DRACOON

Date: *February 20, 2018*
Source: *monitor.at*
http://www.monitor.at/storyid/article/sicheres-enterprise-file-sharing-in-zeiten-einer-wachsenden-bedrohungslage/

Press Report

Guest article – Dieter Steiner, DRACOON Secure enterprise file sharing in times of growing threat

Dr. Dieter Steiner, CEO at the German cloud provider DRACOON, (photo: DRACOON)

Regensburg, February 20, 2018 – When choosing a business cloud solution, organizations should make the highest demands regarding security and take no chances.
from: Dr. Dieter Steiner

Only an enterprise file-sharing solution designed for maximum data security can effectively protect businesses from data misuse and industrial espionage. Many German companies, especially SMEs, are not yet sufficiently aware of the growing threat situation. Many only react when they have already become victims of an attack.

As explained in the BKA report on cybercrime published last autumn, 82,649 cases of cybercrime were registered in 2016, a staggering 80% increase over the previous year. The number of unreported cases will be many times higher. Even the official number of ransomware cases has almost doubled. According to police statistics, the total financial damage caused by cybercrime was more than 51 million euros. The attackers often target trade secrets, identities and sensitive data.

An enterprise file sharing solution should include the following features to ensure the highest levels of data security for users:

Effective authorization management

Entitlement control requires companies to have absolute control over sensitive corporate data and to be able to pinpoint who has access to which data. It also makes sense if user rights can also be limited in time. The download and upload releases should also be limited in quantity and time. The additional separate sending of passwords, for example by text message to the recipient's mobile phone, guarantees increased access protection of the data.

Client-side end-to-end encryption

Another aspect for maximum possible security is a triple encryption of the data – in this case triple means client-side encryption, encryption on the transmission path and on the server or the storage system. This guarantees that only the users authorized by the company have access to the company-internal data.

Many software manufacturers – above all also from the USA – propagate an integrated coding of the data. However, this happens on the server side, so when the data is already in the sovereignty of the provider. Thus, the providers also have access to the keys and thus also to the data. Such a method would, for example, not allow certification under European data protection law – keyword EU GDPR conformity – which DRACOON provides with its solution.

Integrated ransomware protection

Should ransomware, despite precautions, encrypt local drives or network drives, the data must be stored in a protected cloud environment so that they are spared from the attack. Thanks to DRACOON's integrated versioning, no files are lost: a ransomware attack overwrites the data with the encrypted data – the unencrypted versions are automatically stored in the recycle bin and can be completely and safely restored.

Dr. Dieter Steiner is CEO of DRACOON.