CENTRE FOR
CYBER SECURITY

Threat assessment

The cyber threat against the telecom sector

1st edition June 2022

Indhold

CENTRE FOR
CYBER SECURITY

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave juni 2022

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

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

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

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

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

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

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

The cyber threat against the telecom sector

The purpose of this threat assessment is to provide decision-makers in the telecom sector with an updated insight into the cyber threats against the sector. In the assessment, the Centre for Cyber Security lowers the threat level of cyber espionage against the sector from **HIGH** to **MEDIUM** and raises the threat level of cyber activism from **LOW** to **MEDIUM**. The present assessment replaces the 2019 threat assessment for the telecom sector.

Key assessment

- The threat of cyber crime is **VERY HIGH**. The general threat from criminal hackers against Danish companies also extends to the telecom sector. Some types of companies, including within the telecom sector, may be particularly vulnerable to cyber crime. The threat of cyber crime is serious to the point where telecom companies are the targets of daily reconnaissance or compromise attempts by hackers.
- The threat of cyber espionage is **MEDIUM** against the Danish telecom sector. The threat level is lowered from **HIGH** to **MEDIUM**, as it is assessed that the sector is currently not a high-priority target for attacks. Foreign states, however, retain the capacity for espionage against the telecom sector and compromise of telecom infrastructure, and it is possible that the sector in Denmark will be the target of attempted cyber espionage.
- The threat level of cyber activism is raised from **LOW** to **MEDIUM**. The Centre for Cyber Security raises the threat level based on activist cyber attacks against Western European NATO countries in connection with the situation in Ukraine. It is possible that pro-Russian hackers will turn their attention to targets in Denmark, including the telecom sector.
- The threat of destructive cyber attacks is **LOW**. It is less likely that foreign states will conduct destructive cyber attacks against Denmark. Private companies and public authorities operating or relying on suppliers in conflict areas are more exposed to the threat, though.
- The threat of cyber terrorism is **NONE**. Serious cyber attacks whose intention is to mimic the effect of conventional terrorism require technical skills and organizational resources that are currently not available to militant extremists. In addition, there is limited intention among these groups for cyber terrorism.

Introduction

Denmark is one of the most digitised countries in the world. Effective and secure digital communication between humans and machines is a precondition for the digitised society, making availability, confidentiality and integrity of telecom services crucial to the functioning and security of society.

This threat assessment provides an overview of the cyber threats against telecom providers in Denmark that offer electronic communication networks and services to public authorities, private companies, and private citizens. Examples of telecom services include voice call and Internet connections through landlines or mobile networks, and services dedicated to communication between machines, also known as Internet of Things (IoT).

Cyber attacks against the telecom sector serve different purposes. While some attacks mainly constitute a threat to the targeted companies and their finances, others may also carry implications for company customers. Cyber attacks that threaten telecom services are particularly serious, as unavailability of these services may, in addition to being a nuisance to individual users, impact production in companies and prevent other critical sectors – including the emergency services, and the energy supply and health sectors – in Denmark from functioning optimally.

This threat assessment is divided into sections dealing with the threats of cyber attacks in support of crime, espionage, activism, destructive attacks and terrorism, and describes the current threat situation with a warning horizon of two years. The assessment concludes by giving an outline of the impact of 5G on the cyber threat against the telecom sector.

Significant changes compared to the 2019 cyber threat assessment are the lowering of the threat level of cyber espionage from **HIGH** to **MEDIUM**, and the raising of the threat level of cyber activism from **LOW** to **MEDIUM**.

Following Russia's invasion of Ukraine on 24 February 2022, Denmark is facing a changed security policy landscape in which the future, in many respects, seems more uncertain than ever. This uncertainty has also spread to the cyber realm where the threat situation may change with little warning if, for instance, the relationship between the NATO countries and Russia were to deteriorate markedly.

The Centre for Cyber Security is keeping a constant eye on the threat situation, including trends abroad that may impact the cyber threat against the Danish telecom sector, and will update the threat assessment in case of any major changes to the threat landscape.

Cyber crime

The threat of cyber crime against the telecom sector is **VERY HIGH**. As a result, it is highly likely that telecom operators in Denmark will become targets of attempted cyber crime within the next two years.

