Assignment – *i*Premier case study

Assignment Questions: Each question carries 10 Marks.

1) iPremier, a publicly-listed company, was the victim of a 75-minute DDoS attack. The company's handling of the attack was severely lacking in professionalism and preparedness. iPremier had no established protocols for responding to DDoS attacks, and its Business Continuity Plan (BCP) binder contained outdated information and listed employees who had left the company. Even upper management struggled to handle the crisis effectively, with the Vice President and legal adviser more focused on protecting their own positions than on collaboratively addressing the issue.

   If I were Bob Turnely, iPremier's CIO, I would have immediately disconnected the company from the internet and launched a thorough forensics audit to determine the cause of the attack. I would have also try my level best to mitigate the damage and restore service as quickly as possible. In the meantime, I would also communicate with the customers regularly and be transparently about the attack and the steps iPremier is taking to resolve it. I would have also offer compensation to customers who were affected by the attack by being transparent it would make the costumers have trust on us thus reducing PR damage and helping the company rebound from the crisis.

2) iPremier's response to the DDoS attack was hampered by outdated operating procedures and lack of proper documentation.

   The company's TRP, DRP, and BCP were not up-to-date which is in fact show a glaring lapse in security as these documents are very important during a crisis as they help in mitigating the effect of the damage caused by the crisis,

   the transfer of servers from Qdata to its in-house servers was poorly managed as Qdata was severely understaffed and had delayed the implementation of latest hardware and software making it easy for hackers to exploit various bugs usually present in outdated and poorly secured servers.

   Additionally, iPremier had not made proper software documentation, which made it difficult to restore its systems from backup.

   iPremier could have implemented several technical and procedural measures to mitigate the impact of the attack, including:

- Rate limiting to prevent attackers from flooding its servers with traffic
- A load balancer to distribute traffic across multiple servers and improve resilience
- Network traffic monitoring to quickly identify and respond to DDoS attacks
- A plan to contact its ISP or a security service provider for assistance in the event of a larger or more sophisticated attack
- An updated DRP, TRP, and BCP
- A communication plan to keep customers informed during the attack
- Transparency with customers about the attack and the steps being taken to mitigate it
- Compensation for affected customers

By implementing these measures, iPremier could have better handled the DDoS attack and minimized the impact on its business and customers.

3) Following the DDoS attack, iPremier can better prepare for future attacks by:

- Updating its DRP, TRP, IRP, and BCP to reflect the latest threats and best practices.
- Investing in AI and ML-powered security solutions to detect and respond to attacks in real time.
- Segmenting its network and isolating critical systems to prevent attackers from overwhelming the entire network.
- Implementing a zero-trust security model to verify all users and devices before granting access to IPremier's network and workstations.
- Partnering with other organizations to share intelligence and best practices.
- Building a cyber militia of volunteers trained to defend against cyberattacks.
- Improving employee knowledge on cybersecurity through regular training and awareness programs.
- Conducting regular security checks by cybersecurity experts to identify and address vulnerabilities.
- Having a backup of server, database and other such IT hardware which can be used as a load sharer or be activated in an instant when the main website is operationally non functional due to attacks.

By taking these steps, iPremier can make it more difficult for attackers to launch successful DDoS attacks and minimize the impact on its business and customers.

4) Following a DDoS assault, these aspects would prick my anxiety:

1. The financial ramifications of said attack: The assault may inflict a considerable financial dent due to the revenue downturn, the downtime ramifications, and the remediation cum recovery expenses.

2. Reputational destruction resulted from the hit: All forms of DDoS assault can wreak havoc on a firm's image, particularly the aspects of reliability and overall trustworthiness.

3. Secure processes of the business’s data and systems: A DDoS ambush could potentially camouflage other forms of hidden breaches or even notorious malware infections.

given the prevalence and sophistication of DDoS attacks and the proliferation of DDoS attack kits in the Dark web:

- Use artificial intelligence (AI) and machine learning (ML) to detect and respond to DDoS attacks in real time. AI and ML can help to identify patterns in traffic patterns and to develop automated responses to attacks.
- Segment its network and isolate its most critical systems. This will make it more difficult for attackers to overwhelm iPremier's entire network and will help to protect its most important data and systems.
- Implement a zero-trust security model. This means that iPremier will not trust any user or device by default. All users and devices will be required to authenticate and authorize themselves before they are granted access to iPremier's networks and systems.
- Partner with other organizations to share intelligence and best practices. This will help iPremier to stay up-to-date on the latest threats and to learn from the experiences of other organizations.
- Build a cyber militia of volunteers trained to defend against cyberattacks. In the event of a DDoS attack, iPremier could activate its cyber militia. The militia members would work together to monitor network traffic, identify malicious traffic, and block it from reaching iPremier's servers.

