Assignment 6

by Nikhil T M

Submission date: 02-Nov-2021 10:15AM (UTC+0530)
Submission ID: 1690753598
File name: PES1UG20CS821.pdf (162.64K)
Word count: 1766
Character count: 9022

Assignment 6

Name:Nikhil T M
SRN:PES1UG20CS821
Section:F

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

Ans information technology service has played a major role in UVA’s mission . Virginia Evans was the (CIO) chief information officer in the University been responsible for coordinating central IT Infrastructure ,planning,applications and many more . the ITS Organization Successful at managing hundreds of servers For a different types of work groups of myried of servers and applications and there were Hundreds of computers used by students and employees in the University needed to be constantly patched.and the ITS organization was least successful over the University computers with the latest security patches.Information technology service Organisation it is a place where the IT work of the university were handled and taken care. The service is also described as “Being in a trusted partner and strategic resource to the university‘ the information technology (IT) services were used to involve in every single activities done by or taken place In the university.they provide All the security Tony sensitive information of employee staff, students, faculty . It is the main job of the Information technology service providers. And the other topmost priority was to secure There financial information and tax information of their employees staffs and students, which attracts the cyber criminals towards the University . So taking care of such sensitive data And providing a needed security to the information of the university is done by information technology service providers.

2. What attracts cyber attacker's to universities?

Ans Most Universities have less cyber security compare to other software companies and Contains more data over the student and the employees also. most of the cyber attacks takes place in the higher higher education University , and reason behind the attack is huge Financial and other data transaction between the University and student which attracts cyber attacks mostly.Higher education have not seen as direct Target for the Cyber crimes as it compared to critical National infrastructure or financial institutes where the most attacks are very common and there are many reasons behind the cyber attacks in university in which higher education is most common targeted in basis of thousands of student data transaction and many potential entry point in the universities hours are easily accessible by the attackers and moreover every university provides high-speed internet connection to their students where is the target for cyber attacks are used the connectivity against other distribution attacks. The rich assets and databases of the employees and students and staff working in the university attracts the cyber attacks and the financial information, personal information of the employees and students are targeted by the cyber attacks. Stolen data from the university are used in many ways a stolen identity and committing fraud from it and selling the data for attractive prices and offers is a common thing to the attackers.

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

Ans The most common attacks made in cyber crimes are spear phishing , unpatched systems, zero-day exploits

(1) Spear phishing

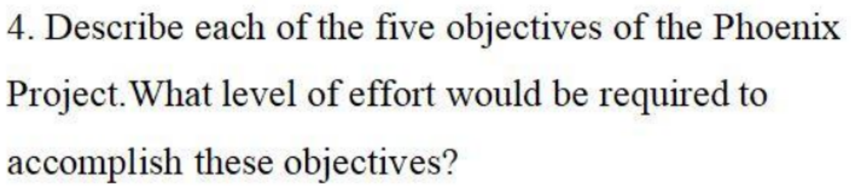
It means transfer of millions of messages or emails to a particular Employees or victim asking them To click on the link which Shared email or a message Which contains an infected file in it. After years of selecting only few persons in organization Or department. Creating email messages particularly for those employees or workers has known as spear phishing It is attacked and on and protected information and it is most popular and most effective attack on human history phishing is done on Particularly Selected individuals and organizations or a company who are targeted by the cyber attackers

(2) The unpatched systems

In this attack defined the computer system which have not been Patched properly. By this means the regular update of a software which are not installed properly in a company Which lead’s to System vulnerability. Software providers like Microsoft’s, iOS, android and adob And so on provides regular updates to there software It should be downloaded regularly To Overcome system Vulnerability .In this attack defined the computer system which have not been Patched properly. By this means the regular update of a software which are not installed properly in a company Which lead’s to System vulnerability. Software providers like Microsoft’s, iOS, android and adob And so on provides regular updates to there software It should be downloaded regularly To Overcome system Vulnerability .UVA’s ITS Has managed hundreds of servers of the word group Which Run Tons of applications Of university computers used by employees and hundreds of students and their systems which needed constant patches

(3) the zero-day exploit

The zero day exploit is a vulnerability In its score it is an unknown exploit in which it exposes the Vulnerability in software or hardware and create Undefinable problems in the system in which data leaves no identity in the system or in a software. That happens in a flaw where are malware is released to computer system before the developer creates a patch To the software.to mitigate these type of attacks a good firewall is mandatory with up to date antivirus with extra protection like safe browsing and ensure the security of the system .these firewalls monitors the traffic and block unauthorized sites which increases the extra protection to the system

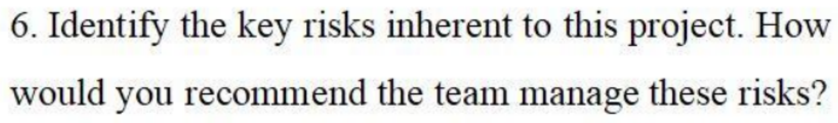


4. Describe each of the five objectives of the Phoenix Project.What level of effort would be required to accomplish these objectives?

