Incident Report Planning Sheet

Create a title after filling information in below. Use bullet for information under each heading and then use the bullets to write a complete report.

Title
Compromised computers at DHS office

Summary
A security breach at the Department of Human Services was determined to be from the cause of faulty network interface cards on the new computers. We were called to go onsite in Victoria to examine the cause of the initial warning and found the solution.

The incident prompts necessary upgrades that need to be installed in order to prevent this from happening in the future.

Timeline
At 9:45am Sissy Spacek was called by one of her office managers about a malware warning they received on one of their computers, she ran a security protocol and 13 of their brand new computers were flagged

At 10:30am Ang Lee notifies me that I need to prepare for a flight to the Department of Human Services (DHS) as sensitive information has been breached.

At 11:30am: I take the helijet from Downtown Vancouver to downtown Victoria that takes about 35 mins

At 12:15pm: I take a cab to the DHS office after landing in downtown Victoria

At 12:30pm Ran initial system scans. But they didn't tell what data had been downloaded. And don't show large downloads have taken place from outside. Doesn't seem like anyone penetrated the firewall

At 3:10pm after taking a walk I returned to the office to test out an idea and discover the cause of the problem is the faulty network interface cards (NIC) in the 20 new computers

At 3:45pm Called Ang to explain the problem.

At 5:00pm Replacement cards should be delivered to the DHS.

At 7:00pm All the new computers have their NIC replaced and servers return online.

Root Cause

The root cause of the problem was the network interface cards inside the computers. They were caused by a defect from the factory. The faulty cards were getting high data outputs that other security scans didnt support. When swapping network cards with a secure network card, the computer was sending out the same readings as a secure computer.

Resolution and Recovery

Replaced the faulty cards within the computers

Corrective and Preventative Measures

Upgrading software security and include security for other devices
Have systems in place that allow professionals to control from their base

In order to prevent similar issues from occurring in the future, the DHS need to upgrade their systems of security. The DHS needs to centralize their security so that professionals, like myself, are able to control and handle similar situations remotely. We have also talked about upgrading the software of the security system - suggesting Symantec's new Integrated Cyber Defense System as a valuable product. With many employees these days utilizing other devices for government work, we should look into broadening cyber security systems to cover all operating softwares and devices used.

To: Ang, Brianna, and Kele
From: Jayden, Tommy, and Evan
Date: March, 07, 2024

Compromised computers at DHS office

Summary

A security breach at the Department of Human Services was determined to be from the cause of faulty network interface cards on the new computers. We were called to go onsite in Victoria to examine the cause of the initial warning and found the solution.

The incident prompts necessary upgrades that need to be installed in order to prevent this from happening in the future. This includes: a centralized system for remote access, software upgrades, and broadening security to include other devices.

Timeline

9:45am: malware detected at DHS
10:00am: Sissy takes affected computers offline
10:30am: I prepare to go to DHS
11:30am - 12:15pm: I traveled to DHS
12:30pm: System scan was ran detecting new issue
3:10pm: Discovered the network interface cards were the cause
3:45pm: I spoke to Ang Lee about the fix
5:00pm: DHS received replacement cards
7:00pm: Everything up and running

Root Cause

The root cause of the problem was the network interface cards inside the computers. They were caused by a defect from the factory. The faulty cards were getting high data outputs that other security scans didn't support. When swapping network cards with a secure network card, the computer was sending out the same readings as a secure computer.

Resolution and Recovery

At 9:45am one of our office managers was browsing local government websites and got a warning from Symantec Norton about malware being detected. He then called Sissy and they ran the Symantec Security Protocol. It flagged thirteen of the brand new computers as having data being sent out onto the net.

At 10:00am Sissy took all of the compromised computers offline, but they were unsure if the damage had already been done. She then called Ang Lee to inform him.

At 10:30am Ang Lee notified me that he spoke with Sissy and they identified malware on their computers. I then prepared for a flight to the Department of Human Services (DHS) office in Victoria at 11:30am..

At 11:30am I boarded the helijet in downtown Vancouver to downtown Victoria, estimated time of arrival is 35 minutes

At 12:05pm After landing in downtown Victoria, I take a cab to the DHS office, estimated time of arrival is 10 minutes

At 12:15pm I arrive at the DHS office and enter inside and talk with Sissy SpaceK about the problem they are facing

At 12:30pm I ran the initial system scans, the scans dont give information about what data was being downloaded or that any large amounts of data was being downloaded from outside. Doesn't seem that anyone penetrated the firewall and compromised the computers

At 3:10pm after taking a walk I returned to the office to test out an idea and discover the cause of the problem is the faulty network interface cards (NIC) in the 20 new computers

At 3:45pm I called Ang Lee to inform him that a solution had been found and discussed what the next step moving forward would be

At 5:00pm the replacement network interface cards were delivered to DHS to be implemented into the affected computers

At 7:00pm all the replacement cards were implemented into the new computers and everything is back online

Corrective and Preventative Measures

In order to prevent similar issues from occurring in the future, the DHS need to upgrade their systems of security. These include:

- The DHS needs to centralize their security so that professionals, like myself, are able to control and handle similar situations remotely.
- We have also talked about upgrading the software of the security system - suggesting Symantec’s new Integrated Cyber Defense System as a valuable product.
- With many employees these days utilizing other devices for government work, we should look into broadening cyber security systems to cover all operating softwares and devices used.