TLP:CLEAR

CENTRE FOR CYBERSECURITY BELGIUM

Incident Handling:
From Chaos to Control

Cyber Tips Webinar – 19 June 2025

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Getting the CERT team involved

CENTRE FOR CYBERSECURITY BELGIUM

More than incident response

- Expert advice
- Help coordinating incidents

Need help?
https://www.youtube.com/watch?v=FMr48xXJeTw

How to get CERT involved

- Reporting form: https://ccb.belgium.be/cert/report-incident
- Priority given to NIS2 entities
- Conditions: https://ccb.belgium.be/cert/incident-handling-cert-general-conditions

Common incident types

CENTRE FOR CYBERSECURITY BELGIUM

Ransomware

Single endpoint, virtual infrastructure, servers & endpoints

Business email compromise

Edge device compromise

VPN, web server, RDP,…

Azure tenant takeover

Infostealer

Cryptominer

Ask yourself the right questions

- **On which system(s) was it detected?**
- **How** did it get there?
- Was it **blocked** by the antivirus?
- **What stage** of an intrusion could this be?
- Examples
  - Successful login blocked by MFA → it doesn't stop here
  - Antivirus alert on a domain controller
  - A webservice crash on a VPN appliance

Learn from incidents

- An incident response does not stop with system recovery
- **Lessons learned**:
  - Appropriate protection?
  - Appropriate monitoring and logging?
  - Appropriate patching?
- Brainstorming, **open discussions**
- Not a blaming exercise

Check out all 4 levels
https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

Detection on a budget

CENTRE FOR CYBERSECURITY BELGIUM

Check your licenses, you might already have some tooling available (e.g. Defender in Azure)

IDS

Security Onion

Log analysis

graylog

elasticsearch + logstash + kibana

Firewall

10 YEAR

OPNsense®

Securing networks made easy

EDR, CIS compliance

wazuh.

AD audit

PING CASTLE BY netwrix

Forensics

Eric Zimmerman's TOOLS

5 measures that may save you

CENTRE FOR CYBERSECURITY BELGIUM

- **Multifactor authentication**
- **Backup** rule 3-2-1-1-(0)
- **Monitoring and detection** (EDR, logs, …)
- **Patching** quickly
- Principle of **least privilege**

3 key preparation measures

CENTRE FOR CYBERSECURITY BELGIUM

Preparing for incidents is not a waste of time!

- Out of band communication channels
- Know who has the right privileges to perform certain actions
- Print out and distribute playbooks and procedures

You can find a lot of **template playbooks** on GitHub! Search for « IR playbooks »
Always adapt template playbooks and procedures to your own organisation!

MFA for admin accounts

- **Hybrid** environment:
  - Entra ID + MFA + FIDO
- **On prem environment**:
  - Yubikey + software solution
- **Next level**:
  - PAM Solution + JIT (just in time) + approval + RBAC + Least Privilege (Cyber Ark, ...)

Source: www.yubico.com

Upcoming Webinars

Quarterly Cyber Threat Report (QCTR) event

- 10 July 2025 – 2.00-4.00 PM CEST

Cyber Tips : protecting against DDoS attacks

- 9 September 2025

Did you know…

…that we have interesting vacancies?

Scan the QR code and discover our job offers for you.

CENTRE FOR CYBERSECURITY BELGIUM

Questions?

Ask away in the Q&A section!

Further questions and feedback can be sent to info@ccb.belgium.be

CENTRE FOR CYBERSECURITY BELGIUM

Technical annex

Ransomware – Single endpoint

- **How does it happen?**
  - Usually through a malware infection:
    - No proper filtering on email attachments
    - Local admin of their device
    - Vulnerable exposed server
- **How to respond?**
  - Isolate the compromised endpoint
  - Confirm the infection vector
    - Possible lateral movement?
  - Wipe and rebuild

Ransomware – Virtual infrastructure

- **How does it happen?**
  - Usually through an edge device connection:
    - Compromised device
    - VPN without MFA
    - Supplier / satellite compromise
  - Often takes place outside business hours
- **How to respond?**
  - Isolate the environment
  - Confirm the infection vector
    - Possible lateral movement?
  - Wipe and rebuild virtual infrastructure
  - Restore from backups
    - Attackers often delete backups first!

Ransomware – Servers and endpoints

- **How does it happen?**
  - Usually through an edge device connection:
    - Compromised device
    - VPN without MFA
    - Supplier / satellite compromise
  - Often takes place outside business hours (Friday nights)
- **What does an attacker do once in my systems?**
  - Privilege escalation, lateral movement until domain admin obtained
  - Spread via PowerShell, WMI, GPOs, …
  - Often data exfiltration will occur first (double extortion) followed by backup deletion

- **How to respond?**
  - Isolate the environment
  - Confirm the infection vector
  - Wipe and rebuild or restore
  - Find the spreading mechanism and remove it
  - Get help if needed!

Ransomware - Tips

- There is little incident response can do if your systems are encrypted
- We **don’t** do negotiation
- We never encourage organisations to pay the ransom but we won’t scold you if you do
- Don’t hesitate to get help!
- **What you should do in case of a ransomware**
  - Always file a complaint to the local **police**
  - Try to identify if personally identifiable data was exfiltrated (**GDPR** obligation)
  - Identify vector, **plug the hole** and **update your procedures**
- **Words of advice**
  - **Backups** ! 3-2-1-1-0 principle
  - Take the opportunity to **get rid of, or upgrade, legacy systems**!
  - Decryptors can be released years after. You might want to keep encrypted data on the side if you can wait.

Business email compromise

- **How does it happen?**
  - Usually through phishing or an infostealer:
    - No MFA or MFA fatigue
    - Password reuse
    - Session token hijack
- **How to respond?**
  - Check for persistence: have new mailbox rules been created?
  - Reset passwords and revoke tokens
  - Install MFA on **all** accounts
  - Conditional access (geoblocking, risky sign-ins,…)

Edge device compromise

- **How does it happen?**
  - Usually through a vulnerability:
    - Unpatched vulnerability or zero-day
    - Legacy systems
    - Misconfigurations
- **What does an attacker do once in my systems?**
  - Lateral movement: user credentials, pass the hash, bruteforce, password spraying
  - Privilege escalation and dump lsass to eventually becoming domain admin --> full Active Directory compromise
  - Establish persistence (C2, new user, scheduled task,…)
  - Data exfiltration, access emails, ransomware

- **How to respond?**
  - Will vary depending on the case
  - Isolate the compromised endpoints
  - Confirm the infection vector
    - Possible lateral movement?
  - Hunt with discovered elements
  - Eradication
  - Remediate: Wipe and rebuild or restore
  - Lessons Learned

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be