Information security in 2021

A time of growth for cyber security – we prevent disturbances in advance

Annual report of the National Cyber Security Centre Finland

Traficom publications

3/2022

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Contents

Now cyber security is no longer in its teens

In 2021, our everyday lives were affected by several information security and cyber incidents. Among other things, scams phishing for online banking credentials may have come here to stay. Last year, Finns lost tens of millions of euros to criminals due to scams.

Nearly everyone encountered text messages spreading the FluBot malware by taking advantage of various topics. The malware was not only a nuisance; the victims also lost their information and money. In addition, the contaminated devices spread the malware further.

Anyone can become a victim of fraud. Every one of us can help the people close to us by spreading awareness about scams.

”Frequent cyber incidents became the “new normal” in 2021

Cyber incidents that affected the smooth flow of everyday life occurred around the world. It is good to keep in mind that cyber incidents do not follow state borders, and their impact may also reach Finland. For example, in Sweden, our neighbouring country, the Coop daily consumer goods chain had to close its stores due to a cyber attack.

Because information security and cyber security affect the everyday lives of an increasing number of people, we at the National Cyber Security Centre Finland are also looking for communication channels that could reach as many people as possible. At the end of the year, we started using the 112 Suomi application to issue notifications about extensive information security incidents affecting Finns.

Our operation is focused more and more on preventing serious cyber incidents. The National Cyber Security Centre Finland and our excellent experts are becoming more widely known, which is helpful in this work. The number of information security events we process is growing every year. In 2021, we reviewed tens of thousands of information security events. They made it possible to prevent a massive number of problems before they turned into something more serious. The number of serious network fault situations in Finland continued to decrease over a long period of time. This means that the operators responsible for Finnish networks and the regulations that support them are clearly on the right path. Counting by our number of incidents, phishing is still at the top. The attack volume of denial-of-service attacks also increased.

Preventive work was done by updating regulations and preparing recommendations in cooperation with telecommunications operators. The work will continue within the framework of the Cyber Security Development Programme published in 2021, among other things. The ‘Tietoturvan suunnannäyttäjä’ (Information security trendsetter) award was granted to LocalTapiola for its contributions to preventive activities.

A lot also happened with regard to regulations. The Finnish Government issued a resolution on improving information security and data protection in the critical sectors of society (Titukri). The aim is to set statutory information security requirements for all critical sectors, and critical information systems must be evaluated more comprehensively than they are today. New regulations on cyber security in connection with the EU Network and Information Security Directive (NIS2) were prepared during the year. Attention will also be paid to cyber security issues in the upcoming EU Artificial Intelligence Act.

There was also cause for celebration in 2021 with the approaching 20th anniversary of our CERT function. CERT-FI was officially established in January 2002. Finland has been a pioneer of information security and cyber security for a long time, and we are also taking up this challenge in 2022.

The year included many challenges related to resources, and the growing pains of cyber security are not over. On the whole, however, the year can be summed up by saying that now cyber security is no longer in its teens. We will face new, larger challenges stronger than ever.

Sauli Pahlman
Acting Deputy Director-General
National Cyber Security Centre Finland

Our KPIs

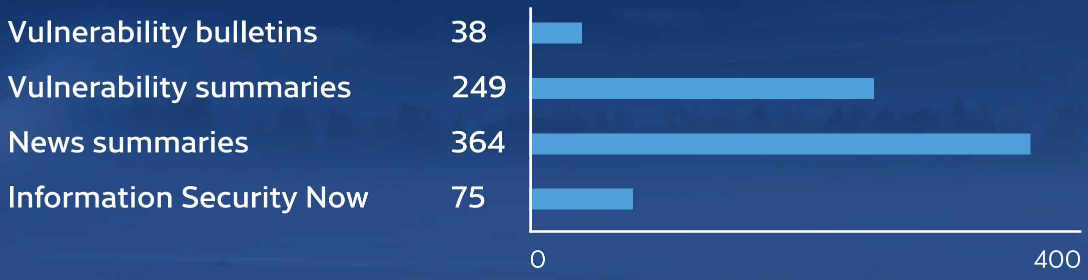
● 2021 ○ 2020

	2021	2020
Uninterrupted on-call duty	24/7/365	24/7/365
Cases processed	17,572	10,892
Alerts	5	1
Shutdowns of harmful sites	5,214	8,500
Cases processed by vulnerability coordination	72	49
Autoreporter	209,237	115,000
Media contacts	141	187
Facebook followers	6,261	6,066
Twitter followers	15,476	13,353

Number of incidents

7	Critical incidents
18	Serious incidents
51	Significant incidents
73	All incidents in total

Communication and bulletins



Vulnerability bulletins	38
Vulnerability summaries	249
News summaries	364
Information Security Now	75

Customer satisfaction surveys

We conducted customer satisfaction surveys during the year concerning our situation awareness products and ISACs. The assessment scale in our surveys ranged from poor (1) to excellent (5). The average of both surveys showing satisfaction was 4.3.

According to the situation awareness survey, our situation awareness products are used to maintain the information security of the organisation, and they provide information about new vulnerabilities and current events. The National Cyber Security Centre Finland compiles the situation awareness based on information from several different sources and distributes it further via a variety of products.

For the National Cyber Security Centre Finland, the ISAC cooperation provides information for constructing and enriching the situation awareness. The cooperation has also made it possible to prevent information security incidents.

The most frequently read situation awareness products are:

- Cyber weather
- Alerts
- Vulnerability bulletins
- Weekly reports

The Information Sharing and Analysis Centres (ISAC) appreciated especially that

- they have an open information exchange via trust networks
- they have information available outside public communications
- the ISACs are an effective and neutral method of communication and exchange of information between the authority and the industry.

Situation awareness products

4.2
2020

4.3
2021

Average

Industry-specific ISACs

4.4
2020

4.3
2021

Average

How did we influence matters?

Digital development constantly makes new services available to us, improves our everyday life and makes it easier, and offers new solutions for global challenges. Even though this development brings good things with it on the whole, the dark side of digital development consists of constantly growing cyber crime and different kinds of incidents.

As with all digital phenomena, cyber threats are also characterised by rapid development. Phenomena related to cyber security are often complex and do not follow the predetermined responsibilities of the authorities. This requires a new kind of ability to act and react from the authorities, too.

The advantage of the National Cyber Security Centre Finland is its wide scope of operations and the diverse technological, legal and social competence that supports it. With their help, we can become organised quickly, if necessary, in cooperation with our national and international partners to respond to different kinds of situations and needs.

The development programme and Titukri as drivers of development

Initiatives were made to improve cyber security. The most important of these were the national Cyber Security Development Programme and the government resolution on improving information security and data protection in the critical sectors of society (Titukri). The development programme improves cyber security over a long period of time, across branch borders. Titukri speeds up the improvement of the level of information security and data protection of society's critical information systems.

