DRACOON

Date: *August 22, 2018*
Source: *IT-Sicherheit (issue 04/2018)*
https://www.dracoon.com/wp-content/uploads/2018/10/IT-Sicherheit-Clipping-Produkttest_klein.pdf

Press Report

The institute for the analysis of IT components (Institut zur Analyse von IT-Komponenten (IAIT)) conducts high-quality, independent tests, workshops and video tutorials as well as interviews for new products and solutions for information technology. Subsequently the results are published by independent media.

The head of the institute – Dr. Götz Güttich – has more than ten years of experience as an IT-consultant and as an expert and chief editor in the IT-sector. Thanks to his long experience in test activities for leading German network magazines his skills reach beyond the theoretical aspects of the IT-business. His main focus lies in the fields of IT-security, storage, network management, network operating systems (Linux, Unix and Windows), terminal servers and virtualising.

Tested: The Enterprise Cloud by DRACOON
A Strong Professional Storage

DRACOON offers a secure cloud storage for enterprises. The German solution also ensures client-side data encryption. This means that all data – on the client, the server and during transport – is safe. Not even DRACOON as the provider can access the saved client data. In our testing-lab we had a closer look at the functions of the product.

The Cloud-Storage was specially designed to meet the needs of enterprises. Therefore, it not only safely encrypts data but also offers a complete and individual branding with its own URL and own design.

It also includes a complete administration function that covers multiple application scenarios. For example, so-called data-rooms can be created with access limited to certain users. Within these rooms it is also possible to give the users certain rights and to generate data-rooms within each other. For instance, it would be possible to grant the user “Andy” who is working in the accounting department full reading and writing rights for all files (or all subordinate data-rooms) in the data-room “accounting”. At the same time, one could only give him reading permission in the sub-data-room “invoices” in the data room of the IT-department.

The DRACOON-solution manages without a central administrator, which is especially interesting. In the beginning, the user who creates the account and generates the first data-rooms has full access to all data in the cloud storage. However, he can appoint other users as administrators of certain data-rooms. As soon as these users have received their admin-rights they can withdraw the access and rights concerning their data-room from the initial administrator. This way they can ensure that only the employees who need the data for

their daily work can read and modify the data. This function prevents IT-employees from accessing all data available in the enterprise.

User roles

DRACOON specifies five different administrative roles that can be assigned to different users. For example, the “configuration manager” can change the system setting whereas the “user manager” can create new users.

The “data-room administrators” on the other hand can manage the rights and users within the data-rooms whereas the “data-room-users” can upload, delete or send files according to their rights. The same goes for the creation of down- or upload links. The latter are of course also granted to all administrators. Furthermore, extern users can temporarily be given access to the data-rooms via the down- and upload-links.

Encryption and Access Options

DRACOON distinguishes between encryption on the client, the server and during transport. While the server and the transport are always encrypted, the client-side encryption has to be activated manually. To act in accordance with the GDPR, personal data should always be client-side-encrypted.

There are multiple ways to access the cloud storage. Firstly, there is the web-application, that ensures a safe management of the system via the internet and also enables the up- and download of files. The client can use these desktop operating systems MacOS (since version 10.8.3) and Windows (since Windows 7) as well as the mobile operating systems Android (since version 4.1) and iOS (since version 9.3) in form of a special app. Moreover, those responsible for IT can incorporate DRACOON in their active directory and a JSON/REST-API supports the connection with third-party solutions such as SharePoint etc.

Further Functions

Next to the previously mentioned features DRACOON also offers an Outlook-Add-In with which mail attachments can safely be send. The file versioning and the reporting-tool are also very interesting, which is why we are going to go into further detail on them in the test.

The Test

For our test we used DRACOON’s free trial version that includes all functions (except the branding-features), with no time limit and the only limit being the storage volume at 10 GBytes – very generous for a free version- and the users limited to ten. To use this offer, one must only create an account on the producers-website (https://www.dracoon.com/free) and afterwards one can start straight away.

