Ransomware pocket guide

Definition Malware which encrypts data and demands a "ransom" for its decryption (blackmail Trojan Horse virus).

Function Ransomware does not just encrypt files on the infected computer, but also anything that can be accessed via the network, such as directories or even entire data carriers. A demand is then sent to the user to pay a ransom. Only by doing so will the user receive the key to decrypt the data. The virus is commonly spread via spam e-mails and "drive-by infection".

Effects The affected data can no longer be read.

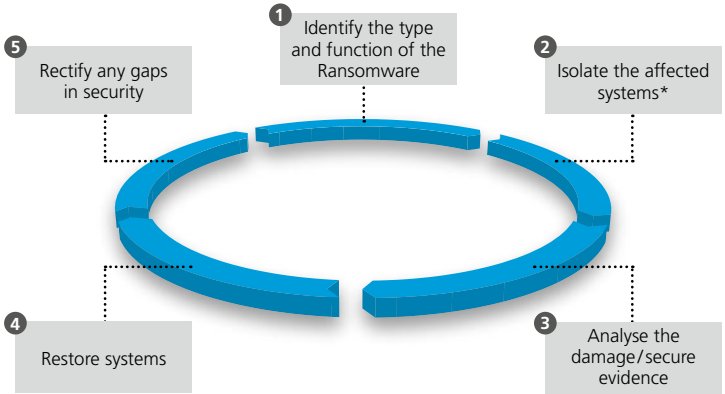
Tips on how to protect yourself against Ransomware

1. **Preventing infection** – Keep anti-virus scanners and spam and Internet filters up to date, be more restrictive in issuing access rights and raise awareness among users.
2. **Curtailing the distribution of the virus** – Isolate any systems affected, block any users affected and segment the network.
3. **Reduce damage** – Regularly create back-ups, store data in a decentralised location and, where possible, redundant, and establish manual emergency processes.
4. **Share information** – Inform law enforcement authorities, provide notifications to MELANI, customers and suppliers, and inform other companies in the industry.
5. **Do not play into the hands of criminals** – Do not pay the ransom wherever possible.

5 principles for creating back-ups

- **Redundancy** – Keep several back-ups at physically separate locations.
- **Planning** – Carry out at least one full back-up per month as well as a daily back-up of any changed data.
- **Data storage** – Keep back-ups as long as possible – at least for a year.
- **Integrity** – Ensure and regularly check the integrity of the back-ups.
- **Confidentiality** – Store back-ups securely. Never keep back-ups on the network permanently.

Procedure in the event of a Ransomware attack



* Where possible. Otherwise, restrict access.