Incident Response Plan: Ransomware

Contents

1 Introduction

Ransomware is an increasingly common form of malware which typically encrypts files, so preventing them being used. Many forms of ransomware will do this on the infected computer and then attempt to spread across the network to other computers, encrypting as they go. The files cannot be decrypted without a specific key, which is held by the attacker who demands a ransom to be paid, usually in cryptocurrency, before the key may be released to the infected organisation.

In addition to those forms of ransomware that encrypt files, other forms may do one or more of the following:

- Steal data that the attacker then demands a ransom not to release or publicise
- Render computers inoperable by encrypting vital system files
- Restrict access to files without encrypting them

A ransomware attack typically begins by a single computer becoming infected with the malware, often via a phishing email (containing a link or an attachment) or a compromised website. Once the malware is installed on the infected computer, it calls base across the Internet to obtain an encryption key from the attacker. It then uses this key to start encrypting data and attempts to spread itself to other computers and network storage. At some point after sufficient data has been encrypted (which could be several months after first infection), the malware issues a ransom demand with basic information about what has happened and how to pay.

This incident response plan describes the steps that must be taken to manage a ransomware 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 ransomware attack

There are a number of steps that must be carried out by Castlereagh Macquarie County Council to respond to a ransomware 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

This plan begins from the point at which it has been confirmed that an incident is a ransomware attack. This confirmation is likely to result from a ransom demand being made, either by the malware itself or by a third party, for example via email. However, the plan may also be invoked if there is a reasonable belief that a ransomware attack is underway, as an early response is key to limiting the impact.

2.2 Containment

Since ransomware will attempt to spread to other computers and devices, it is important to disconnect those that are known to be infected from the network. This will involve removing network cables from the hardware and turning off any Wi-Fi or other wireless connections (such as Bluetooth) as soon as possible. Any other storage devices attached to the infected machines must also be removed.

If the extent of the infection is unclear, it may be appropriate to remove connections between network segments in order to prevent spread. If possible, remove connections to important data that has not been affected, for example key database servers or network attached storage.

In parallel with containment activities, efforts must be made to identify the ransomware involved. If a ransom request has already been received, this may include information about the malware. Various resources are available to help organisations that have been affected by ransomware, including obtaining encryption keys, but they rely upon a clear definition of the malware involved.

Our Managed Service Provider, vendors of anti-malware software and external consultants available via our cyber-insurance company may also have resources available to help.

2.3 Eradication

Once the identity of the ransomware has been established, there are three main options to eradicate the infection:

1. Pay the requested ransom
2. Attempt a clean-up to remove the ransomware
3. Perform a full recovery from backup

In agreement with the recommendations of law enforcement agencies, it is Castlereagh Macquarie County Council's Policy that ransoms will not be paid in these circumstances. Although there are publicised cases of ransoms being paid, there is no guarantee that a solution will be provided by the attacker, and there have been cases where a ransom was paid shortly before the attacker was brought down by law enforcement, resulting in no encryption keys being issued. However, paying the ransom remains an option which top management may consider.

There are websites which make software available to attempt to remove ransomware, but these are very dependent on the specific strain of malware involved. Ransomware is also becoming increasingly sophisticated and resistant to removal, so it is unlikely (although not impossible) that this option will be available.

The safest option can be to wipe and reinstall all affected systems from backup. However, an assessment should be made as soon as possible of the extent to which backups may have been infected by the malware. Our Managed Service Provider will be contacted as soon as a ransomware attack is suspected to being the process of checking backups and restoring from the latest unimpacted version. However, an assessment should be made as soon as possible of the extent to which backups may have been infected by the malware.

The Castlereagh Macquarie County Council incident response team will decide which option is preferable, based on the prevailing circumstances and priorities.

2.4 Recovery

Based on an assessment of the systems and data affected by the ransomware attack, the availability and completeness of backups must be established. This will include:

- The data covered by the backups
- Whether backups have been infected
- The reliability of the backups
- When the most recent backup was taken
- The business and technical implications of restoring from backup

If uninfected backups are available, the recommended approach is to completely restore all affected systems, hardware where necessary and application software and data from backup media.

Note – if backups are found to be incomplete, or the consequences of restoring from backup are felt to be unacceptable, then options 1 or 2 from section 2.3 above may be reconsidered.

Once the identity of the ransomware has been established, appropriate investigation must be conducted into the software vulnerabilities exploited by the specific malware involved. Available patches to address these vulnerabilities must then be installed to prevent recurrence. If no appropriate patches are available (for example if it was a zero-day attack), management must consider the best approach to protecting the organisation until the software vendor addresses the relevant vulnerabilities. This may include taking systems off-line temporarily.

2.5 Notification

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

Given that this type of attack may also involve the theft of data, the need to notify in compliance with regulations (such as the GDPR and Australian Privacy Act) must be carefully considered.

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES