Lab 1 - Cybersecurity Concepts

Cloud computing has many advantages that will allow you to improve your business in many ways. Some of these advantages are: scalability that allows you to have a greater reach, improves agility, which lets you to perform tasks more quickly and easily, and it allows you to have global access that help you to reach more customers; and all of this at very affordable rates. However, it is important to keep in mind that cloud computing also has certain disadvantages and that, if you do not have a good security system, can endanger you business.

Therefore, I will propose a strategy that will help you to migrate your business to the cloud without any worries. Multifactor authentication, for instance, consists of having different methods of recognizing people who try to enter a system. Additionally, there is a security model for information called "CIA triad" and consist of three principles: The first is confidentiality, which ensures that only authorized people can access the information; the second is the integrity, which assures that the information has not been modified or manipulated. The third is availability, which guarantees that data and services will be available whenever necessary.

The security strategy for the company are based on the aforementioned. Initially, I recommend determined groups with hierarchical levels: the highest being the person or people with the most important positions and with the greatest access to information in the company, and the rest of the positions following this exact dynamic. The idea with these hierarchical levels is that, the higher the level, the more protection the account should have since they have access to more information; this ensures that, in case the account is hacked, the damages in the company are not severe.

To guarantee confidentiality, a principle called "least privilege" is applied. This restricts the users permissions to the bare minimum. Given the above, the people belonging to the first hierarchical level will be the only ones with full access to the information, while the people who are in the lower hierarchical levels, certain restrictions on access to information are implemented. On the other hand, to stand for integrity, HTTPS protocols (secure hypertext transfer protocol) are used to guarantee that the information between the user and the server is encrypted, thus preventing it from being stolen, manipulated, or modified. Finally, availability is already guaranteed by having the business in the cloud.

Furthermore, there will be different authentication methods. It is recommended to have at least three authentication methods for a system to be completely secure. That is why, for the highest hierarchical level, the following methods for accessing information are used: First, a password must be entered. Next, a USB-type token must be plugged in the computer, then the computer asks for a code that must reach the person's cell phone to proceed with the entry. Finally, a biometric recognition device is used (it can be one of your preference) that will guarantee that the person who is trying to enter the platform is indeed who they say they are.

Finally, for the other hierarchical levels, the authentication methods that shall be implemented are password and USB token. Although these levels also need good security, thanks to the principle of “least privilege”, the additional use of a biometric identification device is not necessary since these levels have no access to the entire information. By taking into account all of the above and implementing the strategy described, you will ensure that your business will never be in danger in the process of migrating to the cloud.