CENTRE FOR
CYBER SECURITY

Threat assessment

The cyber threat against land and air transport

3rd edition September 2021

Table of contents

CENTER FOR
CYBERSIKKERHED

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

3rd edition September 2021

The cyber threat against the land and air transport sector

This threat assessment outlines the cyber threats against the Danish transport sector. The Danish transport sector is vital to the functioning and stability of Danish society. This assessment is intended to inform decision-makers within the Danish transport sector of the cyber threat in order to improve cyber security measures. The threat assessment can be used in the risk assessment efforts of the sector and in other efforts related to the national strategy for cyber and information security for the Danish transport sector.

This assessment was updated in September 2021. Adjustments have been made to the chapter on cyber espionage. The threat level for cyber espionage has been raised to **VERY HIGH**. Furthermore, minor editorial changes have been made in the other chapters.

Previously, the threat assessment was updated in June 2020 with changes to the cyber terrorism chapters, reflecting the adjusted threat levels in the 2020 annual national threat assessment ”The cyber threat against Denmark”. Also, destructive cyber attacks have been assigned a threat level corresponding to the level determined in the annual national threat assessment.

Key assessment

- The threat of cyber crime against the Danish transport sector is **VERY HIGH**. Cyber crime aimed at extorting money from private companies and public authorities pose a particular threat. Cyber crime may, at worst, disrupt operations in the transport sector and potentially undermine client trust.

- The threat of cyber espionage is **VERY HIGH**. Cyber espionage is mainly aimed at organizations within the aviation sector and ports. The threat of cyber espionage against the Danish railway sector is only **HIGH**.

- The threat of destructive cyber attacks against the Danish transport sector is **LOW**. However, the Danish transport sector can potentially be affected by destructive cyber attacks abroad.

- The threat of cyber activism is **LOW**. Cyber activists often pursue specific issue agendas, potentially causing the threat against the sector to rise without or at short notice. The aviation sector, in particular, has fallen victim to cyber activism worldwide.

- The threat of cyber terrorism is **NONE**. Cyber terrorism presupposes technical skills and organizational resources that militant extremists do not possess at this point. Also, their intent to conduct cyber terrorism is limited.

Introduction

This assessment outlines the overall cyber threat directed at the Danish transport sector. In this assessment, the transport sector covers land and air transport of persons and goods, including infrastructure and services facilitating the mobility of goods and passengers. Drones and ports are also included in this assessment. The maritime sector, however, will not be dealt with in this assessment, as the Danish maritime sector is considered as a separate independent sector. The Danish transport sector consists of several components each with their own individual characteristics and vulnerabilities. This threat assessment analyses the cyber threat directed at the transport sector as a whole, making only limited distinctions between the different components of the sector. Also, transport operations conducted by Danish defence units are not included in this threat assessment.

In addition to being an integral part of everyday life in Denmark, other sectors rely on the transport sector, emphasizing the importance of the sector's cyber resilience.

Cyber attack surfaces are expanding as technological development makes the transport sector increasingly dependent on digital solutions. Vehicles, aircraft and trains are increasingly connected to or controlled by IT systems. At worst, hackers may exploit this connectivity in an attempt to disrupt land and air transport availability or security. IT outages in airline companies or airports abroad that are not the result of cyber attacks indicate how reliant segments of the transport sector already are on systems that are potentially vulnerable to cyber attacks.

This threat assessment is based on the DDIS Centre for Cyber Security's (CFCS) general knowledge of cyber threats and on analyses of examples of cyber attack incidents targeting the transport sector.

This assessment is based on the current threat landscape and operates with a warning horizon of up to two years. Cyber threats are dynamic and constantly changing, affecting society as a whole as well as individual authorities and private companies. Threat and probability level definitions are listed at the end of the assessment.

The exact number of cyber attacks against public authorities and private companies in the transport sector is difficult to determine as not all cyber attacks are reported to the relevant authorities – either because the targeted organization wants to avoid drawing attention to the cyber attack or because the attack has yet to be detected. A new cyber incident reporting system, likely increasing national awareness of cyber attacks against critical infrastructure, was introduced by law in May 2018.

What are cyber threats?
The DDIS Centre for Cyber Security defines cyber threats as threats from cyber attacks in which an actor tries to cause disruption or gain unauthorized access to data, systems, digital networks or digital services. Use of the Internet for other purposes that may have a serious impact on society such as online sale of illegal goods and services is not included in our definition of cyber threats.

Cyber threats are multi-faceted. In this assessment the focus is on the end goal of different types of cyber attacks such as cyber espionage, cyber crime, cyber activism or cyber terrorism. Also, we will assess the threat of destructive cyber attacks.

