Threat assessment

The cyber threat against Denmark 2024

CENTRE FOR CYBER SECURITY

CENTRE FOR CYBER SECURITY

Centre for Cyber Security
Kastellet 30
DK-2100 København Ø

Phone number: +45 3332 5580
Email: cfcs@cfcs.dk
www.cfcs.dk
www.fe-ddis.dk

Table of contents

The cyber threat against Denmark 2024

The purpose of this threat assessment is to inform decision-makers in Danish public authorities and private companies of the cyber threat against Denmark. The threat assessment outlines the different types of cyber threats facing Denmark and can be used as a basis to assist organizations in their efforts to perform cyber security risk assessments.

KEY ASSESSMENT

- THE THREAT OF CYBER ESPIONAGE AGAINST DENMARK IS **VERY HIGH.**

  Organizations with access to information on matters of Danish foreign and security policy are often singled out as potential targets of cyber espionage. Danish critical infrastructure and the Danish Defence are also prime targets for foreign cyber espionage.

  The threat of cyber espionage against Denmark primarily comes from Russia and China. Both states are highly capable cyber powers conducting cyber espionage against targets in Denmark and abroad, among others.

- THE THREAT OF CYBER CRIME AGAINST DENMARK IS **VERY HIGH**.

  Cyber crime affects all levels of society.

  The CFCS assesses that in 2023, there were more ransomware incidents in Denmark and across the world than ever registered.

- THE THREAT OF CYBER ACTIVISM AGAINST DENMARK IS **HIGH**.

  The cyber activist attacks that have regularly struck Danish targets emphasize that cyber threats against Danish companies and public authorities have become the norm.

  The threat of cyber activism against Denmark primarily comes from pro-Russian cyber activists. The CFCS assesses that some pro-Russian cyber activists are linked to the Russian state.

- THE THREAT OF DESTRUCTIVE CYBER ATTACKS AGAINST DENMARK IS **MEDIUM**.

  The threat primarily comes from Russian state-sponsored hackers. However, in the current situation, it is less likely that Russia is intent on launching destructive cyber attacks on Denmark with serious and far-reaching consequences for critical societal functions.

  Several foreign states have the capabilities to launch destructive cyber attacks against Denmark. The threat of destructive cyber attacks can increase with little or no warning if foreign states decide to strike Danish targets.

- THE THREAT OF CYBER TERRORISM AGAINST DENMARK IS **NONE**.

  Since 2016, the CFCS has monitored developments in the cyber terrorism threat, with special focus on militant extremists. The CFCS assesses that, at present, there are no actors with the capability and intent to conduct cyber terrorism against Denmark.

INTRODUCTION

■ Since the CFCS published *The cyber threat against Denmark 2023*, the global security situation has changed. War has erupted between Israel and Hamas in Gaza, and Russia's invasion of Ukraine has shifted into a prolonged war. The global security situation and the competition between states also spill over into the cyber domain. The reason for this is that cyber attacks are but one of several tools that can be used by states to promote their interests.

In contrast to cyber crime, cyber espionage, destructive cyber attacks and cyber activism are the most common tactics in state-on-state cyber operations. Where cyber crime is concerned, the actors are typically non-political and opportunistic in pursuit of financial gain. Consequently, cyber crime can affect everyone, including public authorities, private companies, think tanks, NGOs and individuals.

In other words, the cyber threat is a constant risk that a digitized society like Denmark has to deal with as evidenced by the media coverage of ransomware attacks and cyber activist DDoS attacks.

The CFCS divides the cyber threat into five different categories: cyber espionage, cyber crime, cyber activism, destructive cyber attacks and cyber terrorism. The objective has not been to simplify the threat but to emphasize that the cyber threat is complex and cannot be described from one perspective. Each category is based on the intent of a given type of attack. For instance, the purpose of cyber espionage is to obtain sensitive information, the purpose of cyber terrorism is to conduct terrorism via the cyber domain etc. However, it is not always easy to assess the 0intent of an attack as there may be overlaps between different types of attacks.

Denmark is still at risk of cyber threats

The 2024 edition of The cyber threat against Denmark emphasizes that Denmark is still a prime target for malicious actors. In early June 2024, the CFCS raised the threat level for destructive cyber attacks from **LOW** to **MEDIUM**. The decision to raise the threat level was based on Russia's increased willingness to use hybrid tactics, including destructive cyber attacks, against European NATO member states, emphasizing the fact that an unstable global security situation also expands into the cyber domain.

The threat landscape is constantly evolving. New threat actors emerge while others disappear, and hackers continue to develop new approaches of attack. Below is an outline of the five types of cyber threats the CFCS divides the cyber threat into.

The threat of cyber espionage against Denmark is **VERY HIGH**. Foreign states continually conduct cyber espionage attempts against organizations in

Denmark. They have done so for a number of years and will continue to do so.

Just like the threat of cyber espionage, the threat of cyber crime is **VERY HIGH**. Cyber crime is among the most prevalent threats and can affect individual citizens, public authorities and private companies alike, irrespective of size and critical function. In other words, this type of attack can affect everyone as cyber criminals are opportunistic.

The threat of cyber activism against Denmark is still **HIGH**. Russia's invasion of Ukraine has unleashed a high level of cyber activism. The war in Gaza has been an additional driver which has resulted in the emergence of new cyber activist actors and triggered activity among existing actors. However, the threat of cyber activism still mainly emanates from pro-Russian cyber activists.

The threat of destructive cyber attacks against Denmark is now **MEDIUM**. The threat primarily emanates from Russian state-sponsored hackers but also from non-state hackers with various degrees of ties to the Russian state.

The threat of cyber terrorism against Denmark is **NONE**. The CFCS assesses that, at present, there are no terrorist groups with the capability or intent to conduct cyber terrorism against Denmark. Consequently, it is highly unlikely that Danish public authorities and private companies will fall victim to cyber terrorism attempts within the next two years.

The CFCS uses the Danish Defence Intelligence Service's threat levels and probability degrees, which are explained at the end of the assessment. In this threat assessment, the CFCS describes the threat with a two-year time frame.

Enjoy your reading!

CYBER ESPIONAGE

The threat of cyber espionage against Denmark is **VERY HIGH**. Foreign states continually try to conduct cyber espionage against organizations in Denmark, at times successfully. They have been conducting cyber espionage for a number of years and will highly likely continue for many years to come.

■ The Danish Defence and organizations with access to information on matters of Danish foreign and security policy are prime targets for cyber espionage. However, other organizations are also at risk of cyber espionage. The reason for this is that foreign states conduct cyber espionage for different purposes and against a variety of targets.

