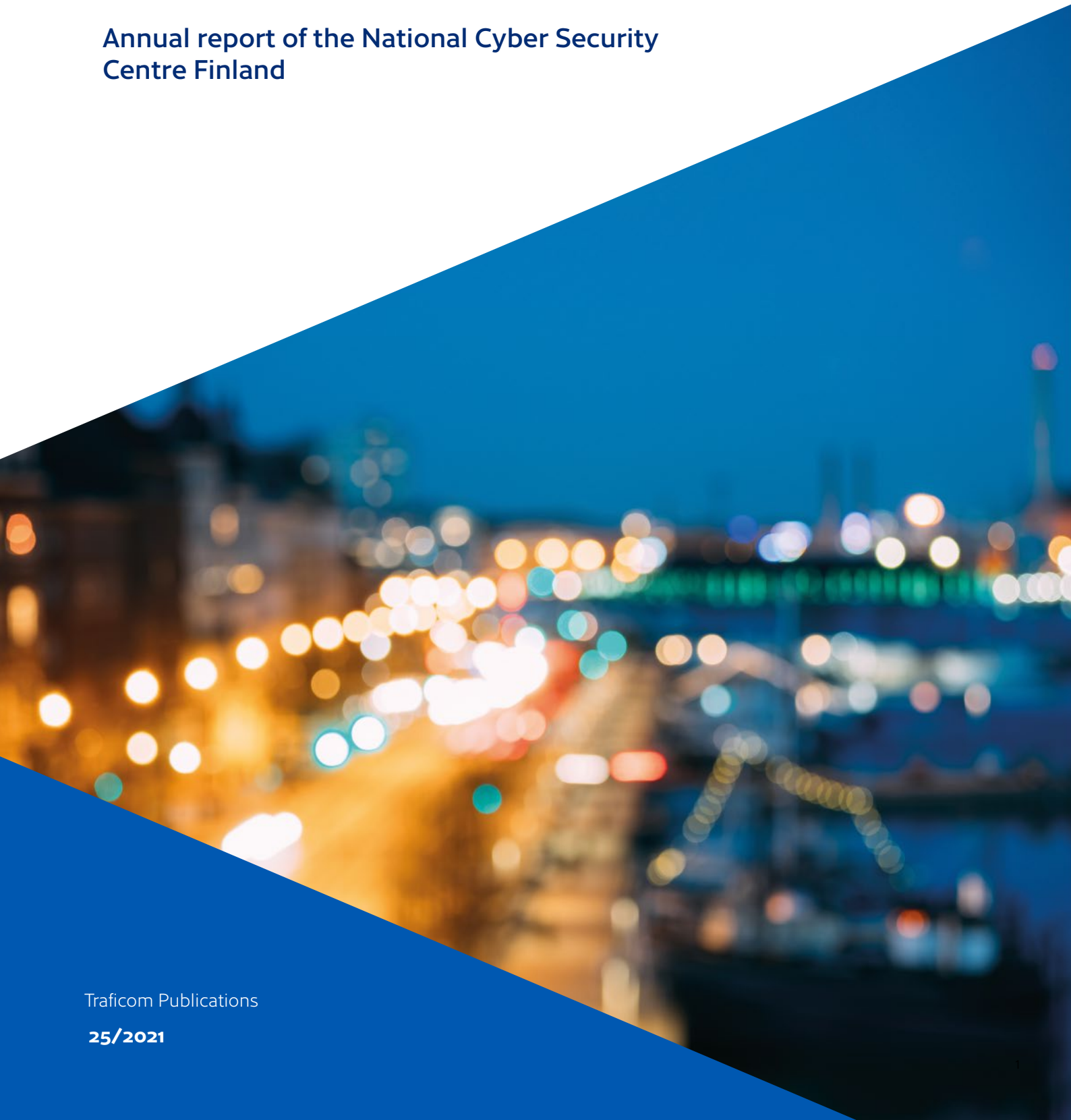
Finnish Transport and Communications Agency
National Cyber Security Centre

Information security in 2020

Annual report of the National Cyber Security Centre Finland



Traficom Publications
25/2021

Contents

Cybersecurity became a permanent item on the management's agenda

The safety of mobile networks, especially 5G, was one of the hottest discussion topics around the world. Instructions on measures to minimise the cybersecurity risks of 5G networks were drawn up in the EU post-haste. New legislation was prepared in Finland to protect the critical parts of communications networks. The national perspective is in a more prominent position than before in the new legislation and additionally, provides new tools for addressing potential cybersecurity risks that threaten national security and defence.

In the past year, we faced the worst data breach in Finland so far when the patient records of the psychotherapy centre Vastaamo ended up in the hands of criminals. Using the stolen data, the attacker blackmailed both Vastaamo, as well as tens of thousands of citizens who had used its services. We helped the victims by means such as collecting instructions on the website tietovuotoapu.fi together with authorities, organisations and companies. The case of Vastaamo sparked discussion in society on the responsibility of corporate management to protect critical information pools and systems. It also served as a reminder that a personal identity code is not a suitable identification method in online services.

The year was also marked by the Emotet malware; we published a warning about it in August. The purpose of the malware is to steal data from organisations. The attack makes it possible to penetrate deep into the target's network and start a ransomware attack, for example. Emotet is a good example of a professionally implemented data breach that is used to gain a foothold and create a backdoor in the targeted organisation.

At the start of the year, the global pandemic sent us to work remotely in unprecedented numbers. This also meant that the use of vulnerabilities of remote work solutions in data breaches, for example, clearly increased. In addition, international cyber trends entered the Finnish telecommunications networks in February, when a wave of scam calls swept over our country. During February alone, Finnish telecommunications operators reported millions of scam calls.

The difficult year still had some good news, too. Jouko Katainen (Ilmarinen), Jussi Törhönen (Enfo), Tomi Vehkasalo (Aditro), Jani Raty (Aditro) received the 'Tietoturvan suunnannäyttäjä' (Information security trendsetter) award for their active cooperation with the National Cyber Security Centre Finland. We were also involved in creating the Koronavilkku coronavirus contact tracing application. It seems that its information security and data protection solutions were chosen well. Now millions of Finns use the application and support the management of the coronavirus situation in our country.

The exceptional year showed that work and business can be safely moved online. We also saw that by cooperating with the authorities and NGOs, we can help with human crises caused by cybercrime. The severity and impacts of the events brought cybersecurity to the management's agenda as a permanent item.

In 2021, we celebrate the 20th anniversary of our CERT activities. These decades have held many surprises.

Make sure you follow our website and social media channels! If you are interested in cyber forecasts for 2021, you can find them at the end of our report.

Helsinki, 11 February 2021

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

Cyber weather phenomena

Network functionality

Disturbances in communications networks

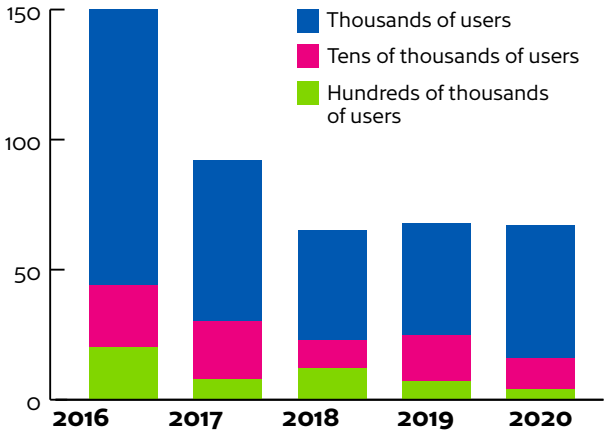
It is important to ensure that Finnish communications networks operate as reliably and free from disturbances as possible. Otherwise, the digital services of our society, for instance, cannot function. Based on the disturbance data we collect, we can analyse the root causes of disturbances and improve the reliability of networks by developing regulations, among other things.

The number of significant disturbances decreased clearly until 2018, and it has remained between 65 and 68 ever since. There were 67 significant disturbances in 2020. The number of critical disturbances that apply to at least 100,000 users decreased, however. As a whole, the trend can be considered positive, even if the decrease in the number of significant disturbances has stopped.

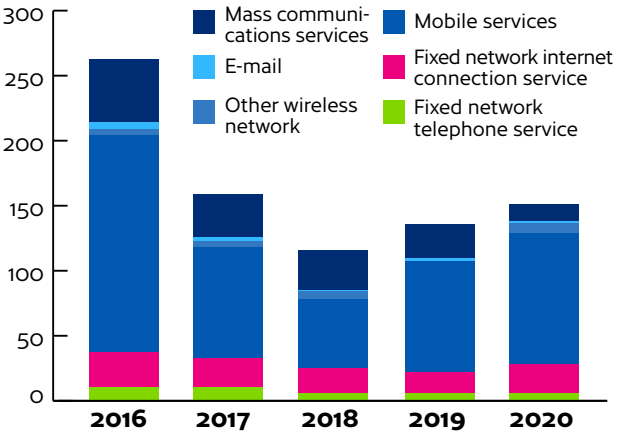
The majority of significant disturbances in Finnish communications networks involve mobile network services, i.e. the functioning of calls, internet connections and SMS. They are caused by factors such as power cuts due to storms that also affect the power supply of mobile network base stations. The mobile network is also technically more complex than the fixed broadband network, for example, which is why disturbances due to software errors, among other things, are more common in the mobile network.

The number of software and power supply system failures has increased since 2019. Careful testing of systems may reduce disturbances. Still, the quality of hardware and software components should also be monitored because unreliable components may not be found in the testing.