In addition to the free version DRACOON also offers multiple fee-based enterprise-versions: with the “Enterprise-Cloud” the data is stored in certified DRACOON-computer centres with unlimited data-volume. This version is viable from 50 users upward. With the “Hybrid-

Version" that is also available from 50 users upward, DRACOON is operated from the cloud. In this case the system stores the files in the client's own computer-centre. On the other hand, the "On-Premise-Version" (>100 users) allows the installation and operation of the DRACOON solution in the clients' own computer centre.

After we created an account, we firstly created multiple user-accounts, data-rooms, assigned rights and checked if the system operated as expected. After that, we installed the Windows-Client on different computers under Windows 10 and used it to automatically synchronise the cloud-storage between these clients. Then we used smartphones under Android 7 and 8 to access our mobile data. Under iOS we used multiple iPads for this purpose. We also took a closer look at the features of Outlook-Add-In and the Reporting-Tool.

Data-rooms and User Management

The creation of the test account, multiple user accounts and data-rooms, as well as the assigning of different rights was relatively easy with help of the navigation bar from the configuration-tool and the entries "users & groups" and "managing data-rooms". If you also want to use the client-side-encryption you first have to activate it under "Settings". The responsible employees need to define a system-emergency-password, with which the data can be decrypted, if a user forgets his personal decryption-password for a data-room. As soon as this is done the system generates a pair of keys and the client-side-encryption is activated. Afterwards the users who want to use this technology on the home page need to determine a personal decryption-password, then the client-side-encryption can be used for all data-rooms.

User-rights and Decentral Administration

Concerning the user-rights the system differentiates between the role of "Auditor" and "Room-manager". The "Auditor" can view the Audit-Log, in which user-activities are being protocolled and can carry out evaluations. The "Room-managers" on the other hand, can manage all data-rooms on the highest level. They have the opportunity to create, delete and rename rooms and to assign quotas. However, they only receive the right to access content in the rooms if it is assigned to them by the corresponding room-administrator. Furthermore, there are the rights "User-manager" and "Group-manager" to manage user-accounts and groups. Self-explanatorily, "Configuration-managers" are able to see all system-settings and modify "all roles".

Ransomware Protection through the Recycle Bin Function

The paper basket that can be activated is an excellent asset for the protection against ransomware-attacks. If such malware infects the client, it too encrypts the data in a connected DRACOON-Webspace. However, this data can be retrieved from the recycle bin at any time. Permissions that can be given for the work with recycle bin include the functions "empty", "restore content" and "see earlier file version".

DRACOON

Client and Apps

The Client for Windows

First, we set up our user-account with its permissions and data-rooms according to our wishes. We then installed the Windows-Client on multiple Windows 10 computers and uploaded different files into the storage from one computer. As expected, the files where then synchronised on the other computers. The client-software acted similarly to other services such as Dropbox or Box.

The Apps for Android and iOS

In the next step we installed the client-programs for Android and iOS on their terminal devices. There we could also use the data from our DRACOON-storage. Accessing the client-side encrypted folders worked easily on all client-systems, just as the work with the uploaded data. Work with the access-rights, user-accounts and groups held no surprises either and everything acted as expected.

The Outlook Add-In and the Reporting Tool

Finally, we would like to discuss further features of the solution. The Outlook Add-In helps users to send files via e-mail-attachments more safely. Plus, after its installation it separates the attachments from the e-mail and uploads them into a special folder in the DRACOON-cloud and merely sends the recipient a download-link. With this link, the data can then be downloaded. If necessary, this process can be deactivated at any time.
The reporting-tool offers users with auditor-rights an overview over all access-rights within the cloud-storage and over data-rooms, users and groups. Moreover, this tool helps identifying users with unwanted permissions and ensures a higher security level. The solution is available as a web application under reporting.dracoon.com. If needed all data can be exported as CSV-files.

Conclusion

DRACOONs solution offers a safe cloud-storage. Thanks to its large range of functions and high performance clients it can be managed as easily as “traditional“ cloud-storages from US-providers. Compared to them however, it scores thanks to the high security level. Not least because of the multiple collaboration options for employees, the solution therefore offers an interesting alternative in comparison with these providers especially for European companies that have to adhere to the GDPR.