A GUIDE FOR RANSOMWARE PREVENTION - FIVE LAYERS OF DEFENCE

The purpose of this paper is to help with a strategy to mitigate ransomware risk.

This guide will firstly explain how the criminal profits of ransomware attacks have created an ecosystem that means this threat is not going away. It will then take you through five layers of defence that you should have lined up against this threat. You will have many of them in place already, but you must get the configuration and execution right. Getting some independent assurance that your defence is working as designed is crucial.

THE RANSOMWARE ECOSYSTEM

It is no longer necessary to explain to people what ransomware is, as a series of high-profile attacks have been newsworthy. The global value to criminals is counted in billions of dollars and has resulted in a thriving ecosystem that keeps it developing one step ahead of the defences. There is a market on the dark web where cybercriminals can sell access to compromised companies or wealthy individuals.

The cybercriminal has found an initial access point (for example, they have placed malware on a computer) and used that access to establish what kind of a target they have hooked. A bigger gang will buy that lead and exploit it by expanding the compromise, stealing documents, and locking up systems. They will use platforms, processes, and software that is developed by big ransomware operators who host services on the dark web.

The approach is three-fold:

- There is a large pool of individual hackers who are continually looking for opportunities to find a victim.
- The tools they are using are continuously being improved and are designed to work at large scale, i.e. ransomware as a service.
- Their target is initially a vulnerability, i.e., they are not after you, they are scanning the business world for an unguarded opening.

The answer to this ongoing threat is to get strength in depth and to test your defences against the latest attacks.

There are five layers of defence that we recommend you invest some time and resources into.

LAYER ONE - THE ATTACK SURFACE

The first job is to 'harden' your internet-facing technology against attack. The initial access/compromise will typically come from one of the following places:

1. Remote Laptop
2. Office desktop
3. Firewall
4. Exposed services
5. Supply chain
6. Hosted service
7. Cloud platform
8. Email system
9. Website

It is a good idea to list all the items in your attack surface (including, but not limited to, the above list) and then:

i. Work out who is accountable for keeping them secure and ask yourself if they have the skillset/knowledge.
ii. Do you have any other controls that are protecting technology? AV, VPN, etc. How do you know that they are working effectively and who is watching the alerts.
iii. What assurance and testing are you getting that (i) & (ii) are lined up properly against the current methods of attack?

iv. And finally, are you training and testing your staff and member competence? Most compromises rely on a human falling for a criminal's trick.

LAYER TWO - LIMIT ACCESS AND PERMISSIONS

In almost all scenarios the criminal has taken over someone's profile. They only have control and access to what that individual has access to and system permissions for.

The work in this layer is to limit the amount of control that the criminal can achieve from any compromised user.

Here is your to-do list:

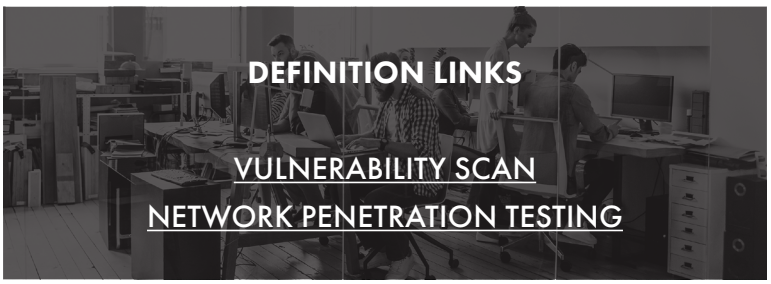
- **Passwords.** These need to be strong and unique. The most important ones should only be in a password manager.
- **Authentication.** The most important systems and services should have an additional layer of authentication after the password.
- **Conditional access.** Consider restricting access by geography, location, and device. This is most appropriate for users connecting remotely to systems and for access to email systems.
- **Access management & permissions.** These should be at the lowest levels required for any role. Administrators of systems should have a separate profile for their day-to-day activity.
- **Syncing.** Google and Apple accounts love to help you by syncing passwords to all the users' devices. This needs to be controlled, especially for senior staff.

If you get this right, the impact of an attack could be confined to a single device rather than the whole organisation. You may want to consider stand-alone assessments of this area that will give you a gap analysis to work on.

LAYER THREE - STOP THEM MOVING HORIZONTALLY

OK, so the criminal has got a foothold in the technology and taken over the identity of a user. They will now use hacking tools and techniques to get to other devices, servers, data stores, etc. They will be trying to get domain credentials, switch off your AV, create back-doors, find documents, extract data, encrypt data and look for back up stores. Most companies have never configured the defences and alerts that are essential to stop this lateral movement.

Here is your to do list for this. You need a vulnerability scan, network penetration test and configuration advice. This one is a job for a cybersecurity company but doesn't need to cost the earth. It should be proportionate to your size and risk.



LAYER FOUR - BACK-UPS AND DATA LOSS PREVENTION

If layers 1 to 3 aren't properly in place you will find yourself with encrypted data and systems. And in most situations your data will be stolen by the criminals to give them a second chance at extortion. When the ransom demand lands, you will have a lot more confidence in your position if your back-up has worked and you have enabled some data loss prevention policies (DLP).

Things to consider on your back-ups:

1. **Location** – who manages the back-up service for you, how do you retrieve it and how long should it take.
2. **Separation** – how is the back-up separated from your live systems? In many situations the back-up ends up being a copy of the encrypted documents.

3. **Alerting** – most back-up services have anti-ransomware configuration and alerting. Does yours have this and has anyone configured it?
4. **Coverage** – as technology develops, so does the spread of where documents are held. Are you confident your back-up captures all your documents.
5. **Completeness** – imagine trying to complete a jigsaw puzzle without the picture on the lid. The back-up needs to be a picture of the whole system, not just the documents. Otherwise, you could be down for weeks.

Many of your systems may have DLPs that can be configured. These can prevent mass download of documents or at least let you know what has been taken. We have seen scenarios where the criminals have not actually taken anything despite claiming they had. Make sure you have correctly configured your case management system, Office 365 and firewall.

LAYER FIVE - INCIDENT RESPONSE PLAN

Many of the ransomware attacks we have been called in to deal with would have been mitigated by a swift and effective incident response plan. The moment you realise an attack is underway is the moment you need to be able to follow a rehearsed process and not be scrambling around just to get in contact with someone.

This is a large topic but here are six actions to get you started:

1. Discuss the subject with a representative set of employees/members and allocate some accountabilities.
2. Make sure you know how to get hold of the right help quickly in an incident and make sure that the contact list is kept up to date.
3. Do an exercise to step through a ransom scenario. This will help you create a list of actions to progress.
4. Make sure your staff know their roles in an incident. This may be as simple as knowing who to alert and how to disconnect their computer from the network/Wi-Fi/internet.
5. Think about communication plans. Who is accountable for making sure the appropriate people are informed.
6. Consider a ransom payment policy or decision process.

SUMMARY

Ransomware is not going away, as you can see from the regular news headlines. It is driven by a thriving criminal ecosystem that morphs and develops to get around new controls that businesses apply.

The best way to stay secure is to work on these layers of defence and get some independent third party assurance.

WWW.MITIGOGROUP.COM