To the cloud

Next, the instructions to migrate to the cloud safely and functionally will be announced.

What we will do is create different types of accounts to guarantee the principle of least privilege. Depending on the importance of the account, the number of authentication factors necessary to enter the system will be defined. Also, a digital certificate will be requested for the company's website, using the https protocol, which encrypts end-to-end messages, promoting data integrity, and avoiding man-in-the-middle attacks.

The accounts that we will create will be the following: common customer, frequent customer, employee, supervisor, boss. In this way, the boss account will use the three types of authentication factors, the supervisor account will use two, “Something that I know” and “Something that I have” and the rest will only use “something that I know”.

Regarding the functions of each type of account, they will be mentioned below:

Common customer: The common customer account is given to new customers. They will be able to access all the items in the store and customize their account to their liking, with the restriction that they can only access their data, also, they will be imposed an amount of money that they cannot exceed.

Frequent customer: This account is granted to those customers who have already proven to be trustworthy by complying with the payment of their previous orders and therefore the restriction of the maximum amount of common customer is eliminated. This division is due to the threat of creating multiple fake accounts to breach the system.

Employee: The employee is the one who can modify the items for sale on the page. Do not have access to customer information.

Supervisor: The supervisor account has the particularity of hosting two account modes, each with different functionalities. We then define the supervisor account and the supervisor account in charge: Supervisor in charge, when the supervisor account is in this mode, the user will have absolute power over the system, will be able to access the private information of the clients in case of any inconvenience he can modify the information stored in the system. Supervisor mode, when the supervisor account is in this mode, the supervisor will be restricted from the most careful functions such as access to user information and if these functions are needed, the boss will be asked to redistribute the problem to the current supervisor in charge.

Boss: This account is unique, its function is to distribute the work, as previously stated there are two types of supervisors, these supervisors change mode over time, so if we have 3 supervisors, only one of them will be the supervisor in charge for a period determined by the company, after this period the charge will be passed to one of the two remaining supervisors. In this way, the only account that will be able to handle the most careful data and carry out the most dangerous changes in the company will be one of the 3 existing supervisors, thus hiding the account with the most power. The only one who can know who the current supervisor is in charge will be the boss. Which in addition to redirecting the work of the rest of the supervisors to the supervisor in charge of the shift, will have the ability to block the account of any member of the company, in this way if in the worst case the account of the supervisor in charge is stolen, the boss can block it.

Note that with this proposal the total power over the system is changing from hand to hand, so if a malicious individual tried to enter the system to delete information from the servers or spy on user data, he would not know. where to attack, since the probability that he will just steal the account of the supervisor in charge is low. Now in case, the boss account is stolen, then the attacker can only remove power, but not exercise it. Then the way to attack the most powerful account, the attacker would have to go through the most protected account of all, which is that of the boss to later find out which supervisor account to steal, which also has good security. Additionally note that although the boss does not have total power over your company, in the worst-case scenario, he can stop all production while solving the vulnerabilities that arise.