CENTRE FOR CYBER SECURITY

Threat assessment

The cyber threat against the Danish energy sector

1st edition February 2023.

Table of contents

CENTRE FOR CYBER SECURITY

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
Email: cfcs@cfcs.dk
1st edition February 2023

The cyber threat against the Danish energy sector

The purpose of this threat assessment is to inform of the cyber threat against the Danish energy sector. The assessment is broadly intended for decision-makers and stakeholders in the companies and authorities that make up the energy sector. The threat assessment can be used in the sector's risk assessment efforts. The present assessment replaces the updated June 2022 edition of the threat assessment against the sector and is valid for up to two years.

Key assessment

- The threat of cyber crime is **VERY HIGH**. Ransomware attacks are the most serious type of cyber crime and occur frequently against energy sector companies and suppliers. The risk of ransomware attacks impacting operational technology (OT) has become a growing concern for companies.

- The threat of cyber espionage is **VERY HIGH**. The persistent threat, posed by Russia and China in particular, results in regular cyber attacks against Danish targets. The energy sector is a high-profile target for both civilian and military reasons. The CFCS assesses that Denmark's continued position as a global leader in the transition to green energy could also be a factor driving the threat.

- The threat of cyber activism is **HIGH**. The threat mainly emanates from pro-Russian hackers, who have intensified their activities following Russia's invasion of Ukraine. Activists continue to target Western organizations, also in Denmark.

- The threat of destructive cyber attacks is **LOW**. Though some states, including Russia, have the capability to launch destructive cyber attacks against Denmark, they do not presently have the intention to do so. The war in Ukraine illustrates that destructive cyber attacks are part of modern warfare and that in times of conflict, the energy sector becomes a high-priority target.

- The threat of cyber terrorism is **NONE**.

Introduction

The energy sector in Denmark

In Denmark, the overall energy sector involves production and supply of different energy sources. In the following, the term energy sector refers to the companies, suppliers and authorities supporting the critical infrastructure that provides Denmark with a stable supply of energy – now and in the future.

To Danish citizens and companies, energy sources such as electricity, district heating, oil and gas are all critical to ensure the smooth running of everyday lives and operations. Also, wind and solar power are becoming increasingly popular energy sources. As the technology develops, the green transition will pave the way for other types of energy sources such as Power-to-X and green hydrogen. As the companies engaged in the various segments of the energy sector are very different, they also have very diverging approaches to cyber security. While the nuances of this complex sector are beyond the scope of this assessment, organizations should always factor in the circumstances unique to their particular organization in their risk assessments.

The cyber threat against the Danish energy sector, as is the case the general cyber threat against Denmark, has been categorized as "serious" since the Centre for Cyber Security (CFCS) published our first threat assessment for the sector in 2018. Since then, the threat environment has become even more complex. The energy sector has to defend against state actors, cyber criminals and cyber activists who, motivated by different intentions, launch more or less targeted attacks against Western energy companies.

The threat levels outlined in this assessment indicate the likelihood of a cyber attack with a certain purpose occurring. The threat levels do not, however, indicate the likelihood of an attack being successful, or the potential consequences of a successful attack.

The threats of both cyber espionage and cybercrime against the energy sector continue to be **VERY HIGH**. Motivated by different intentions, both states and criminal groups are interested in compromising companies operating in the energy sector. While states operate on underlying military as well as civilian motivations and have a specific interest in the energy sector, cyber criminals are constantly on the lookout for opportunities to target new victims.

Tensions between Russia and the West in the wake of Russia's February 2022 invasion of Ukraine have prompted a surge in hacktivist activities. Groups such as Anonymous and Killnet stand out as some of the most active groups, though each with their own separate agenda. As a result of the strong activity, in particular among Russian cyber activists, the current threat level of cyber activism is set at **HIGH**.

The CFCS assesses that the energy sector, too, is at risk of cyber activism, partly because the sector is a critical infrastructure sector, partly because relations between Russia and the EU are conditioned by energy policy issues.

