CENTRE FOR CYBER SECURITY

THREAT ASSESSMENT

The cyber threat against the Danish water sector

February • 2025

Table of contents

CENTRE FOR CYBER SECURITY

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
Email: cfcs@cfcs.dk

February 2025

The cyber threat against the Danish water sector

The purpose of this threat assessment is to outline the cyber threat against the Danish water sector. The assessment can help strengthen risk owners' understanding of the cyber threat landscape and can form part of the basis for the sector's cyber security risk assessment efforts. The assessment is prepared in cooperation with the decentralised cyber and information security authority (DCIS) for the Danish water sector.

Key Assessment

- The threat of cyber crime against the Danish water sector is **VERY HIGH**. The threat mainly emanates from ransomware actors who encrypt IT systems and data with the intent to extort victims for ransom.

- The threat of cyber activism against the Danish water sector is **MEDIUM**. The water sector is less of a priority target than some of the other sectors in Danish society. Nevertheless, the sector fell victim to a serious cyber activist attack in 2024, which temporarily disrupted the water supply for a limited number of consumers.

- The threat of destructive cyber attacks against the Danish water sector is **MEDIUM**. It is possible that public and private organisations in the sector will fall victim to destructive cyber attacks.

- The threat of cyber espionage against the Danish water sector is **MEDIUM**. The Danish water sector is not a priority espionage target to the same extent as other sectors in Denmark.

- The threat of cyber terrorism against the water sector is **NONE**.

Introduction

In light of the global security situation, Denmark is facing an increasingly complex threat landscape. Developments in the physical world impact the cyber domain, and like many other parts of Danish society, the Danish water sector is facing a dynamic threat landscape.

The water sector in Denmark

This threat assessment covers the drinking and wastewater sector in Denmark. The water sector comprises numerous companies of different sizes and for the purpose of this assessment includes companies that treat and supply drinking water, wastewater companies that discharge and clean wastewater, and multi-utility companies that handle several supply types. The collective water sector supplies and handles drinking and wastewater for companies, public authorities and private households. Thus, the water sector also has interdependencies with other critical societal sectors and interconnects with the energy sector through multi-utility companies.

Conversely, the cyber domain may affect the physical world, including the water sector. In late December 2024, a pro-Russian cyber activist hacker group likely compromised operational technology (OT) with weak security mechanisms in a small Danish water utility plant. As a result of the incident, a number of consumers were left without water for several hours and increased water pressure caused a water pipe to burst. However, the attack was quickly detected, and the water supply restored. Nevertheless, the attack is evidence that cyber attacks can affect the supply chain – also in the Danish water sector.

The water sector is critical, not only to the individual consumers but also to private companies and public authorities in other critical societal sectors that rely on the water sector for operational purposes. Critical infrastructure can come the attention of hackers in various ways. State-sponsored hacker groups conduct cyber espionage to obtain access to confidential information, and criminal hackers are using all available means to monetise cyber attacks. By conducting a simple internet search, hackers such as cyber activists, are able to locate internet-facing devices with no or limited security mechanisms, and an organization can thus be breached simply because it is vulnerable.

The Centre for Cyber Security (CFCS) classifies cyber threats into five different categories: cyber crime, cyber espionage, cyber activism, destructive cyber attacks and cyber terrorism and describes the threat landscape based on the purpose of a particular attack. Often, this also provides an understanding of the type of actor behind an attack.

However, it is not always easy to identify the purpose of a cyber attack, and usually, an attack could be multi-faceted. At the same time, there may be overlaps between the different modus operandi of cyber actors. The five different categories thus occasionally overlap in terms of both method and intent, making the analysis process complicated.

This threat assessment clarifies the most probable threat categories, but not the type of attack that the water sector is particularly vulnerable to, or the consequences of a specific attack. This type of expertise is available within the sector, which can use this threat assessment to qualify the collective risk analysis work.

The threat assessment is based on the CFCS's overall domestic and foreign knowledge collection, and operates with a warning time frame of two years. The CFCS uses the DDIS threat levels and probability degrees, which are explained at the end of this threat assessment.

Cyber crime

The CFCS assesses that the threat of cyber crime against the Danish water sector is **VERY HIGH**. Danish Public authorities and private companies will highly likely fall victim to attempts of cyber crime within the next two years. Ransomware attacks in particular pose a threat to the day-to-day operations of the water sector.

