CENTRE FOR CYBER SECURITY

Threat assessment

The cyber threat against the Danish aviation sector

3rd edition September 2021

Table of contents

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

3rd edition September 2021

The cyber threat against the Danish aviation sector

The purpose of this threat assessment is to inform of the cyber threat against the Danish aviation sector. The threat assessment can be used in the sector's risk assessment efforts. The assessment is mainly intended for executives and IT employees working in Danish air traffic control and aviation authorities, in airports, airline companies as well as subcontractors to aircraft manufacturers.

This threat assessment was updated in September 2021. Adjustments have been made to the cyber espionage chapter. The threat of cyber espionage against the Danish aviation sector has been raised to **VERY HIGH**. Also, minor editorial changes have been made in the other chapters.

Previously, the threat assessment was updated in June 2020 with changes in the chapters on cyber activism and cyber terrorism, reflecting threat level adjustments in the annual national threat assessment "The cyber threat against Denmark", published in 2020. Also, destructive cyber attacks have been assigned a threat level corresponding to the level determined in the national threat assessment.

Key assessment

- The threat of cyber crime against the Danish aviation sector is **VERY HIGH**, reflecting the general cyber threat level against Denmark. As a result, private companies and public authorities in the Danish aviation sector will highly likely become targets of cyber crime attempts.

- The threat of cyber espionage against the Danish aviation sector is **VERY HIGH**, meaning that private companies or public authorities in the Danish aviation sector are highly likely to become targets of cyber espionage attempts.

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

- The threat of cyber activism against the Danish aviation sector is **LOW**, meaning that private companies and public authorities in the Danish aviation sector are less likely to become targets of cyber activism attempts.

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

Introduction

This threat assessment outlines the cyber threat against the Danish aviation sector. Thus, the assessment analyses the threat against Danish air traffic control and aviation authorities, airports, airlines as well as subcontractors to aircraft manufacturers.

This assessment is based on analyses of international examples of cyber attacks against airports, airlines, subcontractors and public authorities, which are then compared to Danish conditions and knowledge of threat actors' cyber capabilities and intent. The assessment has been prepared in cooperation with organizations in the aviation sector. The Centre for Cyber Security (CFCS) still has limited knowledge about concrete attacks against the Danish aviation sector.

This threat assessment describes the current threat landscape in the short term, corresponding to a warning horizon of 0-2 years. As cyber threats are dynamic in nature, the threat landscape may change without warning. This applies both in general and to the aviation sector in particular. Threat and probability level definitions are listed at the end of the assessment.

The greatest threat to the aviation sector is cyber crime, including, in particular, ransomware. While any organization is a potential ransomware target, international incidents point to aircraft manufacturers and airports, in particular, as being the most targeted in ransomware attacks. Criminal actors also target airline customer services in order to sell credit card information or reward points.

Finally, the threat of cyber espionage is assessed as **VERY HIGH**.

Cyber crime

The threat of cyber crime against the Danish aviation sector is **VERY HIGH.** The threat emanates from financially motivated criminal individuals and networks.

Malicious actors will look to exploit vulnerabilities in any organization, if financial gain is a possibility.

Some cyber criminal networks target large organizations because of the possibility of big pay-outs – a tactic known as 'big game hunting'. Thus, large airports, airlines and subcontractors are of particular interest to these cyber criminal networks.

Cyber criminals use ransomware for extortion

Many cyber criminals use so-called ransomware. Ransomware attacks are when a victim's computer or data is held hostage, i.e. encrypted, rendering the data or systems unavailable to the victim. The actor behind the attack demands a ransom, typically in the form of crypto currency such as Bitcoin, in exchange for restoring the victim's access to the data. Usually, the actor behind the attack will install malware on the victim's computer by using phishing emails. Most ransomware attacks are successful because the victim is tricked into clicking on a link or opening an attached file in an email, but ransomware attacks may also occur via exploitation of weak remote access controls or known vulnerabilities in Internet-facing systems.

There are many types of ransomware. For instance, criminal hackers conducting targeted ransomware attacks actively pursue administrative networks in specific companies and public authorities.

Ransomware attacks may have serious consequences. For instance, a ransomware attack against Cleveland Hopkins International Airport in April 2019 caused disruptions and disabled flight and information boards, baggage handling and the airport's internal email systems.