The Centre for Cyber Security (CFCS) uses the word "cyber crime" as a collective term for actions in which hackers use cyber attacks to commit crimes for financial gain.

The CFCS assesses that the general threat of cyber crime extends to the telecom sector, making it highly likely that the telecom sector is the target of attempts at compromise or vulnerability reconnaissance on a daily basis.

While criminal hackers do not generally target specific sectors but will attack any public authority or private company with an online presence, some telecom companies are more at risk of, for instance, cyber extortion attacks. Their appeal to hackers lies in the criticality of the telecom sector to society, and the fact that the sector handles sensitive data and depends on high up times on their IT systems and telecom services. Hackers may thus calculate that telecom companies will be more willing to pay ransoms in order to return to normal operations as quickly as possible after an extortion attack.

Extortion attacks involving ransomware may affect telecom services
Ransomware attacks are one type of extortion attacks which constitutes a threat to the Danish telecom sector. In this type of attack, criminals encrypt critical IT systems belonging to public authorities or private companies, making the systems inaccessible until a ransom is paid to release the decryption key needed to unlock them. In addition to encrypting victim data, the criminals also extort their victims for ransoms, threatening to publish data stolen in connection with the attack.

Extortion through ransomware attacks has grown to the point where Danish telecom service providers are highly likely to fall victim to attempted ransomware attacks in the short term.

Danish telecom service providers have fallen victim to ransomware
The TT network, the joint mast operation of Danish telecom providers Telia and Telenor, was hit by ransomware in December 2021. The hackers later threatened to leak the data stolen in the attack. The mobile network was not affected by the incident.

GlobalConnect Denmark, a provider of communication networks, Internet connections, telephony and IT services for businesses, was hit by ransomware in their office network in November 2019. While the attack hit parts of the company's Danish and German business, it did not impact its customers.

In May 2020, GlobalConnect once again became the target of a ransomware attack. This time, the attack affected the company's IT services, crippling the IT systems of several customers. According to the company, the attack did not affect the customers' telecom services.

Ransomware attacks usually target the office network, the main reasons being that the office network, unlike the telecom infrastructure, is almost always connected to the Internet and that staff email accounts are hosted on the office network. For that reason, malware often entering via Email and remote access solutions used for working from home, etc. initially ends up in the office network.

If ransomware in the office network prevents operating staff from accessing the telecom infrastructure from the network, this may complicate the operations of the telecom infrastructure, in turn affecting the telecom services. This is also the case if data or IT tools in the office network that are critical to the provision of telecom services have been rendered inaccessible due to ransomware. In addition, ransomware in the office network may prevent customers from accessing the company's web-based self-service solutions and telecom services.

Should the telecom infrastructure become infected with ransomware, the consequences would be particularly severe. The vulnerability of telecom infrastructure to ransomware is emphasized by the fact that ransomware is also designed to target Linux software and cloud infrastructure widely used in modern telecom infrastructure.

Although several telecom service providers in Denmark and worldwide have been hit by ransomware, there are as yet only few examples of the attacks affecting the provision of telecom services. This is, among other things, the result of the telecom infrastructure traditionally not being directly connected to the Internet. However, selected staff typically have access to the systems in the telecom infrastructure through a portal in the office network, as do suppliers in connection with operational or support tasks.

All access points to telecom infrastructure used by staff or suppliers can potentially also be exploited by hackers. If hackers manage to access the office network, there is therefore a risk that malware, including ransomware, may spread to the telecom infrastructure.

While targeted ransomware attacks are launched by professional cyber criminals motivated by financial gain, other types of extortion attacks whose perpetrators and purposes are more varied also constitute a threat to the telecom sector. This is true of, for instance, DDoS attacks.

DDoS attacks also pose a threat to the telecom sector

The telecom sector is exposed to a persistent threat from Distributed Denial of Service (DDoS) attacks. DDoS attacks involve attackers flooding websites or networks with Internet traffic, rendering them inaccessible to legitimate users as long as the attack lasts.

DDoS attack against Norlys disrupted telecom services
In May 2021, Danish energy and telecom provider Norlys fell victim to a DDoS attack against its DNS servers. The attack affected many of the company’s customers, who experienced interruptions or breakdowns of their Webmail, TV and Internet solutions.