The Cyber Security Development Programme drawn up in 2021 specifies the key measures to improve cyber security throughout the whole society. The time scale of the development programme, which was drawn up through broad-based cooperation, reaches all the way until 2030. The primary goal of the development programme is to create a cyber security ecosystem in Finland that produces vitality and growth, increases the number of jobs in the field, creates the necessary expertise and improves the durability and resilience of our digital society with regard to different phenomena in the cyber operating environment. The development programme is built around four main themes: **top expertise, solid cooperation, a strong domestic cyber security industry and effective national cyber security capabilities.** It is clear that strong national cyber security requires the necessary expertise at all of the different levels of society. As regards the authorities, the National Cyber Security Centre Finland plays a key role in developing expertise among the authorities and companies as well as ordinary citizens. Strengthening the cyber security ecosystem requires long-term efforts to improve cooperation. The National Cyber Security Centre Finland has an important role in developing the cooperation on both the national as well as the international level. One of the most important acknowledged tools for developing cooperation consists of cyber security training activities.

For a strong domestic cyber security industry, special attention must be paid to the European Cybersecurity Competence Centre (ECCC) of the EU that is being established as well as the network of national coordination centres. The National Cyber Security Centre Finland of the Finnish Transport and Communications Agency has been appointed as a national coordination centre, and through this role, the National Cyber Security Centre Finland aims to support the national cyber security market and industry in the increasingly more intense international competition. The last of the development programme's main themes involves increasing the effectiveness of national cyber security capabilities. These capabilities create the basis for the functioning and safety of the whole society and promote our sovereignty in the cyber operating environment.

> **”The primary goal of the development programme is to establish a cyber security ecosystem in Finland.**

Titukri helps to prevent another Vastaamo incident in the future

In 2021, due to the Vastaamo data breach incident, a government resolution was drawn up to improve information security and data protection in the critical sectors of society. We play an important role in this work to ensure that the goals of the government resolution can be met. The government resolution pays special attention to more effective and organised cooperation between the authorities, obligatory information security requirements, regular monitoring of the requirements, identification of critical processes and functions as well as the assessment and auditing of information systems. The National Cyber Security Centre Finland plays a key role in promoting the goals of the government resolution, developing the cooperation in connection with cyber security, and supporting the operations of other authorities. It is clear that the resources of the National Cyber Security Centre Finland should be improved to be able to support other sectors and provide them with even more sector-specific advice and support identified during the work on the government resolution.

Even though the aim is to promote the use of the support measures of the National Cyber Security Centre Finland and the services it provides in different sectors, each sector must continue to develop its own operations towards constantly improving information security. As a rule, information security should be built into the operating culture of critical sectors, and the actors must bear the responsibility for it themselves.

> ” **Information security should be built into the operating culture of critical sectors.**

Working together to stamp out online scammers

Anyone can become the victim of an online scam, and tens of millions of euros have fallen into the hands of criminals. The authorities, companies and organisations carry out a broad-based cooperation against scams. In 2021, information about cyber incidents could be sent directly to mobile phones via the 112 Suomi application for the first time.

Finns lose tens of millions of euros to various kinds of online scams every year. The National Cyber Security Centre Finland cooperates actively with telecommunications operators, the police, other authorities and organisations by combating online scams in particular. The bulletins and warnings drawn up by the National Cyber Security Centre Finland give accurate and up-to-date descriptions of ongoing scams and phishing campaigns. Scam campaigns by criminals are nothing like a hobby or hackers pulling a prank; instead, they are carried out by international leagues of professional criminals. Authorities simply providing information about the problem does not solve it; the entire media sector from the afternoon papers to morning news are needed for educating the public. The press deserves thanks for making the public aware of scam phenomena. The National Cyber Security Centre Finland also participates in the ‘Huijarit kuriin’ (Subdue Scammers) project by the Consumers’ Union of Finland that actively educates people on how to prevent scams.

National Cyber Security Centre Finland began using the 112 Suomi application as a new communication channel. The application was launched by the Emergency Response Centre and is used by nearly two million Finns. During 2021, two warnings about extensive scam campaigns targeting private individuals were sent via the 112 Suomi application. Millions of Finns have been warned about dangerous scams and malware attacks, but new victims nevertheless pop up constantly. The goal is to decrease the number of both the victims and the proceeds of crime in the coming years.

> ” **Authorities simply providing information about the problem does not solve it; the entire media sector from the afternoon papers to morning news are needed for educating the public.**

Together, Traficom and telecommunications operators trip up fraudulent calls and malware that spreads through text messages

Actions by telecommunications operators are needed to get certain scams under control. In 2021, Traficom and telecommunications operators together looked for ways to prevent the forging of phone numbers. In the process of stopping the FluBot malware, the operators' message filters caught more than a million malicious text messages.

Forging the caller's phone number to look like a Finnish phone number is a method used extensively by international criminals to greatly increase the likelihood of Finnish victims trusting the number. Victims could answer scam calls from abroad and comply with criminals´ requests such as handing over their online banking credentials or allowing criminals to remotely control their computer. Starting from last year, forging the caller's number in scam calls from abroad has been a major problem in Finland. In order to correct the problem, Traficom started to work with telecommunications operators to find ways to prevent forging the caller's number to look like a Finnish telephone number. The goal is to prevent and hinder the activities of international criminals. Thanks to the solution, the telecommunications operators can make sure that the number belongs to the subscription customer who has the right to use the number in question. As for the person who gets the call, they can trust that a call from a Finnish number has been made from a Finnish telephone subscription. In addition, a party with a Finnish telephone number and subscription can trust that their telephone number is not used to commit crimes.

Rapid measures were taken with the telecommunications operators to prevent the spread of the FluBot malware

We worked together with telecommunications operators to combat the wave of FluBot mobile malware, which began in the summer. We transmitted up-to-date information to telecommunications operators about the command channels used by the malware to help telecommunications operators filter the malicious network traffic. This made the malware inoperable and prevented the infections from spreading further from a contaminated device.

In November, a more advanced version of the FluBot malware began to spread; it used the DNS Over HTTPS (DoH) protocol as its command channel. It cannot be combated by filtering network traffic without disturbing the operation of several other services. We combated the new FluBot wave by recommending telecommunications operators filter SMS messages spreading FluBot malware, among other things. Over a million such messages were filtered, meaning the measures had a significant impact in controlling further spreading.

Updating the regulation on electronic identification and trust services in cooperation with the industry.

1. Mandatory controls that improve the safety of the end user, such as session identifiers and confirmed target service information.
2. The user is informed in a better and more consistent manner throughout the identification event.
3. New options for authenticating and securing telecommunications connections between different actors.
4. Updated and more flexible requirements on encryption practices that make it possible to deploy new encryption solutions more easily.
5. A separate risk assessment must be conducted on the identification means that assesses the threats and protective measures concerning identification means and factors.

Our services for trade and industry

The National Cyber Security Centre Finland develops and produces cyber security services for the trade and industry and operators critical to the security of supply that help with maintaining and developing information security in the rapidly changing world. The users of the services of the National Cyber Security Centre Finland constitute an information security community, in which information is shared confidentially.

