Cybersecurity Concepts

Miguel Valencia Z.

August 2020

1 Introduction

The decision of migrating the company to the cloud is exceptional. Indeed, it will bring huge benefits in different aspects, such as scalability, flexibility, deployments, location and costs. This all sounds great, but, how to implement this in a safe and functional way? We'll define the Security Strategy for this.

2 Security Strategy

For the migration to be successful, the company must consider the following properties. First, they should use a Multi-Factor Authentication (MFA) system for costumers to log on their services. This is so the client has to provide more than just something they know when authenticating (a password), e.g, by supplying a code/PIN sent to their cellphones, or by providing bio-metric information. In this way, it is harder for a hacker to impersonate a client. A password manager should also be considered, as they provide strong passwords. The company should also use the least-privilege principle. This ensures that if a customer's session is compromised, only that customer will be harmed; the rest of the sessions should remain untouched. Personal data privacy should also be implemented, so client's data isn't jeopardized. This can be done by using encryption, i.e, by coding the data (protecting it from potential eavesdroppers). Therefore, HTTPS should be used instead of HTTP, as in this last one data is sent as plaintext. This will work fine because the browser knows it should trust HTTPS websites based on digital certificates, which are electronic documents that prove the identity of a website. You can always check a website's certificate by clicking the little padlock located in the top of the page. The usage of a Virtual Private Network (VPN) should also be encouraged, especially when using a public network. With this, the information sent will be safe, and the clients can even hide their locations. The web server should also respect the CIA triad: Confidentiality, Integrity and Availability. This is, clients' information should be secret; it shouldn't be able to tamper it and the service should be available whenever the client wants. I think the migration to the cloud is a very good idea, but it also means there must be more safety measures in order for the server to work properly. Everything we discussed should be implemented.