Security Incident Report Plan

An employee of X telecommunications company made a mistake by clicking a seemingly legitimate link and shortly after there were numerous complaints about the server moving slow.

Preparation

My team Skynet Ltd, an incident response team led by me as Team Lead Executive, an Incident Manager, Lead Investigator and a Professional White hat hacker. In addition to the team, the HR manager of the company would be involved with the team in responding to this incident as it involves affecting the employees. Our aim is to tackle this incident effectively. Here are some things our team would need in preparing for this incident to allow a better handling of when it occurs. They are as follows:

* Ensure having Contact Information of team members and possibly of persons outside the organization for backup.
* A mechanism that would allow the user to report the incident anonymously. These could include issuing phone numbers, email addresses and online forms.
* An Encryption software to be used when communicating between team members in the organization(internally) or outside help(externally).
* Devices specifically issued for incident reporting such as laptops for writing reports and analyzing date and smartphones for easier emergency contacting.
* Having a tracking system for tracking incident information, status etc.
* Having a forensics work station to preserve log files and save relevant incident data.

In addition, there are some practices that would be helpful in this phase to help with prevention. These are:

* Ensuring periodic risk assessments of systems and applications are taking place
* Ensuring the host security is firm and hardened
* A malware prevention plan which entails having anti-spam and anti-virus software
* User awareness training so that users are kept in the light of what could happen if they do certain actions, how to identify potential incidents and what they can do in such events.

Detection and Analysis Phase

Our team would now carefully lead an investigation into the matter as to why the servers are moving slow and if it has any relation to the link that was clicked, that seemed legitimate but appeared to be fake. After much deliberation, it has been determined it was a phishing link and within that link came a DDOS attack which caused the traffic on the network causing traffic of calls pilling up and being interrupted frequently. Our team has determined that this attack is a large scale attack and is deemed high threat level. This was determined after we found that it caused persons contact information to be inaccessible to employees and their work devices are also affected. We would then take the next step in mitigating any major problems or losses that might occur.

Containment and Eradication Phase

Before the matter gets worse, our team would devise a strategy that would allow us to contain the attack on a smaller scale. Our team would decide whether to shut down the work stations for a period of time or the servers to help contain the attack. As the team lead , I would then express these decisions to the higher ups and walk through the risk of these decisions and why they are necessary in helping to handle the situation of the DDOS attack. After making sure its contained within a certain level of confinement which involves finding the device it started with, when it started, where the link is from, the effects the attack had and how far has said effects spread.

The next step would be the eradication process, which would involve deleting said link, clearing the network cache, activating the anti-spam and ant-malware software and mitigating all vulnerabilities that were exploited.

Recovery Phase

In the recovery phase, we would attempt to restore systems to when operation was normal and optimal. A thorough investigation into what needs to be cleaned, restoring back ups, checking if new components are needed to be replaced, ensuring stronger stronger security, clearing the log calls withing that time frame after making note of them and possibly patches if needed. Looking into providing higher attack monitoring would help as there is no way to perfectly say it is now completely solved, since it has been attacked once it may happen again but by the Skynet Ltd would then be stronger in tackling this.

Lessons Learned Phase

Our team Skynet Ltd would hold a meeting with the members of the X Telecommunications Company XTC that were involved mostly in the attack to gain some form of understanding of what happened and how we can strengthen the security level for an next possible incident. Ofcourse, this information would be generalized to the entire company to raise the employees awareness. To reassure the company, we at Skynet Ltd, recites our motto which “The Sky is never the limit and the cloud of networks are ever changing”. This is to say , not every thing can be prevented but with keeping up and changing with the times, we can be prepared for and handled effectively.