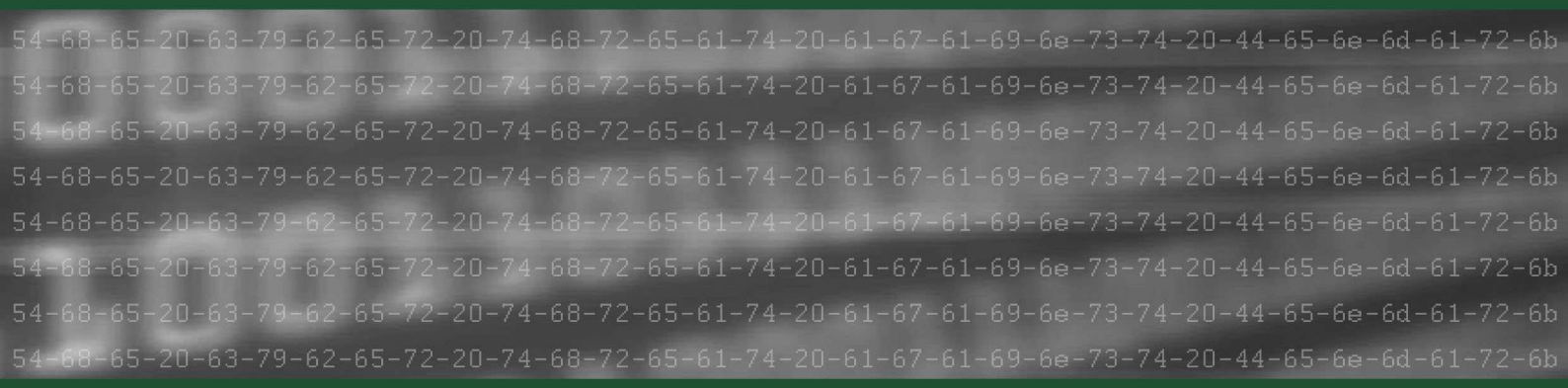
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat against Denmark



Threat Assessment Branch under the Centre for Cyber Security

January 2016

CENTER FOR CYBERSIKKERHED

The cyber threat against Denmark

This assessment describes the cyber threats facing Danish public authorities and private companies.

The assessment has been prepared by the Threat Assessment Branch under the Centre for Cyber Security whose mission is to add to the pool of information available to Danish authorities and companies that support functions vital to Danish society on how to counter cyberattacks more effectively.

Key Assessment

Espionage against Danish state institutions and private companies still constitutes the most serious cyber threat to Denmark and Danish interests. This type of espionage is mainly conducted by state and state-sponsored groups. In recent years, cyber espionage against Denmark has increased significantly, and the methods and techniques employed by the perpetrators have become increasingly sophisticated.

The threat from cyber espionage against Danish authorities and private companies is **VERY HIGH**.

Overall, cybercrime has grown in magnitude and complexity, targeting both public authorities and private companies. Cybercrime could ultimately threaten the existence of small, financially vulnerable businesses. Updated technological tools are readily available online and cyber criminals are increasingly ready to use them to commit online crime.

The threat from cybercrime against Danish public authorities and private companies is **VERY HIGH**.

Despite the easy access to online tools, the number of serious cyberactivism attempts against Danish public authorities and private companies is low. However, some hacktivists have the capability and intent to launch attacks against what they perceive as 'hostile' authorities and companies. If a public authority or a private company were to attract attention from hacktivists, the threat may rise to high or very high overnight.

The threat from cyberactivism against Danish public authorities and private companies is **MEDIUM.**

In extreme cases, cyberterrorism could result in loss of life and destruction of property or extensive financial losses with potentially serious repercussions for Danish national security.

According to the Threat Assessment Branch, militant Islamist groups in particular - like ISIL – could over time acquire cyber capabilities that would enable them to launch harmful attacks. However, currently they have limited capabilities to launch actual online terrorist attacks.

The threat from cyberterrorism against public authorities and private companies is assessed as **LOW**.