The war in Ukraine is fanning the fear of destructive cyber attacks, and since the onset of the war, targets in Ukraine have fallen victim to several such attacks. However, the CFCS assesses that the threat of a destructive cyber attacks specifically targeted against the Danish energy sector is **LOW**. Although several states, including Russia, have the capabilities required to launch destructive cyber attacks, it remains less likely that they have the intention to do so.

Russia's invasion of Ukraine has forced the EU to reconsider its dependence on Russian oil and gas. As a direct result of the current situation, many countries, including Denmark, have decided to accelerate the green transition, severing their dependence on Russian energy. Projects such as the construction of two energy islands in Denmark are predicted to play a key role in the future energy supply. The Esbjerg declaration, designating the North Sea as a green power plant of Europe, is yet another initiative that puts Denmark in a key role in the phasing out of fossil – often Russian – energy sources. Regardless of the speed of the green transition, and the geopolitical context in which it unfolds, the Danish energy sector will remain of critical importance to Denmark as well as to our neighbours and to the EU. This provides the backdrop for the preparation of the 2023 assessment of the cyber threat against the Danish energy sector.

Cyber crime

The CFCS assesses that the threat of cyber crime, in particular ransomware attacks, to the Danish energy sector is **VERY HIGH.** It is thus highly likely that authorities and companies in the sector will become targets of attempted cyber crime within the next two years.

Danish private citizens, authorities and companies are exposed to daily attempts of cyber crime. Energy sector companies and authorities are no exception and are frequent targets of cyber crime attacks of varying complexity. Particularly ransomware attacks pose a severe threat to the energy sector. Having reviewed publicly recorded successful cyber attacks against the European energy sector, the Danish EnergiCERT assesses that ransomware attacks account for as much as 65 per cent of the cyber attacks against the European energy sector since 2015.

In Denmark as well as in the rest of Europe, ransomware attacks have hit across a broad range of energy sector stakeholders, including supply companies, gas distributers, oil terminals and refineries, wind mill producers and sub-suppliers. Besides being frequent and targeting a broad range of victims, ransomware attacks can also carry severe implications for society in general. A case in point is the May 2021 ransomware attack on Colonial Pipeline, the largest pipeline system for refined oil products in the US, that resulted in fuel shortage on the East Coast of the United States.

The energy sector has what cyber criminals want

The CFCS assesses targeted ransomware attacks to be financially motivated and opportunistic, posing a risk across all types of companies and authorities, including in the energy sector. The reasons are multiple. For one thing, the Danish energy sector is comprised of numerous companies, many of which have relatively high turn-overs. This alone makes them attractive victims for criminal groups that assess that the companies will be able to pay high ransoms.

For another thing, the fact that any disruption of the operations undertaken by energy sector companies could have a strong negative impact on the companies themselves and on the society in general only adds to the attraction of energy sector companies as targets for cyber attacks. Paying the demanded ransom may seem like a tempting solution to companies that want to resume operations as quickly as possible. Payment of a ransom demand does not, however, guarantee a quick resumption of operations. As an example, several media outlets have reported that Colonial Pipeline had to use its own backups to help restore the system, despite having paid a reported USD 4.4 million for an encryption key, which, however, proved to be very slow.

Though Russia's invasion of Ukraine has prompted some ransomware groups such as CONTI to flag their political views, it is still the CFCS's assessment that cyber criminals are mainly motivated by financial gain, seizing on whatever opportunities come their way. In other words, cyber criminals most often pick their victims based on a cost-benefit analysis identifying potential entry points and victims most likely to pay up, including the size of the ransoms they are able to pay.

Connectivity increases attack surface
The CFCS assesses that ransomware attacks still mainly target company IT environments. However, society's increasing connectivity increases the risk of attacks spreading from IT to OT, thus potentially amplifying the fallout of ransomware attacks against the energy sector.

IT, OT and IOT – with greater connectivity comes greater vulnerabilities

As technology advances, cyber security is moving beyond the realm of IT. As a result of the accelerating digitalization of modern societies, it is no longer just information that can be found in the digital domain. Many of society's production processes and operations are now also connected to the Internet.

