CENTRE FOR CYBER SECURITY

THREAT ASSESSMENT

The cyber threat against the Danish railway sector

FEBRUARY 2021

CONTENT

CENTRE FOR CYBER SECURITY

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

Cover illustration: Jens Christian Top/Scanpix Denmark

First revision February 2021.

Centre for Cyber Security (CFCS) raises the threat level for cyber activism to HIGH for the Danish transport sector.

CFCS is raising the threat level for cyber activism against the Danish transport sector from **MEDIUM** to **HIGH**. This implies that organizations within the sector are likely to become targets of cyber activism within the next two years.

CFCS raised the overall threat level for cyber activism against Denmark on January 31st 2023. CFCS assesses that this increased threat from cyber activism also applies to the Danish transport sector.

CFCS raised the threat level based on a combination of the pro-Russian cyber activists' significant level of activity against NATO member states, including Denmark, and their more formalized modus operandi and increased capacity.

The threat assessment's core text is not updated, and the section on cyber activism does not reflect the current threat level.

For additional information on why the threat level from cyber activism is raised as well as how the threat manifests itself, please refer to the threat assesment "The CFCS raises the threat level of cyber activism against Denmark from MEDIUM to HIGH" published on January 31st 2023.

The threat assessment is available on www.cfcs.dk/en

The cyber threat against the Danish railway sector

This threat assessment presents an outline of the cyber threat against the Danish railway sector and may be used to form part of the sector's risk assessment procedures. The intended audiences of this threat assessment mainly include management and IT employees with Danish railway operators and infrastructure managers.

Key assessment

- The threat of cyber crime against the Danish railway sector follows the general cyber threat level against Denmark, which is assessed as **VERY HIGH**. Consequently, it is highly likely that private companies or public authorities within the Danish railway sector will fall victim to cyber crime attempts. Though the strongest threat emanates from ransomware attacks, the sector, for instance, also experiences cyber attacks against suppliers and spear-phishing attempts.

- The threat of cyber espionage against the Danish railway sector is **HIGH**. As a result, the sector will likely fall victim to cyber espionage attempts. For instance, foreign states can have an interest in compromising railway sector organizations in connection with large tenders.

- The threat of destructive cyber attacks against the Danish railway sector is **LOW**. Thus, it is less likely that foreign states will direct destructive cyber attacks against Danish critical infrastructure, including the railway sector.

- The threat of cyber activism against the Danish railway sector is **LOW**. It is less likely that railway sector companies and authorities will be targeted by cyber activists. However, the threat may increase should individual organizations become embroiled in a political controversy or in connection with negative mention in the press.

- The threat of cyber terrorism against the Danish railway sector is **NONE**. Militant extremists have, in a few instances, expressed intentions of conducting cyber terrorism but currently lack the capabilities to carry out cyber terror attacks.

About the threat assessment

This threat assessment describes the cyber threat against the Danish railway sector, analysing the threat against Danish passenger and freight operators as well as infrastructure managers, including light rails, metros and private railways.

The assessment is based on analysis of Danish and international examples of cyber attacks against operators and infrastructure managers combined with knowledge of threat actor capabilities and intentions. The assessment has been prepared in collaboration with Danish railway sector organizations.

The threat assessment provides an outline of the current threat landscape and its projected development in the short term – short term being two years for the purposes of this assessment. Due to the inherently dynamic nature of the cyber threat, the threat picture may change without warning, both generally and specifically in relation to the railway sector. The assessment uses the Danish Defence Intelligence Service's threat levels and scale of probability, which are explained at the end of the assessment.

Cyber crime poses the biggest threat to the railway sector, with ransomware attacks being the most serious threat to the railway sector as a whole due to their continued prevalence across critical sectors. In addition, a well-executed ransomware attack could carry serious economic consequences and, at worst, cause disruption of railway services. In addition, attacks via suppliers, Business Email Compromise scams (BEC scams), and spear-phishing attempts also pose a significant threat to actors in the sector.

Cyber crime

The threat of cyber crime against the Danish railway sector is **VERY HIGH**. As the threat against the sector follows the general cyber crime threat level against Denmark, the Centre for Cyber Security (CFCS) assesses it highly likely that the sector will fall victim to cyber crime attacks within the two-year horizon of this threat assessment.

The threat emanates from financially motivated criminal individuals and networks. As most cyber crime attacks are opportunistic, the Danish railway sector may be targeted if the threat actors see the possibility of financial gain.

