Lab: IR/DR/BC Planning

Version 1.0

University of Pittsburgh

This is the draft of lab module for SAHI Project

Table of Contents

Lab: IR/DR/BC Planning

In this lab, you will do exercise about issues of Incident Response (IR), Disaster Recovery (DR), and Business Continuity (BC) planning in healthcare domain.

Part I: Incident Response Planning

An incident response plan (IRP) is a set of written instructions for detecting, responding to and limiting the effects of an information security event.[1] Incident response plans provide instructions for responding to a number of potential scenarios, including *data breaches*, *denial of service/distributed*, *denial of service attacks*, *firewall breaches*, *virus* or *malware outbreaks* or *insider threats*. Without an incident response plan in place, organizations may either not detect the attack in the first place, or not follow proper protocol to contain the threat and recover from it when a breach is detected.

According to the SANS[2] Institute, there are six key phases of an incident response plan:

1. ***Preparation***: Preparing users and IT staff to handle potential incidents should they should arise
2. ***Identification***: Determining whether an event is indeed a security incident
3. ***Containment***: Limiting the damage of the incident and isolating affected systems to prevent further damage
4. ***Eradication***: Finding the root cause of the incident, removing affected systems from the production environment
5. ***Recovery***: Permitting affected systems back into the production environment, ensuring no threat remains
6. ***Lessons learned***: Completing incident documentation, performing analysis to ultimately learn from incident and potentially improve future response efforts

In this part, your task is to write an incident response plan specifying in healthcare domain. You can use UPMC as a potential case study.

Here are some resources to help you complete the IR plan:

1 Incident Response Planning Guideline from Department of Information Security and Policy at Berkeley. (https://security.berkeley.edu/incident-response-planning-guideline)

2 An example document has been given, please check

Part II: Disaster Recovery Planning

A disaster recovery plan (DRP)[3] is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster." The disaster could be natural, environmental or man-made. Man-made disasters could be intentional (for example, an act of a terrorist) or unintentional (that is, accidental, such as the breakage of a man-made dam).

Your task in this part is to write a disaster recovery plan for healthcare domain. You can use UMPC as a scenario to complete your DR plan.

Here are some resources to help you finish that.

1 5 Tips to Build an Effective Disaster Recovery Plan. (http://www.smallbusinesscomputing.com/News/ITManagement/5-tips-to-build-an-effective-disaster-recovery-plan.html)

2 *An overview of the Disaster Recovery Planning Process – From Start to Finish.* (The document has been given, please check)

Part III: Business Continuity Planning

A business continuity plan (BCP)[4] is a plan to continue operations if a place of business is affected by different levels of disaster which can be localized short term disasters, to days long building wide problems, to a permanent loss of a building. Such a plan typically explains how the business would recover its operations or move operations to another location after damage by events like natural disasters, theft, or flooding. For example, if a fire destroys an office building or data center, the people and business or data center operations would relocate to a recovery site.

In this part, your task is also to write a BC plan in healthcare domain. You can use UPMC as a scenario to complete your BC plan.

(A guideline from SANA Institute about BC plan has been provided, pleas check)

Part IV: Summary

Your task is to write three plans: IR, DR and BC independently.

You can use the resources provided in this lab or anything you find online. However, your plan should locate in healthcare domain. UPMC could be a scenario in your plan.

References

1 http://searchsecurity.techtarget.com/definition/incident-response-plan-IRP

2 http://www.sans.org/

3 https://en.wikipedia.org/wiki/Disaster_recovery_plan

4 https://en.wikipedia.org/wiki/Business_continuity_planning