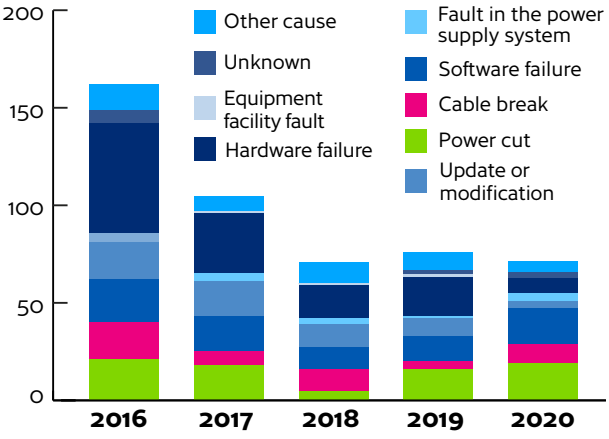
As for updates and modifications, they caused fewer disturbances than before. This is good news and shows that telecommunications operators have worked systematically to develop the maintenance of their services.



Number of significant disturbances of the functioning of communications services in 2016–2020.



Effects of significant disturbances on general communications services in 2016–2020. One disturbance may affect several services.

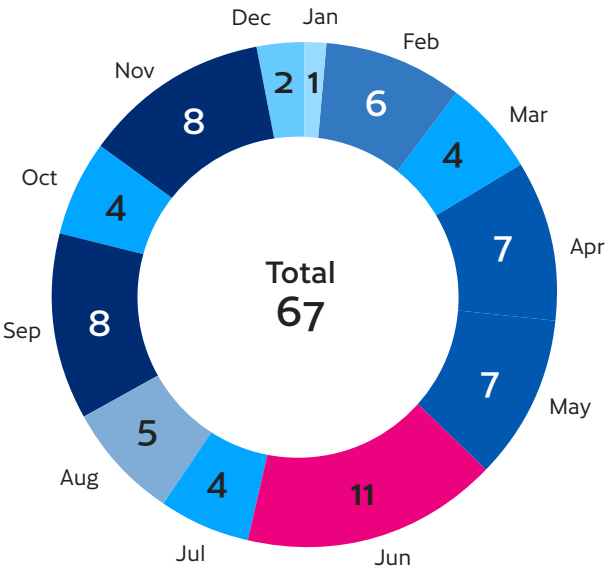


Root causes of significant disturbances in 2016–2020. One disturbance may have several root causes.

Internet connections were breaking up all around Finland and storms caused power failures

The nationwide disruption of the internet connection service in Telia's mobile network on 25 April also attracted the media's interest.

Storms also caused significant incidents. In particular, Päivö on 30 June and Aila from 16 to 17 September caused communication service disruptions. Telecommunications operators, power grid companies and rescue departments managed the disruptions with established routines. The effects of the disturbances remained comparably small compared to the storms a few years before.



Distribution of significant disturbances over the calendar months.

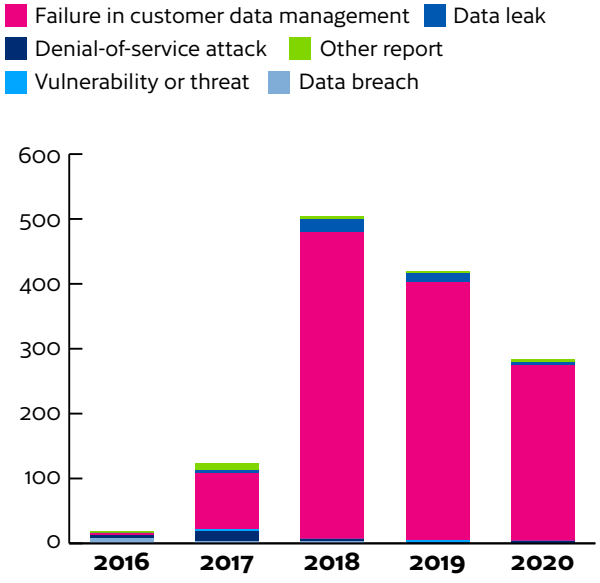
Remote tools caused concern

The public communications services in Finland and the rest of Europe worked well, even though a large number of people started working remotely as the coronavirus pandemic spread.

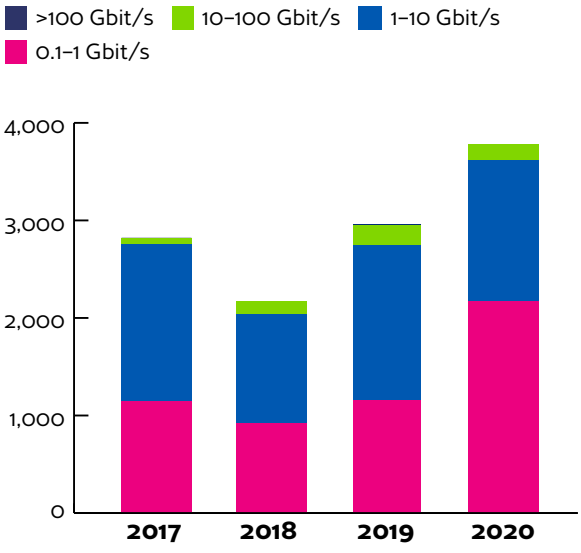
In the early stages of the pandemic, the organisations' own VPN services and international cloud services, among other things, had capacity issues. They were resolved mainly in a matter of weeks. In March, the use of cloud services multiplied globally. In many organisations, the deployment of remote work tools and services was not fully controlled, which could lead to uncontrolled security risks.

We gave advice on using the split tunnel method, among others. For example, the method can be used to steer the software update traffic past VPN, which reduces the load on the organisation's VPN service.

The errors and memory lapses in the processing of online service certificates caused widespread

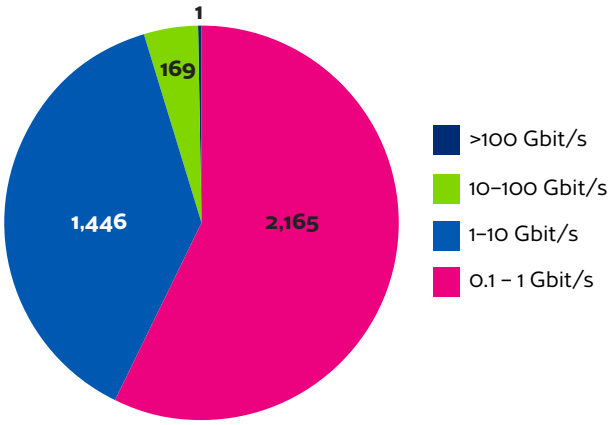


Reports by telecommunications operators on significant information security violations and personal data breaches in 2016–2020.



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

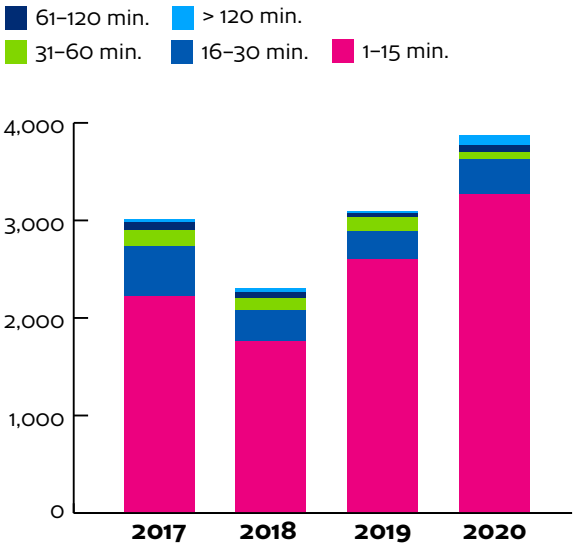
disruptions in the usability of many services. Several of the certificates of Microsoft Teams expired in February. Fortunately, the situation was under control again before the pandemic, because the disturbance struck hard in Western countries where the Teams service is popular. In early March Let's Encrypt had to invalidate in a short notice certificates it had issued. DigiCert had to do the same in July, because it had made mistakes in the processing of certificate requests. It is important that organisations have clear, fast processes for renewing the certificates of their online services.



Distribution of denial-of-service attack volumes in Finland in 2020. Source: Telia

The number of reports of information security violations by tele-communications operators is still decreasing

The reports by telecommunications operators on information security violations have steadily de-creased after the peak in 2018. In a typical personal data breach, a telecommunications operator has registered the wrong address for a customer and sends a letter or e-mail message containing the customer's personal data there. Typically, there are fewer than ten significant information security violations per year. In 2020, five were reported.



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

Denial-of-service attacks

Finnish organisations are increasingly better pre-pared against denial-of-service (DoS) attacks every year. The mitigation services offered by operators and the organisations' expertise have developed and become more widely available, so that the most common DoS attacks can no longer affect the operation of companies very much. Services turning into cloud services have also improved preparedness against DoS attacks.

In exceptional circumstances, the availability of online services is highlighted

In international news, we have read about major DoS attacks that have affected the internet infra-structure services, among other things. Increasingly better precautions have been taken against attacks every year, but an attack with a large volume that lasts a long time may still have an extensive impact on a company's operations.

In the spring, remote work saw unprecedented growth in Finland, too. In some incidents, DoS attacks have had an indirect impact on an organi-sation's internal services such as Skype and VPN solutions, for example. Services critical to remote work should be designed and implemented so that DoS attacks would affect them as little as possible.

In 2020, attacks against systems at schools were also detected. Young people who do not understand the severity of a DoS attack may have been behind the attacks. A DoS attack, or an attempted attack, may be interpreted as a criminal offence for which the perpetrator can be sentenced to a fine or at most two years of imprisonment.

We usually receive reports of DoS attacks with a volume of less than 10 Gbit/s. The volume of the largest attack reported to us last year was 161 Gbit/s.

In the autumn, European operators were targeted by DoS attacks. The attackers targeted various internet infrastructure services, DNS servers in particular. The attacks were reported to have reached up to 300 Gbit/s in volume and lasted for several hours.

Last year, DoS attacks on digital services also occurred in Europe. According to service providers, the DoS attacks they detected were larger than ever before.

