Dear E-shop company

Migrate the web servers to the cloud has numerous advantages, such as an increased security system -because if someone wants to attack the company he will have to go through multiple barriers to access the information online instead of just attack the data center located somewhere- and immediate access to the files from any place due to the ability of multiple servers sites to store any amount of data from everywhere. At the same time, other advantages come from the direct company-client relationship, such as scalability to keep the business working through the most demanding days proportioning the best service to the client, flexibility to make fast deployments, location to reach new horizons and thus reach new costumers and finally the advantage of costs for only to pay for what is consumed on the cloud and no physic space. However, to make this migration correctly we must follow a series of instructions in order to guarantee its total operation.

The strategy to implement is going to be the CIA TRIAD. This is based on three important factors. First of all, the C OF CONFIDENTIALITY, in which only authorized people should be able to access restricted information. To achieve this, we will use the LEAST PRIVILEGE principle. This consists of giving accounts with different accesses and permissions to different people depending on their position on the company. For example, company workers will only have all the information about the products they sell meaning that the only one with complete access to all the accounts, client information, sales, permissions, etc... will be the manager. Now, to guarantee that the manager account maintains safe we will use a triple authentication factor to protect all the info. As the first barrier, we will use a password-based on SOMETHING YOU KNOW, it has to have more or eight digits, upper and lower case letters, at least one number, and one special character and it must not be related to the username. For the second barrier we will use SOMETHING YOU HAVE: a token is a hand-held device with a led that displays a number and the number is synchronized with an authentication server. The number displayed on the token changes regularly, such as every 60 seconds, and the authentication server always knows the currently displayed number. For the last barrier of authentication, we will use SOMETHING YOU ARE and for that, we will use iris scanning. This measures the unique patterns in the colored circle of your eye to verify and authenticate your identity. It can operate at long distances, with some solutions that leverage the modality requiring only a glance from a user.

The second factor is the I OF INTEGRITY. Here the idea is to make sure the information travels safely until it reaches its final destination: the client. To do so, we will use an HTTPS (Hypertext Transfer Protocol Secure) connection which helps create a secure encrypted connection between the server and the browser, thereby protecting potentially sensitive information from being stolen without being noticed as it is transferred between the server and the browser.

The third and last factor is the A OF AVAILABILITY. When we migrate to the cloud we will reach a global infrastructure divided into geographic regions. To achieve that we need to always be available with all the services working and avoid a single point of failure. We will use the FAULT TOLERANCE principle that considers the risk of natural disasters, power outages, and hardware failures as well as adversial threats This assures that there is no single component which, if it stopped working properly, would cause the entire system to stop working completely.

With the application of these methods, we create a secure and complete environment for both company and client information, and so ensuring the privacy and confidentiality of the information processed.

Your cybersecurity expert
SEBASTIAN MARTINEZ