Database dangers in the cloud

Technology, Information Technology

Database Dangers in the Cloud How does a company apply their security to the data they store in the Cloud or what is the standard to protect your data?

One of the recommended ways to secure data stored in the Cloud is through encrypting [Lem12]. However, there are other related issues reported with encrypting as a security application. One of the prevalent concerns is the usability and fitting encrypted data in a predefined block size. As such, other standard protection protocols include: selecting good and unique passwords; as well as practicing backing up the data [Bosnd]. Also, it was appropriately advised " to select a (security) provider who ensures that each client has a separate, private environment and maintains the most up-to-date server security" [Mor11].

What are some examples of Co-Mingling Data: and what are the dangers? An example of co-mingling of data is " data (which) could become unavailable to you just because it was being stored on the same server as data belonging to someone else" (Trappler, 2012, par. 2). The danger of co-mingling of data, as noted, include inability to access the data; information being disclosed to other parties and thus, compromising the privacy and confidentiality nature of the information; being exposed to legal sanctions; among others. As emphasized, " with cloud computing, data from multiple customers is typically commingled on the same servers. That means that legal action taken against another customer that is completely unrelated to your business could have a ripple effect… a search warrant issued for the data of another customer could result in your data being seized as well" (Trappler, 2012, par. 2).

How hard is it to migrate data that is stored in the Cloud?

Data migration was reported to be a major concern in cloud computing especially in cases when cloud providers encounter significant and unforeseen problems. Traditionally, data migration to be stored in the cloud was revealed to supposedly pose no evident dilemmas. According to Goodenough (2013), migrating the data to the cloud should consider factors like the size of the data to be migrated, as well as the time or schedule for migration. As emphasized, " once you decide to migrate to cloud storage, be sure to create a strategy to direct the migration process" [Goo134]. Therefore, the ability to manage data migration depends on the organization's strategy and consideration of relevant factors identified in storing, migrating, and accessing.

What are the dangers in making changes to hardware or configurations in the company or in the Cloud?

Making unscheduled or unplanned changes to hardware or configurations in the company or in the Cloud could pose some dangers in terms of usability, access to information, and apparent dangers in security. It was revealed that:

" Companies should have a policy that states that only tested product configurations… can be deployed within the data center. Only specific versions of firewall hardware can be deployed in the various data centers. Another danger is to have a lack of options, such as single-sourced software or hardware, for various infrastructure components. If there is a common flaw in hardware or bug in software it could lead to a dramatic failure in multiple data centers" [Mac121].

Thus, the overall danger that these changes could inflict to the organization is disruption of the regular course of operations which could mean financial losses and damage in the company’s reputation and image.

References

Lem12: , (Lemos, 2012),

Bosnd: , (Boston University, n. d.),

Mor11: , (Morgan, 2011, p. 1),

Goo134: , (Goodenough, 2013, p. 1),

Mac121: , (Machler, 2012, p. 1),