Several types of ransomware exploit vulnerabilities that have long been patched by software upgrades. The WannaCry ransomware, for instance, exploits a vulnerability, which was patched by a security update in March 2017. Nevertheless, more than 300,000 computers were infected when the global WannaCry attack hit in May 2017. In March 2018, Boeing was infected with WannaCry, indicating that WannaCry continues to pose a threat to systems that have not been updated.

The WannaCry ransomware began to spread to computers worldwide in May 2017. By using WannaCry, cyber criminals were able to encrypt victims' files automatically, delete the original files and demand a ransom to decrypt the files again.

At the same time, the ransomware installed a backdoor on the victim's machine, allowing the attacker to introduce additional malware. WannaCry was able to spread across local networks and the Internet through a vulnerability in the Server Message Block, version 1 (SMBv1).

Cyber criminals steal credit card information and reward points
Cyber criminals are also interested in personal data that can be sold, in particular, credit card information and frequent flyer miles. CFCS also knows of instances where stolen air miles have been traded online as a form of currency.

From August to September 2018, British Airways was the target of a cyber attack that involved unauthorized access to passenger names and emails. The cyber criminals also gained access to passenger credit card numbers along with expiration dates and card verification codes (CVV numbers) once they were entered on the website. British Airways assesses that up to 380,000 customers were affected by the attack. In the wake of the attack, British Airways was ordered to pay a fine of DKK 1.5 billion for breaching the EU's General Data Protection Regulation. In the fall of 2020 the fine was reduced to 173 million DKK.

Criminal actors often try to compromise or exploit suppliers in an attempt to gain access to larger targets, including suppliers in the aviation sector. This type of attack is known as a supply chain attack.

A specific type of supply chain attack is conducted through subcontractors that supply software. This type of attack is known as software supply chain attack. By targeting software suppliers, the attacker is subsequently able to compromise one or several of the companies using software from the supplier. The attacker may compromise the users of the software by delivering malware through software updates.

'BEC scams' pose a threat to the aviation sector
CFCS has noted incidents of BEC scam attempts against organizations in the Danish aviation sector.

BEC scams, also known as CEO fraud, are attempts to trick companies and organizations into wiring funds through false wire transfer requests. Instead of sending emails to a large group of random employees in a company, the hackers conduct thorough research that enable them to mimic legitimate emails by impersonating a CEO, financial executive or consultant in close contact with the top executive office and luring employees into believing that it is an order from the executive office.

The aviation sector is vulnerable to potential insider threats
No organization is immune to insider threats, including the aviation sector. Organizations' security mechanisms often fail to prevent insider attacks as insiders use their legitimate IT access to conduct malicious activities.

As physical access to systems may facilitate breaches, it is vital to pay close attention to systems and data that are isolated from the Internet.

Cyber espionage

The threat of cyber espionage against the aviation sector is **VERY HIGH**.

CFCS assesses that in recent years, the aviation sector abroad has seen an increase in cyber espionage activity. Foreign states have conducted attacks against different types of organizations in the aviation sector. The Danish aviation sector will highly likely also be exposed to attack attempts. CFCS assess that foreign states have a particular interest, for instance, in public authorities within the sector.

Espionage against the Danish transport sector may be motivated by security political interests. The transport sector is part of the Danish critical infrastructure, and foreign states may thus have an interest in increasing their knowledge of capabilities and detecting vulnerabilities in the Danish aviation sector, for instance, in the event of a potential military conflict. Information collection on critical infrastructure may be used to launch destructive cyber attacks or physical attacks against the aviation sector.

State-sponsored hackers have shown interest in technology that may help advance their national aviation sector. Some state-sponsored actors with significant capacities have shown a strong interest in technology that can be used in both civilian and military aviation as well as aerospace. Consequently, aircraft manufacturers and their subcontractors are also main targets of cyber espionage.

It is likely that a targeted, state-sponsored cyber espionage campaign against aircraft manufacturers and subcontractors abroad helped China acquire data required to design and build the engine of its C919 passenger airliner.