By taking these steps, iPremier can make it more difficult for attackers to launch successful DDoS attacks and minimize the impact on its business and customers.

.

Your response should be type written in your own words. There is NO one right answer.
Your responses should be succinct, crisp, cogent and well presented.
All references should be cited appropriately.

DrillBit

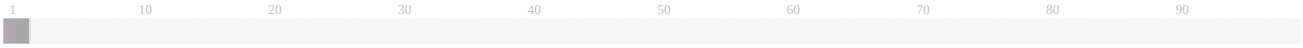
The Report is Generated by DrillBit Plagiarism Detection Software

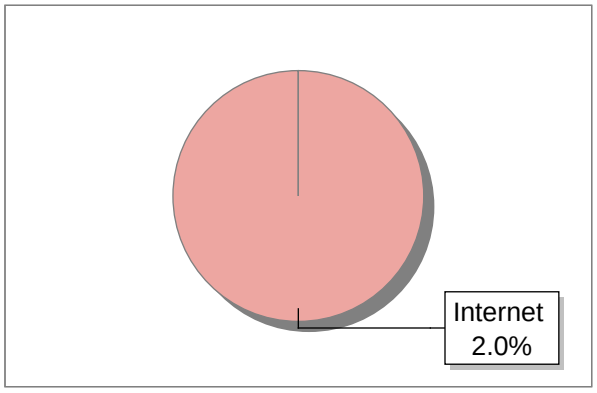
Submission Information

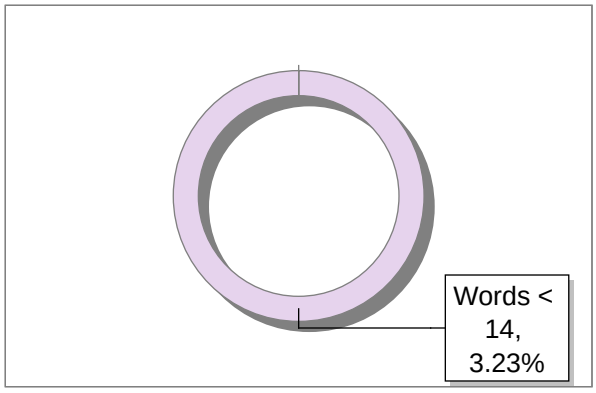
Author Name	U G DHEERAJSAI
Title	ASSIGNMENT
Paper/Submission ID	1076063
Submitted by	jyothih6@gmail.com
Submission Date	2023-11-03 09:26:10
Total Pages	4
Document type	Project Work

Result Information

Similarity **2 %**







Exclude Information

Quotes	Excluded
References/Bibliography	Excluded
Sources: Less than 14 Words Similarity	Excluded
Excluded Source	**0 %**
Excluded Phrases	Not Excluded

A Unique QR Code use to View/Download/Share Pdf File

DrillBit

DrillBit Similarity Report

2	1	A
SIMILARITY %	MATCHED SOURCES	GRADE

A-Satisfactory (0-10%)
B-Upgrade (11-40%)
C-Poor (41-60%)
D-Unacceptable (61-100%)

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	docplayer.net	2	Internet Data

Assignment – *i*Premier case study

Assignment Questions: Each question carries 10 Marks.

1) iPremier, a publicly-listed company, was the victim of a 75-minute DDoS attack. The company's handling of the attack was severely lacking in professionalism and preparedness. iPremier had no established protocols for responding to DDoS attacks, and its Business Continuity Plan (BCP) binder contained outdated information and listed employees who had left the company. Even upper management struggled to handle the crisis effectively, with the Vice President and legal adviser more focused on protecting their own positions than on collaboratively addressing the issue.

   If I were Bob Turnely, iPremier's CIO, I would have immediately disconnected the company from the internet and launched a thorough forensics audit to determine the cause of the attack. I would have also try my level best to mitigate the damage and restore service as quickly as possible. In the meantime, I would also communicate with the customers regularly and be transparently about the attack and the steps iPremier is taking to resolve it. I would have also offer compensation to customers who were affected by the attack by being transparent it would make the costumers have trust on us thus reducing PR damage and helping the company rebound from the crisis.

2) iPremier's response to the DDoS attack was hampered by outdated operating procedures and lack of proper documentation.

   The company's TRP, DRP, and BCP were not up-to-date which is in fact show a glaring lapse in security as these documents are very important during a crisis as they help in mitigating the effect of the damage caused by the crisis,

   the transfer of servers from Qdata to its in-house servers was poorly managed as Qdata was severely understaffed and had delayed the implementation of latest hardware and software making it easy for hackers to exploit various bugs usually present in outdated and poorly secured servers.

   Additionally, iPremier had not made proper software documentation, which made it difficult to restore its systems from backup.

   iPremier could have implemented several technical and procedural measures to mitigate the impact of the attack, including:

- Rate limiting to prevent attackers from flooding its servers with traffic
- A load balancer to distribute traffic across multiple servers and improve resilience
- Network traffic monitoring to quickly identify and respond to DDoS attacks
- A plan to contact its ISP or a security service provider for assistance in the event of a larger or more sophisticated attack
- An updated DRP, TRP, and BCP
- A communication plan to keep customers informed during the attack
- Transparency with customers about the attack and the steps being taken to mitigate it
- Compensation for affected customers

By implementing these measures, iPremier could have better handled the DDoS attack and minimized the impact on its business and customers.

3) Following the DDoS attack, iPremier can better prepare for future attacks by:

- Updating its DRP, TRP, IRP, and BCP to reflect the latest threats and best practices.
- Investing in AI and ML-powered security solutions to detect and respond to attacks in real time.
- Segmenting its network and isolating critical systems to prevent attackers from overwhelming the entire network.
- Implementing a zero-trust security model to verify all users and devices before granting access to IPremier's network and workstations.
- Partnering with other organizations to share intelligence and best practices.
- Building a cyber militia of volunteers trained to defend against cyberattacks.
- Improving employee knowledge on cybersecurity through regular training and awareness programs.
- Conducting regular security checks by cybersecurity experts to identify and address vulnerabilities.
- Having a backup of server, database and other such IT hardware which can be used as a load sharer or be activated in an instant when the main website is operationally non functional due to attacks.

By taking these steps, iPremier can make it more difficult for attackers to launch successful DDoS attacks and minimize the impact on its business and customers.

4) Following a DDoS assault, these aspects would prick my anxiety:

1. The financial ramifications of said attack: The assault may inflict a considerable financial dent due to the revenue downturn, the downtime ramifications, and the remediation cum recovery expenses.

2. Reputational destruction resulted from the hit: All forms of DDoS assault can wreak havoc on a firm's image, particularly the aspects of reliability and overall trustworthiness.

3. Secure processes of the business's data and systems: A DDoS ambush could potentially camouflage other forms of hidden breaches or even notorious malware infections.

given the prevalence and sophistication of DDoS attacks and the proliferation of DDoS attack kits in the Dark web:

- Use artificial intelligence (AI) and machine learning (ML) to detect and respond to DDoS attacks in real time. AI and ML can help to identify patterns in traffic patterns and to develop automated responses to attacks.
- Segment its network and isolate its most critical systems. This will make it more difficult for attackers to overwhelm iPremier's entire network and will help to protect its most important data and systems.
- Implement a zero-trust security model. This means that iPremier will not trust any user or device by default. All users and devices will be required to authenticate and authorize themselves before they are granted access to iPremier's networks and systems.
- Partner with other organizations to share intelligence and best practices. This will help iPremier to stay up-to-date on the latest threats and to learn from the experiences of other organizations.
- Build a cyber militia of volunteers trained to defend against cyberattacks. In the event of a DDoS attack, iPremier could activate its cyber militia. The militia members would work together to monitor network traffic, identify malicious traffic, and block it from reaching iPremier's servers.

By taking these steps, iPremier can make it more difficult for attackers to launch successful DDoS attacks and minimize the impact on its business and customers.

.

Your response should be type written in your own words. There is NO one right answer.
Your responses should be succinct, crisp, cogent and well presented.
All references should be cited appropriately.