Kybermittari

The first year of the Kybermittari tool is now complete, and based on the feedback received, there is demand for a systematic cyber security capability assessment model. Throughout the year, Kybermittari has been presented to interest groups, feedback has been collected, training events held and new ideas tested. In early 2022, a new version of Kybermittari will be published; it takes customer feedback into account, and the changes to the Cybersecurity Capability Maturity Model (C2M2) version 2 published in the summer have also been implemented in it.

Lessons learned from ISAC training that benefit the sectors

During the past year of 2021, we have developed the cyber training of the ISACs of the National Cyber Security Centre Finland in cooperation with ISAC actors*. We have organised training for the Food Supply, Energy, Water and Logistics and transport ISACs in cooperation with Insta and Fraktal. The theme of the training events has been exchange of information, the situation awareness and the role of the authorities in extensive cyber incidents that affect the sector. Good observations have been made and lessons learned from the joint training exercises of the ISAC actors that will help improve the readiness and ability of the sectors in question to face cyber threats.

HAVARO

HAVARO, the national monitoring and early warning system for severe information security violations, was reformed in 2021. The service is now offered to a wider range of Finnish organisations in cooperation with commercial information security actors. Tietoturva ry granted HAVARO an award as the information security product of the year.

* ISACs (ISAC=Information Sharing and Analysis Centre) are cyber security cooperation bodies established in different industries.

Reliable time and location information is a pillar of society

Society is increasingly more dependent on the time and location data generated by satellite positioning systems. The Public Regulated Service (PRS) of the European Galileo satellite positioning system is intended to provide confirmed and continuous time and location information for the authorities and companies critical to the security of supply in all situations.

Parties using the PRS service in Finland include the police, the Finnish Customs, the Finnish Defence Forces and the rescue services as well as companies critical to the security of supply, such as telecommunications operators, banks and the energy sector, in addition to the transport and logistics sector.

This pillar of society – reliable time and location information – received a solid foundation in November 2020 when the Government's Ministerial Committee on Economic Policy stated that the PRS will be deployed in Finland in 2024. We started the work on planning the service together with the future service operators, Suomen Erillisverkot Oy and the Finnish Defence Forces.

> ”The theme of the training events has been exchange of information, situation awareness and the role of the authorities in extensive cyber incidents that affect the industry.

The safety and security of communications networks

Our society is increasingly dependent on communications networks, and the network technologies are developing. In 2021, the information security of 5G networks and the protection of the most critical parts of the network were particular points of concern.

The safety of communications networks has remained a high priority in discussions both at the EU as well as the international level. In the EU, the Member States have discussed the deployment of the most recent generation of 5G networks and their safety with an unprecedented vigour. These discussions will continue, and their weight will grow further as the communications network technology develops and society's dependence on communications networks increases. New regulations on the safety of communications networks entered into force in Finland at the start of 2021. Factors behind the national regulations included especially the joint EU approach to responding to the security concerns related to 5G networks. The work on the security of 5G networks in the EU culminated in a joint toolbox created by the Commission and the Member States that highlights several measures for ensuring the safety and security of 5G networks and the services that rely on the networks for their operation. One of the most central measures among the methods available is the sufficient protection of the most critical parts of the network. The national regulations that entered into force at the start of the year enable the assessment of the critical parts of communications networks from the perspective of national security and national defence. The starting point is that devices that may endanger national security must not be used in the critical parts of the communications network. If such a device is found, its removal can be ordered.

The regulations on the security of the critical parts of the communications network were supplemented with a technical regulation of the Finnish Transport and Communications Agency in the spring of 2021. The regulation clarified the technical specification and identification of critical parts. Both the national regulations as well as the regulation of the Finnish Transport and Communications Agency were drawn up in an extensive cross-administrative cooperation. Representatives of the industry also participated actively in the preparations.

With regard to the regulations that have been drawn up, and the recent regulation in particular, it should be kept in mind that it must be possible to update tools created due to technological development at a rapid schedule. As a result, technological development and the needs for change it creates with regard to regulation, among other things, will be assessed regularly by the Advisory Board for Network Security established early in 2021.

> **” One of the most central measures among the methods available is the sufficient protection of the most critical parts of the network.**

Cyber weather phenomena

The cyber weather maps showed powerful denial-of-service attacks, aggressive malware and a record amount of phishing.

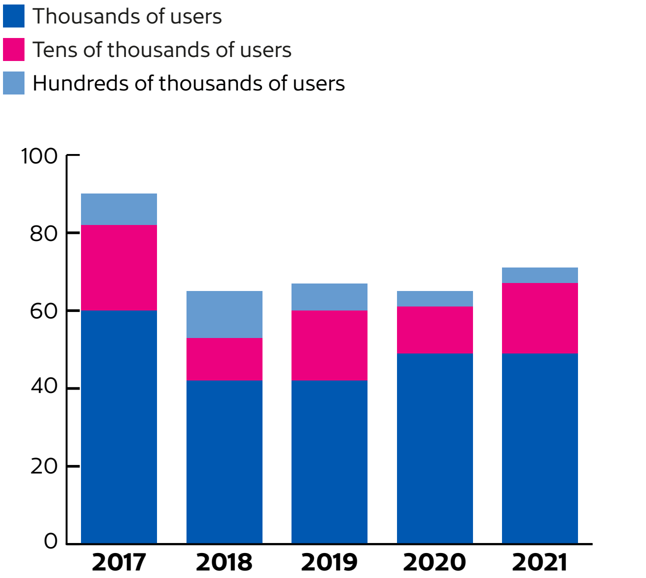
Network functionality

The number of serious network fault situations in Finland continued to decrease over a long period of time. Interruptions in global services affected us, too.

Disturbances in communications networks

In 2021, different kinds of disturbances in the general communications network and international services showed us yet again how dependent we are of functioning connections and different kinds of digital services. A widespread service interruption may affect the critical functions of society – at the same time, the same interruption may also prevent citizens from using social media until the fault has been repaired.

We are used to services being constantly available online. Different kinds of outages in the domestic network, banking services or social media are concrete proof of the importance of risk management and preparation for the users of the services, too. An outage may mean that customers cannot pay for their purchases, the social media account of a small company is not updated and viewers miss their movie on the streaming service.



