Ransomware Resilience

Tip Sheet

2022 and 2023 saw some of the largest ransomware attacks ever seen in Australia including Optus, Medibank, Latitude Finance and more. In the first half of 2023, ransomware accounted for 30% of all data breaches reported to the OAIC, with 1 cyber crime being reported every 7 minutes.

Is your organisation prepared for a ransomware attack?

Here's some practical things you should be focusing on:

Keep your incident response plans updated

Ransomware is different from most other crisis situations so including a scenario for this in your incident response plans will make a huge difference in knowing what to do rather than being caught in blind panic. You should include a ransomware table top exercise as part of these plans.

Build a strong cyber security awareness culture

74%[1] of all data breaches involve the human element, therefore educating everyone in your organisation about cyber security and the threats to be aware of is vitality important. This needs to be done regularly, not just a one off event. Regular monthly phishing simulation tests and educating people on things such as social engineering will reduce risk significantly.

Patching and vulnerability management

Cyber criminals are acting on vulnerabilities within hours of them becoming publicly known and ransomware gangs in particular are taking advantage of targeted victim systems within as little as 48 hours[2]. It is therefore imperative that patching and vulnerability management keeps pace with these threats.

Endpoint detection and response (EDR)

Every system in your organisation, including desktops and servers, should be running a next generation endpoint protection and response solution. This should be capable of isolating the system to limit further damage and impact in the event of a critical situation such as a ransomware event.

Strong authentication and passwords

49%[3] of all breaches that occurred in 2022 involved the use of stolen credentials. Humans make bad choices when it comes to choosing passwords. So in conjunction with a robust organisation password policy, make sure you are enforcing the use of strong passwords combined with MFA where possible on all systems.

Privileged access management

Administrators of systems in your IT infrastructure should use dedicated admin workstations for performing all administrative tasks. Admin credentials should only be used for privileged tasks and not for every day use. They should be stored in a secure vault and rotated regularly (at least weekly, but ideally after every use).

Proactive monitoring and logging

Log, Log, Log as much as you can! This means all key business applications, operating systems, network devices, firewalls, key infrastructure and end user compute systems. If you operate purely in the cloud or have a hybrid setup then logging is essential.

Network security

Use a network detection and response system to collect and analyse network traffic for unusual patterns of behaviour. If this is not possible then collecting logs from key network systems (firewalls, network devices etc) and sending them to a centralised SIEM will be your next best option.

Remote working

Make sure that everyone who works remotely uses an always on VPN when accessing your organisation's network. Authentication should incorporate MFA and ideally an MFA solution that incorporates anti-phishing defences.

Backups

Your organisation's backup solution should have redundancy built in to the design. Recovery tests should be run regularly to ensure the integrity of the data, and ease of access / recovery drills for all key systems should be run at least once a quarter.

[1] 2023 Verizon DBIR, [2] Dark Reading July 2023, [3] OAIC NDBR Jan - Jun 2023 report

"74% of Australians feel data breaches are one of the biggest privacy risks they face today" source: OAIC ACAPS survey 2023

What should you do if you become a victim of ransomware?

01 Invoke your incident response plan for ransomware

- Gather your incident response team and executive crisis management team into a war room
- Declare a ransomware event
- Assume a zero trust approach and follow predefined alternative communications

02 Containment

Contain the threat and if necessary disconnect:

- All affected devices
- All key business systems holding sensitive data
- Internal network connections and the internet

03 Notification and communications

- Notify the OAIC, ACSC and other regulators if required *
- Notifiy all key clients that may have been affected *
- Prepare a formal statement and follow your organisation's communication plan

* seek legal advice

04 Incident response

- Gather your incident response team
- Call an expert incident response company to establish how the incident occurred and to start negotiations with the ransomware criminals