Assignment Two (30%)

Submission due date: 27/9/2020 – 11:59 PM

Ministry of Social Development Security Breach Review

The Ministry of Social Development is New Zealand's largest government department providing services to more than 1.1 million clients. It receives in excess of 230,000 calls a week, and approximately 40,000 online applications a month. Like many organisations in the public and private sectors, the Ministry sought to improve its service delivery. One of these initiatives was the implementation of self-service "kiosks", completed in October 2011. In the Ministry environment, the "kiosks" were essentially ordinary computers that were readily accessible to the Ministry's clients in its Work and Income service centers. These kiosks provided valuable information and tools, with a particular focus on supporting job seekers.

However, the Ministry's information security was breached. In one instance, a breach allowed a client to download 7000 documents from the Ministry's network, via kiosks set up for job-seekers in two offices. These documents included invoices detailing the medical conditions of children in state care, the names of people being investigated for benefit fraud, and pay rates for individual Ministry contractors [1].

Tasks and Marking Criteria [70 Marks Total]

Make sure you read the attached Deloitte report thoroughly and provide a document detailing the following tasks:

1. **[5 Marks]** Provide a figure highlighting the architecture of the Kiosk network and services. The figure must include the network topology, software and services running on the kiosk systems and servers and, the type of security controls/mechanisms in place.

2. **[10 Marks]** Identify and discuss the **shortcomings and vulnerabilities** in the design of the kiosk system and its architecture. You should also mention and explain the type of the **threats** in which those vulnerabilities could potentially be exploited.

3. **[10 Marks]** List and briefly explain the containment strategy, Incident Response (IR) and Disaster Recovery (DR) actions taken by the Ministry in response to the incidence. This should also include actions taken by all incident handlers on this incident.

4. **[10 Marks]** Identify and discuss the **shortcomings and vulnerabilities** in the Incident handling and disaster recovery process and procedures.

5. **[30 Marks]** Citing NIST SP.800-61, NIST SP.800-53 and NZISM [2] and/or other relevant standards discuss in details how such an incident and security breach could have been mitigated by using the following controls:
    a. Deterrent and Preventive controls (e.g. Banners, locks, CCTV, packet filtering, access control, encryption etc.)
    b. Detective controls (e.g. CCTV, HIDPS, NIDS, Audits and logs etc.)
    c. Responsive and corrective controls (e.g. Incident response, removal of malicious files by an antivirus, Backups, Disaster recovery plan, Business continuity plan etc.).

6. **[5 Marks]** Writing and presentation of the report

Notes:

You do not have to rely on the recommendations of the report to suggest adequate controls or improvements and may use your own domain knowledge of the controls. The recommended controls should specify and include the following:

- The type and description of the control
- Description on how the control could/should be applied to the kiosk system, its architecture, processes and procedures
- The type of threats/vulnerabilities those controls will protect the information system from
- How the information system design, processes and procedures could be improved by utilizing the recommended control
- How the information system design, processes and procedures would change based on your recommendations
- How your recommended controls would mitigate or minimize the risks introduced by the identified shortcomings, vulnerabilities and associated threats

- All controls and recommendations must be referenced using appropriate sections in the NIST or NZISM documents, highlighted by the document name and section number (e.g. NIST SP.800.14 Section CP-13)
- Some of the relevant standards and guidelines have been attached as reference.
- NIST SP-800 series standards and guidelines can be obtained from: https://csrc.nist.gov/publications/sp
- Avoid direct copying and plagiarism at any cost. Direct quote should be within "*double quotations*" and "*Italic*". Minimal number of direct quotations should be given in the main report. Attach direct quotations from the standard documents as appendices at the end of the report. References to the guidelines can be in the format of (**examples only**):
    - A two factor authentication system [3] should have been installed to authenticate the kiosk admin. This would have provided an additional layer of authentication for privileged account (i.e. administrator) and would have avoided or minimized the risk and threat of brute force and dictionary attacks against the authentication system. A two factor authentication system must be applied to all admin accounts either accessed from the internal network or remotely. In the case of Kiosk system, a combination of password and pin number sent to a verified admin number would be a good choice. The authentication system and the system generating the PIN number must be placed within the vicinity of the ministry's office which

    is only accessible physically by authorized personnel (i.e. Admins only), ideally in a separate room accessible by a Card.

    The 2FA systems should also be placed within an administrative network and isolated from the internal and external networks by a dedicated firewall and placed within on its own VLAN. The firewall rule restricts access to those resources.