Number of significant disturbances of the functioning of communications services in 2017–2021

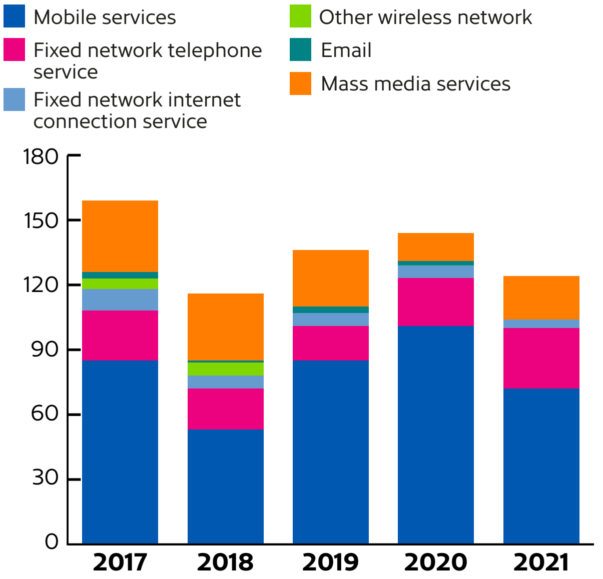
> **The trend can be considered positive, even if the number of significant disturbances has stopped decreasing.**

The status of communications networks in Finland remains stable

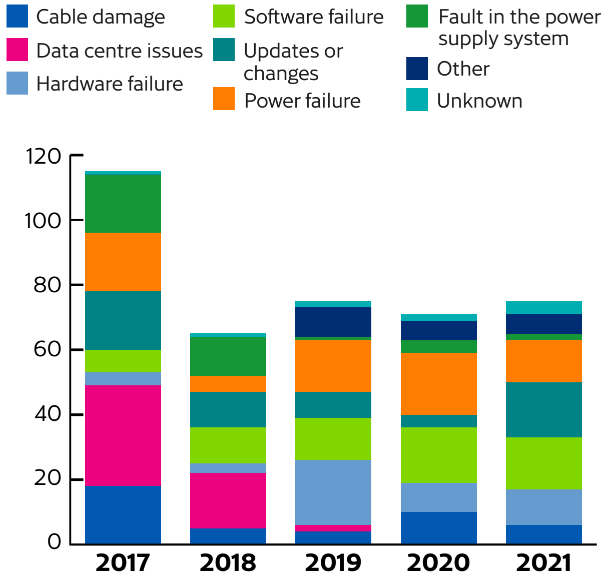
We collect information on disturbances in the domestic communications networks. This allows us to tackle the root causes of the disturbances and improve the safety and reliability of networks in cooperation with the industry.

The number of major disturbances decreased clearly until 2018. Since then, there have been 65–73 disturbances reported per year. There were 73 significant disturbances in 2021. The capacity of our networks has been more than sufficient throughout the pandemic and the increased load.

The number of critical disturbances that apply to at least 100,000 users has decreased in recent years.



Effects of significant disturbances on general communications services in 2017–2021. One disturbance may affect several services.



Root causes of significant disturbances in 2017–2021. One disturbance may have several root causes.

> ” The outages remind us that any service may be interrupted at any moment.

As a whole, the trend can be considered positive, even if the number of significant disturbances has stopped decreasing.

The majority of significant disturbances in Finnish communications networks involve mobile network services, i.e. the functioning of calls, internet connections and SMS. Power failures, different kinds of configuration errors, hardware failures and cable damage, for example, cause malfunctions in the network. Faults could also be caused by a human typing error or an excavator bucket hitting a cable. Telecommunications operators faced their share of denial-of-service attacks, and name servers, for instance, were targeted by attackers in 2021. The attacks did not have any major impact, however.

The big storms in 2021 were called Aatu and Paula, and they hit Finland in late June. In fact, 14 major disturbances in the common communications network services were reported to the National Cyber Security Centre Finland in June. In July, an excavator damaged a fibre cable, which affected the different Valtori services for hours. Well-functioning cooperation between the authorities, telecommunications operators and electricity companies helps with preparing for storms and different kinds of incidents.

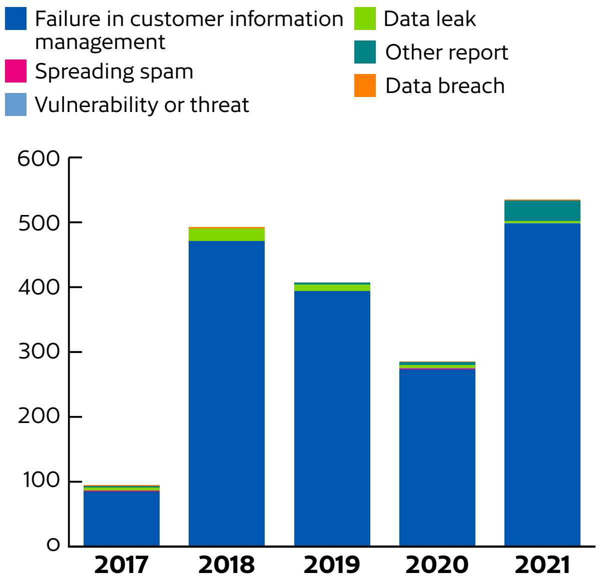
Hiccups in popular and global services were felt here, too

Email services had outages especially in March due to a vulnerability in Microsoft's Exchange email servers. The updates to fix the vulnerability and information security investigations of the servers kept email traffic slow at certain times and locations. A significant vulnerability caused at least momentary interruptions in email traffic when the servers had to be updated as quickly as possible due to the critical situation – even in the middle of the workday.

In September, global service interruptions in Facebook, WhatsApp and Instagram stopped the use of services for several hours on a weekday night. Services such as Microsoft, Slack, Salesforce and Fastly also experienced outages during the year. The interruptions were visible in the availability of different services and in certain websites not working, for example. According to international service providers, problems were caused by different kinds of configuration errors or application design errors, among other things. The outages remind us that any service may be interrupted at any moment. Citizens and organisations should be aware of the fact that social media services may sometimes be unavailable for long periods of time. We are used to the good availability of services, but the examples show that outages may have a harmful impact on issues such as updating the advertising page of an SME or the communication of citizens with their family and friends.

Information security notifications about personal data have decreased

The reports by telecommunications operators on information security violations have steadily decreased after the peak in 2018. A typical case involves a telecommunications operator sending a letter or an email message containing personal data of the customer to the wrong address. There are usually less than ten significant information security violations in a year. In 2021, 17 were reported.

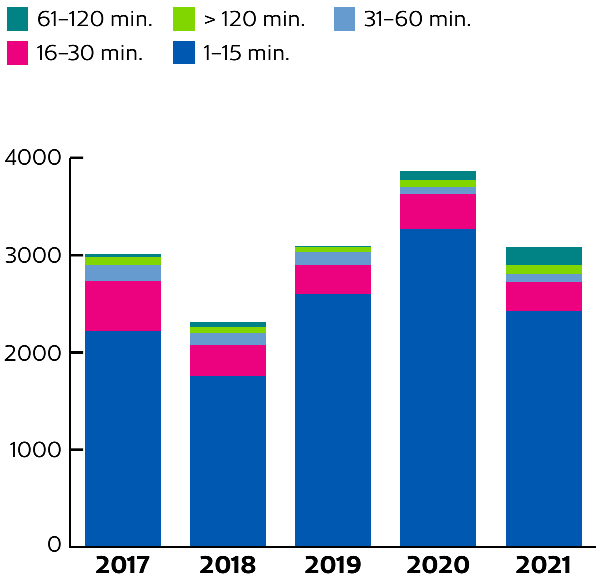


Reports by telecommunications operators on significant information security violations and personal data breaches in 2017–2021. In 2021, more and more telecommunications operators started to report violations, and as a result, the number seems higher than before.

Denial-of-service attacks

The National Cyber Security Centre Finland received dozens of reports about denial-of-service attacks that affected the ability of organisations to function. The attacks caused either short outages in the remote connections of employees, or they involved attacks against an online service, for instance, that lasted for hours.

When repeated, even short denial-of-service attacks can become a nuisance to an organisation if they cause indirect problems in the operation of internal services. We have received several reports in which the attack affected the organisation's VPN connections. If that happens, work may stop momentarily and even remote meetings will have to wait until the connections return. Organisations often change over to cloud services, which are implemented in such a way that they can withstand even major denial-of-service attacks without them affecting the usability of the services.



The development of duration of denial-of-service attacks in Finland. Source: Telia

In municipalities, education digital services were hit

We received reports from municipalities about attacks targeting different education services at schools or addresses of the school's external network. In fact, services should be designed so that even a short-term denial-of-service attack will not disturb services. Reports of an offence concerning denial-of-service attacks are also filed with the police every year. A brief attack may cause interruptions in a service and start the investigative process by the police, for example. It is good to keep in mind that even those under 15 years of age may be held responsible for them. We encourage organisations to file a report of an offence in case of a denial-of-service attack.

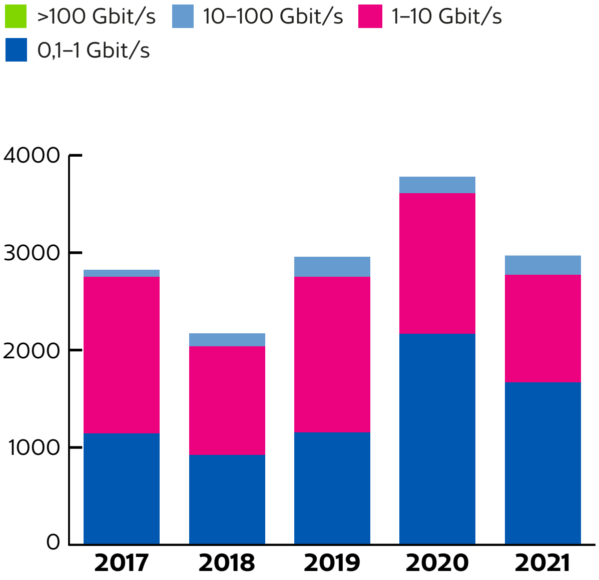
Record-breaking denial-of-service attack volumes

During the past year, we supported several organisations when they faced denial-of-service attacks and supplemented the situation awareness of the attacks in cooperation with our international partners in cooperation. In Finland, a typical size of the denial-of-service attacks reported to the National Cyber Security Centre Finland has been 1–10 Gbit/s. Domestic organisations are prepared for attacks of this size with the help of the operators' mitigation services, for example.

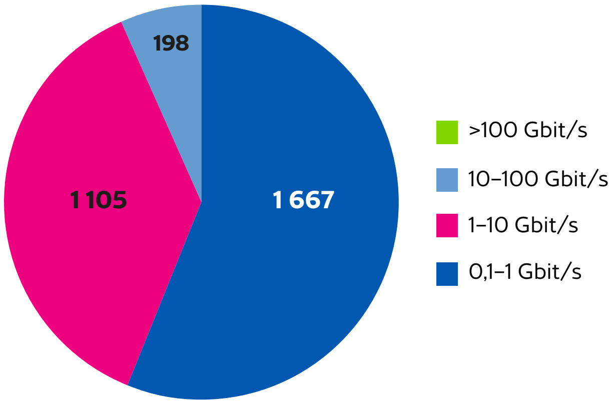
In 2021, a handful of massive, approximately 100 Gbit/s attacks were detected in Finland; among other things, they caused service outages for organisations. We also received a report about the largest denial-of-service attack in Finland so far. The volume of the 260 Gbit/s attack was record-breaking, but the mitigation services managed to prevent it.

In 2021, too, domestic organisations faced denial-of-service attacks linked to a blackmail message. In a few cases, the blackmail message was found in email spam folder, while others had received the blackmail message via an example attack. The threats of larger attacks were not realised, however.

The strength of the example attacks may easily be more than 10 Gbit/s. Around the world, blackmail messages have been sent to telecommunications operators, among others. In addition, major international service providers reported once again about unprecedentedly large denial-of-service attacks against cloud services, for instance. Cloud services are designed to withstand different kinds of attacks, however, and often there is no visible impact on services.



The development of denial-of-service attack volumes in Finland
Source: Telia



Distribution of denial-of-service attack volumes in Finland in 2021.
Source: Telia

> ” The volume of the 260 Gbit/s attack was record-breaking, but the mitigation services managed to prevent it.

Cyber espionage

Vulnerable network devices and services are an object of interest in cyber espionage, because they can be used to access confidential information, communications or systems.

Cyber espionage has continued actively in 2021, too, but Finland has been spared from the worst of the trouble. The aim to take advantage of different kinds of vulnerabilities in cyber espionage operations has been very visible both in public discourse as well as observations related to cyber espionage. The increased use of remote connections due to the growth of remote work has also remained a popular target of cyber espionage.

Vulnerable network devices as targets

Finnish organisations are constantly targeted by different kinds of activities aimed at finding vulnerable services or weak passwords, and this has also continued in 2021. Based on public, commercial or other sources, some of the activities indicate malicious actions by state actors. Password guessing typically affects the cloud services of organisations or other services accessible online.

Vulnerable network devices and services are an object of interest in cyber espionage due to the access to confidential information and communications or other systems. Such hardware and equipment include e.g. email servers such as Microsoft Exchange and VPN solutions such as Pulse Connect Secure. Vulnerabilities in both were revealed in 2021, and taking advantage of them has also been a part of the range of methods used by state cyber actors.

As for vulnerable small and home routers in Finland, they can be used as a part of the attack infrastructure in cyber espionage.

Measures related to network devices and vulnerable services as well as finding and using them are estimated to continue next year, too.

> ” **Based on public, commercial or other sources, some of the activities indicate malicious actions by state actors.**

Several groups have also been visible in Finland

Various Advanced Persistent Threat (APT) groups are focusing their interest on both Finnish companies as well as public administration.

For example, a campaign linked to the NOBELIUM group in the media was also visible in Finland. In a campaign visible in several European countries, the group also known as APT29 and Cozy Bear sent phishing messages or messages containing a harmful attachment to the target organisations. Allegedly, the same group was also behind the harmful change to the SolarWinds Orion management tool that came to light at the end of 2020. The group is also accused of data breaches to several IT service houses around the world in 2021.

Delivery chain attacks are expected to cause large-scale investigations in 2022, when organisations have to investigate if a company, service or system that has been breached has been used in an attempt to access their own systems.

