TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Information security in 2023

Table of contents

Introduction ... 3

In Finland, cyber security is developed on a strategic long-term basis ... 4

- Cyber security requires continuous development ... 5
- Companies have a major responsibility for maintaining and developing cyber security ... 6

Information security in 2023 ... 7

- Threat level remained elevated ... 8
- Denial-of-service attacks ... 9
- Ransomware ... 10
- Phishing and online scams ... 11
- Vulnerabilities ... 12
- Cyber espionage ... 13
- Communications networks were stable in Finland in 2023 ... 14

The year 2023 for the National Cyber Security Centre Finland at Traficom ... 15

- Supporting society's situational awareness of cyber security ... 16
- International cooperation intensified in 2023 ... 17
- Active cyber exercises continued ... 17
- Forecasting work supports preparedness for future phenomena ... 18
- Increasing awareness and communications ... 19
- Network cooperation was further developed in 2023 ... 19
- The security of society was promoted with cyber security development projects ... 21
- Support for developing information security in companies ... 21
- Experiences from the Cybersecurity Label are actively used in monitoring and advocating on EU cyber security regulation ... 22
- Operations of the National Coordination Centre ... 22
- NCSC-FI supported the development of legislation ... 23

Cyber security trends in 2024 ... 24

- Overview of the general cyber security threat level in 2024 ... 25
- Important changes to legislation ... 26
- Rapid technological development will continue in 2024 ... 27
- Information security skill management becomes increasingly important ... 29

Our KPIs in 2023 ... 30

Traficom publications 10/2024
ISSN 2669-8757 (online publication)
ISBN 978-952-311-909-3

Introduction

Now that we are well into 2024, it feels appropriate to take a moment and look back at the previous year. What happened on the front of cyber security? Quite a lot. In terms of threats, we experienced the spreading of ransomware and scam messages as well as denial-of-service attacks. Criminals were being opportunistic and continuously coming up with novel means of trying to penetrate organisations' information systems or scamming money or personal data from individuals. Furthermore, cyber espionage attempts against organisations continued actively. In this criminal business, ruthlessness and immorality know no bounds.

At Traficom, we continuously monitor the phenomena of cyber security and the digital society. We help companies, authorities and citizens prepare for and identify current and future cyber threats. Our work also enables them to influence technological development and minimise the challenges created.

Various threats receive a great deal of visibility in the media and public discussion. The continuous work to develop cyber security carried out on different sectors of society often receives less attention. Cooperation, information exchange, methods and protective technologies are continuously being developed.

Cyber security and everyday information security are about small and large actions. It is all about being careful and vigilant. Keeping the software updates and information security of devices and services up to date. Helping a friend set up their new smart device.

For organisations, information security and its maintenance must be the foundation of all business and operational activities. Good information security is a key part of the social responsibility of organisations in the modern digital society.

Poor information security compromises the company's business operations and at worst can bring them to an end. There are no shortcuts to good information security. There can be no cutting corners.

Taking care of information security means taking responsibility for your own organisation, its employees and customers, and ultimately the cyber security of Finnish society as a whole.

A cyber secure Finland is not created alone: it requires cooperation cutting through all sectors of society. I wish to offer my thanks to everyone who work every day to promote cyber security in Finland.

Jarkko Saarimäki
Director-General

> Good information security is a key part of the social responsibility of organisations in the modern digital society.

Ps. Do you already know about the National Cyber Security Centre Finland's **weekly reviews** and **Cyber Weather**? They both provide important and up-to-date information on what is going on in cyber security. Further information at kyberturvallisuuskeskus.fi/en

In Finland, cyber security is developed on a strategic long-term basis

As society becomes increasingly digitalised, industries and different sectors of society become more dependent of each other. Few incidents today affect only one single industry or administrative branch. Preparing for and responding to modern threats requires close cooperation between the various sectors of society and uninterrupted and quick exchange of information. The connections between management, the situational picture and communications must work well. Decisions must be made with the right information and based on an accurate situational picture. Current and future crises also require increasing investment in communications.

Cyber security is a key part of the comprehensive security of Finland and Finnish society. As with any other form of security, cyber security also requires investment and continuous development in order to respond to existing and future threats. This is especially true right now, as the global security policy situation is changing.

Cyber security cannot be created alone and its safeguarding requires seamless cooperation between companies and authorities based on trust. Finland has a long tradition of this cooperation taking place to promote cyber security comprehensively and extensively between different sectors of society.

The legislation, methods and standards concerning cyber security, preparedness and cooperation between the authorities are developed continuously both in Finland and at the EU level. Education and research on cyber security keep growing stronger in Finland.

The cyber security threat level remained elevated in 2023. Traficom and the Finnish Security and Intelligence Service communicated on the threat level situation in April 2023. The previous notification of an elevated threat level took place in autumn 2022. The reason for this change is that cyber attacks have become more severe and targeted than before.

We increasingly see attackers trying to penetrate a particular organisation. Furthermore, the everyday lives of Finns and the everyday operations of organisations in Finland are impacted by denial-of-service attacks, various scams, malware, phishing and ransomware attacks targeting the ICT environments of organisations. **The National Cyber Security Centre Finland (NCSC-FI) estimates that the threat level will remain elevated in 2024 as well.**

Cyber threat level remains elevated, targeted attacks have become more frequent | Traficom

Cyber security requires continuous development

In Finland, the tasks and roles of different authorities in the area of cyber security are clear. Cooperation between the government level and the operational level works well. Operative cooperation takes place daily, and the authorities have well-organised coordination groups and operating models.

Cyber security and its development are taken into account in many ways in Prime Minister Orpo's Government Programme. Cyber security receives more attention than in previous government programmes. Finland's cyber security strategy will be revised during the current government term. The preparation of the strategy began in 2023. The cross-administrative publication 'Report on the authorities' capacity to act in cyber security matters' was prepared as a part of the official duties included in the Cyber Security Development Programme carried out over several government terms (Government resolution 2021, Cyber Security Development Programme – Valto). A significant share of the report's suggestions, such as increasing cyber security training, identifying critical systems and ensuring their security, are taken into account in the Government Programme, as is the Cyber Security Development Programme from 2021 in general.

The comprehensive security and cyber security management structure will be reformed during the government term under the prime minister. The reform will ensure a clear division of duties and competences and efficient information exchange between the authorities and implement the required legislative changes. Furthermore, cyber security will be strengthened in close cooperation with companies, trade and industry and the third sector, while acknowledging that a large share of critical infrastructure is privately owned.

In the near future, key development needs in the area of cyber security are related to legislation. As technologies and the operational and security environment are rapidly changing, it is important that legislation also keeps up with the development. In preparing for and responding to current and future cyber threats, it is important that we have well-protected systems in place and that competent authorities are able to exchange information more efficiently and faster than before. Cyber events differ from the events of the physical world in that speed is of the essence: managing an incident can be a matter of minutes and seconds.

