Michael Chillemi

Case Study 1

02/20/21

Professor Aakash

1. A denial of service attack is when a over load of traffic is on a network causing it to crash and make it inaccessible to users. A distributed denial of service attack is when a attacker try’s to disturb the normal traffic of a server. A denial of service attack and a intrusion are very different. One of the main reasons is a denial of service attack aims to make a network crash by overloading it with tons of traffic. While intrusion is a force able unauthorized activity being conducted on a network. When a intrusion attack occurs the attacker can be able to steal private information from the network. This can cause lots of damage to a company. Not only can this cause damage to the company but can also hurt their reputation. Both of these attacks are very scary for companies and is why so much time and effort is needed to make sure they have great security to combat these attacks.

2. iPremier’s management culture was not the greatest by any standards. They were unorganized in some aspects and the higher up management was very greedy when it came to profits over security. This resulted in their many failures when they were struck by the Cyber attack on their company. I can definitely say because of their management culture being so money hungry lead to the downfall and lack of preparation for when a attack happened on their system. There were so many opportunities the company had to update or check if their system was secure but, they failed to do so resulting in them not being prepared when a attack occurred. Not only were they not prepared for the attack after, the attack happened they had opportunities to completely create a new system to make sure this wouldn’t happen again. But because of the money hungry management team who wanted to take the less costly route this caused for the FBI to come in because some of their devices commenced a attack on a competing company. If iPremier took the necessary actions these issues would not be present.

3. It was very clear that the company was not prepared for the problems they had to face in the future. One of the many problems was they had outdated manuals and some of them they were unable to locate. A recommendation would be to always have updated manuals available to the staff in case of a emergency. Another problem the company had was half filled logs because it was to costly. Having the logs filled out is another recommendation I would give even though it would cost money it will help keep track of what is going on in the systems. Also another issue was the third party security team they had which was not helpful at all. Even though the owner had connections with the owner of the company they needed to spend more effort in building their security team. One of the last issues was the company had old hardware and known vulnerabilities that they did not fix. Saving the money to not fix and updates these parts of the system has made a dramatic impact on the company for the worse. My recommendation would be to make sure all hardware and vulnerabilities are patched in order to have a secure system.

4. Some of the risk that iPremier faced when dealing with the result of the crisis is many things. One would be in the event of a future attack. Another risk is the loss in reputation with their clients. Ipremier had lots of issues with their security and this attack being successful in showing the company's security is not the greatest can lead to future more threatening attacks. As a example when we later find out that one of the computers was infected and was targeting a competitor company. Some of the main priorities for the company is to make many changes. One would be to update their security team. Another company would have been way better than the one they partnered with. Another priority would be to update their hardware and systems. During the case study it stated that the company relied on old hardware and didn’t update their system because they did not want to spend the money for it. They should invest some of their profits to improve their security system in order to prevent future attacks.

5. Ripley discuses about rebuilding the system because at the time it would be a good approach to solving their security crisis to rebuild a whole new system making sure it is secure. Some of the risks that are involved in doing this is the company website would be down for some time. This would cause loss in profits and stocks which is not what the management team wanted. After the FBI came in contact with them with this information it was actually a good idea that they did not destroy the old system and rebuild it. If they did that all of the data would have been lost about the infected computer and would have looked really bad for the company. If iPremeir took the precautions early and updated their security these issue would have been less likely to occur. If the managers knew what they found out two weeks later they would have made the proper changes they needed to create a better result. One option they could have done is create a backup of the old system so the FBI can investigate and start building their new system at the same time.