UE20CS326 - Computer Network Security

Assignment – *i*Premier case study

PES1UG20CS084

Aryansh Bhargavan

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?

> *i*Premier had no standard set of rules to follow in case of emergency They were just running around trying to see who could help. There was no communication plan at all and the emergency plan was out of date as well. There was no attempt made to brain storm for ideas that could solve the problem. Simply put, *i*Premier was unprepared for said attack. They escalated the issue to QData really late, which ideally should have been the first thing to do.
>
> Apart from that, QData was not chosen due to its proficiency in its respective domain, but due to the fact that it was geographically closer to to *i*Premier's HQ.
>
> If I were Bob Turley, I would contact the senior managers at QData to escalate the issue and set up a conference call with my company's decision makers, this would include managers from network team security team and the legal team.
>
> I would then have called for the website to be taken down for time being to prevent any further attack and disclosure of confidential information such as customer information, payment details etc.

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?

> No, the company's operating procedures were far from being efficient, even though there was an emergency plan, it was out of date, no one knew for sure what kind of attack it even was; a DOS attack, intrusion attack, etc.
>
> The issue was not escalated to QData until very late and Joan was the only person who had some knowledge about the network security. The first thing they should have done is bring the sit down and load a temporarily unavailable web page, so that customers were not disappointed and they would know what was going on. This would reduce customer loss. They should have had a proper escalation matrix and place which could have saved them,

> calling everyone randomly. The emergency plans should have been up to date and should define all of the procedures and should have details regarding the contact persons. They could check the logs on systems for suspicious activity. They should have had a better security fire wall and place, and rather than just relying on QData's network security team, i premier should have had their own network security team as well in place. That should have full access over the data, knowing that it staff had already expressed their concerns over QDat's abilities, QDatas infrastructure should have been reviewed earlier, and proper actions should have been taken. A conference call could have been initiated with every stake holder to discuss the situation in a more effective and efficient manner.

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

> *i*Premier should try to trace the initial hacker so that the sensitive information is not misused. As already mentioned, a contingent or backup plan which can help them not only disable the website immediately but also help them to track the hacker and take appropriate actions should be formed and used in case to trace nay other such attacks on immediate basis. Along with this it is essential that they should strengthen the firewalls and security system.

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

> The first thing that I would be worried about in the aftermath of the attack includes the information of the customers and the credit cards that might have been accessed by the hacker and can be misused. I recommend legal actions against the hacker for the purpose of ensuring that there is no misuse of this information. This requires technical assistance for the purpose of tracing the hacker. Apart from this I would also be worried about the future prospects of the website and ensure that its security is strengthened.