24 Feb 2022 -08:38

Impact of Ukraine conflict on cyber threat in Belgium

Many companies and organisations are concerned about the ongoing tensions in Eastern Europe and are wondering how to protect themselves in the event of a cyber attack. The Centre for Cybersecurity Belgium (CCB) can reassure them to some extent: for the time being, there is no objective evidence of a concrete cyber threat to our country. However, a cyber attack with consequences for Belgian organisations can never be excluded.

In the past, some digital attacks have already had repercussions in Belgium, such as NotPetya in 2017. This attack initially targeted a Ukrainian government service but quickly spread to the business community and was felt as far away as the port of Rotterdam and some Belgian companies.

Building and strengthening cyber resilience

Building cyber resilience remains the best security for organisations and businesses in all circumstances.

Some basic principles for good cyber resilience

- We recommend that companies and organisations develop, update and regularly test a (cyber) contingency plan. It is important that every employee knows what his or her task is in the event of a cyber incident (see the Cybersecurity webinars in FR - NL).
- Keep your contact lists up to date, and keep them on paper as well.
- If necessary, ask for assistance from an external partner/company. Establish agreements in advance.
- Make sure your systems are up to date and always have a proper management of your backups.

For a complete overview of security measures, see the cyber guide: https://cyberguide.ccb.belgium.be/en.

The CCB is closely monitoring the situation and will publish specific advice as soon as this proves necessary.

Centre for Cyber Security Belgium
Rue de la Loi 18
1000 Brussels
Belgium
http://www.ccb.belgium.be

Katrien Eggers
Communications officer
+32 485 76 53 36
katrien.eggers@cert.be