COMPUTER NETWORK SECURITY ASSIGNMENT 1

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

CASE STUDY 01: iPremier

Q1. How well did the iPremier Company perform during the seventy-five-minute attack? If you were Bob Turley, what might you have done during the attack?

Solution: iPremier performed reasonably well during the seventy-five-minute attack. Things would've gone differently if all the measures were put in place, but however, they were able to quell the attack in a relatively short time (before the day's traffic started). When the attack was underway, all the right people were alerted as soon as word reached (Joanne, Leon and Bob, the CIO). Joanne immediately headed to the data centre to analyse the problem and took necessary steps to stop the DDoS attack.

Leon informed several individuals of different departments (legal, financial etc.) of the DDoS attack that was underway, thereby creating unnecessary panic. Bob had to divert his full attention from Joanne (who was reaching the data centre to fix the problem) and juggle it between all the various department heads who were calling to assess the risk and give their opinions.

Joanne had to physically reach the data centre as no one was at the data centre to help solve the attack. Joanne faced hassle to enter the data centre too. If these problems hadn't been there, the attack could've been prevented much faster.

What would I have done during the attack?

I would've …

-> Ensured that only those individuals who are immediately concerned about the attack (the CIO, the Ops team, the response team) are informed first. The main goal during such a time is to defend the site from the attack and prevent panic in the organization.

-> Asked those in the teams to not inform others and create panic.

-> Contacted someone in the organization who has details of the data centre that hosts the server and sought permissions (for Joanne/ the response team) to diagnose and inspect the servers at their data centre.

-> Sought the response team and asked them to monitor the attack progression. The faster the nature of the attack is known, the faster it can be mitigated.

-> Stayed confident and motivated the team to resolve the attack as quick as possible.

COMPUTER NETWORK SECURITY ASSIGNMENT 1

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Q2, Q3. 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?

Solution: The company was definitely deficient in its response procedure. Having Joanne as the sole person in-charge of defending the server from the attack was clearly wrong. An active response team must be in place to handle any form of attack.

Bob was informed of the BCP and the recovery plans but Bob never inspected them and verified if all of them were up-to-date. Incidence response was never carried out; it must've been tried beforehand.

Leon, the Ops team head was unaware of details about the binder. Smooth transition of the post was not done from the old head to Leon; Leon did not know what was the working of certain operations under him.

There must've been a clear chain of command on how such attacks are responded to. Informing the legal head and the PR head was not immediately essential to stop the attack from happening. Having a clear chain on who to be informed when such an attack takes place, would've allowed Bob to focus on foiling the attack rather than thinking of its repercussions.

Joanne faced trouble co-ordinating and communicating with the third-party organization to handle the crisis at hand. iPremier was not aware that all of QData's employees were absent at the data centre. Joanne wasn't allowed access to the data centre immediately on arrival. The response to such an attack would've been a lot faster if there was better communication and co-ordination between the parties concerned.

COMPUTER NETWORK SECURITY ASSIGNMENT 1

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Q4. Now that the attack has ended, what can the iPremier Company do to prepare for such an attack?

Solution: Hosting the database and the firewall as an internal facility must be of at most importance. Relying on 3rd party organizations to host the data can be risky to the business going forward and therefore, the transition must be made quickly.

Mails having single words ('ha' in our case) must be immediately classified as spam and the mail addresses sending those mails must be blocked (for a time period as some of them could be legitimate users whose systems have been hacked).

Strict action must be taken against those employees in the company who were lax during the previous attack. The company must uphold its policy of ensuring that only the right people with sufficient knowledge and experience move higher up the ladder. Employees hired anew must be thoroughly briefed about all the company documents, emergency procedures etc, before they actually start working.

Incidence Response was discussed but never practiced. The organization must ensure it updates all its subsequent recovery and response plans and stays prepared (if there is another attack).

Usage of SYN cookies in all the subsequent connections that are established with the server will ensure that half-open connections are not directly put into the buffer/queue until the ACK packet is received. This ensures that another SYN flood attack does not take place.

Systems are vulnerable just after an attack. The possibility of another immediate attack (by the same organization/individual or someone else) is very high. Beefing up defences just after the attack is very important to prevent any more attacks in the immediate short term.

COMPUTER NETWORK SECURITY ASSIGNMENT 1

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Q5. In the aftermath of the attack, what would you be worried about? What actions would you recommend?

Solution: Critical user information like credit card details of millions of customers can be compromised. A thorough forensic report is needed to identify if the details have been compromised. Customer backlash can be expected and the company must ensure its PR and legal team is well prepared to face the ire of the public.

There is a possibility that we might have lost a certain customer base during the attack time. Analysing the proportion of customers lost to the attack (to other competitors) is essential for the company to identify the proportion of money that ought to be reinvested in wooing those customers back.

Market stocks may tank the subsequent day and the company must be prepared to handle that.

Disclosing to the media details of an attack will in turn raise questions on the poor security framework of iPremier. Ensuring that the competitors and the media do not cause panic and fear in the minds of the general public would be a task to uphold. Presenting a heroic case to the public (even if it is not true in reality) would be essential to keep the customer integrity intact.

The greatest fear would be public anger and the legal and PR team must be given all details of the attack (after analysis is complete) so that our case is strengthened if customers come to know that a DDOS attack has taken place.

Assuring customers that all their data is safe is also another task they must try to accomplish.

Variation in customer traffic on the server in the subsequent days must be made note of, to analyse how customers are responding to the news (if it is released in the media). Any substantial changes in the traffic data must be quickly analysed and resolved so that customer traffic does not either peak (another DDoS attack possibly) or trough (loss of customer base) totally.