**NAME**

**COLLEGE NUMBER**

**Keywords:**

Spyware, malware, stealth, backdoor

**Introduction**

The purpose of standard operating procedure are supposed to give a guidelines in case of a system compromise, a disaster occurrence or any kind of anomaly has occurred within the organisation. In this particular case, we shall check a case by case scenario on what is the SOP in information security environments and what would be the way forward in case of such a activity.

Information and data are key component of the organisation and should be protected with zeal. This cuts across:

The network infrastructure which includes the routers, proxies, LAN connections, P2P computers and all data transmissions protocols.

All web application used as either primary or secondary channels of communications and access. Most of these applications are multiple unpatched and open leakages through which data can easily leak out and wreak havoc Whitman and Mattord (2011).

The system databases. Open ports and poorly programmed apps could leave room for SQL injection activities that eventual, can be exploited by malicious users into the organisation.

Social engineering. Confirmed with threat level as higher in risk, and can be a case of so many system compromises.

**Significance of this SOP**

To act as a guideline to the general stakeholders in the event of a disaster strike, system compromise or a forecast attack. The SOP shall provide a guideline one the processes and steps to be taken in case this breach is detected

**Who is this SOP for?**

In the event of a system breach, the following participants are required to act and take action appropriately to circumvent any further damages.

* The IT staff
* All other departmental staff
* All support staff, indicating with or partially with the organisations systems
* All organisational partners interacting with the system
* All support staff within the company

**Anti-Virus/Anti-Spyware/File Blocking**

There is need to identify malicious programs within the corporate, and thereafter be able to take remedial actions against these programs. The access by these programs into the organisation can have negative consequences that include:

* Loss of company data and information
* Loss of company confined among stakeholders
* Possible loss of patent information

**Trojan horse:**

Presumes itself as an innocent program, when randomly installed by any user in the network, will attach itself into the OS , of the host machine and later launch the attack by leaking the required information slowly.

**Viruses:**

Will multiply and replicate itself on the computer system and later start altering the applications installed in the computer.

Further, the viruses can spy on user’s information, computer and send any files that are essential to the attacker.

This SOP highlights the different threat levels associated with these threat levels as follows:

|  |  |  |
| --- | --- | --- |
| id | attack | level |
| 1 | worm | High |
| 2 | Virus | High |
|  |  |  |

In this regard, there is need to establish the correct method and mechanism for establishing /blocking such viruses and threats that can potentially be of risk to the company and the organisation at any given time.

**When should the SOP implement this?**

Should be implemented anytime when the users are on the network

**How to carry out this procedure**

**Definition of key terms**

|  |  |  |
| --- | --- | --- |
| index | term | meaning |
| 1 | Adware | A software application that automatically renders adverts |
| 2 | Malware | A malicious program that compromises computer systems |
| 3 | Ransom ware | A malicious program that encrypts files until amount is paid |
| 4 | Worm | Continuous set of general harmful programs to the computer |
| 5 | Rootkit | A software program that hides itself in the computer and continuous to gain privileged access to the system |
| 6 | Spam | Unsolicited emails that harbour harmful bait links |

**Antivirus programs**

Antivirus programs protect the system by helping to detect any form of incoming harmful program, flagging it and then stopping it from installation Sukwong, et al (2011) . In other cases, the antivirus also removes itself from the already infected system. The antivirus program should be installed across all computers clients on the systems and regularly updated form time to time to ensure all systems are up to date. IT department shall be in charge of regularly updating the antivirus libraries. In the event of patch, the following services may be disconnected:

* Intranet access
* Certain websites
* Automatically downloads
* Emails from unrecognised domains

**Anti-spy ware**

Should be installed on all operating systems and applications. Most of the spy apps occur on TV sets, CCTV camera severs, laptop cams, and mobile handsets. During implementation, ijjt is required that all staff members quarantine their mobile handsets and limit access to the internal network access Kaeo (2004). Further, staff, enters are not allowed to bring their own devices to work. All CCTV cameras shall have continuous monitoring and frequent backups implemented on the network.

**File blocking**

Certain file extensions that may contain malicious programs such as .min, .exe , or some sort of archival shall be flagged where necessary and incident issues raised with the user. The origin of these files such as emails, links, external websites an USB drives shall be blocked. In case of attack and compromise:

1. The affected systems shall be temporarily disconnected from the network
2. Users operating these systems, shall be automatically logged our and their aces limited
3. An immediate back up shall be established for business continuity
4. Immediate communication shall go out to all the affected parties and clients.

**REFERENCES**

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage learning.

Kaeo, M. (2004). *Designing network security*. Cisco Press.

Sukwong, O., Kim, H., & Hoe, J. (2011). Commercial antivirus software effectiveness: an empirical study. *IEEE Computer Architecture Letters*, *44*(03), 63-70.

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, *48*(8), 72-77.