    - According to the guidelines provided in the SP800-14 section 14-3 (Please see Appendices 3.A - you may copy the relevant rule to the appendices) a firewall (NIST SP.800-41 Section 2.11) should be deployed between the internal network and the external network. This firewall monitors and filters packets from the external and insecure networks destined for the internal hosts. The firewall should filter and monitor port 22, 23, 24, 25 and log any connection attempts on port ports. An IDPS system monitoring the dedicated subnet should inspect the filtered ports for potential violations as instructed by NZISM section 18.4.8 and section 18.4.11. This would have helped reduce the risk identified by Deloitte in section 5.4.
- You may use other sources to gather information about the incident or the architecture of the kiosk or kiosk services and reference them with proper citation. Use any numbering references (e.g. [1], [2,3])

What to submit:

- Please submit a document (preferably a pdf file) containing answers to the tasks in the assignment.
- The report should not be less than 6 and exceed 12 pages (excluding appendices).
- Please provide your answer using the appropriate task numbers (e.g. 1, 2...5.a) and in the order
- Please state the course code and your name on the document header
- Diagrams (if any) must be included in the document file
- Plagiarism will be dealt with under the University policies and “copy and paste” answers will receive much fewer marks than one you have written in your own words.

References:

[1] - Bennett 'mortified' at MSD security breach, Radio NZ, October 2015
[2] - New Zealand Information Security Manual available at: https://www.nzism.gcsb.govt.nz/ism-document/
[3] - Implementing Multi-Factor Authentication, Australian Cyber Security Centre (ACSC), January 2019, available at: https://www.cyber.gov.au/sites/default/files/2019-03/Multi_Factor_Authentication.pdf

The criteria for grading are:

- Completeness – Did you complete all the tasks and how comprehensively? Did you Provide explanation where necessary.
- Accuracy - How well did you complete the tasks?
- Presentation - Did you use the right terminology? Please check for readability, we mark a lot of these and generally we look more favorably on well-structured and well-written ones.

Letter grades

A-range:

Complete, accurate, and well presented. Shows good knowledge and good understanding of methods. Well-argued. Where required, contains good original input from the student.

B-range:

Mostly complete, mostly accurate, and well presented. Shows a good knowledge and fairly good understanding of the methods but either fails to complete some parts of the tasks or is unclear or is poorly argued.

C-range:

Satisfactory performance although some errors in accuracy and/or problems with presentation. Shows only some basic knowledge of the material or fails to understand some important parts of it, or does not provide solutions to a significant portion of the tasks.

D-range:

Poor performance overall, some evidence of learning but very problematic in all aspects mentioned above.

E-range:

Well below the required standard.

	Excellent [8-10] "A"	Good [6-7] "B"	Satisfactory [5-6] "C"	Poor [4-5] "D"	Well Below Standard [0-3] "E"
Victoria University Indicative Characterisation	Excellent performance in most respects to outstanding performance.	Good performance overall but some weaknesses to very good performance	Adequate evidence of learning to good performance	Poor performance overall, some evidence of learning. Fail.	Well below the required standard. Fail.
Work done – Did you complete all the tasks and how comprehensively?	Completed all the tasks or included all relevant points in an answer.	Completed the core tasks or most of the relevant points. Missed some tasks or points.	Completed at least half of the tasks or covered half of the main points correctly.	Started and completed some tasks successfully or included some of the points but these had many wrong answers.	Made some attempt but tasks were not completed correctly or only addressed a small number of points required.
Critical thinking – When answering the questions, how much thought was put into the answers?	Shows understanding of the technical issues from different perspectives; understands the limitations of answers and potential for further investigation.	Strong comprehension of technical issues but limited understanding of limitations or room for improvement.	Exhibits a basic grasp of the technical issues form the most important perspective, without considering others. No real considerations of the limitations of the answers.	Incomplete understanding of technical issues involved. Overall analysis or evaluation is limited and may contain minor errors or deficiencies. Some evidence of reasoning. A cut and paste answer would fit here.	Little or no evidence of analysis, evaluation or the formation of judgements.
Presentation - Did you use the right terminology? Please check for readability, we mark a lot of these and generally we look more favourably on well-structured and well-written ones.	No spelling errors, no discernible flaws in punctuation, grammar and sentence construction.	Very few spelling errors, correct punctuation, grammatically correct, complete sentences.	Lapses in spelling, punctuation and grammar, but not enough to seriously distract the reader.	Many spelling errors, absent or incorrect punctuation, and/or severe grammatical errors.	Difficult to understand what is being conveyed to the reader.