In addition to the development of legislation, the promotion of credible national cyber security, and foreign and security policy influence in the broader sense, requires the development of an ambitious attribution framework. In the context of hostile cyber activity by state actors, attribution refers on the one hand to the analysis and decision-making process identifying the responsible state actor and on the other hand to the public attribution carried out as a response on its basis. In acting against hostile cyber activities by state actors, the key question is who ultimately is the state actor responsible for the hostile cyber activity. For this reason, the attribution process not only requires technical information, but also extensive knowledge and a strategic foreign and security policy evaluation in order to discover the state actor and the motives behind the hostile cyber activity and to consider different response alternatives.

- Government resolution 2021, Cyber Security Development Programme Valto | Government (in Finnish)
- Report on the authorities' capacity to act in cyber security matters | Government (In Finnish)

Companies have a major responsibility for maintaining and developing cyber security

Cyber security and protection as a whole are made up of several different actors. Here, companies play an important role. They are responsible for providing several services that are critical to the functioning of society. Without service providers in the private sector, electronic communications would not exist in practice – or at least they would not be available to all citizens.

For example, telecommunications operators are responsible for the functioning of the mobile connections and offer access to the internet, among other things, via their networks. Without telecommunications operators, terrestrial or cable TV distribution and services would not exist, either. Telecommunications operators and banks offer us mobile certificates and online banking credentials that we can use to log in to e-services and currently also take care of several different matters with the authorities, when necessary.

In Finland, operators are themselves responsible for cyber security in their respective fields of operation together with public authorities. As the operating environment changes, more and more cooperation between the public and the private sector is needed. Such cooperation in cyber security already has a long tradition in Finland both between and within the various sectors of society. This cooperation, which has also sparked interest around the world, has been built and developed systematically in accordance with the principles and concept of comprehensive security. Over the years, the cooperation has been intensified and operating models have been created for it. In addition, the lessons learned from joint exercises are constantly being introduced in practice in the different sectors.

Cyber protection as a whole is created by actors who do their tasks well, cooperation and continuous exchange of information.

> ” Cooperation in cyber security already has a long tradition in Finland both between and within the various sectors of society.

Information security in 2023

Threat level remained elevated

The cyber threat level raised in 2022 remained elevated during 2023. Finland was actively subjected to various cyber attacks, including scams, phishing campaigns and ransomware attacks. Security incidents reported to the NCSC-FI increased by approximately 44% compared to the previous year. There was an increase e.g. in scams, attempted data breaches and scam messages. The NCSC-FI published one alert about the M365 email account compromises in 2023.

As in 2022, the attacks were more targeted and tailored compared to previous years. The capabilities of different cyber threat actors have developed e.g. through easily available services and automation. Threat actors with different motivations make use of the same malware and critical vulnerabilities. Among other factors, this makes it increasingly difficult to separate the actors behind the activities.

The continuing Russian invasion of Ukraine has manifested in the European cyber operating environment e.g. as denial-of-service attacks by pro-Russian hacktivist groups targeted at measures considered anti-Russian. In Finland, denial-of-service attacks were detected from early autumn onwards in particular. The publicly reported motives for these attacks included political reasons. Similar activities were common elsewhere in Europe as well. Denial-of-service attacks against Finnish organisations had no significant impact.

The importance of domestic, low-threshold cooperation between the authorities and companies is particularly emphasised in limiting the impacts of attacks.

Many security incidents highlighted the importance of the organisation's active measures in limiting the impacts of attacks. Based on our analysis, the incidents detected in 2023 emphasised e.g. the significance of implementing multi-factor authentication in organisations.

In 2023, the vocational education and training provider Keuda received the Information Security Trailblazer award for its open communication and response after becoming a victim of a ransomware attack. Fast and open communication in case of a ransomware attack helps the organisation to resolve the incident and recover from it and also supports other actors in preparing for cyber threats.

Information Security Trailblazer | National Cyber Security Centre Finland

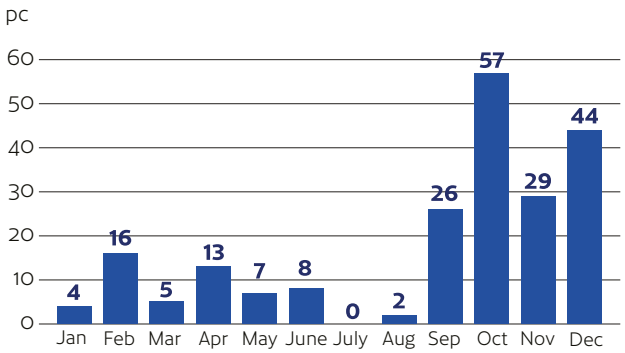
Denial-of-service attacks

Denial-of-service attacks involve driving large amounts of traffic to websites or online services. For regular users, this usually results in the website or service becoming inaccessible or working very slowly. A denial-of-service attack is a simple but flashy attack technique. They are also often covered by media outlets. In most cases, denial-of-service attacks do not cause any visible effects for users, and even at their worst, they usually result in nothing more than short service interruptions.

Nowadays denial-of-service attacks are especially common as a form of hacktivism. Hacktivism is cyber crime that is motivated by a political agenda instead of money. For hacktivists, denial-of-service attacks are a way of expressing discontent in a political decision or other activities and influencing the surrounding information environment. After all, even short service interruptions can increase distrust among the targeted party's customers or stakeholders. Hacktivism has been increasing recently, especially following the Russian invasion of Ukraine in 2022. Both pro-Russian and pro-Ukrainian hacktivist groups have carried out denial-of-service attacks as part of their information influence activities.

In Finland, denial-of-service attacks were reported especially on 4 April, the day of Finland joining NATO, and throughout autumn. In particular, the pro-Russian hacktivist group NoName057(16) targeted denial-of-service attacks against Finnish organisations on different sectors in 2023. NoName is in the habit of celebrating the denial-of-service attacks on their Telegram channel even when the attack has no impact on the functioning of the target site. Some denial-of-service attacks that impacted the functioning of public and central government websites were reported by Finnish media as well. Organisations publicly explained being targets of denial-of-service attacks if their website was down because of this reason. In 2024, denial-of-service attacks are no longer considered to cause reputational damage to organisations. Any organisation can become a target of a denial-of-service attack, and organisations must indeed prepare for application-level denial-of-service attacks as well.

