Feedback Ferret

Security Incident Response Plan

Document Reference	Feedback Ferret – Security Incident Response Plan
Version	3.0
Date Created	June 2013
Effective From	20 June 2013
Issued By	Feedback Ferret – Systems
Changed History	Reviewed – June 2016
Enquiry Point	Mark Spicer Technical Director Feedback Ferret Limited 22 Wycombe End Beaconsfield HP9 1NB United Kingdom Tel: +44 (0) 1628 681 088 Email: mark.spicer@feedbackferret.com

Table of Contents

Purpose of this Document

Feedback Ferret (hereinafter referred to as "the company") takes the threat of security breaches very seriously and is committed to understanding and minimizing risks associated with those threats.

This document provides the company's security breach and incident response plans.

Minimizing the Number and Severity of Security Incidents

In most areas of life, prevention is better than cure, and security is no exception. Wherever possible, we attempt to prevent security incidents from happening in the first place. If a security incident does occur, our goal is to ensure that its impact is minimized. To minimize the number and impact of security incidents, we:

- Follow and enforce all security policies and procedures as defined in the Feedback Ferret – Corporate Security Policies document. This enforcement reduces the chance of a risk being accidentally created by personnel who have not followed or not understood change security procedures or have improperly configured security devices, such as firewalls and authentication systems. The company security policies and procedures are thoroughly tested to ensure that they are practical and clear and provide the appropriate level of security.
- Provide and enforce support for security policies and incident handling across the business.
- Routinely assess vulnerabilities in our environment.
- Routinely check all computer systems and network devices to ensure that they have all the latest patches installed.
- Establish security training programs for both IT staff and end users.
- Develop, implement, and enforce a policy requiring strong passwords.
- Routinely monitor and analyse network traffic and system performance.
- Routinely check all logs and logging mechanisms, including operating system event logs, application specific logs and intrusion detection system logs.
- Verify our back-up and restore procedures.

Security Team

The company has a IS technical team that is responsible for data and network security so the responsibilities and remedies for any breaches will fall to that IS team.

The Company has a well-defined technical solution which is developed using and hosted on industry-leading platforms such as the Amazon Web Services and Liquid Web platforms.

Incident Response Plan

Making an Initial Assessment

Many activities could indicate a possible attack on the company or company systems. For example, a network administrator performing legitimate system maintenance might appear similar to someone launching some form of attack. In other cases, a badly configured system might lead to a number of false positives in an intrusion detection system, which could make it more difficult to spot genuine incidents.

As part of our initial assessment, we:

- Take steps to determine whether we are dealing with an actual incident or a false positive.
- Gain a general idea of the type and severity of attack. We gather information to begin communicating it for further research and to begin containing the damage and minimizing the risk.
- Record our actions thoroughly. These records will later be used for documenting the incident (whether actual or false).

Communicating the Incident

If we suspect that there is a security incident, we quickly communicate the breach to the rest of the core technical team and quickly identify anyone else who needs to be contacted outside of the core team. This will help to ensure that appropriate control and incident coordination can be maintained, while minimizing the extent of the damage.

Initially it is important to prevent an attacker from knowing that we have detected their intrusion as that may trigger them into immediate destructive behaviour. For this reason, and to prevent an attacker from being tipped off, only those playing a role in the incident response should be informed until the incident is properly controlled. Based on the unique situation, our team will later determine who needs to be informed of the incident. This could be anyone from specific individuals up to the entire company and external customers. Communication externally should be coordinated with the client services team.

Containing the Damage and Minimizing the Risks

We plan to act quickly to reduce the actual and potential effects of an attack, hopefully making the difference between a minor and a major one. The exact response will depend on the nature of the attack that faces us. However, the following priorities are considered as a minimum:

1. **Protect human life and people's safety.** Obviously our first priority, but this is not necessarily something which the company would normally need to be concerned with due to the nature of our business and service.
2. **Protect classified and sensitive data.** As part of our planning for incident response, we have clearly defined which data is classified and which is sensitive. This enables the company to prioritize our responses in protecting the data.
3. **Protect other data, including proprietary, scientific, and managerial data.** Other data in our environment is still of great value. We act to protect the most valuable data first before moving on to other, less useful, data.
4. **Protect hardware and software against attack.** This includes protecting against loss or alteration of system files and physical damage to hardware. Damage to systems can result

in costly downtime.