DDoS attacks have the potential to overload critical telecom infrastructure, thus affecting customers’ Internet connections, regardless of whether the attack is directed against the telecom service provider or one of its customers. This has been the case in connection with DDoS extortion attacks, among other things. Telecom company websites can also be targeted, which may impact streaming and email services, etc. provided through the website.

DDoS extortion is an old phenomenon that saw a world-wide revival in 2020. Particularly in the months of May and June 2021, several Danish companies, including telecom providers, fell victim to such extortion. The attacks illustrated how powerful DDoS attacks against critical telecom infrastructure may affect telecom services.

Danish telecom service provider became target of DDoS extortion
In May 2021, Gigabit, now Wizer, became the target of DDoS extortion. The DDoS attack hit the company’s DNS servers and website. The impact of the attack affected customer Internet connections and made it difficult to reach the company via telephone.

The company managed to re-establish its telephone connection and the customers’ Internet connections without having to pay the ransom demanded.

As DDoS attacks do not require advanced hacking skills, the method is readily accessible to different types of actors with different motivations. Such actors may include criminals set on extorting a victim or harassing a rival, or a state determined on disrupting critical infrastructure. Also, there have been several examples of gamers launching DDoS attacks against other gamers or game providers.

Other types of cyber crime also target the telecom sector

In addition to extorting telecom providers through DDoS and ransomware attacks with the aim of turning illegitimate accesses or ransomed data into cash, some criminals use social engineering to trick telecom providers and others into transferring money to the criminals’ accounts.

This type of fraud goes under monikers such as Business Email Compromise and CEO fraud. The attacks vary greatly in complexity, ranging from amateur phishing emails to organized criminals sending credible phishing emails from a compromised supplier or cooperation partner known to the target.

The hackers use information posted online by telecom service providers on the provider’s own or other websites to enhance their credibility to victims. Such information may be related to employees, organization, email addresses, customers or suppliers.

Telecom customer accounts and self-service solutions are other attractive targets for hackers. Self-service portal credentials can be sold on to other hackers, just as the access to a customer's webmail can be used as an entry point for further criminal activities. For instance, the email account can be used to send spam or phishing emails, and the access to a streaming service can be resold.

Posing as the customer, hackers can also use a compromised self-service solution to order a new sim card, allowing them to hijack the customer's mobile number and using it for other criminal activities.

Cyber criminal hackers probe broadly for entry points

Suppliers are used as stepping stones to gain access to the intended target in so-called supply-chain attacks, with suppliers that have legitimate and privileged access to their customers' IT systems being particularly attractive to hackers.

By exploiting suppliers as entry points into telecom service provider networks, hackers can set the providers' perimeter defence checkmate. Similarly, compromise of a software supplier may result in a telecom service provider inadvertently installing software or software updates containing malware in their IT or telecom infrastructure.

Kaseya exploited in ransomware attack

Virtual System Administrator (VSA) is a software product for remote monitoring and operation of IT networks manufactured by US company Kaseya. By exploiting a vulnerability in the product, hackers uploaded ransomware to the VSA servers of Kaseya's customers in June 2021, spreading the ransomware to the computers connected to the servers.

According to Kaseya, around 50 customers, including Managed Service Providers (MSP), were affected by the incident, resulting in an additional 800 to 1500 MSP customers being impacted by the attack.

The CFCS has no knowledge of any Danish telecom service providers being affected by the incident.

Cyber espionage

The threat of cyber espionage is **MEDIUM**. As a result, it is possible that the telecom sector will be the target of attempted cyber espionage within the next two years.

The threat level has been lowered from **HIGH** to **MEDIUM** compared to the 2019 threat assessment. The change has taken place on the basis of a renewed analysis indicating that even though it is possible that foreign states are planning cyber espionage against the Danish telecom sector, it is not currently a high-priority target for attacks.

Cyber espionage against telecom sector focuses on its customers

The main purpose of espionage is to access sensitive information that may provide a state with security policy information or promote its national industry and economy. The Danish telecom sector is in itself not a traditional source of information of a security policy nature, just as it does not develop new technologies that can be immediately employed in support of foreign economies. For these reasons, it is likely that cyber espionage against the Danish telecom sector is not so much directed against the telecom service providers themselves as against the information the telecom service providers possess on their customers and their use of telecom services.

