Security in Organizations (SIO)

Assignment 1 - 2021-2022

Goal:

- Understanding the essence of information security from a practical and theoretical perspective.

Instructions:

- This assignment must be completed by a team of two students.
- The assignment must be written with the Times New Roman font, in size 12pt, with normal spacing. The subtitles are in bold, and the margins must be all of size 2.5cm.
- The original numbering of the questions must be indicated for each answer.
- State your answer in a succinct and clear manner.

Deadline:

- Submit the assignment in a PDF document through Brightspace before **2021/10/07 23:59.**

If and only if you do not have a Brightspace access, you can submit your assignment by email to Anna Guinet (see SIO website) in a PDF document.

Part 1.

A. Explain:

a. what is ransomware, and
b. how computers of individuals are infected, and
c. how infected computers are misused by criminals.

This analysis should be at most 2 pages and should include references to the sources used.

B. Describe:

a. how can ransomware affect *you* personally, and
b. what measure(s) *you* can take to reduce the risks, and
c. what measure(s) *you* actually implement.

Make a distinction between preventive, detective and corrective measures. How would you rate the residual risk that ransomware poses to you?

This analysis should be at most 2 pages.

Part 2.

C. Present the DigiNotar breach and its impact based on the Fox-IT report (see the SIO website).

In the form of bullet points, formulate 10 lessons for organizations from this incident. Make a distinction between:

a. technical lessons and security management lessons.

    b. lessons for organizations like DigiNotar, and for organizations relying on such organization like the Dutch Government.

D. Relate each of the 10 lessons with the corresponding Chapter of the ISO 27002:2013.

On p.35 of the Fox-IT report, it is mentioned that the attack on the DigiNotar certificate issuing systems emerged from the “BAPI-production workstation”. This workstation and the certificate issuing systems were located on the network *Secure-net*. The Fox-IT does not reveal how the attackers gained access to the workstation. However, this is revealed in the court ruling (use Google translate if you do not understand Dutch):
http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2014:4888

E. From the court ruling,

a. state clearly the main reason why the attackers gained access to the “BAPI-production workstation”.

b. Why the firewall did not prevent this?

The part 2 should be at most 3 pages.

The assignment should be seven pages at most.

CALCULATION OF THE GRADE	
Question	Max. points
A. Presentation ransomware	3
B. Impact ransomware	3
C. 10 lessons	2
D. ISO 27002:2013	2
E. BAPI-production workstation	2
SUM	**12**
Grade = (1 + 9*(sum_of_points / 12)) rounded to the nearest 0,5 point.	