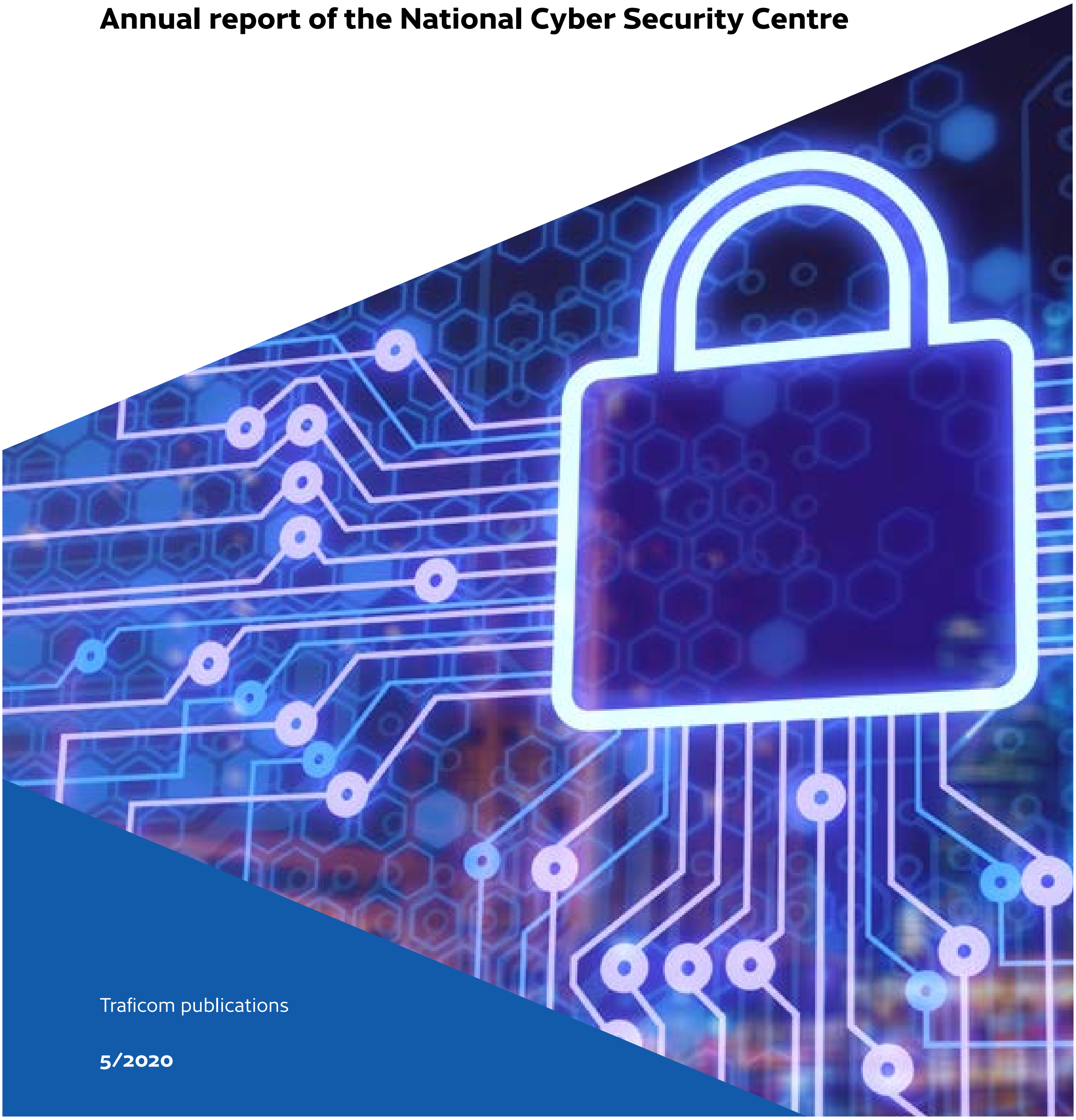
Finnish Transport and Communications Agency
National Cyber Security Centre

INFORMATION SECURITY IN 2019

Annual report of the National Cyber Security Centre



Traficom publications

5/2020

CONTENTS

Society needs information security in daily life – together we are the strongest link 3

TOP 3 SECURITY THREATS AND PROTECTION AGAINST THEM 4

- Threats and solutions for individuals 5
- Threats and solutions for organisations 6
- Significant cyber security events in 2019 8

CYBER WEATHER PHENOMENA 10

- Network functionality 11
- Espionage and influencing 18
- Malware and vulnerabilities 20
- A large-scale ransomware attack can cost tens of millions 21
- Data breaches and data leaks 24
- Phishing and scams 26
- Internet of Things 31
- Key information security risks for individuals, organisations and central government 32

OUR SERVICES 34

- Coordination centre handles thousands of cases every year 35
- Municipalities have an important role in providing everyday services and protecting residents 35
- Information security regulation and assessments 38
- Cooperation and sharing of information 42
- A better grip on cyber security through exercises 48
- Work on the future and development of operations 50
- Our KPIs 58

CYBER WEATHER 2019 AND A LOOK AT CYBER YEAR 2020 60

- 10 Information security forecasts for 2020 61
- Cyber weather 2019 64
- A busy year of publications, events and campaigns 66
- Summary of cyber weather news in 2019 69

Society needs information security in daily life – together we are the strongest link

The widest societal discussion in 2019 concerned the cyber security of 5G technology. We were ready, as our experts have worked on evaluating the technological challenges and potential created by the new technology and standard since 2017. Our ability to produce technical information for the national risk assessment was also appreciated internationally.

Peak moments of 2019 for the NCSC-FI included our international events: the world's first 5G Hackathon and Galileo Innovation Challenge. These events were evidence of smooth cooperation between telecommunications operators, hardware manufacturers and the authorities. Our strength lies in cooperation, and we must hold on to it.

The past year will also be remembered for the rapid exploitation of new vulnerabilities and ransomware with extensive impacts – and it marks the point where scams and phishing became part of our daily life, the new normal. It was also a mega year of cyber security regulation, during which many pieces of legislation on information security entered into force. Among other things, TUPAS authentication protocol became obsolete, and changes in identification and trust services brought competition into this sector.

Cyberattacks targeting the municipal sector were one of the starkest wakeup calls in the field of cyber security last year. They showcased the vulnerability of our society and, among other things, obstructed citizens' basic services and daily life. These cases and the investigations in them have sparked discussion in central government, municipalities and top management in the business world. It is crucial that this matter does not remain at the level of discussion; essential and concrete actions and decisions must be taken to achieve improvements.

In 2019, 'big game hunting' made its way to Finland as a new phenomenon. It refers to criminals targeting ransomware attacks at large companies in the hope of extorting large amounts of money. These attacks have caused serious incidents and even business interruptions for companies, as well as considerable financial losses. The phenomenon has put overall management of cyber risks, which also covers the supply chains and partners, on the agenda in corporate management.

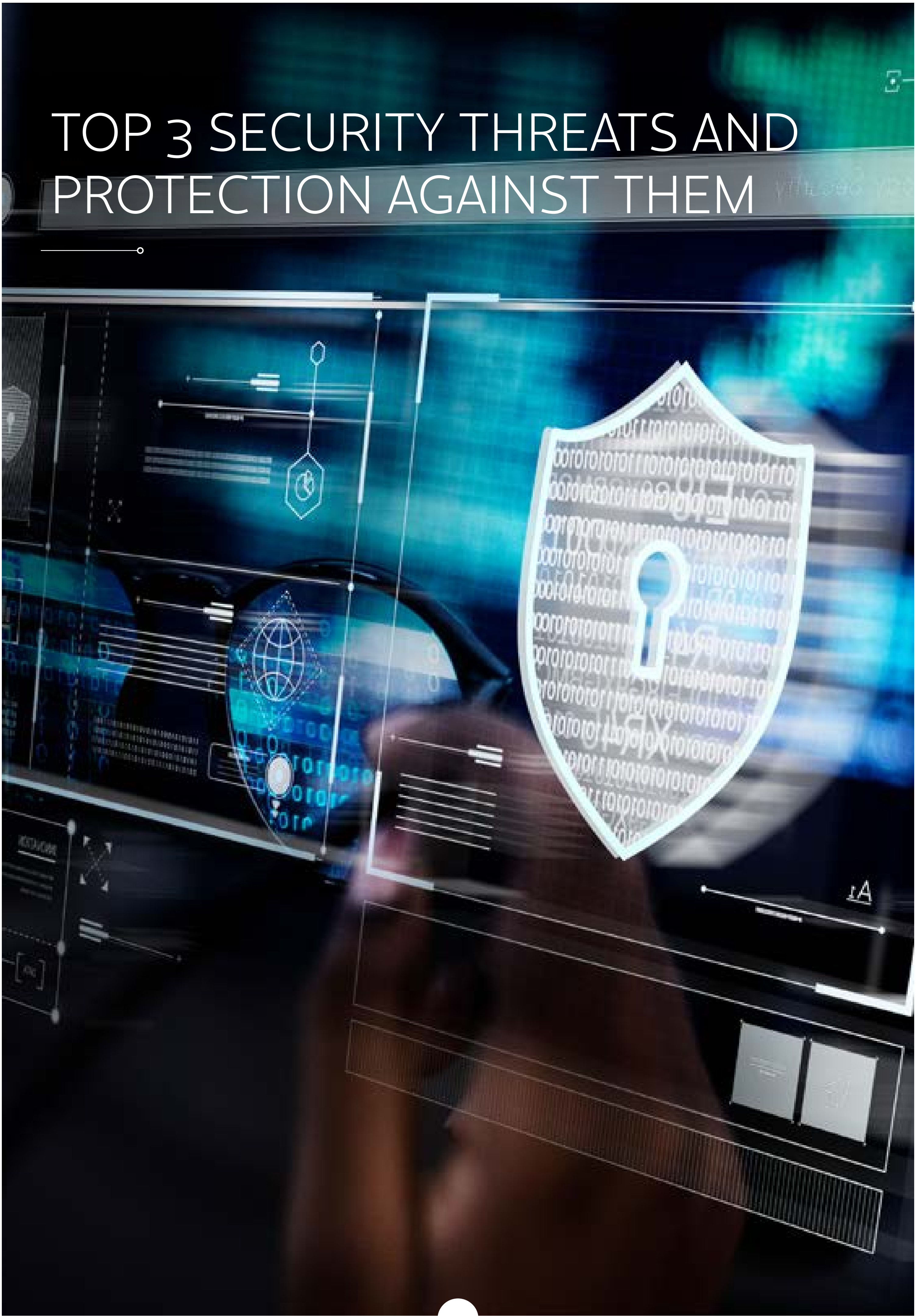
We were pleased with the wide publicity attracted by the Cybersecurity label for consumer devices developed by us last year. This label offers an easy way of improving your personal cyber security. Our active campaign on the social media, TV and radio reached over 2.4 million citizens, awakening their interest in information security!

The new year will bring not only new challenges but also positive development. The interest generated by the guide 'Cyber security and the responsibilities of boards' published at the beginning of the year is a good indicator of companies' willingness to take action.

I had the pleasure of starting my work as Director of the National Cyber Security Centre at the beginning of 2020. Active cooperation with our stakeholders provides an excellent foundation for further development of society's cyber security in 2020.

Helsinki, 19 February 2020
Kalle Luukkainen
Director-General
National Cyber Security Centre
Finnish Transport and Communications Agency
Traficom

TOP 3 SECURITY THREATS AND PROTECTION AGAINST THEM



Threats and solutions for individuals

High-quality passwords, periodic security updates and judicious online behaviour. There has been little change in information security threats and solutions for individuals in recent years. The same principles will help you protect yourself and your most important data now and in the years to come.

THREATS

Scammers make away with your data and money

Everyone is a target for scams and phishing. Scams are part of daily life for companies, the public administration, associations, funds, foundations and educational institutions alike. Some are blatantly obvious, while others are skilfully prepared and targeted and completely credible. The aim of the criminals is to access the organisation's information systems and, for example, send fake invoices or spy on business secrets.

Weak passwords and easy access to e-services

Each one of us may use up to several hundred online services. As you cannot remember dozens of unique passwords, you often end up using the same, simple passwords for a number of services. This increases the risks: in case of a data breach or leak, all the accounts protected with the same password will be compromised.

Unprotected smart devices

Like your mobile phone, smart TV, and computer are certain to contain valuable information about you. Do you know how to take care of their security and updates? A large share of security updates contain patches to fix security issues in your device or software. Using devices which have not been updated is always a risk. It is like an open invitation to hackers.

SOLUTIONS

No need to disclose too much information

A public authority or service provider will not ask for your user IDs or banking credentials online. If somebody requests this information unexpectedly, you should ask why they need it and wonder if the message is genuine. Instead of using the link provided, log in through the service provider's website. This is a safe way of checking if you really need to provide your information or take some action.

High-quality passwords and strong authentication protect your data

At the very least, a good password is a long one. Only use each password for one service. Start using a password manager application. It will remember the passwords for you. Also enable two-step identification and strong electronic identification whenever possible. This will increase the security level of such services as your bank account and social media accounts.

See to updates and product security

By updating your devices, you can also protect them from security threats. If you enable automatic updates, you will not have to think about them yourself.

Are you purchasing a new smart device?
Our Cybersecurity label indicates that the device is safe.

Threats and solutions for organisations

Risk management, preparedness and personnel training are all part of a well-managed cyber security programme in an organisation. As it requires mastering many different areas, cyber security should be a shared practice of the entire organisation.

THREATS

Daily phishing and scams

Companies, the public administration, associations, funds, foundations and educational institutions are targeted by scams and phishing on a daily basis. Some are obvious, while others are skilfully prepared and targeted and they appear to be credible. The criminals use these scams to access the organisation's information systems, for example to send fake invoices or spy on business secrets.

Rapid exploitation of new vulnerabilities – traditional prevention & response is no longer sufficient

Any vulnerabilities that come to light are exploited almost immediately by criminals in their attacks, and organisations should consequently be prepared to update their information systems and applications at an increasingly faster pace. This is particularly important for organisations working with leading-edge technologies and innovations, which are a particular target for both criminals and industrial espionage. Do you know your way around your information environment, applications and systems? If you do not, attacks against your environment cannot be prevented by such means as security updates.

Services centralised and outsourced without planning and assigning responsibilities

Outsourcing key services or providing services for partners increase the risk of cyberattacks. Criminals use an organisation's partners or subcontractors as a stepping stone in their attempts to access the information systems of the actual target, for example by stealing access rights granted to a partner. Incidents of different types may spread widely and to unexpected places if the centralisation or outsourcing of your services has not been planned properly.

SOLUTIONS

Include cyber security in your organization's risk management

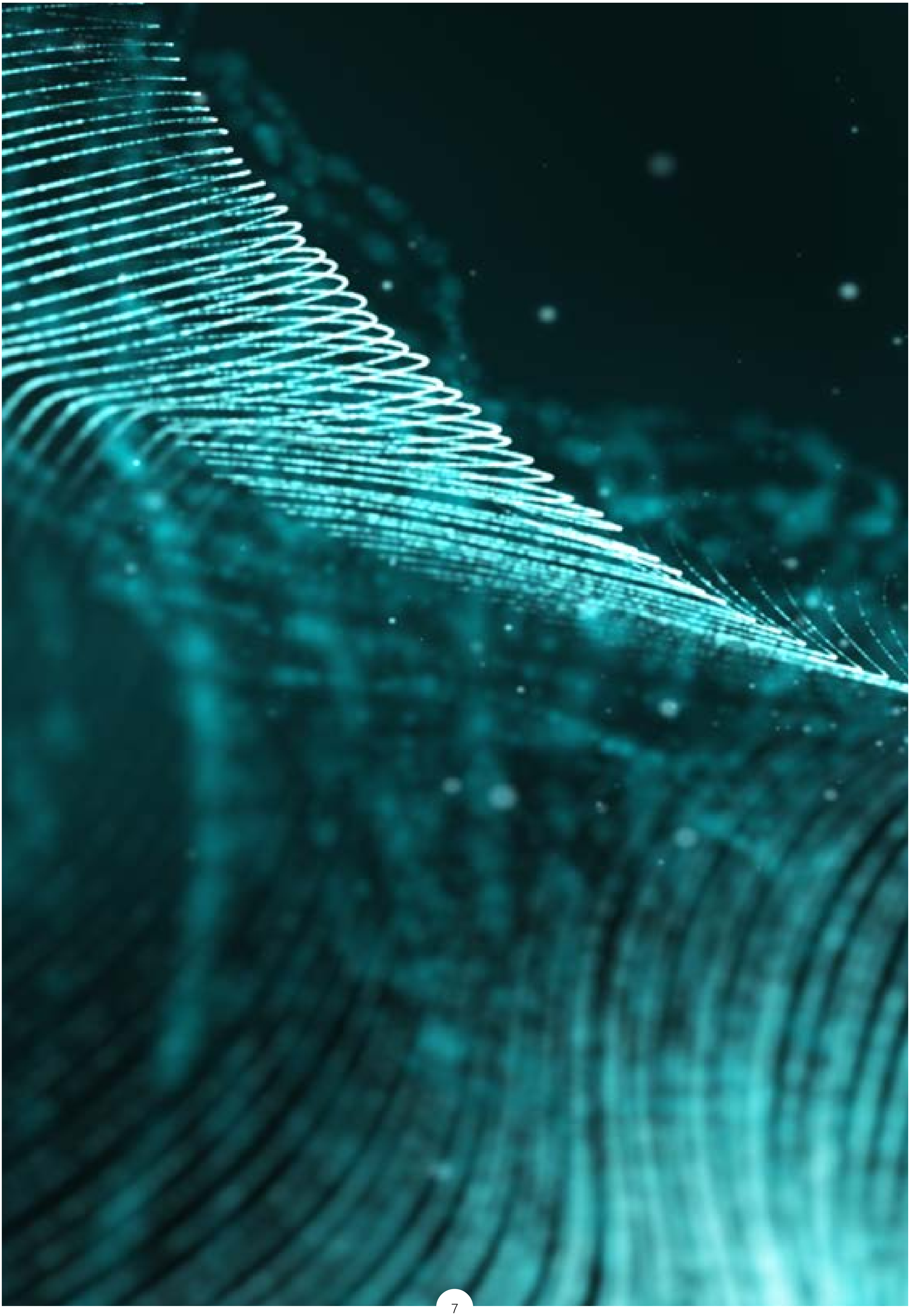
Cyber security risks must be addressed. The same mechanisms apply to them as to more conventional risks: for example, the risk can be eliminated by inactivating a service, or its probability can be reduced by using strong electronic identification. The residual risk can be tolerated if its level is acceptable to the organisation's management.

Practise your response to incidents and emergencies

What will you do if a cybercriminal has hacked into your email system and is sending fake invoices in your name? The best practices can be identified by participating in training and organising exercises on responding to different cyber incidents. This often also is the most cost-effective way of uncovering any shortcomings. If you know your information environment and have practised your routines for updating and backing up your systems, you will do better in both simulated and real crises.

Assign responsibilities to suppliers and identify the dependencies of your services

Before outsourcing services, the supplier's responsibilities, response to incidents, and the dependencies of your services must be defined. You should agree on the operating models and responsibilities with your partners and third parties already in the contract negotiations. This way you will know your roles and responsibilities and be familiar with each other's practices, for example in case of an incident.