The purpose of cyber espionage against the telecom sector outside Denmark has often been to localize or follow single individuals or steal call data and text messages that reveal customers' contacts and communication. However, there have also been examples of general collection of large amounts of call data.

Cyber espionage against the telecom sector may also serve the purpose of listening in on customers' data communication, which may be facilitated by hacking a telecom service provider. However, other methods to this end will often be more effective for an attacker.

There is capacity and possible intent to spy on the telecom sector

Incidents abroad show that foreign states have both the capacity and the intent to launch advanced cyber attacks against telecom companies and telecom infrastructure. The capacity includes espionage through compromise of the telecom service providers' office network or the telecom infrastructure itself.

Compromising telecom infrastructure requires special accesses as well as specialist skills and knowledge, as the infrastructure is not normally directly connected to the Internet and often uses hardware, software and protocols that are different from the IT systems that are part of ordinary office networks.

State hackers stole call data from telecom service providers
A US security company revealed in August 2021 how hackers, which according to the security company were supported by China, had for years stolen call data from telecom service providers in South-East Asia.

The hackers exploited, among other things, a vulnerability in Microsoft Exchange servers made known to the public in March 2021 to steal the data.

The cyber espionage seen against the telecom sector abroad is often linked to security policy interests, such as conflicts between states or between states and certain private individuals or population groups. There are indications that telecom companies in Asia and the Middle East in particular are exposed to politically motivated cyber espionage, while this is not as common in Europe.

According to the CFCS's assessment, it is possible that Danish telecom service providers will become targets of such politically motivated cyber espionage. This is not least the case if a person residing or staying in Denmark is perceived by a foreign state as a target for espionage, for instance because they are believed to constitute a security risk or have contacts or access to information coveted by a foreign state.

States conduct espionage through insecure protocols in telecom infrastructure

Foreign states use the so-called SS7 protocol in their attempts to localize mobile phones and, by extension, their users. The protocols can also be used to intercept a person's calls and text messages. The SS7 protocol is used for interconnecting mobile networks worldwide. The protocol is used in 2G and 3G mobile networks, among other things to determine in which country a mobile phone is located and which mobile phone tower the phone is in range of.

The method is easy to use, and foreign states may have good opportunities to access the SS7 network from their own countries. It is thus possible that foreign states will try to use the method to conduct espionage against targeted individuals who are customers at Danish telecom service providers.

In the 4G and 5G mobile networks that are reliant on the 4G core network, the SS7 protocol has been replaced with the Diameter protocol. As the Diameter has inherited several of the SS7 protocol's weaknesses, it is possible that states will try to exploit these weaknesses as a platform for future espionage activities.

Telecom sector is threatened by cyber espionage through the supply chain

Like cyber criminals, foreign states can use suppliers to the telecom sector as attack vectors for cyber espionage. The threat targets the main supplier as well as their sub-suppliers.

A supplier of IT operations or IT support may be an entry point for direct access to espionage targets through the supplier's remote access. Alternatively, malware can be distributed into an organization by adding the malicious code to a supplier's legitimate software product or software updates. This method is effective, as telecom companies are no different from other companies in that they have to trust their suppliers.

Solarwinds exploited for cyber espionage through supply chain
In December 2020, security company FireEye uncovered one of the most extensive publicly known cyber espionage attacks. Organizations world-wide, including in Denmark, had been compromised through the Orion software from US company SolarWinds. Publicly known victims include Microsoft and Deloitte.

The CFCS assesses the compromise through the SolarWinds software to have been a very serious threat whose likely purpose was espionage.

According to open sources, the attack involved hackers compromising global software provider SolarWinds. In March 2020, hackers inserted a malicious backdoor into legitimate SolarWinds Orion software updates. According to SolarWinds, as many as 18,000 customers world-wide downloaded the compromised updates. The malicious code offered the hackers preliminary access to the victims' systems that they could use as a stepping stone for further action. The CFCS assesses that the hackers only exploited the backdoor to target more high-profile victims.

Danish telecom companies were among those downloading the compromised software. However, the CFCS has no knowledge of the hackers subsequently exploiting the access to these companies.

Cyber espionage against the telecom sector may have a destructive purpose

Cyber espionage can be used in preparation of a destructive cyber attack against the telecom sector. Preparations may include collection of technical knowledge on the IT and telecom infrastructure of the telecom sector, knowledge that can be used to plan a future destructive cyber attack or to install backdoors in the infrastructure to be used for subsequent destructive purposes.

Cyber activism

The threat of cyber activism against the telecom sector is **MEDIUM**. The CFCS has thus raised the threat level from **LOW** to **MEDIUM** compared to the 2019 assessment.

The threat level **MEDIUM** means that there is a general threat against the telecom sector and that it is possible that Danish telecom service providers will become targets of activist cyber attacks in the short term.

The CFCS raises the threat level based on activist cyber attacks launched in connection with Russia's invasion of Ukraine and the subsequent reactions to the war. In the initial stages of the war, cyber activist attacks were mainly aimed at targets in Russia, Ukraine and Belarus but have subsequently spread to include targets in Western European NATO countries. The CFCS believes it possible that pro-Russian hackers in particular will probe for targets in Denmark, including in the telecom sector.

Cyber activism is conducted by individuals and hacker groups that aim to attract as much attention as possible to their agenda or to punish organizations that they perceive as symbolic targets or adversaries of their cause. Cyber activism is typically driven by different ideological or political motives, ranging from animal welfare over political single issues to opposition against governments.

Activist cyber attacks range in complexity from relatively simple DDoS attacks to more resource-heavy hack and leak operations.

The war in Ukraine has triggered an increase in cyber activist attacks against the parties to the conflict. Actors on both sides of the conflict thus constitute a threat in terms of activist-motivated cyber attacks against Denmark, including the telecom sector.

The war in Ukraine has as yet not triggered a significant increase in cyber activism against Danish targets, though this may change with little or no warning if cyber activist groups were to turn their focus on Denmark. Pro-Russian activists may have an interest in punishing or influencing Danish support for Ukraine, including from the telecom sector, while pro-Ukrainian forces may be interested in punishing organizations affiliated with Russia or attacking targets in countries that are perceived as not supportive enough of Ukraine.

The threat thus also extends to Danish organizations or individuals with links to Ukraine that may become collateral damage of attacks directed against targets in Ukraine. Danish victims may, for instance, see their sensitive information leaked in hack and leak attacks against organizations in Ukraine.

Destructive cyber attacks

The threat is **LOW** of destructive cyber attacks. As a result, it is less likely that the telecom sector will become the target of attempts at destructive cyber attacks within the next two years.

Several foreign states, including Russia, have the capacity to launch cyber attacks with destructive effects against critical infrastructure such as the telecom sector. Destructive cyber attacks are cyber attacks whose expected effect is death or personal injury, significant harm to physical objects, and/or destruction or manipulation of information, data or software, rendering these assets inoperable without major restoration.

At present, it is less likely that foreign states have the intention of launching destructive cyber attacks against the telecom sector in Denmark. The threat may increase in connection with a sharpening of conflicts or geopolitical tensions between Denmark and states that have the capacity to launch destructive cyber attacks if their intentions change.

Activities or supplier relationships in conflict areas may raise threat

In conflict areas outside Denmark, the threat of destructive cyber attacks may be higher. This means that telecom companies with activities or supplier relationships in a conflict area may become collateral victims of an attack that is not directed at Denmark as such but broadly directed at organizations operating in the area.

Cyber terrorism

The threat of cyber terrorism is **NONE**, meaning that it is unlikely that companies in the telecom sector in Denmark will become targets of attempted cyber terrorism within the next two years.

The CFCS defines cyber terrorism as cyber attacks designed to create an impact comparable to that of conventional terrorism, for instance cyber attacks causing physical damage to human beings or extensive disruption of critical infrastructure.

The absence of a threat of cyber terrorism is the result of militant extremists having a limited intent and lacking the capabilities required to launch cyber attacks that are destructive on a scale comparable to conventional terrorism.

Militant extremists have for years used the Internet in support of their organizations, and as a tool to plan conventional terrorism and launch simple activist cyber attacks such as DDoS and defacement attacks. Yet there have so far been no examples of terrorists being capable of launching full-fledged cyber terrorism.

5G has not raised the cyber threat against the telecom sector

The introduction of the 5G mobile network in Denmark has not raised the cyber threat against the telecom sector. However, the arrival of 5G may, in time, increase the risk and consequences of cyber attacks, just as the expected increase in number of connected devices can act as a vector for hacker exploitation.

5G is more complex than earlier technologies and by default designed as a cloud solution leaving the telecom sector to face new attack surfaces and vectors. In addition, the task of keeping the telecom infrastructure updated and adequately configured to resist cyber threats can become increasingly demanding. When, within the next few years, Danish telecom service providers have upgraded the core network in the mobile infrastructure to 5G, it will mean the final goodbye to the core network as a contained physical network that is relatively easy to protect against hackers.

In Denmark, the first commercial 5G mobile networks were switched on in late 2020. As yet, 5G is only used in the radio networks, whereas the core network is still 4G. This primarily provides greater data speed. It is not until Danish telecom service providers start building 5G core networks that the functions separating 5G from earlier mobile networks will become accessible.

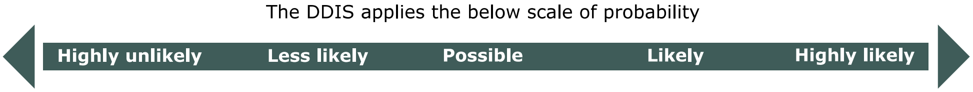
5G will facilitate the design of new services that go beyond mere telecommunication. 5G is thus expected to support new and innovative solutions in cities, in the industrial sector, the transport sector, the entertainment industry and the health sector. As an example, 5G will make it possible to transmit live 3D images from the scene of an accident or from an ambulance to doctors located at a hospital, making it possible for them to more effectively assist the on-scene medics.

Threat levels

The Danish Defence Intelligence Service uses the following threat levels:

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are 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.

Further relevant readings

The Centre for Cyber Security (CFCS) regularly publishes guidance reports and threat assessments. Below is an excerpt of publications of special relevance to the telecom sector. All products are available at the CFCS website.

Effective Cyber Defence
CFCS basic guide on cyber defence and cyber attack management:
https://cfcs.dk/en/forebyggelse/guidance/effective-cyber-defence/

How to protect against DDoS attacks
Guide with recommendations on how to prevent, delay and handle DDoS attacks (only available in Danish): https://cfcs.dk/da/forebyggelse/vejledninger/DDoS-angreb/

Reduce the risk of ransomware

Guide with recommendations for organizations on how to reduce the likelihood of falling victim to ransomware attacks (only available in Danish): https://cfcs.dk/da/forebyggelse/vejledninger/ransomware/

Information security in supplier relationships

Guide with advice on management controls and matching of expectations in the business/supplier relationship (only available in Danish): https://cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

Cyber security in the boardroom

Guide focusing on cyber and information security in the boardroom (only available in Danish): https://cfcs.dk/da/forebyggelse/vejledninger/cybersikkerhed-for-bestyrelser/

Digital hostage takers go big game hunting

Threat assessment outlining the threat from so-called targeted ransomware attacks that may carry serious repercussions to organizations (only available in Danish): https://cfcs.dk/da/cybertruslen/trusselsvurderinger/malrettet-ransomware/

The anatomy of targeted ransomware attacks

Investigation report offering an in-depth outline of the phases involved in targeted ransomware attacks. The report offers concrete advice on how to counter attacks (only available in Danish): https://cfcs.dk/da/cybertruslen/rapporter/anatomien-i-ransomware-angreb/

The cyber threat from phishing mails

Threat assessment offering an in-depth outline of how hackers use phishing and spear-phishing mails in their attempts to compromise or lure sensitive information from companies: https://cfcs.dk/en/cybertruslen/threat-assessments/phishing/

Hackers scan your network for vulnerabilities 24-7-365

Threat assessment describing how hackers probe the Internet for equipment containing vulnerabilities in order to compromise organizations (only available in Danish): https://cfcs.dk/da/cybertruslen/trusselsvurderinger/hackere-scanner-dit-netvaerk/

The cyber threat from intentional and unintentional insiders

Read more on the threat from insiders and find recommendations on mitigating measures: https://cfcs.dk/en/cybertruslen/threat-assessments/insiders/