PES University

UE20CS326 - Computer Network Security

Assignment – *i*Premier case study

NAME : PREM SAGAR J S	SRN : PES1UG20CS825	SEC : H

Assignment Questions:

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?**

- The company iPremier was not ready for such kind of an attack that will lead to an intrusion and the employees were in a confused state during the 75 minute attack, but they have handled the situation in decent way as they were giving their input/advice on what to be done to prevent the attackers from stealing the customers credit card number and other important information,

- There was no chain of command,There was no communication plan and no attempt to “pool knowledge”, The emergency response “plan” was outdated and useless and No one escalated the issue with Qdata until it was too late.

- iPremier Response was not as good as it should have been. Some employees were giving suggestion to shut down the server. Some were willing to let things happen in order to know the impact of that attack. Management was not able to make any decision.

- If I were Bob Turley, At that moment when I got the call from leon and Joanne Ripley about the breach I would have called Qdata to pull the plug and disconnect the website as their firewall had been breached through and not via some website bug. I would take this action so intruders could not be able steal the customers information from the website.

- Take control of communications, Create a conference call with all of the key decision makers to select a course of action, Disconnect from the Network/ Contact ISP/Shut the down system, Analyze the attack in a more detailed manner.

- When Joanne Ripley asked for 24/7 support from the Qdata.I would have offered more support for her as she was the one that figure out the intrusion and helping out with situation.

- As The news about intrusion is spread among the employees I would consider all the necessary inputs/advice from the employees to deal with situation during 75 minutes attack.

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?**

iPremier's Current Operating Procedures :

- Follow emergency procedure Although an emergency procedure plan existed it was outdated and the plan was not tested recently.

- Contact data center for real-time monitoring, physical access, and procedures for remediation.

- Although contact was made, physical access to ops center was initially denied. Qdata's network monitoring staff were incompetent and their key staff was on vacation.

- Identify status of critical assets.

- Unsure about the status of customer and credit card information data.

- Employees of Qdata were not cooperating with iPremier when that attack happened.

- Employees who were working at night shift were not responsive.

Additional Procedures :

- Conference call bridge with key IT personnel, iPremier executives, and key Qdata personnel

- Contact ISP for additional help.

- Document everything, all actions taken with details

- Establish contact with law enforcement agencies

- Check configurations and logs on systems for unusual activities.

- Set up and configure a “temporarily unavailable” page in case the attack continues for a longer period of time.

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

- They should upgrade the firewall and their security system and move to a better IT service provider as Qdata was not very secure in providing the security to iPremier.

- Now since the attack has come to an end, they should update the backup plan like DRPand IRP.

- Develop and maintain Business Continuity & Incident Response Plan.

- Establish when the plan should be put into action.

- Develop clear reporting lines.

- Know your infrastructure.

- Know how to work with your infrastructure.

- Know how to get back to Normal.

- Training and Awareness.

- Testing and Revisions.

- Get reputable and secure hosting service.

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

- I would be concerned about the breach of the database, such that the customer’s information is not misused for embezzlement of their wealth after the attack, hence the customers losing the trust in the company iPremier.

- What data was compromised? (credit card information, customer information, system), Was intrusion malware was installed onto systems?,Was the attack a diversion attempt to mask criminal activity (i.e. fraud)? and Will another attack occur in the near future?.

- Engage with law to identify the attackers, seek legal counsel and lastly document the breach like how the company breached, what caused it, what did we do post-breach and so on.

- Second as stated above try to update the DRP and IRP or in simple words backup planfor future attacks and also train employees in such cases.

- Strengthen the security and firewall of the company by installing the latest security technologies and improving the website program to avoid any website hacking via XSS or CSRF attacks.

- Approach a third-party company for analysis and assessment of the website for further enhancement of the security.

- Working a plan to show the law enforcement and the public that your intentions are good and thereby reducing fallout or affecting the stock of the company.

- Assemble an incident response team, Conduct forensic analysis of attack, Document incident details and lessons learned, Adjust plans and defenses (address inadequate firewall), Hire independent auditor to identify vulnerabilities of current systems and processes and Communicate with appropriate parties (legal, shareholders, customers, vendor, general public & media, regulatory agencies).