Reports of denial-of-service attacks processed by the NCSC-FI in 2023



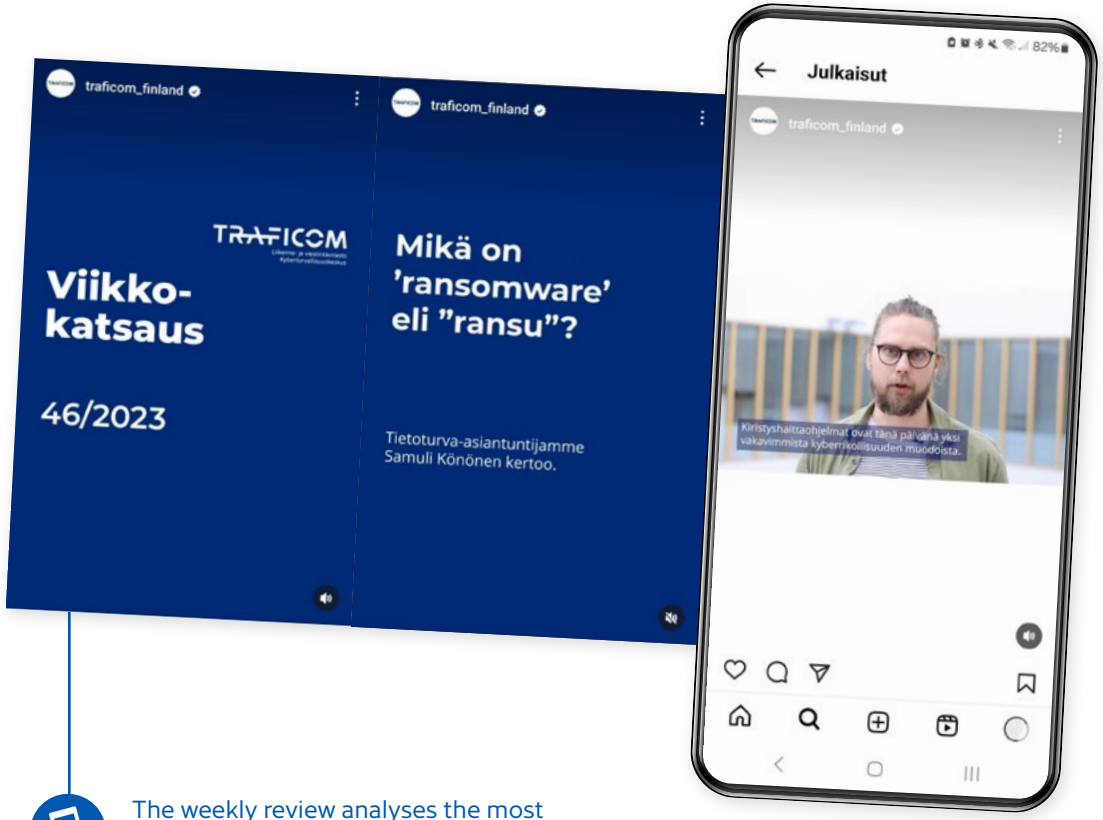
> Nowadays denial-of-service attacks are especially common as a form of hacktivism.

Ransomware

Ransomware attacks increased clearly in Finland at the end of the year, when more cases were reported than during other quarters. The cases have concerned several sectors, but the measures taken by organisations have been able to limit their impact. Up-to-date backup copies, for example, have rescued the situation of many organisations.

In 2023, ransomware actors were generally observed to have become more effective and professional. Around the world, there have been reports of severe ransomware attacks against central governments, legal instances and health care operators. These cases have included leaks of sensitive personal data, and recovery from the attacks may have taken anything from weeks to months. In Finland, the most common ransomware in 2023 was Akira, with related cases reported especially at the end of the year.

Ransomware attacks usually cause significant inconvenience and costs for organisations. It is often difficult to react to a ransomware attack once it has begun. Proper preparation offers far better basis for action when an incident occurs.



The weekly review analyses the most significant national and international cyber events of each week.

Read more about our situational picture products on page 16

Phishing and online scams

In the area of phishing and online scams, the greatest number of reports concerned phishing for bank credentials. A wide range of scams attempting to gain access to online bank credentials were carried out under the names of banks, the Finnish Tax Administration, the police, Kela and other authorities and companies. The second most active scamming type was the phishing of Microsoft M365 credentials, of which the NCSC-FI published a severe alert in week 42. The phished credentials were used in hundreds of email account breaches, the number of which luckily started to decline after the alert was published.

There were several reports in the media of information and cyber security issues concerning various AI-based solutions around the world, e.g. in relation to election security. In 2023, reports of Finnish-language AI-based cyber incidents in Finland were still rare. The NCSC-FI was informed of one high-quality case of AI-based deepfake involving the cloning of a CEO's voice to request a large money transfer, but here too, Finnish was not used.

Scam calls have been tackled with close cooperation of authorities and telecommunications operators for several years now. The new Traficom regulation, which entered into effect at the beginning of October 2023, obligates Finnish telecommunications operators to improve the blocking of calls from foreign phone numbers attempting to spoof Finnish numbers, including mobile ones. The filtering solution designed to accomplish this is now being used by all Finnish telecommunications operators that manage calls from abroad. In fact, Traficom is currently preparing a regulation intended to help prevent SMS scams as well in the future.

The work carried out in Finland in blocking scam calls has also generated exceptionally active international interest, as the implemented model was very advanced even by international standards. Finnish authorities and telecommunications operators have presented the implemented solution model e.g. in the United States in spring 2023.

Blocking spoofed numbers | Youtube (In Finnish)

In the summer of 2023, we published an information security campaign on social media aiming to increase awareness of scamming and phishing.

Read more about the NCSC-FI campaigns on page 19

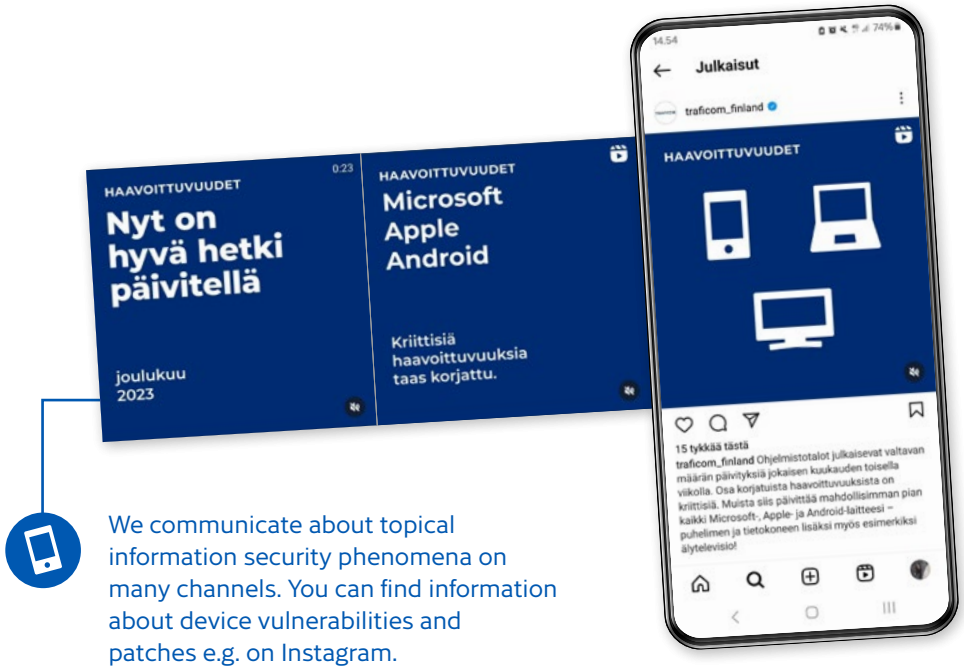
Vulnerabilities

The year 2023 was another lively one in terms of vulnerabilities. Globally, more than 20,000 unique vulnerabilities with CVE identifiers were published. Some vulnerabilities are more critical than others. Of these, the vulnerabilities that enable remote exploitation are particularly emphasised in the everyday work of the NCSC-FI. A critical vulnerability can enable a data breach and even provide the attackers with a chance to install ransomware. The NCSC-FI publishes around 30–40 vulnerability bulletins each year of the most critical vulnerabilities to Finnish users.