5. **Minimize disruption of computing resources (including processes).** Although uptime is very important, keeping systems up during an attack might result in greater problems later on. For this reason, minimizing disruption of computing resources should generally be a relatively low priority.

There are a number of measures that we can take to contain the damage and minimize the risk to our environment. At a minimum, we would:

- Try to avoid letting attackers know that we are aware of their activities.
- Compare the cost of taking the compromised and related systems offline against the risk of continuing operations.
- Determine the access point(s) used by the attacker and implement measures to prevent future access. Measures might include disabling a modem or VPN, adding access control entries to a router or firewall, or increasing physical security measures.
- We would also consider the merits of rebuilding a fresh system with new hard disks (the existing hard disks would be removed, obviously). Ensure that we change any local passwords. We would also change administrative and service account passwords elsewhere in our environment.

Identifying the Severity of the Compromise

To be able to recover effectively from an attack, we would determine how seriously our systems have been compromised. This will determine how to further contain and minimize the risk, how to recover, how quickly and to whom we should communicate the incident, and whether to seek legal redress.

We would attempt to:

- Determine the nature of the attack.
- Determine the attack point of origin.
- Determine the intent of the attack. Was the attack specifically directed at the company to acquire specific information, or was it random?
- Identify the systems that have been compromised.
- Identify the files that have been accessed and determine the sensitivity of those files.

By performing these actions, we should be able to determine the appropriate responses for our environment. A good incident response plan will outline specific procedures to follow as we learn more about the attack. Generally, the nature of the attack symptoms will determine the order in which we would follow the procedures defined in the plan. Since time is crucial, less time-consuming procedures would generally be carried out before more lengthy ones. To help determine the severity of the compromise, we should:

- Contact other members of the response team to inform them of our findings, have them verify our results, determine whether they are aware of related or other potential attack activity, and help identify whether the incident is a false positive. In some cases, what might appear to be a genuine incident on initial assessment will prove to be a false positive.

- Determine whether unauthorized hardware has been attached to the network or whether there are any signs of unauthorized access through the compromise of physical security controls.
- Examine key groups (domain administrators, administrators, and so on) for unauthorized entries.
- Search for security assessment or exploitation software.
- Look for unauthorized processes or applications currently running or set to run using the start-up folders or registry entries.
- Search for gaps in, or the absence of, system logs.
- Review intrusion detection system logs for signs of intrusion, which systems might have been affected, methods of attack, time and length of attack, and the overall extent of potential damage.
- Examine other log files for unusual connections; security audit failures; unusual security audit successes; failed logon attempts; attempts to log on to default accounts; activity during non-working hours; file, directory, and share permission changes; and elevated or changed user permissions.
- Search for sensitive data, such as credit card numbers and employee or customer data, which might have been moved or hidden for future retrieval or modifications. We may also have to check systems for non-business data, illegal copies of software, and e-mail or other records that might assist in an investigation

Recovering Systems

How we recover our system will generally depend on the extent of the security breach. We will need to determine whether we can restore the existing system while leaving intact as much as possible, or if it is necessary to completely rebuild the system.

Data can be restored from a previous clean backup – i.e. a backup made before the incident occurred. However, an incident could potentially corrupt data for many months prior to discovery. It is, therefore, very important that as part of our incident response process, we determine the duration of the incident. In some cases, the latest or even several prior backups might not be long enough to get to a clean state, so we should regularly archive data backups in a secure off-site location or secure online archive repository.

Compiling and Organizing Incident Documentation

The response team should thoroughly document all processes when dealing with any incident. This should include a description of the breach and details of each action taken (who took the action, when they took it and the reasoning behind it). All people involved with access must be noted throughout the response process.

Afterward, the documentation should be chronologically organized, checked for completeness, and signed and reviewed with management and even legal representatives, if necessary. We will also need to safeguard any evidence collected.

Reviewing Response and Updating Policies

Once the documentation and recovery phases are complete, we will review the process thoroughly. With our team we will determine which steps were executed successfully and which mistakes were made.

If we find weaknesses in our incident response plan, which is the reason behind a post-mortem exercise, we look for opportunities for improvement, which may initiate a whole new round of the incident response planning process.