The threat levels in this assessment are based on an analysis of the actors' intention and cyber capabilities in terms of available human and material resources ranging from skilled hackers and malware developers and information on targets that is useful in social engineering campaigns to IT infrastructure, time, funds and access to information. Thus, the scope of an actor's cyber capabilities depends on available resources as well as the actor's ability to exploit them.

Cyber crime

The threat of cyber crime against the Danish transport sector is **VERY HIGH**. Cyber crime covers activities in which the perpetrator uses cyber attacks to commit financially motivated criminal activities.

Cyber criminals are resourceful in their attempts to make financial gain and employ a wide range of cyber attack tactics, some of which are becoming increasingly sophisticated and complex. Cyber crime aiming to extort money from private companies and public authorities poses a particular threat. This specific brand of cyber crime often comes in the shape of ransomware attacks, although cyber criminals may resort to other extortion tactics, for instance, launching DDoS attacks or threatening to leak stolen data.

Extortion attempts by means of ransomware are particularly harmful as they may, at worst, disrupt operations in the transport sector. A case in point is the 2016 ransomware attack against the San Francisco Municipal Transportation Agency in the United States which disrupted the agency’s ticketing systems, allowing passengers to ride for free for three days. A 2018 ransomware attack against the Colorado Department of Transportation encrypted thousands of workstations. In September 2018, the Port of San Diego fell victim to a ransomware attack, causing system and service downtime, although standard port operations were able to continue. The attack took place shortly after the cyber attack against Barcelona Port which caused similar disruptions. The 2017 global WannaCry ransomware attack also affected the transport sector, including Deutsche Bahn and FedEx.

Some cyber criminals threaten to overload company websites or other Internet-facing services with so-called DDoS attacks, unless the victim pays ransom. Usually, such threats are not directed at the transport sector, meaning that the sector is only exposed to a potential threat. DDoS attacks may disrupt the transport sector, for instance by making ticket sales or websites unavailable. DDoS attacks have in a few instances abroad resulted in flight and train delays. As the motives behind these attacks are unclear, it is difficult to directly categorize them as extortion attempts, but the incidents indicate that such attacks could potentially take place.

Hackers may also steal data from public authorities and private companies in the transport sector for extortion purposes. Theft of personal and financial data may undermine consumer confidence in compromised companies, giving criminal hackers an incentive to steal data for extortion purposes.

DDoS attacks against the transport sector
Distributed Denial of Service (DDoS) refers to cyber attacks in which the attacker exploits compromised electronic units to flood the targeted website (webserver) with data traffic, making the website or network unavailable for legitimate traffic as long as the attack is in progress.

In May 2018, a DDoS attack against the Danish state rail operator DSB shortly disrupted the DSB ticketing system. In 2013, DSB fell victim to a series of DDoS attacks, making the company's website, ticket machines, app, etc. unavailable for a limited time. In 2017, a DDoS attack against Sweden's Transport Administration (Trafikverket) brought down the IT systems monitoring railway traffic, causing train delays. In 2015, a DDoS attack against Warsaw's Chopin Airport in Poland caused flight delays due to system breach.

The motives behind these attacks are unclear, but theories include harassment, testing of the compromised organizations' infrastructure and security level or criminals wanting to demonstrate their DDoS techniques and skills to potential buyers.

Fraud in the form of Business Email Compromise scams (BEC scams) remains a threat across sectors. BEC scams aim to trick private companies and public authorities into wiring funds through false wire transfer requests. The criminals typically impersonate in-house executives in order to exploit employee loyalty. This type of fraud is often referred to as CEO fraud. BEC scams may result in significant financial losses for the victim.

In 2016, the Austrian aerospace manufacturer Fischer Advanced Composite Components AG lost EUR 42 million to a BEC scam. BEC scams may, at worst, affect the availability of transport services, for instance, if a supplier of traffic services or of critical components for the transport sector losses liquidity to the extent that it is unable to deliver these services.

Criminals also launch other forms of fraudulent attacks against the transport sector, for instance, breach and misuse of frequent flyer miles and car-sharing service accounts.

Also, cyber criminals target financial and personal data with the intent to exploit them for financial gain. These criminals may attempt to compromise companies in the transport sector that have access to such information. Several hacker groups are systematically targeting payment systems across sectors worldwide. Theft of personal and financial data may undermine consumer confidence in compromised companies.

Criminals also spread malware that tap into the computing power of victim devices for cryptocurrency mining purposes. Cryptocurrency mining malware may affect IT networks and create disruptions in operations, delays in response times and, at worst, outage. In 2018, media reports revealed that Tesla’s Amazon Web Services cloud account was breached by hackers who used computing power for illicit cryptocurrency mining. In connection with the breach, hackers had gained unauthorized access to sensitive information related to test cars.