The NCSC-FI monitors news and discussions on vulnerabilities on a daily basis. In the most severe cases, the NCSC-FI surveys domestic users and contacts organisations directly in case of a suspected or detected vulnerable device. Devices vulnerable over the internet are indeed an easy target for attackers. For example, the network device manufacturer Cisco's vulnerability was used as the starting point of ransomware attacks in many cases in Finland in 2023. According to a well-known information security company, critical vulnerabilities in particular are important for ransomware actors. The Lockbit group, for example, exploited the Citrix Bleed vulnerability in its attacks in 2023 that caused severe impacts globally.

The exploitation of vulnerabilities increases in speed each year. The movements of attackers can be detected around the world just days after the publication of a critical vulnerability. Luckily, the cyber world conducts active exchange of information and word is spread about exploited vulnerabilities. The NCSC-FI prioritises vulnerabilities already exploited around the world in communicating about and surveying various vulnerabilities in Finnish networks.

An already exploited critical vulnerability that allows the attacker to perform commands remotely in a popular online service or device is often the most critical example of this on an annual level. Thankfully, only a few such vulnerabilities occur each year in solutions popular in Finland and require more active measures and work hours from authorities and private sector operators alike.



We communicate about topical information security phenomena on many channels. You can find information about device vulnerabilities and patches e.g. on Instagram.

Cyber espionage

In 2023, cyber espionage attempts continued actively as in the previous year. Finnish organisations were constantly targeted by activities aiming at identifying the services used and finding different kinds of vulnerabilities or poorly protected user accounts.

Targeted malicious email messages and malware aimed at mobile devices were used as part of cyber espionage. Furthermore, cyber espionage was targeted at widely-used cloud services. Based on public, commercial, official or other sources, some of the activities indicate actions by state actors.

There was also the international phenomenon of exploiting vulnerabilities in network devices and email systems more extensively in cyber espionage. Vulnerable domestic and small business routers as well as network drive servers were widely used as a part of the attack infrastructure of state actors aiming to get closer to the desired target and hide the original source of the traffic.

Russia's invasion of Ukraine was still evident in cyber espionage and influence activities. For example, several attacks on critical systems, phishing email campaigns and malware campaigns were detected in Ukraine during the year.

Cyber espionage can increase directly or indirectly as a result of Finland's NATO membership. Elsewhere in Europe, cyber espionage has been targeted e.g. at war-related operators, logistics and industrial and technological product development.

Communications networks were stable in Finland in 2023

In 2023, the operation of communications networks in Finland was stable. Clearly more service interruptions occurred than during the previous year, but the number of serious interruptions was down. Individual interruptions caused momentary disruptions of regional services or emergency traffic, but the majority of the disruptions were short-lived. The considerably stormier weather conditions contributed to the number of disruptions caused by power cuts doubling compared to 2022. In the long term, the number of disturbances in public communications services, particularly more serious faults, will continue to decline, although the overall number of significant disturbances grew considerably compared to the statistically exceptional previous year.

The authorities work in close cooperation with Finnish telecommunications operators in securing the functioning of the networks.

Damage to submarine infrastructure in October 2023

Perhaps the most visible cyber security incident of 2023 was the damage to submarine infrastructure in the Gulf of Finland in October 2023: A disturbance caused by a leak was observed in the Balticconnector gas pipeline between Finland and Estonia in the early morning hours of 8 October. On Sunday 8 October, the NCSC-FI at Traficom received information of a damaged submarine cable between Estonia and Finland in the Gulf of Finland from a Finnish telecommunications operator. The same weekend also saw damage to another telecommunications operator's cable between Sweden and Estonia, meaning that it transmitted traffic at a lower capacity than normal.

Taking care of the reliability and preparedness of public communications networks and services (i.e. telecommunications operations) has been a part of the legislation as well as guidance and supervision of the operators by the authorities already since the 1990s. This work and the continuous cooperation between the NCSC-FI and telecommunications operators have contributed to the fact that damage to submarine cables, for example, has hardly any visible impact on the customers of telecommunications operators.

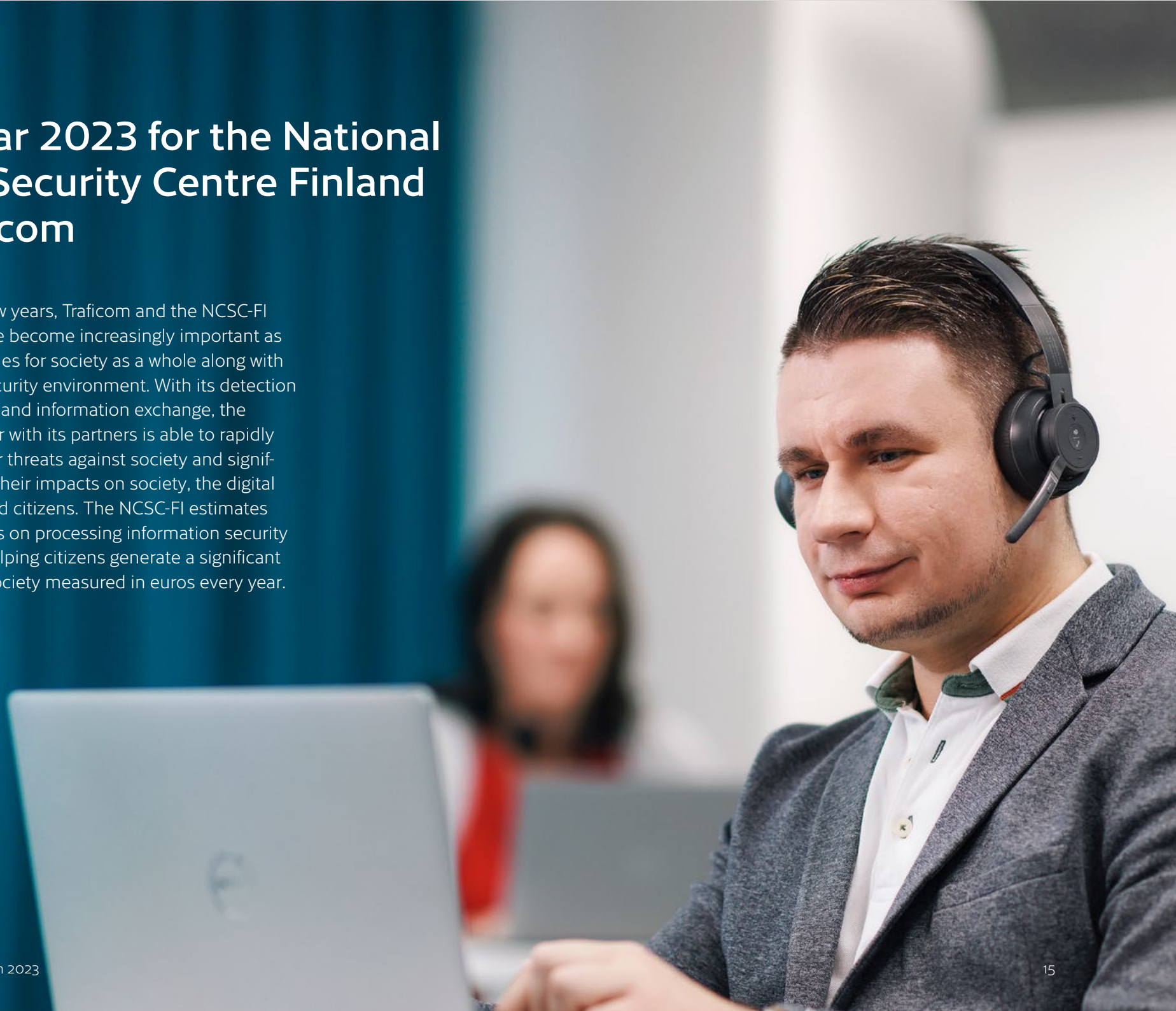
In the October incident, in keeping with normal preparedness procedures, the telecommunications operator immediately transferred the cable traffic between Finland and Estonia to a backup connection, meaning that telecommunications between Finland and Estonia were able to function without issue. In other words, the interruption had no impact on the functioning of Finnish or Estonian telecommunications services.