The CFCS uses the below general definitions
IT: Information Technology. IT systems are made up of hardware and software and can stand alone or be connected to other systems as part of a network.

OT: Operational Technology. Systems that are used to manage and control mechanical performance, including Industrial Control Systems (ICS).

IOT: Internet Of Things. A term denoting devices that are connected to the Internet, including everything from thermostats to refrigerators or cameras. When OT units use Internet Protocol networks and, possibly, are connected via the Internet, this is called Industrial Internet of Things (IIoT).

In recent years, cyber security has increasingly become a focus of company production environments. According to the US Cybersecurity and Infrastructure Security Agency (CISA), for instance, OT is vulnerable to both widely available hacker tools and custom malware designed to target OT assets. The efforts by companies to take their production online, among other things to facilitate remote monitoring of production processes, raise concern as to the impact of this connectivity on cyber security.

The European Union Agency for Cybersecurity (ENISA) has assessed that cyber criminals have the capability to target OT and describes four more or less direct ways in which company OT environments can be breached. A cyber attack can involve malware that directly attacks and encrypts units in company OT environments. Another way is lack of segmentation, which can result in malware spreading from IT to OT environments. Thirdly, if a company has doubts as to whether its IT and OT systems are sufficiently segmented, a cyber attack against the systems could also result in the company itself deciding to halt production in a move to contain the malware. Finally, malware groups can tap into sensitive information about company OT units and use this information for blackmail.

As both IT and OT environments are growing more complex, so are the challenges facing companies when it comes to forming a complete picture of the its infrastructure, including any connections between IT and OT environments.

Ultimately, this could result in ransomware attacks against a company's IT systems impacting on its OT environment as well. Also, in this context the attack on Colonial Pipeline is an example in point. Appearing before the US Senate, Colonial Pipeline CEO Joseph Blount described how the company initially shut down the pipeline in order to contain the attack and to prevent the malware from spreading to the OT network. The six-day shutdown had an extensive impact on the fuel supply, as the pipeline is the largest and most vital pipeline system on the US East Coast.

The opposite was the case when, in 2021, Danish wind turbine maker Vestas fell victim to ransomware. Vestas was quick to announce that their wind turbines were able to operate independently of the affected systems.

The energy sector is complex, and many production, transmission and distribution companies use sub-suppliers. Thus, an additional challenge for companies operating in the energy sector is the fact that they also have make sure that infrastructure beyond their own systems is sufficiently protected.

Suppliers are used as gateways for attacks in so-called supply chain attacks. In this context, suppliers with a legitimate and privileged access to client IT systems are particularly attractive targets for hackers. Recent years have seen a number of notable supply chain attacks, one example being the 2021 ransomware attack against US company Kaseya, which spread to hundreds of its clients.

Cyber espionage

The threat of cyber espionage to the Danish energy sector is **VERY HIGH**, meaning that public authorities and private companies are highly likely to fall victim to cyber espionage attempts within the next two years. Due to Denmark's role as a frontrunner in the green transition, the Danish energy sector will remain a target of cyber espionage, also in the long term.

The CFCS assesses that energy sectors at home and abroad are frequent targets of cyber espionage. Cyber espionage is conducted by foreign states with a strong interest in gaining access to information on foreign, security and defence policy issues. Through its pivotal role in maintaining energy security and in underpinning the Danish government, armed forces and economy, the energy sector is of special interest to foreign states.

Possessing advanced cyber capabilities, Russia and China pose the most significant cyber espionage threat. Both countries pose a persistent threat to Danish public authorities and private companies.

Russia has a vast arsenal of cyber tools that it uses systematically to promote its national interests. Previous incidents have demonstrated that Russia has an interest in the Danish energy sector. As an example of more traditional espionage, a Russian citizen was sentenced to three years imprisonment in 2021 for spying on the Technical University of Denmark (DTU) and fuel cell manufacturers Serenergy A/S. For years, the perpetrator had been passing information to a Russian intelligence service in return for payment.

