SIT763 ASSIGNMENT 2

ANALYSIS REPORT OF NEW ZEALAND

Security risk assessment and business requirement analysis

JAY TRIVEDI

Student ID:218449725

STUDENT ID:218449725

Executive Summary

A cyber-attack mainly targets various computer systems, networks and infrastructures or any personal devices which has a valuable data stored into it. The person or the process tries to absorb the data, functions and various restricted areas without the consent of the victim with a malicious intent. One of the examples of the cyber-attacks are the Panama paper case in which around 11.2 million documents were stolen from the Mossack Fonseca lawsuit and leaked onto the news outlets. The documents were highly sensitive financial details of the Mossack Fonseca's tax returns and offshore company dealing. The report gives a detailed overview of various risks, threats and vulnerabilities faced by the cyber-attacks and its impact on the business criteria. The common areas targeted by the attackers are:

- Private sectors.
- Individuals.
- Government.
- Critical National Infrastructure Providers.

Security Risk Assessment

Assets

Based on the common areas targeted by the cyber-attacks the assets involved within them are as follows:

- Software.
- Hardware.
- Security architecture.
- The network topologies.
- Interfaces.
- Users.
- IT security policies.
- Firewalls.
- The flow of information.
- IT security policies.

Threats imposed

1. Network intrusion.
    - This attack tries to get the unauthorised access to a personnel's computer with the help of malicious methods/person.
2. Botnet
    - In this attack an individual or group of machines are being attacked by a malicious software without the consent of the owner and is usually used to send spam or initiate the DDoS attack.
3. Drive by download
    - It usually occurs when a person is directed to a website intentionally by phishing or spear phishing emails.
    - The threat is when that person automatically downloads which has a malicious data which disrupts the system information flow in the browser or any personal devices without the knowledge of the user.

4. Malware
    - A malicious software that is designed to allow unauthorised access to the computer systems and can also cause disruption of the flow throughout the system.
    - Can be done in different ways to a target computer/system.
    - The most common ways to penetrate the malware onto a computer/network are as follows:
        - Phishing.
        - Water holes.
        - Removable media.
    - One of the most common malwares is ransomware.
    - In ransomware the victim has pay a certain amount in-order to regain the access of the system/network.
    - It can also be a result of visiting a compromised webpage on the net.
5. Denial of service (DoS)/ Distributed DoS
    - In this attack the web service is loaded with huge amount of data which results in slowdown of the system and becomes unresponsive.
    - This has a huge impact on businesses that relies online presence.
    - A common use of this attack is called blackmail for payment.
    - One of the motives for this kind of attack is to get the media attention for a short span of time.
6. Data breaches
    - A data breach is basically release of the private/secure or confidential information to an untrusted organisation/individual.
    - The industries that are impacted by data breaches are academia, airlines, hospitality and social media which depends upon the level of personal information.
    - These organisations that are being involved may face reputational damage which involves customers that leads to loss of business.
    - Individuals are mostly targeted with the help of phishing or scams.
7. Phishing
    - This attack relies on the deceptive use of the mail and exploits the victim.
    - The large organisations are been successful to overcome the threat of phishing while the small to medium enterprises are the most vulnerable ones.

Vulnerabilities imposed

- The vulnerabilities that are imposed by the threats are mostly impacted by the IoT.
- It acts as challenge for the IoT users to maintain the cyber threat awareness along with the usage of all the functionality benefits of the devices.
- In 2019, the researchers found two vulnerabilities that are imposed on the CISCO routers that allows the attacker to access the data and commands transferring through and in the IoT devices connected to it (NCSC, 2018/19).
- The infected routers allowed the attacker to constantly keep track of the intellectual data, transfer of information and easy access to the data of the victim.
- The cyber attackers also attack the third-party chain supply chain organisations to get a direct access to more secure organisations.

Risks imposed

- Based on the threats and the vulnerabilities the risks are imposed upon the supply chain and various managed service providers who outsource their business parts to third parties.
- Due to the interconnected nature of these supply chain systems, it becomes the main attraction for the cyber attackers as they directly attack the customer organisations if the third party is being compromised.
- As because of the data breaches and misuse of the corporate data have raised an issues of privacy concerns.