Cyber espionage

The threat of cyber espionage against the Danish transport sector is **VERY HIGH**. The threat is mainly directed at the aviation sector and ports that are part of the transport sector. As a result, the same threat level is not applicable to the Danish transport sector as a whole. CFCS assesses that the threat against the railway sector remains **HIGH**.

CFCS assesses that in recent years, cyber espionage activities against the transport sector, both in Denmark and abroad, have increased. CFCS assesses that foreign states have shown a continued interest in transport authorities.

Espionage against the Danish transport sector may be motivated by security political interests. Foreign states may also show an interest in the parts of the Danish transport sector that are tasked with supporting Danish defence or foreign states' military, providing transport of military personnel for missions abroad or allowing military use of civil traffic hubs such as airports and ports. Information collection on the transport sector that is part of Danish critical infrastructure may also be used to launch destructive cyber attacks or physical attacks against the transport sector.

Cyber espionage against the transport sector may also be motivated by financial interests. By stealing information in connection with large investments in the transport sector, foreign states may provide their own national companies operating on the international market with a competitive edge. Certain foreign states also conduct cyber espionage against private companies cooperating with the foreign state's national companies or public authorities.

Espionage activities may secure knowledge that is exploited to gain access to new technologies that may prove useful to strengthening and developing a given states' national transport sector. Hence, foreign states may have an interest in conducting cyber espionage against private companies and research institutions developing new technologies or components to the transport sector. For example, private companies associated with aerospace both in Denmark and abroad have been targeted by cyber espionage. Technologies and projects related to other investment heavy and sophisticated transport systems, such as high-speed trains, are also potential cyber espionage targets.

The transport sector also has access to Personally Identifiable Information (PII) on passengers and travel patterns that foreign intelligence services may use to monitor certain individuals.

Organizations in the Danish transport sector may also be exposed to cyber espionage conducted through suppliers, such as software suppliers. In 2021, thousands of organizations fell victim to the so-called SolarWinds attack, including SAS Airlines. Hackers had covertly inserted a backdoor on SAS' systems, although the company publicly stated that it had not detected any signs of backdoor exploitation.

Destructive cyber attacks

The threat of destructive cyber attacks against the transport sector is **LOW**, meaning that the transport sector is less likely to become target of destructive cyber attack attempts within the next two years.

The threat may increase in connection with a heightened political or military conflict, where Denmark are involved.

A number of countries have established cyber capabilities that may potentially be used to launch destructive attacks against critical infrastructure such as the transport sector. Destructive cyber attacks are defined as cyber attacks that could potentially result in death, personal injury, extensive property damage, and/or destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

It is possible that Danish public authorities and private companies may find themselves collateral victims of destructive cyber attacks against targets outside of Denmark, especially Danish private companies in the transport sector operating in conflict areas such as Ukraine and Saudi Arabia where foreign states or organized hacker groups with capabilities to launch destructive cyber attacks have interests at stake.

The transport sector abroad has fallen victim to destructive cyber attacks that have resulted in minor disruptions affecting the availability of the transport sector. In June 2017, several transport companies abroad were infected by the NotPetya attack, which was a destructive cyber attack disguised as a ransomware attack. In Ukraine, Kiev metro and two airports were affected by the attack, and logistics companies FedEx, Deutsche Post DHL Group and DAMCO suffered large financial losses from the attack. In 2017, the Ukrainian transport sector was compromised by the so-called BadRabbit malware, causing flight delays in Odessa Airport and disrupting the ticketing system in Kiev metro, among other things.

IT security specialists and national security agencies have demonstrated how vehicles or aircraft may be breached by hackers, ultimately enabling them to control central systems. Most of these attacks are only successful under the right conditions. However, it is possible that state-sponsored hackers, among others, have the capabilities to exploit the vulnerabilities.

Cyber activism

The threat of cyber activism against the Danish transport sector is **LOW**, meaning that the transport sector is less likely to become target of cyber activism attempts within the next two years.

Globally, the number of cyber activist attacks has fallen in recent years. Cyber activists rarely focus their attention on Danish public authorities or private companies. Cyber activists are typically motivated by specific issue agendas, potentially causing the threat against the transport sector to rise without or at short notice.

Cyber activism is typically ideologically or politically motivated. Cyber activists often target individuals or organizations which they deem opponents to their cause. The transport sector is vital to everyday life in Denmark, and attacks against public transportation may draw attention to hacktivist causes. The aviation sector, in particular, has fallen victim to cyber activism across the world. In recent years, airport and airline websites have been targeted in a series of cyber activist attacks such as defacement attacks. However, CFCS has no knowledge of Danish victims of cyber activism in the aviation sector.