In the spring, the Finnish Security and Intelligence Service also attributed a case of cyber espionage against the Parliament at the end of 2020 to the APT31 operation. In the turn of 2020 and 2021, the Parliament reported a cyber attack, which affected some of its email accounts. As for the Ministry for Foreign Affairs, the Pegasus tool intended for spying on mobile devices had been used in an attempt to spy on its personnel. Its use in cyber espionage became widely discussed in the summer of 2021.

The National Cyber Security Centre Finland advises, provides information and investigates matters

The National Cyber Security Centre Finland actively monitors trends related to cyber espionage operations, observes threats and informs Finnish organisations about them both more extensively as well as in a focused manner. The National Cyber Security Centre Finland offers assistance to parties that suspect that they have been targeted by a cyber espionage attempt or other serious data breach or its attempt. The support may include e.g. advice, technical analysis or coordinating the investigation into the data breach.

In addition, the National Cyber Security Centre Finland carries out national and international cooperation in several different directions with the goal of maintaining an up-to-date situation awareness and ensuring that Finland will be able to prepare for different kinds of developments and threats in advance.

Malware and vulnerabilities

The critical vulnerability in Microsoft's Exchange email server, the vulnerability in the Log4j component as well as FluBot mobile malware spread via text messages were major influences during the year of vulnerabilities and malware.

The Exchange vulnerability attracted cyber criminals and required an alert

In the spring in Finland and around the world, there were news about a critical vulnerability in Exchange email servers being actively exploited. After the vulnerability was published, exploiting it increased rapidly especially among cyber criminal and state cyber actors. We encouraged organisations to investigate affected systems for breaches and guided them through the process. In our instructions, we emphasised especially that simply installing the software update was not enough to keep the attackers away. We also published an alert about the vulnerability in 1/2021.

In the beginning, we detected roughly 300 vulnerable Exchange servers in Finland, some of which had already been breached. It is important to make the general public aware of such a set of vulnerabilities quickly so that exploiting the vulnerability can also be prevented or at least noticed quickly. We contacted more than 250 organisations, and by the end of March there had been 74 breaches reported to us. The vulnerable Exchange servers of Finnish organisations had been updated by the beginning of April.

Many reports about Android malware – FluBot in the lead

Based on the information security notifications we received, the theme of 2021 consisted of different kinds of Android malware. During the year, we received more than 15,400 notifications, over 5,400 of which involved Android malware. An especially large number of information security notifications were made concerning the FakeCop/FakeSpy and FluBot malware.

The second and fourth alert we published during the year involved the FluBot malware. Attempts to spread this Android malware were made throughout the year by means such as text messages sent in the name of delivery services. In June, messages regarding an answering machine became more popular. In November, topics involved voice messages and package deliveries. As far as we know, scam messages were sent to thousands of Finns.

FluBot may steal information from a smartphone, for instance, and use it to send scam text messages that spread the malware as well as other text messages abroad. The attempt to spread the malware may target any device, which means that prevention is important. Companies in particular should know what information is stored on employee phones and draw up a risk assessment on what kind of an impact a data leak caused by malware could have.

The Log4shell vulnerability cast a shadow over the rest of the year

The vulnerability of the Log4j library discovered in early December 2021 was actively exploited, and data breaches related to it also occurred in Finland.

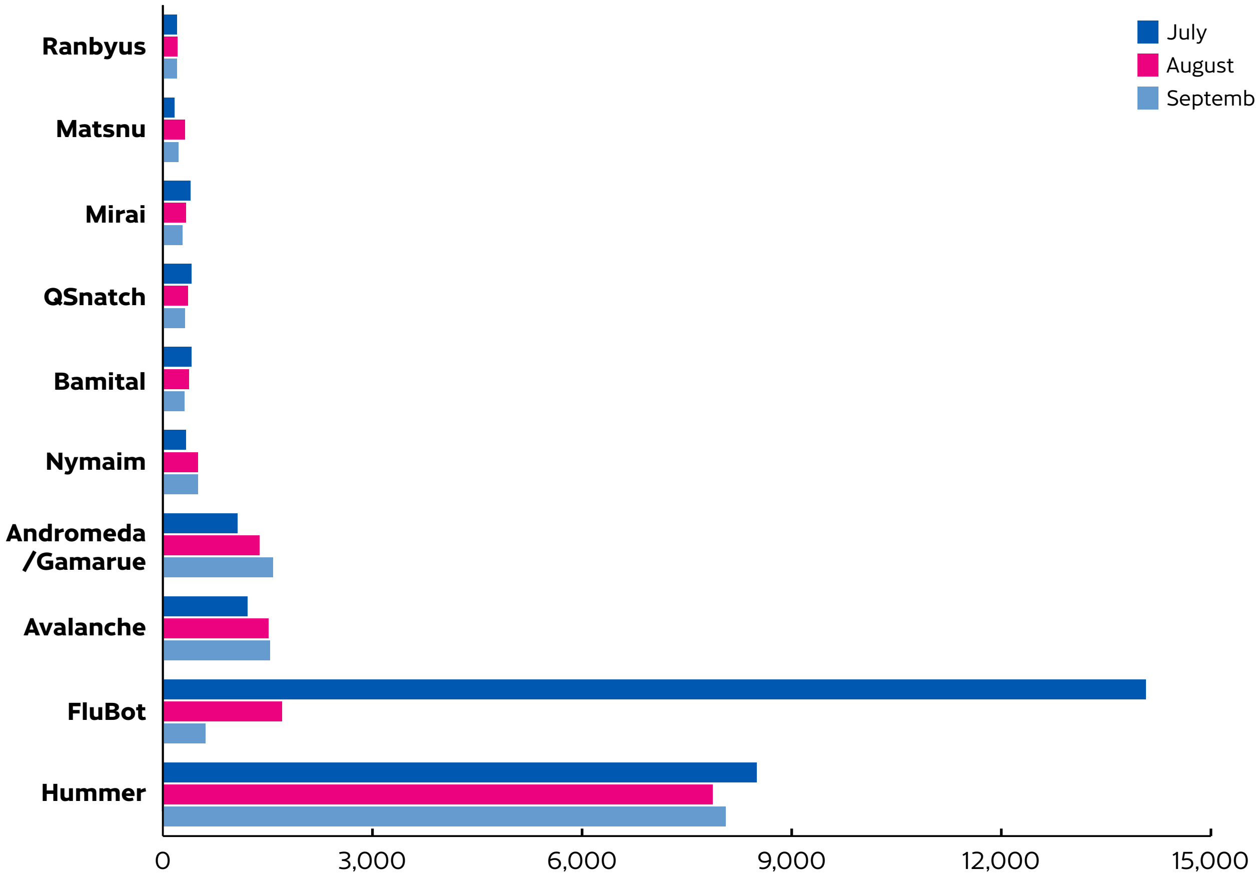
We published a critical alert 5/2021 concerning the vulnerability; it was the last one in 2021. The vulnerability is exceptional, because it applies to a large variety of environments. The vulnerability may affect both the organisations' own ICT environments as well as the cloud services it uses.