Significant cyber security events in 2019

POSITIVE ACHIEVEMENTS

- **Work on the cyber security of new technologies:**
  - 5G Hackathon
  - Galileo Innovation Challenge
- **Impacts of the KYBER 2020 programme:**
  - More organisations arrange cyber security exercises – Our instructions help them get a grasp on the basics of exercising.
- **Improvements in citizens' security awareness and skills:**
  - Cybersecurity label
  - Security tips
  - Online safety guides for children and parents
  - Spoofy – an information security game for children
- **Improving the cyber security of critical infrastructures:**
  - Cyber meter, Kybermittari, for assessing the level of cyber security
  - HAVARO service
  - DNSSEC

INTERESTING PHENOMENA

- **QSnatch malware**
- **Reflection DoS attacks**
- **Successful elections and Presidency of the Council of Europe**

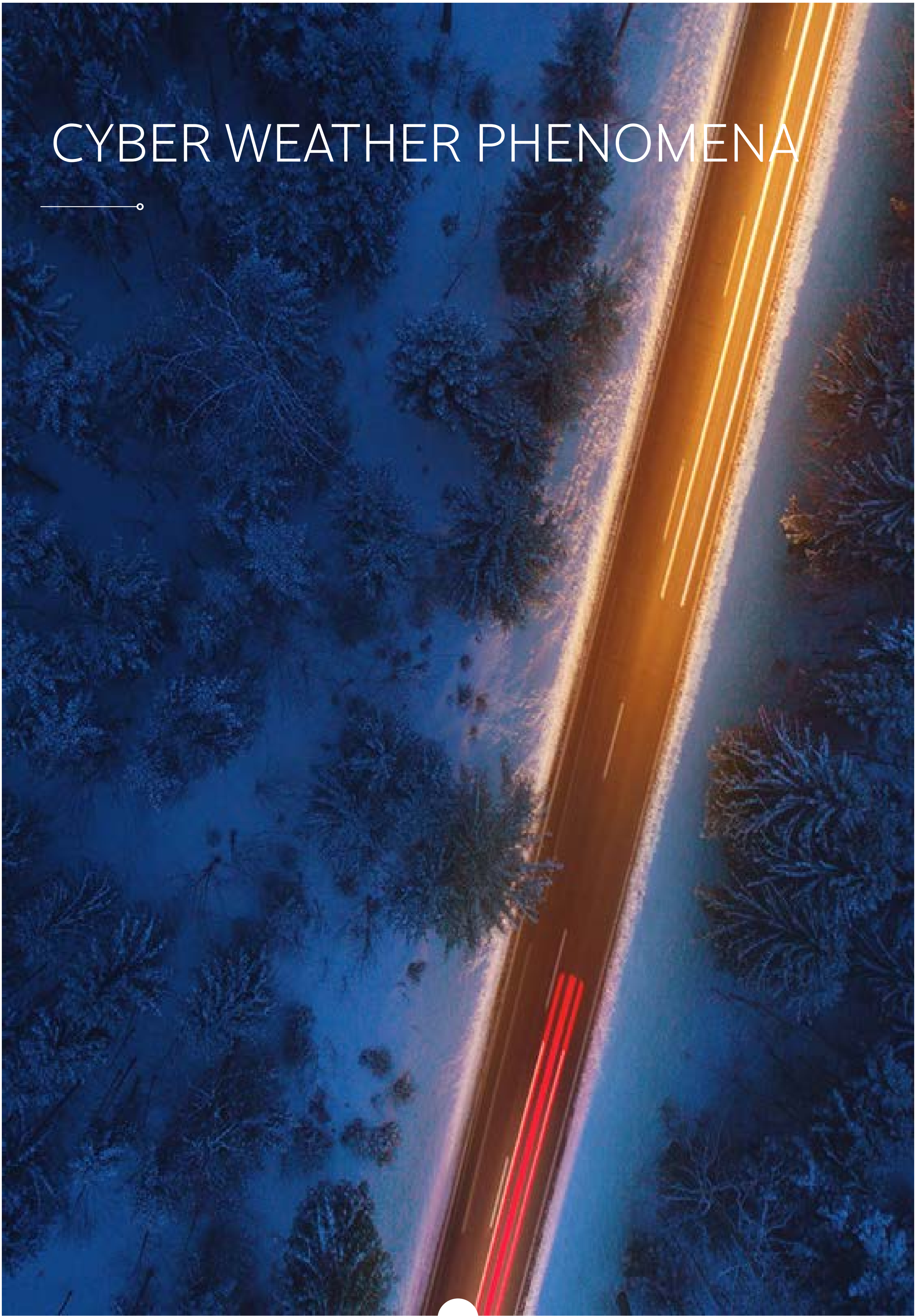
CAUSES FOR CONCERN

- **The new normal: phishing of Office 365 credentials**
- **Big game hunting - Cybercriminals after substantial prey**
- **Cyber security in municipalities**

CHANGES IN INFORMATION SECURITY REQUIREMENTS

- **TUPAS became obsolete**
- **Competition in the electronic identification service market**
- **NCSC-FI criteria support cloud service procurements**

CYBER WEATHER PHENOMENA



Network functionality

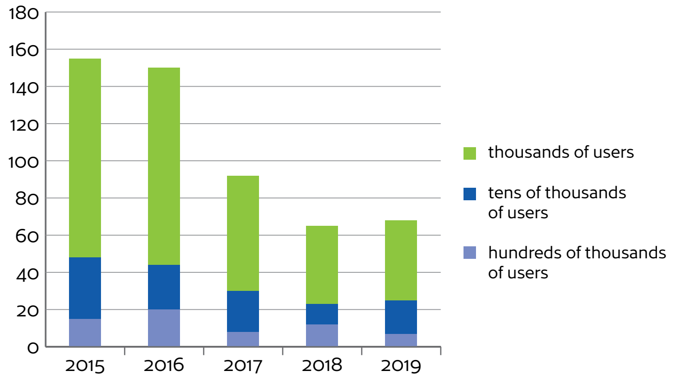
Loss of connectivity caused by high winds and lightning

The longest disturbances in 2019 were caused by weather conditions. In January, Storm Aapeli resulted in power failures and several long-lasting incidents. In June, voltage spikes generated by lightning damaged several power supply systems of communications networks and caused a few major disruptions. While power supply system failures caused by lightning cannot be completely eliminated, overvoltage protection of network components can often prevent equipment failure.

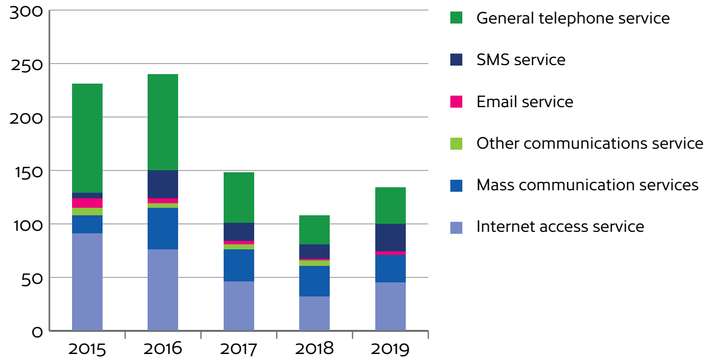
The number of most serious disruptions in domestic communications services has halved since 2018. A reduction has been seen in extensive and serious faults in the terrestrial television network, in particular. On the other hand, the number of incidents affecting approx. 1,000 to 10,000 communications service users increased slightly compared to 2018. The most significant incidents were caused by various hardware and software failures and power outages. However, the total number of significant incidents decreased clearly from 2015 and 2016.

The NCSC-FI assesses that the reasons for the decreased annual number of significant incidents include at least the following:

- the number of major overhaul projects of public communications networks has dropped
- previous network overhauls have resulted to networks and services that are easier to manage and have a higher fault tolerance
- the incidence of major telecommunication cables being damaged during excavation works has reduced
- cooperation between telecommunications operators and electricity network companies has improved.



Major incidents by the number of communication service users affected in 2015–2019.



Major disruptions by communication service in 2015–2019.
One incident can affect several communication services at once.

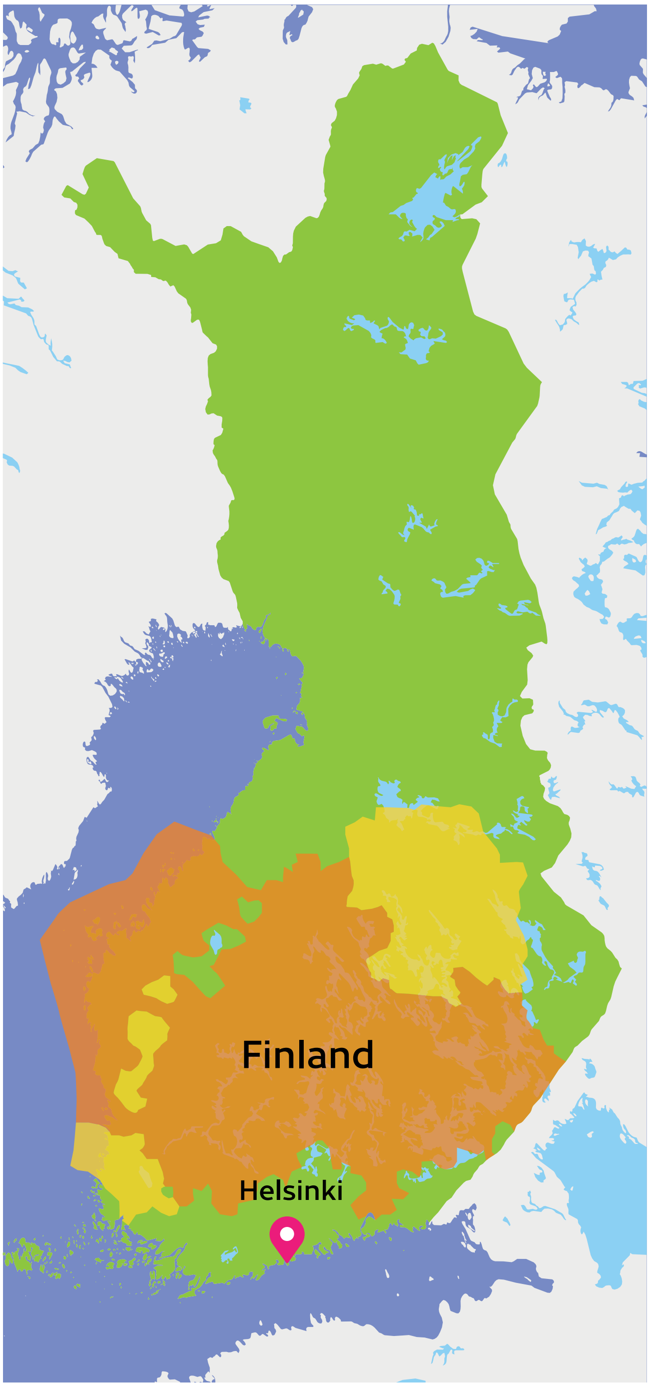
Record-breaking wind speeds left 120,000 customers without power

The regions of Ostrobothnia and Åland Islands bore the brunt of the onslaught as Storm Aapeli hit Finland on 1 and 2 January 2019. The wind blew a great number of trees down on power lines, cutting off electricity supply to devices that maintain mobile networks. Significant disruptions to mobile communication services were experienced in more than one third of Finland. The storm also affected Finland's authority radio network VIRVE, whereas there were no major disruptions to the landline and television networks.

In the Åland Islands, the radio station Ålands radio lost power for a couple of hours. According to news reports, emergency calls were also disrupted for almost 24 hours. Overlapping local shadow areas may have occurred in the mobile services in Mainland Finland, which is why making emergency calls on mobile phones was not possible in some places. According to the Emergency Response Centre Administration, however, the number of emergency calls was at the expected level, and consequently any shadow areas were small.

The most widespread interruptions of mobile communication services were seen on Wednesday, 2 January 2019. In Mainland Finland, significant disruptions had been repaired by 3 January. The situation of public communication services in the Åland Islands remained unclear. According to newspapers, significant outages still occurred on 4 January.

Storm Aapeli cut the power supply to approx. 120,000 households or customers. In comparison, storms Rauli (2018) and Seija (2013) resulted in power failures affecting around 200,000 customers. Despite unprecedented wind speeds, Aapeli had less of an impact than storms in previous years. For this we owe thanks to the effective cooperation between telecommunications operators, electricity companies and the authorities, which has become smoother year by year. Lessons have been learned from storm experiences and the benefits of cooperation.



A view from Traficom's public MONITORi service on 2 January 2019 at 10:31. The areas in which different telecommunications companies experienced disruptions are marked in different shades of yellow. There was a significant deterioration in the services of two telecommunications companies.

Reliability of other ICT services

While public administration bodies and companies have planned measures designed to improve the reliability of their ICT services, an inability to implement these in practice has been typical of their response to major incidents.

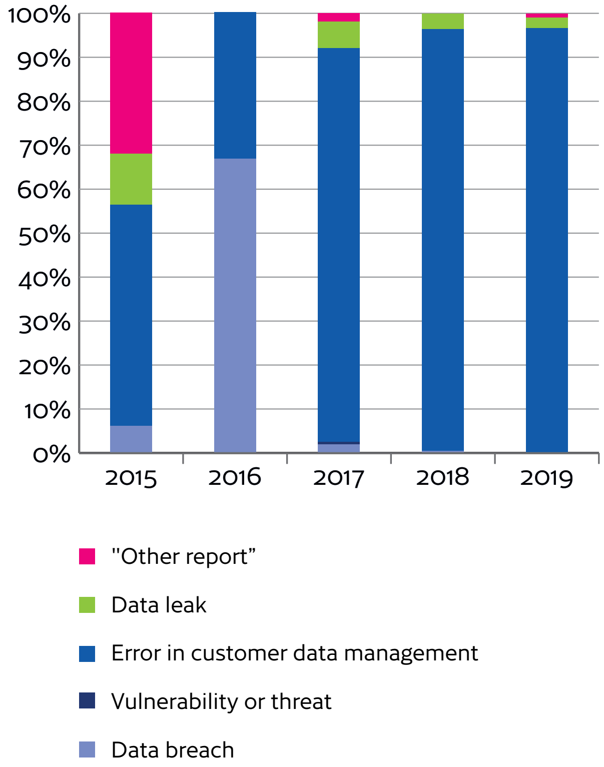
Disruptions had significant impacts especially in healthcare even though healthcare providers have taken precautions to take care of customers and patients also without telecommunication services. ICT incidents slow down work in the healthcare sector and reduce its service capacity, for example when treating a person whose patient history cannot be accessed.

Number of security breaches reported by telecommunications companies has stabilised

Following a strong increase in recent years, the number of security breaches reported to the NCSC-FI has stabilised and even decreased slightly from the 2018 figures.

Most of these reports concern cases in which personal data are destroyed, lost, compromised or disclosed to third parties accidentally or without authorisation. The most typical report relates to an error in the processing of personal data, as a result of which an individual customer's personal data end up in the hands of a wrong person.

The Figure shows telecommunications companies' reports of personal data breaches and their trend in 2015–2019.



July

2019

10.7. Patient information system Apotti was down due to a faulty network switch in the City of Kemi's intranet

11.–18.7. Galileo, the European satellite navigation system, was down for a week. This was due to faults in both ground control centres of the system, which made it impossible to calculate the exact positions of the satellites in their orbits.

September

2019

In September, the old emergency response centre system ELS was deployed for a week to restore the availability of the new Erica system. Erica has been repeatedly affected by disruptions in TUVE, the state's High Readiness Network.

27.9. Patient information system Apotti was disabled in Vantaa due to fibre optic cable failure.

October

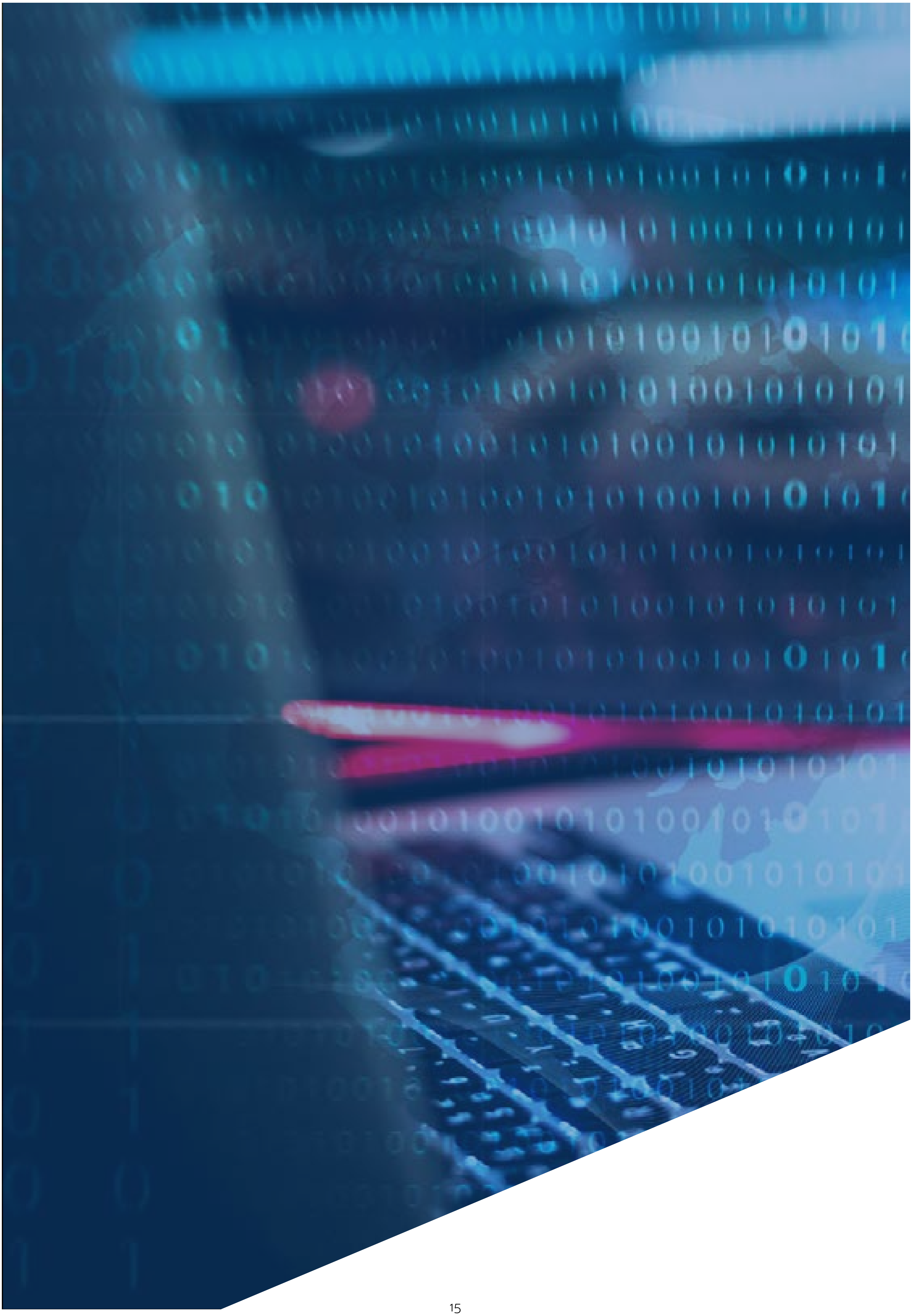
2019

Several disruptions in the public administration's ICT services in October:

10.–18.10. Disruptions in the Population Register Centre's VTJ interface hampered the work of several authorities.

13.–14.10. Disruptions in the VY network maintained by the Government ICT Centre Valtori hampered the operation of the websites and e-services of several central government authorities.

14.10. Incident in Neste's information systems caused a temporary drop in the company's share value. It resulted from hardware failure in the data centre of Neste's ICT service provider.



Denial-of-service attacks: often motivated by interference or extortion

Preparedness for denial-of-service attacks has improved, especially among Finnish companies. While telecommunications companies' networks saw more attack traffic than in the previous year, the impacts of the attacks reported to us were less drastic.

There was a high number of short attacks. Around 80% of all attacks seen in Finland lasted less than 15 minutes in 2019. While the targets of the attacks vary, the Wilma system used by schools comes up year after year. The short attacks may be carried out by young people experimenting with denial-of-service attacks and their effects. 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.

MOTIVES FOR DoS ATTACKS

1 Interference

2 Obtaining financial gain through threats of an attack

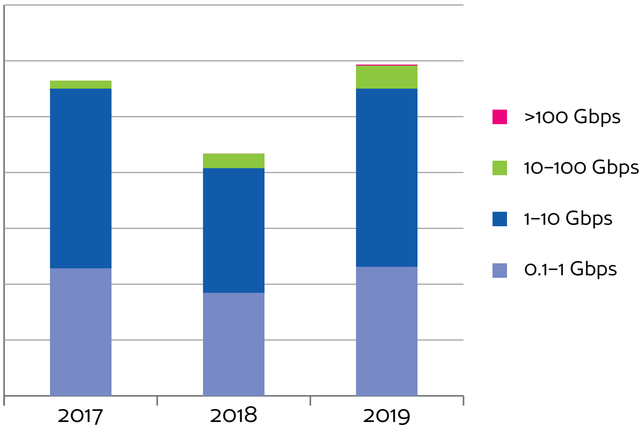
3 Wish to experiment with the impacts of the attack out of interest

Carrying out DoS attacks is technically easy as so-called stresser services are available on the Internet, where attacks can be purchased as a service with no technical expertise required. Many sites selling attacks offer short-term sample attacks for free.

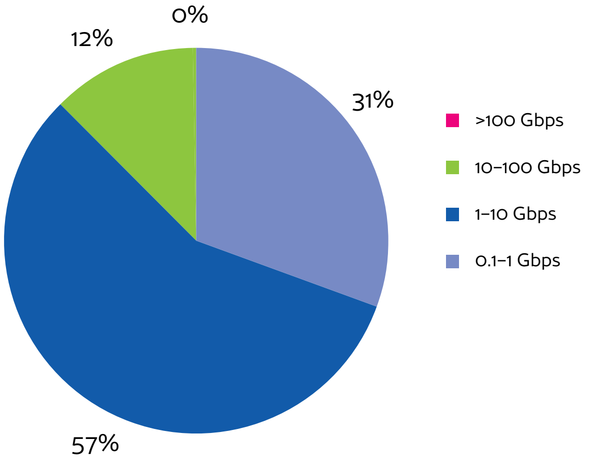
Organisations better protected, yet incidents have not been avoided

In particular, large Finnish organisations are better prepared for DoS attacks than in earlier years. Thanks to the deployment of "scrubbing centres" and cloud services, for example, companies often successfully prevent the attacks and avoid significant impacts on the functioning of their services.