Threat	Level
The threat from cyber espionage	Very high
The threat from cybercrime	Very high
The threat from cyberactivism	Medium
The threat from cyberterrorism	Low

Introduction

Denmark is one of the most digitized countries in the world. Public as well as private sectors have become increasingly dependent on the Internet. Digitization allows for rapid exchange of knowledge and services, but at the same time it facilitates malicious online activity. Cyber threats in and against the West, and by extension against Denmark, are growing in number. Also, technological development contributes to the ever-changing nature of threats, necessitating persistent security measures and preparedness.

This threat assessment describes and evaluates the main types of cyber threats facing Danish networks, and offers guidelines on how to counter these threats. The assessment is prepared by the Threat Assessment Branch under the Centre for Cyber Security, which was set up as part of the national strategy for cyber and information security. In addition, the national strategy recommends that cyber threats be included in risk assessments and risk management strategies of public authorities. Private companies could also use this threat assessment to develop cyber and information security strategies.

The exact number of cyber security incidents against both state institutions and private companies is subject to great uncertainty. Private companies in particular are not interested in calling attention to specific incidents, thus making it difficult to get a clear picture of specific trends in certain sectors. The mission of the Threat Assessment Branch is to cooperate with public authorities and private companies to improve common knowledge and understanding of the threat. In this context, since July 2014, state institutions have been obligated to report serious security incidents to

the Centre for Cyber Security, and private companies was encouraged to report serious cyber incidents to the Centre.

The Threat Picture

Cyber threats are multi-faceted. This assessment focuses on the motivation behind each threat and what the consequences may be for the targeted authority or company. This threat level assessment operates with a time frame of 0-2 years. Threats are dynamic and may thus change overnight, affecting society both in general and the individual authorities and private companies.

When the Centre for Cyber Security holds specific information on attacks or threats against Danish authorities or companies, the Centre will directly inform the authority or company in question.

Cyber Espionage

The aim of cyber espionage is to collect information, for example sensitive or confidential information, intellectual property, trade secrets etc. The espionage may be strategically, politically and financially motivated. Perpetrators go to great lengths to conceal their cyber espionage activities, and the intrusion often remains undetected.

Recent years have seen a significant rise in the number of attempted cyber espionage attacks against Denmark and Danish interests. At the same time, state and state-sponsored groups have grown more advanced in their methods, approaches and efforts to conceal their activities and identities. Advanced state-sponsored hacker groups target state institutions with specific strategic information and private high-tech companies.

In recent years, Centre for Cyber Security has repeatedly detected and prevented cyber espionage against Danish public authorities and private companies, and the almost daily state-sponsored cyber espionage attempts against the Danish Ministry of Foreign Affairs are assessed to originate from state and state-sponsored groups. Similarly, several NGOs have also been attacked, and the Centre cooperates continuously with Danish cyber victims. The Threat Assessment Branch under the Centre for Cyber Security believes that the threat from cyber espionage does not only target key authorities and large private companies. State institutions or private companies with information that other states or companies want access to, could potentially become a target.

It is quite difficult for public authorities and private companies to detect cyber espionage attempts and assess the subsequent ramifications, even if these attempts are detected. Ultimately, cyber espionage may cause a company to lose market shares and thus force it into bankruptcy. So far, we have not seen any examples of bankruptcy among Danish companies caused by cyber espionage.

The state-sponsored hacker groups are increasingly using organizations whose networks they have already gained access to as platforms for attacking more targets with greater security awareness.

Public authorities and private companies could thus become a stepping stone towards the real targets – an element that should be included in their risk management strategies.

The threat against Danish authorities

The threat from cyber espionage against Danish authorities is **VERY HIGH**. It is highly likely that several Danish authorities are prioritized targets for state and state-sponsored groups, and that this trend will continue. As hacker groups continuously perfect their technical skills and capabilities, state institutions will be forced to heighten their security levels and are thus engaged in a constant cyber-race.

Some foreign states specifically target Danish authorities in an attempt to collect information on, for instance, Danish foreign and security policy matters. Illustrative of this are several campaigns launched in 2015 by foreign states targeting the Danish central administration and other public authorities.

The participation of Danish authorities in international negotiations and cooperation forums often leads to attempts at cyber espionage. In 2014, several Danish public authority employees were the targets of such attempts in connection with an international research project. A foreign intelligence service was behind the activity.

The threat against Danish companies

Overall, the threat from cyber espionage against Danish authorities is **VERY HIGH**. In recent years, several state-sponsored hacker groups have specifically targeted Danish companies and this trend will continue.

A serious IT security incident that unfolded in 2014-2015 illustrates this. It involved a Danish company and one of its service providers, both of which were targets of cyber espionage for more than one year. The state-sponsored hacker group behind the incident gained access to the networks of both companies, thus gaining access to trade secrets stored on various computers and servers. The group was also able to record sound from built-in microphones in the companies' computers as well as create screen dumps and record keystrokes, without the companies detecting it.

In the future, Danish companies will highly likely be the targets of even more sophisticated attempts at cyber espionage. This applies in particular to research-intensive sectors in which Denmark is among the global market leaders. In recent years, a number of Danish companies have most likely lost important trade secrets and intellectual property because of cyber espionage. The companies also believe that they are engaged in a cyber-race generated by the hackers' improving technical capabilities on the one side and the companies' security measures and risk management strategies on the other side.

So far, criminal groups lack the organizational and technical skills to launch actual cyber espionage attacks as sophisticated as the ones launched by state and state-sponsored groups; however, recent developments suggest that certain criminal groups are perfecting their technical skills in an attempt to launch cyber espionage attacks, increasing the threat against companies whose competitors could gain competitive advantages through commissioned cyber espionage conducted by criminals.

Spear-phishing
A spear-phishing attack targets individuals in an organization. The aim of the attack may be to gain access to confidential information, usernames and passwords to accounts used in the organization. The hacker will make efforts to install malware on the user's computer, tablet or mobile phone, enabling the hacker to use the compromised information in connection with an actual cyberattack against the organization.
Source: Security recommendations: Spear-phishing – a growing problem, Centre for Cyber Security

The threat from cyber espionage
Espionage targeting state institutions and private companies still constitutes the most serious cyber threat to Denmark and Danish interests. This type of espionage is mainly conducted by state and state-sponsored groups. In recent years, cyber espionage against Denmark has increased significantly, and the methods and techniques employed by the perpetrators have become increasingly sophisticated.

The threat from cyber espionage against Danish authorities and private companies is **VERY HIGH**.

Cybercrime
In the present threat assessment, the term cybercrime covers offences committed against public authorities or private companies with a criminal motive using information technology. This threat assessment will focus on financially motivated cybercrime against public authorities and private companies.

Financially motivated cybercrime typically includes different types of fraud and cyber extortion by means of ransomware, Distributed Denial of Service attacks (DDoS) and unauthorized access to data with the intent to commit extortion, resell sensitive information or commit intellectual property theft. Criminal groupings have demonstrated great ingenuity and technical skills in connection with financially motivated cybercrime.

False invoicing is another cybercrime phenomenon in which criminals may ask a company to redirect a payment by using an email resembling an existing customer mail. Some of these cases have resulted in losses of several hundred thousand Danish kroner.

On 7 December 2015, the security firm FireEye identified the presence of a threat actor called FIN1 which has started using highly sophisticated malware that executes before the operating system loads. The malware is difficult to identify and detect and reinstallation of the operating system is not sufficient to remove the malware either. The group is notorious for stealing credit card data from financial institutions, such as banks and credit institutions. The malware gives access to the victim's network and could also be used for cyber espionage.
Source: https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

Extortion by means of ransomware against Danish private companies and public authorities is growing in magnitude and complexity. Criminals have little trouble launching ransomware attacks as ransomware tools are readily available online. Several of the incidents recorded by the Danish police in 2015 demonstrated great ingenuity as well as technical skills. In the autumn of 2015, a series of fake emails mimicking postal delivering mails from a postal service company, Post Nord, informing customers that their package was unable to reach its destination. The email encouraged the customer to click on a link to read more information about the package. When the customer did so, the ransomware programme encrypted the hard disk, all data stored on it, as well as data found in network-connected devices. A message would then pop up demanding 'ransom' in exchange for decrypting the data.

Ransomware
Typically, ransomware is delivered as a malware infection on a computer system that is activated by a person who in good faith opens an attachment or a link in a malicious email. The malware then encrypts the data on the victim's hard disk and network-connected devices, demanding that the victim pay ransom to the malware operators to remove the encryption – hence the name ransomware.
Source: SIKKERHEDSBULLETIN 1/2015, Centre for Cyber Security

Cyber criminals increasingly use social engineering techniques to make their emails appear credible and trick their victims into activating the malware.

As a result of the easy online access to Distributed Denial of Service (DDoS) tools, criminals do not need to have particular technical prerequisites to launch such attacks. DDoS attacks are also used in financially motivated extortion campaigns involving the demand of bitcoin ransoms. The technical skills of cyber criminals are quite sophisticated in this field.

The economic impact of ransomware and DDoS attacks is potentially very serious if the targeted company loses data or is unable to sell its products online for a period of time. If such attacks were launched against public authorities, the societal repercussions could be massive and might include extended inability to pay social benefits or provide public services.

On 3 December 2015, Wired.com reported on a hacker calling himself Hacker Buba. He hacked into a bank in the United Arab Emirates threatening to leak all the stolen account information unless the bank accepted to pay ransom. When the bank refused, he leaked information about more than 500 of the bank's customers on Twitter.

The threat from cybercrime

Overall, cybercrime has grown in magnitude and complexity, targeting both public authorities and private companies. Small and financially vulnerable companies, in particular, may not be able to survive cybercrime. Updated technological tools are readily available online, and cyber criminals are increasingly ready to use them to commit online crime.

The threat from cybercrime is assessed as **VERY HIGH**.

Cyberactivism

Cyberactivism or hacktivism is aimed at promoting a political agenda with the perpetrator hacking into a website or a computer network for the purpose of conveying a political message. The perpetrator engaged in such an activity is called a hacktivist.

Cyberactivism could be considered an act of civil disobedience through the Internet. Cyberactivism methods include website defacement, which is a form of cybervandalism, which involves the hacktivist changing the visual appearance of the website, leaving political statements, Distributed Denial of Service attacks (DDoS), URL redirections and stealing information.

Minor DDoS attacks have been launched against public websites by private individuals and small groups of so-called hacktivists who try to generate attention around a certain issue. Thus, hacktivists mainly target organizations that have political, geographical or other affiliations with the issue in question. The politically motivated attacks have resulted in websites being taken over by hacktivists and used for dissemination of propaganda or overload of a critical component, resulting in system breakdown. This kind of political activism will highly likely continue.

DDoS against Iceland

On Friday 27 November 2015, hacktivists linked to the hacker group 'Anonymous' launched a DDoS attack against five Icelandic government websites, resulting in the sites being down for about 13 hours. The attack was part of an anti-whaling campaign.
Source:
http://icelandmonitor.mbl.is/news/politics_and_society/2015/11/30/iceland_hit_by_whaling_cyber_attack/

As a result of easy online access to DDoS tools and other types of hacker attack tools, hackers do not need to have particular technical prerequisites to disrupt Danish websites and servers. In addition, technically skilled private individuals could still hack into even major government and private organizations with low security awareness.

The Climate Summit in Paris (COP21)
On 3 December 2015, The Guardian reported that the hacker group 'Anonymous' had leaked login details of more than 1,000 delegates. Though the damage was limited, the fact that the entire user database was compromised demonstrates lack of security awareness.
Source: http://www.theguardian.com/environment/2015/dec/03/paris-climate-summit-hackers-leak-login-details-of-more-than-1000-officials

The threat of cyberactivism
Despite the easy access to tools on the Internet, examples are scarce of cyberactivism against Danish public authorities and private companies. However, some hacktivists have the capability and intent to launch attacks against what they perceive as 'hostile' authorities and companies. If a public authority or a private company were to attract attention from hacktivists, the threat may rise to high or very high overnight.

The threat from cyberactivism against Danish public authorities and private companies is generally assessed as **MEDIUM**.

Cyberterrorism

Just like terrorist acts in general, cyberterrorism is politically motivated and aimed at garnering attention around a terrorist cause through violent acts which often result in physical destruction or death that invokes fear in the target population. Simple cyberattacks, such as DDoS, are not usually considered cyberterrorism, unless the attack is spectacular and reaches the intended target in which case it will invoke the same kind of fear as a physical terrorist attack. Simultaneous combination of simple cyberattacks and physical terrorist attacks could exacerbate the effect of cyberattacks, for example by preventing key public authorities from acting or communicating.

Danish public authorities, private companies and organizations could become targets of cyberterrorism if they, or Denmark as a nation, attract the attention of cyberterrorist groups.

