CIST 3381- Information Assurance & Security
Spring 2022
Case Study 1: iPremier: Denial of Service Attack

L1

Group Number:

Group members' names:

1. michael Chillemi
2. John Raven
3. Amanda Quach
4. Vivian Hin

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 1: iPremier: Denial of Service Attack

Group Number: L1 **Your Name:** Vivian Hin

Question 1) What is a "Denial of Service Attack" and "Distributed Denial of Service Attack"? What is the difference between a DoS attack and an intrusion?

Answer:

A denial of service attack (DoS) is an attack that restrict access to use a specific service of a particular company.

Distribted denial of service attack is an attack that target multiple companies at the same time.

↪ signal machine send packages for other machine to attack the targeted machine/network

→ disrupt normal function and traffic

Intrusion

- goal is to find vulnerabilities
- steal information
- internal attacks

vs.

DoS

- external attacks
- prevent users to access service
- uses large amount of traffic to the site

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 1: iPremier: Denial of Service Attack

Group Number: L1 **Your Name:** John Raven

Question 2: What is the management culture at iPremier? Do you think their management culture was also a reason for their lack of preparation? Why?

Most new management doesn't last long if they don't produce quickly. One of the heads of the company is friends with one the creators QData so they use QData to host even if it's not the best option. Management didn't prioritize cyber security, only prioritized profit.

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 1: iPremier: Denial of Service Attack

Group Number: L1 **Your Name:** Amanda Quach

Question 3: It is clear that the company was not prepared for the problem? Analyze the reasons for their lack of preparation and give recommendations on how could they have been better prepared for the problem.

Out of date manual and unable to locate

~~Mem~~ Logs of the events/Backups were half recorded due to high ~~prices~~ cost
- Small Disk space

No prior pen testing

They used a third-party security company, were 24/7 support over
The phone was ~~unab~~ unavailable and had to drive to the
security company

The company knew of their vulnerabilies, but kept delaying the fixes.

The company did not allocate enough resouces towards security

~~No~~ Lack of proctols (who to call / chain of command)

Remote access to servers (Less time wasted, don't have to travel to company)

~~Doing~~ ~~opening emails/~~ using (Trademarks/copyright iPremier) ~~on~~ → to prevent future problems.

Separate (Hash) Server, Backups, and Database (able to idenify an attak more quickly.)

Fire wall not updates
update hardware

CIST 3381- Information Assurance & Security

Spring 2022

Case Study 1: iPremier: Denial of Service Attack

Group Number: L1 **Your Name:** Michael Chillemi

Question 4: Identify the risks faced by iPremier as a result of the crisis. What are the priorities for iPremier after the attack?

Discuss: - update standard procedure
- firewall outdated/update
- keep better tabs on paper copy procedure
- replace hardware if needed
- better relationship/with quene data
- more organization in company (security team)
- leaking confidential info (employees)
- better to prepare before/preventive measures
- have backups of the system.
- reputation
- what kind of attack/think of future