Regardless of the protection, we sometimes still see service disruptions. They are usually caused by attacks which manage to disable services before the countermeasures kick in. For example, in many cases the target’s firewall is overloaded and will not automatically return to its normal state even after the actual attack traffic ceases. It is worth testing the ability of your organisation’s services to withstand attack traffic and identifying any bottlenecks or weak points in the service in a controlled manner. A good example of this is the exercise carried out by LähiTapiola described by our guest writer, **Leo Niemelä**.



Trends in DoS attack volumes in Finland.
Source: Telia



Volumes of DoS attacks in Finland in 2019.
Source: Telia

The number of DoS attacks has increased year on year. The greatest increase was seen in attacks of over 1 Gbps and over 10 Gbps.

The volume of approx. 69% of all attacks exceeds 1 Gbps, while 12% have a volume in excess of 10 Gbps. Attacks exceeding 10 Gbps in volume and many smaller attacks are seen in Finland every day.

” DoS exercises keep attackers at bay

In LähiTapiola, we have been trying to improve our information security with an open mind over the years. Our established practices include working together with white hats, a bug bounty programme and open communication about information security. This year, we got a chance to carry out a DoS attack against our own online services.

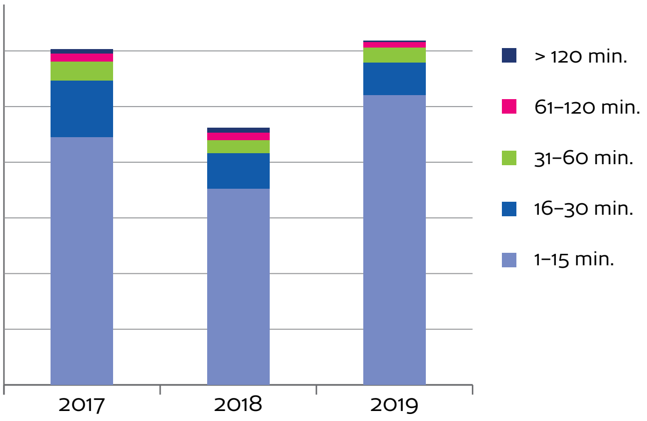
In this attack, which took place in January 2019, we used the tools favoured by cyber criminals. We stressed the company's online services to the content of our nerdy hearts: a global botnet comprising hundreds of computers had the single aim of flooding LähiTapiola's online services. Our goal was achieving an ability to withstand DoS attacks and learning how LähiTapiola's infrastructure copes with stress caused by anomalous network behaviour.

The exercise required a great deal of advance planning in the areas of telecommunications, infrastructure, servers, applications and databases. We mostly had to guestimate the risks and accept the fact that all the risks caused by the exercise could not be predicted. Preparation, planning, communication and the actual exercise required months of planning, courage from the management and – most importantly – seeing the exercise as an investment in the future.

Services that prevent DoS attacks have a toxic effect on attackers. In order to work properly, however, prevention services need to be optimised and configured very carefully, ensuring that even low-volume traffic slowing down the services can be detected and isolated from normal telecommunication traffic. We learned that it only takes surprisingly small volumes of traffic to crash many services.

I encourage companies to carry out practical exercises, because they will help you adjust the defensive actions to the right level and understand in concrete terms the risk areas to which the organisation must pay particular attention.

Leo Niemelä
LähiTapiola



Trends in DoS attack durations in Finland.
Source: Telia

The number of attacks lasting less than 15 minutes has increased since the previous year. Short attacks of less than 15 minutes are probably free sample attacks obtained from stresser services.

The countermeasures launched by the organisation are a key factor influencing the duration of attacks, as criminals usually continue for as long as the attack has a visible impact on the target's operation.

DoS ATTACK TECHNIQUES IN 2019

As in previous years, the total volume of DoS attacks mostly consisted of so-called UDP (User Datagram Protocol) amplification attacks, including the use of network time or domain name services. This technique uses open servers around the world, from which amplified traffic is reflected to the target. Application level attacks were also seen regularly.

As a rising trend, especially towards the end of the year, we saw cases in which TCP (Transmission Control Protocol) handshake traffic was reflected to the target organisation's network. The packet volumes were large enough to also disrupt Finnish servers used for reflecting the traffic, even if they were not the actual target. The perpetrators flooded a number of the target's network addresses at the same time, adding to the challenge of thwarting these attacks.

Espionage and influencing

The trends in state-sponsored cyber espionage remained largely the same as in previous years. Finnish companies and public administration organisations continue to be targets for cyber espionage for both political and economic reasons.

In the global context, we have already witnessed the significant impacts of well-targeted cyber operations. Indications of interest in Finland's critical infrastructure were also observed. Attackers seek weak points in organisations' systems, trying to gain a foothold. Attempts to access systems may also take the form of spearphishing of credentials.

Cashing in on cyber espionage

During the year, corporate espionage with the aim of stealing companies' intellectual property was again prominent. By stealing business information, spies hope to get ahead of competition, for example by benefiting from research and development carried out by others. For the victim, the consequences may include reduced sales or loss of market share as competing products or services which, thanks to the espionage, can be produced at a lower cost to take over the market.

States may try to improve their financial position or achieve other national objectives by combining cyber espionage with investments or other means of economic influence. China, for example, was accused several times in 2019 of spying on the aviation industry and copying technologies to launch its national aircraft production.

New techniques more difficult to detect

Leveraging various public services in cyber espionage became clearly more widespread. If an attacker adds their own content, including hidden commands, to image and video platforms or other cloud services, this is difficult to discover using standard methods for detecting anomalous network traffic.

As these and other techniques become more common, the significance of end-point based detection is emphasised. These solutions have not been deployed widely, even though both commercial and free ones are available.

Supply chain attacks can be discreet

Infiltration of a target through supply chains remains a topical threat. For example, data breaches or infiltration can be carried out by hacking into an IT service provider's or hardware supplier's systems.

Cases in which strategic partners of companies and organisations were used in this manner also came to light last year. Dependency relationships between such companies are closer, and partners are not easy to replace.

Services which are the key to the functioning of digital infrastructure and networks were also used in such targeted attacks, including domain name services. In addition, the reliability of security solutions was at stake when an attempt was made to hack into the Virtual Private Network (VPN) services and solutions used to create secure network gateways.

Employee's private devices can also be used as an entry point for infiltrating the systems administrated by an organisation.

Journalists, researchers and dissidents among the targets

Individuals, population groups and researchers were also spied on in 2019. For example, there were several news reports of China's efforts to monitor its Uighur minority.

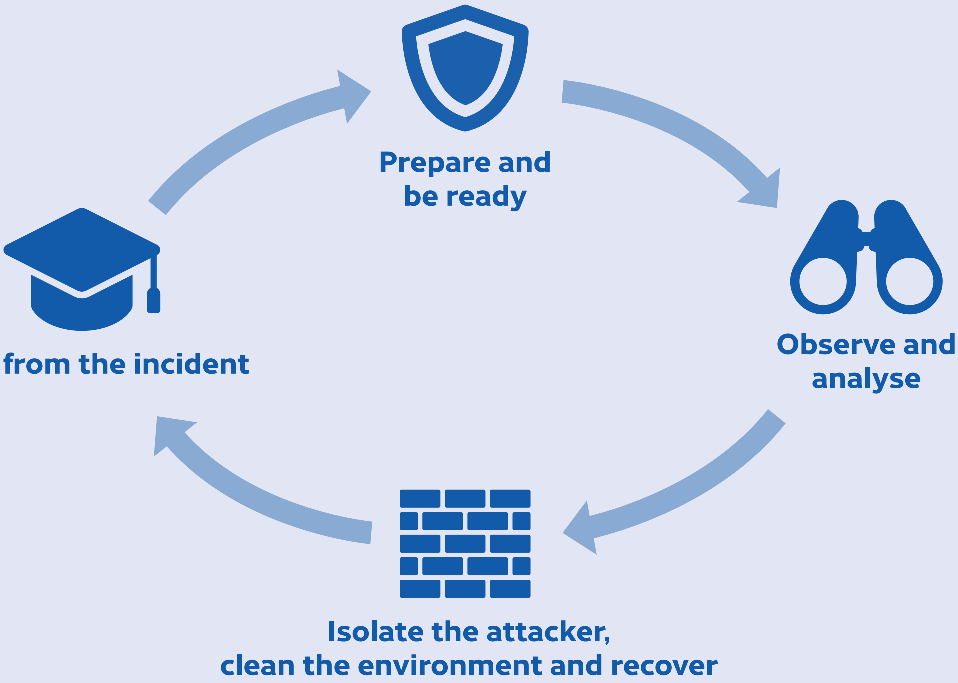
States may also attempt to spy on or monitor their citizens, dissidents and activists living abroad, or journalists or researchers working on sensitive issues. Such efforts may also affect people living in Finland or organisations operating here.

Varying levels of preparedness

Some organisations in Finland are clearly better prepared for the threat of spying than others. The need to be prepared does not only concern operations in Finnish territory; Western companies also need to watch out for attempts to influence them for political reasons, also by means of cyber espionage.

In addition to technical solutions, preparedness should be improved by increasing security awareness. Different kinds of organisations may end up as targets for espionage because of their activities, the information they possess, or their position in a supply chain.

HOW TO RECOVER FROM A DATA BREACH



1 Your organisation received targeted phishing messages two months ago. You find out the sender's address.

- Is this information enough to identify the message and find out to whom it was sent?
- Can you establish if the message has been opened and if the user has clicked on the link it contains?

2 You are notified of malware command-and-control traffic originating from your organisation. The person reporting the issue gives you the timestamp and the domain name of the C&C server.

- Can you identify the device from which the traffic originates?
- Can you find out which application or process generated the traffic?
- How can you make sure that no potential evidence is lost or destroyed during the incident management process?

3 We are trying to reach the person responsible for information security in your organisation to investigate a potential observation related to state-sponsored activities.

- Has your organisation delegated responsibilities for information security matters?
- Can our expert find the contact details of your information security officer, or can they be contacted in some other way?
- Do you know where to find help for investigating the matter further?

Malware and vulnerabilities

The year 2019 will be remembered for the rapid exploitation of new vulnerabilities. The delay between publishing the details of a vulnerability and its exploitation was considerably shorter than before. Consequently, organisations' information security processes should be prepared for the rapid installation of critical updates or the implementation of other prevention measures without delay. Particularly systems connected to the Internet should be kept constantly up to date. For example, critical updates or other mitigations should be implemented immediately rather than at the time of the next maintenance outage.

Exim vulnerability exploited in data breaches at lightning speed

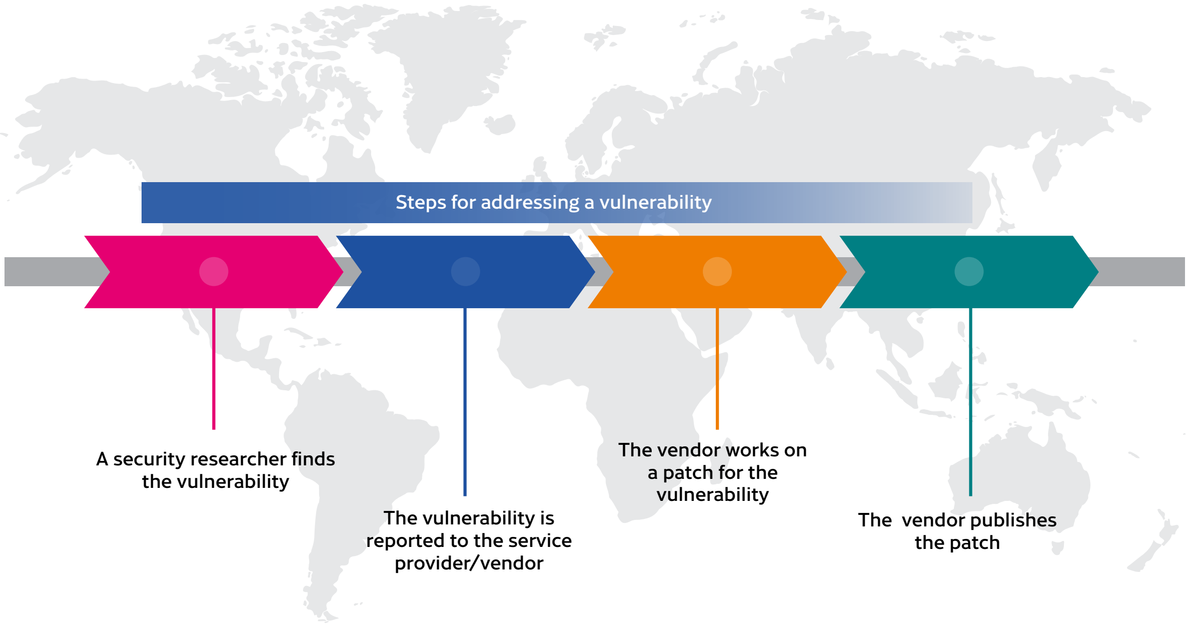
A vulnerability enabling the remote use of Exim email server software came to light on Thursday 6 June 2019. Several data breaches exploiting this vulnerability took place the very next weekend, also in Finland. Consequently, we issued an alert concerning Exim vulnerability exploitation on Monday 10 June.

Mass exploitation of a vulnerability might not start immediately. For example, the so-called BlueKeep vulnerability related to unauthorized remote use of Microsoft Windows Remote Desktop Protocol was found in May 2019. It took several months before a public exploit of the vulnerability was available. Prior to this, the vulnerability had been exploited in individual cases. At the time a vulnerability is published, it is thus difficult to predict how quickly it will end up as a weapon wielded by criminals.

Little or no maintenance on some devices connected to the Internet

Too few devices connected to the Internet are maintained. This became clear when we tracked BlueKeep and other vulnerabilities in Finland. In late May, we scanned Finnish Internet addresses and found 414 vulnerable systems connected to the Internet. The owners of these devices were contacted through telecommunications companies. After almost two weeks, we still found 353 vulnerable systems, which means a drop of only about 15%. Criminals are also on the lookout for systems connected to the Internet that remain vulnerable.

Zero-day vulnerability timeline


Steps for addressing a vulnerability
A security researcher finds the vulnerability
The vulnerability is reported to the service provider/vendor
The vendor works on a patch for the vulnerability
The vendor publishes the patch

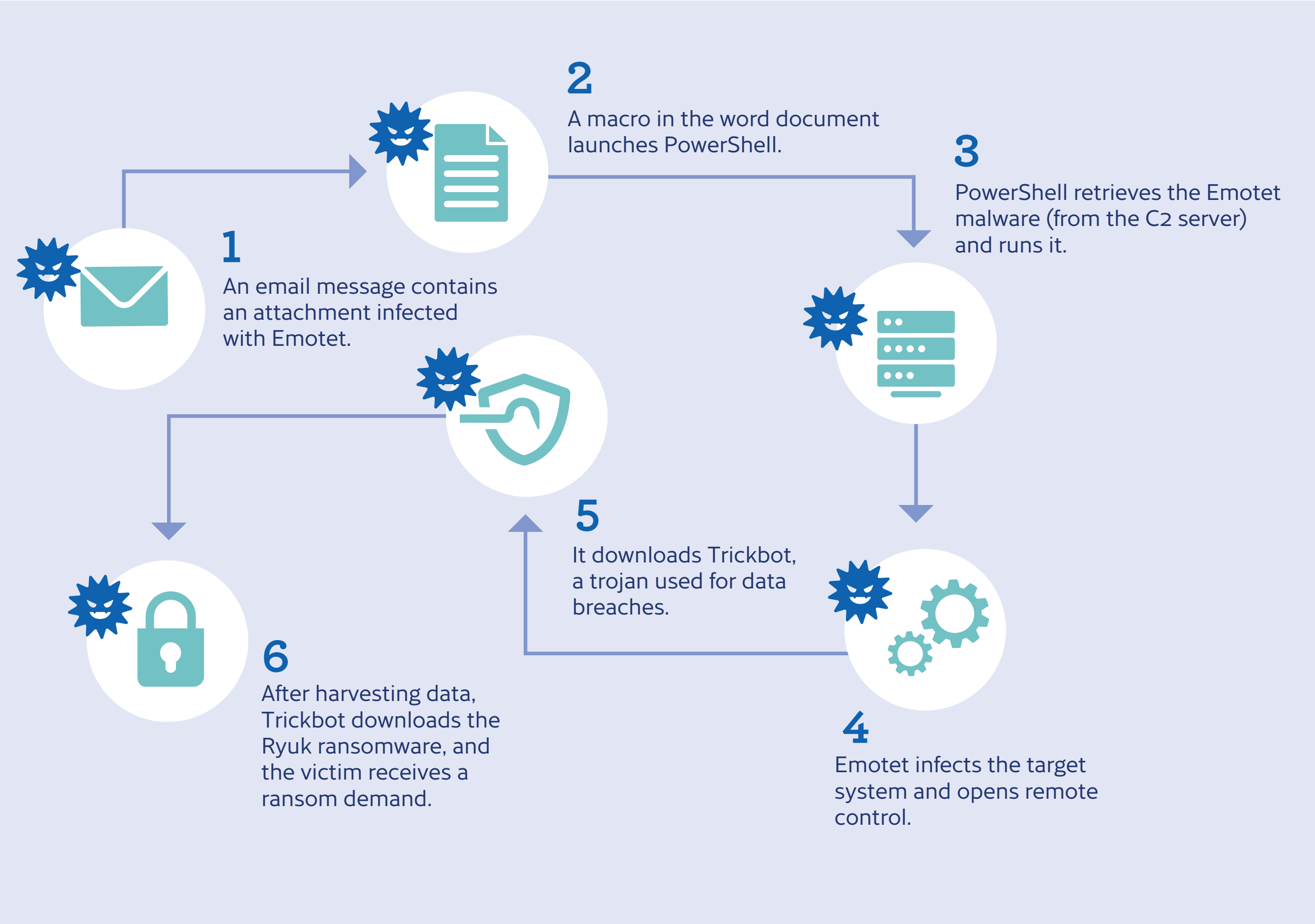
A ransomware attack with major impacts can cost tens of millions

Ransomware attacks with extensive impacts were talked about a great deal last year. In this phenomenon known as big game hunting, skilled criminal groups prey on companies or organisations whose activities would be significantly hampered by a widespread ransomware infection.

Criminal groups specialise and sell their services to each other

While one criminal group focuses on spreading a malware infection as widely as possible, for example by using hacked email threads with malicious attachments, another uses the malware to collect information, such as passwords and credit card numbers, and packages them for resale. A third group, on the other hand, buys its way into the most suitable targets and installs ransomware which encrypts the servers, network disks, and key workstations of the entire network. This paralyses the target's operations. A ransom of tens or hundreds of thousands of euros is demanded to release the victim's data.

This is how the chain of ransomware attacks associated with big game hunting proceeds:



1 An email message contains an attachment infected with Emotet.

2 A macro in the word document launches PowerShell.

3 PowerShell retrieves the Emotet malware (from the C2 server) and runs it.

4 Emotet infects the target system and opens remote control.

5 It downloads Trickbot, a trojan used for data breaches.

6 After harvesting data, Trickbot downloads the Ryuk ransomware, and the victim receives a ransom demand.

Credible scams are difficult to tell from genuine messages

The criminal group spreading Emotet has developed an efficient way of tricking recipients with email messages.

Email threads of previous victims are hijacked and sent on to addresses found in the victim's address book, spiked with an attachment containing malware. In other words, the message contents have been borrowed from a genuine thread, which makes it more difficult to identify the message as malicious. The malware thus spreads from one victim to the next along the thread, relying on trust between the victims. Malicious messages generated in this manner may even be as credible as spearphishing messages sent by state sponsored actors.

Organisations exposed to increasingly serious threat

Victims of big game hunting in Europe have included the Danish health technology manufacturer Demant, the Norwegian aluminium company Norsk Hydro, the German automation technology manufacturer Pilz, the French TV channel M6 and the Spanish media group Prisa.

Ransomware attacks result in soaring costs. According to its own reports, Norsk Hydro incurred total costs of EUR 55 to 65 million in the first half of 2019. Demant, on the other hand, estimated that its costs were even higher, or close to a hundred million dollars.

Attackers deliberately hamper recovery

As a criminal group gains a foothold, it tries to spread the infection in the target organisation stealthily and as widely as possible. Recovering from such an attack by ordinary methods is very difficult. Once the malware has beenactivated, strong encryption is used to hold the system to ransom, often making decryption with today's tools impossible. Criminals typically also hamper recovery from an attack, for example by encrypting not only files and systems but also backup copies and centralised access control data. The attacker then demands a substantial ransom amount in exchange for the encryption key. In publicly reported cases, ransom demands of up to half a million euros or more have been known.