The NCSC-FI formed a situational picture of the case. It monitored the progress of the work to fix the broken cable in close cooperation with the telecommunications operator and other authorities, both nationally and internationally. These activities supported the decision-making of the government.

The October incident is still being processed in Finland and Estonia by pre-trial investigation authorities. The NCSC-FI continues the national and international cooperation with telecommunications operators and other authorities in order to protect the communications network infrastructure and prevent, detect and fix any issues.

The year 2023 for the National Cyber Security Centre Finland at Traficom

Over the past few years, Traficom and the NCSC-FI in particular have become increasingly important as security authorities for society as a whole along with the changing security environment. With its detection ability, networks and information exchange, the NCSC-FI together with its partners is able to rapidly respond to cyber threats against society and significantly mitigate their impacts on society, the digital infrastructure and citizens. The NCSC-FI estimates that its measures on processing information security breaches and helping citizens generate a significant net benefit for society measured in euros every year.

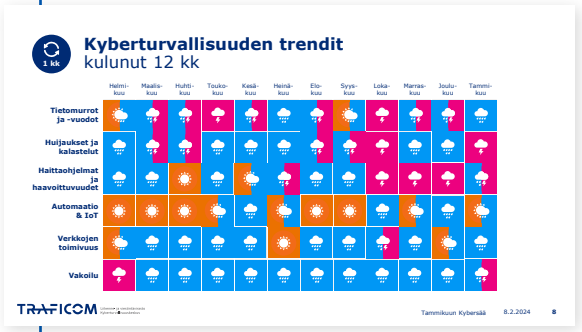


Supporting society's situational awareness of cyber security

The NCSC-FI is tasked with producing a situational picture on national cyber security. It collects information on data network events and shares it with different operators. The generation of the situational picture makes extensive use of national and international sources, such as the networks of organisations critical to the security of supply, other security authorities and the official national and international cooperation networks of the NCSC-FI that are based on voluntary operations and mutual trust. Furthermore, the NCSC-FI receives more than ten thousand voluntary reports e.g. from citizens each year. The clients of the NCSC-FI make use of the situational picture information in developing their preparedness and as a part of their daily operations.

Examples of the public situational picture products include the NCSC-FI's weekly review that analyses the most significant national and international cyber events of each week. In turn, the monthly Cyber Weather report looks at the development trends impacting cyber security over a longer period of time. Both are available on the NCSC-FI website.The NCSC-FI also produces a strategic situational picture on cyber security to be used at the highest levels of government.

The NCSC-FI weekly review | National Cyber Security Centre Finland



The aim of Cyber Weather is to report on cyber events in a concise and easy-to-understand form.

Cyber Weather – news about information security | National Cyber Security Centre Finland

The situational picture products produced by the NCSC-FI have an important role in developing the situational awareness, effectiveness and preparedness concerning cyber security in society. In a survey carried out in 2023 on the public situational picture products, the NCSC-FI products received an excellent evaluation (average of 4.3 on a scale from 0 to 5).

International cooperation intensified in 2023

The NCSC-FI carries out close cooperation on a daily basis with domestic and foreign partners and networks. This cooperation contains e.g. the exchange of information and situational cyber security awareness, in addition to meetings, trainings and exercises. International cooperation increases competence and awareness of the prevalent cyber threat situation. In this way, cooperation helps prevent cyber threats facing Finland.

International networking and cooperation also play an important role in processing various acute information security and cyber incident cases. The networks also enable scaling the Finnish cyber threat situation against the international level.

In 2023, specialists from the NCSC-FI continued to intensify bilateral relations with our key partner countries, such as Sweden and Estonia. The advocacy and coordination of international matters was also strengthened by the creation of the post of director of international affairs.

In 2023, the key themes of international cyber security cooperation were operative cooperation, developing EU cooperation on a strategic level and several cyber security regulation projects at the EU level. Alongside EU cooperation, the NCSC-FI continued its national measures as a part of the national NATO coordination. Finland's NATO membership has expanded international cooperation into new areas. Active cyber exercises continued In addition to up-to-date plans, operating successfully in different security situations requires regular training.

The website of Traficom's NCSC-FI offers information about cyber security exercises

Exercises | National Cyber Security Centre Finland

Active cyber exercises continued

In addition to up-to-date plans, operating successfully in different security situations requires regular training. Exercises offer valuable information for developing the operations, management, communications and situational picture activities at organisations.

During 2023, active cyber security exercises continued at home and abroad. In Finland, more key service providers took part in the exercises than in the previous years. The exercises emphasised inspecting the areas of responsibility in operative interfaces and the related agreements. A cyber threat targeted at a service partner can also affect another organisation's activities.

Future exercises, particularly larger national ones, will look at the internal delivery chains and dependencies of different sectors.

Forecasting work supports preparedness for future phenomena

The future and forecasting work was developed across the NCSC-FI in order to prepare for future phenomena and technological developments and to strengthen the forecasting approach. The building of cooperation with different sectors of society was also continued.

