Emergency Response Toolkit:

HOW TO RESPOND TO A RANSOMWARE ATTACK IN 12 STEPS

Organisations should assume that sooner or later they will be confronted with a ransomware attack. The main question is when. Preparation is key.

This is a guide about urgent actions to take when a ransomware has hit your company.

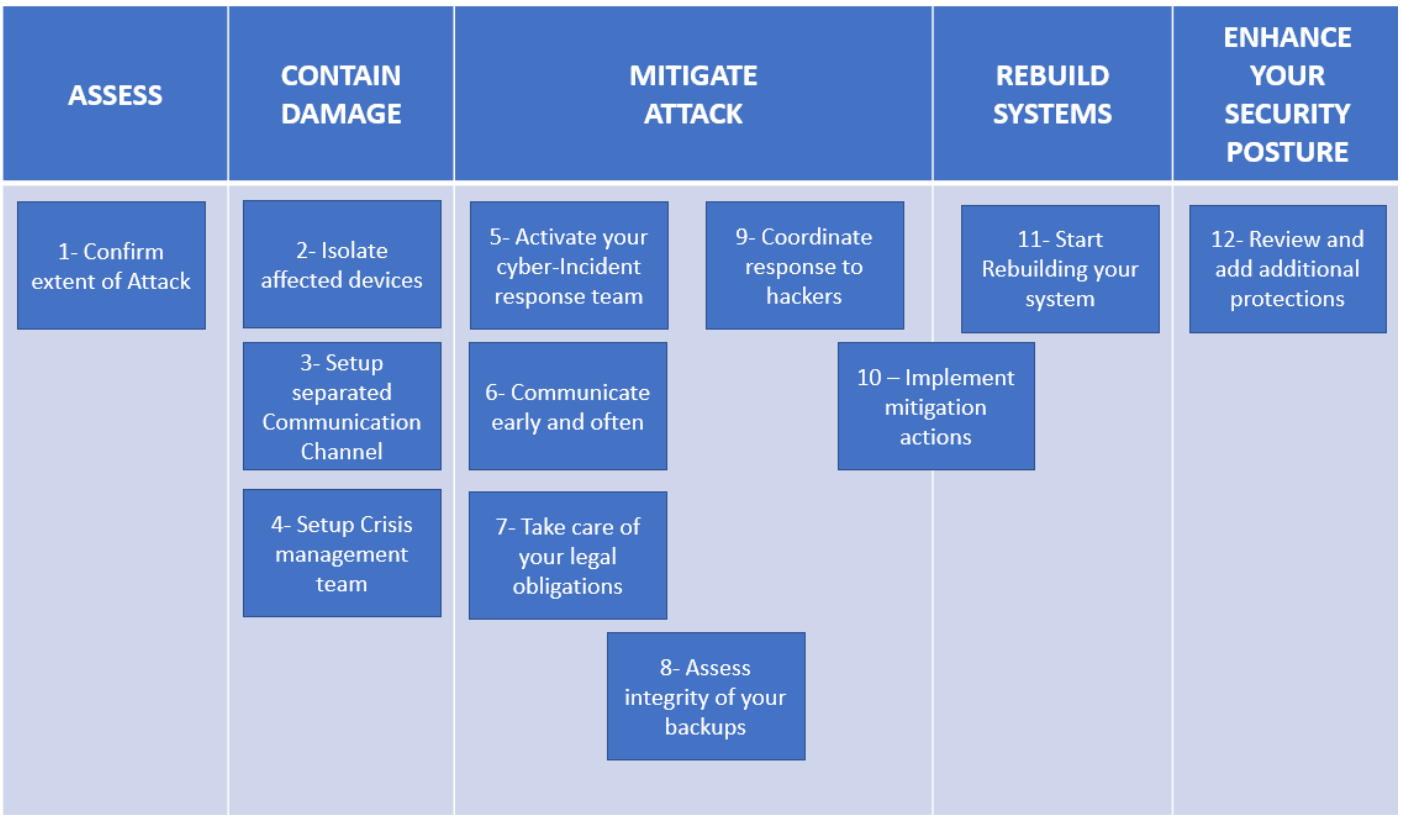
Preparation is key whenever dealing with a ransomware attack. The primary goal is to make sure organisations are prepared and don't need to improvise once a disaster strikes, which will cause additional mistakes that may result in losing even more data.

Preparation includes making sure which teams you need (technical, crisis, communications, …) and how these people can be efficiently reached. While preparing (i.e. your playbook is available, you have put it to the test with an exercise), make sure this also includes a process to keep everything up-to-date.

The steps outlined below are the minimum ones that you will need to follow in case of a ransomware attack, hopefully by applying your disaster recovery plans, if not done so we hope the guidelines below will highlight the important action items.

Recover from a ransomware attack is not done in a few hours and will take typically weeks or months. However, taking actions in the hours following a confirmed attack are crucial.

Visual High level steps



1. Determine and confirm the extent of the Ransomware attack

Rebuilding systems is NOT the first step in your response plan.

Assess the extent of the ransomware attack by focusing on what has been encrypted and/or potentially exfiltrated. Providing an answer to this question is critical to activate a response plan.

This response plan will also provide useful insights on internal and external questions your leadership, employees and the clients might have.

Setting up a response plan is hard if you don't know the extent of the attack. Try to document what data was on the encrypted machines and look for data that may have been exfiltrated.

2. Isolate affected devices

Isolate affected devices as much as possible to prevent any further spread.

When ransomware strikes, it's essential to isolate affected devices as much as possible to prevent any further spread. Assume attackers are already well-embedded in your environment by the time the ransomware attack is performed, so acting fast to contain the impact will be key.

Start by isolating the infected devices and removing them from the network. Plug network cables out, stop network connections (including WiFi-networks).

If your network permits it and is properly segmented, you can also disconnect the infected network segment.

- **Do NOT turn OFF the infected devices, avoid shutting down systems**. There still might be malware installed that is not activated. Having a running system might also help when seeking help from an incident response firm to conduct detailed investigations.
- **Do not start recovery operations as long as the extent of the attack is not known**, this includes the method, time, impacted systems.

3. Set up a separated communication channel

Assume your business communication tools (if still functional) are compromised.

Sensitive communications on the evolution of the incident should be done on a separated and secured channel. Assume your mail systems (if still functional) are also breached and that the attacker has access to those, which means that communication on your network should be limited to the strict minimum. Analyse which systems might be used to communicate internally and externally. Set up a secure communication channel with your technical team, leadership team.

Setting up f.i. Signal or temporary using an external conferencing system (Secure communication tool) and creating separated groups is advisable. You might want to set up a group with the technical managers, a group containing communications responsible and a group towards leadership. Half of the work in dealing with a ransomware incident will be about coordination and communication.

4. Set up a crisis management team

The crisis management team will coordinate all activities required to return your IT systems to an operational state but will also handle business, IT priorities, communication, legal aspects.

Set up a crisis management team (sometimes called business continuity team) that will agree upon business priorities, communication strategy, legal questions and help in resolving prioritisation conflicts when restoring business functions will need to be addressed.

This team should coordinate all internal and external communications, ensuring "one voice" is available during the crisis.

The Crisis management team should include the main business stakeholders, your DPO, communications, legal and an IT representative.

Appoint a crisis manager that will act as the liaison with your technical team(s) and the crisis management team.

Depending on the size of the organisation you might consider having two Crisis management teams, one for the business aspects and one for the operational IT aspects (the last one reporting directly towards the business crisis management).

5. Activate your cyber incident response team

Seek professional assistance from cyber specialists like forensic experts, who can help determine how the incident occurred and prevent a recurrence.

Check if incident response is part of your insurance contract.

Check if you have internal expertise, otherwise hire a professional incident response team to help you in assessing the initial attack vector and the entry point and allow proper mitigation.

6. Communicate early and often

Communicate early and often, keep your internal employees, suppliers, service providers and your customers updated. Hiding this attack is generally speaking not a good idea as it can damage your brand's reputation.

Be as transparent as possible towards your employees, stakeholders, customers or users, and the press about the attack. Even if you don't have all the answers, it's important to inform all your stakeholders. More information: https://www.cert.be/en/crisis-communication-event-cyber-attack.

When your communication systems are unavailable please consider temporary solutions like setting up a communication webpage, SMS-based mass notification systems.

7. Take care of your legal obligations

Ransomware actors are not only interested in you paying the ransom to decrypt the systems but have also often exfiltrated data and will threaten to sell them or make them publicly available if you don't pay.

There are legal obligations as notifying authorities like the DPA/GBA/APD in case of suspicion of data breaches (typically whining 72 hours). https://www.gegevensbeschermingsautoriteit.be/burger/acties/contact (Website in NL and FR available). Involve your Data Protection Officer (DPO).

The legal team and/or DPO can also file a complaint at the local police.

8. Assess the integrity of your backups

Verify that the attackers have not also compromised the security and the integrity of your backup system.

If the backup system is secure which means you have an independent and verified copy of your data, avoiding ransomware payment is the recommended and best option. Therefore you should have confirmation that the backups have not been compromised or accessed (immutable backups are a must).

9. Coordinate your response to the hackers

As a principle you should NOT pay any ransom to criminal organisations.

The Centre for Cybersecurity Belgium (CCB) strongly discourages the payment of a ransom. There might be situations in which payment is the only remaining option, but please bear in mind that the attackers are very likely interested in financial gain so all opportunities to extort you more money will be evaluated by those actors.

Be careful when interacting with the attacker, hiring a professional negotiator is not a silver bullet. There are many cases known of ransom amounts which were doubled after a negotiator was hired and always remember that there is no guarantee the decryption keys will be received.

10. Implement mitigation actions

Implement (minimal) security monitoring services (SOC service), activate an Endpoint Detection. Patch, reset, update known vulnerable systems touched by the attack. Implement Multi-Factor Authentication.

Do not open Internet connectivity for all users, focus first on the users required to restore your IT operations of your crisis management functions.

Patch, reset, update known vulnerable systems touched by the attack. Perform a full reset of all passwords and implement, if not done so, Multi-Factor Authentication. Focus first on Privileged accounts and services (Admin accounts, Admin services).

Implement security monitoring services (SOC service), activate an Endpoint Detection solution of the critical systems like the Authentication, Authorization systems, the systems that are Internet-Facing. The point is that you want to have (better) visibility on activities that are happening on your network.

11. Start rebuilding your systems

Patch, Update, rebuild and reset your authentication system, implement Multi-Factor Authentication

Do not restore a system based on backups close to or after the attack.

Act on the previous points first and then, only then, start activities as to rebuild your system from backups.

Take care not to re-infect clean systems during recovery. Once the system is restored, be sure to check it so that nothing malicious is left on it before adding it back again into your network. Rebuilt your systems based on a prioritisation of critical services, restore servers first then endpoints. It is also recommended to keep a copy of your encrypted data, a free decryption tool for your ransomware strain might become available in the future.

Remove or completely isolate legacy systems and protocols.

12. Review and add additional protections to prevent a future attack

While the focus will be on remediating the attack and rebuilding the infrastructure, company leadership need to be aware that it is possible to be attacked again.

Take time to analyse and document the attack into detail, put new controls, processes, procedures and solutions in place to prevent a subsequent attack.

Webinar available in Dutch and French: https://www.youtube.com/watch?v=r0Iraugn-wo

CERT.be ransomware brochure available in Dutch and French.

Contact

Centre for Cybersecurity Belgium
Rue de la Loi, 16/ Wetstraat 16
1000 Bruxelles/ Brussel
info@ccb.belgium.be

Disclaimer

Responsible editor

Centre for Cybersecurity Belgium
Mr. De Bruycker, Director
Rue de la Loi, 16
1000 Brussels