Several organizations in the water sector have fallen victim to ransomware attacks that continuously target Danish companies and public authorities. Ransomware-as-a-Service (RaaS) groups in particular are launching ransomware attacks against the European water sector, including in Denmark.

Ransomware-as-a-Service: professional organized criminal forums

Ransomware attacks render data and systems unavailable to the victim, often through data encryption, which holds the data hostage. The criminal actors demand ransom, typically in the form of cryptocurrency, in exchange for granting the victim access to the data.

RaaS is a business model similar to the platform economy found in legal markets. RaaS is based on criminal operators running a platform that they make available to other criminal actors, known as affiliates, who use the platform for ransomware attacks.

The model allows even affiliates with little technical skills to make a profit on ransomware attacks even though the RaaS operators take the largest share of the ransom payment. LockBit 3.0, Black Basta and Cactus are examples of RaaS operators.

A ransomware attack may have repercussions for the individual victims, both in the form of potential leaks of sensitive data and economic loss but potentially also for society at large. For example, a ransomware attack in the water sector may have repercussions for the supply security if the attack affects operations.

Criminal hackers may assume that companies that manufacture or deliver vital societal services, including the water sector, are more inclined to pay ransom than other potential targets as vital societal functions in general have a low tolerance for operational downtime.

The CFCS assesses that the groups behind ransomware attacks often are opportunistic in their targeting. When the groups attack targets, for example in the water sector, they aim to breach organizations that they view as attractive targets. The goal for the groups is mainly financial gain rather than making a political statement.

Phishing and spear phishing as attack vectors
In order to conduct a ransomware attack, criminal actors first have to obtain initial access to the victim's systems. They can try to obtain initial access by sending phishing emails to a large number of potential victims. For example, in 2021, several US water utility providers fell victim to a ransomware attack through spear phishing within a period of six months.

Criminal actors use phishing emails to trick recipients into, for example, unsuspectingly granting unauthorized access to IT systems.

Spear phishing is a type of phishing attack that targets specific individuals or organizations. Spear phishing emails are personalized attacks designed to target individual victims rather than a wide net of victims. Spear phishing often requires research into the target organizations or employees.

Phishing and spear phishing are attractive options for criminals as they require fewer technical skill and are designed to attack the part of the supply chain that is the weakest link – the human element. Both phishing and spear phishing emails can seem highly convincing to employees in an organization, who inadvertently and without malicious intent may give criminals access to the systems.

OT systems may become collateral damage
Most of the ransomware types used in attacks by criminal hacker groups are designed to encrypt IT systems. However, an attack on an organization's IT system may affect the company's OT systems used to manage physical operations.

Lacking or inadequate network segmentation between IT and OT systems could make OT systems collateral damage in a ransomware attack that was actually targeting IT systems.

A ransomware attack can potentially affect the delivery of critical services to customers. For example, this could be the case if OT units become infected by the malware, or if the targeted organization opted to shut down production for fear of its OT systems being compromised. Consequently, the organization may be forced to shift to manual operations or completely halt production if manual operations is not possible.

Attacks on software suppliers may also lead to shutdown
Operations may also be affected by a ransomware attack targeting a supplier of OT system software or applications and by the supplier shutting down their services due to fear of the ransomware spreading.

Such a scenario occurred when Norwegian technology company Volue fell victim to a ransomware attack in 2021. The company delivers, among other things, software solutions to utility companies in Europe, including Norway. As a result of the attack and the fear of the ransomware spreading, Volue opted to shut down affected applications providing infrastructure to water facilities that cater to a string of Norwegian municipalities.

The concept of hackers using a supplier as an attack vector is called a supply chain attack. A supply chain attack may affect the supply security in many water utility plants simultaneously if they are clients of the same supplier.

Cyber activism

The CFCS assesses that the threat of cyber activism against the Danish water sector is **MEDIUM**. Even though it is possible that public and private organisations in the water sector will fall victim to a cyber activist attack, the sector is less of a priority target than other parts of Danish society.

As previously described, in late 2024, a small Danish water utility plant was attacked by pro-Russian cyber activists who manipulated the water pressure via the plant's operational systems. As a result of the attack, 450 households were left briefly without water due to low water pressure. Later, approx. 50 households were left without water for several hours as increased water pressure caused a water pipe to burst.

The CFCS assesses that the water utility plant was hit because of low system security and not because the water sector was specifically targeted.