The effects of the vulnerability are not limited to any specific sector, either. The vulnerability may affect office systems, the background systems of organisations as well as industrial automation systems. The vulnerability is critical, because in practice, it acts as a master key to the exposed service.

"The Log4j vulnerability exposes an enormous number of systems to attacks. It is the most serious vulnerability of this decade to date. Log4j may have a larger impact than the WannaCry incident in 2017 that caused billions in damages globally," says Juhani Eronen, Chief Adviser at the National Cyber Security Centre Finland.

The National Cyber Security Centre Finland announced the vulnerability in the media, and we also reminded company executives that the vulnerability should be approached as a risk to the continuity of the organisation's own business. Ransomware may completely prevent the organisation from carrying out its core business, for instance. The real impact of the vulnerability will only be revealed during the next few months, and the methods of exploiting the vulnerability will remain in the toolbox of attackers for years to come.

Types of malware in Q3/2021



In 2021, Hummer and FluBot stand out clearly among the malware observations collected by the Autoreporter system of the National Cyber Security Centre Finland. There have been roughly 8,500 Hummer observations every month. The highest number of observations of a specific malware occurred in July 2021, when there were 14,067 FluBot observations.

Data breaches and data leaks

During 2021, several data breaches occurred around the world in which criminals used ransomware against organisations. Once a data leak has occurred, removing the data from the internet is practically impossible.

A typical feature of the Microsoft Exchange data breaches in the spring was installing a webshell backdoor on the victim's email server. The operating model used in these data breaches has been known already since 2020. The investigation requires a lot of technical expertise and resources, which is why it is good to get help from companies offering information security services, for example. In the spring, we published a guide to help with investigating data breaches.

Ransomware is used increasingly often in connection with data breaches

During the past year, several cases were reported in Finland and around the world in which ransomware had prevented the victims from using their own systems and data, among other things, after a data breach. The most widely discussed case was that of Colonial Pipeline in the United States, which ended with paying the ransom.

According to the organisation's management, the decision was not easy. Paying the ransom is not recommended, because the flow of money supports the business of the criminals and paying the ransom does not mean that the attacker would hand over the decryption key for the ransomware to the victim.

The processing of the case of the psychotherapy centre Vastaamo that became public in the autumn of 2020 also continued in 2021. We received a few reports of websites where the personal data of the victims of the data breach had been published again. When we found out about the sites, we submitted removal requests concerning them. Nevertheless, the unfortunate fact is that once material has been released to the public, it is almost impossible to remove it from the internet.

Protection against data breaches requires a lot of effort

Organisations may suffer a data breach or leak even if everything possible had been done to protect the data. The service or website may have a previously unknown vulnerability, there may be a configuration error, or the login IDs of an employee may have ended up in criminal hands.

Protection against data breaches is a major challenge. It is nevertheless possible to make the breach difficult for attackers and more easily detectable for the defenders. We want to encourage all actors to develop protection and allocate resources to it in the future, too. In many cases, the resources allocated to the purpose may be fairly minor compared to the damage a cyber attack can cause.

> ” **Protection against data breaches is a major challenge.**

Phishing and scams

Text message scams were created at a record-breaking pace and with unprecedented inventiveness. The proceeds of crime gained by the scammers also broke previous records.

Finns were scammed out of tens of millions

This year, too, scammers have gained more than 30 million euros as the proceeds of crime. The sum has increased by more than 60% from the previous year. Thousands of different types of scams in the data network are reported to the police every year, and the financial losses incurred due to them rise into the tens of millions. In 2021, losses of more than eight million euros were caused by the phishing of online banking credentials alone, when criminals obtained the online banking credentials of consumers through phishing and used them to empty bank accounts. Over 800 reports of an offence involving phishing for bank information were filed with the police, and over 1,800 information security notifications were sent to the National Cyber Security Centre Finland.

The phishing of online banking credentials has become an increasingly more elaborate and professional crime. Credentials are typically phished by sending scam messages forged to appear as if they came from the bank. Criminals have now noticed that online banking credentials are used for more than just banking purposes and that they can be used in scams: online banking credentials can also be used for logging in to services by the authorities.

> **”The phishing of online banking credentials has become an increasingly more careful and professional crime.**

In 2021, online banking credentials were phished through messages forged to look like an official service, such as My Kanta or suomi.fi.

In October, the National Cyber Security Centre Finland published an alert concerning the phishing of online banking credentials in the name of official services. The alert was noticed widely in the media, and several news stories were written about it. A notification about the alert was also issued via the 112 Suomi application for smartphones that covers nearly two million Finns. The new alert channel was very well received, and we hope that it has helped us stop the online banking credentials of thousands of customers from ending up in the hands of criminals.

The FluBot malware that spread explosively in Android phones at the start of the year also steals banking information. In addition, it sends thousands of text messages all around the world, causing a massive invoice for the victim’s telephone subscription. The yellow alert issued in June about the FluBot malware was removed when the phenomenon died down. The epidemic recurred soon after the alert was removed, however, and the alert was reactivated in July. The same phenomenon came back yet again in a new form, and another alert about FluBot was published in November. The malware sends scam messages that lead to a download page for the exploit with rapidly changing pretexts. Traficom’s alerts have received plenty of visibility in the media.

Text messages in general gained a major foothold as a tool for scams. The sender of a text message is nearly as easy to forge as the email sender information. So far, text messages have been used for scams less often than email, meaning that its reliability is still considered higher. This makes it an attractive scamming tool for criminals. Still, a link in a text message on the phone screen takes you just as often to a phishing site as a link in an email message. There is still a lot of work to be done in learning not to click.

Internet of Things and automation systems

All devices openly visible in the public network are a cyber security risk. The use of industrial and household IoT devices is easy, but in our experience, it is unfortunately often not secure. The National Cyber Security Centre Finland encourages device manufacturers to develop devices with better information security and aims to promote their visibility. In consumer devices, the Cybersecurity Label shows that the device manufacturer has taken appropriate care of the information security of its device. For organisations, the National Cyber Security Centre Finland recommends the Kybermittari tool.

Risks grow when office and automation systems are united

Traditional office systems (IT) and automation systems (OT) are becoming more and more closely intertwined. One good example of this is Colonial Pipeline, which became the victim of ransomware in May. There were disturbances in fuel distribution throughout the whole West Coast of the United States for several days. The case is significant, because the attack did not affect the fuel distribution automation; instead, it hit the business systems that support it. It was not possible to keep the critical production running, because the related financial transactions could not be made.

For example, similar dependencies are related to the material streams and maintenance systems linked to production. We encourage Finnish companies to examine the risks related to securing their production from this perspective of interdependencies, too.

There are still unprotected devices online

In the annual survey of unprotected automated devices by the National Cyber Security Centre Finland, approximately 12.2 million IP addresses in Finnish virtual space were mapped. Unfortunately, we once again found plenty of poorly protected automation devices of companies and vulnerable consumer IoT devices online.

The automation devices used by companies are not traditionally designed to be connected directly to a public network, which is why their information security controls are not sufficient for the purpose, either. If there is a need to reach these devices via the public network, a sufficiently safe remote connection solution must be deployed.

