Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Systems and Information Security
SEGSI

Topic 8

Systems management

Pinto Leite, Jorge (jpl@isep.ipp.pt)

Systems management

- Systems management is an essential, yet sometimes forgot, task on every organization
- When looking carefully to systems and infrastructures it is evident that there steps are taken when deploying them
  - Configure and connect a new asset
  - Keep the asset and infrastructure running properly
  - Removal when it is going to be replaced
- Systems management might be defined as **the centralized administration of the IT in an organization**

Systems management

- Therefore, it might include several helpers to fulfill the requisites, such as
  - Application monitoring
  - Systems administration
  - Network monitoring
  - Help and service desk
  - Automation
  - Asset inventory
  - IT security and compliance
    - In spite of not being all mandatory or applicable

Systems management

- Some of the helpers were discussed on previous classes, so let's focus on some others
- **Asset inventory**
  - A record of all the assets, hardware or software, are of vital importance for the asset lifecycle, keep a record of hardware including firmware, versions, operating systems and their licenses. By its turn, software inventory, should contain their versioning, patching, and licenses
- **Help and service desk**
  - Provides the ability to create and track issue tickets from a single place, allowing an IT expert to solve them, as well as to track issues, changes and faulty situations

Systems management

- As a common line of all the above, training
- Employees needs to be aware of how to use and manage the new asset effectively, as well as the centralized overview of Systems Management
- Deploying and managing an asset requires time, effort and knowledge
  - For the IT team, to fully usage of the centralized systems management
  - For the internal end users, to adopt eventually new approaches to use them

Systems management

- Applications have been developed for systems management, both open source and paid
- Whatever one is decided to use, as well as developing a proprietary one, its security and goals should be taken into consideration
  - And also eventual associated supply chain

Systems management

- The definition of the characteristics of the new asset must be performed with care
- Depending on the services the asset will be responsible for, its minimal characteristics must be well and correctly observed
- Including here the expected time of operation as the amount of service will probably increase
- As stated previously, this applies to any kind of asset on the infrastructure; however, we will focus mainly on systems and not on other infrastructure components

Systems management

- The *boarding on* of new systems is a repetitive operation
  - *Boarding on* should be understood as the connection of a new system to the infrastructure
- So a new system is bought, and someone must configure it and prepare it to be connected to the infrastructure
- First thing derives from this: where is it going to be placed?
- Wherever it is, it must be in a protected place like a datacenter
- Its configuration should be planned accordingly to the need of the service or services it is going to provide
  - Probably a manual installation (expert mode) and not the default one
- All services that are by default started automatically on system startup should be looked and decided to keep the default behavior or change it

Systems management

- The services it is going to provide might have banners when accessed directly
- By default, each service when accessed directly contains too much information, unneeded for the regular functioning of the service
  - And that is like a gift for potential attackers
- Each service should be configured to provide the least possible information concerning:
  - The environment where it is running (operating system, system name, system versions, etc.)
  - The version of the service
  - Any other unwanted information that will allow a better reconnaissance for the attacker

Systems management

- Standards were developed to assist the organizational structure and skill requirements of an information technology organization, containing standard operational procedures and practices to help the management of IT operation and associated infrastructure
- Information Technology Infrastructure Library (ITIL) was one of those
  - It provides a library of best practices for managing IT services and improving IT support and service levels
- One of the main goals of ITIL is to ensure that IT services are aligned with business objectives, even if those objectives change
- With the introduction of ISO 20000 series it was progressively abandoned, however are still referred to on certifications and courses

Systems management

- Previously the asset lifecycle was mentioned
- It must be kept in mind that the *on-boarding* (deploying of a new asset) is as important as the *off-boarding* (withdrawal of an asset)
- Imagine an application that is replacing an existent one
  - Will the older one still be accessible internally or externally?
- Imagine a physical device that is taken out of production
  - Will it be accessible internally or externally?
- The best option is to start stopping the services it is (or was) responsible for, until none is still necessary
- Then, power it off and disconnected from the network
  - Until that phase, all usual management operations (updating, etc.) must be performed

Systems management

- And what is going to happen to the system after removal of the network?
- Take care of permanent storage it contains
- It should be zeroed (as long as that option is available from its manufacturer or other trusted application for the same operation is available)
- On other cases, the disk should be destroyed with a hammer or similar
  - Same applies to replaced disks of every internal system