Cyber activists launch DDoS attacks on other parts of society
Despite the above-mentioned attack, activists still mainly launch Distributed Denial of Service (DDoS) attacks against Danish organizations. DDoS attacks are used to target user-facing websites and render them inaccessible. Such attacks are mainly disruptive in nature and are of shorter duration.

The CFCS assesses that at this point of time, the Danish water sector is not a priority target for the pro-Russian cyber activists who continuously launch DDoS attacks against Danish private companies and public authorities. Consequently, the threat level for the water sector is lower than the overall threat level for Denmark.

Regardless of the lower threat, the activist threat landscape is ever-changing as new groups or key issues could emerge in the cyber activist community and quickly intensify. As evidenced by the December 2024 attack, organizations in the water sector could land in the crosshairs of activists without any warning.

The CFCS refrains from naming activists

The objective of activism is to draw attention from the outside world. Cyber activist groups seek publicity in Western media and share Western, including Danish, articles about their attacks. Even though the CFCS is familiar with the names of some of the groups, they will not be mentioned in publications unless they are fundamental to providing an accurate threat picture.

Activists can also use other attack techniques
In addition to the attack on the Danish water utility plant in December 2024, there have also been examples abroad of activist groups claiming destructive cyber attacks on water utility plants. These claims are often made in connection with war or conflict, for example the conflict between Israel and Hamas. However, the number of this type of attack is lower compared to the numerous DDoS attacks that regularly hit targets in Denmark or in the West.

The CFCS assesses that cyber activist attacks with destructive effects are opportunistic in terms of target selection and strike targets that have poor protection. Still, this type of destructive cyber attacks is more demanding to carry out than the attacks usually launched by cyber activists. In many cases, it is also difficult to determine whether the attacks have actually taken place and whether they have had any real impact.

The CFCS assesses that just like other types of activism, real and false cyber activist attacks with destructive effects are intended to draw public attention to the activists' cause.

Cyber activists across the world have also targeted victims with defacement attacks in which they alter the visual appearance or change the content of a website, and hack and leak attacks in which sensitive data is stolen and leaked to cause reputational damage to the affected organization.

Cyber activists are part of the new norm
The threat of cyber activism against Danish private companies and public authorities became part of the new norm following Russia's invasion of Ukraine. The threat should be seen against the backdrop of Denmark's role as a contributor of military support for Ukraine and as a member country of the EU and NATO. Pro-Russian activists continuously attack private companies and organizations in Europe and NATO that they view as symbolic of Western support for Ukraine.

Cyber activism is typically motivated by ideological or political concerns and is for the most part carried out independently of states. However, it can be difficult to assess a cyber activist's affiliation with foreign states. In some cases, it is thus difficult to determine whether cyber activists are acting on their own initiative or on that of a state.

Destructive cyber attacks

The CFCS assesses that just as the threat to Denmark in general, the threat of destructive cyber attacks against the Danish water sector is **MEDIUM**. The above-mentioned attack on a Danish water utility plant in 2024 falls within the CFCS' definition of a destructive cyber attack, although the consequences were limited.

The threat of destructive cyber attacks against Denmark primarily emanates from Russia, which is willing to use hybrid means with destructive effects against European NATO countries. The CFCS assesses that this willingness to take risks also includes destructive cyber attacks against the Danish water sector. For years, Russian state-sponsored hacker groups have had the capabilities to launch destructive cyber attacks.

The CFCS assesses that many types of organizations in critical societal sectors could become targets of destructive cyber attacks, including organizations in the Danish water sector. Even though the threat mainly comes from Russia, Iran also poses a potential threat.

The threat from non-state hackers

The CFCS assesses that some non-state hackers are capable of launching destructive cyber attacks with limited impact. The attacks can have different objectives, for instance drawing attention to a cause or an agenda, which is a main characteristic of cyber activism. The CFCS assesses that the December 2024 destructive cyber attack on the Danish water utility plant was an example of just this.

Even though destructive cyber attacks from non-state hackers can support nation state interests, it does not mean that these actors work directly for the state. Pro-Russian cyber activists like the ones who launched a destructive cyber attack on the Danish water sector in 2024 are a good example of how the actions of non-state hackers can support nation state interests. However, the CFCS assesses that some pro-Russian cyber activists are linked to the Russian state.

The objective of destructive cyber attacks is to sway opinion

The CFCS assesses in general that potential destructive cyber attacks will primarily be aimed at swaying the population and decision-makers, for instance by weakening Danish support for Ukraine. The specific physical impact of the attacks will likely be secondary to whether the attacks are able to generate attention.