Companies were blackmailed with denial-of-service attacks in Finland too

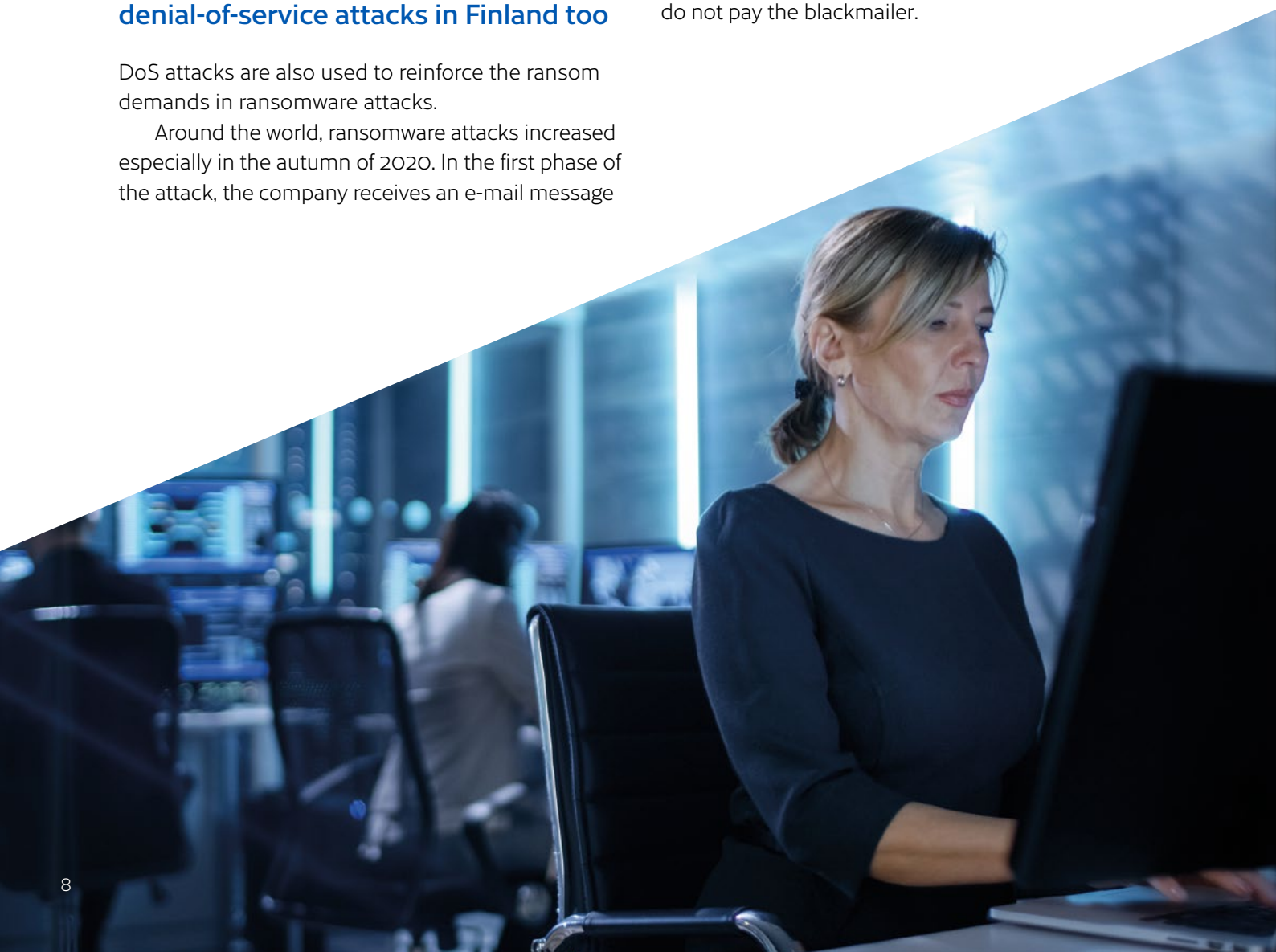
DoS attacks are also used to reinforce the ransom demands in ransomware attacks.

Around the world, ransomware attacks increased especially in the autumn of 2020. In the first phase of the attack, the company receives an e-mail message in which the recipient is blackmailed to pay, typically with BitCoin, so that the attack will not be carried out. The blackmail message is usually sent in the name of a criminal group known in the field or an individual actor. Often the criminals also underline their threatening message with brief but powerful DoS attacks that are used to try to force the target to pay the money to avoid a larger-scale attack.

We know of incidents in which the target has been threatened with an attack amounting to as much as 2 Tb/s. Usually the blackmail messages have been groundless, but the attacker may have carried out smaller DoS attacks.

Finnish organisations have also reported to us about blackmail messages they have received. As far as we know, no threatened large attacks have been carried out, however. The sum of money demanded was fairly small and the senders of blackmail messages varied. The blackmailed organisations had no connecting factors. The attackers seem to have chosen the targets randomly to gain money.

Our old instructions have not changed: do not pay the blackmailer.



Espionage and influencing

In 2020, the focus of cyber espionage appeared to be outside Finland, but Finnish organisations were also regularly targeted by attempted breaches. The biggest news about successful incidents of cyber espionage in the Western countries have focused on the large EU countries, as well as the United States and its allies.

Last year, Norway and the EU also took a more visible stand concerning the backing of cyberattacks, and the EU, for instance, imposed sanctions related to them.

The pandemic was also reflected on cyber espionage

At the start of the year, vulnerabilities were discovered in solutions used to protect information networks and establish secure connections. These vulnerabilities may also have been used in cyberattacks by state actors. The concerns at the turn of the year were related to certain vulnerabilities discovered in Citrix products in particular. During the year, similar vulnerabilities were also found in the products of several other manufacturers related to information networks and their protection.

The following themes in particular emerged as interesting perspectives in connection with the virus pandemic in the spring:

1. Taking advantage of the desire for knowledge and various fears related to the coronavirus in targeted phishing messages or the distribution of malware.

2. Cyber espionage related to the coronavirus, its treatment and vaccine research.

We informed organisations about potential threats directly via our own contacts, cooperation networks and partners.

> ”Even though cyber espionage focused outside Finland, Finnish organisations were also targeted by attempted breaches.

Several major data breaches at the end of the year

The autumn was busy with cyber espionage incidents. For example, the European Medicines Agency (EMA) stated that it had become a victim of a data breach right before a coronavirus vaccine was supposed to receive the Agency's approval. Already earlier in the autumn, Norway had brought up a data breach targeting its parliament, the Storting; according to the country's public estimates, it considered APT28, linked with Russian military intelligence (GU, previously GRU), to be behind the attack.

As for the Parliament of Finland, it reported a cyber attack against itself at the end of December; the National Bureau of Investigation is investigating it as a suspected aggravated data breach and espionage. The Parliament has stated that a few e-mail accounts – including those of Members of Parliament – were compromised in the attack in autumn.

At the end of the year, threats related to subcontracting and delivery chains became reality again when a data breach targeting several American departments and organisations was revealed. The data breach was related to SolarWinds IT monitoring and management products. The attacker had managed to slip its own code into an update distributed to customers. This gave the attacker a way to access all organisations that had installed the update containing malicious code at any time. Such organisations were also found in Finland. As far as is currently known, the attacker only used the opportunity to access a small number of targets it had selected outside Finland.

Traditional methods are still in use

The traditional attack methods, such as brute force password cracking and targeted phishing, are still a part of the cyber espionage toolkit. For example, plenty of password cracking attempts were detected during the year.

National cyber threats related to the functioning of critical industrial production, logistics and energy supply were also present in the Middle East in particular.

Precautions against cyber espionage must be improved further

Even though the detection ability and preparedness of organisations continued to improve, there are still deficiencies in issues such as comprehensiveness of gathering logs as well as their management and analysis. This weakens the ability of Finnish organisations to investigate data breaches or attempted data breaches focused on them. A major share of data breaches can still be solved only partially. Often the investigation cannot reach a definite answer about the course of events and their consequences that would satisfy all parties.

Cyber espionage does not involve just the public administration or political organisations; instead, it can also be targeted at companies as industrial espionage, for example. Targeted cyberattacks commissioned by the customer from a skilled actor should also be taken into account in the preparations. Commissioned attacks also make it more difficult to prepare for attacks and identify the perpetrators.

Malware and vulnerabilities

In the past year, we saw vulnerabilities and waves of malware distribution that required a fast response. Significant vulnerabilities were also found in remote work solutions that had to be updated or at least taken into account in different implementations without delay.

Assess remote work solutions from the perspective of information security

In April, we found several RDP services that were open to the internet. We notified the administrators about the findings and recommended suitable further measures. Vulnerabilities discovered in remote work solutions were used in data breaches, malware distribution and ransomware.

In general, last year offered attackers several opportunities to penetrate organisations' network environments. Information security vulnerabilities in the remote work solutions and file sharing services that had become increasingly popular also offered avenues.

The so-called attack surface in online attacks is significantly increased by the services visible towards the public network or available to the attacker, as well as their weaknesses. Protecting services, restricting their visibility and decommissioning unnecessary services reduces the methods the attacker can use to penetrate the network.

> ”Protecting services, restricting their visibility and decommissioning unnecessary services reduces the methods the attacker can use to penetrate the network.

Once the attacker has reached the intranet, they can guess passwords and take advantage of other vulnerabilities that have not been patched with updates. Remote work solutions must not endanger the information security of any organisation. Exceptional solutions, if they are used, should be removed when returning to normal conditions. If the solutions are not documented, their careful removal is not possible.

Updates can prevent major damage

When a vulnerability is revealed, it is scanned actively immediately after publication. If installing updates is delayed, it must be made certain that an attacker has not already managed to take advantage of the vulnerability.

Before purchasing a new device, you should always check whether updates will be available for its software in the future, too. If updates end, operating systems become more vulnerable to data breaches than before. In Finland too, several old Windows versions are still in use despite the fact that updates are no longer available even in the case of a critical vulnerability.

Emotet spread and ransomware became more common

In August, we issued a warning about a malware program called Emotet that was actively spreading in Finland. Emotet spread by means such as macros and harmful links in attachments. Attempts were made to distribute it through scam messages sent as a continuation of existing e-mail chains. Links and files, as well as forged sender information in e-mail messages play an important role in malware infections. In fact, organisations should pay attention to processing forged sender information in their own e-mail messages.

Precautions against the threat of ransomware should be taken in Finland too, because attacks have become more common and they may be targeted at organisations of all sizes. Ransomware typically activates on weekends or at times when there are fewer employees present. Companies have become less willing or able to pay, which is why criminals are developing new ways to use and sell the information gained. A trend where criminals stole information from the victim and threatened to publish it if the ransom was not paid, in addition to encrypting the data, became more common last year.

> ”Precautions against the threat of ransomware should be taken in Finland too, because they have become more common and may be targeted at organisations of all sizes.

Our assessment of the most significant vulnerabilities in 2020

1. **VPN:** many different vulnerabilities and several manufacturers – all had problems.
2. **Zerologon:** protocol vulnerability that was exploited actively.
3. **SMBGhost/SMBleed:** critical protocol vulnerabilities.
4. **Oracle WebLogic:** actively exploited vulnerability allows access to the server.
5. **TCP/IP Treck / Ripple:** affects hundreds of millions of devices globally.

All of the vulnerabilities have been exploited in data breaches and they have been used in several services, open to exploitation via a remote connection and visible to the public network.

Data breaches and data leaks

Reports of data breaches and data leaks, as well as their attempts increased. No data breaches like the ones targeting the municipal sector in 2019 were discovered, but a data breach of the Finnish Parliament gained public attention in December.

In October, the blackmail of the psychotherapy centre Vastaamo with the threat of a data leak was reported extensively in the news. This was the first known large-scale data breach in Finland. The attacker eventually carried out the threat partially and leaked extremely sensitive material.

Office 365 data breaches and their attempts also continued in 2020. It seems that the number of incidents is not decreasing significantly.

Technical support scam calls became more common in January. They also resulted in data breaches, because the callers told the victims to install remote control software that gave the criminals access to the information on the computer. In March, the calls stopped momentarily when international restrictions on gatherings, due to the pandemic, entered into force.

Your own detection abilities protect you from criminals

Criminals are constantly mapping new attack opportunities, which is why organisations' own detection abilities play an important role in protection against attacks. The ability to detect events that deviate from normal, such as logins at an unusual time or from an unusual place, plays a key role. Attention must also be paid to the quality, amount and sufficiently long storage periods of logs, because events cannot be investigated without high-quality log data.

Data breaches are often also revealed through reports of malware and phishing messages, which is why all information security violation reports are important for building situation awareness.

CASE VASTAAMO

The data breach of the psychotherapy centre Vastaamo was the largest information security violation case in Finland in the past year. The data breach was followed by blackmail messages in which, both Vastaamo and its patients were issued demands to pay a ransom if they wanted to prevent their patient records from being leaked to the internet, where they would be publicly available.

More than 25,000 reports of an offence related to the case have been recorded by the police. Many other organisations and authorities have also participated in helping and supporting the victims of the data breach.

The National Cyber Security Centre supported Vastaamo during the first stages of processing the case. We also assisted the police and the information security company investigating the matter with the technical investigation.

The lessons learned were obvious: you must know your own services and monitor and assess them. If your own resources or expertise are not sufficient, you must ask for help from a professional in the field. Scanning the online services and testing your systems in a cyber exercise are a minor investment compared to a serious data breach.

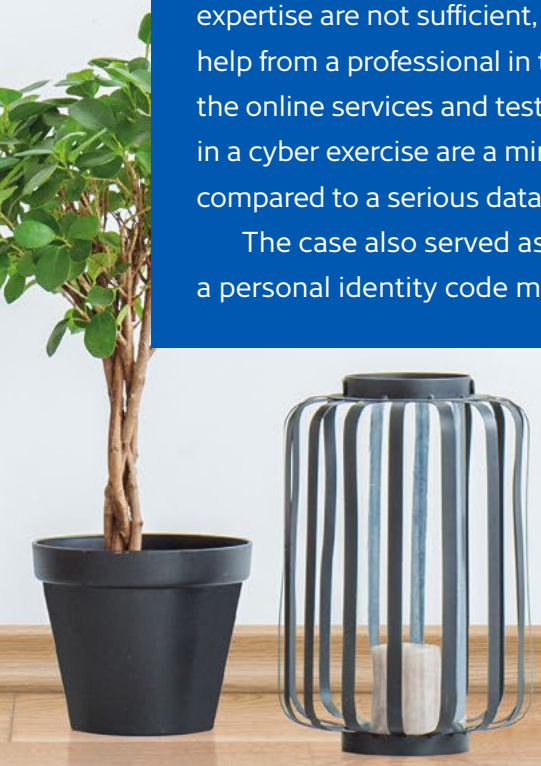
The case also served as a reminder that a personal identity code must not be used to identify the customer in online services. Strong electronic authentication is a safer method.

Versatile and altruistic cooperation offers help quickly

The Vastaamo data breach took a new turn on Saturday night 24 October, when the criminal started to blackmail Vastaamo's customers by threatening to publish their confidential information.

At the National Cyber Security Centre, we got to work on Saturday night. On Sunday, we met with several different authorities, organisations and volunteers to compile instructions for the victims of blackmail. As a result of the work, we published the tietovuotoapu.fi website for those who needed help on Monday 26 October. On the website, we provided a wide range of instructions produced by various parties in addition to contact information that the victims could use to find discussion help.

The tietovuotoapu.fi website showed how well, easily and, if necessary, quickly different organisations can cooperate in Finland. It was amazing to be there to witness how everyone wanted to work for the common good regardless of the limits of their own field or responsibilities. It will be easy to build an even safer society of the future on such trust and ability to cooperate.



> ”The data breach of the psychotherapy centre Vastaamo was the largest information security violation case in Finland in 2020.

Phishing and scams

Phone scams cast shadows over the unusual year

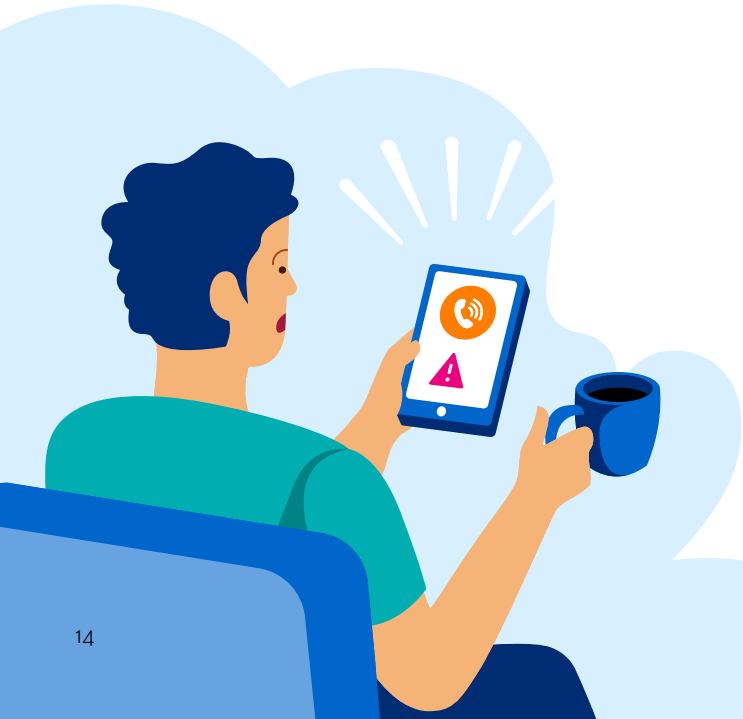
In February, scammers showed that they really had found the Finnish telecommunications network. Prior to that, telephone scams had been rare in Finland.

During February alone, Finnish telecommunications operators reported one million technical support scam calls received. One-ring scams also amounted to one million calls.

In a technical support scam, the scammer calls and tells the target that their computer has a problem. The scammer may claim that the problem is due to malware, a hacker or a "network blockage," for example. In a one-ring scam, the target's phone rings once or twice so that answering the call is completely impossible. The call comes from a number with a foreign area code – Samoa, Papua New Guinea, Tunisia – or a satellite telephone service. Calling the number back may cost as much as 10 euros per minute.

Scam calls have caused much trouble and significant losses to Finns. Our cooperation with Finnish telecommunications operators has helped however, and the number of scam calls to Finland from abroad has been cut down to a minimum. After July, we have received only a handful of reports about the calls.

Getting rid of technical support scams is more difficult because the scammers use false telephone numbers. The calls seem like they are coming from telephone numbers in Finland, the United Kingdom or Sweden, while in reality they come from a call centre where dozens of employees make scam calls to different countries on an assembly line.



Considerable financial losses due to invoicing fraud

Invoicing fraud caused considerable financial losses to organisations again. Among other things, an international group of criminals posed as law offices and the Finnish Financial Supervisory Authority in order to be able to access capital transfers in major business acquisitions.

The most common method of invoicing fraud is to pose as the leader of an organisation and send messages to the organisation's financial staff in the leader's name. The one-time profit obtained by criminal means may reach up to hundreds of thousands of euros. Invoicing fraud is often noticed only several weeks after the damage was done, which makes returning the money much more difficult.

Scam links in SMS caused trouble again

SMS links often lead to subscription scams, malware or other fraud. Scammers used this method liberally. The address of a scam link is not necessarily visible on a smartphone screen, which is why the recipient does not suspect that it is a scam.

Scam messages were sent especially in the name of the Finnish postal service Posti and various courier services. Their purpose was to infect Android phones with malware and direct Apple users to phishing sites. You must not allow applications that you are not familiar with to be installed on your phone. If you do allow it, malware that sends thousands of SMS abroad may result in massive costs to the subscription.

Internet of Things and automation systems

Attack against an automated critical infrastructure system

The past year included attacks on automated critical infrastructure systems when attackers targeted Israel's water system. The first strike took place in April, and two new attempts were detected in June. Israel managed to prevent the attack that might have done significant harm to the population.

This is the first known attempt of causing physical harm to citizens with IoT and automation systems. Previous strikes have primarily targeted data and information systems. Iran was suspected to be the attacker. The attack is considered as the first sign of real acceleration of cyberwarfare.

Thousands of devices and systems are still unprotected

The study of vulnerabilities in printers published in September shows that there are still plenty of information security deficiencies in smart devices connected to a network. The study found approximately 500,000 unprotected printers online, 50,000 of which were studied in more detail. Approximately one half of these could be hijacked so that the intruder could print out documents with the device.

In our annual survey of unprotected automated devices, we mapped approximately 1,280 networks and 12.8 million IP addresses in Finnish virtual space. The largest group we detected included various building automation devices, which were found in approximately 800 IP addresses. Roughly 120 industrial automation systems and approximately 30 critical industrial automation systems were found. We discovered approximately 1,000 unprotected automation systems in Finnish networks.

The numbers did not change significantly compared to the surveys of previous years and therefore, the work on the information security of devices and systems must continue and be intensified further. The more devices with information security deficiencies are added to the network, the more the network's usability and information security suffer.

> ”The more devices with information security deficiencies are added to the network, the more the network's usability and information security suffer.

On the internet, an unprotected device is an attractive target for intruders. For example, the device can be harnessed for DoS attacks, or it can offer easy access to the company's network.

A significant change in the IoT world is on the horizon

Information security problems in IoT devices and automation systems have made many people aware of the need for different kinds of information security requirements and certificates.

The Cybersecurity Act of the EU that entered into force in June 2019 specified a certification system for European information security; the certification of IoT devices based on it is also planned in the coming years.

ETSI 303645 Cyber Security for Consumer Internet of Things: Baseline Requirements, the first official information security standard for smart consumer devices, was published in June 2020.

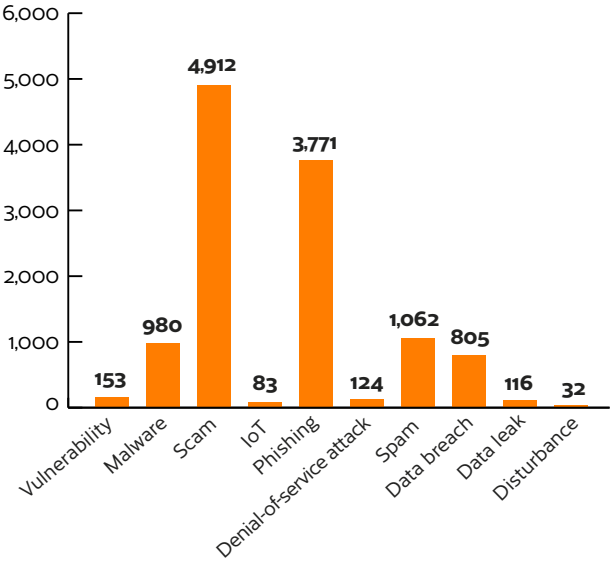
The Commission also noted that the information security of devices connected to a network must be improved by legislative means. The Radio Equipment Directive (RED) of the EU is considered one of those means. Preparations have started for delegated act on the information security of radio equipment under the directive. The regulation will have a major impact on the world of IoT.

Our services

Coordination Centre – first aid for information security violations

The information security experts of our Coordination Centre provide first aid and advice for victims of information security violations. The number of incidents processed by our centre has increased by more than 100% since 2019. The number of incidents at the time was 4,500, but in 2020 the figure was over 10,900.

The number of incidents increased in practically every category we use for classifying information security deviations. We received the largest number of reports about different kinds of scams and phishing.



Number of incidents by type in 2020.

Several reports about the Emotet malware

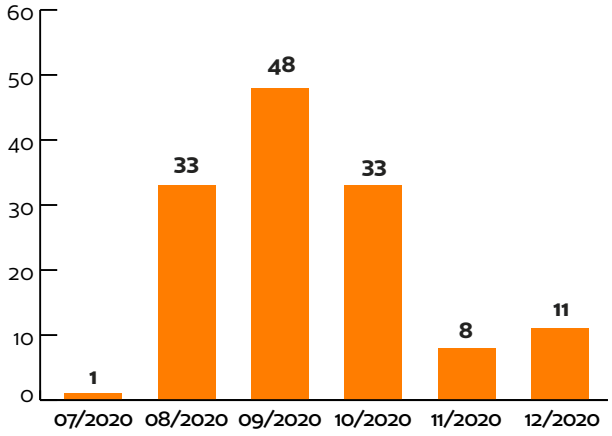
Emotet is a good example of malware used to gain a foothold and create a backdoor in the targeted organisation. It is used by criminals who commit data breaches professionally. We received the first reports of attempts to distribute the Emotet malware in August 2020.

Thanks to the organisations' own information security controls, a significant number of Emotet incidents remained only attempts. Others fared worse. In incidents of infection, our duty officers advised several victimised organisations on how to recover.

We published a yellow warning on the active distribution of the Emotet malware in Finland on 18 August 2020. We removed the warning in November, even though the threat of the malware had not disappeared completely. We received good news in January 2021, when the Emotet bot network was taken down in an international police operation.

When a campaign distributing malware hits Finland, our Coordination Centre gets to work immediately. We uncover the essential details of the campaign. We offer help with protecting yourself from the threat by sharing the malware's identification information in our different channels.

In order to combat malware attacks, organisations should use a variety of protection methods, such as training the personnel and building technical controls.



Number of reports related to the Emotet malware by month.

Identification information – Indicator of Compromise, IOC

- For example, an IP address, domain or URL used by the malware as a command channel.
- Can your organisation search for traffic in logs based on identification information during the past year, for example?

Need for vulnerability coordination has increased

Incidents of vulnerabilities that require coordination between the manufacturers, information security investigators and the product's user groups and its different components are reported to the Coordination Centre weekly. Most of the incidents are fairly simple, and they are related to online services and IoT devices.

Reports related to online services mainly involve implementation errors in individual services and their background systems. In such incidents, the service providers or the subcontractors that created the code can fix the vulnerability themselves. This is why, as far as it is known, no damage has occurred in these incidents that were reported to us. In 2020, we also received more reports than in previous years concerning information security deficiencies and suspicions related to deficiencies.

> Responsible manufacturers usually fix vulnerabilities quickly, and at their best, update open systems without delay. However, the total number of open services at risk does not seem to decrease.

Nearly all of the vulnerabilities reported in IoT devices were elementary implementation-level errors or insecure default settings. In most incidents, an attacker would be able to take control of the device through the vulnerability. The processes to fix vulnerabilities can be slow and difficult.

We discover plenty of services open to the internet that are used to ensure security or control various systems. The need for openness often seems to be debatable. Plenty of different kinds of attacks are targeted at open services, and even a single weakness or wrong setting can expose them to a data breach.

The most severe vulnerabilities last year were related to incidents in which a new vulnerability was found in a service, several of which are found online. For some reason or another, these services were also open to the internet. Responsible manufacturers usually fix vulnerabilities quickly, and at their best, open systems are updated without delay, but the total number of open services at risk does not seem to decrease.

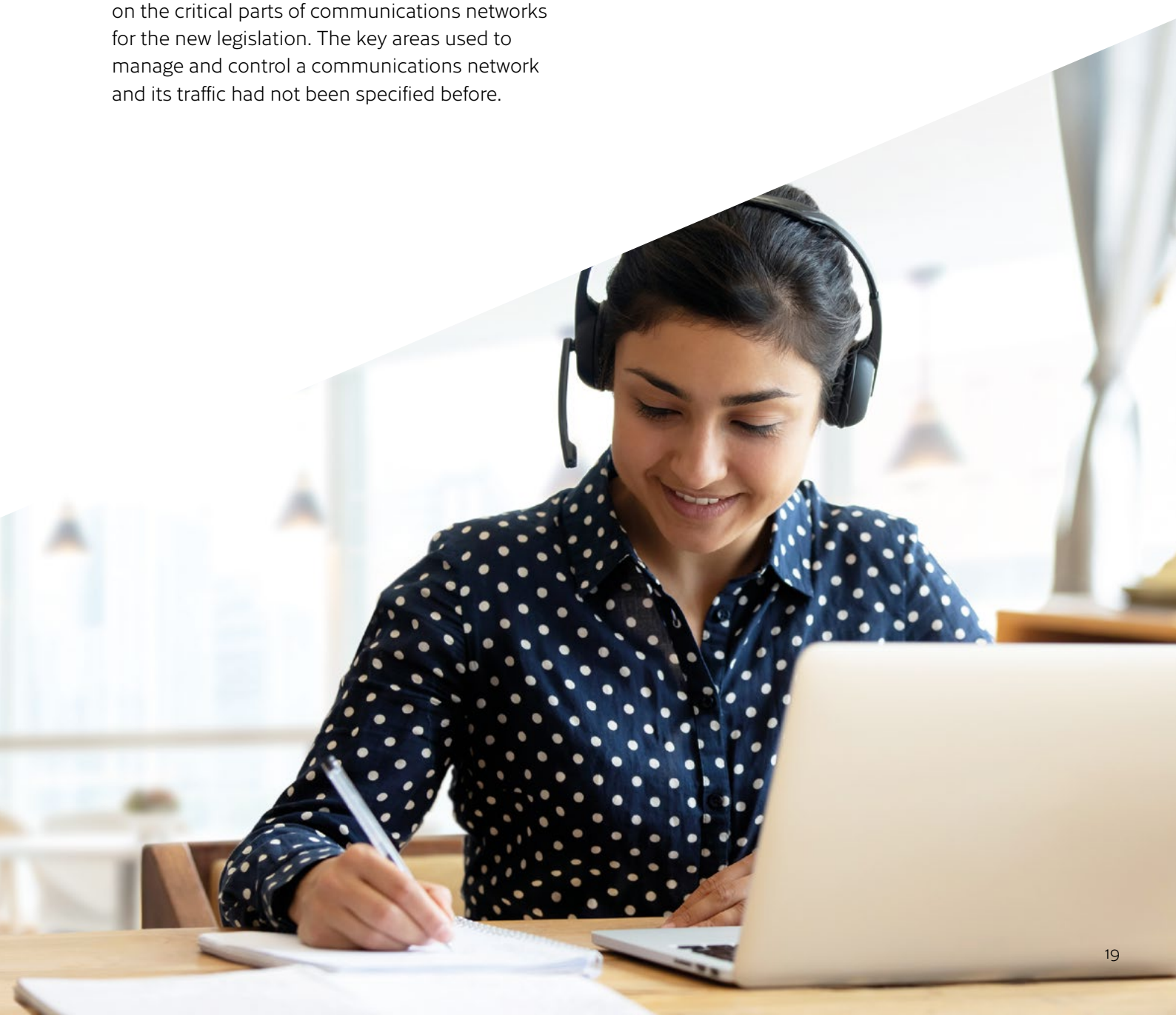
Security regulation

National security goes deeper into communications networks

The security of mobile networks and especially the 5G networks was one of the hottest topics all around the world throughout the year.

In the EU, politically neutral instructions on measures to minimise the cybersecurity risks of 5G networks were drawn up post-haste. As for Finland, new legislation was prepared to protect the critical parts of communications networks. Both were visibly present in our work when drawing up EU-level instructions and preparing a regulation on the critical parts of communications networks for the new legislation. The key areas used to manage and control a communications network and its traffic had not been specified before.

For decades, national security and national defence have been a perspective involved in the regulation of the security of communications networks and services. The national perspective is in a more prominent position than before in the new legislation, and it provides new tools for addressing potential cybersecurity risks that threaten national security and defence.



Location Information Service – the new home of network infrastructures

In October 2022, we Finns will be able to use the Location Information Service (Sijaintitietopalvelu). At that time, anyone doing excavation work will be able to get information about the locations of cables and pipes, as well as telecommunications, electrical and water supply, and sewerage infrastructures. The purpose of the service is to make the work of designers and excavators easier and more efficient. It will also reduce the costs and service outages due to accidents during excavation for telecommunications operators, electricity and water supply and sewerage companies, and those who use their services.

A centralised information point will improve the awareness of network operators about the location of each other's physical network infrastructure and make the cooperation between them easier. According to our regulation (71/2020 M), the information must be submitted to the Location Information Service in a specific format, which will improve and facilitate the usability of the information. The regulation has also made the technical specification of the Location Information Service's functionalities and technical interfaces easier.

There is still a long way to go before the Location Information Service is in production use, but with the cooperation between representatives of different fields, parties representing excavation operators and Suomen Infratieto Oy, we can reach our goal.

The pandemic showed that the eIDAS Regulation of the EU requires reform

In the exceptional situation, the need for remote services, remote meetings and electronic agreements exploded. Therefore, assessing the need for changes in the eIDAS Regulation of the EU was also topical.

Based on the regulation, service providers can gain an EU-level approval for their electronic trust services that are needed in administration and business for the digitalisation of agreements and services, for example. In addition to information security, the agreement also applies to legal validity.

We started a discussion in Finland about the need for changes and collected the experiences gathered in international and domestic work into an assessment memorandum in June.

In Finland, strong electronic identification is a familiar and established service, but electronic signatures and other electronic trust services are used much less. We received quite positive feedback on our observations from the field.

The requirements should be specified and the selection of services should be increased in the reassessment of the eIDAS Regulation. This would ensure uniform regulations in the different Member States and improve the preconditions for supply. In turn, the increased offering of trust services that meets the customers' needs would make it easier to acquire them. For example, there is a lot of uncertainty related to the selection and deployment of electronic signature services of different levels.

The EU Trust Mark is a sign of the EU level approval of the electronic trust service.

Assessments

The Koronavilkku application was assessed in record time

Like last year, the national and international security policy phenomena were reflected in the targets of our assessment. The coronavirus situation also added its own special touch to our assessment activities. The obligations and principles of protection concerning international classified information did not essentially differ from normal conditions. It was also true that for our part, we were able to support the management of the coronavirus situation by assessing the information security of the Koronavilkku application produced by the Finnish Institute for Health and Welfare to support the breaking of infection chains and the application's background system. We also assessed several Finnish encryption products intended for protecting classified information.

Advice on secure video-conferencing solutions and support for the use of cloud services

The increasingly rapid growth of the demand for our advisory services continued. In addition to protecting the traditional processing environments of classified information and critical infrastructure, our support was requested for the selection and deployment of secure videoconferencing solutions in particular. The growth of support needs related to cloud services also continued. The updated version of the Criteria to Assess the Information Security of Cloud Services (PiTuKri) we published in March was adopted eagerly based on the feedback received.

Satellite systems are already visible in the everyday lives of people

Global satellite navigation services are becoming a part of people's everyday lives faster and faster. Satellite positioning is an integral part of everyday services and it is no longer just a tool for navigating from one place to another. The game industry, different kinds of service applications, optimising vehicle mileage, sports and exercise: satellite positioning plays a key role in all of these.

Galileo, the EU-funded global navigation satellite service, has gained a strong position beside GPS during 2020 in nearly all terminal devices that use positioning. The Chinese BeiDou – which was officially commissioned in August 2020 – as well as the Russian GLONASS also contribute to the improvement of positioning accuracy and reliability.

The more satellites the user device can receive, the better the positioning accuracy. Galileo is the most accurate of these global systems, and it is also the only system to offer a dual band reception option for consumer-level receivers.

Galileo and EGNOS on a development path

The Galileo reached a new stage in February: the Search and Rescue (SAR) emergency message service was deployed in full. Galileo's SAR service is the first system in the world to offer the sender of the emergency message an automatic acknowledgement of the message being received. The development of the other Galileo services also progressed nearly as planned, even though the coronavirus slightly delayed the schedules.

Satellite services of the National Cyber Security Centre

Our satellite service has had discussions with GNSS users and especially highlighted the benefits that can be gained from the Galileo and EGNOS services in the future. We are in a constant dialogue with Finnish business life so that the companies in the field can prepare for future market changes. The European GNSS Agency (GSA) has also been included in the discussions.

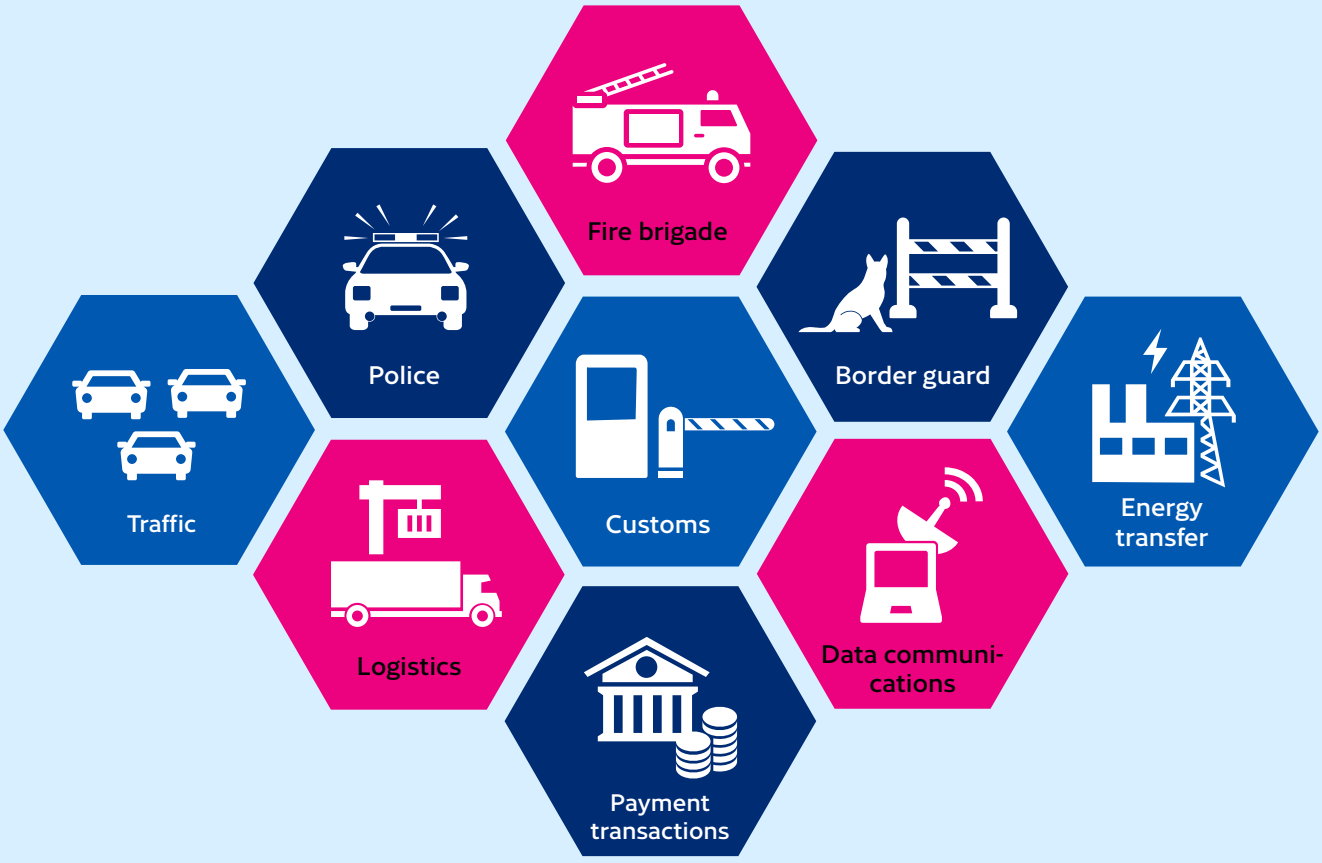
The programme to prepare for the deployment of Galileo's most security critical part, the Public Regulated Service (PRS), was drawn up in 2020. The end result was a PRS implementation plan approved by all branches of government that forms the basis for both the project's funding solutions as well as the operative planning of the service. In November 2020, the Government's Ministerial Committee on Economic Policy stated that the PRS will be deployed in Finland in 2024, and the construction of the national infrastructure required by the service will start in 2021. The construction will start with design and the related specification of technical architecture during 2021.

Your mobile phone is not alone!

See all Galileo-capable devices.

www.useGalileo.eu

Galileo helps society stay functional!



kyberturvallisuuskeskus.fi/en/our-activities/satellite-navigation

Cooperation and sharing information

The situational awareness and information exchange of ISAC information sharing groups is better than ever

The members of our ISAC (Information Sharing and Analysis Centre) information sharing groups form a national network with close to 300 members; its core task is to share field-specific information and experiences related to cybersecurity and cyber threats.

The operation of trust networks has become established and expanded every year, 2020 included. The functioning of the ISAC for logistics and transport in particular settled into its groove, and new member organisations joined the network.

The ISACs' situational awareness related to cybersecurity that has developed since previous years and their information exchange also gave us better opportunities to observe field-specific special characteristics of cybersecurity and take them into account.

The information received from the groups plays an important role in creating a national cybersecurity situation picture. In addition, the groups play an important role in managing disturbances and promoting cybersecurity in different sectors.

ISAC, i.e. Information Sharing and Analysis Centre. The groups are cybersecurity cooperation bodies established in different fields and based on trust.

ISACs of the National Cyber Security Centre Finland:

- Central government
- Finance
- Water management
- Internet service providers (ISP)
- Social welfare and healthcare
- Energy
- Chemical and forest industry
- Food supply, sale and distribution
- Media
- Logistics and transport

Remote work solutions, cloud services and the Act on Information Management in Public Administration on the table

In the ISACs, too, the functioning and safety of remote work solutions and monitoring solutions for remote environments were discussed often. In addition, the discussion topics included the information security of videoconferencing solutions, use of cloud services while maintaining information security, and ensuring the compliance of the organisation's operations and information systems with the Act on Information Management in Public Administration.

In cooperation with the groups, we develop training activities related to the management of disturbances, among other things. A pilot exercise of the ISAC for internet service providers (ISP-ISAC) was carried out last year. In 2021, the training activities of the trust networks that we support will be expanded. You can read more about the training activities on page 28.

The year's successes

Many Finnish and international information security communities turned several of their traditional information security conferences into virtual events.

Inexpensive virtual events offered the information security officers of small Finnish companies in particular a unique opportunity to observe the results of topical and high-level information security research. Hopefully, the practice will continue one way or another in the future, too.

Effects of the Network and Information Security Directive and cooperation

The Network and Information Security Directive (NIS) turned four years old. The Directive regulates the information security, risk management and preparedness of service providers that maintain the critical fields of our society and obliges key service providers to report information security incidents. This is the first directive that jointly regulates the cybersecurity of critical fields, and it is currently being reformed. With us, the effects of the NIS Directive have been the most visible in critical fields, in which information security awareness has increased. Nevertheless, there are still deficiencies in expertise and monitoring.

The Directive issued several fields a requirement to report significant information security incidents. The most significant case in 2020 was the Vastaamo data breach in the healthcare sector. The case led to changes in the regulation of information security and measures to improve information security and data protection. In November, the Ministry of Transport and Communications set a cross-administrative working group tasked with mapping the information security of fields that are critical to the functioning of society, as well as the needs to change the legislation on data protection.

Legal texts alone will not raise the level of information security

No legislation alone can improve the information security of networks or information systems. Companies must include processes and measures that improve risk management and information security as a part of their daily business activities. As for the supervisory authorities, they must ensure that the companies' operations and the quality of systems comply with the law. Detailed instructions, recommendations and orders by the authorities help guide operators in the right direction; more of these should be available in Finland, too.

The NIS Directive is the first EU-level regulation that aims to raise the level of information security in critical fields all over Europe. This involves long-term work that requires first and foremost commitment from the management, but also active dialogue between the private and public sector, as well as close cooperation between the authorities.

Form for reporting significant network and information system incidents for operators of essential services:

www.kyberturvallisuuskeskus.fi/en/report

The coronavirus crisis electrified the international cybersecurity cooperation

We acted as the Chair of the CSIRT network of the European Union during the period 1 January 2019–31 June 2020. The network intensified its operations and monitored the effects of the coronavirus situation on cybersecurity during 18 March – 6 May.

The most important observations were related to the information security of remote work arrangements, the sufficiency of remote connection capacity and the use of the coronavirus as a theme in phishing and malware campaigns. Hospitals and research centres were clear targets of special attention. After a more intense operating period, the international situation involving the cybersecurity impacts of the pandemic has been monitored through normal cooperation.

The coronavirus has been visible in all activities of our international cooperation networks. The operations in general have become more intensive and systematic.

Many international communities have not wanted to ease up the minimum protections of classified information, even though this operating method has slowed down the cooperation to a degree. It is nevertheless also true that the exceptional situation has sped up the design, implementation and accreditation processes of the data processing environments of classified information.

More reliability with training

Exercises are one of the basic services of our centre. We support organisations critical to the security of supply in exercising, participate in national cyber and cooperation exercises and develop tools to support training.

The Emergency Powers Act adopted by the Parliament and the instructions to work remotely changed the cyber exercise activities for 2020. Before, most cyber exercises for continuity management were arranged as in-person events. Due to the coronavirus, service providers and organisations interested in exercising had to develop new training models in a short period of time that took issues such as remote work and the uncertain future prospects of their business into account.

As part of our continued effort to meet the training needs of organisations critical to the security of supply, we will invest in the scalability of our services. This way, we can meet the increased interest for cyber exercising. Based on our surveys and interviews, the National Cyber Security Centre conducted a preliminary report on the future need for our services; its results will be ready in the spring of 2021.

We asked some of the cyber exercise providers to name their essential insights from 2020:

Martti Setälä, Insta Digital Oy:

”Be bold and leap into the world of remote training, it’s rewarding.

Digipooli network of the Finnish national emergency supply organisation:

”It’s easier to find more players for a remote exercise.

Anu Laitila, Nixu Oyj:

”Include everyone as equally as possible during the exercise and make sure your equipment is up to speed before starting.

Cybersecurity Label

The Cybersecurity Label for smart consumer devices was published in November 2019 with three pilot products. The label is the first of its kind in the world to be granted by an authority, and it sparked international interest from the start.

We granted six new labels. They also included two applications. One of these is the Koronavilkku coronavirus contact tracing application that has been downloaded 2.5 million times, which increased awareness of the Cybersecurity Label. The Cybersecurity Label granted to Signify's Philips Hue smart lighting system also brought international visibility.

Development of the Cybersecurity Label

Our studies show that the credibility of the Cybersecurity Label is based on it being granted by a trustworthy authority. This will also be the case in the future, and the label is also owned by Traficom. As demand increases, it is important to ensure availability, which is why the technical inspections are being outsourced to commercial operators. The first of these started at the end of 2020. Both Finnish and foreign information security companies have been interested in carrying out inspections.

When the Cybersecurity Label was published, its requirements were based on the technical specification of ETSI. The first official IoT standard in the world, based on the ETSI specification, was published in June 2020. The requirements of the Cybersecurity Label were also updated to correspond to the brand new standard. The Cybersecurity Labels granted before the standard was published will be updated in connection with the annual review.

The free Traficom Anycast service will improve the reliability of .fi domains

In 2020, we deployed the Traficom Anycast name service to improve the reliability of .fi domains. We offer it as a secondary name service for .fi domain registrars – free of charge – now and in the future. In our Traficom Anycast webinar in October, we talked about the service and its benefits to domain registrars.

The Traficom Anycast service is based on the anycast network maintained by the Canadian Internet Authority (CIRA), which is considered one of the best services in the world.

The service provides added security and offers a hardware, software and routing package that name services can use to improve their tolerance of distributed denial-of-service attacks, among other things.

The anycast technology is widely used in the root domain name services of the internet as well as the .fi root domain name service, but as a rule, the added security of anycast technology is not used on the name servers specified for .fi domain names.

You can get a .fi domain name from a domain registrar.

If the name service malfunctions, it does not only incapacitate the digital service; in the worst case, it will also stop all goods traffic and service production. For this reason, attention should be paid to the reliability and information security of the name service.

You can find more information about the deployment of the Traficom Anycast service from your own domain registrar or from us at the address **fi-domain-tech@traficom.fi.**

A domain name system, DNS, is an internet system that converts domain names into IP addresses. Thanks to the name service, numerical addresses can be replaced by names that are easier to remember.

The hubs of the anycast network are located in North America, Europe and Asia on the world map.

Safer 5G with lessons learned

In 2019, we participated in organising the first hacker event in the world that was focused on the information security of 5G, the 5G Cyber Security Hackathon. In February 2020, the parties that set the hackathon challenge shared their experiences of the event at the 5G Leading Edge Forum. It became clear that without the hackathon, we would have missed information that can be used to improve the security of 5G products further.

At the end of 2020 – based on the lessons learned at the hackathon – we started to draw up the reference architecture for 5G Standalone networks. Our aim is to describe the best architectural methods and ones related to maintenance processes that can be used to operate the 5G network securely. We want to use the reference architecture to respond to common technical threats that the 5G networks will face.

The results of the work on the reference architecture will be tested in the 2021 5G Cyber Security Hackathon, where hackers can test the methods that have been drawn up in an authentic network environment. The reference architecture will be published as a document that will be freely available for all operators and manufacturers.

KYBER 2020 and the revamped HAVARO service

In 2020, the KYBER 2020 programme of the National Emergency Supply Agency was brought to a successful close. The projects related to the programme, such as training, the Kybermittari cyber security meter and the KYBER-terveys cyber healthcare project, were also finished. In addition, we made progress with the revamped HAVARO service.

In the new service model, commercial service centres (SOC) provide the HAVARO service for their customers in cooperation with us.

We piloted the new service model throughout the year with several service centres and their customers. The commercial deployment of the HAVARO service will take place during 2021.

In 2021, we will start the Cyber Climate Project (Kyberilmastohanke) with the aim of developing our ability to use data and information to create a national cybersecurity situation picture, new services and operating models, and respond to cybersecurity threats and security incidents.

HAVARO

Kybermittari – A new cyber threat management tool for managers

The goal of the Kybermittari tool that we released in October is to improve the ability of organisations and society at large to prevent cyber threats.

