SEKTOR CERT

Threat Assessment

4th of April 2024

TLP:CLEAR

Introduction

SektorCERT is the Danish cyber security centre for critical infrastructure.

SektorCERT continuously monitors the cyber threat to the Danish critical sectors and keeps the sectors informed about the current threat level and recommendations for action.

SektorCERT's assessment is made on a 5-step scale, which is based on an international standard. The scale goes from green as the lowest level (normal threat picture) to red as the highest.

The overall assessment of the threat level consists of this threat assessment and the Handbook on SektorCERT Threat Assessments.

This threat assessment

The threat assessment provides both the background to the assessment and recommendations on which technical and organisational measures each actor should focus on validating the effectiveness of. The technical and organisational measures are selected based on the specific cyber threat.

The threat assessment can be found on the next page, while the measures listed are described in the Handbook on SektorCERT Threat Assessments.

Threat Assessment Handbook

The handbook is an important element in the organization's overall assessment of actions that should be taken. It lists additional actions that are relevant depending on the specific threat level.

The numbers on the opposite site, all refer to the 25 recommendations listed in the Handbook on SektorCERT Threat Assessments.

The handbook can be downloaded from SektorForum or from the SektorCERT website.

Publication of threat levels

When SektorCERT changes the threat level, it will be announced via SektorForum and the SektorCERT website.

SEKTOR CERT

Threat assessment

The threat assessment of the 4th of April 2024 remains BLUE

The following represents the reasoning behind the assessment:

- There is a general risk of serious hacking activity, malware or other malicious activity.
- There is a potential for malicious cyber activities, but SektorCERT does not see cyber activities among its members that can be expected to impact critical infrastructure.
- SektorCERT observes in the sensor network and in reports in the media and from partners that there is generally still ongoing activity aimed at identifying and exploiting vulnerable systems - both globally and in Denmark. This activity does not target the critical sectors specifically, but organisations within these sectors can be targeted by opportunistic attackers and should continuously work to secure their infrastructure and employees.
- In week 12, a member (operating with water and wastewater) of SektorCERT was hit by a ransomware attack. The attack only affected the member's administration. So far, SektorCERT is aware of 3 ransomware attacks against companies in the water sector within Europe's borders in 2024. None of these attacks have affected the OT-environments. However, ransomware can have serious consequences, and we encourage all our members to protect themselves against this threat as well.
- DDoS attacks continue to be reported in both Denmark and other parts of the world, but at this time we do not believe that these attacks have the direct potential to impact critical infrastructure.
- The geopolitical conflicts we are witnessing, and the cyberattacks related to these, have the potential to affect organisations in Denmark due to the use of technologies from one of the parties or collaboration with one of the parties. However, we assess that the scale of these activities is too low to affect critical infrastructure.
- We assess that many companies have good protection against current attack methods, which means that the risk of industrial control systems being affected is low.

Review recommendations and take action

SektorCERT encourages all actors, regardless of the current threat level, to implement all 25 recommendations from the handbook.

Based on the current threat assessment, SektorCERT encourages all actors to follow the recommendations from the handbook in relation to threat level BLUE and validate that the following technical and organizational measures are working as intended:

- Firewall [1]
- Exposed services [2]
- Multifactor validation [9]
- Update of systems [10, 11]
- Contingency plans and emergency procedures [12, 24]
- Log collection [13]
- Map network entries [15]
- Segmentation [16]

SEKTOR CERT

Phone number:

+45 88 32 71 40

E-mail:

info@sektorcert.dk

PGP key:

C2EF 6314 7860 2B1E 2341 ACF4 DBC3 511D 3D06 BB3A

Visiting and mailing address:

Sommerfuglevej 2A
6000 Kolding

Bredgade 45
1260 København K

CVR number:

41369841

Satellite phone number:

+88 16 22 45 60 29

SINE radio (DK):

7312056