It is likely that state-sponsored Russian hackers conduct cyber espionage against Danish critical infrastructure in preparation for destructive cyber attacks in the future. Such attacks could become a reality if the states decide to attack Danish targets. In addition, it is highly likely that China conducts cyber espionage against targets in Denmark, among others, in an attempt to gain information and transfer technology.

The main threat of cyber espionage comes from Russia and China

The main threat of cyber espionage against Denmark comes from Russia. In addition, the CFCS assesses that China is an active and persistent cyber espionage threat. Both states have significant cyber capabilities which they use to conduct cyber espionage against targets abroad and in Denmark.

Other states, including North Korea and Iran, also have cyber espionage capabilities. However, they primarily use their capabilities to conduct cyber espionage against their neighbouring countries. It is less likely that these states are currently giving priority to cyber espionage campaigns against Denmark. However, it is still possible that organizations in Denmark could fall victim to cyber espionage by other countries besides Russia and China. The reason is that some cyber espionage actors are opportunistic, not always leveraging targeted attacks but rather looking for systems that are easy to access. In addition, the threat from these states could quickly change if Denmark was to become a prime espionage target as a result of international events.

Foreign states look to steal information on foreign and security policy issues

It is highly likely that both Russia and China use cyber espionage to gain access to information on Danish foreign and security policy issues, among others. They can use this knowledge to challenge Western norms and increase their international clout, potentially at the expense of Danish interests.

The CFCS assesses that Denmark is target of this type of cyber espionage along with other NATO and EU countries. The reason is that Russia and China are widely interested in gaining insights into the West's stance on foreign and security policy agendas, conflicts and events. The West's support for Ukraine, for example, is a topic of interest to Russia.

However, other conditions could also add to a more specific interest of Denmark's foreign and security policy stance from foreign states. For instance, it is likely that Denmark's geographical location in the Baltic Sea contributes to the threat of cyber espionage from Russia in particular. At the same time, it is highly likely that Russia and China's cyber espionage activities against Denmark are motivated by the Kingdom of Denmark's geographical location and role in the Arctic.

CYBER ESPIONAGE POSES A THREAT TO SOCIETY AND ORGANIZATIONS

Cyber espionage can have serious consequences for society as a whole and for the individual organization affected. Some consequences are evident while others are easy to overlook as they are intangible or will not materialize until a later point in time.

From a national perspective, cyber espionage could have consequences for Danish national security and interests, among others, for instance if foreign states gain access to information that they can exploit in a military conflict or international negotiations. Intellectual property theft can also weaken Denmark's trading position and ultimately the Danish economy.

For the individual organization, the consequences of cyber espionage encompass financial losses or reputational damage, loss of customer trust and confidence, and loss of competive advantage. At the same time, cyber espionage can trigger regulatory fines if personal information is compromised.

Cyber espionage can be used to provide information of general and specific value to the states. For instance, they can use cyber espionage as a means to build general knowledge of Denmark's foreign and security policy priorities and Denmark as a strategic actor. However, cyber espionage can also be used to allow them access specific information on Denmark's stance in international negotiation situations.

Russia conducts cyber espionage in preparation for a military conflict

It is highly likely that Russia is also conducting cyber espionage against Denmark in preparation for a potential military conflict with NATO. Combined with other types of espionage, this would put Russia in the best possible position to prepare for a military conflict.

Russian cyber espionage activities against Denmark are rooted in Russia's strong general interest in NATO member states triggered by the role that the individual countries could come to play in a potential military conflict between Russia and NATO. In addition, Russia has extended its interest and cyber espionage reach to Denmark due to the Kingdom of Denmark's location in the Baltic Sea and the Arctic, where Russia has military interests.

As a result of Russia's cyber espionage activities in preparation for a potential conflict with NATO, the Danish Defence is at a high risk of cyber espionage. However, Danish defence suppliers and other organizations which, in Russia's view, support the Danish Defence or other military organizations of NATO countries are also at risk. It is highly likely that Russia, among other things, is interested in gaining access to information on the capabilities of the Danish Defence and NATO, their organizational structure, plans and personnel.

Critical infrastructure organizations in Denmark are also at risk of cyber espionage. The reason is that Russian state-sponsored hackers are likely conducting cyber espionage against these organizations in preparation for destructive cyber attacks. Cyber espionage facilitates hackers' access to organizations, allows them to build knowledge on the systems and networks of the organizations and establish backdoors, ultimately enabling them to launch destructive cyber attacks on the organizations with little or no warning in the event of an escalating crisis or war.

China also uses cyber espionage to gain access to knowledge and technology

It is highly likley that China also wages cyber espionage campaigns designed to promote its interests and technological development goals by acquiring knowledge and technology from abroad in pursuit of these ambitions. As a result, organizations across the world, including organizations in Denmark, are at risk of falling victim to Chinese cyber espionage campaigns.

Several Danish private companies and research institutions are at the forefront of their field and thus possess knowledge that makes them potential targets of cyber espionage. This is especially true for organizations that has knowledge which is of strategic importance to China's economic and technological development. These areas include information and communications technology, artificial intelligence, pharmaceuticals and quantum and aviation technology.

In addition, Danish defence companies are prime cyber espionage targets for both China and Russia as they hold knowledge and technology that the two states can use to increase their own military capabilities. In addition, defence industry knowledge can provide insights into the military capabilities of Western countries.

Opportunistic cyber espionage – a threat to all levels of society

The CFCS assesses that organizations in Denmark are generally at risk of getting compromised by foreign states. The reason is that some state-sponsored hackers are opportunistic in their targeting and continually attempt to compromise targets in bulk, making every organization a potential target even if they are not obvious targets of espionage.

For instance, it is highly likely that some state-sponsored hackers try to gain access to multiple systems and networks by exploiting a well-known vulnerability

STATES USE BOTH SIMPLE AND ADVANCED TACTICS

State-sponsored hackers often have the capabilities to launch advanced cyber espionage operations, including exploitation of zero-day vulnerabilities, which are vulnerabilities that have not been security patched and thus are hard to mitigate. For instancce, in December 2023, open sources reported that Russian state-sponsored hackers exploited a zero-day vulnerability in Microsoft Outlook to spy against the energy, transport, tele and defence industries in a number of NATO member states.

However, state-sponsored hackers also use more simple cyber espionage tactics. For instance, they can trick employees into clicking on a link or an attached file in a phishing email, thereby letting them into the organization's systems. In addition, they can gain access to systems via known vulnerabilities or brute force attacks.

It is likely that state-sponsored hackers primarily turn to advanced tactics if simple attacks prove inadequate, and the prospect of high financial rewards looks positive. This could be the case in relation to cyber espionage against high-priority targets.

It is likely that state-sponsored hackers primarily turn to advanced tactics if simple attacks prove inadequate, and the prospect of high financial rewards looks positive. This could be the case in relation to cyber espionage against high-priority targets.

or by sending a large number of phishing emails. The CFCS assesses that the purpose is to conduct cyber espionage, among other things, against compromised victims that are deemed to be of interest. Alternatively, the hackers can use the compromised devices as part of their infrastructure to gain entry into other organizations.

Some state-sponsored hackers also try to gain access to multiple victim systems by targeting a common supplier, for instance through so-called software supply chain attacks. In these attacks, hackers compromise a software supplier in order to hide malware in apparent legitimate updates. Once the update is released, the software users risk compromise, potentially affecting thousands of users.

Another example of a supply chain attack encompasses hackers compromising cloud service providers, thereby potentially getting access to customer data or systems. In addition, hackers can, in some instances, exploit the integration between the cloud service provider and customer networks to compromise and steal data from customers that are deemed to be prime espionage targets.

Cyber espionage is a versatile and widely used tool

Foreign states also conduct cyber espionage for other purposes than the ones described above.

For instance, foreign states conduct cyber espionage to spy against ethnic groups and dissidents residing abroad. China, for instance, uses cyber espionage to try to control and oppress the Chinese diaspora in general and dissidents in particular, including minorities such as the Uighurs and Tibetans.

In addition, the CFCS assesses that foreign states use cyber espionage, among others, in support of influence campaigns, including hack and leak attacks intended to influence the population of Western countries. In such attacks, hackers steal and leak internal documents or data in order to send a message or cause damage to an individual, an organization or a country's reputation. The leaked information could be edited or manipulated to support a certain message.

However, the CFCS assesses that cyber espionage in support of oppression and influence campaigns has mainly been directed at targets abroad. It is less likely that Denmark is being targeted with these specific cyber espionage purposes in mind.

READ MORE

More threat assessments available at **cfcs.dk**

CYBER CRIME

The threat of cyber crime against Danish public authorities, private companies and citizens is **VERY HIGH**. It is highly likely that Danish public authorities and private companies will fall victim to cyber crime within the next two years.

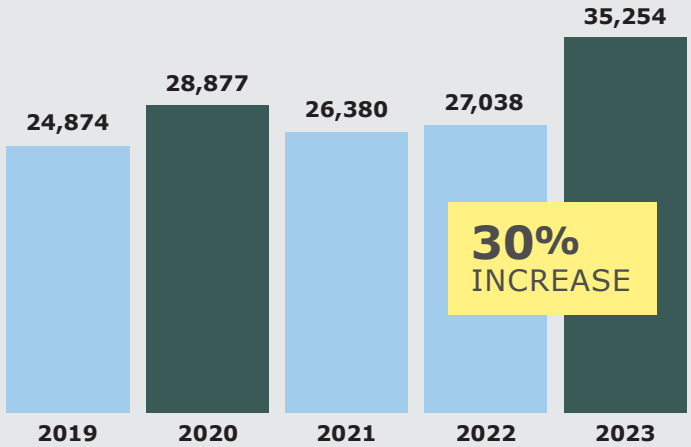
■ Cyber criminals are typically looking to exploit their unauthorized access to data and systems for financial gain. Cyber crime is among the most notable cyber threats to Danish society and can have serious consequences for both private citizens and organizations. This is evident, for instance, when personal information is leaked, when companies are forced to suspend operations or when they ultimately have to close down as a result of an attack.

Ransomware affects all levels of society

The ransomware threat has not diminished. The CFCS assesses that in 2023, the number of ransomware attacks in Denmark and worldwide was greater than ever registered.

Ransomware attacks involve attempts by criminals to extort public authorities or private companies by rendering their data and systems unavailable, often

IT CRIME REPORTS IN DENMARK WERE AT A RECORD HIGH IN 2023



- The figure shows the development in the number of reports of it-related economic crime from 2019-2023
- From 2022 to 2023, there was an increase of 30 percent (corresponding to 8,220 reports)

It-related economic crime encompasses crime on the internet for financial gain by means of it systems and phones. This type of crimiminal activity includes Business Email Compromise fraud (BEC fraud), credit card fraud, ransomware, mass extortion and trade fraud where buyers wire funds for a product that is never delivered. The numbers have been provided by the National Special Crime Unit's annual report for 2023, which is available at the website of the Danish police.

THE ATTACK ON AZEROCLOUD

The impact of ransomware attacks can extend beyond the intended target. For instance, if you store data with an external provider, a ransomware attack on the provider could have dire consequences.

In August 2023, Danish hosting provider AzeroCloud fell victim to a ransomware attack. According to AzeroCloud, the criminal hackers managed to encrypt all data, including backups. As a result, most of AzeroCloud's customers lost all their data. In March 2024, AzeroCloud announced that it had filed for bankruptcy.

through data encryption. Typically, the criminals behind ransomware attacks will demand payment in cryptocurrency in exchange for decryption.

Everyone is a potential ransomware target given the opportunistic nature of cyber criminals. Any type of organization, no matter the profile and size, can become a target. Hackers target small and medium-sized companies where little effort is required to breach security measures. At the same time, they target large companies in the hope of maximizing profits. For instance, manufacturing companies are attractive targets for ransomware actors looking to make a huge profit. Manufacturing companies typically have relatively high turnovers and are thus in a financial position to pay high ransoms. In addition, they can be pressured further as they cannot afford the downtime that could result from the ransomware attack.

Some of the criminal actors typically behind ransomware attacks have also employed other extortion tactics. For instance, some groups steal data from victims without encrypting the victim's data but subsequently threaten to leak or sell the stolen data unless the victim pays a ransom. This could have a significant impact on the affected companies and authorities but also on their partners, customers, citizens, etc. if their data is leaked. Criminal hackers often leak data on so-called dedicated leak sites (DLS) on the dark web.

During the course of 2023, there have been examples in Denmark where cyber criminals have attempted to extort organizations by threatening to leak stolen personal data. For instance, several media have described how criminal hackers gained access to personal information and documents in an attack on Danish real estate chain EDC. Subsequently, the hackers tried to extort EDC, but when the company refused to pay ransom, the stolen information was leaked on the dark web.

Victims can never be sure that their files or systems will be unlocked or that their stolen data will be deleted. For instance, in February 2024, it was revealed that the LockBit ransomware group lied about destroying stolen data after the victims had given in to extortion demands.

Cyber criminals also participate in other types of cyber crime

Cyber criminals employ different measures for financial gain, and cyber crime is thus not limited to extortion or ransomware attacks. For instance, cyber criminals can make money by selling data and system access and by tricking their victims into wiring money to them.

Well-established underground markets exist where cyber criminals can sell compromised data or system access to other cyber criminals. Hackers specializing in obtaining and selling access to compromised systems or networks are called Initial Access Brokers (IAB).

NOTORIOUS RANSOMWARE GROUPS EXTORT DANISH VICTIMS

Danish organizations are not immune to extortion by cyber criminals. Different ransomware groups that cause significant damage to organizations across the world regularly claim to have also hit Danish targets. During the course of 2023, at least five notorious ransomware groups had listed Danish victims on their respective DLS. When the groups publish the names of compromised organizations on their DLS, it is an attempt to coerce them and future victims into paying ransom.

Ransomware groups demand millions of dollars in ransom each year. For instance, US and UK authorities claim that the LockBit ransomware group has received more than USD 120 million in ransom payments and that it has executed attacks against more than 2,000 victims.

In addition to buying and selling system accesses, cyber criminals also sell malware and services to each other. This form of platform economy contributes to increasing the extent of cyber criminal attacks and their financial rewards. The possibility for hackers to purchase specialized services raises the likelihood of a successful cyber attack. In addition, trade and exchange of services between cyber criminals allow them to expand their capabilities as hackers can hone their skills in individual parts of the attack chain.

Fraud is another common type of cyber crime. BEC scams are the most frequently reported type of fraud against public authorities and private companies. BEC fraud involves criminals trying to steal money from organizations by sending them fake money transfer requests. In some incidents, the hackers compromise a legitimate email account with a company or its partners and subsequently manipulate the employees into wiring funds to them. On a global scale, BEC fraud is among the most lucrative forms of cyber crime. Denmark has also seen its fair share of BEC fraud resulting in significant financial losses. For instance, in 2023, a Danish local authority paid fake invoices at a value of approx. DKK 1.5 million in a BEC scam.

Fraud that specifically targets individuals often comes in the form of phishing, resulting in credit card and online banking fraud. For instance, cyber criminals use malware to steal login credentials, but many attempts at fraud against individuals are not cyber-enabled. Cyber-enabled and non cyber-enabled credit card and online banking fraud lead to significant financial losses each year.

Cyber crime affects everyone, ranging from large organizations to single individuals, which is why it is relevant to describe the most common techniques used by cyber criminals. However, the techniques are not solely for cyber crime purposes. Foreign states also use these attack techniques to achieve their goals.

Cyber criminals exploit vulnerabilities

Most cyber criminals often exploit known software vulnerabilities to launch attacks. In this context, a vulnerability is a weakness in a piece of software that could be exploited by hackers to compromise information security. When a vulnerability becomes known, a security patch that will fix the vulnerability will typically be issued in response. Old vulnerabilities, however, are still being exploited because some companies and authorities fail to patch them successfully. The CFCS assesses that cyber criminals are generally quick to exploit new vulnerabilities.

Cyber criminals also exploit unpatched vulnerabilities, so-called zero-day vulnerabilities. In 2023, several cyber attacks were launched via zero-day vulnerabilities. It is likely that some criminal hackers either detect zero-day exploits themselves or buy them from other hackers. In addition, cyber criminals buy and sell zero-day exploits for large sums at underground markets.

CRIMINAL HACKERS TARGET COMPANIES WORLDWIDE

In 2023, several companies were compromised through a so far unknown vulnerability in the file transfer software MOVEit. By attacking a widely distributed software programme, the hackers were able to attack numerous companies and exploit their unauthorized access to extract data.

The campaign was attributed to the criminal hacker group CL0p. CL0p has continually extorted victims by naming them on its DLS. Danish companies have also been affected by Cl0p's campaign.

Cyber criminals can also find exploitable vulnerabilities in internet-connected devices used by private individuals and businesses. These devices often go by the name Internet of Things (IoT). IoT devices encompass cars, televisions, printers and network equipment. The distribution of internet-connected devices carries a significant security risk as IoT devices are inherently more vulnerable to security threats and attacks as their security measures are weaker than the ones seen in regular computers. As a result, they can provide a relatively direct entry point into a network. At the same time, the wide distribution of devices has significantly expanded the attack surface for cyber criminals.

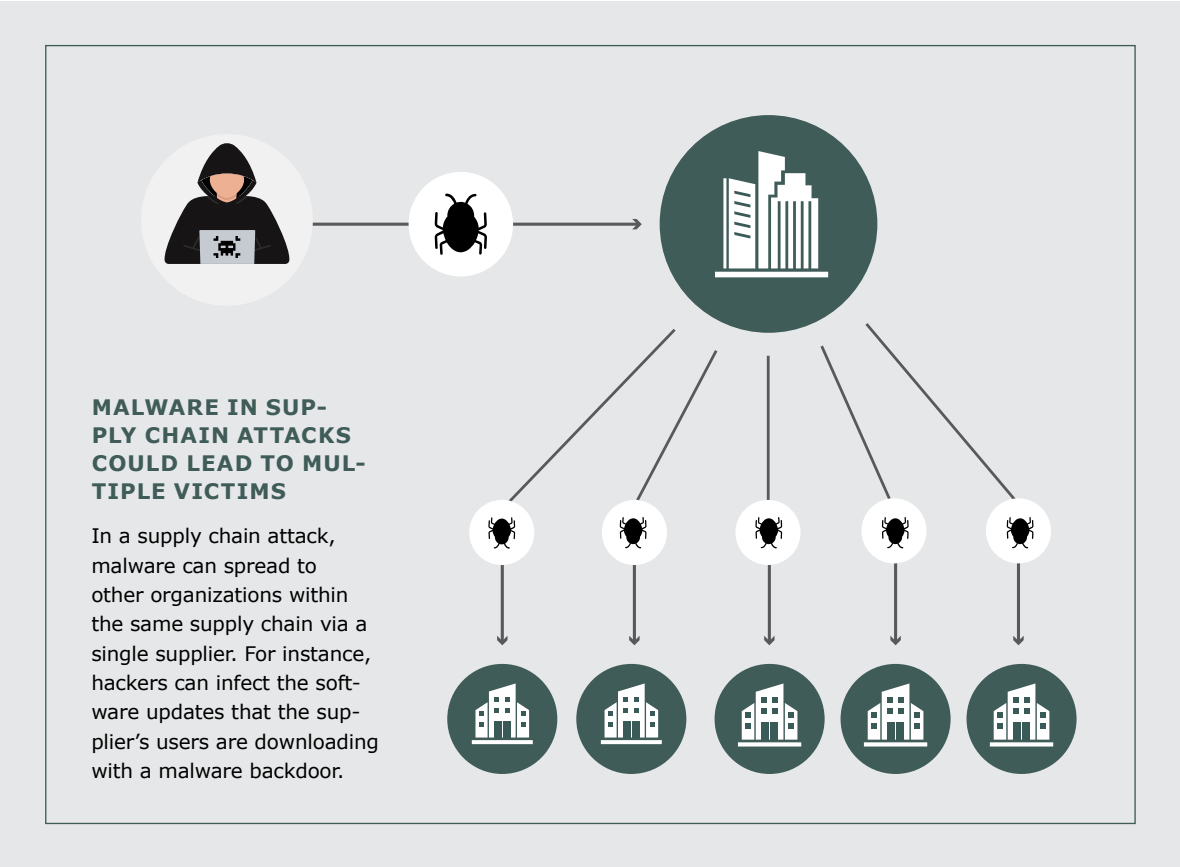
Criminal hackers exploit supply chains

Hackers can try to gain access to customer networks or systems through suppliers and software providers. To this end, a supplier or software solution can be used as a stepping stone for attackers to launch attacks on other targets. Once a supplier is compromised, the supply chain could suffer serious direct or indirect consequences. Supply chain attacks are effective as hackers can gain access to multiple targets by compromising a single link in the supply chain.

Cloud solution providers are also prime targets of cyber attacks as some organizations use this type of solution to store their data. Cloud services have become indispensable tools for many private companies and public authorities, offering flexibility, convenience and cost efficiency. Attacks on cloud providers could thus have far-reaching consequences as they cater to a broad range of customers offering standard services as well as services tailored to the specific needs of their customers.

RANSOMWARE ATTACK AGAINST FINNISH CLOUD-HOSTING COMPANY AFFECTS SWEDISH ORGANIZATIONS

In January 2024, the Finnish company Tietoevry was hit by a ransomware attack. Tietoevry offers, among other services, cloud hosting for many Swedish organizations. According to the provider, the ransomware attack hit one of the Swedish data centres which affected multiple Swedish companies. Furthermore, the attack caused the payment system of a number of Swedish authorities to stop working. According to open sources, the attack also affected authorities' it systems, e.g. the health journal system in Uppsala.



MALWARE IN SUPPLY CHAIN ATTACKS COULD LEAD TO MULTIPLE VICTIMS

In a supply chain attack, malware can spread to other organizations within the same supply chain via a single supplier. For instance, hackers can infect the software updates that the supplier's users are downloading with a malware backdoor.

Phishing

The CFCS assesses that phishing emails still remain among the hackers' weapons of choice. Phishing is used by all types of hackers because it is effective and easy to leverage. In phishing attacks, the sender tries to trick unsuspecting recipients into disclosing personal or other sensitive information or allowing unauthorized access to it systems, among others. Phishing is often the most common route used by ransomware actors to achieve initial access.

Cyber criminals have long used phishing but the method keeps evolving. The CFCS has previously described how chat bots allow hackers to streamline the production of phishing emails. For more information, please read the CFCS threat assessment *Hackers exploit generative AI* on the website of the CFCS.

Exploitation of weak or recycled passwords

Another simple yet effective attack technique used by cyber criminals is brute force attacks. The term covers different types of attacks in which hackers try to guess combinations of usernames and passwords, for instance by exploiting passwords from previous data leaks or by systematically guessing combinations across several different user accounts.

CYBER ACTIVISM

The threat of cyber activism against Denmark is **HIGH**. The threat mainly emanates from pro-Russian cyber activists and affects all sectors of society. However, the attacks have often been pointed towards the financial and transport sector as well as the area of authority under the Danish defence ministry. It is highly likely that cyber activists will launch attacks on Danish public authorities and private companies within the next two years.

■ Cyber activism is cyber attacks carried out by groups or individuals with the purpose of raising awareness to a specific cause or issue. Cyber activists are typically motivated by ideological or political beliefs, ranging from single issues to individuals or organizations perceived to be opponents of their cause.

Cyber activism against Danish targets has become the norm

The high threat of cyber activism against Danish private companies and public authorities has become the norm following Russia's invasion of Ukraine. The threat should be considered in the context of Denmark's role as a provider of military support to Ukraine and as a member state of the EU and NATO. Pro-Russian activists continually attack companies and organizations in Europe and NATO that they view as being representative of Western support to Ukraine.

The pro-Russian groups are a good example of how the actions of cyber activists can support nation state interests. However, that does not mean that they work directly for the state. The CFCS assesses that some pro-Russian cyber activists are linked to the Russian state.

The typical form of cyber activism is motivated by ideological or political concerns and is for the most part carried out independently of states. However, it can be difficult to assess a cyber activist's affiliation with foreign states. In some cases, it is thus not clear whether cyber activists are acting on their own initiative or on behalf of a state.

The pro-Russian cyber activist group NoName057(16) has claimed responsibility for attacks on Danish targets. For instance, in February 2024, the group claimed to have been behind a series of DDoS attacks that took down a number of Danish websites.

Even though the threat of cyber activism against Denmark primarily emanates from pro-Russian activists, the threat can also arise from other cyber activist communities without warning. A case in point was the international attention triggered by the Quran burnings in Denmark and Sweden in early 2023. In response to the burnings, several cyber activist groups launched DDoS attacks on Danish and Swedish websites. At the same time, they also called on other activists to launch cyber attacks on Danish and Swedish targets. The DDoS attacks struck smaller and larger critical sector companies and authorities. For instance, the central bank of Denmark and a number of Danish hospitals, including Rigshospitalet, Denmark's largest hospital, were the targets of DDoS attacks.

The attacks are disruptive but not devastating

Cyber activists mainly use DDoS and defacement attacks against Danish private companies and public authorities. They typically attack the victims' user-fac-

THE TOOL KIT OF CYBER ACTIVISTS: MOST COMMON ATTACK TECHNIQUES

DDoS
DDoS stands for Distributed Denial of Service and is a cyber attack in which the attacker floods a server with internet traffic. Hackers exploit compromised computers to send massive volumes of data traffic to a target website (web server) or network. The aim is to render the website or network inaccessible to legitimate traffic while the attack is ongoing. For instance, if the server that is under attack hosts the victim's user-facing website, a DDoS attack can render the website unavailable to users.

Defacement
Defacement of a website is an attack that alters the visual appearance of a website. For instance, attackers can change the content of the defaced website with a picture or a message which supports the issue or case they stand for.

Hack and leak attacks
A goal or sub-goal of hack and leak attacks can be to cause reputational damage to the affected organization, for instance by leaking internal documents or data from a compromised system or network.

ing websites. Both DDoS and defacement attacks can render the victims' websites temporarily unavailable. DDoS attacks disrupt websites by overwhelming them with malicious traffic. Defacement attacks occur when activists infiltrate a website and replace its content with their own messages. Both types of attack are disruptive but not destructive per se to the victims' systems. The downtime of victim websites contributes to drawing attention to the activists' cause.

Both types of attack are relatively simple, and the activists do not need to develop advanced technical skills in order to execute them.

