iPremier Question and answers

Name : Ankith J Rai
SRN : PES1UG19CS069
SEC : B

1)

a) Early in the morning a DDOS attack happened on the iPremier company.Joanne(technical operation team leader) and leon(employee at the IT DEPT) were the first responders,But both of them were not sure what had happened to the website.

b) Leon contacted the newly appointed CIO Bob Turley about the attack but leon was not able to explain properly what was the reason for the attack.

c) The help desk of the company kept receiving calls from the company's customers about the non availability of the website for their use.The company kept receiving email's whose subject line had only one word 'ha'.This made them realize that somebody is performing a DDOS attack and hacking the website.

d) Qdata host's most of the iPremier's computer equipment and databases and they provides the company's connectivity to the internet.Qdata is the one who protects the iPremier website from attacks.After the attack began Joanne rushed to Qdata in order to get understand more about the attack and the websites incoming traffic.

e) The company was not even prepared for any find of attack.The employee's had not been trained before hand about the procedures in case of an emergency and the

BCP(Business Continuity Plan) binder has not been updated at all.

f) The CIO tried to manage the situation in the most efficient manner but he too was confused what to do in the situation on hearing all the suggestions made to him.

If I was Bob Turley then I would have done the following things:

A) During the attack:

1) If I was sure that the attack was stealing the data from the database then I would have immediately ordered to pull the plug's as customer data is more valuable.

B) After the attack:

1) I would have called a meeting immediately in order to update the BCP.

2) I would have then instructed all the employee's in the company to be trained for some time on what procedures had to be followed during any kind of emergency.

3) I would have put a special team in place to check and rectify all the holes that are there in the website where an attacker can exploit.

2)

Ans)

a) Yes,the iPremier Company CEO had already expressed his concern to the new CIO Bob Turley about deficit in operating procedures in a session with him.

b) The CEO had also mentioned that the new CIO Bob Turley has been appointed by the company in order to take the company to a next level in the corporate world.

c) Operating procedures like the Business Continuity Plan(BCP) binder was already obsolete and the people who worked on it had left the company already and the present employee's knew nothing about it.

d) The iPremier company did not even have a DRP(Disaster Response plan) and IRP(Incident Recovery plan) and the new CIO ignored it thinking it is already present as it is a must for any publicly-listed company which was a mistake on his part.

e) If the employees were trained in an efficient manner then they could have stopped the attack from causing such a havoc.

3)

Ans)

a) Yes,the operating procedures were deficient in responding to the DDOS attack.

b) The out of date and obsolete BCP and having no DRP(Disaster Response plan) and IRP(Incident Recovery plan) caused the failure to stop the the DDOS attack.

Additional procedures that could have been in place are:

a) Regular training of employee's on security must be there so that they can resist, withstand and recover from the attacks.

b) The BCP should be updated and maintained and all the employees must be given a copy of the updated BCP before hand itself so that they know what to do in case of an emergency.

c) The Qdata must have employees always monitory the network so that fraudulent or harmful ip address must not access the website.

d) Qdata must improve its firewalls so that any harmful traffic trying to pass is blocked.

e) DRP and IRP must be formulated and maintained so that no such attack again causes disruption to the website.

4)

Ans) The things that can be done by the iPremier Company are:

a)iPremier must formulate a new BCP(Business Continuity Plan) with the latest procedures and methods.

b) Train the employees at regular interval's how to mange and how to tackle an emergency like an attack on the website.

c) The firewall's must be improved so that no fraudulent or harmful ip address can access the website.

d) As customer details are very important hence they need to be kept safe,for this purpose good ciphers must be used on the database so that anytime another attack takes place no customer data is lost.

e) Lack of security provided by Qdata caused such a havoc on the iPremier company.So the company move computing to an internal facility.Even though it is expensive it is still worth it as if another attack of such happens iPremier might lose a lot of money and ultimately might have to shut down itself.

f) Another viable option is switch to another partner(to host iPremier's computer equipment and databases) who have used latest technologies and methodologies and are at a good position to protect iPremier’s website and database from another possible attack.

5)

Ans) I would be worried about the following things:

a) If the customer personal information has been stolen or not.
b) The stock price of the company falling down which will lead to loss to the company.
c) As the attack has caused inconvenience to customer’s the customer might shift shopping from iPremier’s to it’s fiercest competitor MarketTop which will lead to lot’s of loss for the company.
d) If there is any evidence left of the attack so that the company can check where the holes are there in it’s network.

The actions I would recommend are:

a) The BCP , DRP and IRP must be immediately formulated and put into execution.
b) Use a good cipher to encrypt the database of the company so that no such attack’s in the future may cause the customer personal data to be stolen.
c) Train employees on how to handle emergencies and how to overcome them.
d) Update the firewall with the latest technologies so that it’s performance is better.
e)iPremier must set up it’s own internal facility for computing as they don’t need to depend on another company to host them and provide them security.

References:

Austin, R. D., & Short, J. C. (2009). **Case** 1: The **iPremier** Co. (A): Denial of Service Attack (Graphic Novel version). New York: Harvard business school publishing.