China is involved in extensive cyber espionage worldwide, including against Danish authorities and organizations. China's military and intelligence services hold powerful cyber tools and capabilities, allowing the country to gain full and permanent access to organization information. China poses a constant and long-term threat in pursuit of promoting its national security and foreign policy as well as its economic and commercial interests.

Energy politics is security politics

The war in Ukraine has accelerated the green transition, and the move towards renewable energy has been proclaimed as a shift away from Russian energy. Consequently, it is likely that foreign states, especially Russia, want to gain insight into the large construction projects that will shape Europe's future energy supply – projects in which Denmark plays a key role.

Energy islands and wind farms – Denmark as a European hub for energy

For years, Denmark has been a renewable energy pioneer. Future construction projects will strengthen Denmark's leadership and make it a hub for European renewable energy. According to Danish energy enterprise Energinet, the planned energy islands in the North Sea and Baltic Sea will be able to supply 6GW of power – enough energy to meet the average electricity consumption of six million households.

The Esbjerg Declaration, signed to make the EU self-sufficient with energy, sets a joint target for Denmark, Belgium, the Netherlands and Germany to deliver at least 65GW offshore wind power by 2030.

Cyber espionage is also used in preparation of future destructive cyber attacks. Destructive cyber attacks aimed at disrupting or even destroying critical infrastructure will often require complex or time-consuming operations.

The green transition puts Denmark in the spotlight

The CFCS assesses that the green transition and the technology required to support it are of great interest to foreign states for both civilian and military reasons.

States are continually looking to prepare for the future, achieve competitive advantages, and to secure their position in the international hierarchy. Even though the green transition in Europe has been fast-forwarded by the Russian invasion of Ukraine, transition to renewable energy will become a global issue at some point.

While China and Russia currently pose the most serious cyber espionage threat, the CFCS assesses that other countries also focus on developing their cyber capabilities and likely will represent a future cyber threat to Denmark. The CFCS assesses that Iran, North Korea, Vietnam, Pakistan and India, among others, also have the capabilities to conduct cyber espionage. However, these states likely do not have any interest in attacking Danish targets.

It is possible, however, that in a more long-term perspective the green transition will make new state-sponsored cyber actors turn their sights on knowledge held by Danish public authorities and private companies. Their motive would be to skip the development phase of the green transition in a bid to strengthen their own competitiveness. Particular targets of this form of cyber espionage include companies developing, selling and producing costly green transition technology.

Foreign states use an array of cyber espionage techniques

Cyber espionage typically targets IT systems and networks containing information such as emails and documents which are of interest to foreign states. The accessibility of this information to foreign states varies depending on factors such as the victim's IT systems and the attacker's capabilities and tools. Consequently, foreign states use a diverse array of attack techniques.

Simple attacks include so-called brute force attacks, in which hackers try to break into IT networks by guessing usernames and password combinations. Hackers may also set up false websites, luring the victims into entering their usernames and passwords. The spreading of malware through phishing, for example, is also a relatively simple attack technique, which is still very popular.

Cyber attacks can also be conducted by exploiting vulnerabilities in IT systems such as hard- and software errors, lack of updates or misconfigured servers. In some cases, the detection of vulnerabilities in common IT systems turns a wide selection of organizations into potential targets.

Foreign states – just like other types of hackers – often apply the same tools and techniques across multiple targets. On the one hand, recycling of methods and tools enables foreign state attackers to economize their resources and to attack multiple targets in one go or over a prolonged period of time. Russia and China thus have the capabilities to launch multiple simultaneous espionage campaigns against targets around the world, including in Denmark. On the other hand, recycling of techniques and tools makes it easier to detect the attacks and use the lessons learned from previous attacks to help prevent future attacks.

The threat to suppliers

Suppliers and sub-contractors may act as gateways for more advanced attacks, including software supply chain attacks in which malware is hidden in otherwise legitimate updates and spread to unsuspecting clients.