Activists can also use hack and leak attacks against their victims that involve leaking documents or data acquired by compromising a system or network. Hack and leak attacks can spark uncertainty and concern with their victims as to the potential consequences of a data leak. The potential consequences can impact customer trust in the affected organization. The attack itself does not, however, have a devastating impact on the victim's systems.

Cyber activists claim responsibility for destructive cyber attacks
The CFCS assesses that some cyber activist groups are intent on launching destructive cyber attacks but have limited capabilities.

Cyber activists primarily pose a threat to organizations with weak security measures in place. As a result of weak security measures, even cyber activists with limited capabilities can compromise a system.

CYBER ACTIVISTS WARN OF LARGE-SCALE ATTACK – WITH LIMITED ACTUAL IMPACT

An example of how cyber activists put out misleading information about their attacks is from the summer of 2023. Two pro-Russian groups warned that they would launch the world's largest ever cyber attack on European banks in collaboration with a known cyber criminal group.

The groups stated on their social media platforms that the aim of the attack was to put an end to Western support for Ukraine. The groups emphasized that they would not only launch DDoS attacks. However, in the subsequent period, only a few DDoS attacks against European banks were registered – and none of them had any significant impact.

Some cyber activist groups have claimed responsibility for destructive cyber attacks in connection with conflicts, for instance the conflict between Israel and Hamas and Russia's invasion of Ukraine. However, few of the attacks have had any recognizable impact.

Several confirmed and unconfirmed attacks have been directed at internet-facing operational technology (OT). OT encompasses technologies that enable real-time control, monitoring and data collection from physical devices. OT is primarily used in the industrial sector but also in other sectors such as the defence and hospital sectors. If cyber activists compromise OT in organizations that manage critical infrastructure, the consequences could be severe. It could affect a lot of people and disrupt the delivery of essential services. The CFCS continually monitors developments in the cyber activist threat landscape.

The CFCS assesses that both actual destructive cyber attacks and false claims of destructive cyber attacks are aimed at drawing public attention to the activists' agenda. By falsely claiming to be responsible for destructive cyber attacks, the activists can draw attention to their cause without having to develop the capabilities to carry out the actual attacks.

The communication practices of cyber activists can shape a false narrative that impacts the threat landscape

The primary goal of cyber activists is typically to draw attention to their cause. Consequently, any mention of their attacks is almost equally important as the attacks themselves. Oftentimes, activists amplify alleged attacks and exaggerate their impact. The misleading communication is a tool used by cyber activists to reinforce their political narrative and the psychological effect of their cyber attacks.

Cyber activists use their social media platforms to exaggerate the impact of their attacks, for instance by describing simple DDoS attacks on user-facing websites as incidents causing operational disruptions in critical infrastructure even though this is not actually the case.

FOLLOW US

X@Cybersikkerhed

LinkedIn@Centre for Cyber Security

DESTRUCTIVE CYBER ATTACKS

The threat of destructive cyber attacks against Denmark is **MEDIUM**. In June 2024, the CFCS raised the threat level from **LOW** to **MEDIUM**. The decision to raise the threat level is based on Russia's likely increased willingness to use destructive hybrid tactics against European NATO member states. The CFCS assesses that this increased risk appetite also includes destructive cyber attacks.

CFCS' DEFINITION OF DESTRUCTIVE CYBER ATTACKS

The CFCS defines destructive cyber attacks as attacks that could result in:

- death or personal injury
- signicant property damage
- destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken

Hackers launching destructive cyber attacks particularly use wiper malware to achieve their objectives. Wiper malware is a type of malware designed to delete, overwrite or encrypt data, making them inaccessible.

However, in the current situation, it is less likely that Russia is intent on launching destructive cyber attacks on Denmark with serious and far-reaching consequences for critical societal functions.

The threat level primarily reflects the risk of small-scale destructive cyber attacks, including attacks with limited impact on critical societal functions. However, small-scale attacks can still have a serious impact on the victim and society at large. Even if destructive cyber attacks have no consequences for critical societal functions, they can cause insecurity and affect society as a whole.

Even if it is less likely that Russia will launch destructive cyber attacks with serious and far-reaching consequences, the CFCS assesses that hacker groups linked to Russia are continually preparing the capability to launch destructive cyber attacks against Denmark. The likelihood of this type of attack occurring could thus increase at short notice or without any warning – particularly if the conflict between Russia and the West escalates or changes.

In that case, potential targets could include critical infrastructure systems. If these systems do not work, it could affect the capability of the Danish Defence to carry out its mission or otherwise affect the population or the political system's resilence in connection with an escalating conflict with Russia.

The threat primarily comes from Russia

Should Denmark fall victim to a destructive cyber attack in the current situation, Russia would be the most likely perpetrator. The threat of destructive cyber attacks primarily stems from Russian state-sponsored hackers, but non-state hackers with various degrees of ties to the Russian state also pose a threat.

Destructive cyber attacks are but one of various hybrid tactics that Russia can use to achieve strategic benefits. Russia's overall purpose of using hybrid tactics against the West is to put pressure on decision-makers and populations, for instance by creating confusion and insecurity.

The CFCS assesses that in the current situation, Russia will make efforts to conceal its involvement in destructive cyber attacks, making it difficult for the affected countries to respond to Russia's hybrid activities, especially if the attacks cannot be unequivocally attributed to Russia. For instance, Russia can launch attacks mimicking criminal ransomware attacks, in which data is encrypted but subsequent decryption is not possible. There have been previous examples of such fake ransomware attacks.

However, the ransomware attacks that have hit Danish organizations within the past few years have highly likely been conducted by criminal hackers aiming to achieve financial gain rather than destroying data or infrastructure. The CFCS expects that future ransomware attacks will, for the most part, be carried out by financially motivated criminal hackers.

State-sponsored hackers could also try to conceal their involvement in destructive cyber attacks by posing as activist hackers, for instance by creating websites or accounts on different platforms where they pose as cyber activists and claim responsibility for destructive cyber attacks.

Another way for Russia to conceal its involvement in destructive cyber attacks is to convince other actors to carry them out on its behalf. As a result, non-state hackers also pose a potential threat.

As mentioned in the section on cyber activism, the CFCS assesses that some cyber activists are intent on launching destructive cyber attacks but that they primarily pose a threat to systems with weak security measures in place.

FOREIGN STATES ARE CAPABLE OF LAUNCHING SIMPLE AS WELL AS ADVANCED DESTRUCTIVE CYBER ATTACKS

Destructive cyber attacks are possible by employing advanced or less advanced techniques. For instance, hackers can exploit widespread vulnerabilities to launch simple wiper malware attacks on poorly protectced targets. This type of attack does not necessarily require a long time of preparation.