In 2023, the key focus area of the future and forecasting work was to examine the realisation of different cyber scenarios in order to understand possible development paths in the future operating environment. The forecasting continued assessing the impacts of artificial intelligence, and Traficom initiated work on its third report on AI. The report to be published in winter 2024 focuses on the use of AI in promoting cyber security and on AI-based cyber security solutions. This third report on the theme complements the prior AI reports that focused on AI risk management and cyber attacks enabled by AI. The reports have heard from a wide group of information security professionals from the private and public sectors and research institutions. The reports are realised in cooperation with the National Emergency Supply Agency.

Furthermore, the cyber security and risk management of implementing local mobile networks was discussed in the forecasting work. It is likely that in the future, many actors critical to the functions of society will take advantage of local mobile networks tailored to their own needs in order to digitalise their operations and make them more efficient. New kinds of risks and competence requirements are linked to these network implementations, and it is important to take them into account in implementing the networks. Publications on the themes mentioned above were also produced for the website of the NCSC-FI. The reports and instructions were realised in cooperation with the National Emergency Supply Agency.

Traficom will organise the third 5G hackathon in 2024. This year's Hack the Networks event to be held in May focuses on the security of local 5G networks used as a part of critical infrastructure. Further information hackthenetworks.fi/en

- The security threat of AI-enabled cyberattacks | Traficom
- Cyber security and risk management in the application of AI | Traficom (In Finnish)
- Instructions on the cyber security and risk management of local mobile networks | National Cyber Security Centre Finland (In Finnish)

The second part of the report commissioned by Traficom's NCSC-FI and the National Emergency Supply Agency, 'The security threat of AI-enabled cyberattacks', was presented in late 2023.

Increasing awareness and communications

In preparing for and responding to cyber threats, communications play a central role. As society is quickly becoming increasingly digitalised, information security skill management and their continuous development are important skills. Without awareness of different threats, you cannot prepare for them or prevent them.

Issues related to cyber security, particularly threats, come up very quickly in public discussion. They both interest and worry people. When talking about cyber security, it is important to discuss it based on accurate and up-to-date information. Traficom meets this need for information by continuously producing and distributing information on cyber security to different target audiences. Strategic situational picture analysis is produced to support cyber security decision-making at the highest levels of government. The NCSC-FI's weekly review and the monthly Cyber Weather report provide information to the general public on what kind of scam messages or phishing campaigns they can experience in their everyday lives.

The annual Information Security Seminar organised together with the National Emergency Supply Agency in October attracted more than 2,000 participants. Traficom's website and social media accounts reach a wide range of target audiences every day. Furthermore, Traficom specialists regularly provide interviews to the media. The website offers instructions, guides and tips on how to develop everyday information security skills. Communications campaigns at exhibitions and events targeted at different audiences are ways we increase cyber security awareness in society.

The planning and concept creation of an extensive national cyber security communications campaign for the general public was initiated in 2023.
The campaign will be implemented together with the Digital and Population Data Services Agency and the National Bureau of Investigation in late spring 2024.

The e-services information security campaign effectively reached its target audience in Meta with a very reasonable CPM price.

Read more about the information security skills of citizens on page 29

Network cooperation was further developed in 2023

In 2023, the network cooperation of the NCSC-FI developed strongly. The significance of the Information Sharing and Analysis Centres (ISAC) was particularly highlighted in producing the situational picture and in the mutual exchange of information between sectors critical to society in relation to preparedness and incident management.

Interest towards network activities increased in the past year. Several new organisations joined the ISACs and the wellbeing services counties were invited to join the health care and social welfare ISAC. In 2023, new ISAC information sharing groups were established for the municipal sector, information security companies and energy operators. This development will continue in 2024 as well, as information sharing groups are intended to be established e.g. for the real estate and building sector and for high-tech operators.

The information exchange relating to networks became more international in 2023. Finland has been an increasingly active member on international forums, and bilateral international networking has also intensified considerably.

Cooperation and information exchange between authorities was another target of active development. The NIS cooperation group of regulatory authorities prepared for the national implementation of the NIS2 Directive. The NIS2 Directive will increase the number of regulated sectors and bring additional tasks to existing regulatory authorities. The NIS cooperation group will expand considerably in 2024, as the new NIS2 regulatory authorities will join the group. In preparation, Traficom expanded its existing advisory services on information security to regulatory authorities in 2023. Furthermore, the already active information exchange between security authorities has further intensified due to changes in the security environment.

The social significance of ISACs acting as trust networks has increased in the past year, and the networks are an increasingly important part of the national situational picture on cyber security and the management of incidents. During 2023, the exchange of information in trust networks was intensified and the exchange of information across sectoral borders was improved. Preparedness and hybrid influence were increasingly highlighted in the ISACs. Cyber exercises also received increased investment.

The NCSC-FI also invested in topical information exchange with different networks. Examples of this include the weekly sectoral report piloted in the autumn and the operative information sharing sessions on severe and acute information security threats organised on short notice as necessary. Some of these sessions have been targeted to a wider audience of operators critical to security of supply, in addition to the trust networks. An operative information sharing session on a significant information security threat received more than six hundred participants on one day's notice.

” In 2023, new ISAC information sharing groups were established for the municipal sector, information security companies and energy operators.

The security of society was promoted with cyber security development projects

In recent years, the NCSC-FI has implemented several projects for improving the cyber security of actors vital to society and thereby the preparedness as well as the cyber security of society as a whole. In these projects, the National Emergency Supply Agency has played a key role, both in funding the projects as well as supporting their implementation. The Ministry of Finance has also participated in funding the development projects implemented by the NCSC-FI.

The development projects funded and supported by the National Emergency Supply Agency target companies vital to society and their cyber security. In turn, the development projects funded and supported by the Ministry of Finance focus on developing the cyber security of public administration.

Implemented services include:

- **Havaro**, which observes serious information security threats targeted at Finnish companies and issues warnings about them. Havaro.fi/en
- **Hyöky**, Hyöky, a national attack surface analysis service to improve cyber security in municipalities. Hyöky | NCSC-FI (In Finnish)
- **Kybermittari**, a free service for cyber security assessment and development. It is targeted at the management of organisations as well as information security and data protection experts as a concrete tool for cyber security management, sector-specific comparisons and steering of development investments. Kybermittari.fi

The development projects funded by the National Emergency Supply Agency are funded through the Digital Security 2030 programme of the National Emergency Supply Agency, and they follow the goals set in the programme.

The development projects funded by the Ministry of Finance are funded from the implementation programme for digital security in public administration 2020–2023 (Haukka).

Support for developing information security in companies

In 2023, the NCSC-FI granted a total of approximately EUR 5.2 million of support to 251 companies to improve their information security. Of this amount, around EUR 3.2 million have consisted of support of up to EUR 15,000 and EUR 2 million have consisted of support of up to EUR 100,000. All in all, the NCSC-FI processed grant applications from 409 companies in 2023.

Around 40% of the grant applications were rejected, e.g. due to the company not meeting the legal requirements or submitting an incomplete application, making it impossible to ensure that the requirements of the grant are met. All in all, 740 companies applied for a total of approximately EUR 19 million of support by the end of the year, when only EUR 6 million of appropriations were reserved. Of the reserved appropriation of EUR 6 million, the remaining EUR 0.8 million will be granted in the first half of 2024.

Experiences from the Cybersecurity Label are actively used in monitoring and advocating on EU cyber security regulation

The Cybersecurity Label published by the NCSC-FI in 2019 indicates that the product or service with the label meets Traficom's requirements for a good basic level of information security. The requirements of the label are based on a European standard. The label can be granted to a consumer device that can be connected to the internet, i.e. an Internet of Things (IoT) device. These include smart TVs, smart bracelets and household routers, for example.

In 2023, the Cybersecurity Label was granted to one new device. Currently, a total of 25 devices have the label. For its part, the cooperation with the cyber security authority of Singapore that started in 2021 has increased the number of labels in recent years.

The importance of the role of the Cybersecurity Label in indicating the information security of devices will be reduced with the changes in EU regulations that will enter into force in the coming years. Information produced in the Cybersecurity Label activities are actively used in monitoring and advocating on EU cyber security regulation. The NCSC-FI at Traficom will prepare to change its operations to meet the duties in accordance with the regulations mentioned above.

Operations of the National Coordination Centre

In early 2023, a new centre for cyber security research, development and innovation, the National Coordination Centre Finland (NCC-FI), was established at the NCSC-FI at Traficom with the task of creating conditions for Finnish cyber security operators, such as companies, universities and research institutes, to participate in international research and development work. The NCC-FI is a member of the competence and cooperation network of national coordination centres of EU Member States and the European Cybersecurity Competence Centre (ECCC).

The NCC-FI received project funding from the Digital Europe Programme for the term 2023–2024 to distribute further to third parties for the implementation and spreading of modern cyber security solutions and innovations. With the funding programme, the European Commission aims to increase cyber security capacity and strategic solvency in the Member States.

The first application round for financial assistance ran from 16 June to 16 August 2023. The assistance was available for SMEs registered in Finland. The decisions of the first application round organised by the NCC-FI were issued on 15 November 2023. A total of approximately EUR 485,000 of financial assistance was granted to 13 applicants. A total of EUR 500,000 of financial assistance was available, and the applications amounted to EUR 633,000.

> ” With the funding programme, the European Commission aims to increase cyber security capacity and strategic solvency in the Member States.

NCSC-FI supported the development of legislation

Cyber security regulation has received a commendable amount of attention at the EU level and nationally, and the attention is further increasing. The most important regulation projects in 2023 included work on the national implementation of the NIS2 Directive and implementation coordination on the EU level, completing the negotiations on the Cyber Resilience Act, negotiations on the Cyber Solidarity Act and the preparation of the new eIDAS Regulation. Traficom, and the NCSC-FI as a result, are to receive increasing amounts of new tasks in monitoring compliance with cyber security legislation.

As a part of Traficom, the NCSC-FI supports the development of legislation by offering its expertise to the drafters. In 2023, the NCSC-FI issued statements on dozens of prepared regulations in Finland and the EU and took active part in cooperation groups in its sector in order to ensure high-quality drafting of regulation and compliance with existing regulation.

The NCSC-FI guides and monitors information security, reliability and preparedness in telecommunications operations and the information security of electronic identification and trust services and providers of digital infrastructure and service providers referred to in the EU Network and Information Security Directive (the NIS Directive). The NCSC-FI also monitors the realisation of the protection of confidential electronic communications. As a part of Traficom, the NCSC-FI also issues regulations that specify legislation for the operators it supervises and advises citizens and companies alike on compliance with regulations on a daily basis.

The regulations are reformed regularly to correspond to the changes in the cyber security environment and technological development. An example is the work on reforming the regulation on information security in telecommunications operations carried out during 2023. The reformed regulation will be issued in early 2024.

In 2023, compliance with regulation was monitored e.g. by processing hundreds of disturbance and information security notifications and by issuing case-specific monitoring decisions, e.g. on the use of cookies on websites. The NCSC-FI also implemented inspections of telecommunications operators' data centre access control and marine cable landing sites.

In terms of regulation, the key EU projects in 2023 included work on the national implementation of the NIS2 Directive and implementation coordination at the EU level, completing the negotiations on the Cyber Resilience Act, negotiations on the Cyber Solidarity Act and several work group discussions on strengthening the protection of critical infrastructure.

Cyber security trends in 2024

The cyber security threat level will remain elevated in 2024 as well.

Overview of the general cyber security threat level in 2024

The year 2024 will likely see an increasing number of ransomware cases around the world, and they are likely to be more severe and advanced than before. This situation will also concern Finland, but the active and careful protection and prevention measures and cooperation of companies will be able to limit the threat considerably in the future as well.

The phenomenon of Ransomware-as-a-Service (RaaS) will become increasingly common, making it easier for cyber threat actors with different motivations to use ransomware in their operations. New malware versions are also likely to appear, and ransomware actors will aim to improve their attack methods and likely keep zero-day vulnerabilities as a part of their operational tools.

In 2024, cyber criminals will increasingly aim to exploit AI-based technologies. AI will be developed e.g. to analyse published software updates to create vulnerabilities and methods to exploit them. AI technologies will also be developed for automation. The further development of these methods can allow criminals to automatically look for vulnerabilities in billions of network devices very quicky after their updates are published. This can make the campaigns of ransomware actors extremely effective.

Critical vulnerabilities will continue to be surveyed in Finland in 2024. Dozens or hundreds of domestic organisations are required to take rapid measures e.g. to patch critical vulnerabilities in their network devices.

Products with insufficient information security features will continue to frequently enter the consumer markets.

Denial-of-service attacks against the websites and services of various organisations will continue to be active. The implementation of denial-of-service attacks requires no special technical skill. An attack can be bought as a service from criminal operators. Organisations must prepare for denial-of-service attacks as a part of their daily operations.

Cyber espionage will remain active in 2024 as well. For a state engaged in espionage, cyber espionage is an affordable and efficient method for gaining significant amounts of confidential data. The target of cyber espionage may not necessarily notice being spied on. State actors will aim to use different vulnerabilities to access a variety of confidential data. In Finland, it is the task of the Finnish Security and Intelligence Service to prevent foreign espionage, also online.

One NCSC-FI campaign theme reminded the public of information security in household appliances.

Älyäostoksiin.fi (In Finnish)

Instructions – Denial-of-service attack | National Cyber Security Centre Finland

Important changes to legislation

Cyber security regulation will continue to increase in 2024, both in the EU and in Finland. One of the key areas for the operations of the NCSC-FI is the completion of the national implementation of the new Network and Information Security Directive (NIS2) planned for the autumn of 2024. The new act will bring new tasks for the NCSC-FI, and in 2024, it will prepare for these tasks and offer support for the operators it supervises once the act enters into force.

