UE20CS326 - Computer Network Security

PES UNIVERSITY, BANGALORE

Department of Computer Science and Engineering

***i*Premier Case Study**

Submitted By-

Name: Adarsh Kumar

Class: 5th Sem | B

SRN: PES2UG20CS016

UE20CS326 - Computer Network Security

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?**

Ans: iPremier Response was not as good as it should have been in the beginning. 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.
A part from management decision some the technical guys were really giving some helpful advice if that were followed seriously then the company would not end up as it did on 26 Jan.

Turley should at least pull the plug out until that morning because at night not many consumers do shopping as it was e-shopping company. This action might have closed all the connection what attacker was trying make and any data flow might have stopped immediately as the connection is closed.

During the attack time few important steps I would have done:

- Call a team meeting with senior IT expert and get appropriate help.
- Setup a recovery team to determine the extent of the intrusion.
- Try to contact some security company expert to get proper advice and support.
- Devolve a remediation plan.
- Identify all the Server's impacted by the intrusion by the help of expert.

If I was Turley then I have done bellow changes as soon as joined the company

1. Change Hosting Company

As it was mentioned in the case that Qdata did not have latest technology and because of this, it lost its market leader position. Qdata could not retain their experienced staff. That's why their customer service was not up the mark. iPremier is suggested to find new service provider that must have latest technology, which could help companies to stop DoS attacks. Following are the advantage and disadvantages of choosing this option.

Advantages

iPremier will have a company that can give extra security.

It will help to increase customer trust.

It will reduce the chances of DoS attack in the future.

Disadvantage

It will be costly for iPremier and expenses will increase.

It will consume time when shifting to new servers.

2. Make Strategic Alliance

iPremier can have strategic alliance with Qdata. iPremier has strong financial position. They can invest into Qdata to improve technology. Following are the advantages and disadvantages of choosing 2nd option.

Advantages

Service charges will decrease.

iPremier will have decision making power in Qdata.

Disadvantages

iPremier will have to bear initial investment cost.

3. Create New IT Firm

iPremier is suggested to form its own IT firm that will make sure that the security system is working correctly. It should have its own data storage system where customer data is stored separately and that data can't be sent outside the company

one incident-response team should be there 24/7 who can monitor data coming in going out of the company at some certain intervals.

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?

Ans: iPremier, a company, powered by young and energetic youth was unprepared for the 75 minutes attack, that took them completely by surprise. From the case, this was due to too having too much faith in Qdata's abilities to control these situation

In my opinion, Qdata and iPremier really dropped the ball on this by not thinking steps ahead. They did not have a contingency plan or any plan of sort for this worst-case scenario. iPremier had placed too much faith into Qdata's ability to handle the situation or threat. The first thing I noticed the company did was panic, since there was no crisis strategy/disaster plan. The attack couldn't have happened at the worse time since the attack happened during a high traffic period. If this attack was done by competitors than they got what they were looking for by hurting the reputation of the company. If I was Bob Turley, I may be worried if I'm still going to have a position still, since I was not prepared for this infrastructure break. Bob did not go over all known threats to the infrastructure risk matrix and develop procedures to immediately identify the type and risk. These threats would need to be continually assessed as new ones emerge and the identification would have helped determined the right procedures for defending against them. My first move I would've of made is open a line of communication with Qdata to discuss any risk measure we may have to take. I would not have let the attack go on for so long without pulling the plug to our servers so the customer information cannot be stolen. I would also increase my security against attackers. Having system and users use stronger encryption passwords. Have better real-time monitoring, with a backup plan that has went through testing. Train my employees to better understand the type of attacks and train them on how to handle emergency situations. Even after that make another business continuity plan and test it end to end than repeat. Keep all the software up to date that will better protect from viruses and attacks. You may want to hire an outside audit team to keep a check and balance.

The biggest problem is the host provider. If I was Bob, I may want to build a much better relationship with my provider, showing the importance of this never happening again. Since in sense it's my company's reputation which is on the line. If that don't work, I would go get a more reliable/reputable host provider. With a high-class support and infrastructure, with better security measures. Besides of the updating I would do to the software; Firewalls would also need to up dated. This will protect my company from viruses and also protect from the "whatever" employee. Again, training my employees on what not to do is really important. Train them on emails and what type of emails are at risk. Tell them to always inform somebody on any obscene gestures they computer may be exhibiting. Especially any "ha" emails.

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

   Ans: As the attack ended the company should have done there following things first

   - They should have done full audit and try to find out the main cause of the that attack
   - Company should appoint a permanent Cyber security expert in his company.
   - An incident-response team should me make and appointed at the company and made active especially at night because most of these attacks happen at night time only.
   - They should announce a bug bounty program and invite the third-party organization to find the vulnerabilities.
   - They should have their own two cyber teams one BLUE and another RED one should try protect and other should try to attack the system.

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

   Ans:
   After the attack, locate the portal through which the crumb-bag entered. This could be the e-mail program or browser. This may be easier said than done. Give it a shot. Next, this portal must be disconnected/uninstalled from the Internet to prevent any such attack in future.

   If the customer information has been stolen then what the evil intend of the hacker are they trying to do some kind of negation for customer details or that that lead them to attack the system.

   What is the motivation behind the attack. Is the rival company intensely asked someone to defame iPremier company to affect the business.

My biggest concerns are Legal, Public Relations, Stock Prices, Customer Information and Network Security as least important after the attack. The attack just proved to any competition that my firewalls can be hacked. In looking who could be the one responsible. I would be looking at my competition and what would they have to gain in my attack. Since in sense if I pulled the plug than it would take at least 24 hours to get back running. Even if I did not pull the plug and I rode the attack out than I would still have to shut down business because of then security breach. No matter which route taken, I would still be at lost once my firewalls proved to be vulnerable.

There a lot of equations to look at. This is the main reason I would have an outside Network Operations Centre (NOC). They will provide all the monitoring I may need for any issue that may arrive even the increase of bandwidth.

References:

- https://www.ukessays.com/essays/information-technology/ipremier-co-denial-service-attack-1860.php
- https://www.ukessays.com/essays/information-technology/ipremier-co-denial-service-attack-1860.php
- https://www.youtube.com/watch?v=gFNGfUhCwbk

THE END