DRACOON

Date: *February 21, 2019*
Source: *IT-Finanzmagazin*
https://www.it-finanzmagazin.de/cloud-bafin-eba-verschluesselung-85648/

Press Report

More control with cloud storage; BaFin & EBA prefer encryption (MaRisk/BAIT/GDPR)

External cloud storage is a significant risk to the data protection of financial institutions. Without further security measures the financial institutions lose some of their control when outsourcing their data. Furthermore, data is constantly leaving the company during day-to-day business. The transport as well as the external storage space of this data can be unsafe. Even so, technical solutions were only hesitantly implemented by financial institutions for a long time. Over the past two years, this has prompted legislators and supervising institutions to take action. Especially one measure has been mentioned repeatedly in their new laws, regulations, requirements and recommendations concerning financial institutions: the data encryption.

By Marc Schieder, CIO Dracoon

Cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) have become an established part of the highly sensitive IT infrastructures in the financial sector. Already in 2017, Accenture (https://www.accenture.com/t20170905T060414Z__w__/us-en/_acnmedia/PDF-60/Accenture-Global-Risk-Study-2017-Banking-Report.pdf) reported that nearly 82 per cent of finance companies relied on cloud services. The market research institution Markets and Markets states in its market forecasts until 2021 (https://www.marketsandmarkets.com/Market-Reports/finance-cloud-market-1053.html?gclid=EAIaIQobChMIj6jqrcal2QIVCx-GCh3lnwi7EAAYASAAEgLG5fD_BwE) that the use of clouds within the finance sector will grow constantly – with an average annual growth rate of up to 25 per cent. However, the use of external cloud services also entails some risks – from a security as well as data protection perspective. Outsourcing data and the use of an external infrastructure is always linked with a partial loss of control over the security of the outsourced data. That is why financial institutions should inform themselves of the security and data protection measures of their potential provider, before buying a cloud storage solution. This also goes for the implementation possibilities of additional security measures. Some cloud services for example already provide “out of the box” safety mechanisms.

“Only if only the user of the cloud storage and no one else is in a position to inspect his data can he fully guarantee the protection of his customers' data. An encryption solution makes this possible”

However, for many companies – even in the finance sector – this is still not self-evident.

Encryption solutions – by far not the standard in the finance sector

The Gemalto-study The 2018 Global Cloud Data Security Study (https://www.accenture.com/t20181029T101708Z__w__/us-en/_acnmedia/PDF-85/Accenture-Technology-Advisory-Cloud-Readiness-Banking.pdf#zoom=50) – in which the finance sector with nearly 15 per cent made up the largest group of the respondents – paints a clear picture. Only 53 per cent of the respondents said that their company pursued a proactive compliance approach with their cloud use. And only 47 per cent stated that their company used an encryption and access management solution.

That is all too understandable. Because in Accentures' Cloud Readiness Report – Banking at the end of last year only 45 per cent of the respondents stated to have an extended knowledge in managing cloud infrastructures. Furthermore, merely 37 per cent said there company had plans to extend their security and compliance of the cloud use. A worrying number. However it can be expected to not last very long. In the past two years pressure from the legislator and supervision of the leading institutions has increased drastically. Laws, regulations and recommendations concerning data protection have been implemented. They explicitly suggest financial companies to implement an encryption solution to protect their data.

BDSG and GDPR – encryption helps data protection

Encryption as a data protection measure was first mentioned in the Bundesdatenschutzgesetz (BDSG) (https://dsgvo-gesetz.de/) in 2009. However, at that time it was only mentioned in the annex. In the revised version from 2018 it is now explicitly mentioned in the paragraphs 22, 48, 64 and 66 – as an effective measure to protect personal data. In the event of data being stolen or accessed by unauthorised third parties, companies - provided they have encrypted it - can expect relief. The normally required immediate notification of the subjects affected by data misuse may be waived.

"These requirements can also be found in the European general data protection regulation (GDPR), implemented last May. Here the articles 6, 32 and 34 are of importance."

Since disregarding the DSGVO requirements can result in considerable penalties, they are more binding. Here too – an encryption provided – reliefs are granted in case of data misuse. In addition to the elimination of the need to inform the affected parties immediately, the person concerned can also expect a reduction in his or her fine. However, it is not only due to the BDSG and DSGVO regulations that it makes sense for financial institutions to secure their data with an encryption solution.