The high threat level is underpinned by trends among cyber criminals who are increasingly cooperating and exchanging services among themselves under market-like conditions. This practice is known as Crime-as-a-Service and enables criminals to buy access, tools and infrastructure against payment. In this way, criminals can launch cyber attacks without having to develop the tools themselves. This type of cooperation increases the specialization and effectiveness of the cyber criminal community, creating robust and organized supply chains, which facilitate targeted ransomware attacks, among other things.

Serious ransomware attacks threaten the Danish railway sector

Ransomware is a serious threat to the Danish railway sector, as it remains a popular tool amongst cyber criminals, who launch attacks across sectors. In addition, ransomware attacks against the Danish railway sector are serious as they, at worst, may cause disruption in services or delays in the critical infrastructure.

Ransomware attacks involve cyber criminals gaining access to an organization's network and subsequently encrypting the organization's data, rendering it inaccessible. This allows the cyber criminals to hold organization data, systems and units hostage and subsequently demand ransom, paid in cryptocurrency, to unlock the encrypted data.

Legacy systems create risks

The widespread use of legacy systems is a special challenge facing the Danish transport sector, including the railway sector. Legacy systems may be vulnerable to cyber attacks, as the systems often date back to before cyber security was a concern. As a result, it is a complicated or very costly affair to update or change the systems. At times, it is even impossible to update the systems or ensure they meet today's IT security standards. Legacy systems thus provide a potential attack surface across all types of cyber threats.

Some cyber criminal networks target large organizations on the reasoning that the bigger the victim, the larger the profit. As they often perform critical societal functions, large operators and infrastructure managers are attractive targets to such criminal networks, because hackers expect such authorities and companies to be more inclined to pay very large ransoms.

The travel information systems of Deutsche Bahn where hit during the global WannaCry ransomware attack in 2017.
Photo: P. GOETZELT/Scanpix Denmark

The attacks are targeted in the sense that the hackers first spend time compromising the victim before working their way further into the organization network in order to inflict the most damage possible. Several days may lapse between initial access and ransomware deployment. Also, it is likely that some criminal hackers sell the initial access to other criminal hackers.

However, large and critical societal actors are not the only targets of interest to cyber criminals. CFCS is aware of incidents in which small and medium-sized companies in the Danish transport sector have caught the attention of cyber criminals that were scanning broadly for weaknesses without being branch specific. Ultimately, for the hackers it all comes down to finding the easiest path to securing ransom payment.

In early 2020, US railroad construction and maintenance firm RailWorks Corporation announced that it had been hit by a ransomware attack. During the attack, which the company referred to as a sophisticated cyber attack, the hackers managed to compromise the company's systems and inject malware. In addition, the hackers gained access to personally identifiable information belonging to current and former employees as well as suppliers.

Cyber attacks against suppliers may prove an easy point of entry

Suppliers are attractive targets to hackers, as the compromise of one supplier may act as an entry point to numerous organizations, to the supplier's customer data or provide access to vital parts of a sector's infrastructure. Suppliers deliver vital services such as cloud solutions, data storage and other IT services.

Suppliers often have unhindered access to many of their customer's networks and data. Compromise of a single supplier may thus enable an actor to move unchecked across several customer networks and data. Cyber attacks against suppliers may thus be based on numerous motivations, including espionage or financial gain.

The biggest cyber attack in the world was launched through a supplier
In December 2020 the cyber security firm FireEye discovered one of the most comprehensive cyber attacks in history.

The attack was executed by compromising the company SolarWinds, who delivers software to organizations all over the world. The hackers applied a malicious code to one of SolarWinds legitimate software updates called Orion. Almost 18.000 costumers all over the world downloaded the compromised update, and the malicious code gave the hackers the initial entrance to the systems of the victims.

CFCS knows of several cyber attack incidents against suppliers to the railway sector in Denmark, including a major hacker attack in 2020 against a supplier to Aarhus Light Railway. The attackers stole large amounts of data from the sub-supplier, including information on the light railway.

In addition, in 2020 several employees with the Danish Metro Company (Copenhagen Metro) received suspicious emails containing malware from a well-known supplier. It turned out that the email correspondence with the supplier had been compromised by criminal hackers, who had sent emails to the Metro Company through the supplier's legitimate email account, making it difficult for the Metro Company employees to spot the attack. However, the Metro Company managed to ward off the attack. Known as email thread hijacking, this attack technique is widely used across sectors and involves hackers compromising a business partner's email account and sending responses to ongoing email correspondence with the victim's contacts. The infected emails appear to come from a trusted sender and are sent as a response to existing email conversations.