The Danish energy sector, like other parts of the critical infrastructure, is dependent of a number of different suppliers and sub-contractors, including soft- and hardware manufacturers and also units provided with managed service agreements. Consequently, complex supply chains place great demands on the individual companies as regards supply chain management.

In March 2020, hackers hid a customized backdoor in SolarWinds's widely popular Orion IT network management system. According to SolarWinds, the backdoor was distributed via infected software updates to as many as 18,000 organizations across the world. The attack was one of the most widespread supply chain attacks ever, and the CFCS has assessed that the attack was launched by state-sponsored hackers with cyber espionage in mind. Open media have reported that the infected update had been installed in IT systems belonging to a number of Danish energy companies, making them potentially affected by the SolarWinds attack. However, the CFCS assesses that the hackers primarily used the backdoors against key US federal government agencies and major private companies. US authorities have attributed the attack to the Russian intelligence service SVR.

The threat of cyber activism to the Danish energy sector is **HIGH**, indicating that it is likely that the energy sector will fall victim to activist cyber attacks within the next two years.

On 31 January 2023, the CFCS raised the threat level for cyber activism from **MEDIUM** to **HIGH.** This was partially based on the activities of pro-Russian cyber activists against NATO-countries, including Denmark, and the enhanced capacities of the activists.

The CFCS assesses that activists, in particular those of pro-Russian sentiment, primarily attack symbolic targets. Energy security concerns are at the centre of the conflict between Russia and the West. Consequently, Danish energy companies could become targets of cyber activists even though neither the sector nor Denmark is the target of a separate threat.

Pro-Russian hacker group KillNet has been very active in their support for the Russian regime. The CFCS has knowledge that KillNet, communicating through social media platform Telegram, has threatened to launch DDoS attacks and ransomware attacks against a number of named European energy companies.

Cyber activism is conducted by individuals and hacker groups who launch cyber attacks to attract maximum attention to their cause or to punish organizations. Cyber activism is typically motivated by ideological or political concerns, ranging from single issues to opposition against rulers. Cyber activists attack victims whom they consider symbolic targets as well as opponents of their cause. Cyber activists are capable of launching different types of cyber attacks, ranging from simple overload attacks and website defacement attacks to more resource-heavy hack and leak operations.

The pro-Russian hackers are increasingly formalising the planning and execution of their cyber attacks. Several of the most active, pro-Russian groups have also created dedicated platforms with the purpose of mobilising resources for DDoS-attacks.

DDoS remains the preferred tool for cyberactivists

Pro-Russian hackers primarily carry out DDoS-attacks. These kinds of cyber attacks have a disturbing effect on the victim and attracts attention without any destructive or lasting consequences for the victim.

Recently, however, there have been indications that some activist groups have ambitions for more destructive cyber attacks. Pro-Ukrainian groups have on several occasions described how they have attacked industrial control systems in Russia, also claiming targets in the energy sector. Irrespective of whether the attack did in fact take place, it is an indication that some cyber activists have an interest in carrying out more advanced cyber attacks.

Destructive cyber attacks

The CFCS assesses that the threat of destructive cyber attacks against the energy sector is **LOW**, meaning that the energy sector is less likely to fall victim to destructive cyber attack attempts within the next two years.

Destructive cyber attacks

The CFCS defines destructive cyber attacks as cyber attacks that could result in death, personal injury, significant physical damage or destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

The fact that the threat level is low indicates that it is less likely – not unlikely – that the energy sector will fall victim to a destructive cyber attack. A number of foreign states continually develop their destructive cyber capabilities, with both Russia and other foreign states possessing advanced capabilities for destructive attacks. Consequently, the threat very much depends on whether cyber-capable foreign states are also intent on destructive cyber attacks, and a change in intention could quickly reflect in an increase of the threat.

Focus on ressource security

The CFCS maintains the assessment that Russia currently has no intention of launching a destructive cyber attack on the Danish critical energy infrastructure.

