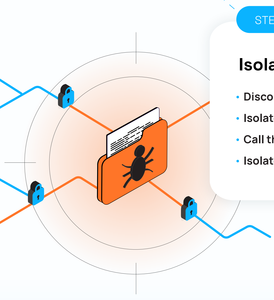
Ransomware attack
Respond in 5 steps

STEP #1

Identify the attack

- Your IT systems **aren't responding** or are acting strangely
- A large number of your **files are changing**
- A **ReadMe document** pops up

What (absolutely) not to do
Never contact the attacker directly to start negotiating.



STEP #2

Isolate and contain the attack

- **Disconnect the IT** from the Internet
- **Isolate** the parts of the network that have been infected
- **Call the internal CERT** or contact an external CERT
- **Isolate your backups** to prevent them from being infected

STEP #3

Get organised to respond to the incident

Activate a crisis management unit

- **Implement your crisis management protocol** (organisation, resources, processes)
- If no plans have been made, **gather the decision-makers** and set up the procedure
- Check that your **BIA is up to date** so you can plan the steps to get your IT back to normal

Tip
Keeping this procedure in a safe place and developing it in advance can save time.

Remediate

If there is a CERT, **exchange** and provide information on how to eradicate the incident.

Tip
The Advens CERT's incident response sheets can help you to follow the best practices.

Freely available on our website!

Initiate crisis communications

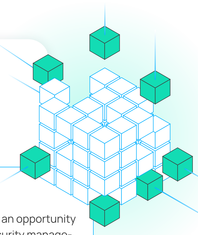
- **Inform** your internal teams and give instructions
- **Reassure and communicate** immediately with your ecosystem
- Anticipate future **media** requests

Tip
Depending on the applicable laws, you may be required to report the attack to the **relevant authorities**.

STEP #4

Recover and rebuild your IT

- Recover and rebuild the critical elements of your IT **securely**
- **Strengthen** the other parts of the information system



Tip
This step provides an opportunity to update your security management procedures (administration access control, etc.).

STEP #5

Finalise and determine when the crisis is over

- Make the return to normal **"official"**
- **Maintain** the tools and measures put in place (e.g. EDR)
- Arrange an internal **post-mortem**
- Ensure you have the resources (time, money, energy) to **finalise the security plan**

It has become essential to protect yourself to avoid the risk of cyber attacks.

The Advens CERT has published incident response sheets to use in the event of an incident.

Find them on GitHub!
github.com/cert-advens/IRM

By inwox