Other widespread attack techniques are also effective

Spear-phishing is another widely popular attack tool in the criminal hacker arsenal that can be used against the Danish railway sector. Spear-phishing resembles regular phishing attempts but differ in the sense that the targets are not random but selected. Hackers often use social engineering to tailor the attack to their target. Emails are typically prepared to make them seem relevant, convincing and credible to the target, for example by using the target's name, personally identifiable information or other information collected during prior reconnaissance.

Fraud in the form of so-called BEC scams still poses a threat across sectors. BEC scams are aimed at luring companies and authorities into transferring funds via fake emails containing instructions on how to wire the funds to the threat actor. Cyber criminals typically pose as in-house executives, harnessing the fact that employees will comply with instructions by superiors. This method has thus acquired the sobriquet CEO fraud. BEC scams may cause major economic losses to the targeted company or authority.

CFCS knows of BEC attempts against the railway sector in Denmark. A senior employee within the company Keolis, which is responsible for the daily operations of the Aarhus light railway and which is to be responsible for the daily operation of the Odense light railway, was compromised, possibly with the aim of using the individual's personal information or account to carry out BEC scams against other company employees. However, the employee reacted quickly, and the attack was averted.

The threat from intentional and unintentional insiders

All organizations face potential insider threats, with organizations in the railway sector being no exception. It is often the case that in-house security measures do not provide protection against insiders, who are capable of carrying out their activities solely by using their legitimate IT accesses.

Insiders may be divided into intentional and unintentional insiders. The unintentional insiders are employees who do not realize that their behaviour may damage the organization. Intentional insiders, however, are employees who deliberately violate in-house security policies for their own gain or with the aim of causing harm to the organization.

CFCS assesses that unintentional insiders account for as much as half of the security incidents in an organization.

Cyber espionage

The threat of cyber espionage against the railway sector is **HIGH**. The general threat level of cyber espionage against Denmark is very high, as foreign states persistently try to steal information from the state and several sectors. Though CFCS has seen no indications that the Danish railway sector is an equally interesting target for espionage activities, we still assess that foreign states have the intention and capacity to conduct cyber espionage against certain segments of the railway sector.

Several countries, including Russia and China, conduct cyber espionage to expand their national scope for action and to avoid strategic miscalculations in an ever-changing foreign-policy landscape. Unlike cyber crime, which is mainly driven by financial profit, cyber espionage is conducted by state-sponsored groups on the prowl for information, including information on development of new resource-heavy technologies, dual-use technologies, passenger lists, and information that may hold relevant overlaps into other sectors.

To the extent that parts of the transport sector are tasked with supporting Danish defence or foreign states' military, providing transport of military personnel for missions abroad or allowing military use of civilian traffic hubs such as airports, harbours and railways. In connection with such operations, these segments may be of interest to foreign states.

State-sponsored groups may also have an interest in railway sector tender procedures, as illustrated by examples abroad of hacker groups attempting to gain access to railway operator information prior to tender submissions. Between February and March 2018, hackers attacked several agencies connected to the Kuala Lumpur-Singapore high-speed rail project. At the time, several Chinese companies were bidding on the project against Japanese and South Korean businesses. In addition, it is possible that state-sponsored hackers carried out reconnaissance against the California High-speed Rail Authority prior to a large bidding round in 2017.

In October 2015, hackers tried to steal security information from Japan Railways Hokkaido via the company's administrative network. The hackers sent spear phishing emails deploying the Emdivi RAT ransomware. Subsequently, the hackers tried to extract information from the system, including information on prevention of railway crime, railway communications systems, security procedures and security information. However, the attack was averted, and the hackers did not gain access to the coveted information.

China’s new Silk Road

China is an active and advanced cyber actor with extensive cyber espionage and destructive cyber attack capabilities. Most of China’s cyber capabilities are governed by the Chinese intelligence services and military and have seen a strengthening in recent years.

The ”Made in China 2025” programme identifies ten key essential industries within which China aims to be a world leader. The new Silk Route is an essential component in this effort, as its goal is to secure a strong trade network across the world with strong and stable means of transportation. Consequently, China has shown a strong interest in railway tenders and undertakings across the world, including in Europe.

China has on several occasions shown an interest in Danish infrastructure, including railway infrastructure. In 2018, the China Railway Tunnel Group, a subsidiary of the state-owned China Railway Group, contacted Helsingborg municipality in Sweden, proposing to build a nine km long railway tunnel between the towns of Helsingborg in Sweden and Helsingør in Denmark. In addition, the company proposed the construction of a 14-15 km vehicular traffic tunnel connecting to the Helsingør highway at the town of Snekkersten.

The Danish Transport, Construction and Housing Authority, The Danish Road Directorate and The Swedish Transport Administration are currently assessing the possibilities of a fixed-link between Helsingør and Helsingborg. This assessment has no connection to the Chinese offer.

Destructive cyber attacks

The threat of destructive cyber attacks against the Danish railway sector is **LOW**.

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

The majority of destructive cyber attacks so far have resulted in data destruction, with the hacker either deleting or encrypting data without the possibility of file recovery. Even within this wide definition, destructive cyber attacks are relatively rare.

A number of countries are developing destructive cyber capabilities that can be used against critical infrastructure, such as the railway sector, in connection with a heightened military or political conflict. To this end, cyber espionage is used as a tool to map critical infrastructure.

In the short term, it is less likely that foreign states are intent on launching destructive cyber attacks on the Danish railway sector. However, their intention may change should Denmark become embroiled in a serious conflict with countries that hold destructive cyber attack capabilities.

Foreign railway sectors have been the targets of destructive cyber attacks, which to a lesser extent interrupted the availability of the railways. In 2017, several railway sectors abroad fell victim to the NotPetya attack, a destructive cyber attack disguised as a ransomware attack. Later in 2017, the metro in Ukraine's capital Kiev was hit by the so-called BadRabbit malware.

Cyber activism

The threat of cyber activism against the Danish railway sector is **LOW**. Consequently, the Danish railway sector is less likely to fall victim to cyber activism attempts within the next two years.

Cyber activism is typically ideologically or politically motivated, and cyber activists often target individuals or organizations that are perceived as opponents to their cause. Cyber activists may draw massive attention to their cause by attacking websites of railway companies, as such websites typically have many visitors. Similarly, railway information display boards are interesting targets for cyber activists as the boards provide a highly visible platform for their messages.

Cyber activists also target public authorities and private companies that are perceived as symbolic targets; even if these organizations are not directly involved in whichever controversy that has grabbed the activists' attention. The attacks may also be random in the sense that hackers attack opportunistically wherever they see an opening for gaining access to systems or exploiting vulnerabilities.

Despite the low threat level of cyber activism, several actors in the railway business list harassment and cyber activism at the top of their cyber security concerns, notably the attack technique known as DDoS attacks or overload attacks. DDoS attacks involve hackers exploiting compromised computers to cause unusually high volumes of data traffic congestion, overloading the targeted website or network. The goal is to render the website or network inoperable for legitimate users while the attack is ongoing.

DDoS attacks may prove serious if directed at customer-facing services such as travel information systems, departure and arrival information, and ticketing systems. This type of attack may cause reputational damage to the railway companies as a result of the inaccessibility of customer services.

In September 2019, the Danish state rail operator DSB was hit by a DDoS attack that paralyzed several of its online services for hours, including the ticketing system making passengers unable to buy tickets via the DSB ticket machines, app and website. Previous DDoS attacks on the DSB in 2013 and 2018 also had negative consequences for the company. DDoS attacks are a worldwide phenomenon, an example being Swedish railway operator Trafikverket that fell victim to a DDoS attack in 2017 causing massive delays.

In mid-2020, a new trend emerged involving criminal actors using DDoS tactics in extortion attacks, posing as infamous Advanced Persistent Threat (ATP) groups, such as "Fancy Bear" and "Lazarus Group", and threatening to launch large-scale DDoS attacks unless the victims agreed to pay ransom. So far, most targets of this tactic have been found in the financial sector and the energy sector. However, as railway operators run customer-facing services, the Danish railway sector may fall victim to this type of attack in the future.

Cyber terrorism

The threat of cyber terrorism against the Danish railway sector is **NONE**, making it unlikely that the sector will fall victim to cyber terrorism attempts within the next two years.

CFCS defines cyber terrorism as attacks with the intent of causing the same effect as conventional terrorist attacks, meaning cyber attacks resulting in personal injury or property damage or widespread disruption of critical infrastructure.

