A safe jump to the cloud

With the boom that the internet has presented in recent decades and with it the birth of the so-called cloud, the world is experiencing a stage of globalization as it has never done before. Multiple companies provide cloud computing services, and it is becoming a necessity to be competitive in today's market. However, it is also necessary to update the security requirements implemented. It is not the same to have information stored on physical hardware, where it is protected traditionally, to having information distributed on servers in different parts of the planet which are accessed remotely.

Almost everything should revolve around the principle of least privilege. Your employees have different responsibilities and tasks and should only be able to do what their job demands. For example, a cashier only needs to alter the database to make sales but need not view or change the personal information of customers without higher supervision. The same goes for a sales report. The greater the responsibility, such as a manager's account, the more difficult it should be to authenticate. This is where multi-factor authentication comes in, which combines different layers of security to log in (something you are, something you know, and something you have). In this way, if the manager's password is leaked in a cyberattack, the attackers will still not be able to enter the system and modify information, as they would need to violate another layer.

The principle of least privilege is also a layer of security against insider attacks. It is impossible to fully trust all employees, even less if the company is of considerable size. Restricting their access to the server ensures the integrity of most of the information stored in case of internal corruption.

Besides, it must be ensured that the transit of information between customers and the store's server is secure since it includes sensitive information (such as credit card numbers, addresses, or personal documents). The way to do this is through the Hypertext Transfer Protocol Secure, better known as HTTPS, which ensures through encryption that the data travels safely through the channel. This way if an attacker steals information they cannot understand it and it will be useless. And to ensure customers that their purchase is secure, it is necessary to acquire a digital certificate to validate your website identity, this to prevent possible phishing attempts and data theft.

Once the data has arrived safely on your server, you must ensure that it is also protected in its quiescent state. One way to preserve sensitive information is through hashing algorithms. As hash functions are very difficult or impossible to invert, if you steal the data that has already passed through the hash function you cannot do anything with it. This is a safe way to verify passwords without explicitly saving them on servers.

These are recommendations to secure data in normal situations, but it is essential to be prepared for reasons of force majeure, such as natural disasters, power outages, or even damage to server hardware. Systems must be designed to avoid a single point of failure: everything can collapse if you do not have alternative plans.

It is worth highlighting the most important of all: it is necessary to protect oneself from cyber-attacks and to promote safe practices to circulate on the network. If a person is very public on the internet, posting their activities throughout the day on their social networks constantly then it will

be much easier to carry out a cyberattack against them. Passwords are usually created with some meaning for the owner (to facilitate their memorization), but this creates vulnerabilities and allows cybercriminals to have a starting point in cracking your password. In these cases, it is advisable to use a password manager, software capable of generating secure and mostly random passwords, so guessing them will be much more difficult. It is worth remembering why it is not advisable to use the same password on more than one website: if a massive data leak occurs in one site then the attacker will have access to all the others. If the leaked password is unique to the site, then the attack is contained.

Also, caution should be exercised with the use of public Wi-Fi networks. It is difficult to know if it is a legitimate network or if it is being operated by a thief looking to steal your data. A virtual private network, or VPN, helps by creating an encrypted tunnel between your device and a remote server operated by the VPN service.

To conclude, the internet and the cloud have brought with them innumerable benefits, but with it brought new challenges. In a market that is constantly evolving, it is essential not to be left behind and to look for new ways to protect our data. It is useless to give up and believe that cyber-attackers will get what they want anyway because it is a depressing mentality; and although it has become increasingly difficult to protect yourself, it is a necessary effort today: all precautions are little.

References:

- AWS Educate. (n.d.). Amazon Web Services, Inc. Retrieved August 9, 2020, from https://aws.amazon.com/es/education/awseducate/