It is less likely that Russia in the current situation will launch destructive cyber attacks with serious and far-reaching consequences for critical societal functions, including attacks on the Danish water sector. Even though such attacks are currently less likely, the CFCS assesses that Russian hacker groups are preparing to be able to launch this type of destructive attacks on critical infrastructure in Denmark in the event of an escalating crisis or war. Consequently, the threat of such attacks could rise with little or no warning.

However, small-scale cyber attacks could have serious consequences for the Danish water sector, including attacks with limited impact on supply security. Even in the event that destructive cyber attacks have no consequences for the supply security, they could cause uncertainty and affect society at large.

Weak security precautions a potential entry point for attacks

The water sector could be an interesting target for hacker groups for several reasons. It is likely that the selection of targets for potential destructive cyber attacks will be determined by established entry points and ease of accessibility. For instance, weak security measures in OT systems could become of interest to opportunistic hackers. The CFCS assesses that weak security measures were the reason why a Danish water utility plant fell victim to a cyber attack in December 2024.

At the same time, the sector is crucial to civilian and military infrastructure. As a result, the sector could become a target of interest to state hackers as it delivers services to different sectors and authorities, including manufacturers of pharmaceuticals and critical technology. It is possible that the water sector could fall victim to cyber espionage attempts in preparation for future destructive cyber attacks in a bid to weaken other critical sectors in the event of an escalating crisis or war.

State-sponsored hacker groups could use cyber espionage to install so-called backdoors on compromised systems.

Backdoors – electronic shortcuts in systems

A backdoor is an unauthorized way to gain access to a system, for instance through a software error or configuration. A backdoor can be deliberately installed by a person who has had access to the development of the software or the configuration of the system. A backdoor can also be part of malware on the system.

Cyber espionage will often precede a destructive cyber attack but is not a prerequisite for all attacks. In some cases, hackers can launch simple destructive cyber attacks with little preparation against systems with weak security measures in place.

States can try to cloak their involvement in destructive cyber attacks

Foreign states can try to cloak their involvement in destructive cyber attacks, making it harder for countries affected by hybrid activities to respond. States can use different ways to cloak their connection to an attack.

The CFCS assesses that in the current situation Russia will try to cloak its involvement in potential destructive cyber attacks, for example by launching attacks mimicking criminal ransomware attacks, in which data is encrypted but subsequent decryption is not possible.

State-sponsored hackers can also try to conceal their involvement in destructive cyber attacks by posing as activist hackers, for instance by creating websites or accounts on different platforms posing as cyber activists claiming responsibility for destructive cyber attacks. This phenomenon is known as ’faketivism’. In popular terms, faketivism is when a state-sponsored group launches cyber attacks that look like cyber activism.

Cyber espionage

The CFCS assesses that the threat of cyber espionage against the Danish water sector is **MEDIUM**. It is possible that the sector will fall victim to cyber espionage attempts within the next two years.

The CFCS assesses that the Danish water sector is not a priority espionage target to the same extent as other sectors in Denmark. It is likely that the threat primarily comes from wide espionage campaigns against multiple victims, and that the threat is not directed specifically at the Danish water sector.

However, the CFCS assesses that foreign states, including Russia and China, have a persistent interest in the Danish energy sector. Multi-utility companies which deliver energy as well as manage drinking and waste water could thus face a greater cyber espionage threat than the rest of the water sector.

The objective of cyber espionage varies
Foreign states conduct cyber espionage for different purposes. State-sponsored hacker groups, for instance, can conduct cyber espionage for the purpose of gaining access to knowledge that could support technological development objectives and thus promote the economic interests of states.

State-sponsored hackers also conduct cyber espionage if the opportunity presents itself, for instance as a result of making use of a widely known vulnerability. In this way, the water sector could become a victim of cyber espionage without being the intended target.

In general, foreign states like Russia and China have a persistent interest in conducting cyber espionage against organizations in Europe, including in Denmark. This interest also applies to critical infrastructure organizations. Both Russia and China have significant cyber capabilities and both states use cyber espionage to gain access to different types of knowledge held by their victims.

Attempts of cyber espionage can be directed against the email systems used by an organization. If a hacker group manages to compromise an email system, they can use this access to collect information on the organization and its employees – knowledge that the hacker group can use to send spear phishing emails from the victim's system to other network users.

