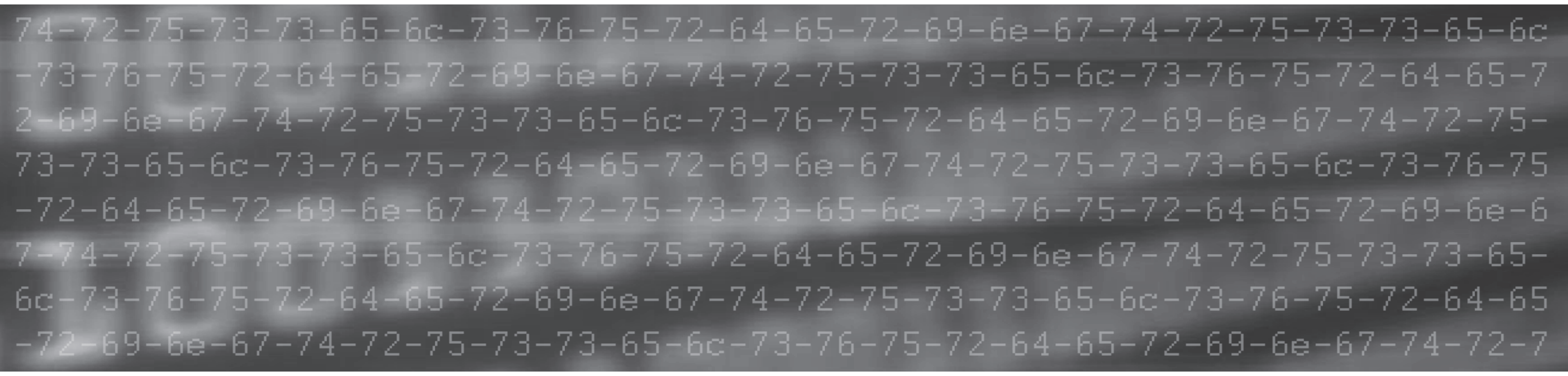
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat against the Danish energy sector



Threat Assessment Branch under the Centre for Cyber Security

September 2018

Threat assessment: The cyber threat against the Danish energy sector

This threat assessment outlines the cyber threats facing the Danish energy sector. The Danish energy sector is of vital importance to the functioning, stability and wealth of the Danish society. This threat assessment could, for example, be included in the energy sectors' risk assessment in relation to the national Danish cyber and information security strategy.

Key assessment

- The threat of cyber espionage against the Danish energy sector is **VERY HIGH**. The Centre for Cyber Security (CFCS) assesses that foreign nations use cyber espionage as an instrument to benefit their own energy sectors or as leverage in potential political or military conflicts. During the past year, the Danish energy sector has been subject to a number of attempted cyber espionage attacks.
- The threat of cyber crime against the Danish energy sector is **VERY HIGH**. Cyber crime aimed at disrupting IT networks and IT infrastructure could, at worst, threaten energy supply.
- The threat of cyber activism against the Danish energy sector is **LOW.** However, as activists are often driven by single-issues, the threat level may suddenly increase.
- The threat of cyber terrorism against the Danish energy sector is **LOW**. We assess that militant extremis militant extremists have limited abilities and resources to carry out serious attacks. Even though they in a few cases have expressed an interest in conducting cyber terrorism, they currently don't have the capability.
- We assess that in the short term, foreign states are less likely to launch destructive cyber attacks against critical infrastructure in Denmark, including the energy sector. However, the threat may increase in connection to a heightened political or military conflict with certain countries.

Introduction

This threat assessment provides an overview of the threats against the Danish energy sector. The energy sector is vital to the functioning of Danish society as it supplies the country with energy, including energy to other critical sectors. In addition, energy security is an important competitive parameter that helps ensure Denmark's ability to attract companies with special energy needs such as data centres, which will account for an estimated third of Danish energy consumption by 2040. The energy sector is thus crucial to the functioning, stability and wealth of the Danish society.

The Danish energy sector includes a diverse range of companies that plays a vital role to the production, transmission and distribution of electricity and natural gas in Denmark. The energy sector is not only vital to Danish society, but also to the countries connected to the Danish electricity and natural gas grid. This threat assessment provides an overview of the cyber threats facing the energy sector as a whole, making only limited distinctions between the different components of the sector.

The Danish energy sector

The Danish energy sector consists of three types of companies related to their role in the energy supply chain: Production of electricity and gas, transmission at a national level and distribution to consumers. At present, there are approx. 80 companies bound to be connected to the supply grids in relation to the security of energy supply.