Practical example

Financial institution

Canadian Interbank Network: phishing threat

- In the year of April 2018 there was an outburst of phishing emails from the Canadian interbank network which contains e-Transfer alerts (Phishlabs, 2019).
- The receivers have been told that they have receiving emails regarding funds and more from various tax rebates from the Canadian Revenue Agency.
- They were being prompted to use their bank and login with a fake version of their normal online banking system.

Business requirement analysis

Based on the New Zealand reports the business areas that are mostly impacted by cyber threats are as follows:

- Private sectors.
- Individuals.
- Government.
- Non-Government businesses.
- Critical National Infrastructure.

Most issues recorded are from the following:

- Highest number incidents were reported from overseas.
- Then comes from the domestic sources.
- And lastly the source is still unknown.

From the incident reports of 2018-19 the highest number of cyber-attacks are due to phishing where the attacker/organisation gets the access of the username and password of vivid sectors (NCSC, 2018/19). This causes a huge impact on all the business sectors as the technology is evolving and so is the business areas. As moving towards the online venture through e-transaction this acts as welcome gateway for the cyber attacks to happen. Along with this comes the data breach attack where the business is impacted due to loss of private, financial and institutional data without the consent of the organisation/individual. This leads to various privacy issues among them. Iot (Internet Of things) plays a huge role in this process as every device is connected via internet hence it comes with certain drop backs. The network intrusion attack affects almost all the sectors as they can access the personnel's computer without their authorisation. One of their examples is the breaches in the academia and research institutes where both were targeted with an intension of intellectual property and for the commercial espionage purposes. This is followed by the human errors that are being performed with lack of knowledge among the employees. This is an attraction for malware attacks in the businesses, where the employee unintentionally downloads the malicious software that would result in downgrade of the business and may also lead to loss of financial resources. This is followed by the denial of service attack where the employee is targeted with a large number of requests that would slow down the process of the network and weakens the security gates which leads to business breakdown.

Real world example

New Zealand business website

In December 2015 it came to light that the NCSC noticed that the New Zealand business website was being directed to the visitor's web browser so that the malware was being automatically downloaded into their system (NCSC, 2015/16). The attacker found out a vulnerability in the website's unpatched content management system and inserted the malicious code.

Strategy

- Cyber security awareness programs should be made mandatory for all the employees in the organisation along with the citizens in order to broaden their knowledge of prevailing threats.
- Making the process for reporting of cyber threats should be made easier.
- 24/7 availability of the educative tools so that people can stay safe and secure.
- Efforts should be made to educate the children and the elderly for the usage of technology and its threats.
- Sharing of researches among people.
- Increased supply of skilled cyber security workers should be made.
- Increase in the support of the industry and professional organisations to promote a systematic management of cyber security across vivid organisations and workplaces.

Summary

- With evolving technologies and its usages are followed by various cyber threats which can be entered under minimal loopholes into the system and can disrupt the network.
- Based on the security risk assessment and its impact on the business stream cyber threats can be easily contained by applying the given strategy to have a safe environment.
- The NCSC is taking speedy precautions to contain the threats and have already started its implementation in various sectors as seen above.

References.

- Ncsc.govt.nz. 2020. *NCSC - Incidents*. [online] Available at: <https://www.ncsc.govt.nz/incidents/> [Accessed 22 April 2020].
- NCSC, Cyber Threat Report 2018/19: a cyber threat report from the year 2018/19, retrieved 22 April 2020, <file:///C:/Users/61451/Downloads/NCSC-Cyber-Threat-Report-2018-2019.pdf>.
- Phishlabs, 2019 Phishing Trends And Intelligence Report: a report on phishing trends 2019, retrieved 22 April 2020 <https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf>.

- New Zealand Government, New Zealand’s Cyber Security Strategy 2019: a strategy report on cyber threats 2019, retrieved 22 April 2020 <https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf>.