Workshop 8 - Week 9

INFO30006 Information Security and Privacy 2020

Task 1

Navigate to ninite.com and use the home version of Ninite to download one or two apps.

a. What are the advantages and disadvantages of using a program like Ninite?
b. What extra features would you want in order to use this in a business environment?

Note: Ninite is Windows only. If you are using another OS, watch this YouTube video to see how it works: https://www.youtube.com/watch?v=M5NYC3BNhqs

Task 2:

Imagine you are the IT administrator of a small business organization and are responsible for managing the organization's computers. The cybersecurity department has notified you of a vulnerability, which is already being exploited in the wild. The impact of the vulnerability is large and has already impacted the infrastructure of several foreign government organizations. A fix is already available as part of a major operating system upgrade (e.g. Windows 10), but your organization is not running this version of Windows due to the continued use of some legacy software.

a. What are the challenges involved in securing your organization from this threat?
b. How might the organization handle this situation?

Task 3

Imagine you are consulting for a small business with 15 employees. The business does not have a dedicated IT technician, but the assistant manager has strong IT skills. Consider the list of security mitigation strategies at https://www.cyber.gov.au/sites/default/files/2019-03/Mitigation_Strategies_2017.pdf. Of these:

a. Which are the top 5 strategies you would recommend the business implement? Why?
b. Which do you expect a typical small business of this size is probably using already?

Task 4

For this task you should split into groups. Each group should select one of the following attacks/data breaches:

- Olympic Destroyer
- Mirai
- WannaCry
- ShadowHammer

Discuss the following points:

- Who was (likely) behind the attack & what was their aim?
- How did the attack work?
- Who was affected by the attack?
- How could the attack have been prevented/mitigated?
- What lessons should small/large businesses learn from the attack?
- How fearful should businesses be of this type of attack?