Ransomware Protection

Advice on protecting your organisation against ransomware, how to manage backups, and potentially successfully recover from an attack.

Netscylla Cyber Security Ltd

Introduction

Ransomware is a type of malware (**Mal**icious soft**ware**) that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware that impacted the Global businesses in May 2017.

Normally you are asked to make a payment (often demanded in a cryptocurrency such as Bitcoin), in order to unlock your computer (or to access your data). However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files. Occasionally malware is presented as ransomware, but after the ransom is paid the files are not decrypted. This is known as wiper malware.

For these reasons, it's essential that you always have a recent offline backup of your most important files and data

Why ransomware works

In 2019 there were several report instances of ransomware affecting organisations in North America

- https://heimdalsecurity.com/blog/ransomware-payouts/
- https://www.itgovernance.co.uk/blog/the-5-biggest-ransomware-pay-outs-of-all-time
- https://safeatlast.co/blog/ransomware-statistics/

But its not just the Americans that are quick to pay-out. In 2017, the Korean web hosting firm Internet Nayana received the largest ransom demand ever (a whopping $1.14 million), which they also ended up paying. During their negotiations, some of their data was permanently deleted. To make up for the incident, Nayana offered free hosting for life and refunds to its affected customers.

Therefore, ransomware is a lucrative business model for criminal enterprises.

Finally consider that besides the actual payment, ransomware attacks involve additional costs (recovery, legal and compensation) and reputational damage against your brand.

Should the ransom be paid?

In Great Britain NCSC supports the National Crime Agency (NCA) recommendations. **The NCA generally advise not to pay the ransom**, as there is no guarantee that you will get access to your device (or data).

About this paper

Netscylla is a practitioner of red-teaming and phishing, and on occasion we perform simulated ransomware infections for organisations. We will cover some of the approaches that you can employee at an organisational level, that could help defend and ultimately recover from a ransomware attack.

Table of Contents

Preventing Ransomware

Prevent malicious code from entering your environment

You can reduce the likelihood of malicious content reaching your network through a combination of:

- filtering to only allow file types you would expect to receive;
- blocking websites that are known to be malicious;
- actively inspecting content;
- using signatures to block known malicious code.

These are typically done by network services rather than users' devices. Examples include:

- mail filtering (in combination with spam filtering) which can block malicious emails and remove executable attachments;
- intercepting/guard proxies, which block known-malicious websites;
- internet security gateways, which can inspect content in certain protocols (including some encrypted protocols) for known malware;
- safe browsing lists within your web browsers which can prevent access to sites known to be hosting malicious content. In addition to standard anti-virus and anti-malware protection.

Prevent malicious code from running on devices

A 'defence in depth' approach assumes that malware will reach your devices. You should therefore take steps to prevent malware from running. The steps required will vary for each device type and OS , but in general you should look to use device-level security features such as:

- Centrally manage enterprise devices in order to either:
    - only permit applications trusted by the enterprise to run on devices using technologies including AppLocker, or
    - only permit the running of applications from trusted app stores (or other trusted locations)
- Consider whether enterprise antivirus or anti-malware products are necessary, and keep the software (and its definition files) up to date.
- Provide security education and awareness training to your people;
- Disable or constrain macros in productivity suites, which means:
    - disabling (or constraining) other scripting environments (e.g. PowerShell)
    - disabling autorun for mounted media (prevent the use of removable media if it is not needed)
    - protect your systems from malicious Microsoft Office macros

In addition, attackers can force their code to execute by exploiting vulnerabilities in the device. Prevent this by keeping devices well-configured and up to date. We recommend that you:

- install security updates as soon as they become available in order to fix exploitable bugs in your products;
    - enable automatic updates for operating systems, applications, and firmware where possible.
- use the latest versions of operating systems and applications to take advantage of the latest security features;
- configure and harden host-based and network firewalls, disallowing inbound connections by default

Backups

We have summarised managing backups into three simple rules:

- 3-2-1;
- Offline;
- And Regular.

Through applying the guidance outlined in these rules, you should have an effective solution to cover the business against accidental data loss and potential malware/ransomware related attacks.

The 3-2-1 rule

Is critical data saved in multiple backup locations?

It is vital to keep multiple backups and to logically separate them. Maintaining resilient backups means that if one is compromised, at least one other remains. The most common method for creating resilient data backups is to follow the '3-2-1' rule:

- at least 3 copies;
- on 2 devices;
- and 1 offsite.

This strategy is popular because it scales effectively (including the use of the cloud for an offsite backup) and can give you confidence that your critical data is safe from a localised incident. However, it does not require any backup location to be offline – hence the need for our first offline rule.

The offline rule

At any given time, are one or more backups offline?

The purpose of an 'offline backup' (or a 'cold backup') is to remain unaffected should any incident impact your live environment. This rule has become a recent addition due to the nature of synchronising your backups in a 3rd-party or cloud-based environment. If ransomware has already compromised your system, it could have started encrypting your files, and these ransomed files could be syncing to your backup provider. It now more important than ever to keep an offline backup for sensitive or business critical data.

How to securely keep an offline backup?

You can do this by:

- only connecting the backup to live systems when absolutely necessary
- never having all backups connected (or 'hot') at the same time
- With at least one backup offline at any given time, an incident cannot affect all of your backups simultaneously.

Using cloud storage to hold an offline backup is a good idea because it guarantees physical separation from your live environment. However, unlike conventional backup storage, you cannot take your cloud storage offline by simply unplugging it and storing it in a secure place. Though there are a few steps that can be taken to apply the same level of protection.

Identity Access Management (IAM)

The first step to protect any cloud storage is to secure and uniquely identify all individual accounts. For cloud services this almost always appears as username and password credentials (or API and SECRET keys). All users/roles able to access cloud backups should be properly protected with appropriate permissions and policies. Without a trusted identity, ransomware should not be able to penetrate your cloud storage and start encrypting any cloud-based data.

Access Control Lists (ACLs)

Some cloud storage services offer more advanced access controls for identity and connectivity. If these controls are available, they should be configured to only allow authorised clients to create new versioned backups (or append to existing ones), and deny connection requests while the storage is not in use ('cold'). If a ransomware infection occurs while your cloud backup is offline (denying connection requests), it will not be able to reach the cloud storage, giving you the same level of confidence as unplugging an on-premises storage drive. In the event of a ransomware incident occurring whilst your cloud backup is connected, ransomware acting with limited privileges can only create new data, and cannot overwrite your existing backups!

Client management

A backup client is a device/service with credentials to access your cloud storage. Cloud backup clients should not have valid credentials while your cloud storage is not in use; what we mean here is that credentials or access keys should be rotated frequently or where possible after each synchronisation. The number of backup clients should also be kept to a minimum with standard user permissions, with limited or no privileges to modify cloud backups directly.

Following these practices, a ransomware infection can only compromise your cloud backup if it occurs on an authorised client and while your cloud backup is being used.

The regular rule

Is critical data backed up regularly?

Finally, backups should be created on a regular basis. The more frequently backups are created, the less data you are forced to recover. Not only should your backups be created frequently, they should also be regularly tested to check they work as expected.

Recovery

The recovery rule

Have you actually tested your recovery capabilities? Are you confident that whether through accidental data loss, or a malware/ransomware attack that you can restore lost data or business critical functions?

While all measures can be used to try and prevent a security incident from affecting your backups, it is best to have a backup plan for your backups.

Are your on-premise backups restorable and recoverable?

Netscylla has witnessed several issues with client's on-premise backup solutions. Problems have arisen in the following forms:

- Network backup & storage are additionally infected with ransomware;
- Storage devices become full & stop recording recent backups (last good state may be several years old?);
- Backup & recovery has never actually tested, resulting in:
    - Failed recovery
    - Additional time & resources required to restore business critical functions

Netscylla recommends that backup and recovery solutions should be assessed annually to ensure that the business' restore procedures are accurate, up-to-date and easily actionable.

Is the data in cloud backups restorable and recoverable?

While the on-premise concerns are equally applicable to the cloud, cloud infrastructure may have some extra perks.

Some cloud storage services allow you to restore modified data back to an older version, and recover deleted data for a limited time after it was deleted (It is best to confirm this in writing with your provider, rather than assuming this is the case, different platforms and services have different backup and recovery routines). If ransomware does manage to affect your cloud backup, you can potentially use these features to restore back to a last known-good state.

Conclusion

Netscylla have highlighted *Prevention, Backup and Recovery* techniques against ransomware attacks. Hopefully, your organisation has already got some or most of these defensive measures in place, we recommend that you test your security and recovery functions at a minimum annually, so that you can rest assured that your business can resist or restore from an unfortunate targeted ransomware attack.