An individual production automation device that is visible in the public network exposes the entire production network to a major risk, because it gives the attacker an opportunity and a channel for moving on to the other parts of the production network. The attitude of many consumer device manufacturers towards information security is sloppy. The original implementation method of the devices may not have any information security at all, or the manufacturer does not correct any of the vulnerabilities discovered. For example, domestic devices used as a part of a botnet controlled by criminals are a constant threat to all internet users and services. A bot army of consumer devices can create earth-shattering denial-of-service attacks.

A contaminated domestic IoT device also opens our homes to online criminals. Consumers can reduce this risk significantly with their own choices. The cheapest option is rarely the best one with regard to the information security features. If the device cannot be updated, it belongs with the other waste electrical and electronical equipment.

Year of the Cybersecurity Label

Traficom's Cybersecurity Label helps consumers identify secure products. The Label's area of influence expanded in October 2021, when Traficom started mutual recognition of the Cybersecurity Label with the cyber security authority of Singapore. This means that products that have received the Cybersecurity Label are now also approved by Singapore.

In addition, we developed the cooperation by offering commercial actors the opportunity to carry out the technical inspection related to granting the Cybersecurity Label. The first to take advantage of the opportunity was the Norwegian company NEMKO; it inspected Datek's Smart Hub, which received the Cybersecurity Label in June. We hope that the cooperation with commercial actors will also continue to be fruitful in the future.

Cyber weather 2021 and a look towards 2022

Cyber security is headed towards prevention. Regulations aim to achieve reliability and security, but everyone can affect information security in everyday life. Valuable volunteer work to improve cyber security awareness is being done in the field. Among other things, we have campaigned for information security for the elderly.

10 information security forecasts for 2022

1. Regulation expands over new technologies and into new industries

There are currently several legislative projects ongoing in the European Union aiming to, among other things, clarify the rules of digital services, make artificial intelligence, smart devices and data management safer, and specify the information security obligations of different actors. The new regulations also actively plan for and create new digital security actors in the EU playing field.

2. Technology as a stage for the competition of superpowers

The competition between the superpowers is turning increasingly quickly into a competition for the technological mastery of the world. This is visible in e.g. the standardisation of technology, in which China in particular is strengthening its role in accordance with the China Standards 2035 programme. This means that Finnish technological innovations are also interesting targets of cyber espionage.

3. Not everyone can keep up with digitalisation

The coronavirus pandemic sped up the digitalisation of services, and more and more services are available online around the clock. Digitalisation makes dealing with the authorities easier and speeds up everyday life – but not for everyone. The lack of digital skills, language skills or an online connection may weaken the feeling of inclusion in the digital environment. When developing services, more and more attention should be paid to accessibility and inclusion.

4. Semiconductor shortage continues

The semiconductor shortage shows no signs of easing off. Organisations may have to wait for new devices for months, meaning that they may need to use devices that have reached the end of their life cycle longer and building new protection solutions will take longer than planned. In fact, care should be taken when purchasing equipment, because disturbances in availability and the increase in prices attract cheap copies to the market. Even though Europe and the United States are attempting to reduce their dependency on the Asian semiconductor factories, the shortage is expected to continue long into 2022.

5. Smart devices should be recycled, too

New technologies can help with finding solutions for combating climate change, but the other side of the coin is the increasing environmental load created by the growing number of smart devices. This means that you should ensure that the electronics and smart devices that have reached the end of their lifecycle are recycled, repair the devices, if possible, and ask the seller about updating smart devices. Traficom's Cybersecurity Label helps you when shopping for a smart device.

6.

The need for cyber security experts is diversifying

As new regulations and cyber security meld into a part of the daily functions of companies, the need for experts increases further. Companies are no longer looking just for coders; instead, the demand for more broad-based expertise in digitalisation, cyber security and data will grow.

7.

The borders of cyber espionage and crime are becoming even more blurred

The tools and methods used in cyber espionage and criminals resemble each other more and more, and cyber crime becoming professional leads to more advanced and financially motivated cyber attacks. At the same time, it is also true that authoritarian countries use different kinds of actors as intermediaries in order to reach their goals, which makes it more difficult to identify the motives of the perpetrator and the attacks.

8.

Not even cars are safe from cyber attacks

New cars are even smarter than their predecessors, and one car may have dozens of different kinds of software. You must ensure that the software of cars is up to date in the same way as any other software. Will this mean that we will see the first malware attack against cars in 2022?

9.

Artificial intelligence helps with data breaches

Artificial intelligence is being deployed in companies at an accelerating rate, and criminals are also keeping up with the times. Artificial intelligence and machine learning can be used to create even more believable deep fake videos or take advantage of bots for targeted phishing. In fact, in 2022 artificial intelligence may be behind a CEO scam to help with getting inside the organisation, for example.

10.

Major changes in the use of ransomware

Even though many organisations have understood the importance of backup copies and the authorities are also chasing the criminals behind malware, ransomware are by no means a forgotten threat. In the future, problems will be caused by data leaks or the disruption of operative functions, especially in OT networks, instead of encrypting the data.

Cyber insurance is becoming increasingly more popular globally, which may also create new incentives and ways of getting money for cyber criminals when the ransom is paid by the insurance company. The instructions of the National Cyber Security Centre Finland remain the same: do not pay the criminals.

Cyber weather in 2021

⚠ Alert 🩹 Vulnerability

Vastaamo **patient data is shared** online again		Jan
Scam text messages about OmaPosti torment Finns every day		Feb
A critical vulnerability in the Exchange email server is exploited actively	⚠	Mar
The Pulse Connect Secure remote access vulnerability is exploited internationally in espionage cases	🩹	Apr
The Cybersecurity Label sparks interests in an international smart device information security webinar		May
Measures for improving cyber security in society are defined in **the Cyber Security Development Programme**		Jun
A vulnerability in the **Windows** Print Spooler service caused long-term problems for organisations	🩹	Jul
A phishing campaign spreading in Instagram succeeded in hijacking many user accounts		Aug
A vulnerability allowing commands to be carried out with permission from OMI was found in the OMI component of **the Azure cloud service**	🩹	Sep
We issued notifications about information security incidents for the first time in the **112 Suomi application**.		Oct
We published the first **report on artificial intelligence** in Finland		Nov
A critical vulnerability in the Log4j component required immediate attention to secure operations	⚠	Dec

Do you or your organisation need help with preventing information security violations, or do you have any questions about the regulations related to cyber security? We also evaluate and approve information systems.

We develop and supervise the reliability and security of communications networks and services. You can reach us as follows:

by email: kyberturvallisuuskeskus@traficom.fi
customer service: +358 295 345 630

Follow us and our news
kyberturvallisuuskeskus.fi
@CERTFI
facebook.com/NCSC.FI

Report an information security violation to us
kyberturvallisuuskeskus.fi/en/report

Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland

PO Box 320, FI-00059 TRAFICOM
tel. +358 29 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-777-8
ISSN 2669-8757

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre