CENTRE FOR
CYBER SECURITY

Threat assessment: 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 may be used in the sector's further work with risk assessments. This assessment is directed mainly at top management and IT employees in the Danish air traffic control and aviation authorities and in airports, airlines and subcontractors to aircraft manufacturers.

December 2019

Danish Defence Intelligence Service
Kastellet 30
DK-2100 Copenhagen

Tel.: +45 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Key Assessment

- Like the general cyber threat level against Denmark, the threat of cyber crime against the Danish aviation sector is **VERY HIGH.** Thus, it is highly likely that private companies and public authorities in the Danish aviation sector will become targets of cyber crime attempts.

- The threat of cyber espionage against the Danish aviation sector is **HIGH**. It is likely that private companies or public authorities in the Danish aviation sector will become targets of cyber espionage attempts.

- The threat of cyber activism against the Danish aviation sector is **MEDIUM**. This means that it is possible that private companies and public authorities become targets of cyber activism. However, the threat to the individual organisation may increase in connection with, for instance, negative publicity.

- The threat of cyber terrorism is **LOW**. Even though militant extremists have occasionally expressed an interest in conducting cyber terrorism, they currently lack the capabilities to do so.

- There is a potential threat of destructive cyber attacks. It is less likely that foreign states will launch destructive cyber attacks against critical infrastructure in Denmark, including the Danish aviation sector.

Introduction

This threat assessment describes the cyber threats against the Danish aviation sector. In this assessment the Danish aviation sector is defined as Danish air traffic control and aviation authorities, airports, airlines and subcontractors to aircraft manufacturers.

This assessment is based on analyses of international cyber attack examples 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 following a dialogue 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 is based on the current short term threat landscape and operates with a warning horizon of 0-2 years. As cyber threats are dynamic in nature, the threat landscape may suddenly change, both in general and in relation to the aviation sector specifically. The threat and probability levels applied in this threat assessment are defined at the end of the report.

The greatest threat to the aviation industry is cyber crime, including, in particular, ransomware. Any organization is a potential ransomware target. Internationally, aircraft manufacturers and airports, in particular, have been victims of ransomware attacks in the aviation sector. Criminal actors are also interested in compromising airlines' online customer services to enable the resell of credit card information or reward points.

This assessment also describes the high threat of cyber espionage. State-sponsored actors have shown particular interest in compromising the sensitive personal customer data, which airlines store.

Cyber crime

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

The actors are interested in exploiting organizations, if they believe it is possible to exploit vulnerabilities to launch a cyber attack for profit.

Some cyber-criminal networks target large organizations because of the possibility of making a bigger profit, a tactic known as 'big game hunting'. Thus, in the aviation sector large airports, airlines and subcontractors are of particular interest to these networks.

Cyber criminals use ransomware as a means of extortion

Many cyber criminals use so-called ransomware. Ransomware attacks are when a victim's system 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 mails. 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 text messaging or banner advertising on a website.

There are many types of ransomware. Increasingly, targeted ransomware attacks attempt to exploit, for instance, administrative networks in specific companies and public authorities.

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

Several types of ransomware exploit vulnerabilities, which have already been solved with software upgrades. The WannaCry ransomware 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 upgraded.

The WannaCry ransomware began to spread to computers worldwide in May 2017. By using WannaCry, cyber criminals were able to encrypt files automatically on the victim's computer, 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 install additional malware. WannaCry was able to spread across local networks and the Internet through a vulnerability in the Server Message Block, version 1 (SMBv1) protocol.

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 reward points. CFCS also knows of instances where stolen reward points 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 connection with the attack, British Airways was ordered to pay a fine of

DKK 1.5 billion for breaching the EU’s General Data Protection Regulation.

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 supply chain attack.

A specific type of supply chain attack is conducted through subcontractors that supply software. By attacking 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 upgrades.

’BEC scams’ pose a threat to the aviation sector

CFCS have knowledge of organizations in the Danish aviation sector exposed to Business Email Compromise Scams (BEC) attempts.

BEC scams, also referred to 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 which enable them to write seemingly legitimate targeted emails, for instance, impersonating a CEO, financial executive or consultant in close contact with the top executive office and thus luring employees into believing that the wire request is an order from the executive office.

The aviation sector is faced with potential insider threats

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

Physical access to systems can facilitate breaches. It can be particularly relevant to pay attention to this issue in relation to systems and data that are isolated from the Internet.

CFCS and the Danish Intelligence and Security Service (PET) have prepared a threat assessment on the cyber threat from intentional and unintentional insiders. The threat assessment provides additional information on the threat and recommendations for mitigating measures and is available on the Danish Defence Intelligence Service’s website.

Cyber espionage

The threat of cyber espionage against the Danish aviation sector is **HIGH**. In general, the threat of cyber espionage against Denmark is very high, as foreign states persistently attempt to steal information from the state and specific sectors. The threat of cyber espionage is especially directed at those segments in the Danish public sector that engage in foreign, security and defence policies. CFCS have no knowledge of an equally high level of activity against the Danish aviation sector. CFCS do have knowledge though of one organisation in the sector that has been compromised by state-sponsored actors. CFCS is also aware of examples of state-sponsored attempts to compromise civil aviation authorities abroad. We assess that foreign states have both the intent and the capacity to conduct cyber espionage against the sector.

Cyber crime is to a large extent conducted by groups motivated by financial gains whereas cyber espionage is conducted by state-sponsored groups seeking access to information. In the aviation sector, state-sponsored actors have in particular shown an interest in exploiting technology that may develop and improve their own national aviation sector. Some state-sponsored actors with significant capacities have shown a strong interest in technology that can be used in both civil and military aviation as well as aerospace. Consequently, the threat from cyber espionage is also to a high extent directed at aircraft manufacturers and their subcontractors.

It is likely that a targeted state-sponsored cyber espionage campaign against aircraft manufacturers and subcontractors abroad helped China develop the motor for the C919 passenger airliner.

Also, state-sponsored actors have shown an interest in the aviation sector, in a broader perspective. 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.

If visitors to the website opened documents on the website, their computers would risk being infected. If an employee at an aircraft manufacturer or in a member country accessed one of the articles, it would raise the risk that the actor gained unauthorized access to the organization’s network. This method is known as watering hole attacks.

Watering hole is an attack method, in which a legitimate website such as a web shop is infected with malware. Regular users of the website would risk getting infected with malware. A watering hole attack seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit regularly.

Furthermore, state-sponsored groups have shown an interest in personal data, likely because it would allow them to map travel patterns of certain individuals and organizations.

Cyber activism

The threat of cyber activism against the Danish aviation sector is **MEDIUM.** Cyber activism is typically driven by ideological or political motives. Cyber activists often target individuals or organizations, which they deem opponents to their cause. Especially activism against airports has a great visibility, which potentially can draw a lot of attention to the messages of cyber activists.

Even if authorities and private companies are not directly involved in the issue that caught the cyber activists' attention, they still risk becoming targets of cyber activism 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.

The CFCS also knows of website defacement attacks on airports and airlines.

Website defacement is an attack method 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.

Airports and their websites, in particular, are popular among cyber activists who may 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. There are examples of cyber activism abroad against airports in connection with diplomatic or political crises.

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

Destructive cyber attacks

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 less likely that foreign states have the intent to launch destructive cyber attacks against critical infrastructure in Denmark, including against the aviation sector.

The aviation sector abroad has fallen victim to destructive cyber attacks that caused minor disruptions affecting the availability of the sector. In June 2017, numerous 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.

The threat of destructive cyber attacks 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 – the threat from destructive cyber attacks may increase in connection with a conflict.

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 overload the targeted website (webserver) or a network with a flood of data traffic, making the website or network unavailable for legitimate traffic as long as the attack is ongoing.

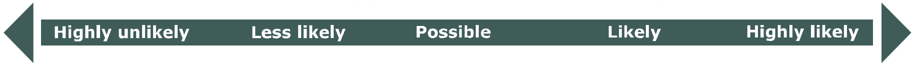
The aviation sector is also hit by DDoS attacks. In 2015, a cyberattack against Polish Airline LOT meant that approx. 1,400 passengers temporarily stranded in Warsaw Airport.

Definition of threat levels

The 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 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


Highly unlikely
Less likely
Possible
Likely
Highly likely