Technical Center of Technological Technologies

Andrew Maddox

Incident Response Plan

### Table of Contents

[I. Cover Page 3](#_Toc52620470)

[II. Table of Contents 4](#_Toc52620471)

[III-V. General Information 5](#_Toc52620472)

VI-[. General Information/Body 6](#_Toc52620473)

**General Information**

The current infrastructure of the main office of the Technical Center of Technological Technologies consists of two hundred main desktops running windows 7 and half of them have currently been infected with the Cinderella Virus/Malware. The reason this infection has occurred is due to a current employee following a phishing link and receiving the wrong application which has currently infected some files with the extension CO, DOC, OC. This infection was found later then planned and was not found quickly due to inefficient observation of files and security aspects, lack of employee knowledge on phishing attacks, and the malware itself is stored on a low system memory and does not reduce available memory. Given this information the company will better be able to combat the issue and resolve what is currently at hand.

**Response to the Incident**

The core cause computer for this infection has been isolated along with all the other devices also infected so spreading of the issue should be determined ineffective currently. A new implementation of anti-phishing campaigns including frequent warning emails, better observation, and phishing courses to combat possible future mistakes. The IT team has been handling the majority of the response to this incident and the current computers will most likely be scrapped as the current hardware was needing revision thus a complete rehaul will be more beneficial for the company. The rehaul of systems was not required for the current systems as it could have been handled through other means but as the rehaul was already needing to be done with employee complaints about slow computational power. This response to the incident will result in happier employees with higher processing power and combatant to the current systems installation of the infected files. The current systems and setup could be combatted with certain antivirus software which will also be installed as a portion of the rehaul. Another area of concern is the lack of diligence with some of the IT department and some of the individuals in the IT department will be let go due to this issue. Many of these issues arose from neglect in the current IT department staff not including all of these individuals but some. This will be beneficial to the company having new individuals in the IT department and removing the core issue with a rehaul of systems and some employees.

**Current Damage and Expenses**

Given the current rehaul of half the systems and an upgrade to Windows 10 from Windows 7 expenses will have to be calculated. The current average for the new desktops being purchase for the HP ProDesk 400 Series will be $600 per system at full price not including possible bulk reduction. This will average $60,000 for the rehaul of 100 systems for the current infrastructure. Since the initial infected devices will be replaced, we will also include the other 100 systems in the rehaul. This will make the total for the rehaul of 200 systems $120,000 along with the addition. This was not a required rehaul as far as system replacement but a well needed one given the current infrastructure. Getting Bitdefender Gravity Zone Business Security for 200 devices for a year will cost around $4,088 dollars. This given will make the overall rehaul for the current infrastructure $124,088 and will be discussed with management for further bulk options or discounts that could be received for such a large number of devices. Nothing on the server end was affected so there will be no revisions on that area of concern.

References

Cinderella Description Labs. (n.d.). Retrieved from <https://www.f-secure.com/v-descs/cinderel.shtml>

GravityZone Business Security Enterprise. (n.d.). Retrieved from https://www.bitdefender.com/business/smb-products/business-security.html

HP ProDesk 400 Microtower Desktop / Business PCs. (n.d.). Retrieved from https://store.hp.com/us/en/mdp/desktops/prodesk-400-microtower-244040--1

Online VSUM - Cinderella Virus. (n.d.). Retrieved from http://wiw.org/~meta/vsum/view.php?vir=304