1st Laboratory

Juan Murcia

August 2020

TSF, an electronic shop (e-shop) wants to migrate its services to the cloud due to the recent growth in the sell numbers thanks to the recent Tax-free days the government has realized. In order to perform this transtion as secure and fast as possible I've been tasked with the work of perform a security route plan.

The first thing that TSF ought to consider is to make this change as gradually as possible, to avoid loosing access (availability) to it's platform during the change of the hosting servers, for this purpose all the server architecture and layout must be planed while the shop is still operating on premise, and deploy the new server before shutting down the own ones.

Having this recommendation in consider, a parallel step must be performed, which consist in the data transportation to the new cloud server, non-sensible information can be sent without major security measures, but sensible information such as users info like payment method, residence, etc. must be sent encrypted and using a dedicated canal to the cloud provider if possible, all this information has to be stored using redundancy (having several backups of it) being stored with good security measures. Therefore accomplishing confidentiality and integrity.

All employees must have a responsible manage of their credentials, a good password criteria to avoid weak passwords has to be considered when an employee is registering to the shop platform, adding to that a second authentication factor has to be implemented for the employees, using SMS or a token generator app. However employees that handles sensible data such as important employees of the billing department or similar must authenticate different when is needed to read or use such information, a biometrical authentication factor might be considered and these employees must avoid at all cost public transportation, so that their 2FA hardware/software can't get stole, avoiding possible attacks, although making a transportation method for all employees is really expensive, implementing a transportation system for these sensible data handlers employees would be cheaper.

All webpages related to TSF e-shop must be implemented using https protocol and the certificate must be obtained using a digital auditor to achieve security compliance. If it's needed, telework can be implemented using the current premises as VPN's to route employee house traffic to the cloud provider through the enterprise VPN, however telework ought to be restricted following the least privilege concept, so that the employee can not access other information not related to it's role.