Ans The first object was to determine the extent of the intrusion, the Objective was to make sure the level of infected system and the a access gained by the attackers us on them. The second objective was to bring up a remediation plan To make sure all the old systems affected by the attackers has been addressed in timely manner and then let the system enter to ‘go-dark’ Face in which the entire university internet could go down to get back with a new security system for the UVA . The third objective was to execute limitation plan to start the phase 2 to track the activities of the cyber attackers by developing (MOP) method of procedure which helps to protect the applications and rebuild the data on The system which were compromised and identifying all the impacted workstations by intrusion evaluating password management system of university to encourage the end users and after the dark phase . The fourth objective was to restore the data service securely after the go dark phase and test them properly to make sure all the university systems are working properly. The UVA spent a large amount of money and mans power to accomplish the mission The level of effort by the stealth army of 176 people in order to achieve the object. With the help of UVA employs for the project communication do you doing it in private outside the university via Google, Google document and other consulting taken from Microsoft's employees and government agencies.

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

Ans The various stakeholders associated with the Phoenix Project are internal stakeholders and external stakeholders.internal stake holders in the Phoenix Project includes UVA's most senior levels like the BOV, deans and vice presidents also all faculty, students,staff,alumni and retirees.whereas the external stakeholders in the Phoenix Project includes the governor's office, the attorney general,the general public and the press such as newspaper ,television stations,media. I Would have divided into groups the internal and external stakeholders the groups will be given certain task to complete with Priority wise as internal will take over the security breach damaged Servers and systems by the cyber criminals and to check on the systems which were compromised and to protect Other Servers and systems Before the Cyber criminals get their hand on them and external stakeholders deal with the university activities which were happening in the time of attack and Shutting down the programs And all systems and servers of the university to protect them by cyber criminals And the Groups should Report day every single step of updates done by the group stakeholders to the authority of universities.



6. Identify the key risks inherent to this project. How would you recommend the team manage these risks?

Ans There has been number of key risk associated in the finished project going dark phase was not so easy task for them as the time period was a whole weekend and Internet connection in the university will be complete shut down In the time period and if the security compromised Got to know by the public, time managing problems could arise in the UVA programme And events, human resources or potential technical issues could occur and so on but the chief information officer (CIO) Virginia Evans Took full responsibility on the attack ,considered it What is the topmost priority for her and she came up with a wonderful team she decided to be part of the Project And team for every single step to make it successful mission. It was a big challenge to get all remediation Work done in a short time. Teams are made to manage the project with the complete focus, they came up with the well orchestrated Plan and time schedule and they were successful in creating the team structure and assigning them the leads and keeping regular meetings with them to get the team rushed through process to go dark Face as soon as possible to take down the attackers from the University.

7. When and how should the success of the Phoenix Project be evaluated?

based on my analysis they should have been there System Health check on Every single servers in the university on day to day process and they should have started the Phoenix projects after the ‘Go-dark‘phase , It could have been a right time as the complete UVA’s Internet could be down for a whole weekend,The practice of announcement of new systems in the university could be done In the particular time. The university should start training their students By bringing awareness to them about cyber attacks and prevention of them and how not to fall for the traps of the cyber attacks.The Phoenix project, the project was started in university of Virginia where a major security breach occurred in 2015. The completion in various Intervals after its success. The dark phase was the promising time to start the first encounter and two test adjustments of the systems and to measure the strength of the security in the system . This should be The evolution to check the stability of the system of university and to prevent future attacks by the cyber criminals. Dark phase was to Shut down the network connectivity of the complete

University systems, it was needed to rebuild servers systems of the university and to encounter the Vulnerable accounts and servers By the cyber criminals and to stop from moving to others our systems and the conducted teams In worked hard to accomplish to given mission They were in check of the given project implementation and secondly to check the effectiveness After the rebuild servers systems .

Assignment 6

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		