Sara Palacios Chavarro
Sexto semestre
Análisis forense y gestion de incidentes
Universidad del Rosario
Agosto, 2020

A new security proposal for e-shop

Being part of the companies that use cloud computing to host their web servers could be difficult since they need to protect every data or information before it ends up in the wrong hands. Throughout this essay, as a Cybersecurity consultant, I will show and explain the important factors to take into account when you're migrating your system to the cloud to have a great Security Strategy and avoid attacks.

First of all, it is necessary to understand what cloud computing is and why should national or international companies should use it. According to Amazon Web Services "Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases". It will reduce your costs and allow you to have all your information on any device. The main benefits of this are: agility, elasticity, cost savings and it lets you deploy globally in minutes.

Now that you know which are the benefits of cloud computing, the second step is to take care of your clients and protect their information. To achieve this there is something called Multi-Factor Authentication (MFA), it consists of giving some extra security factors to a user who is trying to log into your website. It means that besides the username and password, which is something they know, the person will need to confirm a code (something that is given) and if they want, allow face or fingerprint recognition (something they are). A great security login should include these three factors in order to help the clients to have a safe account.

After securing your users it's important to give them privileges because even when someone passes the login security it can still be a malicious person so managing privileges on your website will help you to prevent modifications and misuse of your resources. The principle of least privilege will help you with that problem, it limits "...access rights for users to the bare minimum permissions they need to perform their work." (Wouse, 2017) so they will have privileges like reading and maybe writing but won't be able to modify any of the main characteristics of your company. Please notice that the privilege depends on the type of user who is logged in, of course, there is the superuser who can have access to everything, like the owner and the administrator of the company, but also an editor can have more privileges than a normal user but no as much as the owner.

Another important factor to consider is the encryption, it is mandatory to have all your data encrypted. digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks" (Lord, 2019) Since the idea is to transmit material through networks you will need to use the right transport protocol, the most common is HyperText Transport Protocol Secure also known as HTTPS, that "encrypts data being sent back and forth with SSL encryption" (Christensson, 2008) It will allow a safe navigation and data protection. Along with this protocol, the protection could be even better if you use a Virtual Private Network (VPN) that uses "encryption and other security mechanisms to ensure that only authorized users can access the network and that the data can't be intercepted. This type of network is designed to provide a secure, encrypted tunnel in which the data is transmitted between the remote user and the private, corporate network." (Beal, s.f.)

In conclusion, protecting your website and the information it has is easy, you just need to make sure to accomplish all these factors, manage the user privacy and privileges and then secure your network by working with HTTPS, there are more ideas and ways to protect your servers but joining the ones that I gave you your bases will be strong and your system will be completely secure. It is not difficult but effective and your users will end up thrilled with the service you are providing. Cloud computing is the future and Cybersecurity comes with it, so be aware of the benefits and the requirements that are needed to join to cloud.

References

Beal, V. (n.d.). *VPN – virtual private network*. Retrieved from Webopedia: https://www.webopedia.com/TERM/V/VPN.html

Christensson, P. (2008, October 10). *HTTPS Definition*. Retrieved from Tech Terms: https://techterms.com/definition/https

Lord, N. (2019, July 15). *What Is Data Encryption? Definition, Best Practices & More*. Retrieved from Digital Guardian: https://digitalguardian.com/blog/what-data-encryption

Wouse, M. (2017, November). *principle of least privilege(POLP)*. Retrieved from Techtarget: https://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP