Question 1

* 1. In order to prevent for further attacks, I would use the Top-Down Approach
* Top-Down Approach allow for quick decision making, when looking to solve a problem, it is done by looking backwards on what may have caused the issue
* It does not make a difference between high-frequency low severity and low-frequency high severity events (Chandana, 2020)
  1. Laws that the City of Johannesburg can use to prosecute attackers on online systems:
* Electronic Communications and Transactions(ECT) Act 25 of 2002, Section 86(1): Unauthorized access to, interception of or interference with data, states that subject to the Interception and Monitoring Prohibition Act ,1992(Act No.127 of 1992), states that any person who intentionally have access to any type of data without an authorization to do it, is automatically guilty of an offence
* Section 87(2): Phishing is known as an offence under section 87(2) on the ECT Act, which states that any person that commits and offence with the intent of getting an unlawful advantage by forging data to be produced with the intention to make it look like real information; the person can either pay a fine in which the value is not specific, or spend time in jail on a maximum of 5 years (Ameer-Mia, Pienaar, & Kekana, 2019)

1.3 The above scenario is regarded to be an incident, because it has disrupted all the normal or daily operations of the entire city, causing chaos and delaying several kinds of transactions

1.4

1.5

Question 2

2.1

A distributed denial of services attack is when hackers make an attempt to crash an online system by loading it with unnecessary data; (Petters, 2020)

However it mostly attacks online services and targeted websites. Their purpose is to overpower those services with a lot of traffic than the network usually accommodates, only to make the website deadly.

The amount of traffic may consist of forged packets, more requests for connection or more incoming messages

Some of the network layers in the OSI model suffer DDoS attacks for example, in the network layer which is layer 3, the attacks can be known as Internet Control Message Protocol Floods, and Internet Protocol/ Internet Control Message Protocol Fragmentation. In layer 4 which is the transport layer, the attacks may include Transmission Control Protocol connection exhaustion. (Weisman, 2020)

Hacked computers or bots can be referred to as zombie computers, which can form “botnet”, which are used to overload the websites with more data that they can handle. Botnets use a large amount of data to exceed the large amount of data that the targeted victim uses (Weisman, 2020)

A Denial of Service attacks consist of many different kinds of attacks in which their main design purpose, is to disturb services. Most companies make use of DoS in order to perform stress testing on their networks. (Petters, 2020)

DoS can also be a type of service attack in which a group of computers are used to overflow a ser with Transmission Control Protocol and User Datagram Protocol packets; they are also used to individually shut down machines and networks, in order for them not to be used by other users (Keary, 2018)

On the other hand, DDoS occurs when a group of systems target a single or unique system with a Denial of Service attack; therefore the targeted network will be getting a large amount of packets from different locations. (Keary, 2018)

2.2 **Steps to prevent a DDoS attack**

* **Build redundancy into the infrastructure**: by doing this, makes it hard for any attacker to launch a DDoS attack on your servers, and also spreading those servers across various data centers with good load balancing system in order to make it easier to distribute the traffic between them; also, it can be very effective if the data centers be located in various locations across the country, and ensuring that those data centers be connected to different networks , and that there no single point of failures (Rubens, 2018)
* **Configuration of the network hardware against DDoS attacks:** by having a configuration on the firewall or the router to drop incoming Internet Message Control Protocol packets or to prevent DNS responses that are not part of your network, or are outside, doing so by blocking UDP port number 53 (Rubens, 2018)
* **Increase bandwidth:** it is important to have more bandwidth than the attacker can handle, in order for you to deal with spikes in traffic that can be caused by a malicious threat (Rubens, 2018)
* **Outsourcing:** by having providers to make implementation of cloud scrubbing services to fight attack traffic in order to remove the biggest part of the traffic causing the problem, before it causes damage on the victims’ network; it is advisable that those measures are done before having to suffer an attack, in order to have a quick response in case it happens (Kartch, 2016)
* **Activation of a WAF(Web Application Firewall):** is some kind of layer of protection that stays between a website and the amount or traffic that the website receives
* **Incident Response Plan:** one has to ready to implement a good response program, and also include a DDoS mitigation plan in order to succeed with the quick response

2.3

Analyze security risks

Develop a security plan

2.4

Biography

Petters, J. (2020, March 29). *Varonis.* Retrieved April 5, 2020, from Varonis: https://www.varonis.com/blog/what-is-a-ddos-attack/

Weisman, S. (2020). *Norton.* Retrieved April 06, 2020, from Emerging Threats: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

Keary, T. (2018, November 21). *Comparitech.* Retrieved April 6, 2020, from Comparitech: https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/

Chandana. (2020, March 5). *SimpliLearn.* Retrieved April 13, 2020, from SimpliLearn: https://www.simplilearn.com/top-down-approach-vs-bottom-up-approach-article

Ameer-Mia, F., Pienaar, C., & Kekana, N. (2019, October 22). *ICLG.com.* Retrieved April 11, 2020, from iclg.com: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa

Rubens, P. (2018, June 26). *eSecurity Planet.* Retrieved April 12, 2020, from esecuritypanelt.com: https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html

Kartch, R. (2016, November 21). *Software Engineering Institute.* Retrieved April 12, 2020, from Insights.sei.cmu.edu: https://insights.sei.cmu.edu/sei\_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html