**MN502 Assignment 1**

Part A

Network security is a bunch of layers put int place for network, these layers are policies in the system that control what can and can not happen. Some examples of network security are firewalls, data loss prevention, VPN’s and access control. Network attacks from hackers have a major effect on today’s society, damage can be caused to:

* Customers and their friends and family
* Certain individuals
* Companies
* Government structure

These are just of the many few stakeholders that can be affected from network attacks from hackers. Cyber security hackers usually hack into networks for a certain motive, whether that motive is for self-gain, control, reputation or just for fun.

According to the *(116 Must-Know Data Breach Statistics for 2021, 2021)* the average cost of a data breach is 3.6 billion dollars. A huge number of money for a small business for one network attack on their system. The cost is not also the issue, sensitive information and personal information leaked can affect many peoples lives. Once that is also on display it and never be taken down be fully taken down from the internet.

The first network attack that happened between the period of 2016 to 2021 was the company LinkedIn which is owned by Microsoft. Getting hacked in 2021 and more than 700 million accounts were found for sale on a hacker forum. Second on the list was Facebook that was also hacked in 2021, over 533 million accounts with information on contact details and person information was leaked in a data breach. The data was also found online for sale, confirming the breach. Finally, also in 2021, over 7000 Microsoft servers were hacked, many Australian cooperation business use the exchange email service. Which holds a lot of precious data.

The reason why these attacks were successful, is because the hackers found a way to retrieve data through a hole in the system. Obviously, this exploit or hole in the system, wasn’t seen by the company. So, hackers have taken advantage of this opportunity and succeeded. Not only have these hackers succeeded in getting data from the data breach, but they can be found above from the following attacks, selling the information and gaining a profit from it.

The following three scenarios take the following information security definition as so:

Asset: LinkedIn, Facebook Database and Microsoft Servers

Threat: The threats in these attacks were data breaches of databases and control of servers

Threat actor: individual’s and possible coordinated groups of individuals with the intent to benefit from the attack

Vulnerability: None of the articles specifically say where the attacks took place, but they would of given them access to the databases and servers through some sort of format.

Attack vector: Again, as mentioned above none of the articles mention what the attack path was for these breaches, probably mainly due to privacy and other people the information on how to do a data breach.

Attack surface in the context of these attacks: To be able to gain control of the SQL databases and the servers, the hackers would had to obtain passwords through methods to do so.

The scenarios that involve LinkedIn and Facebook were database breaches, the working mechanics of that attack would of involved the attackers breaching the passwords of the database. To be able to get access to the SQL database were the information is contained they need an administration password to be able to look at it and copy the information from the tables.

The scenario with Microsoft, would have involved the attacker’s breaching passwords to multiple servers. Once the attackers were able to crack the passwords of those servers they would have had access to the data inside the servers (mostly likely stored inside a database). They could take a copy of the information and store in somewhere else for safe keeping and use server commands such as shutting down the servers if they wished to do so. The main purpose of this attack though was to steal information though.

Part B

There are many types of network attacks that can be done, the most common types are:

* Computer Virus
* Worm
* DDOS
* Trojan
* Adware/Spyware
* Computer Worm
* Rootkit
* SQL injection
* Phishing

Back in 2011 one of the biggest network attacks happened on PlayStation. Where hackers were taking attention back at Sony after a lawsuit was put on one of the hackers selling jailbroken PlayStation 3’s online. The hackers DDOS the servers and stole 77 million player details from PSN. The network went down for quite a while and PlayStation came out informing the public that credit card information and personal details had be stolen by the attackers. The damage done by the data breach cost PlayStation 105 million euros.

Two techniques that can mitigate network attacks are:

* Firewalls
* Build in incident response plan

Firewalls are an automated program that defends computers or certain applications from attackers and viruses. It is always a good idea to have sensitive information or your computer to have protection. A firewall is a simple and great method for doing so, Windows has its own inbuilt firewall system called Windows Defender. A built-in incident response plan is a great way to have instructions written for employees on actions to take when there is a data breach. Having a plan for response is better than having no idea at all when an attack does happen.

Overall, no matter how many defences you put in place for a system to be fortified there will always be ways for your network to be breached. Learning from past cases and mistakes is a good way to reinforce cyber security for companies. Having good practise and maximising defences for a network and having experienced and hardworking employees. Is the best way to defend against cyber-attacks.

# Bibliography

*116 Must-Know Data Breach Statistics for 2021*. (2021, Aug 27). Retrieved Sep 4, 2021, from upguard: https://www.upguard.com/blog/data-breach-statistics

9news. (2021, March 10). *Australian corporations hit by massive Microsoft Server hack*. Retrieved 9 2, 2021, from 9news: https://www.9news.com.au/technology/australian-corporations-hit-by-massive-microsoft-server-hack/de83dbbd-1296-451a-abd7-537a71c51e99

Cisco. (n.d.). *What Is Network Security?* Retrieved 9 1, 2021, from Cisco: https://www.cisco.com/c/en\_au/products/security/what-is-network-security.html

*LinkedIn denies data breach with 700 million records*. (2021, June 30). Retrieved 9 2, 2021, from itnews: https://www.itnews.com.au/news/linkedin-denies-data-breach-with-700-million-records-566707 LinkedIn Hacked

*Massive Facebook data breach leaks info on millions of users*. (2021, April 5). Retrieved 9 2, 2021, from techradarpro: https://www.techradar.com/au/news/massive-facebook-data-breach-leaks-info-on-millions-of-users

Phillips, T. (2016, April 26). *Five years ago today, Sony admitted the great PSN hack*. Retrieved 9 3, 2021, from eurogames: https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today

*What Motivates Hackers?* (1, 9 2021). Retrieved n.d., from waldenu: https://www.waldenu.edu/online-doctoral-programs/doctor-of-information-technology/resource/what-motivates-hackers