<date that the hw is uploaded>

Introduction to cyber security 156360

semester a 2020-2021

hw # \_1\_

machon tal english speakers

|  |  |
| --- | --- |
| Teudat zehut | Student Name |
| 006798775 | Gila Odes |
| 209927128 | Tamar Harizy |

Question 1

Links to articles used for Security Report:

Cyber Attack on France Beijer Ref -

https://www.cybersecurity-insiders.com/cyber-attack-on-france-beijer-ref/

Montreal's STM public transport system hit by ransomware attack

https://www.bleepingcomputer.com/news/security/montreals-stm-public-transport-system-hit-by-ransomware-attack/?&web\_view=true

**Security Report Week of October 18th Cyber Security Threats**

Over the past week (in fact over the last 4 days!) there have been two incidences that have proven to us, again, how much damage and expense cyber-attacks cause. The first attack occurred in Montreal and was an attack on the STM public transport system. The second attack occurred in France and was an attack on an air-conditioning and refrigeration company *Beijer Ref*. in both of these cases, the cyber-attacks fell under the category of Ransomware attacks as hackers demanded large sums of money to rectify the damage they caused.

*Montreal's STM public transport system hit by ransomware attack*

**Who were the attackers? What Category of hackers are they? What was their motive?**

This ransomware attack was so recent that the exact identities of the hackers have not yet been revealed, however, it is believed that a gang of online hackers are responsible. This gang have created a ransomware software “RansomExx” which is a is a rebranded version of the Defray777 ransomware. This virus has been affecting online system services since June. This continual hacking of companies to force those attacked to “pay-up!” places our attackers in the **Black-Hat** category as their motives are criminal. Their greed and want of money was a motivating this behaviour (along with the fact that they are simply getting away with it).

The attack surface of this ransomware attack was their “RansomExx” operators which latch onto the Network and encrypted files – then spreading laterally throughout the system by gaining access to the windows controller. The system was vulnerable to the attack as files on the system were not encrypted and even though the company did have in-place some cyber-security, it was not enough to deal with this type of attack.

**What was the attack surface? What vulnerability did they exploit?**

IT systems, the main website and Customer Support were all down due to this attack.

**Which assets could be attacked? Which CIAS’s were attacked?**

Seeing as this was a ransomware attack – the sole purpose was to shut down the services of the company (effect availability) so that they can be exhorted for Ransome. The fact that the hackers had access to the entire system is a definite breach of Confidentiality and them changing the software to force their own software on the server is a breach of Integrity. Specifics of Availability, the buses and transport lines still functioned; however, those people with disabilities who generally use a door-to-door service (which they order online) could not access this service.

*Cyber Attack on France Beijer Ref*

(a)When asked who the attackers were – we do not know. All we know is that whoever organised the attack falls into the **Black-Hat** category as they were doing this for criminal motives to gain money through Ransome.

(b) The attack surface was files which they stole and used as a way into the servers using a file encrypting malware.

(c) The vulnerability in this case is a lack of robust security measures.

(d) During the attack critical systems and manufacturing systems were affected and caused the strain on availability.

(e) In this case, as in the case above, availability of resources was the value that took the most strain. Confidentiality in the France division was effected too but integrity was maintained as the COO confirmed to be the case.

f both articles)

To combat these cyber-attacks, one should be well informed as to how to best protect oneself from cyber-threats which often prey on common vulnerabilities such as a lack of proper basic security and other elements discussed in the following article:

https://www.compuquip.com/blog/top-5-cybersecurity-threats-and-vulnerabilities

Question 2

**An assessment of the Security of our Home Computer:**

Below is a table of common threats to the security of your home computer (including the level of risk, consequences and likelihood of occurrence)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk Level  (1 high) | Consequence  (1 low) | Likelihood  (1 low) | Attack Surfaces | Threats |
| 2 | 5 | 5 | Directly to the hardware itself | Steal the computer |
| 2 | 4 | 5 | The internet and your email server | Send you a virus via email/ downloads |
| 3 | 3 | 4 | Links to your account information through internet banking from your computer | Steal your credit card information |
| 3 | Depends on the situation  3 | 5 | Saved passwords in your browser/ files on your computer/ linked to your Microsoft account etc | Steal your passwords to sites etc |
| 4 | 2 | 4 | Login virtually to your computer and access your accounts using pre-saved passwords | Hack your social media accounts |
| 3 | 4 | 1 | The operating system on your computer | Erase the personal files on your computer |

We can protect our home computer from these threats by:

- Keep it in a safe location (not out in the open) with moderate security.

-Do not save your passwords in your browser or on the computer (or anywhere where a person can easily find them).

-Do not use the same passwords for everything – as if a person knows one they will then have access to all your accounts.

-Protect your computer and important documents with good passwords and potentially two-step verification methods

-Back-up important files onto an external hard drive/ cloud

- Do not enter your credit card information (and the like) into unsecure websites.

Question 3

A concrete example where confidentiality takes precedence over integrity is in places such as a psychologist’s office. A patient is far more concerned that their personal history and sessions remain absolutely private, than they are concerned of the accuracy of those accounts (or the fact that that someone may have access to change any such records). A psychologist gains trust with his cliental based partly of the fact that he promises that their conversations and therapy sessions remain exclusively private – without this He cannot function as a trustworthy psychologist.

Question 4

A concrete example where integrity outweighs confidentiality is that of a bank. For bank users the most important consideration is that all the money that they put in the bank (and their other personal details) are accurate and cannot be changed by anyone other than the official banking personal. It is far more important to people that their banking amount is reflected correctly and that their details are not changed, rather than that their age or address is know to people. We would not even care as much if someone were to see our personal details if there was absolutely no way in which they could change the amount of money in our account or access that money in any way.

Question 5

A concrete example where availability is of utmost importance is places of Medical Care (e.g. Hospitals and clinics). for these institutions having accurate information on patients – such as their medical history, allergies etc. – are of paramount importance in order to give the correct and safe medical care. Therefore, these facilities focus on insuring that they always have this information available to them and would care a lot more if anyone where to hack into patient files as this breeches patient confidentiality and could effect the healthcare given. A cyber security threat on availability would be most detrimental to these institutions and could cause major damage (and even death). Seeing as information is key to the wellbeing of all those in healthcare facilities and access to the necessary information is always a concern – we believe that this is the best example of where availability is the primary concern.