TechBros Incident Report

A logo for a company

Description automatically generated

Prepared by: Terrelle Thomas (TechBros Manager)

Last Modified: July 10, 2023

Developed By: NSAEF

Created: Version 1 July 2022

Purpose

The TechBros, a trusted computer seller provider to the consumers of the Pittsfield County in New Rochelle, New York. TechBros stores information related to students, staff, and internal business operations, as well as manages and maintains technical infrastructure required to house and maintain this information.

This Cyber Security Incident Response outlines the procedures TechBros uses to detect and respond to threats to assets own by TechBros. More specifically, this plan defines the roles and responsibilities of various TechBros staff with respect to the identification, isolation, and repair of data security breaches, outlines the timing, direction, and general content of communications among affected stakeholders, and defines the different documents that will be required during various steps of the incident response.

TechBros also implements practices designed to proactively reduce the threats to the company assets.

such as training staff with respect to legal compliance requirements, following appropriate physical security and environmental controls for technical infrastructure, and deploying digital security measures such as firewalls, malware detection and numerous other industry standard systems.

In the event of a cyber security incident, TechBros staff have been trained to expeditiously deal with the matter. TechBros staff are trained on a yearly basis to recognize anomalies in the systems they regularly utilize, and to report any such anomalies as soon as possible to the Incident Response Manager so the Incident Response Team can be mobilized. Throughout the year the Incident Response Manager and members of the Incident Response. Team is kept up to date on the latest security threats and trained in modern techniques of incident remediation. The availability and protection of the information resources managed by the systems we maintain is of paramount importance to our school district and will always be a core value of our organization.

**Incident Summary**

|  |  |
| --- | --- |
|  |  |
| Incident ID | DSA-45A7TY |
| Breach Type | Denial-Of-Service Attack |
| Incident Severity | Medium |
| Effect of The Incident | Loss of Revenue |
| Incident Owner | Terrelle Thomas |
| Earliest Flagged Evidence | Unusual High Traffic In The Network |
| Most Recent Flagged Evidence | Locked Out of The Company Network |
| Type of Incident | Deliberate Software Attack |
| Date Incident Originated | March 1st, 2023 |
| Date Incident Was Detected | March 22nd, 2023 |
| How Was Incident Detected | Locked Out of Computer Network and Files |
| Scope of Incident (Districts/System Affected) | All Departments, Computers and Servers |
| Date Incident Corrected | June 1st, 2023 |
| Corrective Action Type | Reduction Mitigation Strategies |
| Time to Resolution | 3 Weeks and 3 Days |
| Reason for Closure | Resolved |

***Summary of Incident Symptoms***

1. Internet Disconnection
2. Slow Access to Files
3. Inability to access a specific file.
4. Excessive Amount of Spam Emails
5. An IP address makes an unusual large number of requests in a limit lifespan.
6. Log analysis indicated a large spike in network traffic.

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated with medium confidence

***Summary of Incident Type and Scope***

1. The employee’s of TechBros couldn’t enter the company assets such as server and computers when they try log in back to do their work.
2. All the employees from the different sections of the company were affected by the software attack.
3. The usual auditors of the servers couldn’t enter the server system to audit the server. They were locked out of the server system.
4. Even though some of the computers was regular open, all TechBros files was either locked from the network.
5. The log of the week that the threat happens, there was unusual high level of traffic happening in the TechBros network system.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A close-up of a document

Description automatically generated

***Process Improvement Plan***

***Summary of Corrective Actions***

1. Update TechBros Security Policies
2. Update or Upgraded Security Measures

**Summary of Migration Process and Internal Communications**

1. Do assessments test on the company to identify all assets in the company are counted for.
2. Identify the threat that is happening in the situation.
3. Identify the effect that the threat had on the company asset.
4. Do internal investigations by the company and external investigation from law enforcement to figure the suspect of the crime.
5. After prosecution, identify the vulnerability of the assets and figure how the crime was would put into the action.
6. Plan and excuse measures such as avoidance strategies to prevent this attack from happening anytime again.

A close-up of a document

Description automatically generated

A close-up of a paper

Description automatically generated

***Communication Log***

|  |  |  |  |
| --- | --- | --- | --- |
| Communication Date | Communication Type | Recipients(s) | Purpose |
| 03-22-23 to 04-10-23 | Verbal | Incident Owner | To report the symptoms of the treats that the company have face unusual traffic on the network |
| 04-11-23 to 04-21-23 | Verbal | Employee’s | Let to do Assessment and audit on the company assets to seek any changes |
| 04-22-23 to 04-28-23 | Verbal | Incident Owner | Report their findings of the attack |
| 04-29-23 | Verbal | Law Enforcement | Report any loss and giving play by play of the situation |
| 04-30-23 to 05-15-23 | Verbal, Written, Visual | Law Enforcement | Investigate The Matter, Find Possible Suspects, Interview the Company, Report Their Findings, Bring the Suspect to Justice and Be Witness of the Trail |
|  |  |  |  |



***Areas of Success Summary***

1. No other devices connected to TechBros was not affected during the attack.
2. No physical hard damage to the business
3. No loss of data or confidential data was reported loss or release to the public.

***Areas in Need of Improvement Summary***

1. Company Network
2. Company Software Security Measures

***Recommended Improvements to Avoid Future Incidents***

1. Update/or Upgrade Company Network
2. Upgrade or Upgrade Software Measures such as Firewall’s

|  |  |  |
| --- | --- | --- |
| Improvement | Timeframe | Cost ($) |
| 1. Update/or Upgrade Company Network | 1 month | 2,000 |
| 1. Upgrade or Upgrade Software Measures such as Firewall’s | 1 month | 2,000 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Closure Notes**

1. The company needs to keep a better eye of unusual traffic in the network.
2. TechBros needs bi-weekly training and practice on software attacks.
3. Our Incident Response Plan works very good to the incident but always can get better.
4. The company is like other companies that needs to update their security measures to the fullest and don’t slack on measures.
5. The Company needs to but harder security measures on their assets to prevent any harder effects.
6. The Response Plan helped to resolve the different attack issues that TechBros faces on a daily.