Also, state-sponsored actors have shown an interest in the aviation sector more broadly. A case in point is the November 2016 cyber attack against the UN aviation organization ICAO. A state-sponsored actor inserted malicious code into articles posted on ICAO's website, likely in an attempt to gain further access to other parts of the aviation sector.

CFCS knows of an older example involving state-sponsored actors compromising a Danish organization in the aviation sector.

Airline companies also face the threat of cyber espionage. State-sponsored actors have shown an interest in exploiting personal data, likely in an attempt to map travel patterns of certain individuals and organizations.

Organizations in the Danish aviation sector may also fall victim to cyber espionage conducted through suppliers, such as software suppliers. In 2021, thousands of organizations fell victim to the SolarWinds attack, including SAS Airline. 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 Danish aviation sector is **LOW**.

As a result, it is less likely that the aviation sector will become target of destructive cyber attack attempts within the next two years.

However, the threat may increase in connection with a heightened political or military conflict.

A case in point was the NATO Trident Juncture exercise in October-November 2018, when areas in northern Norway were exposed to electronic attacks in the form of GPS jamming that ultimately disrupted the civil air traffic. Even though GPS jamming is an electronic attack – and not a cyber attack per se – CFCS assesses that the threat of destructive cyber attacks may increase in connection with a conflict.

A number of countries have cyber attack capacities that could be used destructively against critical infrastructure such as the aviation sector. Destructive cyber attacks are defined as attacks that could potentially result in death, personal injury, 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 the Danish transport sector may be affected by destructive cyber attacks against targets abroad. The aviation sector abroad has fallen victim to destructive cyber attacks that caused minor disruptions affecting the availability of the sector. In June 2017, several aviation companies abroad were affected by the NotPetya attack, which was a destructive cyber attack disguised as a ransomware attack. In Ukraine, two airports were affected by the attack.

Cyber activism

The threat of cyber activism against the Danish aviation sector is **LOW**, meaning that the Danish aviation sector is less likely to be targeted with cyber activism attempts within the next two years.

In recent years, the number of cyber activism attacks has dropped worldwide. Cyber activists rarely target Danish public authorities and companies. Cyber activists are typically motivated by specific issues, and the threat against the aviation sector may thus change overnight.

Cyber activism is typically driven by ideological or political motives. Cyber activists often target individuals or organizations, which they deem opponents to their cause. Activism against aviation has a high level of visibility. In recent years, there have been a number of cyber activist attacks, for example, website defacement attacks, on airports and airlines. However, CFCS has no knowledge of Danish victims of cyber activism in the Danish aviation sector.

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

> Website defacement is an attack in which the attacker makes changes to the visual appearance of a website. For instance, the attacker may insert a text or a picture on the front page of the website.

Cyber activists may be able to draw a lot of attention to their cause if they succeed in attacking the airports' websites as these typically have many visitors. Similarly, airport information boards are highly visible, making them interesting targets.

The aviation sector constitutes a potential target to activists that are concerned about the environment. For instance, the climate activist group 'Heathrow Pause' threatened to disrupt air traffic in Heathrow Airport in London in September 2019.

DDoS attacks

Actors also use DDoS attacks. DDoS is short for Distributed Denial of Service and is a flooding attack. Hackers exploit compromised computers to flood the targeted website (webserver) or a network with data traffic, making the website or network unavailable for legitimate traffic as long as the attack is in progress. DDoS attacks are used by various types of hackers, including cyber activists as well as cyber criminals.

The aviation sector is no stranger to DDoS attacks. In 2015, the Polish Airline LOT's base in Warsaw Airport fell victim to a DDoS attack that left approx. 1,400 passengers temporarily stranded.

Cyber terrorism

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

This means that it is highly unlikely that the Danish aviation sector will become target of 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 of critical infrastructure.

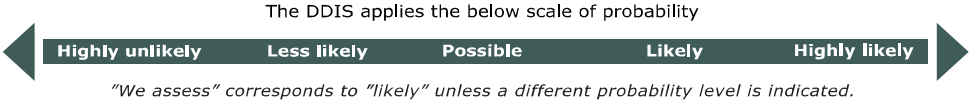
Cyber attacks of such serious magnitude presuppose technical skills and organizational resources that militant extremists currently do not possess and also, their intent is very limited.

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



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

Additional relevant publications

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 aviation 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/