Mandatory Assignment 3

Bendik Egenes Dyrli, Øystein Andreassen, Anne Grethe Heltne

03.11.2017

Exercises

Ex. 2

Assume that a security model is needed for the protection of information in your class. Using the CNSS model, examine each of the cells and write a brief statement on how you would address the three components occupying that cell.

Technology	Material is delivered through secured “instructure Canvas” sessions through web browser.
Confidentiality	Only students and teachers of the course should have access to the course material
Integrity	Material and assignments, including delivered assignments should not be tampered with.
Availability	When logged in students and teachers should have access to the material
Storage	Course material should be stored on a secured server
Processing	Students should be able to access course material and assignments, and deliver answers for assignments
Transmission	As Canvas is web based all material and assignments need to be transmittable
Policy	Course material should be generally available, while assignments have specified time periods of availability which is set by the teacher. Deliverance of assignments are also bound to this timeframe.
Education	Training and documentation for teachers how to use the system and set up policies. Students should have documentation on how to use and access.

Ex. 3

Consider the information stored on your personal computer. For each of the terms listed, find an example and document it

Threat	Robbers stealing the hard drive
Threat agent	Robbers
Vulnerability	Weak encryption,weak password on encryption, no encryption at all
Exposure	Physically available
Risk	The risk of robbery is low
Attack	Robbers are made aware of the computer system, breaks into the house when no one is there and takes the computer system or hard drive
Exploit	Lockpicks or other physical methods of breaking into a house

Ex. 4

Using the Web, identify the chief information officer, chief information security officer, and systems administrator for your school. Which of these individuals represents the data owner? Data custodian?

Since it's hard to tell apart from the people who is working as what at UiA, we didn't find to much, other than we know that Sigurd Kristian Brinch is system administrator. To say it in the terms of the exercise, Brinch can be acknowledged as a Data Custodian.

Ex. 5

Using the Web, find out more about Kevin Mitnick. What did he do? Who caught him? Write a short summary of his activities and explain why he is infamous.

Kevin Mitnick primarily used social engineering to break into computer systems in the late 20th century. He was caught by Tsutomu Shimomura. He is famous as he broke into big companies and government entities. He was also the first hacker on the FBI top 10 wanted list. He wrote a book called Ghost in the Wires and got interviewed about it. A movie and a documentary was created about him as well.

Case Exercises

The next day at SLS found everyone in technical support busy restoring computer systems to their former state and installing new virus and worm control software. Amy found herself learning how to install desktop computer operating systems and applications as SLS made a heroic effort to recover from the attack of the previous day.

Questions

Q1.

Do you think this event was caused by an insider or outsider? Why do you think this?
The email subject and body is generic enough to which it could have been massively spread with no specific target in mind, it also seems to spread through the use of the victim's contact list.

But from the information given it seems the only purpose of the virus was to stop or halt production and causing the company damage in form of lost productivity, one could assume it's launched from a competitor to gain an advantage, or from a disgruntled employee.

Given the lack of evidence either way, we can't justify a particular party.

Q2.

Other than installing virus and worm control software, what can SLS do to prepare for the next incident?
Install spam filters at the edge, and implement rules for which extensions are allowed as attachments.
Also user education is important, to keep reminding the users to always be aware of opening attachments and clicking links in emails, even from trusted sources. The technical support department could send out fake phishing emails and see how many employees who click on the link in the email. This way they can see if they need to have more security courses.

TQ3.

Do you think this attack was the result of a virus or a worm? Why do you think this?
Assuming that it is self replicating by sending itself as an attachment to the contacts in the victim's contact list, this is a worm. [1]

Sources

[1] https://usa.kaspersky.com/resource-center/threats/computer-viruses-vs-worms