[company]

3/17/2017

From: Team X
To:
Subject: Incident Report Template

Hello,

We have completed our incident report template. The report is designed to allow executives to quickly learn about and gauge the business impact of a security incident, while providing in-depth details and evidence to technical staff. A ‘Lessons Learned’ sections is also included for reflection and self-assessment, so we can continually improve our incident response process and identify areas of weakness.

Please see the attached report template, and feel free to reach out to us with any questions or concerns.

Regards,
Team X

[company]

Incident Response Report

Prepared 17 March 2017

Table of Contents

Executive Summary

- Overview of information to be provided in the rest of the document
- Type of incident
- Clearly state impact to the business
    - Compromised systems, downtime, etc.
    - Residual risks incurred by the business
- How it happened (summary)
- Corrective action plan (how we are going to fix this)
- How we can adapt to prevent this in the future

Incident Overview

Type of Incident: <malware, bruteforce, DoS, network scan, backdoor, etc>

Priority: <[high|medium|low]>

- High: data exfiltration, remote execution, privilege execution, passwords cracked, pivoting, data loss, high profile malware/spyware, privacy breach, monitoring
- Medium: Contained breach (passwords hashes stolen stolen but not cracked), malicious binary detected and mitigated early, DDoS attempts
- Low: Ineffectual attacks, scans, brute force attempts

Initial Detection: <date>

Incident Time Frame: <period where malicious activity took place/is still taking place or estimated time frame>

Total Response Time: <x minutes>

Affected Operating Systems:

- Operating System
- IP/Network/hostname configuration
- Known Services
- Installed software versions
- Patch Level

Affected Users:

Incident Description:

Recovered Evidence

- Evidence supporting the fact that the incident occurred
    - Must be specific
    - Prove that this was a targeted attack
- Include the following:
    - Source and destination addresses
    - Timelines of activity
    - Screenshots
    - Network traffic captures
    - Log snippets
- Report damage done, if any:
    - Passwords cracked
    - Access obtained
    - Files deleted
    - Etc

Business Impact

- Goal: Describe the impact to the company in business terms
- Think about: “what does this incident mean to the business?”
    - How business procedures were disrupted
        - Customers can’t buy things
        - Employees unable to access services to do their jobs
    - How revenue may have been lost
    - E.g. customers were unable to access our website for 3 hours, lost estimated $50,000 in sales
- Consider extent of customer dissatisfaction, and how to mitigate

Primary Cause

- The initial vulnerability that allowed the event to occur or spread
- The people, process, technology targeted
- Points of weakness, how they were discovered

Response Process

- Describe the steps our team took to respond, in chronological order
    - Initial detection
    - Information gathering
    - Assessment
        - Purpose/end goal of malicious activity
        - Determine impact and immediate threat
    - Containment
    - Prevention
    - Recovery
- Be as specific as possible
    - This timeline can be used to assess gaps
        - Essentially “what we’re missing”

Residual Risk

- Any continued risk to the business revealed by this attack
    - E.g. customer credit cards exposed and obtained
- Rank risks that were exposed in order of highest priority to least priority

Remediation Plan

- Describe what has/will be done to clean up technical damage
    - Restore user accounts
    - Replace compromised systems
    - Etc.
- Describe what has/will be done to address risks
    - If possible give a timeline of when these will be handled
- Clearly delineate what has been done and what still needs to be done
- How can we prevent this from happening again?
    - Technical solutions
        - Network security
        - Application security
        - Etc.
    - Non-technical solutions
        - Written policies
        - Physical security
        - Etc.

Lessons Learned

- What went wrong to allow this to happen?
    - Is there an inherent architectural flaw in our network?
    - Is there a necessary process/workflow change?
- What went wrong in our response?
    - Could we have responded faster?
    - Were there any major blocking factors throughout our response?
    - What can we change to eliminate these inhibitors?
        - Internal process changes?
        - IR workflow changes?
- Consider both technical and non-technical factors