One of the first steps for companies is to study the basic information security practices published in early 2024 that act as a concrete guide in starting the implementation. Compliance with these practices is essential as companies aim to meet the requirements set by the NIS2 Directive. Companies must be prepared to change and intensify their cyber security practices to better respond to modern digital threats.

Manufacturers of digital products are to expect regulation related to product safety. The date of application of the information security requirements set in the Radio Equipment Directive (RED) has moved to August 2025, giving companies more time to prepare. The directive applies to all devices directly or indirectly connected to the internet. The compliance specifications will be published during 2024. The Cyber Resilience Act (CRA) is expected to enter into force in 2024. The CRA will apply to all internet-connected products throughout their life cycle. The application of the regulation is expected to begin gradually with the obligation of vulnerability notification applied in 2026 and the other obligations in 2027. Manufacturers should already begin to prepare for the basic-level information security requirements. The CRA will challenge manufacturers to develop strong cyber security procedures and integrate them into their production processes already in advance.

The overall reform of the Emergency Powers Act led by the Ministry of Justice will also continue in the coming year, and Traficom and the NCSC-FI will continue to produce statements from the perspective of their sector.

Rapid technological development will continue in 2024

One of the key trends in 2023 was the rapid development of generative AI. Generative methods have been used to produce realistic but fake images, videos and texts. This development is generally considered to lead to the spreading of disinformation and to make it increasingly difficult to separate fact from fiction.

It is likely that generative AI methods can be used to create video in real time during 2024. This will also enable the creation of videos where the facial movements and speech of fictional or existing persons can be synchronised in a realistic manner to create the impression of authenticity. There are several business purposes for creating these videos with the target person's consent, and their use is likely to become increasingly common.

Videos created for scamming purposes and without the target's consent are generally referred to as deepfakes. The real-time generation of deepfakes can further increase scamming opportunities in many sectors. Scamming targeted at companies can use deepfakes e.g. to modify the facial movements and voices of company directors to create the impression of a genuine message.

Once the technology to model faces and voices becomes more common, credible deepfakes can also be created of private individuals. Such deepfakes can facilitate identity theft and various scams where a person's identity is used for fraudulent purposes.

In scamming that targets private individuals, deepfakes modelling real or fictitious persons can give the impression of a more personal interaction between scammers and their victims. This can enhance the victims' emotional connection with the scammers and make them more susceptible to fraud. Relative or romance scams in particular are likely to start using faked voice and video. Scammers can e.g. invent crises or tell any manner of stories in the hope of monetary support. Generative AI technologies can also easily produce credible fake documents to support fraudulent stories. New types of scams are likely to be invented as people learn to be wary of the previous ones.

Cooperation between industry, researchers and public authorities is central to the fight against fake content. From as early a stage as possible, the services to be developed should also be assessed from the point of view of exploitation, and various ways of detecting and preventing exploitation should be sought. Joint efforts can lead to better identification methods and protection mechanisms. For example, advanced techniques for identifying fake videos have already been developed. AI-based systems aim to detect signs that a video or image has been generated, and they try to distinguish genuine content from fake content. Various techniques have also been presented to ensure the authenticity of the content.

Deepfakes can also be used as a part of wider information influence campaigns. Such campaigns can aim to influence public opinion, spread false information or create confusion in society.

Increased awareness of the existence and possible risks of faked content could encourage the general public to be cautious and critical towards digital content. Regulatory measures could also promote the responsible use of AI and set stricter requirements for the developers of generative models. Continuous competition between developers and information security specialists is characteristic of technological development. While security measures are taken, attackers come up with new ways to go around them.

AI methods and generative AI in particular will also be developed for the purposes of defence. They are expected to provide better tools for the maintenance of secure system settings and the analysis of information security incidents as well as opportunities for automated response to security threats. The year 2024 will see various AI-assisted solutions for the detection and processing of information security incidents.

In software production, the use of AI can have many impacts on the cyber security of the systems created. In addition to actual software production, AI has been used to create test cases, which facilitates system development and maintenance. The development of AI models could help developers produce safer code and identify potentially risky code or poor practices. They could likewise help identify vulnerabilities and information security flaws in software.

” While security measures are taken, attackers come up with new ways to go around them.

Information security skill management becomes increasingly important

Cyber crime and criminality are constantly evolving. For example, the technologies and techniques used in different scams and phishing campaigns are developing and becoming increasingly sophisticated and devious. Identifying them becomes more challenging for anyone.

As society is quickly becoming increasingly digitalised, information security skill management and their continuous development are important civic skills. More and more often, private individuals are targeted by cyber attacks such as phishing, data breaches, attempts to hijack social media accounts, ransomware and scam messages. This also includes the various forms of information influence, such as spreading disinformation. For this reason, it is important to invest in maintaining and developing the information security skills of citizens as well as maintaining and developing their media and technological literacy.

The cyber security skills of citizens vary significantly. Some need help with basic issues, such as password and software updates as well as identifying scams. Others have excellent information security skills.

Cyber security also involves trust. If people do not trust the electronic services or products provided by a company or organisation, they do not want to use them, either. The more digitalised society and the services it offers become, the more important it is to pay attention to good information security and maintaining trust. Active, open and regular communications will help with maintaining trust. Both good things and problems must be communicated openly and transparently. In a digitalised society, attention must also be paid to the realisation of inclusion.

Today, public discussion on cyber security focuses greatly on AI and AI-generated deepfakes. When talking of threats, it is good to remember that we are also preparing for them. Just as AI enables novel scams and cyber attacks, it offers means to protect against them.

The National Cyber Security Centre Finland (NCSC-FI) supports the cyber skills of citizens on all levels of information security

Kyberturvallisuuskeskus.fi/en

Our communications specialists show how technology enables ever more devious deceit as a tool for cyber scamming and information influence.

Deepfake: how deepfakes amplify cybercrime and information influence activities | Youtube (In Finnish)

Our KPIs in 2023

Alerts
1
(2022: 1 pc)

Scamming
4,963
(2022: 3,519 pc)

Phishing[1]
9,266
(2022: 5,787 pc)

Data leaks
111
(2022: 104 pc)

Data breaches[2]
1,014
(2022: 1,026 pc)

Data breach attempts[3]
383
(2022: 127 pc)

Automatic reports
209,416
(2022: 188,561 pc)

Information security incidents in total
18,625
(2022: 12,947 pc)

Facebook followers
7,190
(2022: 6,939 pc)

X followers
17,200
(2022: 16,805 pc)

Media contacts
152
(2022: 142 pc)

Customer satisfaction with our situational picture products
4,3
(2022: 4,3)

1 In 2023, we received 3,881 reports of phishing for bank credentials.
2 Including the social media accounts of citizens,
3 Biggest relative increase from the previous year

National Cyber Security Centre Finland (NCSC-FI)
at the Finnish Transport and Communications Agency Traficom
PO Box 320, FI-00059 TRAFICOM, Finland
tel. +358 29 534 5000

Kyberturvallisuuskeskus.fi

Traficom publications 10/2024
ISSN 2669-8757 (online publication)
ISBN 978-952-311-909-3

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre