Data Filter for the Cloud

Solutions in black and white are not suitable for cloud computing

„Cloud or not cloud" is the wrong question and a „completely secure cloud" the wrong requirement. Instead key questions to be asked are, what is stored where as well as how is it processed. Therefore classification models and data encryption are mandatory, in order to be able to make the right choice and accomplish additional protection for cloud offerings.

The cloud is convenient: There are offerings, enabling data access everywhere, handing on access to colleagues, partners, customers or others all over the world as well as enabling synchronization of working environments.
However, , considering possible security deficiencies the price to pay for such convenience could be high. One of the risk are third parties getting unauthorized access to enterprise data too.
Yet, to allow the cloud either for anything or nothing, is not the answer, but to find a subtle balance between convenience and security.

Any organization has non-critical information, which can be processed by any application in the cloud. Aside companies possess data, whose processing can be outsourced under legal requirements, and other information not being allowed to leave the organization's responsibility area. But, instead of claiming an overall "secure cloud", precise security requirements can be tied data, being classified beforehand, and their proper processing procedures. In case it is legally permissible the organization can also safeguard its data with proper service level agreements (SLAs). SLAs formally define the services a cloud provider has to deliver as well as the charges for these services. Also, as part of the agreements availability, warranty, reaction time as well as security standards could be defined.

In order to be able to ponder convenience against security, it is key to understand, where generalization is possible and where a finer granularity is important (see also "Golden Rules …"). Here, many times proven and tested data leakage prevention (DLP) procedures could be a good solution.

The seven golden rules for handling the cloud provide a good motivation for a real time data classification as a prerequisite for the processing in different cloud systems.

DLP Can Help

With the operating systems' own mechanisms it is not possible to overcome the threat potential – neither on clients nor on servers. However, for convenience reasons the direct access from a client or another end device should be made available. Therefore DLP for the cloud has to be placed on the endpoints. Here solutions are beneficial, that are able to check data content at the file interfaces on clients and servers and which, if needed, can initiate a classification in real time. Such products have to meet the following requirements:

- Plug-in functionality: capability to integrate custom connections and classification models via a simple standard interface.
- Direct reaction to different cloud systems and the available application (like dropbox)
- Proper flexibility: as a result of the content-aware file checking it is not sufficient to "allow" or "forbid" something, but to enable any complex, automated action chain, including monitoring and encryption on the client.

Though these requirements are adding a further dimension to the DLP issues, at the same time solutions, which up to now had been in use for monitoring data, leaving an enterprise via USB sticks or traditional applications, can be used for securing cloud services as well.

This way, an organization can determine exactly, what data is suitable for what specific cloud provider, cloud service or even consider a public cloud. To this end the cloud as such is classified more subtle, in order to get an exact overview of the availability, SLAs and costs. Thus organizations can benefit from higher scalability and cost structures in the cloud, without putting security on risk.

itWatch GmbH ✦ Aschauer Str. 30 ✦ 81549 Munich
Phone: +49 (0)89 / 620 30 100 ✦ Fax: +49 (0)89 / 620 30 10 69 ✦ www.itWatch.info ✦ info@itWatch.de

Real Time Classification

In case a consistent data classification hasn't been made yet, the company can do this in real time: Often certain user group and employees are reliable enough, so that the choice of the correct data classification, that is rating the criticality of the information, can be entrusted to them. For these cases a dialogue may be the right tool, because here the user can classify in real time the data to be outsourced to the cloud. The classification and the whole action together with the involved information is logged and can later be analyzed in predefined reports. Afterwards user groups with a lower level of trust can use the classified data according to their access privileges.

Conclusion

Security in the cloud can be simply deployed at the endpoints and on servers, using DLP-methods and without burdening firewall systems with too much context dependency. The right DLP-procedure ensures the control of the data flow from the internal environment to different cloud services or virtualized environments. A fine-grained classification of the cloud and its usage as well as the real time classification of outbound data from the cloud can help, find the suitable measures for protection. With the proper classification, the data can find itself the environment suitable for its criticality, where it is visible only for certain applications and users.

Golden Rules for a Secure Use of the Cloud

- The cloud can be considered a secure data store, if proper encryption is applied to the data. That is true for enterprise data, if they are encrypted with company keys, which cannot be broken. Thus information can always be outsourced to the cloud, if the encryption and decryption is done on company own secure system kernels and if the decrypted data doesn't leave the enterprise network.

- All services related to the keys for securing privacy in the cloud, that is its generation, management, usage, etc., are not to be kept in the cloud, if the protected information holds risks, which cannot be delegated.

- Keys of different quality should be used: There are company keys, that are not visible (not even for the IT department) in plain text, and optional crypto keys, which can be negotiated and exchanged with customers, partners or other third-parties. Here secure procedures for the exchange have to be used.

- Field specific encryption for shared cloud applications (like Doodle) is likely to prove elusive, because the mere existence of the data allows for important conclusions. Also in many cases the "convenience" is lost, when it comes to natural sorting functions and arrays.

- Applications should not be permitted for use within the secure company infrastructure, unless its integrity has been proved, this way ensuring, that no malware from the cloud has infiltrated the application.

- Software-as-a-Service (SaaS) delivers „software from the cloud". The problems with security start as soon as the data and the application meet within the cloud, that is, when potentially risky data are being processed by potentially unknown applications on third-party "kernels", where the cloud operator has administrative access to. The problem: Data has to be in plain text for an application to be able to process it. This implies, that data, in order to be processed in the cloud, have to be decrypted first or be transmitted in plain text to the cloud. Hence, only data without privacy requirements should be processed in the cloud.

- Keep in mind: Liability for security deficiencies (e.g. concerning privacy of personal data) cannot be delegated (e.g. to the cloud provider) or be dispensed of by contracts.

by Dipl. Inform. Ramon Mörl, CEO itWatch GmbH

First released in kes · May 2012 © SecuMedia Verlags-GmbH