Incident Response Plan: Denial of Service

Contents

1 Introduction

A denial of service (DoS) attack occurs when a (usually Internet-connected) service is flooded with network traffic or service requests, making it unavailable to legitimate users. This traffic may originate from a small number of systems or, more commonly, from a huge number of devices that are under the attacker's control – this latter situation is known as distributed denial of service (DDoS) attack.

Attacks may vary in length from minutes or hours to (more unusually) days and may come in several waves. Depending on the target of the attack, the motive of the attacker could be political, purely malicious or financial (for example as a form of extortion). It is important however, to be able to recognise the difference between a DoS attack and legitimate demand for the service, for example during a scheduled sales event, and this relies upon good communication between the business and the IT provider.

At the technical level, various methods may be used to attack a target by overloading one or more of the resources of the system, for example the network, the processor or the application itself. Each of these has its own methods of mitigation that may be considered.

This incident response plan describes the steps that must be taken to manage a DoS attack and attempt to limit its impact.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Castlereagh Macquarie County Council systems.

The following policies and procedures are relevant to this document:

- *Information Security Incident Response Procedure*

2 Responding to a denial of service attack

There are a number of steps that must be carried out by Castlereagh Macquarie County Council to respond to a denial of service attack, so that the impact on the organisation is minimised and recovery may take place as quickly as possible. These steps must be coordinated with the actions set out in the *Information Security Incident Response Procedure* which provides an overall framework for the management of such incidents. The steps below are organized to fit in with this framework.

2.1 Detection and analysis

Understanding more about its source and method are key to containing a DoS attack. Investigations must be made via available software tools to clarify answers to the following questions:

- Is it a DoS attack? Could it be a result of legitimate interest in the website for some unexpected reason, for example unplanned publicity?
- What is the source of the attack? Is it a single IP address or multiples, and where do they appear to originate from?
- How is the denial of service being achieved? Is it at the network level, application level or via some other method?
- Is any other suspicious activity taking place at the same time, for example unauthorised access attempts?

2.2 Containment

Depending on the answers to the above questions, a number of actions may be available to help to contain the attack, such as:

- Scaling up capacity to cope with the increased demand, for example network bandwidth or cloud server capacity
- Restrict access to the IP address under attack, if multiple IP addresses are used to provide the service
- Deliberately degrade the level of service available, for example by disabling computationally intensive features such as search
- Use a Content Delivery Network (CDN) provider to make static versions of the website available at multiple locations (although this may not be available at short notice)

Records must be maintained of the actions taken, so that they may be restored once the attack is over.

2.3 Eradication

The specific actions required to eradicate the attack will depend on the method it uses, although containment may be all that is possible. The attack may cease of its own accord, but further waves are certainly possible. Typically, no malicious software is installed in a DoS attack, although care must be taken to check whether the attack was a cover for other activities which might include exploiting software vulnerabilities to obtain access to the network.

Log files may need to be reset, and storage space freed up if these were affected.

2.4 Recovery

In most cases, restore from backup will not be required, unless the attack has resulted in some form of data loss. Any vulnerabilities that were exploited as part of the attack will need to be addressed, ideally via patching or reconfiguration.

A review of the incident may identify weaknesses in the current infrastructure and applications that could be fixed to prevent reoccurrence.

2.5 Notification

It is recommended that relevant law enforcement agencies are notified of the denial of service attack as soon as possible. Depending on the scope of the attack, it may also be appropriate to inform partner organisations, such as suppliers who have network connections, about the incident.

Given that this type of attack does not typically involve the theft of data, the need to notify in compliance with regulations (such as the GDPR/Australian Privacy Act) must be carefully considered.

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES