CASE 1

Q) A finance-based organization found malware on one of their workstations connected to the network.

Hired a security consultant to revamp that machine

All done—Is the case closed?

1. No, Since the effected computer is connected on the network and hence, we need to install security protocol on the networks. We have to install the security protocol after we have analysed how much damage has been already done and how much of data has been compromised. Also, If the damage is intangible then all then all the systems need to be revamped

CASE2

Q) A famous medical practice center was hit by Crypto locker, a type of ransomware virus. It rendered the practice inoperable for several days, and crippled its technology for more than a week. The attack made its way onto one of the center's computers via an email attachment, which had the appearance of a vendor invoice.

Once on a computer, it searched for files to encrypt. This included files on the computer itself as well as those on the center's network that were accessible via mapped network drives. Files on any drive letter or network share that could be located and accessed (with a program such as Windows Explorer) was accessed by the ransomware.

Write a mitigation strategy? How will you impart your knowledge on future software to overcome such attacks?

A) Mitigation strategy:

1.Data should be back-upped every time a new commit is done to the system

**2.Data Encryption will allow the Sensitive data to remain secure even if it is locked out of your reach**

**3. Avoiding use of unknown pen drives (can contain the virus)**

**4.Updating all antivirus software as well as system software so that all the patch files can patch the existing bugs in the system**

**To avoid such attacks we need to design software which follows Risk Management Framework (RMF):**

**1. Understand the business context.**

**2. Identify the business and technical risk.**

**3.Synthesize, prioritize and rank the risk.**

**4. Define the risk mitigation strategy.**

**5. Carry out fixes and validate.**

**CASE 3**

**Q)** **Org 3 is a large organization in the technology sector that, owing to a large range of products and services, maintains a large number of websites. Suspicious activity had been reported from one of the smaller websites and so Org 3 commenced an investigation.**

**It was discovered that the website had an SQL injection vulnerability that had not been detected and had been present for over 5 years, despite being a relatively uncomplicated example of an SQL injection. Attackers had exploited the issue and used the SQL injection to upload a web shell, giving them greater access to the hosting server. The attackers extracted the contents of the database, and then uploaded tools to the web server from which to attack the internal network. The tools had included password extraction tools and privilege escalation exploits. Using these tools, the attackers compromised an account with domain administrator privileges and were attempting to compromise hosts that bridged multiple internal networks when Org 3 identified and stopped them. It was found that the attackers had gained access to a number of credit card details, as well as sensitive details around Org 3’s clients.**

**It was also assessed that had they not been stopped when they were, the attackers would have been able to access significant quantities of sensitive data about Org 3 and Org 3’s clients.**

**Q1)** **Write down the reasons for the specific failures leading to compromise.**

**A1) There were no regular checking of server and system. The password was not regularly changed. Also, since the organisation was big it had no security measures in place to the database of their clients and their confidential details even if they did. Their alert systems were vulnerable to these attacks hence didn’t flag them.**

**Q2)** **Write your incidence response practice for immediate action?**

**A2) Shut down the main server where there was a suspicious activity. Check all the system which were connected to that server and take a backup of important data and format the systems. Revamp the Machines as well as alert clients about their information leakage**

**Q3)** **Write down the necessary counter measure against this action?**

**A3) The server must regularly be checked. They must also keep a unique password which is difficult for password extraction tools to know the password as it will go for a brute force attack. The password must also be regularly changed.**

**CASE 4**

**Org 7, an African based manufacturing company became the victim of a <some> attack of their corporate email service. During a feedback session regarding a failed bid for a significant tender between Org 7 and the potential purchaser, Org 7 was informed that their submission was essentially identical to one of their competitors although more expensive. Org 7 were of the understanding that their offering and proposed strategy was unique to them as a company.**

**In response, Org 7 decided to investigate this incident further, realizing this was unlikely to be coincidental given they had recently laid off several employees. As the lay-offs occurred prior to the completion of the bid process, investigations initially focused on identifying key individuals involved in the bid, and critical assets responsible for transmitting and storing the related confidential data. After a few days of assessing the sources and accessibility of data, the compromise of their corporate email service was confirmed. The email service provider was immediately contacted and asked to supply information that would assist with the investigation. In response to the request, Org 7 was provided with the available access logs, the past 20 days, which was in-line with the service they had purchased. A review of the limited log data identified an unknown IP address having accessed five employee email accounts across a number of weeks. Each of the unauthorised accesses was found to exceed 45 minutes in length and often occurred for several hours. Lookups on the unknown IP address found it to be registered to a competitor. In attempt to contain the incident the passwords were immediately changed on the five email accounts identified. Log data provided for the following weeks showed failed login attempts on the date the passwords were changed and an additional log on attempt for a previously unidentified email account.**

**Overall, twenty email accounts were found to be using the compromised password. Limited visibility meant Org 7 was unable to determine how many of the twenty accounts were compromised as well as exactly what had been taken from them. It was assessed that a competitor had gained access to sensitive emails and likely used this information for the purposes of commercial advantage during the bid process.**

**Q1)** **What is the type of attack?**

**A1) Brute force attack.**

**Q2) Write your incidence response practice for immediate action?**

**A2) Change the password and keep a better security password. Also, keep files with important and sensitive information as encrypted files**

**Q3)** **Write down the necessary counter measure against this action?**

**A3) Regular change of password. Regular check of the logs.**

**Q4)** **Mitigation strategy to avoid these attacks?**

**A4) Regular change of password. Regular check of the logs.**

**Q5)** **Security guidelines to avoid these attacks?**

**A5) 1. Use Picture captcha so that a brute force attack cannot survive**

**2.lock the account after some attempts at passwords.**

**3. Send mail to the users referred email id/ Back up Email Id If logged in from a different IP address then the users usual.**