More advanced and targeted destructive cyber attacks typically require sigificant preparation.

The purpose of attacks is likely to sway the population

It is likely that potential Russian destructive cyber attacks will primarily be aimed at swaying the population and decision-makers, including weakening Danish support for Ukraine.

As destructive cyber attacks are frequently used in support of influence operations, the CFCS assesses that many types of organizations in critical sectors could become potential targets of destructive cyber attacks. Following the Russian invasion of Ukraine in 2022, Ukraine has been a frequent target of destructive cyber attacks, ranging from supermarkets to government authorities. The purpose of most of the attacks was likely to put pressure on and burden the Ukrainian society.

Even though destructive cyber attacks are launched with the overall purpose of destroying something, the attacks could be tools to achieve other strategic objectives in which the damaging impact is secondary. In the current situation, it is likely that the specific physical impact of potential attacks on Denmark would be secondary to the hackers launching them. Rather, the primary aim would be to create widespread attention.

DESTRUCTIVE CYBER ATTACKS HAD LIMITED IMPACT

Destructive cyber attacks can have very different consequences depending on the targets and attack techniques. As mentioned, in the current situation, it is less likely that Russia is intent on launching destructive cyber attacks on Denmark with serious and far-reaching consequences for critical societal functions. However, small-scale cyber attacks could also have an impact on critical societal functions.

An example of a destructive cyber attack with limited impact on critical societal functions took place in Ireland in December 2023. The attack hit a water utility and, according to the media, left some 200 households without water for two days. In the attack, the computers of the water utility were defaced with an anti-Israel message.

Other states have the capabilities to launch destructive cyber attacks

Several foreign states have the capabilities to launch destructive cyber attacks. Even though the threat mainly comes from Russia, Iran also poses a threat. It is likely that Iran has previously launched destructive cyber attacks against Western targets.

For instance, a group calling itself CyberAv3ngers have claimed responsibility for a number of destructive cyber attacks on poorly protected OT equipment in Western countries. In this connection, the group designated all equipment produced in Israel as legitimate targets in response to the conflict between Israel and Hamas.

VOLT TYPHOON HAS CONDUCTED CYBER ESPIONAGE AGAINST CRITICAL INFRASTRUCTURE IN THE UNITED STATES

In February and later again in March 2024, CISA, NSA, FBI and a number of other US authorities and international partners issued warnings about the Volt Typhoon hacker group. According to the warnings, the group is a Chinese state-sponsored group that has targeted critical infrastructure.

According to several media, the group has been active since mid-2021 and possibly even longer and has continually compromised systems and made attempts to retain unauthorized access. It compromised the systems of critical sectors such as the transportation, water and waste water system and energy sectors in the United States and Guam, which is part of US territory.

US authorities assess that Volt Typhoon compromised the targets with the purpose of being able to move from one it system to other OT systems for subsequent destructive cyber activity. Authorities assess that the group will make use of destructive cyber attacks in case of geopolitical tensions and military conflicts between the United States and its allies and China.

The US Cybersecurity and Infrastructure Security Agency has publicly linked CyberAv3ngers to Iran's Revolutionary Guards Corps (IRGC). In addition, the United States has sanctioned six individuals from the IRGC over the group's destructive cyber attacks on US targets. The attacks are thus an example of how state hackers can disguise their attacks as activism.

China primarily uses its extensive cyber capabilities for espionage purposes. It is highly likely that China also has the capability to launch destructive cyber attacks. Still, it is highly unlikely that China is currently intent on launching destructive cyber attacks on Danish targets. However, in a heightened conflict, the likelihood of China launching destructive cyber attacks could change. In such a case, China would likely direct attacks on adversaries which are expected as opponents in a potential future conflict. This includes countries in China's vicinity or countries that would in all likelihood support Taiwan in a potential war between China and Taiwan.

READ MORE

More threat assessments available at **cfcs.dk**

CYBER TERRORISM

The threat of cyber terrorism against Denmark is **NONE**. The CFCS assesses that, at present, there are no actors with the capabilities and intent to conduct cyber terrorism against Denmark. Thus, it is highly unlikely that Danish public authorities and private companies will become targets of attempted cyber terrorism within the next two years.

■ As of yet, the CFCS has no knowledge of any examples of cyber terrorism. Since 2016, the CFCS has monitored developments in the cyber terrorism threat, with special focus on militant extremists and developments in both their capabilities and intent to launch cyber terrorism.

The CFCS defines cyber terrorism as serious, politically motivated cyber attacks aimed at creating effects comparable to those of conventional terrorist attacks, such as cyber attacks causing physical harm to humans or property.

The Centre for Terror Analysis (CTA) under the Danish Intelligence and Security Service (PET) assesses that the threat of conventional terrorism against Denmark and Danish interests is at the level of significant, which is category 4 out of 5. CTA assesses that the conventional terrorist threat to Denmark emanates from militant Islamists, in particular, and to a lesser extent from right-wing extremists, anti-establishment extremists and left-wing extremists. In addition, CTA assesses that a terrorist attack will most likely be carried out by lone actors or small groups of individuals using easily accessible means. The CFCS assesses that these individuals and groups have neither the intent nor the capability to launch serious cyber attacks aimed at creating effects comparable to those of conventional terrorist attacks.

FOLLOW US

X@Cybersikkerhed

LinkedIn@Centre for Cyber Security

PERSPECTIVE:
FROM CYBER THREAT TO CYBER SECURITY – THE PERPETUAL RACE AGAINST HACKERS

■ From the previous chapters, it has become clear that Denmark is facing different cyber attack threats. The next chapter thus provides an overall introduction of how focus on cyber security can help prevent hackers from compromising systems.

The chapter deals with some overall security measures and specific themes that may make a difference in the cyber security battle. However, cyber security needs to align with individual organization needs and requires continuous effort and adaptation to the ever-changing threat landscape.

Simple attack techniques must be rendered ineffective

Knowledge of the cyber threat may help organizations to prioritize security measures. Unfortunately, simple attack techniques still provide easy points of entry for state actors and cyber criminals. Many organizations struggle to keep basic security measures intact. If security measures have not been put in place, hackers will be able to exploit the security gaps.

Nevertheless, the issue of cyber security has become increasingly relevant, and many organizations in Denmark are taking important and necessary steps to address cyber security issues. More initiatives are on the way, and the implementation of the NIS2 Directive, for instance, will help improve cyber security efforts across all levels of society, not only in Denmark but also across the EU.

Cyber security training should be mandatory for all employees

Regardless of the security measures implemented, employees might still inadvertently let attackers into the organization. Employees, and especially their interaction with hackers through phishing emails, plays a role in the majority of cyber attacks.