State-sponsored hacker groups can also use entry points into victim systems to launch other types of cyber attacks. For instance, a critical infrastructure system which has been compromised for the purpose of cyber espionage can also be used in preparation for potential future destructive cyber attacks in the event of a war or conflict. However, as mentioned, not all destructive cyber attacks require prior cyber espionage.

USA: Chinese state-sponsored hackers were planning attacks on US critical infrastructure

In February 2024, US authorities announced that a Chinese state-sponsored hacker group known as Volt Typhoon had compromised the IT systems in several critical sectors in the United States, including the water sector.

According to the US authorities, the activity of the hacker group in the victim systems indicates that the main purpose was not exclusively espionage. The purpose of the attacks was rather to gain access within the compromised systems that would allow the hacker group to launch destructive cyber attacks against US critical infrastructure in the event of a war or conflict. According to the authorities, it was clear that Volt Typhoon had positioned itself in the victim systems in such a way that would allow it to move laterally to infect connected OT systems should it become necessary.

The US authorities have observed indications that Volt Typhoon had maintained footholds within some victim IT environments for at least five years.

Cyber terrorism

The CFCS assesses that the threat of cyber terrorism against the Danish water sector is **NONE**. It is highly unlikely that public authorities and private companies in the Danish water sector will fall victim to cyber terrorism attempts within the next two years.

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

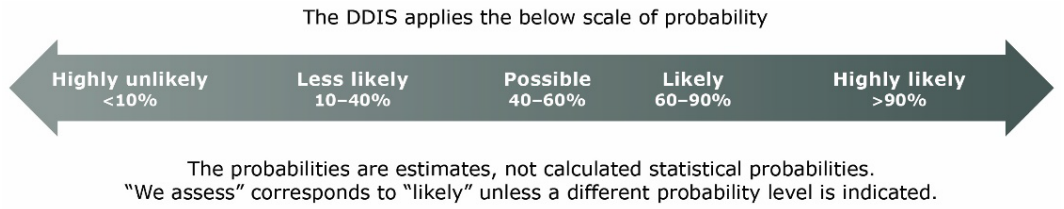
The CFCS assesses that militant extremists have neither the intention nor capability to conduct a cyber attack on the water sector in Denmark with the same impact as conventional terrorism.

Threat levels

The Danish Defence Intelligence Service uses the following threat levels.

NONE	There are no signs of a threat. There are no actors with both the capacity and intention for attacks/harmful activity.
LOW	There are one or more actors with the capacity and intention for attacks/harmful activity. However, either the capacity or the intention or both are limited.
MEDIUM	There are one or more actors with the capacity and intention for attacks/harmful activity. However, there are no indications of specific planning of attacks/harmful activity.
HIGH	There are one or more actors that have the capacity for and are specifically planning attacks/harmful activity or that have already carried out or attempted attacks/harmful activity.
VERY HIGH	There is either information that one or more actors are initiating attacks/harmful activity, including information about time and target, or that one or more actors are continuously initiating attacks/harmful activity.

An applied threat level reflects the DDIS' assessment of the intention, capacity and activity of one or more actors based on the available information.



Other relevant publications

The Centre for Cyber Security publishes threat assessments and cyber security guides on a regular basis. Below is a list of publications that could be relevant for public authorities and private companies in the Danish water sector. All publications are available at the CFCS website.

The cyber threat against Denmark 2024
In this annual threat assessment, the CFCS describes the general cyber threat of cyber crime, cyber espionage, cyber activism, destructive cyber attacks and cyber terrorism against Denmark.

The cyber threat against the Danish energy sector
The threat assessment ”The cyber threat against the Danish energy sector” describes the different cyber threats facing the Danish energy sector.

Guide to counter ransomware attacks
The guide ”Reduce the risk of ransomware” (available in Danish only) presents a number of recommendations that organizations may follow to reduce the risk of falling victim to a ransomware attack. The guide also provides recommendations on how to handle a potential ransomware attack once the organization has been breached.

How to protect against DDoS attacks
The guide ”Protection against DDoS attacks” (available in Danish only) presents a number of recommendations on how organizations can protect themselves against DDoS attacks.

Guide on how to counter phishing attacks
The guide ”Protect your organization against phishing attacks” (available in Danish only) provides recommendations to organizations on how to counter threat from phishing emails.

Guide on cyber security in supplier relationships
The guide ”Cyber security in supplier relationships” provides recommendations on how to establish and maintain good cooperation between the client and the supplier of IT operations throughout the cooperation period, from supplier selection to termination.