CENTER FOR CYBERSIKKERHED

HOW TO PROTECT YOURSELF AGAINST DESTRUCTIVE CYBER ATTACKS

In light of the present threat level for destructive cyber attacks, CFCS recommends that private companies as well as public authorities revisit their current cyber security measures. If the situation changes and the threat of destructive cyber attacks becomes more pronounced, it might prove too late to start developing precautionary measures. The following are three areas that require particular attention:

1. Prevent attacks

- Ensure that all internet-facing systems and services are patched.
- Protect all remote access connections with multi-factor authentication (MFA).
- Ensure that employee devices and software are patched.
- Use strong passwords and avoid recycling them.
- Ensure data and critical systems are protected with offline backups and verified through recovery testing.
- Regularly update incident response plans and conduct periodic testing to ensure their effectiveness.

2. Detect attacks

Implement comprehensive logging for all internet-facing and critical internal infrastructure systems and services. Proactively monitor logs and look for possible signs of wiper malware attacks, such as:

- Alerts from security products (antivirus, firewall, IDS etc.).
- Unauthorised creation of new privileged user accounts.
- Group policy changes.
- Creation of new scheduled tasks.
- Deletion of shadow copies or of local log files.
- Abnormal file activity, including bulk deletion, overwriting and renaming of files.

3. Mitigate attacks

If an ongoing destructive cyber attack is detected (e.g. a wiper malware attack), mitigation should be carried out in a structured manner:

- Isolate infected devices and systems from the rest of the network.
- Activate the crisis response plan if necessary.
- Seek external assistance if required.
- Prioritise identification and mitigation of exploited vulnerabilities before back-up recovery in order to avoid reinfection.

For additional inspiration and advice, see CFCS guidelines at https://www.cfcs.dk and the technical minimum requirements for government authorities at https://www.sikkerdigital.dk

For more information on logging, see CFCS' guideline "Logging – part of resilient cyber defence" at https://www.cfcs.dk/logning

The CFCS situational centre can be contacted at all hours at tel. 3332 5580 or by email at cert@cert.cfcs.dk.