Energinet is Denmark's only national Transmission System Operator (TSO). Energinet owns and operates the transmission systems for electricity and natural gas in Denmark. The electricity and gas production is regulated by guidelines established by Energinet.

Denmark is a key node in the European energy and natural gas grid, for instance in relation to the Baltic Pipe project designed to transmit natural gas from the North Sea through Denmark to Poland. Denmark is service provider for the electricity exchange in the Nordic and Baltic countries. Denmark has been chosen to host a joint Nordic operational centre, Nordic Regional Security Coordinator, which is the joint office for electricity transmission system operators in Denmark, Finland, Norway and Sweden.

What are cyber threats?

The Danish Defence Intelligence Service's Centre for Cyber Security (CFCS), defines cyber threats as malicious acts that attempt to disrupt, or gain unauthorized access to data, systems, digital networks or digital services.

The cyber threat landscape is diverse. In this assessment, the focus will be on the objectives of the adversaries conducting the cyber attacks, ranging from cyber espionage, cyber crime and cyber activism to cyber terrorism as well as the potential threat of destructive cyber attacks.
The threat levels in this assessment are based on analyses of the actors' intention and cyber capabilities in terms of the human and material resource available to the actors, ranging from skilled hackers, malware developers or information on targets that is useful in social engineering campaigns to IT infrastructure knowledge, time, funds and access to information. Thus, the scale of an actor's cyber capabilities depends on the actor's resources as well as the ability to exploit it.

This threat assessment is based on the current threat landscape and operates with a warning time frame of 0–2 years. As the cyber threats against the Danish energy sector are dynamic and multidimensional, the threat landscape may change rapidly both in terms of the overall threat, as well as in relation to the threat facing individual authorities and companies. The threat and probability levels applied in this assessment are defined at the end of the assessment.

Many cyber attacks against public authorities and private companies, including attacks on energy sector companies, go unreported. Sometimes organizations refrain from reporting attacks to avoid drawing attention to the fact that they have been compromised, and at times the attacks go undetected. In May 2018, the Danish government introduced a new incident reporting system that will help raise awareness of cyber attacks against critical sectors, ultimately strengthening government security and ensuring more coordinated efforts and initiatives.

Cyber espionage

The threat of espionage against the energy sector is **VERY HIGH**. CFCS assess that the threat is mainly directed at production and transmission companies.

Over the past years, there have been a number of attempts of hacking against the Danish energy sector. For example, CFCS assesses that several of the targeted attempts in 2017 were launched to gain access to Danish energy sector organizations through so-called spear phishing and watering hole attacks. CFCS assess that these incidents were cyber espionage attempts by a state-sponsored actor affiliated with a foreign intelligence service. CFCS assess that cyber threats from foreign states are growing increasingly persistent.

Denmark is pioneering country in regards to energy security and the transition from fossil fuels to green energy. Denmark is also a European energy and natural gas hub, playing a key role in the exchange of electricity and natural gas in Europe. As a result of the key position, foreign states may have a particular interest in the Danish energy sector, for instance in private companies and public authorities affiliated with the Baltic Pipe and Nord Stream 2 pipeline projects.

The exchange of electricity and natural gas across national borders means that the threat is not confined to any single geographic location. The interest in one country's energy supply could motivate an actor to conduct espionage against neighbouring countries supplying electricity or natural gas to that specific country.

Cyber espionage against the energy sector may be rooted in both political and economic motives. For instance, cyber espionage may give the actor access to knowledge that provides a technological and competitive advantage, for example within green technology development, or knowledge that would allow them to promote national energy policy interests.

Cyber espionage poses a potential threat to the energy security in Denmark. Espionage against critical infrastructure could be used in the preparation of destructive cyber attacks or physical attacks against the energy sector in connection with a crisis or conflict.

Some countries are also engaged in cyber espionage against companies that cooperate with their own national companies or authorities, allowing them to monitor partners and companies that may influence national organizations. For example, US authorities have accused the Chinese military of conducting cyber espionage against US companies, in connection with negotiations with the state-owned China National Offshore Oil Corporation, claiming that Chinese hackers specifically targeted information related to the negotiations.

Other countries are likely also involved in cyber espionage against energy sectors around the world. According to US and British authorities, Russian hackers have launched multiple cyber espionage attempts against energy sectors worldwide in the past few years.

State-sponsored hacker groups also attack IT systems across industries that share the same IT vulnerabilities, irrespective of their relevance as cyber espionage targets, and energy sector companies are not immune to these types of cyber attacks.

Baltic Pipe and Nord Stream 2
The Baltic Pipe is a proposed natural gas pipeline running from the North Sea through Denmark to Poland via the Baltic Sea. The pipeline will allow transportation of 10 billion cubic metres of natural gas per year.

