Company Security Report

Due date: Sunday 28th October 2018 at 23:59

Please note: This is a research assignment **not** an implementation assignment. i.e. you are gathering information through research. You **must not try to hack** into a company to find vulnerabilities.

Assignment Specification

You have started working in an FTSE/ISEQ listed company (this will be assigned to you). This company has received a directive from its CEO to increase security awareness. You have been asked to compile a report for the company. The detail of the report is defined to include the following tasks:

Task 1:

Describe the business that your assigned company is involved in. In particular identify their assets that will need most protection (their "Crown Jewels") such as client lists, current product pricing, future acquisitions, safety, intellectual property etc.

The company is concerned about its internal security awareness. You must:

- Identify at least four websites where you can get details of the most current malware threats.
- Compile a list of eight of the most recent threats which may be of specific interest to the company, including the following information:
    - The risk analysis of the threat
    - What type of threat it is
    - How it works
    - How you can remove it

The CEO is concerned about ransomware so you must detail the use of ransomware in online attacks.

Task 2:

There is a concern about how the company's internet presence makes it vulnerable. You will write a report on the footprint of the company.

- The first part of this section should consist of a discussion on what footprinting is and a selection of what methods are employed and how.
- Write up the details of any weaknesses which could be exploited in the targeted company based on your research of the company activities and footprint.
- Give solutions to resolving these weaknesses.
- Explain whether and why a company security policy should extend to social networking and other uses of the internet. Detail specific threats.

Task 3:

The company has a number of concerns around physical and digital access to private parts of the company property. An external security expert has informed management that social engineering could be used to bypass the authentication systems. You are asked to report on this.

- The first part of this section should detail what social engineering is and how it might affect the company specifically giving examples
- The second part of this section should detail good practise that should be employed in the company for both physical and digital authentication, this should take account of the nature of the business.
- Finally you are asked to provide recommendations around what authentication systems should be implemented to prevent physical access.

Submission Criteria

Your final report including all three tasks should be between 3000 and 8000 words and should have accompanying diagrams and graphics to support your findings and conclusions. Each task of the report carries equal marks. The report must be completed individually.

NOTE: **Any content copied and pasted will be discarded**; all work must be your own. The report should be **12pt New Roman font, single line spacing**. Your report should include a title page, table of contents, page numbers and bibliography.

Please refer to the late submission penalties below:

- Up to 1 calendar week delay: 20% of the marks available for the assessment
- Up to 2 calendar weeks delay: 50% of the marks available for the assessment
- Over 2 calendar weeks delay: 100% of the marks available for the assessment