COMPUTER NETWORKS SECURITY

ASSIGNMENT 5 - THE PHOENIX PROJECT

BY: RAJDEEP SENGUPTA

SRN: PES1201800144

SECTION: C

Q1. Describe the role of Information Technology Services (ITS) in fulfilling UVA's mission.

Ans1. **Information Technology Services were responsible for installing and monitoring all the computer networks throughout the University of Virginia. ITS was responsible of maintaining several hundreds of servers in the university for the following purposes:**

1. **HR**
2. **Student information**
3. **Financial information**
4. **And other data**

They also regularly patched the university computers for cybersecurity threats.

Q2. What attracts cyber attackers to universities?

Ans2. **University of Virginia is known as one of top-ranked universities for research intensive work in all fields. It has 22,000 students, 2,800 faculty members and 10,000 full-time staff who generate huge amounts of digital data onto their servers. This data can be very important and have a huge impact on the university if leaked. It includes personal information on the people in the university and confidential data on research projects. This makes this university a huge hotspot for cybersecurity attacks from the outside world.**

Q3. What are the most common attack methods and approaches for mitigating those attacks?

Ans3. **Some of the most common attacks nowadays are:**

- **Zero-day attacks**
- **Spear Phishing**
- **Malware Attacks**
- **Phishing Attacks**
- **Cross Site Scripting(XSS) Attacks**
- **SQL Injection Attacks**
- **Distributed Denial of Services(DDoS) Attacks**
- **Man in the Middle Attack**
- **Social Engineering Attacks**

Some of the common approaches to mitigate these attacks are to regularly keep monitoring the network through Intrusion Detection Systems and Firewalls and releasing regular security patches.

Q4. Describe each of the five objectives of the Phoenix Project. What level of effort would be required to accomplish these objectives?

Ans4. **The five objectives of the Phoenix Project are as follows:**

1. **Determine the extent of the intrusion:**
   Pre-investigation of intrusion was performed several weeks before in order for a more in-depth assessment
2. **Develop a remediation plan:**
   A detailed plan was developed which involved all the systems in the university to go-dark in order to allow new security system to be enabled
3. **Execute the remediation plan**
   Preparation for the going-dark phase by choosing the time, identifying all workstations impacted by intrusion, evaluating password management system etc.
4. **Harden UVA's defenses**
   Further strengthening was required to block malicious activity
5. **Restore services**
   All systems had to be restored and tested at the end of go-dark phase

Q5. Describe the various internal and external stakeholders associated with the Phoenix Project. How would you recommend the project team communicate with each stakeholder group?

Ans5. **The internal stakeholders included the BOV, vice presidents, deans, faculty,staff, students, retirees and the alumni. The external stakeholders included the attorney general, Microsoft services, Mandiant Inc., the governor's office, the general public and the press(newspaper).**

The best way for managing communication for this project is that the internal stakeholders should be informed prior to the go-dark phase whereas the news should only be available to the external stakeholders after the go-dark phase when the systems are restarted with the new security systems.

Q6. Identify the key risks inherent to this project. How would you recommend the team manage these risks?
Ans6. **One of the biggest risks was if the project became public. Since this was a project to enhance the cybersecurity of all the systems and a leak from the project meeting to the public may cause immediate failure and lure cyberattackers. Other risks included scheduling conflicts with University of Virginia's programs and events, potential technical or human resource issues, system documentation shortcomings etc.**

The best way would be to choose an agile approach for this project and hold regular meetings with complete isolation in order to prevent any leaks. Then team leaders have to be assigned for each subtask/domain. In this way, an organised way can be thought of which would be of great help. Each member working for the project should be made to sign a non-disclosure form stating that they cannot leak any work to the outside world.

Q7. When and how should the success of the Phoenix Project be evaluated?
Ans7. **The success of the Phoenix Project can be measured mainly after the go-dark phase. The go-dark phase implements the security measures into the systems by turning off the internet and restarting all the machines. In this way, any compromised machines will not be able to spread any malwares or viruses. After the go-dark phase, all the measures taken and patches can be tested and any failures can be rectified. Some testing through small unharmful attacks can be performed to check how the systems are handling. This is the perfect way to imitate some dangerous attack and get prepared for any in the future.**

Also, the objectives can be checked if they have been achieved before deadline to ensure success of the project.