The Nord Stream 2 project is aimed at establishing a gas pipeline carrying Russian natural gas to northern Germany via the Baltic Sea. The pipeline is capacitated to carry up to 55 billion cubic metres of natural gas per year.

Denmark’s total annual consumption of natural gas is approx. 2.5 billion cubic metres. The Nord Stream 2 pipeline and the Baltic Pipe pipeline will cross in the Baltic Sea.

Cyber crime

The threat of cyber crime is **VERY HIGH**. Organizations in the Danish energy sector face targeted cyber crime attacks as well as the risk of becoming targeted by cyber criminals in attacks against a large number of targets.

In this assessment, cyber crime denotes criminal activities where cyber attacks are motivated by financial gain, for example financial and personal information theft, fraud and extortion.

Cyber criminals are resourceful, and employ a wide range of cyber attacks, some of which are advanced and complex. Cyber crime aimed at extorting money from private companies or public authorities constitutes a particularly significant threat, that often takes the shape of ransomware attacks. However, cyber criminals have also been known to extort their victims in other ways, for instance by launching DDoS attacks, or by threatening to leak stolen data.

There are cyber criminal networks functioning and operating organised on longer terms. Some networks are performing targeted and advanced cyber attacks, stealing or extorting large amounts of money from authorites and companies. Some criminal networks have specialised in compromising victims worldwide, and while these attacks are not technical advanced, they are well organised and comparable to those on industrial level.

Known ransomware attacks against energy sector companies include the 2015 attack against the Danish energy distribution company, NRGi, that fell victim to a targeted cyber attack, that severely disrupted its business systems. Even though the cyber criminals were unsuccessful in accessing critical networks, the ransomware attack affected NRGi's administrative IT infrastructure.

Attacks aimed at disabling administrative IT networks and IT infrastructure may, at worst, threaten energy supply. This could become the case if cyber criminals successfully infect critical systems with malware such as ransomware, or if a ransomware attack against the administrative networks impedes the control and upkeep of the critical systems. Such an attack may also affect the company's finances to a degree where it can no longer financially uphold its operations.

Companies in the Danish energy sector have been exposed to Business Email Compromise scams (BEC), in which criminals have impersonated in-house executives to trick company employees into wiring funds to the criminals' accounts. This was the case when, in May 2018, Energinet was targeted in an attempted BEC scam in connection with the appointment of a new CEO. Criminals impersonated the new CEO, but fortunately vigilant Energinet employees and best practices foiled the attack.

Even though no IT systems were compromised during this attack, it still reflects the threat posed by fraudulent emails and misuse of company and personal information. Should cyber criminals launch attacks via compromised company email accounts, it would make it all the more difficult for the company to detect the attack in time.

Examples of criminal cyber attacks against the energy sector

Below is a non-exhaustive list of the most typical cyber criminal attacks against the energy sector.

Ransomware attacks

Like many other types of malware, ransomware is typically spread via phishing emails or infected websites visited by the victim. Ransomware attacks render the victim's data or systems inaccessible, and ransom is demanded in exchange for restoring access to the data. There are many different types of ransomware. Sophisticated ransomware attacks typically target administrative networks in specific private companies and public authorities.

Infection with other types of malware

Cyber criminals frequently distribute other types of malware that could be used to steal personal and financial information that is subsequently sold to third parties or exploited by the criminals. Crypto currency mining malware is a new type of malware that is used to tap into the computing power of victim devices to mine crypto currencies.

Targeted extortion

A new trend has emerged among cyber criminals that involve groups specializing in stealing sensitive company and client information for extortion purposes. Threats of launching DDoS attacks via the Internet are also used as a means of extortion. Cyber criminals often demand very large sums of money from their victims.

Scams
So-called Business Email Compromise scams (BEC) are aimed at tricking companies and organizations into wiring funds by sending fraudulent emails requesting wire transfers. Cyber criminals impersonate an in-house executive (often the CEO); hence the often-used name CEO fraud.

Cyber activism

The threat of cyber activism is **LOW**.

Even though the energy sector abroad has been the target of cyber activism, CFCS assesses that the Danish energy sector is not a prioritised target for cyber activists. In general, cyber activists rarely focus their attention on Danish authorities or companies. However, some cyber activist networks and individuals have the capabilities and resources to launch cyber attacks. Consequently, the threat posed by cyber activists may suddenly increase, should Danish energy authorities or companies land in their crosshairs.

Cyber activists employ an array of simple cyber attacks, for example DDoS attacks. They also launch defacement attacks in which hacked websites and social media profiles are defaced with political messages. Some cyber activists have been known to leak sensitive information stolen from personal email accounts to draw attention to their cause.