Kybermittari gives the organisation a view that shows the various important aspects of cybersecurity with their objectives and maturity levels. Kybermittari displays the level of cyber risk identification, protection, detection, response, and recovery in organisations. The tool also provides information on potential development targets, reference data and a common language for discussing cybersecurity and its development.

In October, the National Emergency Supply Agency also published the results of the 'Kyberturvallisuus eri toimialoilla' (Cybersecurity in different fields) survey. The Finnish-language development version of Kybermittari was used as its basis. The key observation was this: If the management makes a commitment and leads the cyber strategy as a part of the company's overall strategy and risk management, the company will be better prepared for cyberattacks and able to survive them.

If necessary, the corporate management can get valuable information through Kybermittari on how their preparedness for cyber risks compares to the average of their field or other partners who have carried out the measurement. Kybermittari can also be used to visualise the maturity level of one's own supply chain.

The many possibilities of Kybermittari: From confidential information sharing to national cybersecurity

If they wish, organisations can share the assessment results produced with Kybermittari confidentially with our centre. Based on these results, we can draw up anonymised reference and recommendation levels that we can offer to organisations to support the use of Kybermittari and the development of cybersecurity. We can also use this situation awareness with the planning and steering of national measures. In addition, we can use the results confidentially in our statutory duties, thereby improving the situation picture. You can find further information on Kybermittari on our website.

www.Kybermittari.fi

KYBERMITTARI ASSESSMENT PROCESS:

”If the management makes a commitment and leads the cyber strategy as a part of the company’s overall strategy and risk management, the company will be better prepared for cyberattacks and able to survive them.

Our key figures

Based on the figures, we had a hectic, exceptional year. Reported malicious sites and the number of incidents we processed doubled compared to the previous year. Our group of followers on social media grew and people were happy with our situation awareness products.

1
Alerts

24/7/365
Uninterrupted on-call duty

115,000
Autoreporter

13,353
Twitter followers

24
Incidents processed by vulnerability coordination

8,500
Shutdowns of harmful sites

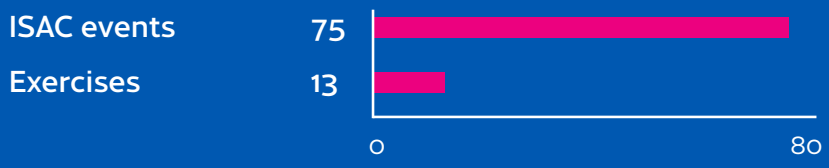
10,892
Incidents processed

6,066
Facebook followers

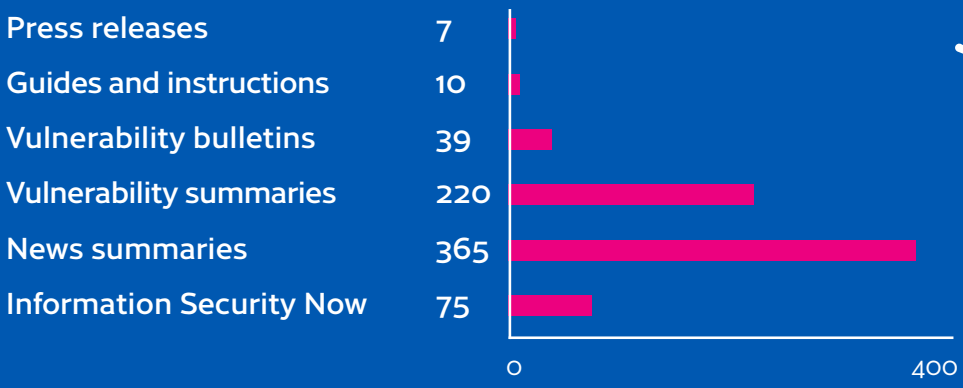
Number of incidents

4	12	51	67
Critical incidents	Serious incidents	Significant incidents	All incidents in total

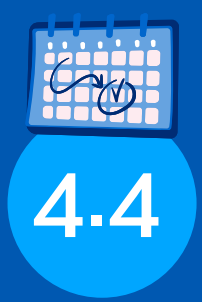
Events and exercises



Communication and bulletins



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).



Usefulness

People are satisfied with our situation awareness products

Average

Survey to the ISACs of different fields

Grade

Cyber weather 2020 and a look towards 2021

10 information security forecasts for 2021

1. Something bad will also happen in 2021

In many organisations, the risk management cannot keep up with digitalisation. Solutions are deployed blindly without assessing, let alone understanding, the risks they cause. The end result may be miserable for citizens, the organisation itself, and society as a whole. The cyber year 2020 was not fun, but we also foresee dark clouds gathering over the coming year.

2. More regulation, more stability

People are already longing for sun in the rainy cyber weather. More and more efforts are made to manage cybersecurity risks with national and international regulations. The requirements increase especially in fields that are critical to the functioning of society. There is also a desire to restrict trade on data, including human health data, by means of regulation. This may even lead to splitting major technology giants into smaller pieces.

3. Telling real from fake will become even more difficult

Deepfake and other AI-based solutions offer an opportunity to make our information environment even more confusing. Populists and troublemakers in international politics take advantage of it mercilessly.

4. Bringing competence up to a sufficient level will take a long time

The demand for professionals needed by the digital society is growing. This also applies to information security and data protection experts. The need has been identified and the education is being developed in the right direction, but change happens slowly.

5. Criminals make virtual currency with cyberattacks

More and more cyberattacks in which tens of thousands is still small change will be seen in Finland. An especially serious threat involves ransomware attacks; anyone from small workshops to international high tech giants may be targeted.

6. Remote work is here to stay – and so are the risks

In 2020, people rapidly changed over to remote work mode. Some parties built their remote work solutions in a hurry on top of a motley assortment of quick fixes. Putting this mess into order will take a long time.

7. The quest for quantum-proof encryption is becoming more intense

Quantum computers took another step further in 2021. In fact, the information security industry is urgently preparing for the age of quantum computers. The number of quantum-proof encryption product solutions is increasing steadily.

8. The competition between technological superpowers is accelerating

The effects of the competition between technological superpowers also reach the shelves of phone and application stores. The Chinese-made Huawei vs. the American iPhone – what kind of technologies and applications can be used in these devices in the future?

9. Cyber influence between countries increases continuously

Cyberattacks, disinformation and hybrid influence are growing. Influencing people and attacks in cyber environments are often cheaper and less noticeable online than in the physical world.

10. Cybersecurity is finally on the management's agenda

The Vastaamo case brought cybersecurity and data protection to the management's agenda. Development requires long-term work, however, because cybersecurity threats are changing constantly. Our Kybermittari is an excellent tool that can give the management an overview of the organisation's level of cyber competence quickly.

Cyber weather in 2020

January

Regulation 66 on disturbances in tele-communications services entered into force.

In addition to countries, companies are also spied on.

February

Office 365: Phishing for user IDs continues, data breaches increase.

Technical support scam calls: Finns have received hundreds of thousands of calls. The number of incidents has exploded.

Certificate incidents: Microsoft forgot to renew its certificates, which caused disturbances in the Teams services.

EKANS – The 1st ransomware targeted at automation systems in the world was discovered.

March

Coronavirus: Non-existent protective devices and test packages for the coronavirus on sale. People's distress is exploited in disseminating malware, scams and espionage.

Technical support scam calls: The calls ended on 24 March.

Data leaks in different loyal customer systems. The information of Finns also ended up in the wrong hands.

April

Coronavirus: Vaccination research as a potential target of espionage.

Telia's internet connection disruption on 25 April.

May

Postal scams: Thousands of SMS leading to a subscription scam, phishing or malware were sent in the name of the Finnish postal service, Posti.

Ransomware attacks: Black-mailers auctioned stolen data.

The Sandworm group attempted to penetrate vulnerable Exim e-mail servers already in August 2019.

Ransomware attack against a critical Finnish infrastructure system.

June

Technical support scam calls: The calls started again.

EKANS malware attacks were targeted at Honda and the ENEL Group.

Several critical vulnerabilities that affected the information security of VPN services, among other things.

Top figures: 12 significant communications network disturbances, three of which were caused by the Päivö storm.

= International news highlight

Technical support scam calls: The calls continued. Hundreds of thousands of calls were made to Finland.

Certificate incidents: DigiCert invalidated several certificates on 11 July. This affected the functioning of several Finnish services.

Observations of Finnish hacked and vulnerable servers related to VPN software.

Plenty of critical vulnerabilities published. Many security holes in network devices were exploited.

The EU imposed sanctions against state-sponsored cyber attackers for the 1st time.

New wave of ransomware. Several ransomware attacks against the healthcare field detected around the world.

The Zerologon vulnerability is exploited actively.

The Aila storm: Nine significant disruptions that were brought under control quickly.

Detected threats of denial-of-service attacks increased.

Office 365: More data breaches, phishing messages were sent from hacked e-mail inboxes.

The number of Emotet incidents decreased, the warning issued on it was removed.

Data leak in Estonia; several ministries targeted.

The information security company FireEye and the European Medicines Agency became targets of espionage.

July

August

WARNING 1/2020: The Emotet malware is actively distributed in Finland.

The Norwegian Parliament became the target of a data breach. Norway accused Russia for the cyberattack.

The 1st official standard on the information security of consumer IoT devices was published.

Global CenturyLink disturbance on 30 August. The volume of traffic on the entire internet decreased by 2%.

September

October

Office 365: ID phishing with credible Zoom meeting invitations.

Psychotherapy centre Vastaamo: The company and the customers were blackmailed by threatening to publish patient records and personal data.

Reports of DoS attacks with a widespread impact that were also visible in the functioning of the services.

November

December

A backdoor was found in the SolarWinds management tool – opportunity for data breaches and espionage.

Kotiturvalistit – the citizen campaign for information security started.

Data breach in the Finnish Parliament on the news.

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

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

by e-mail: 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, 00059 TRAFICOM
tel. +358 29 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-763-1
ISSN 2669-8757

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre