Lab 15.1: CSIRT
IN618 Security

June 8, 2015

Introduction

In last week's reading we learned about the need to organise *Computer Security Incident Response Teams* (CSIRTs) and to prepare incident response plans before security incidents occur. In this lab we will work in small groups to start preparing plans to respond to various incidents.

1 Instructions

In your groups, discuss responses to the questions below. At the end of the class session you will briefly present your responses to the rest of the class. Each person on the team will then individually write a document with an initial response plan for your incident type and submit it in class on Thursday.

2 Questions to consider

In your CSIRT plan you should answer the following questions.

1. Considering the example response priorities on the session 14.1 slides, what are the appropriate priorities for the CSIRT in your scenario?
2. What are some ways that people in your organisation might initially recognise this type of security incident? How should they report their concerns?
3. Who should perform the initial assessment of the incident and what are some steps they may take to perform it?
4. What are the initial steps the CSIRT team will take to contain the damage caused by the incident?
5. What evidence might the team need to collect and preserve from the incident?
6. Outside of your organisation, who may need to be contacted as part of the incident response? What do they need to know? Who should manage that communication?
7. What final steps need to be taken to fully recover your orgainisations systems and restore normal operations?

3 Incident

Prepare a response plan for the following incident:

Logs show unusual access to a database containing sensitve customer account information, including payment details. The database was accessed using an exisiting account, but outside of normal business hours, and the queries run aren't typical.

4 Submission instructions

Prepare a document outlining your response plan and submit a hard copy at the beginning of Thursday's class. This document is intended to be an initial draft of a response plan that will be refined and developed further. You may need to do some research about the nature of the security incident to prepare a plan.

To get full marks for this lab you need to address all questions above in a well written (with correct spelling and grammar, of course) and well formatted document. Although this is not a research paper, you should note and cite any references you use, since they may be valuable when working on a finished plan. Although there are no specific length requirements of limits, you should expect to submit about two A4 pages.