BaFin & EBA – encryption ensures safe data outsourcing

For supervising offices for financial institutions such as the Bundesanstalt für Finanzdienstleistungen (BaFin) and the European Banking Authority (EBA), the outsourcing of data to the cloud is a regulatory relevant process. That is why financial institutions need to comply with defined regulations when outsourcing their data storage to the cloud.

"Firstly the minimum requirements for risk management of banks (MaRisk) (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1709_marisk_ba.html) and the banking supervisory requirements concerning the IT (BAIT)

(https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html) that were defined in 2017 need to be mentioned."

In order to prevent third parties from accessing the data, encryption solutions should be used. Some cloud providers state which encryption methods they use. Interested companies can therefore consult with external experts in order to assess the solutions' security level.

Last November the BaFin added an orientation guide (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_181108_orientierungshilfe_cloud_anbieter.html) explicitly for outsourcing company data to cloud providers. It points out that data security must be ensured throughout the entire "outsourcing chain" - in the case of cloud storage, from the bank to the cloud provider's server and back again. Already last July the European Banking Authority (EBA) published a recommendation (https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_DE.pdf/afd89dc3-45a7-4054-a642-d03b4e35fa1f) concerning the outsourcing of company data to a cloud. Here too, the necessity of special protection measures, for example encryption technologies, is mentioned.

"From a data protection as well as from regulatory perspective, it makes sense for financial institutions to consider encrypting their data."

But what should an encryption solution that complies with policies and regulations look like?

Server-side encryption only offers partial protection
Some cloud storage services offer their clients the option of encrypting the data they have provided for the cloud server for them. This is also called server-side encryption. This way the data is protected at its storage place - within the cloud as well as during transport. However, since the provider performs the encryption, at least its administrators have the possibility to view the data. Furthermore, the risk remains that the provider interprets the data for analysing purposes or gives inquiring authorities, e.g. intelligence agencies, access to the data. These encryption solutions hardly comply with the guidelines set by the European and German legislators as well as by the supervising companies. In addition, the provider's servers, on which the keys and passwords for decrypting the data are usually located, are a lucrative and therefore highly frequented target for cyber criminals due to the large number of customers. Therefore an encryption on the clients' side, a so-called client-side encryption, is better.

User-friendliness helps establishing a secure cloud storage solution
Even the best solution is useless if it is not accepted by the employees. That is why interested companies should look out for a secure and at the same easy to operate solution, when choosing their new cloud-storage.

„Some solutions offer clients for Microsoft Windows. This means that the cloud storage is integrated into the common folder structure and can be used as a common local storage space."

If large data needs to be send via e-mail, solutions with Outlook-plugins can help. Here the user can decide whether annexes per se or from a certain size should be send via cloud-storage. The file is then uploaded into the cloud storage and the e-mail only contains the link to the online-storage place.

End-to-end encryption gives cloud users back control over data protection
Client-side encryption is also called end-to-end encryption. Here the data is encrypted by the authorised user on his or her computer or mobile terminal device, before it is uploaded to the cloud. Only he has the key and password. Only he can decode the data again. The cloud provider and its administrators as well as the company internal IT-departments have no access possibility. They only have access to the control information that enables them to forward and route the encrypted data. During the transport as well as during storage in the cloud the data is only available in its encrypted form. Unauthorised third parties would at best be able to obtain keys and passwords with considerable effort, money and time. For this they would first have to bypass the IT security of the financial institution.
With the help of such a client-side encryption the regulation by the BDSG, the GDPR, BaFin or EBA can easily be met.

"Meanwhile a considerable number of such client-side encryption solutions that also comply with high standards of user-friendliness are available on the market."

Financial institutions that want to meet the growing requirements for data protection and data security just need to choose the fitting provider for their companies' needs.

About the author: Marc Schieder, CISO Dracoon

Marc Schieder is the Chief Information (Security) Officer at Dracoon (https://www.dracoon.com/). He is responsible for the product lifecycle from the innovation to the conception and development and further to the operation and a long-term quality assurance. Schieder completed a dual curriculum in the field of informatics and communications design. Furthermore, he has more than 15 years of international professional experience as an independent business man, managing director and chairman in the fields of individual software development, Software-as-a-Service, cloud computing and telecommunications.