Certain hacker groups and individuals in cyber activism networks have significant cyber attack capabilities. Even though cyber activist attacks are a rare occurrence, the threat may rise overnight. Hackers are able to mobilize quickly in connection with an issue, for example, in the wake of political debates and incidents involving the transport sector. A case in point was the 2016 and 2017 DDoS attacks against the websites of Vienna and Rotterdam airport respectively. In both incidents, the attacks were likely related to political issues in connection with Turkish nationals' entry into the countries concerned.

Even if Danish authorities and private companies are not directly involved in the controversy that has grabbed the activists' attention, they still risk becoming targets of cyber activism simply because they might be considered symbolic targets. Cyber activist attacks may also be random in the sense that hackers tend to attack easily accessible or vulnerable targets.

Another form of attack technique is hack and leak of sensitive data. For example, in 2016, a cyber activist leaked a large amount of sensitive data, claiming that it was stolen from a Russian airline in protest against Russia's actions in Ukraine and Syria.

Cyber terrorism

The threat of cyber terrorism against the Danish transport sector is **NONE**.

As a result, it is highly unlikely that the Danish transport sector will fall victim to cyber terrorism attempts within the next two years.

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

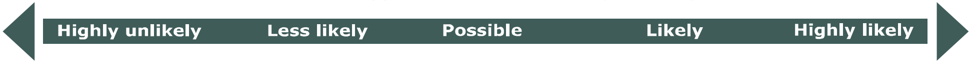
Cyber attacks of such serious magnitude presuppose technical skills and organizational resources that militant extremists do not possess at this point in time. At the same time, their intent to conduct cyber terrorism is very limited.

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 highly unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are less 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 highly likely.

The DDIS applies the below scale of probability



Highly unlikely **Less likely** **Possible** **Likely** **Highly likely**

”We assess” corresponds to ”likely” unless a different probability level is indicated.

Further relevant readings

The Centre for Cyber Security (CFCS) continuously publishes guidance and threat assessments. Highlighted below are a number of publications of particular relevance to the Danish land- and air transport sector. All publications are available on CFCS' website.

The cyber threat from intentional and unintentional insiders
CFCS has prepared the threat assessment 'The Cyber Threat from Intentional and Unintentional Insiders' in cooperation with the Danish Intelligence and Security Service (PET). The threat assessment addresses the cyber threat and presents recommendations for preventive measures. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/insiders/

The threat from cyber attacks against suppliers
The threat assessment "Cyber Attacks against Suppliers" focuses on the cyber threat against suppliers and the supply chain. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/supply-chain/

Guide on managing supplier relations
The guide "Informationssikkerhed i leverandørforhold" (only available in Danish) contains a set of recommendations on how to manage the relationship between organizations and suppliers. Read the guide here:
https://cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

The cyber threat from phishing emails
The threat assessment "The Cyber Threat from Phishing Emails" gives a detailed outline on how hackers attempt to use phishing and spear phishing emails to exploit companies or trick them into passing on sensitive information. Read the assessment here: https://cfcs.dk/en/cybertruslen/threat-assessments/phishing/

Guide on how to counter phishing
The guide "Vejledning: Phishing - Beskyt organisationen mod phishingangreb" (only available in Danish) is intended for executives, and it presents a series of concrete recommendations that contribute to organizations' efforts to protect against and counter phishing attacks. Read the guide here:
https://cfcs.dk/da/forebyggelse/vejledninger/phishing/

Cooperation between cyber criminals
The threat assessment "Do Cyber Criminals Dream of Trusting Relationships?" describes how established cooperation relationships, division of labour and exchange of services inside the criminal environment contribute to creating a very high threat of cyber crime, in general, and targeted ransomware attacks, in particular. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/organised-cyber-crime/

The threat from targeted ransomware attacks
The threat assessment ”Criminals Tighten the Digital Thumbscrew” describes the threat of targeted ransomware attacks that may potentially have serious repercussions for an organization. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/double-extortion/

Guide to counter ransomware attacks
The guide “Reducér risikoen for ransomware” (only available in Danish) presents a number of recommendations that organizations may follow to reduce the risk of ransomware attacks. Also, the guide provides recommendations on how to handle a ransomware attack once an organization has been hit. Read the guide here:
https://cfcs.dk/da/forebyggelse/vejledninger/ransomware/

The anatomy of targeted ransomware attacks
The investigation report “The Anatomy of Targeted Ransomware Attacks” outlines how a typical targeted ransomware attack plays out and presents specific recommendations for protective measures. Read the report here:
https://cfcs.dk/en/cybertruslen/reports/the-anatomy-of-targeted-ransomware-attacks/

Cyber attacks against HR departments
The threat assessment ”HR Departments are also Hit by Targeted Cyber Attacks” highlights how hackers attempt to use HR departments as an easy entry point to compromise organizations. The assessment also comprises recommendations on how organizations can provide support to their HR departments, including both technical measures and awareness. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/cyber-threat-against-hr-departments/