Since Russia's invasion of Ukraine in February 2022, concerns about Russian cyber attacks against the Danish energy sector have dominated the public discussion. The physical sabotage against the Nord Stream 1 and 2 gas pipelines in the Baltic Sea in September 2022 has only served to deepen concerns about whether energy infrastructure will be implicated in the conflict, including outside of Ukraine. It is currently unclear who was responsible for the sabotage.

Throughout 2022, Ukraine fell victim to a number of destructive cyber attacks. According to several IT security companies, Russia was responsible for attacking a number of Ukrainian public authorities and private companies with so-called wiper attacks that permanently deleted data from the victims' systems. It has also been reported that in April 2022, a Ukrainian energy company was hit by an advanced cyber attack that directed malware and wipers against a number of industrial control systems with the purpose of crippling the country's power supply.
Russia's more conventional attacks with drones and missiles have emphasized the role of the energy sector as a high-priority target to Russia in a conflict situation. Russia targeted critical infrastructure when the attacks against Ukraine were intensified in

October 2022. As many as 30% of Ukraine's power plants have been destroyed, according to President Volodymyr Zelenskiy.

Destructive attacks could spread

The CFCS assesses that in connection with conflicts, there is a heightened risk that destructive cyber attacks could spread to victims outside of the actual conflict zone, especially in connection with the war in Ukraine.

On the day of the Russian invasion of Ukraine, US communication provider Viasat fell victim to a wiper attack dubbed AcidRain, which resulted in thousands of satellite modems, in particular in Europe, having their configuration wiped. Denmark along with the EU and a number of close allies attributed the attack to Russia and assessed that Russia was well aware that the attack would have destructive consequences outside of Ukraine.

The attack on Viasat demonstrated how the impact of destructive cyber attacks can extend beyond the intended target. According to open sources, the attack caused German energy company Enercon to lose remote control of its wind turbines. The 2017 NotPetya attacks is another example of a cyber attack whose impact extended far beyond the intended target.

Foreign states continually bolster their destructive cyber attack capabilities

The CFCS assesses that foreign states continually bolster their capabilities for launch-ready destructive cyber attacks. Foreign states use cyber espionage for instance to prepare destructive cyber attacks that could be launched in the event of an escalating crisis or war.

Cyber espionage can provide access to critical infrastructure which foreign states could then attempt to destroy or disrupt in connection with a serious crisis or war. In 2022, US authorities repeatedly warned against the threat of cyber attacks against industrial control systems. According to the FBI, the Triton malware used by Russian hackers in previous attacks still poses a threat to energy companies across the world. Being a destructive malware that targets industrial safety control systems, Triton has the potential to impact the physical processes of energy production. Also, CISA warned that malicious actors have proved capable of gaining full system access to some industrial control systems.

The preparation of destructive cyber attacks will often involve the mapping of organizations, systems and network units, for example industrial control systems. By acquiring knowledge of organizations and systems, hackers are able to develop customized malware. In addition, hackers are able to establish so-called backdoors in compromised systems which they can later exploit to launch destructive cyber attacks. It is thus vital that private companies and public authorities pay attention to whether their systems are at risk of compromise, as a compromise could, in addition to causing loss of vital information, be a first step towards a future destructive cyber attack.

Cyber terrorism

The threat of cyber terrorism against the Danish energy sector is **NONE**, meaning that the Danish energy sector is highly unlikely to fall victim to cyber terrorism attempts within the next two years.

The CFCS defines cyber terrorism as cyber attacks aimed at creating effects similar to those of conventional terrorism, including cyber attacks causing bodily harm or major disruptions of critical infrastructure.

Such serious cyber attacks require technical skills and organizational resources that are currently lacking among militant extremists. At the same time, the intention is limited.

Threat levels

The Danish Defence Intelligence Service uses the following threat levels.

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.

The DDIS applies the below scale of probability

The probabilities are estimates, not calculated statistical probabilities.
"We assess" corresponds to "likely" unless a different probability level is indicated.