Full name: Joel Benjamin Bates-Webber

Student ID: 103641169

Teacher's name: Christopher Lyell

Unit code and title: 2021-VE02-VU21990-Recognise the need for cyber security in an organisation

Assessment task title: Attacks, defence and methods

What cyber-attacks happen on enterprises? Security threats have been real since the early days of man when we first had something valuable, we decided to keep secure. As the age of technology came, we had something new to defend, with new methods of attack to defend from. In this time, our biggest security threats are cyber-attacks. The information stored on servers and databases provides a risk to billions of people's privacy and lively hoods across the world, which brings huge amounts of attention from well-intentioned and ill-intentioned people.

The cyber-attacks that happen across the world daily vary hugely. Once an individual or a group has a means to infiltrate and attack your system or network, they can insert malware to make computer components malfunction, become a 'Man in the middle' and steal information you were intending for a recipient, flood your network with traffic to slow down server's or networks, and of course rely on any organizations weakest security link, humans, to hand over sensitive information using phishing.

By no means is my list exhaustive. There is always going to be an ever-growing list of methods of attack that we must defend against. Malware (malicious software), likely the biggest cyber-threat, is also the broadest cyber-security concern. If this software is inserted into a system, it can do a variety of damage, such as holding your private information for ransom making it inaccessible to you (ransomware), steal any variety of confidential information (spyware), or it can even damage your hardware.

What common equipment is used to protect organizations from cyber-attacks? Although we have tools like operating system firewalls, hardware firewalls, and virus protection software, a lot of what we have to protect ourselves from attacks with is common sense and in the equipment that we already use. For example, the switches we use to wire our computers together already have technology in them that stops some kinds of attacks by verifying senders and receivers of data. Some safety steps businesses and even individuals can take are to always keep software and operating systems up to date, because with every update comes patches to security flaws.

However, arguably, the most important thing is to train your employees! Many attacks are made successful due to employees giving away sensitive information, or access when they shouldn't. Teach them how to stop creating vulnerabilities and your company will undoubtedly be safer.

What methods and tools are available to protect organization data? Keeping data, or information, safe is obviously a huge priority for everyone. Especially for computers, keep everything on a need-to-know basis. As I mentioned previously, people are the biggest weakness to security. Have IT admins give

accounts to employees that only have access to what they need, this way, no extra information can be leaked. Employ preventative maintenance measures to ensure updates are done and that hardware is kept up to date. Due to some old hardware being unable to receive newer updates, use fresh hardware to remove vulnerabilities.

Can a cyber-attack have a negative or positive impact on the enterprise, customers and the wider public? To this question I say: Of course! This topic is far too wide for me to give all covering examples, but I can make you think about it. If a cyber-attack is small enough, it may wake an enterprise up to the real threat cyber-attacks pose, on the other hand if it's too big, the enterprise could be destroyed. Customers may never have a positive cyber-attack due to them realizing that they may be unable to trust their provider. In regard to the wider public, it really comes down to whether they are affected by the event.

I would like to end on this; the likely hood and trends of a successful cyber-attack lie where the reward of the attack becomes worth the difficulty/cost. The value of the reward for an attack depends on who is carrying it out and their incentive.

Cyber-threats are more real and more present than ever before. Stay aware, stay safe.

References:

1. **https://www.cisco.com/c/en_au/products/security/common-cyberattacks.html**