CFCS assesses that even though militant extremists have occasionally expressed an interest in conducting cyber terrorism, they currently lack the technical capabilities and organizational resources to deliver on their intentions.

The new signalling system – ERTMS

The new single European standard system European Rail Traffic Management System (ERTMS) is slated for rollout in Europe by 2030. In Denmark, the system has already been implemented on several railway lines, and a complete national rollout of the system is expected by 2030.

With the implementation of the ERTMS signalling system, the running of the trains will no longer rely on physical trackside signals but rather on a digital system, providing a higher degree of centralization. Thus, the consequences of ERMTS system compromises could potentially be more far-reaching than disruptions to the current systems, as it will be possible to create larger and geographically wider disruptions than previously.

The control and monitoring of the new signalling system is located in two control centers. This picture shows the control center located in Copenhagen. Photo: Thomas Rousing/Ritzau Scanpix

ERTMS-based signalling systems are designed to be fail proof. The general philosophy behind the system is that the train will stop if confusion arises as to incoming signals. Consequently, it will be difficult to cause a train wreck via the system. Conversely, though, this same safety precaution could be exploited to create a situation in which the train is forced to stop. For instance, a well-planned DDoS attack may cause disruptions and inconvenience to passengers.

The new signalling system is based on European standards, causing new cyber security challenges to arise, as a common European standard enables hackers to exploit knowledge on system vulnerabilities detected in other European countries to target the Danish system. Prior to introduction of the ERTMS system, this was only possible to a very limited extent due to the differences in national systems. In addition, it is possible for a hacker abroad to study the overall

specifications for parts of the Danish system, as this information is accessible in the publicly available ERTMS standards.

In 2014, a US railway company fell victim to a cyber attack launched by foreign hackers who disrupted the signals via the company's operational systems, causing several days' delay. Though the company did not rely on the European ERTMS system, the incident is testament to the feasibility of attacking a railway company via centralized signalling systems.

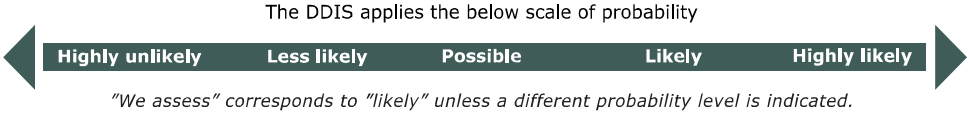
References

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



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

Further relevant readings

Center for Cyber Security (CFCS) publishes guides and threat assessments continuously. Below are some published products with particular interest for the railway sector. All products are accessible on CFCS website.

Organized cyber crime

The threat assessment "Do Cyber Criminals Dream of Trusting Relationships?" describes how established personal collaboration relationships, the division of labour and the exchange of goods and services in the criminal environment online supports the very high threat of cyber crime in general and the threat of targeted ransomware attacks in particular. You can find the assessment here:
https://cfcs.dk/en/cybertruslen/trusselsvurderinger/organised-cyber-crime/

The anatomy of targeted ransomware attacks

The investigative report "The anatomy of targeted ransomware attacks" maps out how targeted ransomware attacks typically happens and contains specific advice on how businesses and government institutions can protect themselves better. You can find the report here:
https://cfcs.dk/en/cybertruslen/rapporter/the-anatomy-of-targeted-ransomware-attacks/

Cyber attacks against suppliers

The threat assessment "Cyber attacks against suppliers" describe the cyber threats faced by suppliers. You can find the report here:
https://cfcs.dk/en/cybertruslen/threat-assessments/supply-chain/

The Cyber Threat from Phishing Mails

The threat assessment "The Cyber Threat from Phishing Mails" describes the threat from phishing emails. The assessment concludes that most cyber attacks today starts with a phishing mail. You can find the threat assessment here:
https://cfcs.dk/en/cybertruslen/trusselsvurderinger/phishing/

The cyber threat against HR-departments

The threat assessment "The cyber threat against HR-departments" describes the cyber threat against HR departments and includes advice on how to mitigate cyber attacks against HR departments. You can find the threat assessment here:
https://cfcs.dk/en/cybertruslen/trusselsvurderinger/cyber-threat-against-hr-departments/

The cyber threat from intentional and unintentional insiders

CFCS and the Danish Security Intelligence Service (PET) have jointly prepared the threat assessment "The cyber threat from intentional and unintentional insiders", which is available on CFCS website. It contains information on this specific threat and recommendations for preventive measures.
You can find the threat assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/insiders/