Name/id: Abdelkareem Yousef Mamdoh Soubar/19110022
Assignment Title: Delivato resubmission
Course Tutor: Eng. Moath Sulaiman
Submission Date: 11/7/2022

When having a security plan, we need to follow certain procedures and regulations to ensure the integrity of the security of the Delivato’s foundation.

You may ask yourself, how would these procedures be implemented? These can be provided by the following points.

- Securing the servers physically.
  - We could improve this point, by employing security guards that would allow only authorized personnel to have access to the rooms that contain the information that is sensitive and is crucial for the running process of our company.
  - If by any chance an unauthorized person was able to go through the security guards checkpoint,we tend to use biometric procedures. These could include including a fingerprint scanner at the door that is used to access the server rooms. In addition to a fingerprint scanner, a face recognition system can be also used. The reason that we implemented biometric measures, is that the ability to manipulate information can be really hard.
  - CCTV cameras are installed to record and check every one who enters important room such as the server and make sure that the right person is using the card in case they passed the security guard
- Having a backup policy.
  - Since failures are bound to happen, a backup plan and policy must be well thought of. Imagine if we lost all the information and data that our company runs on, this can severely impact our foundation to the point of bankruptcy. Once the data is lost (God forbid), we are certain that we have important and essential information that would enable our company to complete the running process in no time.
  - We would use mulie location backups and they will be used as a cold backup plus having hot backups in the compny such as snapshots for the servers, that would be happening every weekend.
- Constantly checking for vurlanbilities.
  - Our security department must always be updated with new penetration techniques that are stronger than the ones that we know from before. This can be achieved by using strong penetration testing tools and for sure our security team would have the enough knowledge that would ensure the security of our servers.
  - our policies must be based on data and testing, so we would use audit tools to check for how strong our virtual security is, and in our case we would use nessuss, wire shark, and nmap.
    Nessuss would be used to test the website and server for vurlanbilities to check if we need to update or upgrade any of our server/ software that we are using.
    Nmap is used to check the network between the Clint and the server, in case of having a port that's not protected that can be used to access the server without permission, and that what we need to protect our selves from.
    Wire shark is used to check the data that is being sent between the Clint and the server and make sure that it is encrypted and secured
    Some false positive results need to be dropped from the list of vurlanbilities.