Non-state actors, including ISIL, have expressed an interest in launching cyberattacks against key societal functions. Nevertheless, in the short to medium term, it remains highly unlikely that terrorists will be able to launch harmful cyberattacks of this type, as they lack the prerequisite capabilities. A few Islamist militants are likely capable of launching simple cyber operations, such as

DDoS attacks. Terrorists will increasingly turn to the Internet for propaganda purposes, for instance by issuing threats.

The threat from cyberterrorism
In extreme cases, cyberterrorism could result in casualties and destruction of property or extensive financial losses with potentially serious repercussions for Danish national security.

According to the Threat Assessment Branch, militant Islamists groups in particular - like ISIL - could over time acquire cyber capabilities that would enable them to launch harmful attacks. However, at present, they have limited capabilities to launch actual terrorist attacks over the Internet.

The threat from cyberterrorism against public authorities and private companies is assessed as **LOW**.

Recommendations

The Centre for Cyber Security recommends the following publications in Danish to public authorities and private companies available at the homepage:

- Effective Cyberdefence
- Spear-phishing –a growing problem
- How to limit the threat from Ransomware and
- How to counter a DDoS attack

In addition, public authorities and private companies should have detailed knowledge of their own infrastructure and regularly conduct risk analyses based on their vulnerabilities, enabling them to identify the potential consequences of the different types of attack and thus implement contingency plans to counter such attacks.

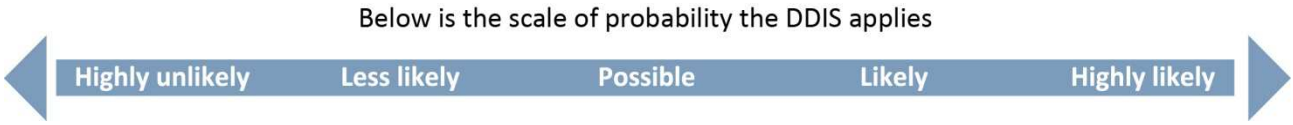
The Centre for Cyber Security recommends that Danish public authorities and private companies implement the ISO27000 standard information security management system and would like to direct attention to the Knowledge centre for implementation of ISO27001 on the website of the Danish Agency for Digitisation.

Finally, it is important to hire employees or have access to individuals with the right skills to handle cyber security.

Terms and definitions

In order to facilitate the reading of this threat assessment, we have prepared a brief outline of the special terms and definitions used in our assessments.

Intelligence assessments almost always contain elements of uncertainty. The level of probability in assessments must thus always be made clear. To facilitate this and to ensure that all analysts express levels of probability consistently, we use standardized phrases to indicate probability, in particular when making key assessments.



The scale does not express precise numeric differences but merely informs the reader whether something is more or less probable than something else. In other words, this scale shows whether we assess the probability to be closer to 25 per cent than to 50 per cent. This is the best way for us to ensure consistency between analyst intention and reader interpretation.

Probability levels are not an exact science but are intended to give the reader an indication of our level of certainty. Probability levels, terms and definitions used in this risk assessment are as follows:

Degrees of probability	
”It is highly unlikely that ...”:	We do not expect a certain development. Such a development is (almost) not a possibility.
”It is less likely/doubtful that ...”:	It is more likely that something will not happen than vice versa.
”It is possible that ...”:	It is a likely possibility, however, we do not have the basis to assess whether it is more or less possible that something will happen.
”It is likely that ...”:	It is more likely that something will happen than vice versa.
”It is highly likely that ...”:	We expect a certain development. It has (almost) been confirmed.

Threat levels

The following five threat levels, ranging from **NONE** to **VERY HIGH**, are used in threat assessments prepared by the Threat Assessment Branch.

Definition of National Threat Levels	
None	There are no indications of a threat. There is no acknowledged capability or intent to attack. Attacks/harmful activities are unlikely.
Low	There is a potential threat. There is limited capability and/or intent to attack. Attacks/harmful activities are not likely.
Medium	There is a general threat. There is capability and/or intent to attack and possible planning. Attacks/harmful activities are possible.
High	There is an acknowledged threat. There is capability, intent to attack and planning. Attacks/harmful activities are likely.
Very High	There is a specific threat. There is capability, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.