COMPUTER NETWORKS SECURITY ASSIGNMENT 3

CASE STUDY-IPREMIER

BY: RAJDEEP SENGUPTA

SRN: PES1201800144

SECTION: C

Q1. How well did the iPremier Company perform during the seventy-five minute attack? If you were Bob Turley, what might you have done differently during the attack?

A1. The iPremier Company was not at all prepared for attacks of this kind. The way they acted during the 75 minute attack clearly showcased their lack of responsibility, lack of leadership and lack of preparedness. However, Bob Turley did a good job by prioritizing and making everyone focus on safety of customer information.

If I were Bob Turley, I would have acted a bit quickly. I would have **taken the servers offline immediately**. This would have prevented the attackers to steal or infect the servers and databases. I would have **pulled the plug much sooner** to reduce the aftereffects of the attack. Since Bob Turley had been recently hired and spent almost three months, he should've been aware of the poor capability of the systems to prevent and deal with cyber attacks.

Q2. The iPremier Company CEO, Jack Samuelson, had already expressed to Bob Turley his concern that the company might eventually suffer from a "deficit in operating procedures". Were the company's operating procedures deficient in responding to this attack? What additional procedures might have been in place to better handle the attack?

A2. Yes, the company's operating procedures were deficient in responding to the attack. There was not much that they could do to stop the DDoS attack after it had started. The **only way was to take the servers and databases offline**.

They should have installed **protection systems prior to any mishaps** like this. They should also have had a **backup plan**. Their fault was that **their firewalls were so weak**. They could have installed **honeypots** on their database servers to immediately capture and **notify when their servers got poked** around by outsiders.

Q3. Now that the attack has ended, what can the iPremier company do to prepare for another such attack?

A3. First of all they should **analyse what and why** the attack happened. Then they should create a map of the most vulnerable servers so that these are at the highest security in the hierarchy. They should set up **honeypots** and other **detection systems**. They can also use services like **CloudFlare** for DDoS protection. And most importantly, they should create a **backup plan** along with **backup servers** so that if this attack happens again in the future, they can immediately shut down the old servers and switch to the backup servers and function. Finally, a strong and robust mechanism should be placed in their network which can **track the location** of cyber attacks in today's world.

Q4. In the aftermath of the attack, what would you be worried about? What actions would you recommend?

A4. The actions that I would think of taking are:

- Strengthen and harden the website application firewall from DDoS and other cyber attacks
- Country traffic monitoring and blocking ➜ in this way, it can easily be located which country the attack is coming from and the traffic from that region can be blocked for a certain time period
- Creating honeypots and intelligent detection mechanisms
- Recover website application

The most worrying part about this attack is to figure out **how much information has been stolen** by the attacker and deal with that. They should **check their logs** as the logs are the only trace left to analyze after the attack. **Legal actions** must be taken against the hackers. I would also worry about the reputation in the market and the stability of market value of this company.