Five measures for data security

The service provider SSP Europe has compiled five measures that companies should take when they want to exchange and collaborate through the cloud.

In the digital age cybercrime and economic espionage flourish. According to data from the Federal Office for the Protection of the Constitution, German companies thus incur annual losses of at least fifty billion euros. According to the 2014 study "Data Breach Investigation Report" by the American telecommunications company Verizon, which has investigated more than 63,000 incidents in 95 countries, digital espionage attacks are now the biggest threat to data security in companies. The more disturbing it is, that German companies are the worst protected in Europe, according to the current information risk index.

Collaboration in the cloud provides business opportunities for companies: Communication and data exchange can become more efficient. In addition to employees, external partners can also be involved so that companies can pursue their business objectives more effectively. Market researchers such as Gartner, 451 Research and Experton Group call such a solution as an Enterprise File Sync and Share Platform. In 2015, they expect a strong trend towards central corporate solutions for data exchange. Based on experiences with customer projects on cloud storage, Dr. Dieter Steiner, CEO of the Munich-based service provider SSP Europe GmbH, knows: "Every company has a great interest in ensuring that sensitive data is optimally secured in the cloud during the collaboration process." Only with the help of modern encryption technology can be guaranteed, that criminals or even state intelligence services can´t access the documents.

Right administration as an important component

The cloud storage expert SSP Europe recommends companies to take five measures to achieve the highest possible level of security during collaboration in the cloud with comparatively little effort.

Firstly, user role concepts should be created. Because if a company does not clearly regulate which users are allowed to process which type of data in which way, security gaps arise due to improper handling of access, transmission or storage of data. Therefore, it is important that a cloud store reflects the organizational structures of the company. This can be achieved by means of multi-level rights management for users and data rooms. In this way, it is possible to determine the possibilities that the persons have in the various data rooms. For example, you can specify what actions the recipient of a document can do with it - reading, copying, changing, commenting, or forwarding.

Secondly, data traffic should be encrypted. When exchanging data with external partners, between locations at home or abroad, or when using mobile devices, the experts recommend a comprehensive data encryption. This should be present in the transmission of data (channel encryption), on the server, which also applies to the cloud storage (server-side encryption), as well as on the end-users (local encryption). By impressions of SSP Europe GmbH the need for client-side encryption is often overlooked by cloud storage providers. "In this way, even the service provider, who hosts the data, does not have access to the sensitive content", Steiner emphasizes.

Thirdly, companies should choose the cloud storage provider and the location of the server on which the data is stored advisedly. The market shows a clear trend towards domestic suppliers. Data centers in Germany and Europe should be certified according to the ISO / IEC standard 27001. This serves the data protection, also domestic and foreign secret services be ignored according to SSP.

Companies often do not realize that they have become a victim of industrial espionage, but rather when it is already too late and a new product development that invests a lot of capital and know-how is suddenly cheap by another company on sale. Therefore, the cloud provider should periodically review and evaluate the protocol and log files, or even monitor them in real-time.

Fourth, companies should implement software for Enterprise Mobility Management. This is a system that comprehensively links and interconnects smartphones and tablets in the business environment. Apart from security aspects, the equipment of the employees should be coordinated so well that the cooperation works smoothly.

One of the biggest weaknesses in companies today are mobile devices. The uncontrolled use of smartphones or tablets by employees is a serious threat, not only in security updates, but also in the transmission and storage of data. Data are often protected by means of presets on the devices in a cloud, which the company does not have access to. Thus, mistakes in the configuration or carelessness of the application create a gateway into the data world of a company.

Employees as a safety risk

Fifthly, companies should sensitize their employees. Because they face the largest and in many places underestimated threat for sensitive data. Many users are unaware of the security gaps they create, for example by the automatic sync capabilities of mobile devices or insufficiently secure cloud services.

Companies should therefore run in two ways: on the one hand, to make the data theft more difficult by means of high technical hurdles and to offer secure solutions, but on the other hand also to train the employees' ability to deal with critical data and their awareness of self-responsibility.

The original article can be found at http://www.crn.de/software-services/artikel-105439.html