Some countries use cyber activist groups as cover to influence public opinion abroad, especially in countries with opposing interests where public opinion may help influence decisions.

No Nuclear Power Plant Group

Outside Denmark, fake cyber activists have launched attacks on the energy sector. In 2014, a previously unknown group called No Nuclear Power Plant Group claimed responsibility for a cyber attack against South Korean Korea Hydro & Nuclear Power Co Ltd. Based on the evidence; however, the South Korean authorities attributed the attack to North Korea.

Cyber activism may go hand in hand with traditional political activism. In 2013, in the wake of protests in Canada against the establishment of a gas pipeline, cyber activists launched a campaign against a number of authorities and companies by compromising their websites. In 2016, cyber activists launched a DDoS and hacking campaign against selected websites as a protest against the establishment of the Dakota Access Pipeline in the United States.

Even if Danish national authorities and private companies are not directly involved in the issue that caught the activists' attention, they still risk becoming targets of cyber activism simply because hackers could consider them symbolic targets. For example, the Turkish energy company, Izmir Gaz, was exposed to cyber activism in July 2016 as a reaction to the Turkish government's handling of the attempted coup d'état earlier in the year.

Cyber terrorism

The threat of cyber terrorism against the Danish energy sector is **LOW**.

CFCS assess that even though militant extremists have expressed an interest in launching cyber terrorism, they lack the capabilities and resources required to launch serious cyber attacks at present.

Therefore, the threat against the energy sector in Denmark, with the intention of causing the same effect as a conventional terrorist attack, as for example a cyber attack that causes physical injuries or widespread disruption of critical infrastructure, is low.

Destructive cyber attacks

Several states are actively building destructive cyber attack capabilities as they present a potentially powerful instrument of leverage.

CFCS assess it less likely on short term that foreign states will launch destructive cyber attacks against critical infrastructure in Denmark, including the energy sector. The threat may increase, if Denmark were to find itself involved in a political or military conflict with a country that holds destructive cyber capabilities.

Destructive cyber attacks

We define destructive cyber attacks as attacks that could potentially result in death, personal injury, property damage, or destruction or manipulation of information, data or software, rendering it unfit for use unless extensive restoration is undertaken.

Being vital to society, the Danish energy sector may become a victim of destructive cyber attacks if foreign states turn their attention to Denmark.

It is possible that destructive cyber attacks against targets outside of Denmark may have negative spillover effects on Danish companies and public authorities, especially on companies and authorities operating in conflict areas, where foreign states have repeatedly launched destructive cyber attacks, for example in parts of Eastern Europe, the Middle East and Southeast Asia. The 2017 NotPetya attack in Ukraine highlighted that destructive cyber attacks could spread to organizations outside the mentioned conflict areas.

Over the past few years, the energy sectors in Ukraine, South Korea and Saudi Arabia have fallen victim to a number of destructive cyber attacks. The attacks were likely state-sponsored and triggered by regional conflicts and tension.

The attacks abroad have typically targeted energy production companies, but CFCS assess that the threat could potentially affect the entire energy sector, as disruptions fully or partially could affect the energy supply.

The destructive cyber attacks against the energy sector in Ukraine that led to power outages in 2015 and 2016 are known examples of cyber attacks against the energy sector abroad. CFCS assess that the energy technology used in Ukraine shares a large number of similarities with the technology used in the Danish energy sector, including protocols and equipment. Consequently, similar attacks could be launched against Denmark.

Information collected through espionage could be used in the preparation of destructive cyber attacks, consolidate the link between the threat of cyber espionage and the threat of destructive cyber attacks. Companies or authorities that have already been compromised are thus more vulnerable to destructive cyber attacks.

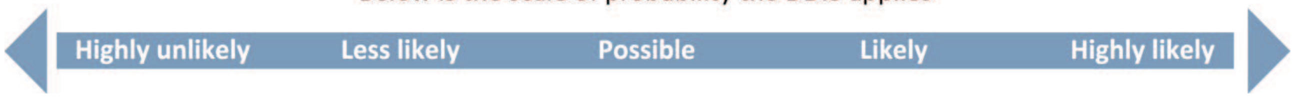
Over the past few years, methods and tools like AutoSploit and ICSSploit have become available online. These tools target vulnerabilities in industrial equipment and make it easier for hackers to find vulnerabilities in critical infrastructure that could be exploited to launch destructive cyber attacks.

Threat levels

The Danish Defence Intelligence Service (DDIS) uses the following threat levels, ranging from none to very high.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.

Below is the scale of probability the DDIS applies



Highly unlikely · Less likely · Possible · Likely · Highly likely