There are several methods used to initially infiltrate an organisation's systems and spread the malware in its intranet. Comprehensive information security management and ensuring a good basic level of security in all areas are thus emphasised in protection.

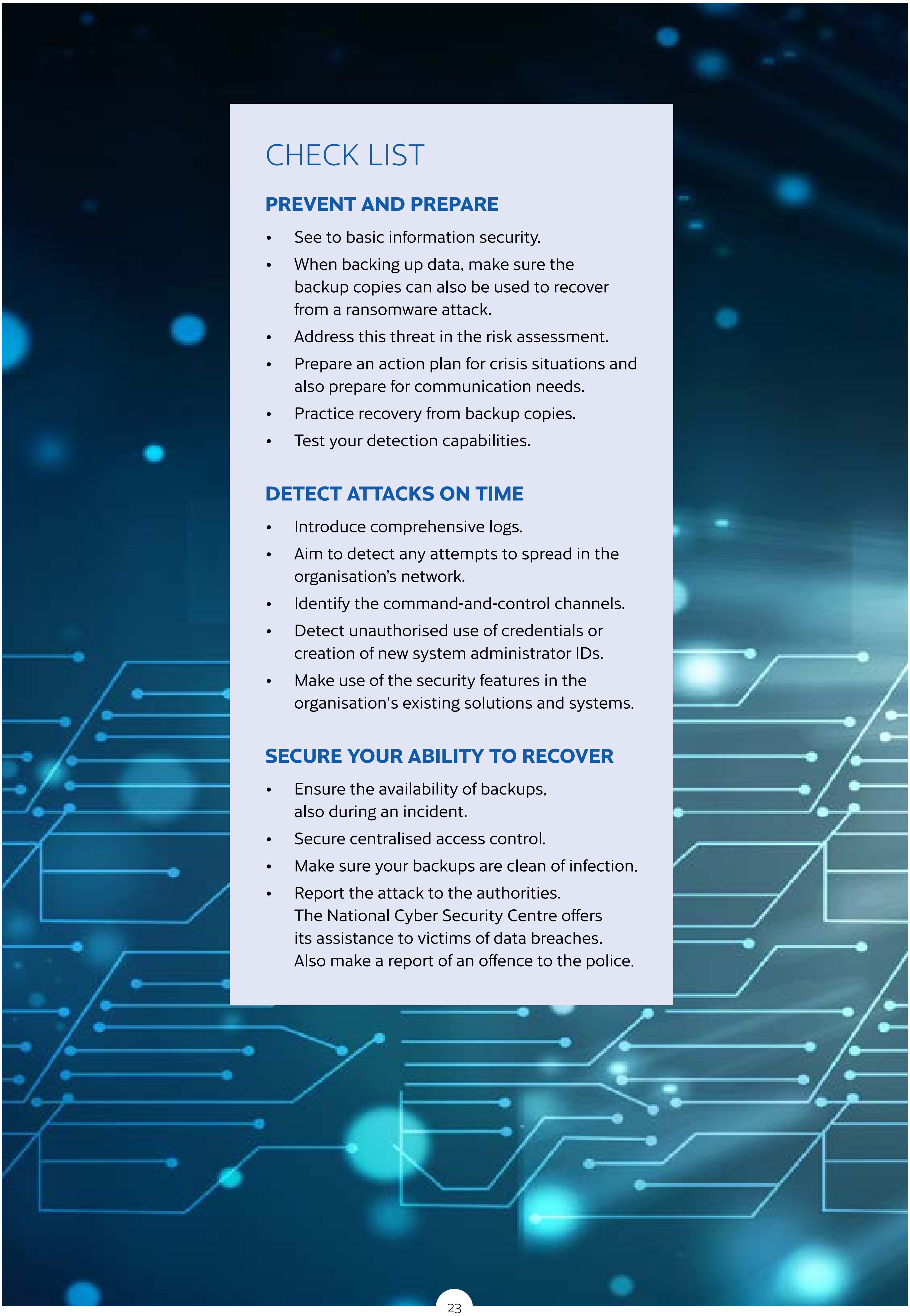
If an attacker gets their foot in the door anyway, however, it is very important that the organisation is able to detect anomalous events and attempts to spread the infection before encryption is initiated.

Sometimes this is not enough, and the attacker goes ahead to the encryption phase. In this case, practiced recovery methods and backups that can be deployed even in an extensive incident will be helpful. These backups must be protected and kept out of reach for attackers, even if they waited for the right moment in the systems.

Paying the ransom encourages criminals to find more victims

Likely targets are difficult to identify in advance. Indications of criminals being particularly interested in large and solvent companies and organisations whose production activities can be significantly hampered by ransomware have been seen globally. Such fields as regional government, municipalities and the healthcare sector have also been in the line of fire.

It is impossible to say whether ransomware cases will become more common in Finland. As long as no ransom is paid to attackers, the message is that cybercrime does not pay. This would mean that Finland will not become an attractive target for attackers. On the other hand, if paying the ransom becomes a common practice, criminals will quite certainly also have a field day.



CHECK LIST

PREVENT AND PREPARE

- See to basic information security.
- When backing up data, make sure the backup copies can also be used to recover from a ransomware attack.
- Address this threat in the risk assessment.
- Prepare an action plan for crisis situations and also prepare for communication needs.
- Practice recovery from backup copies.
- Test your detection capabilities.

DETECT ATTACKS ON TIME

- Introduce comprehensive logs.
- Aim to detect any attempts to spread in the organisation’s network.
- Identify the command-and-control channels.
- Detect unauthorised use of credentials or creation of new system administrator IDs.
- Make use of the security features in the organisation's existing solutions and systems.

SECURE YOUR ABILITY TO RECOVER

- Ensure the availability of backups, also during an incident.
- Secure centralised access control.
- Make sure your backups are clean of infection.
- Report the attack to the authorities. The National Cyber Security Centre offers its assistance to victims of data breaches. Also make a report of an offence to the police.

Data breaches and data leaks

Office 365 scams stand out among last year's incidents. Office 365 data breaches mostly leverage credentials obtained by phishing. The purpose of data breaches is to gain access to confidential data, to commit invoicing frauds using stolen data, or to perpetrate new data breaches using stolen credentials.

> ” Several Finnish municipalities were victims of data breaches during the summer. For the data breaches and cyber security situation in the municipal sector, see the dedicated article on page 34.

Data breaches in municipalities in summer 2019

Cases of cyber criminals targeting large companies or public administration organisations became more widespread in the spring. By disrupting their activities, the attackers may attempt to extort considerable amounts of money. The targeted organisations have incurred significant losses from this phenomenon known as big game hunting. For more information on this topic, see page 34.

Unclear division of responsibilities results in data breaches

When an organisation is planning outsourcing and service agreements, the responsibilities for maintaining and updating systems and software should be considered carefully. In 2019, we were informed of many data breaches caused by a failure to update systems or hardware in cases where responsibility for maintenance was not clearly assigned. In a multi-operator environment, not only responsibilities but also the rights to shut down systems and process logs should be agreed on in advance. Joint exercises with service providers are usually a good way of clarifying responsibilities for maintenance and problem situations.

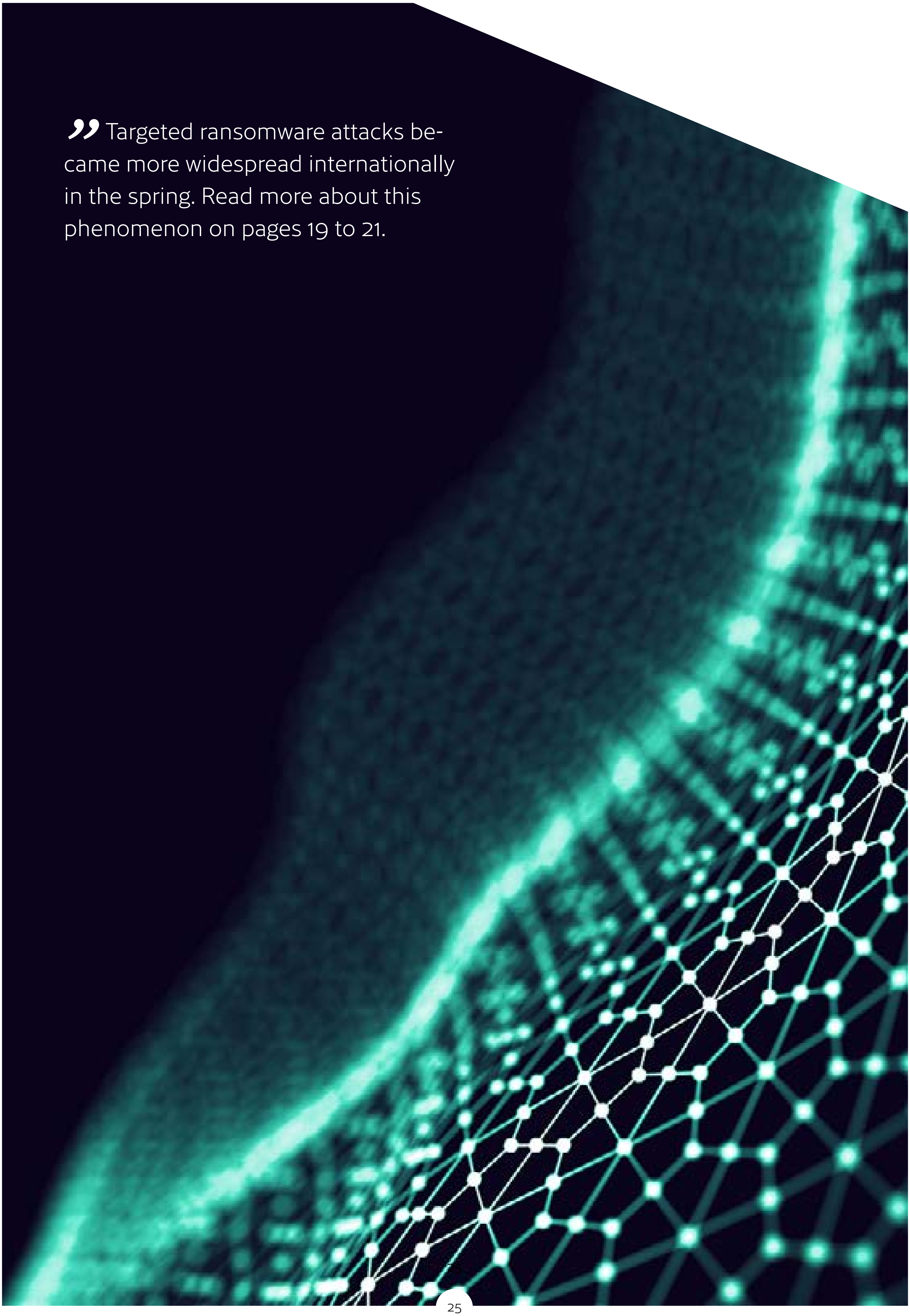
Instructions for employees and shared practices prevent data leaks

The processing of protected data in such environments as public cloud services may result in a data leak risk. Employees should also be issued with instructions on what to do during business travel, for example, to ensure that sensitive data does fall into the lap of cyber criminals. Unfortunately, the lack of the organisation's own solutions or practices, or their failure, may result in situations where taking the easy way out creates a data leak risk.

Data breach is an offence

The more reports of data breaches and leaks we receive, the better we can update our situational awareness of cyber security and help other victims. Organisations should remember that a data breach or an attempted breach is an offence, and we recommend that you report these incidents to the police. Please remember that if personal data ends up in the wrong hands as a result of a data leak, you must report it to the Data Protection Ombudsman.

”Targeted ransomware attacks became more widespread internationally in the spring. Read more about this phenomenon on pages 19 to 21.



Phishing and scams

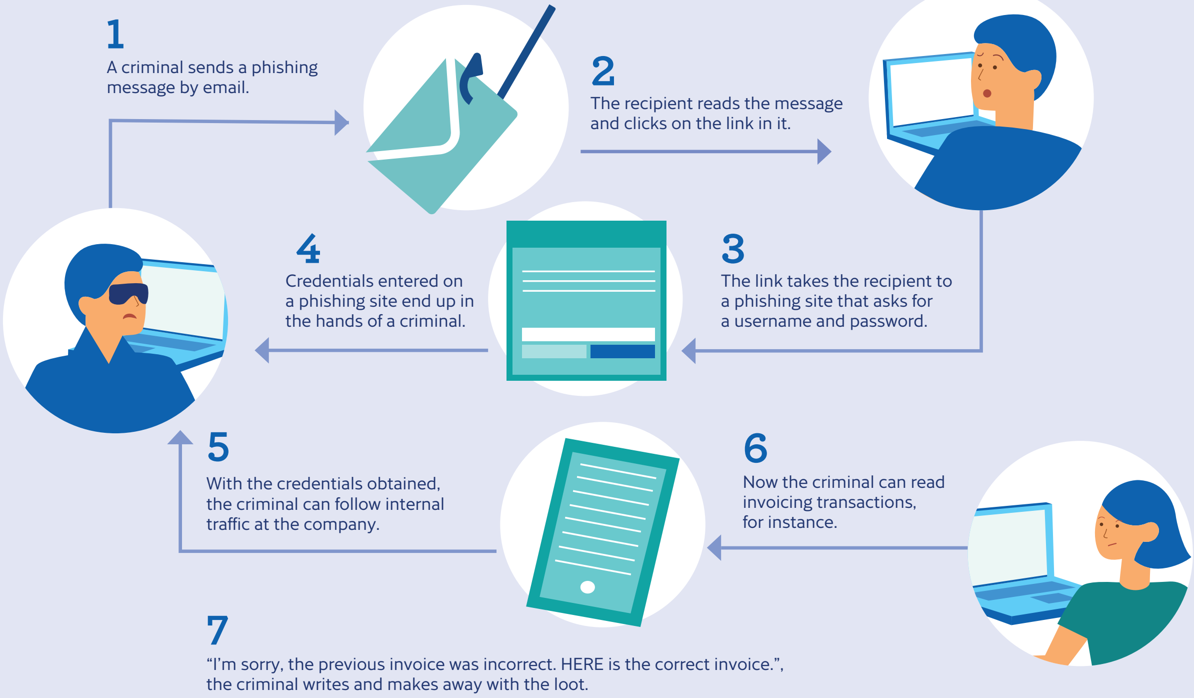
Phishing of user IDs and passwords was par for the course in 2019. Scam messages directed recipients to various phishing websites. Many different ploys were seen: accept your bank's new terms of use compliant with the directive; open the file distributed by your colleague on the intranet; log in to the service again; verify your login to the cloud service or social media account. In none of these cases was the link provided in the message genuine; they were sent by scammers. Any banking credentials and passwords entered on such phishing sites thus ended up with scammers who used them for data breaches. Regrettably, such cases were commonplace in 2019.

Office 365 phishing and data breaches are a fact of life

As early as June 2018, we published an alert about attempts to phish Office 365 email credentials. The alert remained in effect for more than a year, until we finally took it down on 16 September 2019. This phenomenon is no less common or eliminated, however, as Office 365 credentials are still stolen by criminals every day. We took the warning down in the autumn because there were fewer reports of new ways of exploiting these credentials. The threat of phishing and data breaches has not diminished, however, and we continue to receive reports of Office 365 breaches almost every day. In addition, credentials obtained by phishing have been used more rapidly in data breaches in the past year, and this trend is expected to continue.

In summer 2019, we published the guide Protection against Microsoft Office 365 credential phishing and data breaches, which is available on our website in Finnish and English. The introduction of multi-factor authentication is particularly helpful in protecting yourself, and when implemented correctly, it helps prevent the use of credentials which have ended up in the wrong hands. According to Microsoft, almost all Office 365 data breaches could be blocked by means of two-factor authentication. It unfortunately looks as though Office 365 data breaches will also continue in 2020. When maintaining the Office 365 environment, similarly to other cloud solutions, we recommend the use of separate maintenance IDs, in which case less damage is caused to the entire cloud solution if the credentials are stolen.

Phases of an Office 365 scam



1 A criminal sends a phishing message by email.

2 The recipient reads the message and clicks on the link in it.

3 The link takes the recipient to a phishing site that asks for a username and password.

4 Credentials entered on a phishing site end up in the hands of a criminal.

5 With the credentials obtained, the criminal can follow internal traffic at the company.

6 Now the criminal can read invoicing transactions, for instance.

7 “I'm sorry, the previous invoice was incorrect. HERE is the correct invoice.”, the criminal writes and makes away with the loot.

Hacked email accounts as scamming tools

The year 2019 also brought us CEO scams and other invoicing fraud cases. The stream of fake emails and spoofed messages was never-ending. Scam messages were also sent from hacked email and social media accounts. In cases known as CEO scams in Finland, a person pretending to be the CEO approaches the officer responsible for payment transactions in the organisation and asks for a payment to be made quickly to an account, usually one in another country. The fraudster appeals to urgency and confidentiality, says they are in a situation where it is difficult to communicate, and insists on rapid action.

In addition to companies, all types of organisations from sports clubs and libraries to hospitals and parishes have been targeted by CEO scams. Faking such messages and making them look like they were sent by the real CEO is easy, not only on email but also on other messaging channels. New tricks in 2019 have included requests to replace accounts into which salaries are paid by those belonging to fraudster as well as purchasing gift cards for various online services and sending the codes to the fraudster. Especially when a gift card is bought as a business gift, a certain amount of secrecy is part of the bargain and helps the fraudster sound credible.

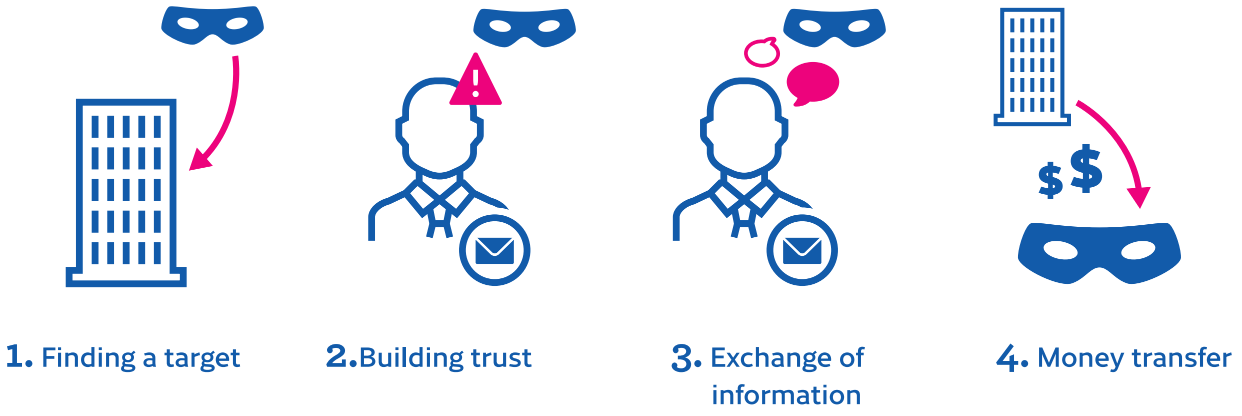
Do not trust text messages

The share of text messages in all scams continued to grow in 2019. For example, subscription scams as well as investment and money laundering scams landed into mobile devices as text messages. We have already learned to consider email as a channel for scammers, but text messages do not yet have the same reputation. The scammers knew how to make the most of this perception. A text message you read on your smartphone may contain links that take you to untrustworthy phishing and scamming sites just as quickly as emails.

The largest text message scam campaigns, which were operated under the name of the postal services, were already seen at the beginning of the year and in the spring. A forged message informing the recipient of the arrival of a consignment appeared on the recipient's phone in the same thread as genuine text messages from the postal services, which was why they seemed credible. You should suspect a scam, however, if a link sent by ‘postal services’, instead of taking you to a notification of a parcel, brings you to a competition, a draw or the opportunity to buy for one euro entertainment equipment costing hundreds.

In addition to subscription scams, text messages were also used to phish banking credentials and bypass strong identification.

Many paths lead to a subscription trap: advertisements, scams, social media messages, text messages, online searches, chain letters. The lure can be a prize draw, competition, survey, notification of the arrival of a parcel or some other message, but the end result in most cases is the same: the victim is persuaded to believe they have participated in a competition and won a prize, such as a telephone or television for one euro, but the small print shows that the consumer has now committed to paying a monthly fee for a service they do not need. While victim does not get the prize they looked forward to, the scammer who went off with their credit card number collects 80 euros each month.



BEC – Business Email Compromise, or invoicing fraud.

SCAMS OBSERVED IN FINLAND IN 2019

EXAMPLES OF EXTORTION SCAMS

- **Porn extortion scam:**
The victim receives an email in which the scammer claims to have hacked into their computer and installed on it spyware which, for example, has recorded the victim watching adult entertainment. The scammer demands a ransom for not publishing the sensitive recording. Sometimes an attempt is made to add credibility to the extortion by referring to a past password leak: "I have your password, so you know I am telling the truth.”

- **Death threat scam:**
The scammer claims to be a contract killer hired to murder the victim. Once again, the victim could get off the hook by paying a large sum of ransom money.

- **Spam extortion:**
A scammer threatens to ruin the company's reputation by launching a huge spam campaign under the company’s name unless a ransom is paid.

- **Denial of Service extortion:**
The blackmailer threatens to flood the company's information network with a large volume of traffic unless the company pays a ransom. In some cases, these threats may come with a short DoS attack carried out by cyber criminals as a free sample.

EXAMPLES OF INVOICING FRAUD

- **CEO scam:**
The scammer pretends to be the organisation’s CEO and approaches the financial officer by an email, social media message or other. The idea is to persuade the officer to transfer money to the scammer's account under some pretext.

- **Mandate fraud:**
The fraudster pretends to be a manager and asks the payroll officer to replace the details of the account into which their salary is paid by the fraudster’s account details.

- **Gift card scam:**
The fraudster impersonates a manager and makes a request to organise some gift cards quickly. Once the fraudster has access to the card codes, they can be converted into money.

Internet of Things

The Internet of Things, which used to be considered a phenomenon of the future, is today part of our daily life. Various entertainment services, sports events and consumer technologies have familiarised us with smart devices. Services can also be provided on platforms which were not available in the past, including soft toys which double as a baby monitor and have a remote monitoring feature, or voice command devices used to control your home. Outsiders may gain access to both video and audio material through vulnerabilities in such devices.

Devices connected to the Internet remain vulnerable. No improvement in the security of firmware was achieved in 2019, either. An extensive study carried out by information security company Cyber ITL (https://cyber-itl.org/2019/08/26/iot-data-writeup.html) showed that manufacturers of Internet of Things (IoT) products keep repeating the same mistakes in their products year after year, and no improvement has taken place in more than a decade.

Insecure IoT devices also in Finland

We also come across many vulnerable IoT devices connected to the Internet in Finland. For example, devices with information security deficiencies can be harnessed to bot networks to amplify denial-of-service attacks. IoT devices played a particularly large role in amplifying the Mirai bot network in 2019. The unfortunate fact is that as the Internet of Things becomes more widespread, criminals find new opportunities for making money.

The information security level of IoT devices has been poor so far. Fortunately, the need for international IoT standards has been put on the agenda both in Europe and the United States. The situation of consumers and companies indeed improved in late 2019, for example as new regulation and the Cybersecurity label were introduced. We hope they will support as many consumers as possible with their decisions on purchasing smart devices.

Up with testing! Better IoT starts in the product development phase

IoT has brought not only benefits but also security challenges. These challenges must be addressed before an IoT device is connected to the Internet.

The challenges vary by device. The security challenges related to devices used for locking up your home, for example, are considerable. The best way to respond to these challenges is addressing information security features already in the design and development phase.

More research will be required to assess the overall situation and challenges. However, we can say that a solid foundation will help maximise the benefits of IoT technology. A secure Internet of Things is underpinned by security-conscious software development, careful testing and regular updates of the technologies.

In addition to the challenges, services provided using IoT devices have plenty of potential.

Key information security risks for individuals, organisations and central government

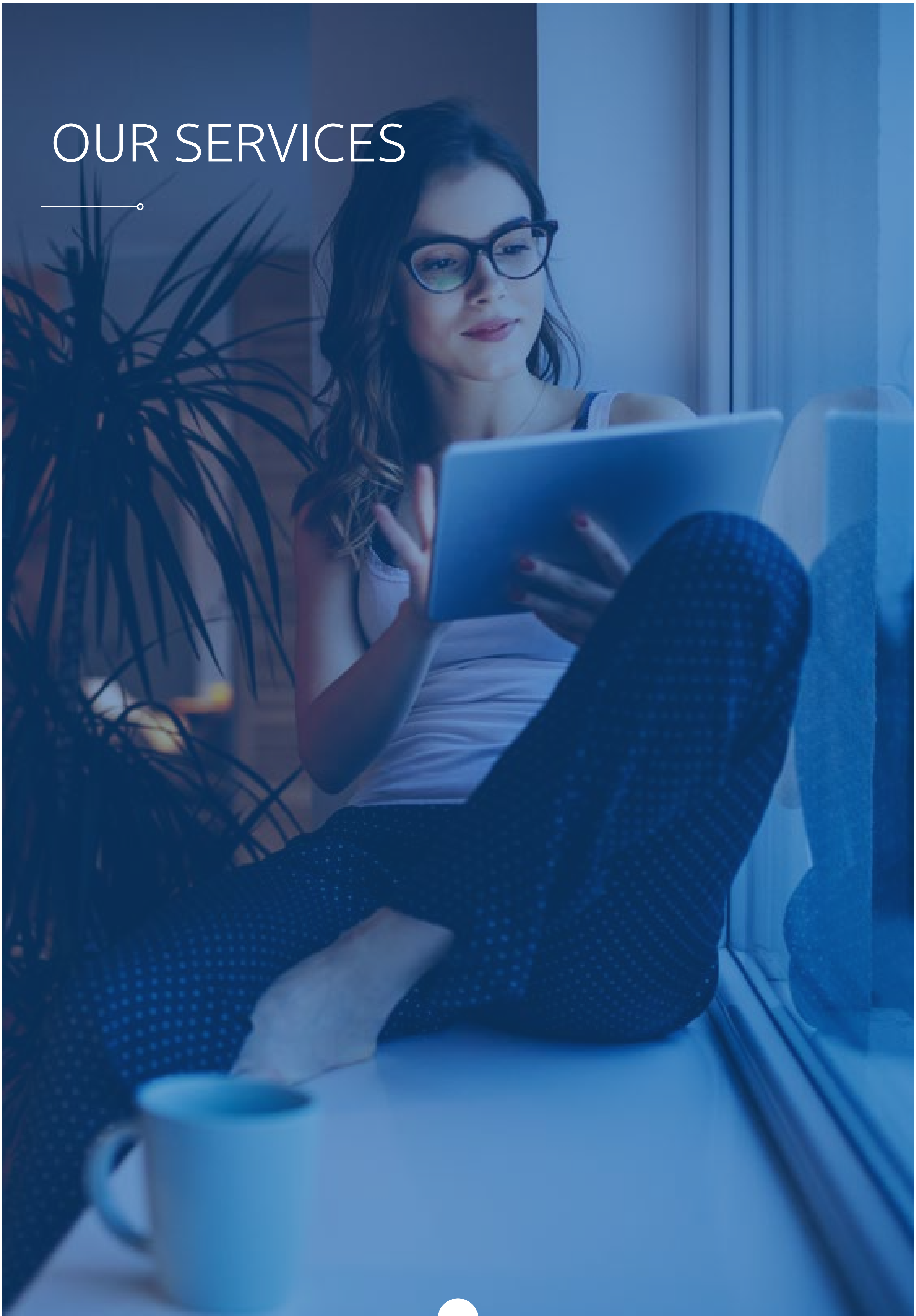
This is our evaluation of the most significant risks related to key cyber security phenomena in 2019. We have highlighted examples of cases showing how the risks might have been seen by individuals, businesses, municipal organisations and central government.

The direction of the arrow describes the trend of the situation compared to 2018. In our view, the general cyber security risk level in Finland in 2019 remained almost unchanged compared to 2018. Rather than having diminished, the threats associated with the risks have remained unchanged or become more serious.

= The risk has remained unchanged ▲ The risk has grown

NETWORK FUNCTIONALITY	= While the use of digital services is growing, people are not fully dependent on their operation.	= An increasing number of organisations are prepared for ICT service incidents. However, the contingency measures are not always sufficient.	▲ Maintaining old ICT systems takes up resources that could be used to improve the reliability of, maintain and develop shared systems.
DENIAL-OF-SERVICE ATTACKS	= Compromised home routers and other IoT devices continue to be used for DoS attacks.	= Organisations should prepare for DoS attacks when planning and procuring network services.	= Public services are a regrettably popular target for DoS attacks. The functioning of critical services, in particular, should be secured in all situations.
ESPIONAGE AND INFLUENCING	= The likelihood of Finnish persons being targeted by espionagehas remained largely unchanged. Dissidents and political influencers with connections to authoritarian countries risk being spied on.	▲ Companies are targeted by espionage to advance both economic and political goals. By interfering with organisations' activities, an effort can also be made to influence society.	= Governmental organisations remaina significant target for espionage. Spies attempt to gain political ground, acquire information on decision-making, assess preparedness level and capabilities, and prepare for other types of unwanted influencing.
MALWARE AND VULNERABILITIES	= Vulnerable IoT devices get infected quickly by malware. Automated software updates are becoming more commonplace.	= Attackers seek and quickly hack into devices exposed to the Internet. Vulnerabilities of industrial automation devices have also been exploited.	▲ In particular, the importance of managing vulnerabilities and maintenance have been emphasised.
DATA BREACHES AND DATA LEAKS	= The risk of data breaches has remained almost the same since last year. The number of major credential leaks has gone up.	▲ Ransomware cases are more common. Especially the number of O365 breaches grew.	▲ The central government is subject to the same threats and risks as other organisations. The number of data breaches and data leaks has increased.
SCAMS AND PHISHING	▲ Scammers are growing more skilful. Extortion scams, phishing for banking credentials and subscription scams are becoming increasingly difficult to thwart.	▲ Unfortunately, cases of phishing for company account details may not have yet reached their peak.	= CEO and invoicing scams are also common in central government, but the risks are understood better.
INTERNET OF THINGS	= The security of consumer product software has not improved for years. The Cybersecurity label and improving standardisation support consumers in choosing secure devices.	▲ Firmware security has not improved for years.	= The challenges remain unchanged, and entirely new major risks have not emerged.

OUR SERVICES

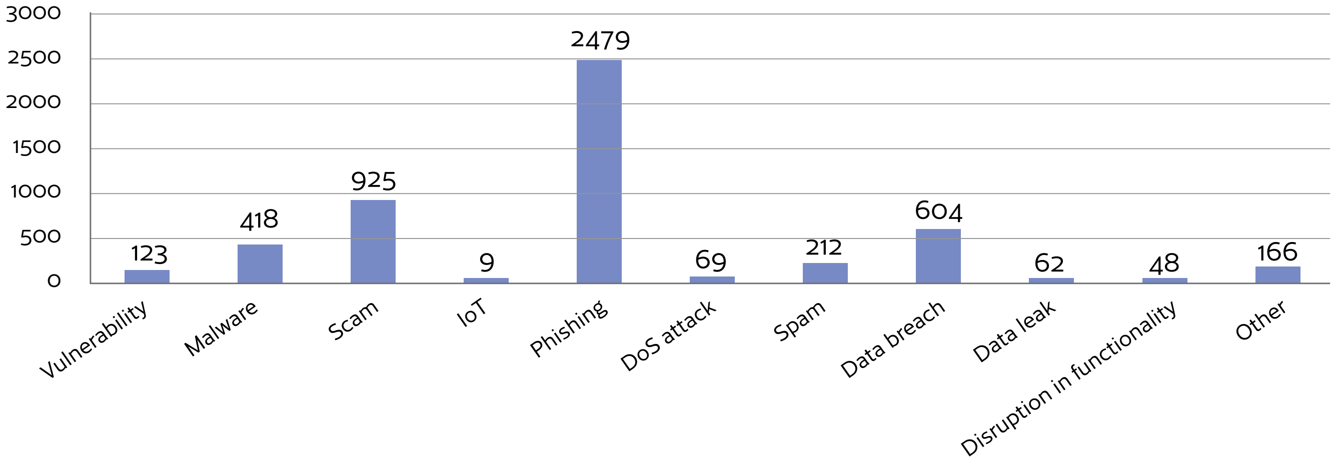


Coordination centre handles thousands of cases every year

Our Coordination centre advises and supports numerous victims of security breaches daily. Individual citizens and large enterprises or municipalities alike may need assistance. Our service is known as incident response (IR).

The severity of an information security incident is assessed by two persons. We are often able to provide assistance already during the initial contact. Cases requiring detailed technical analysis or coordination over a longer time span are transferred to a more detailed review.

Fast operating methods – which, in the best case, have also been practised in advance – and knowledge of your own environment and systems will be helpful if you happen to be attacked.



In 2019, our Coordination centre handled around 4,500 cases. The numbers in the graph do not include cases processed automatically by our Autoreporter system.

We deal with thousands of cases every year. Office 365 cases, in particular, increased the number of data breach incidents. Various scams, including subscription scams in emails and text messages, have been an additional nuisance this year.

Our most memorable customers in 2019 were the municipalities of Kokemäki, Pori and Lahti. They got first-hand experience of what it is like to be targeted by a cyberattack.

In all three cases, the cities reported the incidents to our Coordination centre as soon as they discovered what was happening. This gave us optimal possibilities to support and advise the cyberattack victims.

With Lahti and Kokemäki, we held regular meetings to discuss the current situation, the recovery or protection measures taken, and the plans for further actions.

Municipalities have an important role in providing everyday services and protecting residents

When municipal services work, no one takes any notice. Municipalities have a duty to maintain many different services. Several Finnish municipalities were targeted by a cyberattack in 2019, and the cyber security of municipalities came up as a discussion topic.

The standard of cyber security in municipalities varies, and there are major differences regarding the availability of both financial and personnel resources. The problem often lies in a lack of adequate investment in cyber security. Services are implemented inexpensively and with no plans for their maintenance.

Cyberattack still hampering health services in Lahti National Bureau of Investigation: "We will do everything we can to catch the agents of evil" YLE news 13 June 2019

"Blackmailers demand a ransom from the City of Kokemäki – malware has the city's network on its knees"

YLE news 30 July 2019

"Another data breach in Satakunta: City of Pori the latest target"

YLE news 8 August 2019

To save resources, municipalities also make maintenance as simple as possible, which may mean operating a number of service packages in a single network. Consequently, an attack against the network can cause widespread impacts in one fell swoop.

A busy cyber summer for the cities of Kokemäki, Lahti and Pori

An attack targeting the city's information network in Kokemäki hampered and disrupted the city's service provision and functions extensively. For example, the attack disabled the city's emails and payment transactions.

In Lahti, the direct costs of the attack against the city's information network had reached approx. EUR 900,000 by the turn of the year. The amount of indirect costs is also put at hundreds of thousands of euros, as the users could not do their work while the network was down. As a precaution, the City of Lahti had to be disconnected from the network of Päijät-Häme Joint Authority for Health and Wellbeing.

While the attack in Pori caused less damage, things could have been much worse.

During the summer and autumn, we participated in investigating the cyberattacks on the municipalities of Pori, Lahti and Kokemäki. A common denominator for these cases was direct impacts on ICT services, in particular. The targeted municipalities sustained a data breach, in which malware was used to gain access to the municipality's information network. Rather than going after these municipalities specifically, the attackers caught in their net easy targets with a low level of information security. This allowed them to achieve significant impacts with little effort.

In the most serious case, the attacker was able to operate within the network due to inadequate network segmentation and widely used maintenance rights. On the other hand, the municipality's up-to-date security software responded quickly to the anomalous malware activity, and the highly skilled service provider quickly blocked any additional damage, which could have been significant. Regardless of this, the total costs of the cyberattack amounted to hundreds of thousands of euros, and it had long-lasting effects.

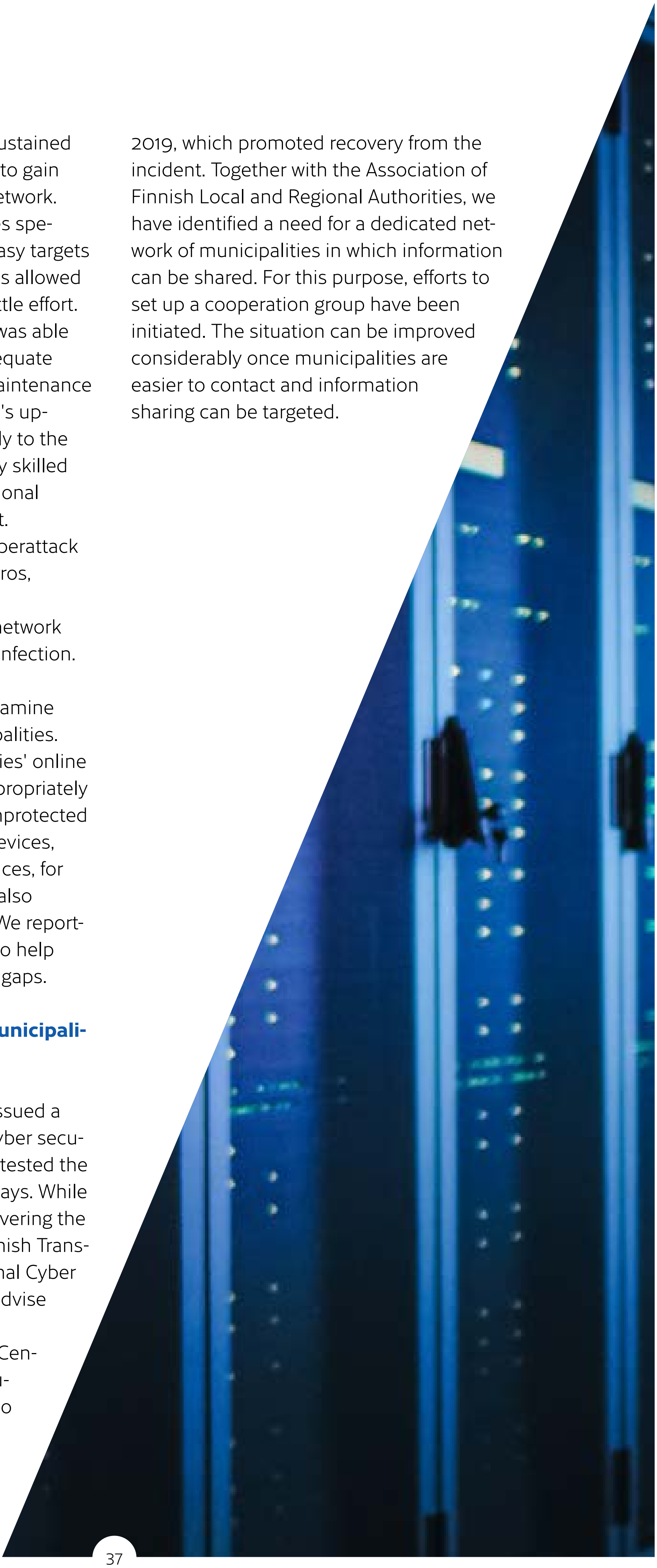
In the other cases, well-implemented network segmentation prevented a wider malware infection. Backups also enabled faster recovery.

The events of last summer led us to examine the level of information security in municipalities. Our observations indicate that municipalities' online environments contain many services inappropriately connected to the Internet. They include unprotected office equipment, network management devices, various database servers and internal services, for example the entire intranet. Problems are also caused by obsolete software and servers. We reported our observations to the municipalities to help them eliminate these information security gaps.

Cooperation and networks support municipalities' cyber security development

In autumn 2019, the Security Committee issued a recommendation aiming to improve the cyber security of municipalities: "Recent events have tested the municipalities' cyber security in different ways. While the responsibility for taking actions and covering the costs rests with the municipalities, the Finnish Transport and Communications Agency's National Cyber Security Centre and other authorities will advise them and support their investigations.“

Currently, the National Cyber Security Centre does not have an overall idea of the municipalities' cyber security status, as they do not have an obligation to report incidents. Some municipalities submitted reports in 2019, which promoted recovery from the incident. Together with the Association of Finnish Local and Regional Authorities, we have identified a need for a dedicated network of municipalities in which information can be shared. For this purpose, efforts to set up a cooperation group have been initiated. The situation can be improved considerably once municipalities are easier to contact and information sharing can be targeted.



Information security regulation and assessments

A mega year of cyber security legislation

Many pieces of legislation relevant to information security and cyber security entered into force in 2019. Among other things, amendments to acts on identification and trust services opened up this field for competition. The entry into force of the Cybersecurity Regulation, on the other hand, put the role of the European Union Agency for Network and Information Security (ENISA) on a permanent footing and enabled the establishment of a European cyber security certification scheme.

The drafting of many other pieces of legislation also continued, including an update making the national Information Society Code consistent with the provisions of the European Electronic Communications Code. An ePrivacy Regulation was also drafted in the EU.

In addition to the legislative projects of the past year, we also supervised and enforced earlier legislation.

