt sich unter anderem die Dateiversionierung aktivieren

Nach dem Login mit den neuen Anmeldedaten muss der Benutzer zunächst den Nutzungsbedingungen zustimmen und sein Passwort ändern. Das ist sehr gut, da auf diese Weise sichergestellt wird, dass niemand mit dem zuvor unsicher per Mail zugestellten Passwort weiterarbeitet. Nach der Definition des neuen Passworts landet der Anwender auf der Startseite der Web-Anwendung von DRACOON und kann mit der Arbeit beginnen.

Datenräume und Benutzer verwalten

Im nächsten Schritt machten wir uns daran, diverse Benutzerkonten sowie Datenräume einzurichten und darauf unterschiedliche Rechte zu vergeben. Das alles geht verhältnismäßig einfach über die Menüleiste und die Einträge „Benutzer & Gruppen“ sowie „Datenräume verwalten“. Soll die client-seitige Verschlüsselung für die lokale Verschlüsselung der Daten zum Einsatz kommen, so muss diese aber zunächst unter „Einstellungen“ aktiviert werden. Dazu müssen die zuständigen Mitarbeiter erst einmal ein System-Notfall-Kennwort definieren, mit dem sich Daten entschlüsseln lassen, wenn ein Benutzer eines Raums sein persönliches Entschlüsselungskennwort vergessen hat. Sobald das geschehen ist, erzeugt das System das Schlüsselpaar und die client-seitige Verschlüsselung wird aktiv.



Die mobilen Apps ermöglichen sowohl den Zugriff auf „normale“ als auch auf client-seitig verschlüsselte Datenräume

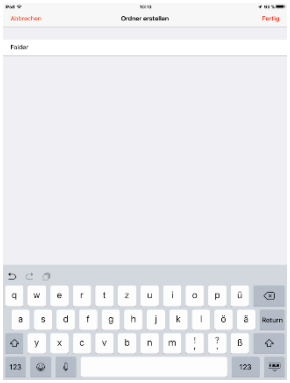
Anschließend müssen die Benutzer, die diese Technologie nutzen wollen, auf der Startseite noch ein persönliches Entschlüsselungskennwort festlegen, danach lässt sich die client-seitige Verschlüsselung für die vorhandenen Datenräume nutzen. Übrigens gibt es auch die Option, für einen Datenraum ein bestimmtes Datenraumkennwort festzulegen, mit dem sich die Daten anstelle des System-Notfall-Kennworts entschlüsseln lassen. Das ergibt beispielsweise bei Datenräumen Sinn, in denen Daten liegen, auf die Administratoren, die das Systempasswort kennen, keinen Datenzugriff erhalten sollen.

Generell funktioniert die Verwaltung der Benutzer und Gruppen bei DRACOON so, wie man das von anderen Lösungen her kennt. Es gibt die Option, einen Benutzernamen zu vergeben und eine E-Mail-Adresse festzulegen. Danach schickt das System eine E-Mail an die eben definierte Adresse, die Informationen zum Login und das

Erstanmeldepasswort enthält. Auch bei den neu angelegten Nutzern ist es nach dem ersten Login nötig, das Passwort zu ändern und die Nutzungsbedingungen zu akzeptieren, anschließend können sie mit dem System arbeiten. Dabei erhalten sie allerdings immer nur die Konfigurationsmöglichkeiten, die ihnen ihre Rechte erlauben. Sie dürfen also nur die Datenräume nutzen, auf die sie Zugriff haben und haben nur Gelegenheit, Aktionen durchführen, die für sie freigeschaltet wurden.

Benutzerrechte & dezentrale Administration

Bei den Benutzerrechten unterscheidet das System übrigens zwischen den Rollen „Auditor“, der das Audit-Log einsehen kann, in dem die Nutzeraktivitäten protokolliert werden und der dazu in der Lage ist, mit dem Recherche-Tool Auswertungen vorzunehmen und „Raummanagern“, die alle Datenräume der obersten Ebene verwalten. Sie haben dabei die Möglichkeit, Räume anzulegen, zu löschen, umzubenennen und Quotas zu vergeben. Das Recht, auf die Inhalte der Räume zuzugreifen, erhalten sie allerdings nur dann, wenn ein entsprechender Raum-Administrator das zulässt.



Dank der Apps für Android und iOS lassen sich nicht nur Daten unterwegs nutzen und teilen, sondern auch Datenräume und Ordner erstellen

Außerdem gibt es noch die Rechte „Benutzermanager“ und „Gruppenmanager“ zum Verwalten von Benutzerkonten und Gruppen. „Konfigurationsmanager“ können die Systemeinstellungen einsehen und modifizieren und „Alle Rollen“ erklärt sich selbst.

Abgesehen von den Rechten lassen sich bei der Definition eines Benutzerkontos noch die Authentifizierungsmethoden (Active Directory, E-Mail, OAuth, OpenID oder Radius) festlegen, definieren, in welchen Gruppen der User Mitglied ist und angeben, welche Rechte der Anwender in welchen Datenräumen hat.

Ransomware-Schutz durch Papierkorbfunktion

Der aktivierbare Papierkorb eignet sich übrigens hervorragend zur Abwehr von Ransomware-Angriffen. Befällt eine solche Malware einen Client, so verschlüsselt sie zwar auch die Daten in einem angebundenen DRACOON-Webspace, diese lassen sich aber jederzeit unversehrt aus dem Papierkorb wiederherstellen. Die Rechte, die für den Papierkorb des Datenraums vergeben werden können, umfassen dabei die Funktionen „Leeren“, „Inhalte wiederherstellen“ und „Frühere Dateiversionen einsehen“. Was die Gruppenverwaltung angeht, so lassen sich den Gruppen die

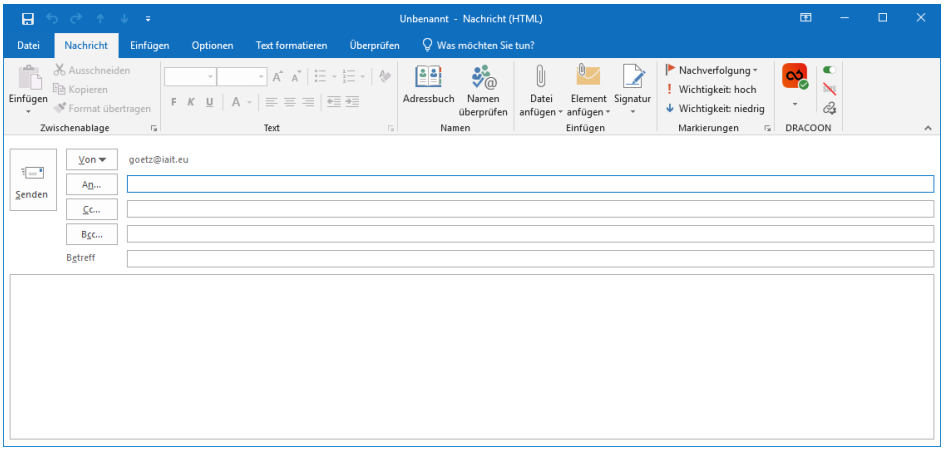
gleichen Rollen und Rechte auf Datenräume zuweisen, ähnlich wie einzelnen Benutzern.

Die Definition der Datenräume

Beim Anlegen der Datenräume vergeben die zuständigen Mitarbeiter einen Namen, beschränken bei Bedarf die Größe und aktivieren auf Wunsch den Papierkorb und die Dateiversionierung. Dabei gibt es auch die Option, Daten aus dem Papierkorb nach einer bestimmten Zeit automatisch zu löschen und ein Raumprotokoll zu aktivieren. Darüber hinaus lassen sich den Datenräumen an gleicher Stelle Raum-Administratoren und Raum-Administratorgruppen hinzufügen.

Der Client für Windows

Nachdem wir unsere Benutzerkonten mit ihren Rechten und den Datenräumen entsprechend unserer Wünsche eingerichtet hatten, installierten wir auf diversen Windows 10-Rechnern den Windows-Client und luden diverse Dateien von einem Rechner aus auf den DRACOON-Speicher hoch. Wie erwartet wurden die Daten dann auf die anderen Rechner synchronisiert und die Client-Software verhielt sich ähnlich wie von anderen Diensten, wie Dropbox oder Box her, bekannt.



Das Outlook-Add-In von DRACOON lässt sich für jede Mail oben rechts ein-, beziehungsweise ausschalten

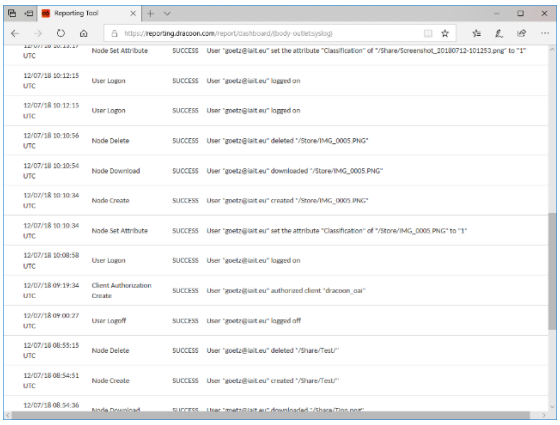
Einen Unterschied gibt es allerdings: Die DRACOON-Lösung bindet den Datenspeicher als Laufwerk und nicht als Ordner ein. Deshalb benötigt sie auch auf dem Client-Rechner einen – oder beim Zugriff auf mehrere unterschiedliche Konten mehrere – Laufwerksbuchstaben.

Die Apps für Android und iOS

Im nächsten Schritt installierten wir auch noch die Client-Programme für Android und iOS auf entsprechenden Endgeräten und konnten dort ebenfalls die Daten auf unserem DRACOON-Speicher nutzen. Der Zugriff auf client-seitig verschlüsselte Ordner funktionierte auf allen Client-Systemen problemlos, genau wie die Arbeit mit den hochgeladenen Daten. Auch bei der Arbeit mit den Zugriffsrechten, den Benutzerkonten und den Gruppen kam es zu keinen Überraschungen und alles verhielt sich wie erwartet.

Freigaben, das Outlook-Add-In und das Reporting-Tool

Gehen wir zum Schluss noch kurz auf die weiteren Features der Lösung ein. Die „Freigaben“ ermöglichen das Hoch- und Herunterladen von Dateien auch für Nutzer ohne DRACOON-Konto. Dabei lassen sich Begrenzungen und Ablaufzeiten definieren, aber auf Wunsch auch Passwörter für den Zugriff vergeben, die separat, zum Beispiel via Kurzmitteilung, übermittelt werden.



Das Reporting-Tool gibt genauen Aufschluss darüber, was für Aktionen von wem im Cloudspeicher durchgeführt wurden

Das Outlook-Add-In hilft den Anwendern, den Versand von Dateianhängen via E-Mail sicherer zu gestalten. Dazu trennt es nach seiner Installation die Anlagen von den Mails ab, lädt sie in einen dafür festgelegten Ordner in den DRACOON-Speicher und schickt den Empfängern lediglich einen Download-Link, über den sie die Daten herunterladen können. Dieses Verhalten lässt sich bei Bedarf jederzeit deaktivieren.

Nun zum Reporting-Tool: Dieses bietet Nutzern mit Auditor-Rechten einen Überblick über sämtliche Zugriffsrechte innerhalb des Cloudspeichers, die Datenräume und Benutzer und Gruppen. Das Werkzeug hilft darüber hinaus beim Identifizieren von Nutzern mit unerwünschten Rechten und sorgt so für ein Anheben des Sicherheitsniveaus. Die Lösung steht als Web-Anwendung unter reporting.dracoon.com zur Verfügung. Bei Bedarf lassen sich alle vorhandenen Daten auch als CSV-Dateien exportieren.

Damit die Übersicht gewahrt bleibt, können Auditoren die Ausgabe auf bestimmte Zeiträume beschränken und Filter setzen. Es steht auch ein Event-Log zur Verfügung, das sich durchsuchen lässt und alle Aktionen sämtlicher User mit Downloads, Authentifizierungen und so weiter auflistet.

Fazit

Die Lösung von DRACOON bietet einen sicheren Cloudspeicher, der sich dank des großen Funktionsumfangs und der leistungsfähigen Clients genauso einfach nutzen lässt wie „traditionelle“ Cloudspeicher US-amerikanischer Anbieter – im Vergleich dazu jedoch mit einem hohen Sicherheitsniveau punktet. Damit stellt die Lösung, nicht zuletzt dank der Vielzahl an Collaboration-Optionen für Mitarbeiter, eine hochinteressante Alternative zu diesen Anbietern dar, insbesondere für europäische Unternehmen, die auf die Vorgaben der DSGVO achten müssen.