The Assignment of Computer Networks Security

(UE19CS326)

Documented by Anurag.R.Simha

SRN	:	PES2UG19CS052
Name	:	Anurag.R.Simha
Date	:	14/10/2021
Section	:	A

1. 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?

A.
The company iPremier was quite hasty during the attack. During the attack, the company reckoned oodles mitigation schemes that seemed to fail by all means. Bob Turley got hit by sentiment during the attack. He felt too dire and fatigued. Little could the company analyse the reason for this atrocious attack to take place. They were completely oblivious about the kingpin of this attack. 'Shut off the power, pull the cords out of their sockets, go dark, kill it...everything' (iPremier(A), Peter Stewart). All the plans during the emergency were outdated. This dialogue delivered by Peter Stewart showed the reckless decision he made. If I were in Bob Turley's shoes, I would initially estimate all the possible methods of attacking the server. Next, I would arrange for interrogation with those employees I believe are cynical. Then, with the aid of my friends and colleagues, I would request them to secretly organise for an investigation, corroborating that the information remains veiled. By no means would I allow the FBI or the media to get aware of the rampageous situation.

2. 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?

A.
The company's operating procedures were pretty deficient in responding to this attack. They were perplexed about the impeccable action to take. The communication was also poor to an extent within the company. For, Leon replied to bob that he was uncertain if the emergency procedures instigated. Not until the call of Joanne did he (Leon) know about a binder that he had never set his eyes on (iPremier(A)-Denial of Service attack). They were also dubious if the attack was a DDOS attack. They could have better analysed the method this attack was launched and suspect any imposter among them. For, imposters are the sole reason for any crime. Social Engineering is a nefarious domain in cybercrime, employed by cyber ruffians to triumph their satanic goals. They could have asked if Qdata could lend a helping hand during the alarming situation. Contacting law enforcement agencies was also an option.

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

A.
Now that the attack has halted, iPremier could pour light upon building up a more impenetrable firewall to stay safe. They could also consider taking advantage of a virtual private network and install 'trusted' anti-virus programmes. The recruitment of security experts who administrate the security of the company's systems is a great choice. They should be aware of when the plan must take effect. Arrangement of training and awareness programmes related to cybersecurity and cybercrimes is a vital desideratum.

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

A.

In the aftermath of this attack, I can't stop thinking about the mastermind of this attack. I would also be worried about the futility of the firewall since it was facile to penetrate through. All in all, the loss of any vital details that's solely important to the company would keep me awake at night. If any customer data is compromised, then the company must look into it forthwith. The impact on the business of this company and the implantation of any backdoors would keep me worried. Diversion of criminal activity, with the aid of this attack, is a major cyber fraud case. If secretly there's ransomware software installed on any computer that's of utmost importance, then the game is over. After this attack, another worry is about the confidence in the company's shareholders. I would endorse the company to upscale its security measures by building an impenetrable firewall, hence foiling any nefarious black hat hackers. Recommending the recruitment of security personnel is not a poor choice. If done so, there's an added advantage to the security of the company. A thorough forensic analysis of the attack is also an applaudable recommendation. A check on the loss of any credentials must be the primary responsibility of the company.

References:

Austin, R. D. and Short, J.C. (2009) ‘The iPremier Company (A): Denial of Service Attack’. Harvard School of Business Administration.

****