Khai Phan Thanh (100901164)

BTN710

1. Name 5 malware types of your choice. For each type describe how it is propagated and for three of them provide a real-life example. (1 point for naming, 2 for propagation description, and 1 for each example)

* **Virus**: The virus stays in the file. Even if the user receives the data without executing the data, the system will still be safe because only when the user runs the data can the virus transfer to the user’s computer like any other file is executing. Once the virus is out and infects one of the files/programs, it can quickly spread to others and hard to keep track even by the anti-virus program. I was once experiencing with viruses when I download a private file (a cracked game) on the wrong website. When I execute, the anti-virus keeps telling there is a virus in the system, and the notification just goes up non-stop. As a result, I have to re-install Windows to remove all of the viruses.
* **Worms**: One of the methods to receive worms is via emails or phishing emails. The worms will be spread out into the user's computer when the user clicks on a file attached to the email. Not only that, but they also detect the user's mailing list and automatically send itself to other people. Since worms use the internet to infect other users, one of the results users could face is the slowdown of the internet, especially the server. The damage mostly stays on the system vulnerabilities, not really on the user's system. At my workplace, one time, a colleague of mine received a phishing email, where the head title seems to be a document sent from another employee in the building. Without any awareness, she opened up the file but didn't notice that the data was named as (something.docx.exe). After just about 5 minutes, the entire server and internet connection in the office was slow down very quickly, and the IT department came it and had to reset the server and remove the worms.
* **Spyware**: Unlike above malwares, where it requires actions from the end-user, spyware can come from any of the downloads you have, and it will secretly install on your computer without you and even anti-virus aware. Spyware is used to track users' habits, such as browsing the Internet or any behaviour activity and sending the data back to the sources. Users will only notice about spyware when they experience a very long wait time to access the Internet (the more spyware, the more Internet usage) or a slow down on the computer. At least 50% of users who use computers, especially on the Windows platform, have spyware on their computers. I have once experience with spyware, where I notice there is a considerable amount of usage for the uploading (about 1mb/s). It caught me right there because I knew I wasn't using any apps or work required to upload anything. However, I can only watch it sending up my information over the Internet because there is no pop-up from my Anti-Virus about that, so I have no clue where I should start to remove it.
* **Ransomware**: It works like a virus, except that when the ransomware attack, it will lock up all of the data stored on the device, and the user will have to pay a “fee” to rescue it. The virus will encrypt the data in a certain way that only the one who made the attack knows how to solve it. Since there is no way to determine what kind of malware will hit your computer, it could be an easy one, like Spyware or a super hard one like ransomware. It is good to avoid unknown websites or sources even not to download anything. Most targeted for ransomware will be a company or individual with lots of valuable data. The only way to get out of this is to replace a hard drive, which means all of the data will be gone if there is no backup.
* **Trojans**: sometimes known as Trojan Horse, begin to replace worms because they both have a similar attacking way. Still, Trojan provides broader methods of access to user’s data. Instead of a suspicious email, Trojan is hidden from a website, and the link to the site will be hidden into one of the programs (a regular, trusted one) or sometimes email. When the user clicks on one of those, a website will be pop-up, and the Trojans have been given permission to access the system. Unlike worms, Trojan can steal your data, install more malware, modify user’s data and even worse, destroy the data. However, Trojan cannot duplicate itself until it found worms, and the result will be endless.

1. Name 3 types of attackers discussed in the book and slides. For each type list an incentive. (1 point for naming and 2 for each incentive). As we go forward, we come across new types of attackers. Think of an attacker type not mentioned in the book or slides (2 bonus points).

* **LulzSec** explained that they felt as "latter-pirates" and boasted they were "god" when they could attack a site, and Sony is among them. One of the potential reasons why they chose Sony is because, just before the first attack a few months, there is a court case related to the jailbreaking PS3. On the first Sony attack, the PSN system had to go offline for a few days to avoid the attack. The main reason overall is they just attack for the attention of the world.
* **Anonymous**is the largest hackers group that still exists in the world today. Anonymous is very well-known in the IT industry as well as the world for the attack achievement. Their target is mainly about a political, legal matter, societal injustice and related. The main reason is they want to speak up, but instead of protesting, they are hacking. It seems to spread the message more because the website they usually attack the one that has lots of traffic coming in and out every day. They typically don't have a motive for an attack, when they want to do, they just do it. The signature method Anonymous group uses is to have a botnet system to send a massive amount (more than a million) traffic to the targeted website. The website will then be shut down in just a few minutes (because they can't handle all the incoming traffic).
* **Edward Snowden**is a well-known hacker for his information leaked about the NSA is spying on the cities all over the time. He revealed facts and evidence that the NSA has been collecting ten million Americans' telephone records every day, which telecommunication company was forced to do so. Besides telecommunication companies, online communication companies such as Google, Facebook, or Yahoo also targeted to do so. Prism is secretly developed to help NSA "surveillance" American citizens from a distance without their awareness and consent. His action is to raise the awareness of all people around the world that they might not be safe as they think they are. The government is always watching you without you even being aware.
* **DCLeaks is an old group formed in June 2016 based on America. The group seems to “registed” in America but it is represent and working for a Russian group called Fancy Bear. What they do, is to aim and tell the truth about U.S decision-making on critical situation and about American politician life. The member was arrested in 2018 for charged against obtaining access and distributing information of about 500.000 American citizens voter as well as personal email of many politician. They also acknoledge about the interference in the 2016 US elections.**

1. In security planning we need to consider both “weakest link principle” and “defense in depth” (3 points each). Explain each separately, and describe their role in providing security (3 points each).

* **Weakest link principle** refers to the weakest spot in the security system that has a higher chance of getting attack than the other. The software must be able to sustain for an attack even if it was attacked on the weakest possible spot. If the software/system is unable to maintain after an attack, the principle is considered a failure and the security developer must work on it as soon as possible. The role here is to identify which is the weakest spot in the application security and see if it is sustained or good enough to handle an attack or not. Security developers can’t equally develop all aspects since there will be one important than the others.
* **Defence in depth** is to entirely focus on security in one aspect (known as single-point vulnerabilities) and consider that would have higher chances of being attacked than other security aspects. Security develops a chain of “shields” to defence several countermeasures from attackers. This prevents attackers from getting into the system because they have to breach multiple defence lines to gain control.

1. Consider the relation between Seneca College and yourself. Explain each PIPEDA principle in this context, either using an example or an explanation. Do this in less than 50 words per principle. (3 points per principle)
2. **Accountability**: Seneca College is responsible for my personal information (such as personal email address, phone number, home address…) and assigned a specific who is trustable enough to account for all of the data.
3. **Identify** **Purpose**: Seneca College will be disclosed to students which information they will collect and use for which purpose. Upon agree from the student side, Seneca College will be able to collect that information. Still, they are not able to use any of that information without consent from students.
4. **Consent**: Students have the right to accept or deny any information usage requests from Seneca if they feel uncomfortable, and Seneca College will not be able to use it. Seneca College, on the other hand, must inform students what kind of information they will use and use for which purpose.
5. **Limiting** **Collection**: Seneca College can only collect information that will be required from the College site to prove the students is part of Seneca College. The data can only be used for lawful means.
6. **Limiting Use Disclosure and Retention**: Seneca College can only retain student’s personal information as long as the student is still participating in Seneca. After that, Seneca has no right to use any of that information, without Student consent. Unless required by law or with permission from the student, Seneca College cannot use that personal information for any purpose.
7. **Accuracy**: Seneca College has the right to keep student’s information up-to-date, with precision and complete as much as required for future use (if necessary, and with student’s consent)
8. **Safeguards**: Sensitive data must be carefully protected, and responsibility belongs to Seneca if the information is leaked or used without acknowledge.
9. **Openness**: Students at Seneca College must be prompted about the policies and practices relating to how Seneca will manage and keep their personal information.
10. **Individual** **Access**: Seneca College must give their students access to the information they provided to Seneca.
11. **Challenging** **Compliance**: Students who provided information to Seneca must meet compliance that all the information is correct, accurate and ready to be used when is required
12. You are asked to choose between two different countermeasures to protect the internal network of a company. You have evaluated the total value of  the internal network to be around $2,000,000. You have estimated that on average, there are 5 successful attacks, with an average exposure factor of 80% (per attack). The candidate countermeasures are:
13. **Countermeasure A: Intrusion Detection System (IDS)**

* This IDS system detects abnormal behavior within the network reduces the damage (loss) of a compromise by 85%. The company needs to spend $20,000 per year to purchase the license for the IDS software.

1. **Countermeasure B: Firewall**

* This firewall controls the incoming and outgoing traffic of a network. This helps reduce the probability of a compromise by 60% and the damage of a compromise by 50% on average. The company can buy this firewall for $100,000. Each year after the first year, the company needs to spend about $10,000 on updates and maintenance.

For each countermeasure you should calculate the net countermeasure value for a year, for 2 years, and for 5 years, and compare the two countermeasures for 1, 2, and 5 year plans.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Base Case | Countermeasure A | Countermeasure B |
| Asset Value (AV) | 2.000.000 | 2.000.000 | 2.000.000 |
| Exposure Factor (EF) | 80% | 80% | 80% |
| Single Loss Expectancy (SLE) = AV\*EF | 1.600.000 | 1.600.000 | 1.600.000 |
| Annualized Rate of Occurance (ARO) | 50% | 50% | 25% |
| Annualized Loss Expectancy (ALE): = SLE \* ARO | 800.000 | 800.000 | 400.000 |
| ALE Reduction for Countermeasure | N/A | 800.000\*15% = 120.000 | 400.000\*50% = 200.000 |

1 year

|  |  |  |  |
| --- | --- | --- | --- |
| ALE Reduction for Countermeasure | N/A | 800.000\*15% = 120.000 | 400.000\*50% = 200.000 |
| Countermeasure Setup Cost | N/A | N/A | 100.000 |
| Annualized Countermeasure Cost | N/A | 20.000 | 10.000 |
| Annualized Net countermeasure value | N/A | 100.000 | 90.000 |

2 year

|  |  |  |  |
| --- | --- | --- | --- |
| ALE Reduction for Countermeasure | N/A | 800.000\*15% = 120.000 | 400.000\*50% = 200.000 |
| Countermeasure Setup Cost | N/A | N/A | 100.000 |
| Annualized Countermeasure Cost | N/A | 40.000 | 20.000 |
| Annualized Net countermeasure value | N/A | 80.000 | 80.000 |

5 year

|  |  |  |  |
| --- | --- | --- | --- |
| ALE Reduction for Countermeasure | N/A | 800.000\*15% = 120.000 | 400.000\*50% = 200.000 |
| Countermeasure Setup Cost | N/A | N/A | 100.000 |
| Annualized Countermeasure Cost | N/A | 100.000 | 50.000 |
| Annualized Net countermeasure value | N/A | 20.000 | 50.000 |

* In the first year, countermeasure A would have better net countermeasure value than countermeasure B. However, the later on (many years later), it seems that countermeasure B has better value due to it low annualized cost (only expensive for its setup cost), therefore, A is better in the short-term but B is better in the long-term.