CENTRE FOR
CYBER SECURITY

Centre for Cyber Security

at the Danish Defence Intelligence Service

The DDIS' Centre for Cyber Security
The cyber threat against Denmark is real. Danish public authorities and private companies are the targets of daily attempts of cyberattacks from hackers who seek to steal research results, business plans and innovative ideas vital to Denmark's future.

At the same time, Denmark has become increasingly dependent on the Internet and digital solutions. Thus, a high cyber security level is of great importance to Denmark's future development, welfare and prosperity as well as for society's security and trust in the public sector in a digitalised everyday life.

A part of the Danish Defence Intelligence Service
The Centre for Cyber Security was set up in December 2012 within the Danish Defence Intelligence Service (DDIS). As a part of the DDIS, the Centre has access to the special intelligence-based knowledge about cyber issues available to the DDIS while the attachment also creates a number of synergies.

The Centre for Cyber Security is the national IT security authority, Network Security Service and National Centre for Excellence within cyber security. The Centre's mission is to advise Danish public authorities and private companies that support functions vital to society on how to prevent, counter and protect against cyberattacks.

Countering cyberattacks
The Centre's Network Security Service regularly analyses internet traffic to/from the authorities and companies that are connected to the Network Security Service to detect signs of intrusion.

When the Network Security Service detects a possible attack against a connected organisation, the Centre's technicians conduct advanced analyses to quickly determine the nature of the threat.

In case of a cyberattack, the Centre will directly inform the targeted organization, and if necessary, give advice on how to resist the attack. In particularly serious incidents, the Centre may also send a team of technicians to assist the organization.

Prevention of cyberattacks
As the national IT security authority and Centre for Excellence within cyber security, the Centre informs and advises on preventive measures and issues guidelines and recommendations to Danish public authorities and private companies on strengthening of their cyber security efforts and preventing cyberattacks.

In addition, the Centre is responsible for approving and supervising electronic information systems and installations that process classified information. Also, the Centre is in the process of developing core competences in terms of securing industrial control systems, including in particular the so-called SCADA systems (Supervisory Control and Data Acquisition).

The threat assessment
The Danish Defence Intelligence Service (DDIS) assesses that Danish public authorities and private companies are the targets of extensive and increasing number of espionage attempts via the Internet. The threat comes from state-sponsored actors in particular, who seek to conduct espionage with the intent of promoting their national economic, military and societal developments. The rapid technological development means that the cyber threat is constantly changing, necessitating persistent security measures and detection capabilities.

Supervision of the telecommunications sector
The Centre for Cyber Security is the national regulatory authority on information security and preparedness in the telecommunications sector, which means that the Centre contributes to the drafting of regulations on this issue and conducts regular supervision to ensure that the telecommunications providers comply with the regulatory demands.

Have you been exposed to serious IT security incidents?
In order to provide the best possible service in terms of preventing, resisting and handling cyberattacks, it is essential that the Centre's Network Security Service holds the necessary data to create the best possible overview of the current security situation regarding the Danish Internet infrastructure. Consequently, public authorities are obligated to report serious IT security incidents to the Centre for Cyber Security, and private companies are also encouraged to report serious cyber incidents to the Centre. For further contact information regarding reporting serious IT-incidents, go to our website at www.cfcs.dk.

Legal framework
The Centre for Cyber Security Act stipulates unambiguous and restrictive rules for the Centre's mission. In connection with the commencement of the Act, the Centre has also established an internal compliance function to ensure that the Centre complies with existing laws and regulations as well as internal procedures and relevant standards at any time. Also, the Centre is determined to ensure that sensitive personal data is always processed with respect to the rule of law and personal liberty.

Contact details:

Centre for Cyber Security
Danish Defence Intelligence Service
Kastellet 30
2100 Copenhagen

For personal visits:
Holsteinsgade 63
2100 Copenhagen
Email: cfcs@cfcs.dk
Phone: +45 3332 5580

Follow us on Twitter (@cybersikkerhed) and LinkedIn