Consequently, organizations should continuously train employees in cyber security and awareness, right from the beginning of their onboarding process. Further, the it security organization and top management should make sure to implement security policies and measures in support of these efforts, including organizational, technological, behavioural, and physical measures and policies. The top management should also foster a security culture where employees are not afraid to admit mistakes and know where to report security incidents, among other things.

Support strong passwords

Passwords illustrate the interaction between information security and technical support of employees. On the one hand, employees are responsible for creating strong and unique passwords that are known only by them. On the other hand, the organization should educate employees on password security and introduce password strength requirements that help employees create strong passwords. The organization can also support its employees by providing an approved password manager. A password manager is a software application for storing login credentials securely. Thus,

MULTI-FACTOR AUTHENTICATION COULD HAVE PREVENTED SERIOUS RANSOMWARE ATTACK

In 2021, US company Colonial Pipeline fell victim to a ransomware attack in which hackers were able to access the company's network by using a compromised password for a VPN account that did not use multi-factor authentication.

The attack forced the company to temporarily shut down the main pipelines carrying fuel to the US East Coast. The repercussions were severe as the shutdown affected oil prices, among other things, and resulted in fuel shortage in the area.

the user needs only to memorize one very strong password: the one for the password manager.

Install multi-factor authentication
Multi-factor authentication is an example of another effective security measure designed to help employees and organizations. When private organizations, public authorities and individuals use multi-factor authentication to protect their email accounts or critical systems, they rob hackers of some of their primary tools. For instance, they prevent hackers from exploiting brute force attacks in which they systematically try to guess or crack weak and re-used passwords. Multi-factor authentication also makes it harder for hackers to exploit login credentials accessed via phishing or spear phishing emails.

Multi-factor authentication could have prevented many successful cyber attacks, including cyber attacks that have subsequently had serious consequences for the organizations affected and in some instances for Denmark as a whole.

Update software
Other steps that could be taken by private companies, public authorities and individuals include updating software when new versions or security updates are released from the supplier, including updates of operating systems, applications, and firmware on mobile units, IoT units and servers. Software should be updated as soon as new security updates are released as hackers are quick to exploit known vulnerabilities. If possible, automatic security updates should be applied. If this is not an option, it is important to stay informed of which serious known vulnerabilities are being actively exploited by hackers. The organization should also develop procedures to minimize the risk of a known vulnerability being exploited until updates are available. A measure could be to isolate the vulnerable unit from the rest of the organization's network or disconnect the unit from the internet – an approach that could also become relevant when hackers exploit zero-day vulnerabilities.

When getting outsmarted by hackers can still happen to the best of us
It is less a question of if a cyber attack on a public authority or private company *will* occur and more one of *when* it will happen. With the proper preparation, organizations will be able to increase their chances of detecting the hackers and containing the compromise. At best, organizations will be able to successfully prevent hackers from achieving their goals.

OUTSOURCING OF SECURITY IS A VIABLE SOLUTION, BUT RESPONSIBILITY CANNOT BE OUTSOURCED

Many organizations opt to outsource their it operations, including it security operations. However, outsourcing does not relieve the organization from its security responsibility. The organization needs to set relevant it operation and security requirements for their suppliers. Also, the organization must continually conduct inspections to ensure effective compliance and adequacy.

For additional guidance, read the CFCS guide *Cyber security in supplier relationships* on the website of the CFCS.

It is key that the top management provides the support needed for the organization to address compromises, for instance, by preparing and regularly practicing contingency plans and business continuity plans in case of a crisis. Other security measures are of a more technical nature but still require support from the top management. Technical measures, for instance, include a fully functional backup. Most organizations are aware of this security measure because ransomware attacks have repeatedly highlighted the importance of a full-fledged backup support feature. By keeping backup offline or offsite, it will prove significantly harder for ransomware actors to encrypt the actual backup.

Other technical measures such as monitoring, segmentation and rights and access control management deserve more focus as they could prevent many ransomware actors and state actors from achieving their goals.

Also, the CFCS and it security companies often encounter challenges triggered by insufficient logging when investigating specific security incidents. Logging is the backbone of a resilient cyber defence as it enables organizations to investigate where, when and how hackers gained unauthorized access as well as their movements inside the organization's networks.

From cyber threat to risk assessment

It is the individual organization's responsibility to determine how it wants to prioritize and address security issues within the framework of the law and other regulations and ensure compliance with the organization's objectives and ambitions. Security comes at a price and can also come at the expense of, for instance, availability. Knowledge of the cyber threat is one aspect in such a risk assessment, which helps the organization to prioritize resources and security measures. Another aspect is understanding of the organization's operations and priorities.

Even though anyone can become a victim of cyber crime, certain public authorities and private companies are more at risk. Traditionally, state actors mainly focus their attention on organizations working within the realm of foreign, security and defence policy. The sophisticated cyber criminals that are a focal point of our investigative efforts are more opportunistic in their approach, targeting high-profit companies for extortion and fraud.

This threat assessment provides an overall status of the cyber threat against Denmark. In addition, the CFCS has published several other threat assessments outlining sub-elements of the threat landscape, which are available on our website. Also, the CFCS regularly publishes new risk assessments.

Guides on how to improve cyber security are also available on the CFCS website. The guide *Effective Cyber Defence* provides a detailed introduction to the security measures outlined in this chapter, including recommendations on how to address the cyber threats that organizations face.

PLEASE FIND OUR OTHER GUIDES ON THE CFCS WEBSITE

FOLLOW US

X@Cybersikkerhed

LinkedIn@Centre for Cyber Security

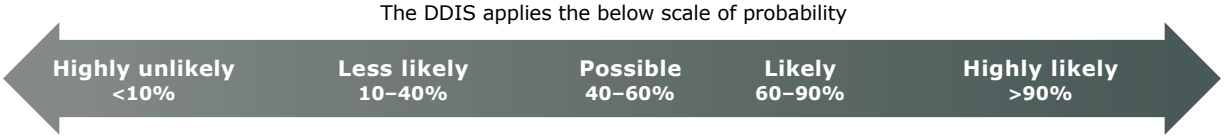
THREAT LEVELS

The Danish Defence Intelligence Service use the following threat levels.

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

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

The DDIS applies the below scale of probability



The probabilities are estimates, not calculated statistical probabilities
"We assess" corresponds to "likely" unless a different probability level is indicated

THE CYBER THREAT AGAINST DENMARK 2024

1st edition
September 2024

Foto
Cover, DRONERUNE
Page 10 and 29, SCANPIX

FE CENTRE FOR CYBER SECURITY

Centre for Cyber Security
Kastellet 30
DK-2100 København Ø

Phone number: +45 3332 5580
Email: cfcs@cfcs.dk
www.cfcs.dk
www.fe-ddis.dk