Much-needed competition in the identification services market

The amendments to the Act on Strong Electronic Identification and Electronic Trust Services, which entered into force in early 2019, opened up the market for strong electronic identification services for much-needed competition. The so-called identity service brokers were thus able to launch their operations. An e-service provider can now subject identification service providers to competitive bidding and, if necessary, put all means of identification at their customers' disposal under a contract with a single identity service broker. In the past, several contracts were needed. By encouraging competition in the market, the prices paid for services can be reduced and the use of strong identification in electronic services can be promoted. Widespread use of strong electronic identification will help build a safer digital society.

End of the road for TUPAS

The TUPAS protocol, which Finnish people have got to know from online banking and which has a long history in strong electronic identification, reached the end of its story. Developed in Finland, TUPAS was an advanced strong electronic identification solution. A decision to give it up was made, however, because it no longer met modern security requirements for strong electronic identification. It was replaced by OIDC and SAML protocols, which meet the current requirements and are widely used internationally. This development is an apt reminder of how systems and services need to be constantly developed with both current and future safety requirements in mind.

Focus on regional network reliability

Over the last few years, the recently deployed regional networks and the actors operating them have been a focus of our inspections. Our goal has been ensuring sufficient reliability of the networks, and the services offered across the networks, from the word go. Regional networks refer to dozens of local fibre networks built by different local groups to provide broadband connections.

In the inspections, we go through the requirements related to telecommunications network functionality, its power supply, earthing and incident management. The aim is to improve the actors' awareness of the minimum requirements and to provide them with advice on improving resilience. The operators may also be obliged to remedy any shortcomings identified in the inspections. While the inspection always focuses on an individual operator, we also collect information on the effectiveness of and needs to change regulation. Additionally, the inspections have an important role in developing regulation on operational resilience and the overall security of society.

Cookies in the limelight

The so-called Planet 49 ruling issued by the Court of Justice of the European Union fuelled public discussions on cookies in the wake of the General Data Protection Regulation (GDPR). Unfortunately, this ruling failed to create a clear policy on such cases.

The ruling states that active behaviour on the part of a user is required in order for a data subject to give their consent to using cookies. In addition, the service provider must provide information on the period for which the cookies are stored and whether third parties are able to access the information collected. However, the court ruling does not express an opinion on whether consent should be requested by such means as a pop-up window. It remains to be seen if the pending Regulation on Privacy and Electronic Communications will bring changes to the situation.

Systems for protection of international classified information in great demand

National and international security policy phenomena were also reflected on the targets of our assessment which had a particular focus on protecting international classified information. We assessed a number of environments essential for the functioning of society in which processing of classified information was subject to approval by the national authority. In addition to information processing environments, we approved several new versions of Finnish encryption products.

The general tone of last year in the NCSA-FI was positive, as we were able to support a number of authorities and companies in dealing with their needs related to processing classified information, which in some cases were exceptionally critical. We were able to issue accreditation for our most significant assessment targets of the year. The development of national and international phenomena also predicts extremely interesting challenges in 2020!

A cookie is a small text file which an Internet browser stores on the user's device. For example, cookies make it possible to collect purchases in the shopping basket in an online shop before checking out. Provisions on cookies are laid down in section 205 of the Information Society Code. It is based on the European Directive on privacy and electronic communications, which is to be replaced by a regulation.

NCSC-FI's advisory services were well received – shorter inspection turnaround times

As in the previous year, the need for information security advice grew. In 2019, support and guidance were needed especially for protecting the critical infrastructure of our society and classified information in information systems. The results of our advisory services were seen as higher levels of maturity in our assessment targets which, among other things, shortened inspection turnaround times.

Criteria for assessing cloud service security

Both the public administration and private sector have for long questioned the information security of cloud services. The criteria for assessing the security of cloud services published by us were thus positively received.

The Criteria to Assess the Information Security of Cloud Services (PiTuKri) support the authorities in the application of the new Act on Information Management in Public Administration. It also contains tools for assessing the security of cloud services and the risks associated with them, as well as describe good practices which promote security in cloud services and which can also be used by private sector.

We have received a great deal of good feedback on and suggestions for developing the criteria. In early 2020, we will publish a new version of the criteria based on both the feedback and our observations.

Updated assessment criteria help improve the security of identification services

In 2019, we updated our assessment criteria for strong electronic identification based on experiences gathered from the assessment reports and information security audits. The criteria support the providers and auditors of identification services in developing and evaluating the security of the services. We also rely on these criteria when assessing the security and compliance of both existing and new identification services in the market. While the criteria are primarily intended for those who provide or assess strong electronic identification services, they also lay a good foundation for developing other identification services.

The updated criteria contain a separate section on mobile identification solutions and applications used in identification services. Its aim is to improve the security level of applications currently in use and those to be deployed in the future. The criteria are based on the mobile application standard of the Open Web Application Security Project (OWASP), which in our opinion creates the best starting points for developing secure applications. The criteria could not have been completed without an excellent task group, which consisted of experts representing manufacturers and identification service providers.

Our criteria are unique on the global scale and have also attracted international interest. They have been warmly received by a number of regulatory authorities and operators providing identification solutions and services.

Mobile identification solutions are rapidly becoming more common, and it is obvious that the majority of future solutions will be based on a mobile terminal device and an identification app installed on it. Mobile solutions have also come up in EU Member States' eIDAS notifications and the opinions of the Member States' cooperation network which precede them. In particular, the opinions have highlighted security assessments related to the storage of cryptographic keys and the suitability of biometric verification factors. You can familiarise yourself with our guideline 211/2019 O, Assessment guideline for electronic identification services, on our website https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Assessment_guideline_for_electronic_identification_services_211_2019_O_EN.pdf

Device manufactures discovered the benefits of Galileo

Galileo, the EU-funded global navigation satellite service reached an important milestone in 2019: by September 2019, one billion terminal devices which support the use of Galileo Open Service, mainly smartphones, had been sold. The fact that device manufacturers discovered the potential of Galileo thus was the most significant change trend of the year.

Brexit undermined global coverage

In 2019, the Galileo system relied on a total of 22 satellites, allowing it to reach global coverage. As the United Kingdom announced its intention to leave the EU, Galileo's British ground segment installations – the Galileo Security Monitoring Centre in Great Britain and sensor stations on the Falklands and Ascension Island – were disconnected from the system. To remedy the situation, the construction of a Security Monitoring Centre was launched in Spain.

Planned diversification of services until 2024

Galileo's navigation services are currently in the Initial Services phase. The official launch of the public navigation service, Open Service (OS), will probably take place in late 2021. The other Galileo services will be introduced one at a time following a separate approval process in 2021–2024. The greatest interest will be focused on the High Accuracy Service (HAS) offered free of charge, in which 20 cm positioning accuracy has been promised. The service is considered especially significant for developing autonomous modes of transport.

Outage in July attracted attention

In July 2019, the Galileo services were down for almost a week, apart from the Search and Rescue (SAR) services. This understandably attracted attention not only in professional circles but also in the media. Service users did not notice a major change in their satellite navigation services, as consumer devices typically use all available global positioning satellite systems in parallel, which in addition to Galileo include GPS, GLONASS and BeiDou. The service outage was caused by human error during a system update. The incident was investigated thoroughly, and a

YOU MAY CARRY GALILEO IN YOUR POCKET, TOO

The EU’s Galileo satellite navigation system produces highly precise positioning and timing information. The Galileo system is operated by the European Global Navigation Satellite Systems Agency (GSA) under the steering of the European Commission. You may be a Galileo user, too, as most of the current mobile phones and smart devices designed for consumers already use the signals of Galileo satellites.

number of measures were introduced to ensure that similar errors can be avoided in the future.

Galileo capability in US devices improved accuracy and reduced interference

Once the use of Galileo frequencies was approved in the United States, device manufacturers in that country started capitalising on Galileo in 2019. The capability to receive Galileo signals, which had up till then been inactive in some US-produced devices, could be enabled by software updates. Smartphones and other advanced mobile devices equipped with processors able to receive Galileo signals on two separate frequency bands were launched.. This had a positive impact on not only positioning accuracy but also signal reception in cities. The most widespread processor of this type was Qualcomm’s Snapdragon 855.

Work on Galileo continues, with additional responsibilities for NCSC-FI

As the competent Finnish PRS (Galileo Public Regulated Service) authority, we continued to prepare for PRS deployment under the guidance of the Ministry of Transport and Communications. Several branches of administration in the central government as well as companies responsible for services critical for society brought up their need to introduce a verified positioning and timing service. The plan is to launch the design of service architecture enabling national PRS use in 2020.

In 2019, the Ministry of Transport and Communications also transferred the responsibility for preparing the operative activities of other Galileo services to the NCSC-FI. In late November and early December 2019, we organised a large-scale Galileo Innovation Challenge event, which drew a big and international group of participants to Helsinki. At this event, new modes of use for Galileo's services were developed, incident detection techniques were examined, and innovations related to integrating Galileo's services with robotics were brainstormed. The event was part of the Efficient deployment of satellite navigation systems in Finland action plan published by the Ministry of Transport and Communications in 2017.

Cooperation and sharing of information

Summary of our information sharing groups' news

Our information sharing groups, or ISACs (ISAC=Information Sharing and Analysis Centre), are cyber security cooperation bodies established in different sectors. Their main purpose is to share information and experiences, thus improving organisations' and sectors' ability to protect themselves against digital threats.

We draw on information produced by the ISACs to form the national situational awareness of cyber security.

See below for the most important news and highlights of the different sectors in 2019.

SECTOR	SPECIAL CHARACTERISTICS	NEWS
CENTRAL GOVERNMENT	Central government organisations face the same information security threats as other actors. Following the agreed practices has saved government actors from many scams, including invoicing scams (BECs).	Preparation for the elections and EU Presidency were the highlights of 2019. The PiTuKri criteria and Cloud Strategy helped form a shared view in discussions on cloud services. The new cyber security strategy strengthened leadership in national cyber security.
FINANCE	The activities were launched in spring 2019. The members are active and work together to develop the sector. Fraudulent messages sent in the name of banks and DoS attacks against operators are commonplace.	The TIBER-EU framework recommended by the EU guides the sector to organise regular and scenario-based exercises related to threats. The exercises should be based on situations that are as realistic as possible. The TIBER-FI framework is being updated, and together with the NIS Directive, it will be part of the framework of recommendations and regulations applicable to the operators.
WATER SUPPLY	Well-functioning automation systems are at the core of the business, and protecting and maintaining them is thus a priority.	The group has completed its first year. It has shared experiences, guidelines, information and tools for improving cyber security. A continuation of the KYBER-VESI project of 2018 is being planned. The ISAC will also participate in this.
TELECOMMUNICATIONS OPERATORS (ISP)	Telecommunications companies and Internet access points have a special role in detecting information security threats. Threat scenarios being discussed include DoS attacks and malicious Internet traffic routing changes..	Information on recent cases was shared, the business impacts of regulation were discussed, and development of practices in order to respond to new cyber security threats was considered. In summer 2019, ISAC chairmanship was transferred from Traficom to the sector.
SOCIAL WELFARE AND HEALTHCARE	The confidentiality and data protection of patient and client information are continuous challenges which are resolved, among other things, by means of information security. The Ministry of Social Affairs and Health published the first national cyber security guidelines for the social and health sector. The Ministry is working on a national operating model for reporting cyber security incidents and creating situational awareness in the sector.	Dissemination of the Kyber-Terveys project's results began. New development projects are being planned. EU regulation on medical devices will change, as a result of which cyber security requirements will be introduced. The Act on Information Management in Public Administration brought new information security requirements to the social and health sector.
ENERGY	The sector has plenty of both joint and operator-specific exercise activities. The extremely strong trust between operators enables active sharing of information.	Perspectives related to IoT and cloud service use and information security. Exchange of views on the NIS Directive and cyber security maturity assessments associated with it. The sector tested the Cyber meter assessment tool produced by the NCSC-FI and the National Emergency Supply Agency, which enables companies to carry out self-assessments of their cyber security maturity level.
CHEMICAL AND FOREST INDUSTRY	The international nature of the activities and strong dependence on automation systems.	Office 365 scams kept cropping up throughout the year. Dependence on service providers and their processes was a particular talking point.
FOOD INDUSTRY AND RETAIL DISTRIBUTION	Food production as well as the trade and distribution sector are fully digitalised. Using automation, robotics and IoT to improve business efficiency is commonplace.	In this sector, operators were also pestered by O365 scams, in particular. The introduction of new technologies in business processes additionally takes place at a fast pace. This poses significant challenges to proactive information security management.
MEDIA	The reliability of network connections and systems in both fast-paced news work and electronic communications are highlighted in the sector. In addition, the activities and journalists are the object of interest which companies must also address as part of their information security.	Preparedness for cyber threats in the media sector has been strengthened by both personnel training and IT innovations, such as the use of cloud solutions.
LOGISTICS AND TRANSPORT	As a result of the strong digitalisation development in transport and logistics, a need to increase information sharing in the sector has been identified.	L-ISAC was launched in early 2019, and networking has got off to a good start.

Network and Information Security Directive (NIS): For the first time, EU Member States to notify information security incidents significant for society

2019 was the first full calendar year following the entry into force of the Network and Information Security Directive (May 2018). In February 2020, EU Member States reported for the first time on information security incidents important to society having occurred during the entire year 2019. The reported information is used to develop cyber security both at the national and EU level.

The NIS Directive imposes minimum obligations on the providers and operators of essential infrastructure regarding risk management of network and information systems, monitoring of information security, and reporting. These obligations have been transposed into national sectoral laws. In Finland, the obligations and the operators to which they apply are supervised by sector-specific authorities. Any incidents are also reported to us at the National Cyber Security Centre.

> ” In 2019, Finland notified one significant information security incident in the healthcare sector. Eight other significant incidents were notified.

In 2019, Finland notified one significant information security incident in the health care sector. It consisted of a cyberattack and data breach targeting the local government sector (read more on pp. 36 to 37). Eight other noteworthy incidents were notified for 2019. All in all, they were very similar to incidents in 2018, which concerned Office 365 phishing, hacked passwords, and unauthorized system logins. Finland did not notify any significant information security incidents between the Directive's entry into force in May 2018 and the end of that year.

The NCSC-FI is Finland's single point of contact for information sharing between EU Member States. We also coordinate national and international cooperation. The sector-specific supervisory authorities in Finland established an NIS cooperation network, which met four times in 2019. A common electronic incident reporting form is available to operators on our website. The network has also produced presentation materials and press releases for the operators.

Form for reporting significant network and information system incidents for operators of essential services:
https://www.kyberturvallisuuskeskus.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus

Energy

Energy Authority

- Operators of the electricity distribution network and high-voltage distribution network
- Electricity transmission system operator: Fingrid
- Gas transmission system operator: Gasum

Healthcare

National Supervisory Authority for Welfare and Health Valvira

- Social and health service providers
- Medical device manufacturers
- Information system manufacturers for social and healthcare sector

Financial sector

Finnish Financial Supervisory Authority

- Banks
- Central units of banks
- Branches of EU banks

Financial sector infrastructure

Finnish Financial Supervisory Authority

- Stock exchange: Nasdaq

Transport

Traficom

- **Aviation:** Air Navigation Services Finland, Finavia Helsinki-Vantaa Airport
- **Shipping:** Vessel Traffic Services Finland Oy; Ports of Turku, Naantali, Hamina-Kotka and Helsinki
- **Rail transport:** Finnish Transport Infrastructure Agency as the rail network operator, Finrail Oy
- **Road transport:** Traffic Management Finland as the traffic management company

Water supply

Ministry of Agriculture and Forestry ELY Centres

- Water production plants which supply receive over 5,000m^3 of water a day

Digital infrastructure

Traficom, National Cyber Security Centre Finland

- Telecommunications operators (DNS)
- Internet exchange points (IXP)
- DNS domain name service providers
- .fi country code register

Digital services

Traficom, National Cyber Security Centre Finland

- Cloud services
- Search engines
- Online marketplaces

Not applicable to small/micro enterprises

The obligations to notify data breaches and information security incidents apply to operators in the energy, transport, financial and healthcare sectors as well as water production plants supplying/receiving more than 5,000 m3 of water a day. The Directive also applies to digital service providers, or large and medium operators providing cloud computing services, online search engines and online marketplaces.

Peaceful elections and smooth EU Presidency underpinned by routine cooperation

Preparedness pays, even if reliability of election results is not a concern

Two elections were held in 2019 – national parliamentary elections and European Parliament elections. Elections are one of the fundamental pillars of democracy. Finnish elections are some of the safest in the world, if not the safest.

Safety is a feeling that can be eroded when we are faced with different threats and risks. Among other things, it is influenced by trust in the authorities' ability to prevent security threats. Such elements as being able to trust the election process play a key role in this. We wished to be involved in fostering this trust together with other key election authorities, ensuring that election interference, which is seen in many countries of the world, cannot gain a foothold in Finland.

In Sweden, a denial of service attack targeted the election results system in the 2018 elections. In France, a party's information systems were hacked in an effort to create a scandal based on a data leak in 2017, to say nothing about the US presidential elections in 2016.

One DoS attack was observed during the Finnish parliamentary elections, which the National Bureau of Investigation is investigating as a suspected case of aggravated interference with communications. The other cases of election interference targeted individual candidates.

Our ability to conduct elections almost without incident was underpinned by close cooperation between the authorities, in which the NCSC-FI was able to participate. Thanks to this cooperation, each organisation's role during potential incidents was clearly defined. Everyone knew whom to contact if problems did arise.

Finland's Presidency of the Council of the EU

The elections went well, but more sustained efforts were required after a short breather of a few months. From July till December 2019, Finland held the Presidency of the Council of the EU. During this six-month period, several meetings of ministers and public servants were held in Helsinki, while Finland was a prominent object of media interest, at least for the European media. Minimising any risk to our reputation thus was a major concern. The cyber dimension was once again safeguarded in good cooperation between the key authorities.

Cooperation will always carry the day

From the perspective of cooperation, the elections and Council Presidency were handled as routine tasks in many ways. The central government network based on ISAC cooperation lays an excellent foundation for trust, also in special cases and when Finland is in the limelight more than usual. Good shared practices were created as the cooperation was stepped up for the visits of President Trump and President Putin in 2018, and these practices were also followed in 2019. Although the configuration of partners may change slightly, cooperation and trust help to launch each preparedness measure. Where necessary, this enables a rapid response to incidents during normal conditions, even unexpected ones.

The purpose of election interference is to erode citizens' trust in society and the democratic system and decision-making that underpin it. Election interference may also be associated with more extensive systematic activities or hybrid influencing.

The aims of influencing may include manipulating societal discussion. In other countries, election interference directed at the voting system, voters, parties and the media has been observed.

NATIONAL CYBER SECURITY CENTRE'S ROLE IN SECURING SAFE ELECTIONS

” From the perspective of personal data and information security, 2019 was a particularly important year for Finnish society. Not only did two major elections take place in Finland one after the other but Finland also held the Presidency of the EU Council last year.

Guaranteeing the safety of these events in cooperation between various authorities was an obvious choice and highly important. Different global signals indicated that Finland should also prepare for threats and their realisation. The authorities initiated close cooperation in the lead-up to the first elections, ensuring that the elections could be held freely and without interference. The close cooperation also enabled the authorities to share information with different actors as quickly as possible.

From the perspective of the National Bureau of Investigation, both elections were conducted without significant interference. In the lead-up to the parliamentary elections, the online election results service was targeted by a heavy DoS attack, and the website went down for a short while. We now know that this attack was an isolated incident, rather than indicating large-scale organised activities aimed specifically at the elections. There was no way the perpetrators could influence the outcome of the elections by means of the DoS attack. As a phenomenon it is serious, however, as it targeted one of the cornerstones of a free and democratic society.

The National Bureau of Investigation found that the level of preparedness for safeguarding the elections was sufficient and worth investing in. From the perspective of cyber security, the elections were conducted very smoothly, for which special thanks go to all actors who participated in making it possible.

In terms of cooperation between the National Bureau of Investigation and the National Cyber Security Centre, the year 2019 was rather busy. Among other things, we focused on issuing alerts about and preventing Office 365 data breaches. Extensive information sharing and campaigns increased Finnish people's awareness of this phenomenon significantly. Our efforts have also been noted outside Finland. While the National Bureau of Investigation continues to investigate the data breaches, Finland currently enjoys a particularly good reputation, especially in the context of this phenomenon.

Marko Leponen
National Bureau of Investigation

” Finnish elections depend in many ways on information systems and their security, even if voters use a pen to fill in a printed ballot paper. The Ministry of Justice's election information system, which comprises the voting register and which is used to publish the election results, plays a key part in conducting the elections successfully.

The work to combat election interference was intensified before the parliamentary and European elections of spring 2019. The Cyber Security Centre took on an active role in forming situational awareness of cyber security for the elections, improving cooperation between authorities, and supporting the maintenance of the electoral information system. The NCSC-FI convened Vaali-VIRT, a network of authorities that included all key stakeholders of the elections. The network practised incident management together, shared information and maintained situational awareness during the elections through common snapshots.

The Ministry of Justice regarded the Cyber Security Centre's contribution to securing elections as essential. The facilitation of inter-authority cooperation produced concrete results. The experts at the Cyber Security Centre identified key actors, assisted in creating international situational awareness and supported the cooperation.

Heini Huotarinen
Ministry of Justice

A better grip on cyber security through exercises

From a project to a basic service

Supporting exercise activities became a part of our basic services during 2019. The planning work launched in connection with the KYBER 2020 programme funded by the National Emergency Supply Agency turned into a new central element of our service package. Together with our other services, exercise activities help us serve society's cyber security more diversely than ever. Our main focus is on organisations critical for security of supply, for which we provide guidance and support in issues relevant to exercise activities.

By conducting exercises, an organisation can improve its operational capabilities and ability to respond and recover, thus reducing the adverse effects of incidents and attacks. Participating in exercises has been a part of our activities for a long time. By participating in exercises and simulating our services in them, we have also been able to develop our own activities while helping other organisations to arrange realistic exercises. Thus, the purpose of the exercise support function is sharing this developed expertise with other critical actors.

The year 2019 saw many cyber exercises that helped companies improve their preparedness and capabilities. According to the feedback, the exercise support service was found useful and considered necessary also in the future. The experience from last year shows that organisations critical for security of supply are increasingly willing to improve their cyber capabilities by means of exercises. The number of exercises organised with our support has thus gone up steadily since 2016.

A manual for organising cyber exercises and a booklet of exercise scenarios for 2020

In 2019, we published our manual on instructions for organising cyber exercises, in which we shared the lessons learned and experiences accumulated by the NCSC-FI through participation in dozens of cyber exercises, planning and running the exercises, as well as analysing their results. Guided by these instructions, organisations can plan a cyber exercise from start to finish, either alone or with an expert partner.

We also organised a Cyber Exercise Scenarios 2020 workshop in late 2019, which was attended by authorities and representatives of key companies in the cyber security sector . The workshop produced a total of 20 practice scenarios to support organisations' exercise activities. The booklet can be found on our website.

Development of exercise activities continues

The NCSC-FI will continue to survey and identify the training needs of organisations critical for security of supply in the coming years. We will conduct an annual survey to map organisations' wishes and challenges and will monitor changes in their ability and willingness to organise exercises. Through these surveys, we will continue to keep in touch with target organisations and actively support their cyber exercises.

In addition to support measures for the exercises of organisations critical for security of supply, such large joint exercises as TAISTO, TIETO, KYHA and Cyber Europe will bring together many of these and other organisations.

Joint FINEST19 exercise for Estonian and Finnish authorities

In March, we organised FINEST19, an exercise simulating a cyber incident in critical electricity infrastructure together with the Estonian information security authority CERT-EE. This was the first international joint exercise for the Finnish and Estonian CERT teams, and it was organised by the NCSC-FI. The exercise was carried out in cooperation with the transmission system operators Fingrid in Finland and Elering in Estonia.

This particular exercise focused on tackling together a cyber crisis affecting both countries in critical infrastructure. Key priorities in the exercise were effective and safe communication measures and the creation of a shared situational awareness. The exercise scenario focused on a disruption in power supply, and, in addition, included a cybercrime perspective.

Regarding cyber exercises, the NCSC-FI lends its support to the following areas:

- launching the planning of an exercise
- finding a suitable partner
- supporting scenario planning
- simulating the National Cyber Security Centre's services in the exercise
- assuming the role of an observer in the exercise
- assisting in the analysis following the exercise.

Work on the future and development of operations

Cybersecurity label shows the way forward for European smart device standards

To receive a Cybersecurity label, the compliance with our requirements must be verified. These requirements are mainly based on the draft European standard ETSI EN 303 645 Cyber Security for Consumer Internet of Things. We participate actively in the development of the standard, thus striving to ensure compatibility with the potential future European requirements. This will make it easier for Finnish companies manufacturing IoT devices to enter the international market.

IoT certification has attracted a great deal of interest – and continues to do so. This topic has been raised also in the context of the cybersecurity certification scheme whose groundwork was laid with the entry into force of the EU Cybersecurity Act in June 2019. Once completed, the ETSI standard is seen as one potential candidate to be used as a requirement source for IoT certification. The European Cybersecurity Certification Group , tasked with preparing the launch of the certification system, has shown interest in our Cybersecurity label, and we could also be able to participate in developing European certification.

As seen on TV, more information on the website

The Cybersecurity label was launched on 26 November 2019. We organised television and social media campaigns to spread awareness of it. Once consumers learn to recognize the Cybersecurity label and the amount of labelled devices on the market increases, we can be satisfied with its effectiveness . For more information on the requirements for the Cybersecurity label and instructions on applying for it, visit www.tietoturvamerkki.fi.

While the Cybersecurity label is intended for consumer devices and services, manufacturers offering business solutions have also shown interest in it. The costs of the audits in terms of money and time have sparked discussion on whether a version of the label based on self-assessment should also be created.

We will continue to develop the Cybersecurity label concept further based on our experiences. We will also follow developments in European requirements. If they change, we will be standing by to update ours. This way we can best support Finnish companies' access to the international markets.

WEBSITE
SEO
SOCIAL NETWORK
WEBSITE
MOBILE
WEBSITE
SEO
MOBILE
WEBSITE

Significant expansion in DNSSEC use

Low uptake of a free service available since 2011

In the Finnish .fi root domain name service, DNSSEC was rolled out in stages in the early 2010s. In addition to the .fi root DNSSEC signature, we offered the users of .fi domains access to DNSSEC free of charge.

Despite the early introduction of the service, absence of charges and many DNSSEC campaigns, there has been little or no increase in DNSSEC use in Finland.

In early 2019, registrars reselling .fi domain names did not offer DNSSEC to their customers at all in practise. Only around 5,000 of the .fi domains were DNSSEC protected. Approximately 7% of Finnish Internet traffic went through resolving name servers with DNSSEC validation.

Successful campaign increased DNSSEC use

Following discussions with our stakeholders in early 2019, the idea of organising a national DNSSEC Launch Day was born. Its purpose was to bring together domain name registrars and Internet access providers committed to using DNSSEC, maintain a public list of them, and spark public discussion about the need for DNSSEC.

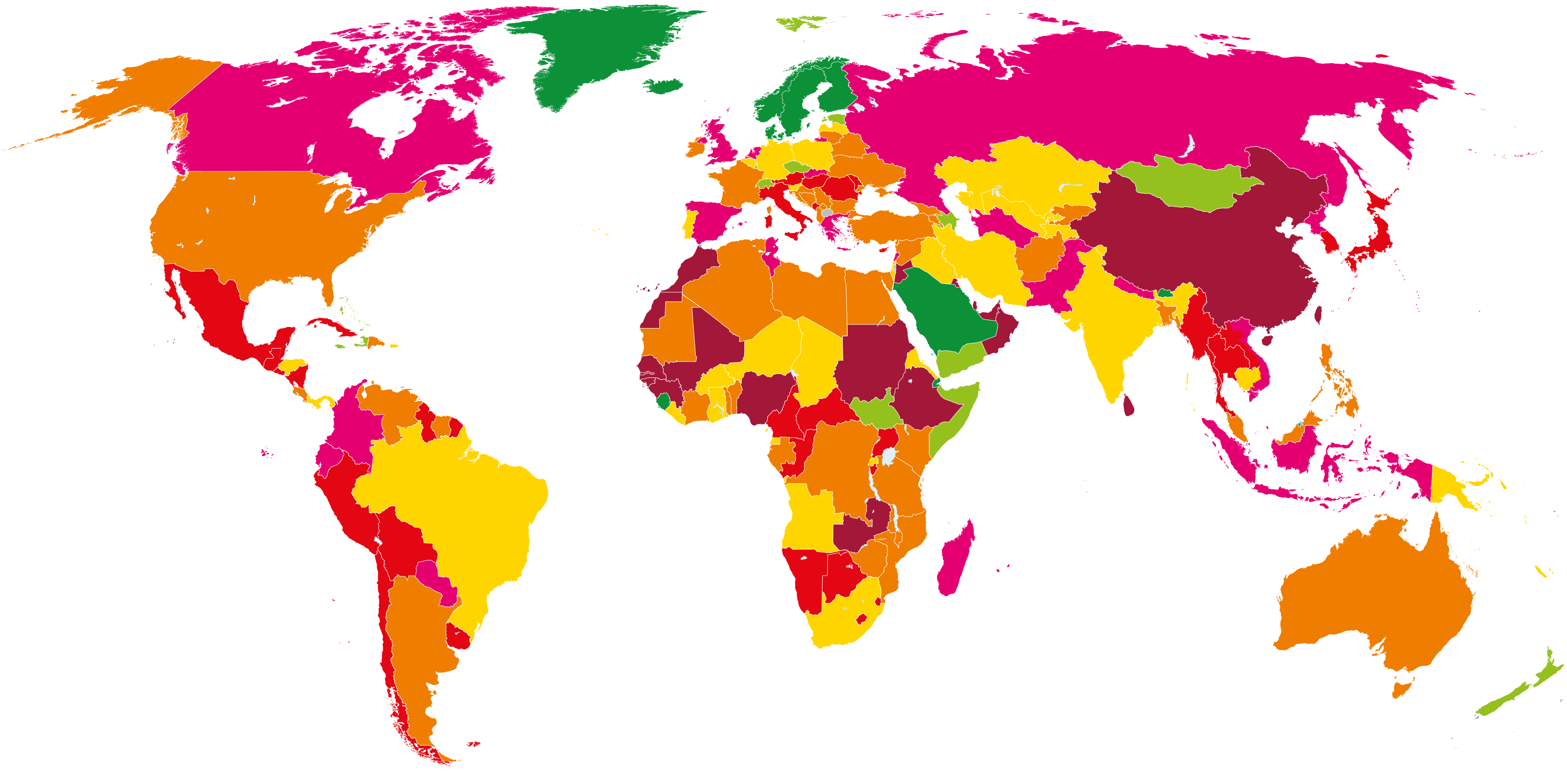
As the Launch Day was selected 5 September 2019, and 33 domain name registrars and three Internet service providers participated in the campaign.

The number of domain name registrars using DNSSEC validation increased significantly. In late 2019, more than 250 .fi domain name registrars offered DNSSEC validation to their customers, and the number of DNSSEC validated .fi domain names was almost 10,000. This is twice the figure in 2018.

The DNSSEC validation rate increased during the year from 7% to over 90%, as large Finnish ISPs introduced validation on their resolver name servers. The validation rate we achieved is high even on a global scale.

Domain Name Security Extensions (DNSSEC) is a technology that ensures the authenticity and integrity of the response provided by the domain name system. DNSSEC makes it possible to validate the response returned by a name server or detect attempts at DNS spoofing. DNSSEC is one of the key security features for ensuring that the address and content of a web page opened by the user match and that e-mails end up with the recipient indicated by the address. However, protecting your domain name with DNSSEC is not enough to benefit Internet users. DNSSEC signatures must also be validated in Internet traffic, otherwise users will also receive DNS responses with a corrupt DNSSEC signature. This validation is carried out by resolver name servers, which are typically maintained by Internet access providers.

DNSSEC Validation Rate by country (%)



FIGURES

265 Number of .fi domain name registrars offering DNSSEC to their customers

10 255 Number of DNSSEC validated .fi domain names

92,2% DNSSEC validation rate in Finland

Efforts to ensure 5G network security continue

The efforts that started in 2018 with a study on the cyber security of 5G networks in 2018 was followed in 2019 by national and EU level 5G risk assessments.

The EU is now working on a toolkit to support risk management in 5G networks. This work will produce information on the basis of which 5G technology providers and users can make realistic risk assessments and build safe solutions.

So far, the transition to 5G technology has been identified as a larger paradigm shift than any previous generation of mobile networks. The introduction of new 5G features and operating models will change the role of operators, bring about networks tailored to local needs, possibly expand the field of regulatory control, and create completely new risk management requirements for operators using 5G features. The network, now a data transfer tube, will increasingly become a shared platform for information processing and data production in which there no longer are clear boundaries between networks. This will enable new functionalities and opportunities, which will also be used by operators providing essential functions. At the same time, increasingly important functions of society will rely on 5G networks.

The changeover from previous network generations towards a 5G world will require active sharing of information, reviewing the boundaries of government steering, a more extensive dialogue between actors and, ultimately, a new regulatory approach. At international level, country-specific and EU-wide recommendations, legislation and regulation will create additional challenges in the 5G information security landscape.

In addition to a theoretical approach, we also wanted to promote technical expertise related to the information security ecosystem built around 5G technology as EU level cooperation. In order to bring the hacker and information security testing community, equipment manufacturers, the NCSC-FI and the world of science closer together, we organised the 5G Cyber Security Hackathon, the world's first hackathon focusing on 5G information security, between 29 November and 1 December 2019 in cooperation with the University of Oulu, Ericsson and Nokia.

It was attended by nearly 100 hackers from over 10 different countries, and it provided a unique learning opportunity for all parties. We are still analysing the results of this event, and the lessons learned from the hackathon will be shared and the experiences will be discussed with decision-makers of the digital world at the 5G Leading Edge Forum on 13 February 2020.

KYBER 2020 and Digital Security 2030

Last year marked active efforts to develop our operation. For example, we improved our network leadership (ISAC activities) and exercise activities in keeping with the National Emergency Supply Agency's KYBER 2020 programme. We also made decisive progress in the development of the HAVARO service. Based on feedback, the customers have found our development work necessary.

More support for companies critical for security of supply

Companies critical in terms of security of supply, in particular, have seen the development of our operations as new services and capabilities and more effective cooperation. We have built trust together with the National Emergency Supply Agency, for example by participating in cyber security development specific to different sectors and pools.

Building strong national cyber security

The KYBER 2020 programme of the National Emergency Supply Agency will be followed by the Digital Security 2030 programme, the planning of which began in 2019.

The Digital Security 2030 programme aims for involving a larger group of actors in more in-depth development of national cyber security. We have been closely involved in the planning of this programme, in which business life and the pools have also been invited to participate.

In 2019, a strategic objective, key contents and operating methods for achieving the objectives were formulated for the programme. The model of agile development will be followed in further work on the programme, and the aim is to ensure the commitment of both business life and the authorities to it.

New cooperation agreement with far-reaching potential

Last year, we signed a new cooperation agreement with the National Emergency Supply Agency, which guarantees a minimum of EUR 4,000,000 in annual funding for our operations. This will allow us to work systematically for the continuity and security of activities in companies critical for security of supply.

As part of the agreement, we have drawn up a development plan for the NCSC-FI. For example, we can address the strategic objectives of the National Emergency Supply Agency's cyber security development better in the future. We have also striven to improve our operational capabilities, enabling more effective scaling in case of extensive incidents. The plan also includes new services that could provide us with situational awareness of a higher quality and allow us to identify new threats.

The National Emergency Supply Agency is a reliable partner that supports our operations and efforts to develop them.

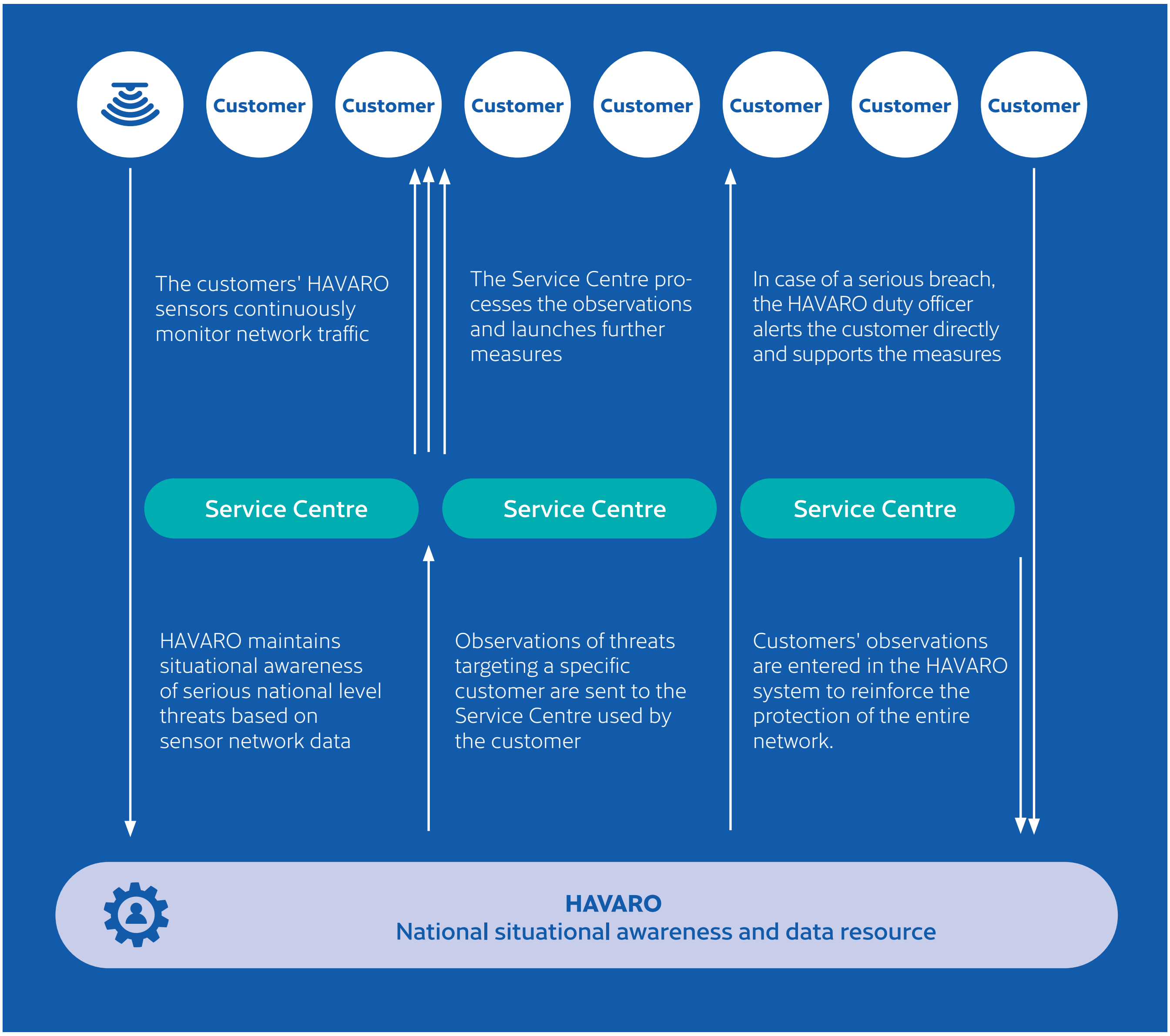
Welcome to the updated HAVARO service!

Our HAVARO service alerts customers to malicious network traffic targeting them and helps prevent security threats. The customers currently include companies critical for the security of supply and central government organisations. Using malicious traffic, an outsider may gain access to a customer's business secrets or cause financial losses by interfering with the customer's financial transactions.

The HAVARO service update was launched in 2017 as part of the National Emergency Supply Agency's KYBER 2020 programme. The new service will come into production in 2020.

Easier access to HAVARO service

HAVARO will be available for Finnish organisations in summer 2020 once it is included in the product range of commercial service centres (SOCs) providing information security services.


Customer
Customer
Customer
Customer
Customer
Customer
Customer
The customers' HAVARO sensors continuously monitor network traffic
The Service Centre processes the observations and launches further measures
In case of a serious breach, the HAVARO duty officer alerts the customer directly and supports the measures
Service Centre
Service Centre
Service Centre
HAVARO maintains situational awareness of serious national level threats based on sensor network data
Observations of threats targeting a specific customer are sent to the Service Centre used by the customer
Customers' observations are entered in the HAVARO system to reinforce the protection of the entire network.
HAVARO
National situational awareness and data resource

HAVARO service model

The new service model will replace the HAVARO version for authorities we have provided since 2011. Based on cooperation between the NCSC-FI and commercial information security actors, HAVARO will respond to customer needs more comprehensively and precisely than before.

Future needs

We have also addressed future development needs and requirements in the planning and implementation of the new service and had numerous constructive discussions with our customers and other stakeholders during this project. We have received valuable feedback and development ideas at many workshops and joint events.

Our partner in service development is Reaktor Innovations Oy. Thanks to agile software development methods, the new system and its application components have reached the testing phase in good time, and the production will be launched stepwise.

Room for new partners

In 2019, HAVARO's new service and operating model was clarified in cooperation with Service Centres. We disambiguated the terms of the service, making it possible to offer the HAVARO service to a high standard while responding to different customer needs.

We would also welcome new partners to the HAVARO ecosystem, including Service Centre actors and technology suppliers. Come and join us in building the foundation pillar of Finnish cyber security!

Vulnerability coordination

The most important case in the field of vulnerability coordination in 2019 was related to Fidelix building automation equipment.

In the Team Whack series broadcast by YLE in March 2019, a group of hackers tested Fidelix building automation devices and found several vulnerabilities. We coordinate the efforts to fix these vulnerabilities and inform device owners. Regardless of our information activities, the number of unprotected devices connected to the Internet decreased slowly, excluding devices managed by third parties.

Building automation devices connected to the Internet have been coming up in our security surveys of Finnish information networks for years. The vulnerabilities of these devices would enable attackers to harm building users. Reaching device owners has been difficult, however, and this is why there has been little or no reduction in the number of vulnerable devices.

Our vulnerability coordination will help anyone who discovers a vulnerability or a serious bug to collaborate with software manufacturers and other similar actors. We always handle vulnerability information responsibly. Our aim is that information about the vulnerability and the appropriate patch and updates to deal with the problem are communicated to all those who need this information, also end users. We strive to ensure that as many significant vulnerabilities as possible are also fixed and that the patches are installed.

Our KPIs

As the figures show, 2019 was a busy year for us. While shutting down harmful sites and attending ISAC events kept us on the move, in other respects 2019 was similar to the previous year.

24/7/365
Uninterrupted on-call duty

2
Alerts

83208
Auto-reporter

4500
Number of "tickets" processed

25
Cases processed through vulnerability coordination

4500
Shutdown of harmful sites

5500
Facebook followers

11000
Twitter followers

Number of incidents

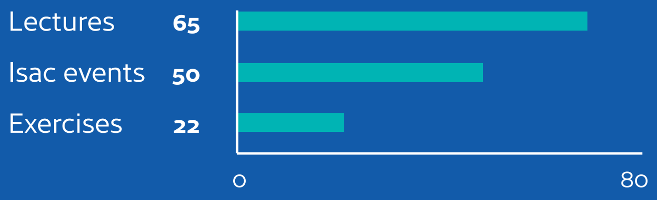
7
Critical incidents

18
Serious incidents

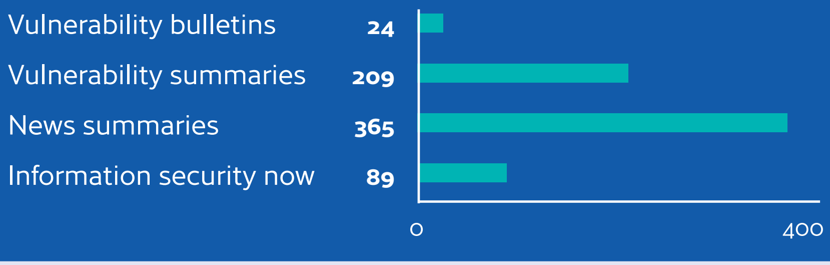
43
Significant incidents

68
All incidents together

Events and exercises



Communication and bulletins



During the year, we conducted customer satisfaction surveys related to our situational awareness products and ISACs. The grading scale in our surveys was from poor (1) to excellent (5).

Sector-specific information sharing groups were regarded as useful. Items deemed especially important included networking and the enabling of exchange of information.

Satisfied with our situational awareness products

4,2

Average

Survey addressed to sectoral ISACs

4,4

Grade

CYBER WEATHER 2019 AND A LOOK AT CYBER YEAR 2020

> ” The nature of cybercrime is not sufficiently understood. The majority of cybercrime is opportunist, international and automated. When a person or an organisation assesses its risk of being targeted by an information security incident, they assume that the targets must be of interest for the attacker, whereas in reality the targets are typically selected at random.

10 information security forecasts for 2020

The information security forecasts for 2020 are based on a joint assessment made by the National Cyber Security Centre and our cooperation networks. Whether our forecasts will be proven accurate remains to be seen in late 2020.

1 Automated information security solutions that utilise artificial intelligence are developing

As the offer increases, the use of SOC services, among other things, will diversify and increase.

2 Services will be produced in multi-layered and multinational subcontracting chains

When outsourcing services, it is crucial to examine and specify the components, dependencies and responsibilities that are essential for information security. Making retrospective changes is often challenging, especially if shortcomings only emerge at the time of incidents. The same problems apply to private and public organisations alike. Disruptions of services may also hamper the functioning of society.

3 The impact of cyber security on business operations will be taken into account better than before

Business depends on digitalisation. The risks associated with it should be routinely included in the risk management measures. Organisations have woken up to this situation, which is seen as the emerging needs for risk-based assessment models related to the functioning of information security.

4 Protection is inadequate because the nature of cybercrime is not sufficiently understood

The majority of cybercrime is opportunist, international and automated. When a person or organisation assesses their risk of being targeted by an information security incident, they assume that the targets must be of interest for the attacker, whereas in reality the targets are typically selected at random.

5 More cyber security exercises

While the activities are often well planned, in a real situation, panic and chaos can take you by surprise. To improve the situation, an increasing number of organisations practise their response to incidents and develop their activities based on the observed shortcomings.

6 Discovered information security vulnerabilities are exploited at a faster pace

Routine update publishing and update processes are no longer enough. To support software updates, new types of security solutions must be introduced to improve detection.

7 The need for versatile information security experts is growing

The competence areas of technical experts of information security are differentiating. People with business insight and, for example, non-technical competence related to procurement are needed in the expert team.

8 Data and operations are moving to the cloud

Cloud services will diversify. Rather than storage only, cloud services will offer centralised functionalities that have traditionally been implemented in the organisation's own network. When introducing cloud services, the following question will be increasingly important: Is the division of responsibilities between the cloud service provider and the organisation clearly defined?

9 The popularity of information security assessments will increase with rising awareness

In the context of information security, ensuring sufficient competence and levels will become increasingly important. An assessment carried out by a third party makes it easier to provide proof, for example to customers.

10 The standard of information security is linked to staff awareness

Information security in organisations will stand and fall by the personnel. Even an individual employee can block phishing, invoicing fraud, or e-mails containing malware. It pays to invest in training and exercises!

How did we do in our security outlook for the past year?

Very well! All our forecasts hit the bullseye.

Correct!

We had prepared for the increase in the use of cloud services and new technologies, and the challenges related to their emergence. As the offer increased, we also predicted that the trend of outsourcing information security would continue.

We noticed that slowly but surely, information security would make its way to organisations' overall risk management and improve their protection against cyber threats. Protection measures are indeed needed as online crime becomes more widespread and state-sponsored cyberattacks are commonplace.

Last summer, disruptions in municipal services sparked discussion. The cases were an unpleasant reminder of how dependencies on digital services create unexpected but also serious situations.

The need for basic information security skills and the human aspect came up. This theme is also topical today. For example, the personnel's information security skills and ability to recognise online scams essentially improve the security of the entire community. Leaks of credentials that appeared innocent and payment fraud were commonplace, also in Finland.

While the security of devices connected to the Internet has not improved in the last decade, there were also glimpses of light, as the Cybersecurity label made it easier to identify secure consumer devices.

1	**The cloud comes with force, and the change is cause for both joy and concern**	YES
2	**Outsourcing of information security will increase**	YES
3	**Cyberattacks by governmental actors and news reports on them will continue**	YES
4	**Still room for improvement in the basics of information security in organisations**	YES
5	**Information security will become part of business-oriented risk management**	YES
6	**Significance of human information security will grow**	YES
8	**Significance of information security in consumer devices connected to the internet will be emphasised**	YES
7	**Dependency on digital services creates surprising situations**	YES
9	**Familiar threats that were deemed minor are gradually becoming more severe**	YES
10	**New technologies determine the information security challenges in the 2020s**	YES
+1	**We will not see malware epidemics targeted at mobile devices**	YES

Cyber weather in 2019

January

Storm Aapeli wreaked havoc in communications networks, especially in the Åland Islands

Hackers gained access to systems through RDP remote services open to the Internet

February

CEO scams became more widespread. Hacked Office 365 email accounts were exploited in the scams

🌐 Cybercriminals made millions out of CEO scams and big game hunting

March

DoS attacks aiming at election interference in several European countries

🌐 Data breach targeted at Norsk Hydro caused major financial losses

A great number of IoT devices connected to the public Internet in Finland. The topic was discussed in YLE's Team Whack broadcast.

April

A DoS attack targeted the online results service during the parliamentary elections

🌐 Suspicions of online spyware belonging to NSA in the US having ended up in the hands of a Chinese group

May

Bluekeep vulnerability can lead to an autonomously spreading malware epidemic

Big game hunting groups take advantage of common malware

June

⚠ **Alert 01/2019:** Vulnerability in Exim e server exploited in data bre

Attack against a municipali Lahti

A great number of sextortio scams reported

🌐 = International news

July

Galileo incident, service down for a week

Attack against a municipality: Kokemäki

email
eaches

ty:

on

August

Government websites targeted by DoS attacks

Alert 02/2019: Vulnerabilities in Microsoft Remote Desktop app exploited in data breaches

Attack against a municipality: Pori

September

Alert for Office 365 data breaches removed

Cyber criminals caught in international operations

October

Information security of IoT devices has not improved in 15 years

QSnatch malware discovered widespread in network attached storage (NAS)

Among other things spies go after inventions. Data also collected on people

Reflection DoS attacks

November

Cybersecurity label helps consumers make safer purchases of smart devices for their homes – Finland the first country in Europe to start ensuring the security of smart devices

Multi-factor authentication would prevent most Office 365 data breaches

December

Our annual survey again detected more than 1,000 unprotected devices in Finnish information networks

Subscription scams were spread by text messages, emails and links in advertisements as well as through search engine optimisation

DNSSEC deployment got off to a good start

A busy year of publications, events and campaigns

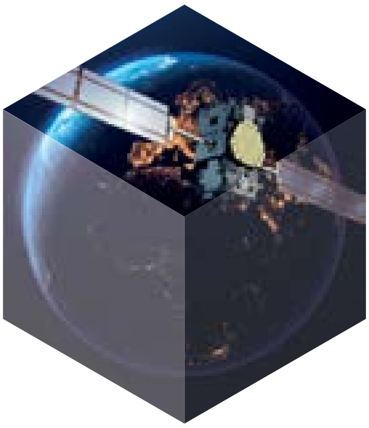
Here you will find a few highlights of our busy year of publications in 2019. Hopefully, as many people as possible found our guides and campaigns helpful.

CAMPAIGNS AND EVENTS

Cyber security tips from security expert Teijo (videos with English subtitles) https://www.youtube.com/playlist?list=PL8zUniisouhV17H1efojhIYi_CToKTk_X (in Finnish)

Cybersecurity label guides consumers to intelligent smart device purchases (in Finnish) https://tietoturvamerkki.fi/

World's first 5G Cyber Security Hackathon https://www.kyberturvallisuuskeskus.fi/en/news/70-top-hackers-around-world-gathered-finland-worlds-first-open-5g-cyber-security-hackathon-was

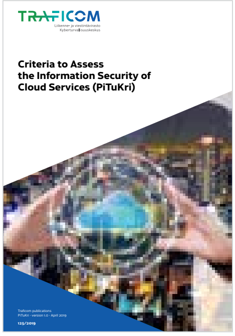


Galileo Innovation Challenge: International teams innovated services for the EU's Galileo satellite navigation system https://www.kyberturvallisuuskeskus.fi/en/news/international-teams-competed-innovation-challenges-eus-galileo-satellite-positioning-services

PUBLICATIONS

TRAFICOM
Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta

Protection against Microsoft Office 365 credential phishing and data breaches. English translation available. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_MS365_eng_sivut200919HR.pdf


TRAFICOM
Criteria to Assess the Information Security of Cloud Services (PiTuKri)

Criteria to Assess the Information Security of Cloud Services, English translation https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/PiTuKri_v1_0_english.pdf

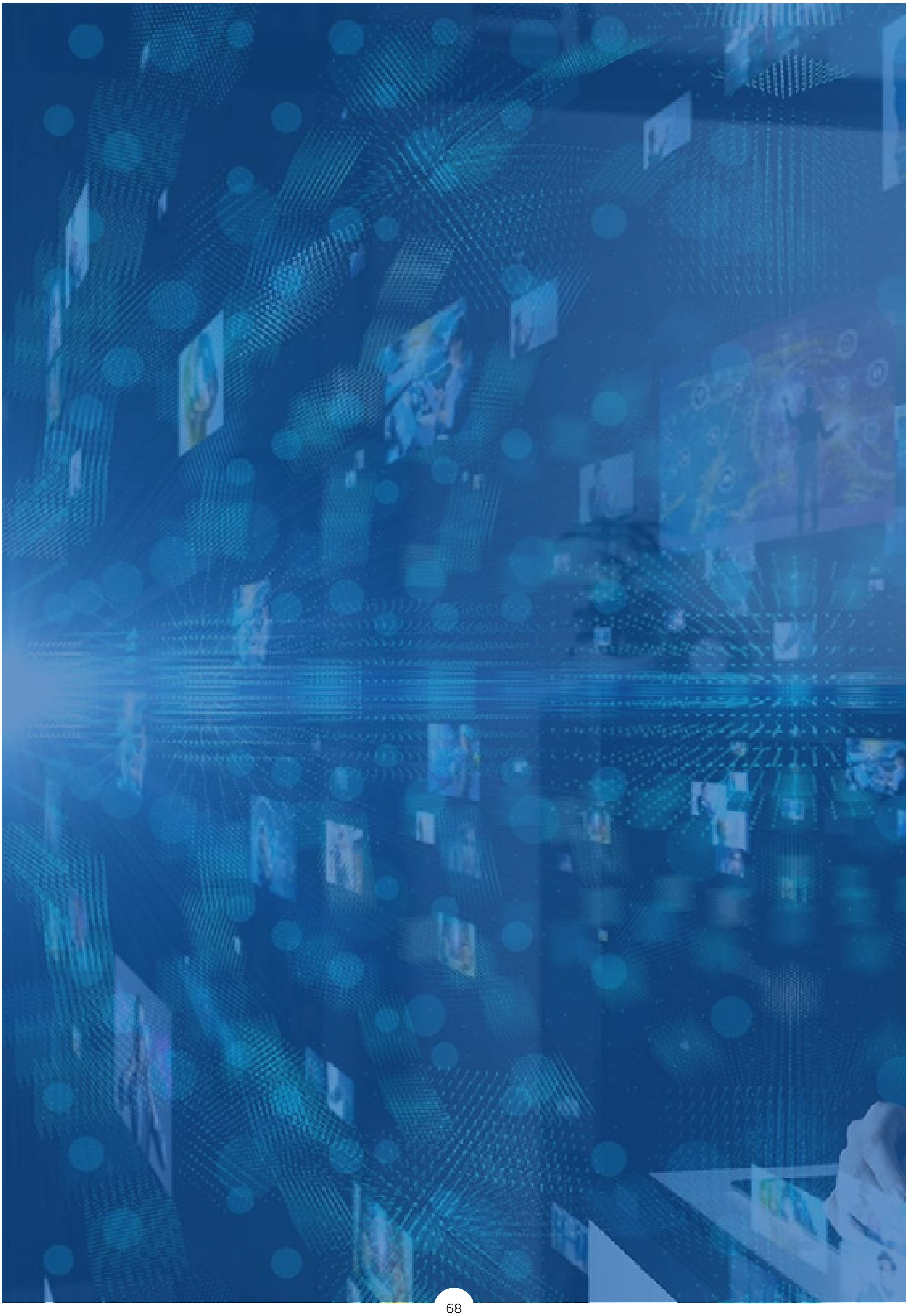
Instructions for organising cyber exercises – A manual for cyber exercise organisers (in Finnish) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

TURVALLISESTI NETISSÄ
OPI KÄYTTÄMÄÄN NETTIÄ TURVALLISESTI TÄMÄN HAUSKAN OPPAAN AVULLA!

Guides for safe online conduct for children and parents (in Finnish) https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvallisesti-netissa-oppaat-lapsille

SEE ALSO

- Viewpoints to the standardisation and certification of information security (in Finnish) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf
- How to protect yourself against online scams https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/how-protect-yourself-against-online-scams
- Keeping your information secure both at home and at work https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/keeping-your-information-secure-both-home-and-work
- Kyber-Terveys project: Information security and data protection requirements for social welfare and healthcare procurements (in Finnish) https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja
- Assessment guideline for electronic identification services https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Assessment_guideline_for_electronic_identification_services_211_2019_O_EN.pdf



Summary of cyber weather news in 2019

January

- Storm Aapeli wreaked havoc in communications networks, especially in the Åland Islands (in Finnish) https://yle.fi/uutiset/3-10578072

February

- CEO scams became more widespread. Hacked Office 365 email accounts were used in the scams (in Finnish) https://yle.fi/uutiset/3-10676320
- Cybercriminals made millions out of CEO scams and big game hunting https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/

March

- Data breach targeted at Norsk Hydro caused major financial losses (in Finnish) https://www.tivi.fi/uutiset/kiristyshaittaohjelma-aiheutti-pohjoismaiselle-yhtiolle-viikossa-jopa-36-miljoonan-euron-tappiot/abfb80fb-6078-3c89-88699567673ea39d
- A great number of IoT devices connected to the public Internet in Finland. (in Finnish) https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa

April

- A DoS attack targeted the online results service during the parliamentary elections (in Finnish) https://yle.fi/uutiset/3-10731312
- Suspicions of online spyware belonging to NSA in the US having ended up in the hands of a Chinese group https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html

May

- Bluekeep vulnerability can lead to an autonomously spreading malware epidemic (in Finnish) https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/etatyopoytaratkaisun-kriittinen-bluekeep-haavoittuvuus-vaatii-kiireellista
- Big game hunting groups take advantage of common malware (in Finnish) https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuuksien-hyvaksikaytto-synkensi-toukokuun-kybersaata

June

- Alert 01/2019: Vulnerability in Exim email server exploited in data breaches https://www.kyberturvallisuuskeskus.fi/en/vulnerability-exim-email-server-exploited-data-breaches
- Attack against a municipality: Lahti (in Finnish) https://www.tivi.fi/uutiset/kyberhyokkays-sekoitti-lahden-jarjestelmat-vakavat-hairiot-jatkuvat/30bfba87-5e49-461a-9443-4389ddb349e5

July

- Galileo incident, service down for a week (in Finnish) https://www.tekniikkatalous.fi/uutiset/undefined/ffb69bba167a-4bae-b654-2ef46cc7c03b
- Attack against a municipality: Kokemäki (in Finnish) https://yle.fi/uutiset/3-10899982

August

- Government website targeted by DoS attacks (in Finnish) https://yle.fi/uutiset/3-10933059
- Alert 02/2019: Vulnerabilities in Microsoft Remote Desktop app exploited in data breaches https://www.kyberturvallisuuskeskus.fi/en/vulnerabilities-microsoft-remote-desktop-app-exploited-data-breaches
- Attack against a municipality: Pori (in Finnish) https://yle.fi/uutiset/3-10913191

September

- Alert of Office 365 data breaches taken down (in Finnish) https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/office-365-sahkopostin-tietojenkalastelua-koskeva-varoitus-poistettiin
- Cyber criminals caught in international operations https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019

October

- Security of IoT devices has not improved in over 15 years https://cyber-itl.org/2019/08/26/iot-data-writeup.html
- QSnatch malware found to be widespread in network disks https://www.kyberturvallisuuskeskus.fi/en/news/qsnatch-malware-designed-qnap-nas-devices
- Among other things, spies go after inventions. Data also collected on persons https://www.zdnet.com/article/iranian-hackers-credential-stealing-phishing-attacks-against-universities-around-the-world/
- Third parties used to reflect DoS traffic to the actual target https://www.kyberturvallisuuskeskus.fi/en/ajankohtaista/2019-lokakuun-kybersaa

November

- Cybersecurity label helps consumers make safer purchases of smart devices for their homes – Finland the first country in Europe to start ensuring the security of smart devices (in Finnish) https://tietoturvamerkki.fi/
- Multi-factor authentication would prevent most Office 365 data breaches https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

December

- Our annual survey again detected more than 1,000 unprotected devices in Finnish information networks https://www.kyberturvallisuuskeskus.fi/en/news/over-one-thousand-unprotected-automation-equipment-finnish-networks
- DNSSEC deployment got off to a good start https://www.kyberturvallisuuskeskus.fi/en/news/use-dnssec-leaped-forward-finland-using-digital-services-becoming-more-secure

Do you or your organisation need help with preventing information security breaches, or do you have questions about legislation related to cyber security? 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:

via email: cert@traficom.fi
Customer service: 0295 345 630

Follow us and our news
https://www.kyberturvallisuuskeskus.fi/en/
@CERTFI
https://www.facebook.com/NCSC.FI/

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

Finnish Transport and Communications Agency Traficom
National Cyber Security Centre
PO Box 320, FI-00059 TRAFICOM
p. +358 29 534 5000

kyberturvallisuuskeskus.fi

ISNN 2669-8757 (online publication)

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre