Explanatory notes to the Regulation on information security in telecommunications operations

Table of contents

I. Background and legal basis of the Regulation

The Regulation is related to Chapter 29 of the Act on Electronic Communications Services (917/2014, hereinafter AECS) laying down provisions on the quality requirements for communications networks and communications services and on the obligation of a communications provider, such as a telecommunications operator, to maintain the information security of their services, messages, traffic data and location data, and Chapter 33 laying down provisions on the management of information security and interference and related notifications.

Quality requirements for communications networks and communications services

The Regulation is related to section 243, subsection 1, paragraphs 1, 2, 7, 9, 10, 11 and 13 of the AECS, pursuant to which public communications networks and communications services and the communications networks and services connected to them shall be planned, built and maintained in such a manner that:

1) the technical quality of electronic communications is of a high standard and information security is ensured;

2) the networks and services withstand normal, foreseeable climatic, mechanical, electromagnetic and other external interference as well as information security threats;

7) the data protection, information security and other rights of users and other persons are not endangered;

9) the networks and services do not cause unreasonable electromagnetic or other interference or information security threats;

10) they function together and can, if necessary, be connected to another communications network, and

11) modifications made to them will not cause any unforeseeable disruptions for other communications networks or services;
13) the responsible telecommunications operator is also otherwise able to meet its obligations or those imposed under this Act.

Under section 243, subsection 2 of the AECS, the quality requirements referred to in paragraphs 1, 2, 10, and 11 above shall be commensurate with the number of users of the communications networks and services, the geographical area served, as well as their significance to the users.

According to section 243, subsection 3 of the AECS, the measures to protect the information security referred to in paragraphs 1, 2, 7 and 9 listed above mean measures to ensure the security of operations, communications, equipment and programmes and the security of information material. The measures must be commensurate with the seriousness of threats, level of technical development to defend against the threat and costs incurred by these measures.

Furthermore, all quality requirements referred to in section 243, subsection 1 of the Act also apply to significant associated facilities and services related to communications networks and services according to section 243, subsection 4 of the Act[1].

[1] Pursuant to section 3, subsection 1, paragraph 8 of the AECS, an *associated service* means a conditional access system; electronic programme guide; number translation system; identity, location and presence service and similar service associated with communications networks or services that enables the provision of a communications network or service or supports the provision of services via them. As for paragraph 9 of the same section, *associated facilities* mean an associated service and buildings, entries to buildings and building wiring, ducts, masts and other corresponding physical structures, facilities or elements associated with a communications network or service that enable the provision of a communications network or service or support the provision of services via them.

This Regulation specifies the above technical requirements of section 243 under section 244, subsections 2, 3, 5, 8, 12, 13, 14 and 16, pursuant to which regulations issued by the Finnish Transport and Communications Agency may relate to:

2) electronic and physical protection of a communications network and the related site;

3) performance capacity, information security and functionality as well as their maintenance, follow-up and network management;

5) structure of communications networks and technical characteristics of communications network termination points;

8) interconnection, interoperability, signalling and synchronisation;

12) technical documentation and statistics as well as the form of related documents and their storage;

13) standards to be complied with;

14) associated facilities and services to the extent that they affect the requirements for communications networks and communications services laid down in section 243;

16) other comparable technical requirements set for a communications network or communications service.

Correspondingly, section 247 of the Act lays down obligations of the communications providers, including telecommunications operators, to maintain information security. Pursuant to subsection 1 of the section, when transmitting messages, communications providers must maintain the information security of their services, messages, traffic data and location data. Pursuant to subsection 3, the information security measures must be commensurate with the seriousness of threats, level of technical development to defend against the threat and costs incurred by these measures.

Under section 247, subsection 4, the Finnish Transport and Communications Agency may issue further regulations on information security referred to in subsection 1 above and elsewhere.

According to section 3, paragraph 40 of the AECS (in Act 456/2016), traffic data means information that can be associated with a legal or natural person and is processed for the purpose of the conveyance of a communication as well as information on the call sign of a radio station and the user of the radio transmitter, and on the starting time, duration or transmission site of a radio transmission. According to section 3, paragraph 22 of the AECS, electronic communication means information that is transmitted or distributed electronically.

Management of information security and interference

Section 272 of the AECS provides for the measures taken by telecommunications operators and certain other parties to implement information security. According to subsection 1 of the section, these parties have the right to undertake necessary measures referred to in subsection 2 to ensure information security:

1) in order to detect, prevent, investigate and commit to pre-trial investigation any disruptions in information security of communications networks or related services;

2) in order to safeguard the possibilities of the sender or recipient of the message for communications; or
3) in order to prevent preparations of means of payment fraud referred to in Chapter 37, section 11 of the Criminal Code planned to be implemented on a wide scale via communications services.

Measures listed above in subsection 1 may include:

1) automatic analysis of message content;

2) automatic prevention or limitation of message transmission or reception;

3) automatic removal of malicious software that poses a threat to information security from messages;
4) any other technical measures comparable to those referred to in subsections 1–3.

Pursuant to subsection 3 of the section, if it is evident due to the message type, form or some other similar reason that the message contains malicious software or commands, and the measure referred to in subsection 2, paragraph 1 cannot ensure the attainment of the goals referred to in subsection 1, the content of a single message may be processed manually. The sender and recipient of a message whose content has been manually processed shall be informed of the processing, unless the information would apparently endanger the attainment of the goals referred to in subsection 1.

Pursuant to subsection 4 of the same section, any measures referred to in the section shall be implemented with care, and they shall be commensurate with the seriousness of the disruption being combated. Such measures shall not limit freedom of speech, the confidentiality of a message or the protection of privacy any more than is necessary for the purpose of safeguarding the goals referred to in subsection 1. Such measures shall be discontinued if the conditions specified in this section for them no longer exist.

The Regulation specifies the technical implementation of the measures referred to above under section 272, subsection 5 of the AECS.

The Regulation and especially its obligations related to the disconnection of an internet access service in particular are also related to section 273 of the AECS laying down provisions on the obligation to remedy a hindrance. Pursuant to subsection 1 of the section in question, if a communications network, service or device creates serious economic or operational hindrance to other communications networks, services or connected services, device, the user or other person, the telecommunications operator or owner or holder of the communications network or device shall take immediate measures to correct the situation and, if necessary, disconnect the communications network, service or device.

Pursuant to section 273, subsection 2 of the AECS, any measures referred to in this section shall be implemented with care, and they shall be commensurate with the seriousness of the disruption being combated. Such measures shall not limit freedom of speech, the confidentiality of a message or the protection of privacy any more than is necessary for the purpose of safeguarding the goals referred to in subsection 1. Such measures shall be discontinued if the conditions specified in this section for them no longer exist.

In the cases referred to in section 273, subsection 1 of the AECS, the Finnish Transport and Communications Agency may decide on repair measures, including disconnection of a network, service or equipment.

II. Other regulations and recommendations of the Finnish Transport and Communications Agency related to the matter

This chapter describes other regulations, recommendations and instructions of the Finnish Transport and Communications Agency related to the topic of this Regulation.[2]

Regulation on disturbances in telecommunications services addresses various types of disturbances in telecommunications. The regulation covers both events where services

[2] Regulations, instructions and public recommendations can be found on the page https://www.traficom.fi/fi/saadokset?group=kyberturvallisuus.

offered by a telecommunications operator are subjected to or threatened by a significant information security violation (*information security incident*) and events that prevent a communications service from functioning or cause significant disturbance (*functionality incident*). The Regulation imposes obligations on telecommunications operators concerning the detection and management of information security and functionality incidents as well as related notifications and statistics.

Regulation on critical parts of a communications network provides for the identification and documentation of the critical parts of a communications network and issues more specific regulations on the definition of the critical parts of a communications network than in the Act.

Regulation on resilience of communications networks and services and of synchronisation of communications networks imposes minimum obligations on telecommunications operators concerning, among other things, the resilience of the power supply of devices used in the implementation of communications networks and services, the resilience of devices and connections and the physical protection of devices.

Regulation on electrical protection of communications networks contains obligations on the protection of public communications networks as well as the equipment and communications networks connected to them against overvoltage and overcurrent of climatic origin and caused by electrical equipment.

Regulation on the quality and universal service of communications networks and services concerns the measurement and management of the functionality, performance capacity, reliability and quality of communications networks and services. The Regulation contains general obligations that apply to all public communications networks and services as well as special requirements for telephone services, internet access services and television services.

Regulation on the technical implementation and ensuring of emergency traffic contains requirements concerning public communications networks to ensure that emergency calls and emergency text messages and essential emergency services information related to them is transferred from telecommunications networks to the emergency response centres. The requirements also ensure better chances of success for emergency calls in different cases of congestion in the network and in the event of communications network disturbances.

Recommendation on contingency planning for telecommunications operations provides telecommunications operators with advice on how to ensure compliance with the contingency planning obligations of the Act on Electronic Communications Services. This recommendation, which is partly confidential, is not a public, all-encompassing guide on preparedness, continuity and contingency planning. Instead, it covers issues that the Finnish Transport and Communications Agency recommends telecommunications operators take into account as part of their contingency planning obligation and their existing preparedness procedures.

The recommendation *'Filtering traffic in telecommunications operators' networks to certain communications ports for information security reasons'* applies to the filtering of traffic in internet access services.

Communication on the information security of services implemented abroad refers to the types of information to be provided to users on communications services with an international dimension. Some telecommunications operators implement their communications services partly or completely outside Finland or use services provided by foreign companies. Therefore, the service may be subject to legislation that differs from the Finnish legislation, and the users of the service must be made aware of this. In addition to the telecommunications operator also ensuring the information security of

its service in such a situation, users can independently evaluate the types of threats that their communications and traffic data are subjected to on the basis of such information.

The recommendation *Common Nordic Recommendations on SS7 Security Issues* includes measures to improve the security of SS7 signalling. The recommendation is confidential.

Instruction on recording information on traffic data processing contains instructions on how to apply section 145 of the AECS. The section provides for the obligation of a communications provider to save further event log information on any processing of traffic data relevant to confidentiality and privacy security, if this is technically feasible and does not cause unreasonable additional costs.

III. Objective of the Regulation

The objective of the Regulation is to:

1. contribute to the information security of public communications networks and services;
2. safeguard confidentiality and the protection of privacy in electronic communications; and
3. ensure that information security measures by telecommunications operators are comprehensive, systematic and effective.

The provisions of the Regulation aim at achieving these objectives, and the objectives guide the application of the Regulation. The objectives mentioned above should provide the starting point for all matters related to the implementation of information security in public telecommunications.

Pursuant to section 3, paragraph 28 of the AECS, information security means the administrative and technical measures taken to ensure that data are only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data and information systems can be used by those who are entitled to use them. In other words, information security covers the measures taken to safeguard confidentiality, integrity and availability of communications. The purpose of the Regulation is to contribute to the realisation of these objectives.

The Regulation defines the minimum requirements concerning the implementation of information security measures. The Regulation is intended to make the consideration of information security issues part of the everyday operations of telecommunications operators. In other words, the Regulation serves to ensure that information security factors are taken into consideration routinely and, through effective processes, as part of the implementation of communications networks and services.

IV. Other implementation options

This Chapter describes the other alternative implementation methods that were considered during the drafting of the Regulation.

Scope of application of the Regulation

The scope of application of the previous regulation was limited to public telecommunications operations, with the exception of the obligation related to the prevention of interference (section 9.1), which also applied to public authority networks interconnected with a public communications network. During the preparation of the Regulation, the Finnish Transport and Communications Agency assessed the need to extend the expansion of the scope of application to e.g. local mobile networks that are not public

communications networks, or so-called critical dedicated networks specified in the Regulation on critical parts of a communications network, in addition to public authority networks. However, no clear need for this emerged during the processing by the working group. In any case, section 273 of the AECS provides for a general obligation to remedy a hindrance. In addition, the requirements related to information security can be taken into account when agreeing on interconnection. As a result, it was found that there is no need to expand the scope of application of the same section of the new Regulation (15.1).

Nevertheless, the Virve 2.0 implementation model was taken into account in expanding the scope of application; in the model, a telecommunications operator provides the network service instead of a public authority network (network service for official communications) and a service provider provides the communications service related to communications with the authorities. The application of the new Regulation was also extended to cover these matters so that the scope of application of the Regulation would not be limited compared to the previous one in practice.

Specifying the obligations on taking information security into account

The previous regulation only defined the aspects of information security to be taken into account on a general level. Even though the definitions were flexible, in the experience of the Finnish Transport and Communications Agency, their guiding impact remained correspondingly very general. As a result, the options evaluated by the Finnish Transport and Communications Agency when preparing the Regulation were maintaining the previous definition, supplementing it with more detailed criteria, or changing the definition completely so that the Regulation would rely fairly directly on the information security domains defined by the European Union Agency for Cybersecurity ENISA.[3]

In the survey conducted in the summer of 2022,[4] the parties that issued statements with their views on the topic found that the obligation in the previous regulation was not too high-level. The statements noted that the obligations should be high-level enough to allow the telecommunications operator itself to choose the information security solutions.

The Finnish Transport and Communications Agency finds that a more detailed specification than before is nevertheless necessary to support the objectives of the Regulation and improve its guiding effect. The relatively general previous definition of the obligation has not supported matters such as monitoring and inspections when the Regulation has not set more detailed obligations on the different aspects, the implementation of which could have been monitored with inspections on an individual level. The Agency also assessed a choice between supplementing the previous definition and adopting an approach in accordance with ENISA. The Finnish Transport and Communications Agency finds that the choice of ENISA's approach is supported by the fact that it will make it possible to rely on the information security controls defined and recommended by ENISA in the implementation of the obligations. In that case, the documentation of compliance with the requirements by telecommunications operators and their monitoring from the perspective of the authority are both simpler compared to a situation in which telecommunications operators would have to draw up documentation on same or similar obligations corresponding to a regulation that was divided in a different way, causing extra work. For multinational telecommunications operators, choosing ENISA's approach and taking advantage of the controls recommended by ENISA avoids the establishment of

[3] ENISA Guideline on security measures under the EECC, 4th Edition, July 2021 (hereinafter ENISA's guidelines or ENISA GL).
[4] Teletoiminnan tietoturvasta annetun määräyksen (67 A/2015 M) ajantasaistaminen: Kysely kokemuksista ja kehitysideoista (Updating the Regulation on information security in telecommunications operations (67 A/2015 M): A survey of experiences and development ideas), Doc. no Traficom/16241/09.09/2022.

different national requirements and also promotes the possibility of using the same documentation in different countries.

Compliance with certain standards related to mobile networks

The previous version of the regulation did not include obligations related to compliance with standards. There are no security standards that would apply to all telecommunications operations in general, but there are standards for different technologies and functions, and by relying on them it is possible to ensure compliance with generally accepted practices.

5G mobile networks and the new services they enable will play a central role with regard to the economy and the information society. In addition to the 5G network, LTE technology will also continue to play an integral role as a basic mobile network technology for a long time. Therefore, the importance of ensuring the information security of these networks is highlighted at the same time as the more complex 5G technological environment is setting higher risk management requirements than before.[5]

Ensuring the security of mobile networks as a part of the critical infrastructure of society is now more important than ever. For its part, the partnership project of standardisation organisations (3GPP) has responded to security-related concerns by drawing up security standards that equipment manufacturers and telecommunications operators in the mobile network can use to transparently prove and verify the realisation of the necessary security functions in their systems, communications networks and services. The security standards are compilations of standards that collect key functions related to the security of 4G and 5G equipment together.

The Finnish Transport and Communications Agency finds that it is justified to evaluate the use of standards focusing especially on the security of new mobile network generations in the Regulation as well as in telecommunications operators' own operations as a part of the realisation of the overall security of mobile networks. In the working group during the drafting of the Regulation, some of the members saw the proposed standard-specific references that would impose an obligation in a negative light, because the detailed implementation of standards was considered to limit the options of telecommunications operators in selecting security solutions and potentially also equipment suppliers. It was also considered a problem that the detailed list would become obsolete quickly as the standards were updated, meaning that a list drawn up in connection with an update of the regulation would no longer correspond fully to the security needs.

To take care of the security requirements of the mobile network, the Finnish Transport and Communications Agency has evaluated the following implementation options:

1. On the level of the Regulation, no references are made to specific standards or their security functions. The option can be supplemented by a reference to security standards as a recommendation in the explanatory notes.
2. The Regulation imposes an obligation to comply with certain sections of mobile network standards in the Regulation by topic.
3. The Regulation imposes an obligation to comply with the standards listed in general.

The Finnish Transport and Communications Agency finds that using the standards of 3GPP is a well-working method of ensuring that the components used in the implementation of networks and services meet certain cyber security requirements on the basic

[5] See Selvitys 5G:n kyberturvallisuudesta, Yhteenveto (Report on the cyber security of 5G, Summary), Traficom Publications, 14 May 2019, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Selvitys%205Gn%20kyberturvallisuudesta%20yhteenveto.pdf as well as Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, NIS Cooperation Group, CG Publication 01/2020 (hereinafter 5G Toolbox), p. 3–4.

level. By referring to the standards, it is possible to ensure that already specified security functions will be implemented and deployed appropriately as far as possible. A simple recommendation on compliance with the standards would not meet this goal, and therefore option 1 was not selected. A decision requiring compliance with standards has also been chosen at least in Austria and Germany, where requirements on compliance with the 3GPP standards have been set as a part of improving the security of mobile networks.[6]

Option 2 was not selected because the standards are technology-specific, and referring to the 3GPP standards on mobile networks is not an appropriate solution with regard to the sections of the Regulation that impose general obligations. Overall, references to sections of individual standards to impose an obligation would unnecessarily increase the complexity of the Regulation and the need for updates.

Option 3 was selected, and it was decided to implement it in an Annex to the Regulation concerning standards, because it was the most feasible of the options. The aim of the obligation is not to require telecommunications operators to take their own measures to verify that the components supplied by equipment manufacturers meet the requirements in question; instead, the aim is to adopt appropriate procedures that ensure in the ways specified by the telecommunications operator that the security functions described by the standards are taken into account and, if necessary, implemented in the operations of the telecommunications operator throughout the life cycle of the systems in question. The obligation is not intended to affect the product development cycle of equipment suppliers; it is intended to ensure that the security functions specified for the versions of facilities implemented by the telecommunications operator are taken fully into account or that their non-implementation is justified and the risks are managed in other ways.

BGP routing

The previous version of the regulation did not discuss the security issues related to BGP comprehensively. BGP is a central internet routing protocol, and any intentional or unintentional disturbances of it may have serious consequences for information security. The BGP routing protocol does not have built-in security features, which has led to a situation in which the security of BGP is mainly managed with security features built afterwards on top of the protocol. The security features selected for the Regulation are based on ENISA's BGP information security recommendations[7].

In the summer of 2022, the Finnish Transport and Communications Agency investigated the deployment status of BGP security features by the telecommunications operators. The survey focused on ENISA's information security recommendations[7] concerning the security of BGP.

Some of BGP's features improving information security have been mentioned as examples in these explanatory notes. Their use is not obligatory, because the Finnish Transport and Communications Agency did not consider them necessary at the time when this Regulation was issued. The necessity has been assessed based on the impact of the security features.

Taking account of both BGP's key role in internet routing as well as the internal lack of security of the protocol in question, the Finnish Transport and Communications Agency

[6] BSI Technical Guideline TR-03163: Security in Telecommunications Infrastructure and Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen – Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020) § 6(2) and Annex 1 https://www.ris.bka.gv.at/eli/bgbl/II/2020/301/2020070.
[7] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp.

has found it necessary to specify obligations for telecommunications operators that maintain and improve the status of BGP's security.

Specific requirements for interfaces

In the previous regulation, Chapter 3 applied to the prevention of and protection from interference in interconnection and customer interfaces, closure of unnecessary services and protocols and prevention of IP traffic in interconnection and customer interfaces. The development of communications networks, new use cases and service-based architecture solutions (service-based interface, SBI) have added new interfaces to the communications networks of telecommunications operators. In addition, the signalling protocols of older network generations are still widely used in parallel with the new signalling protocols.

In the survey on the Regulation implemented in the summer of 2022, the parties that issued a statement had varying opinions on the requirement to protect signalling interfaces. Some saw no need for more specific regulations. Others considered it a good idea but thought that it should remain a high-level requirement. One opinion noted that all measures used to ensure disruption-free operation of critical communications in public communications networks should be required from telecommunications operators. The parties giving their opinions saw no need to take the mobile network slicing security issues into account in the new version of the Regulation, or they thought that a high-level reference to the existing recommendations would be sufficient.

In the view of the Finnish Transport and Communications Agency, there will be a need to issue more detailed regulations on the protection of interfaces in the future as the communications networks develop. The Regulation is largely based on existing recommendations.

Filtering out malicious traffic in SMS and MMS services

The previous regulation did not include any specific information security obligations concerning SMS or MMS services. In recent years, however, these services have been used widely to spread malware and scam messages, which has required telecommunications operators to take measures to combat the problem.

In the survey implemented in the summer of 2022 before the Regulation was drawn up, the opinions on expanding the obligation to filter out malicious traffic to cover SMS or MMS services were neutral, or it was considered necessary.

The technical solutions and capabilities available for filtering vary somewhat depending on whether the SMS or MMS service is involved, among other things. The Finnish Transport and Communications Agency finds that in order to ensure the appropriate filtering capacity, there is a need to regulate on the matter. As options, the Agency has considered requiring a content-based capacity of filtering malicious traffic from both the SMS and MMS services in all cases, as well as an option in which the application of this requirement would be limited regarding the lesser used MMS services, in which there are no well-established solutions for filtering available, unlike for the SMS service. Taking account of the relatively very minor use of the MMS service, the Finnish Transport and Communications Agency does not consider it justified to require an ability for content-based filtering for this service without exception, when the costs it would presumably cause are weighed against alternative methods that can be used to address the spread of malware or scam messages via MMS messages. As a result, in the model chosen for the Regulation, the telecommunications operator can use other methods instead of content-based filtering in certain cases.

Measures on the filtering of outgoing email traffic from consumer connections

Concerning the obligation to filter unlimited email traffic, i.e. port 25, the Finnish Transport and Communications Agency has assessed the options of a) maintaining it as is, b) removing the obligation and leaving the filtering measure to be determined based on the *Open Internet Regulation*[8] and section 272 of the AECS, as well as c) adding an exception to the filtering obligation for situations in which the consumer requests the removal of the filtering measure.

In the autumn of 2022, the Finnish Transport and Communications Agency investigated the situation of restricting SMTP traffic in internet access services in other European countries. Based on the non-comprehensive information received from other supervisory authorities, outgoing email traffic to port 25 from consumer connections in particular is filtered in several countries, but there are also countries in which this traffic is not filtered at all by main operators. As a rule, it was also discovered that consumers nevertheless had the option of requesting the removal of the filtering measure when filtering is carried out. As far as it is known, in other countries this filtering is not based on a mandatory regulation, like in Finland.

In 2022, the Finnish Transport and Communications Agency issued a decision that, unlike the Regulation, applied to a similar filtering measure in certain corporate connections in which the Regulation does not require filtering.[9] The decision assessed whether the telecommunications operator had grounds to apply the restriction of outgoing email traffic to telecommunications port 25 that was mandatory for consumers also to certain corporate connections. In the situation assessed in the decision, there were no sufficient grounds for this when the matter involved connections other than consumer connections intended for data transfer over the mobile network with a fixed IP address. The decision did not comment on whether the restriction would be justified for corporate connections in other situations.

In the survey implemented in the summer of 2022 before the Regulation was drawn up, filtering unrestricted outgoing SMTP traffic from consumer connections was still considered necessary. The Finnish Transport and Communications Agency also requested opinions on whether the Regulation should be developed so that, upon the consumer's request, the telecommunications operator should remove the restriction from the connection. Two telecommunications operators that issued an opinion on the matter did not consider this justified. One opinion noted that establishing separate consumer connections that operate on their own rules for a few users would not be reasonable administratively or with regard to the costs.

The Finnish Transport and Communications Agency finds that keeping a filtering obligation concerning consumer connections in the Regulation in principle is still justified to prevent information security threats. The measure addresses the threat of malware aiming to send spam from a terminal device or malicious traffic caused by incorrectly configured email servers. It is estimated that removing the obligation would increase the amount of spam, even though the spread of spam sent from consumer connections is currently limited by the more commonly used DKIM and SPF methods as well as the use of various reputation-based systems that limit the use of IP addresses available for sending email from consumer connections.

With regard to maintaining the obligation, attention must also be paid to the effects of limitation on offering an email server from a consumer connection. It can be estimated that in consumer use, the filtering measure very rarely causes a significant hindrance

[8] Regulation (EU) 2015/2120 of the European Parliament and of the Council laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.
[9] Yritysliittymästä lähtevän sähköpostiliikenteen rajoittaminen (Restriction of outgoing email traffic from a corporate connection), Doc. no. Traficom/9900/09.00.00/2021.

to users, even if it restricts the implementation of an email server with the connection. It is not possible to estimate exactly how large a share of consumers would want to run their own email server via the connection in a situation in which filtering would not be used. However, it can be estimated that the user group in question would be fairly small, which is also indicated by the fact that in recent years the Finnish Transport and Communications Agency has only received a few enquiries on the harmful impact of filtering gate 25. In addition, connections such as those intended for corporate use, in which filtering measures are not used, are typically also available to customers.

Were the Regulation to require telecommunications operators to disable filtering upon the customer's request, this would cause costs to the operators. The telecommunications operator would need to implement an option in the provisioning environment to change the filters used on a connection-specific basis. Depending on the connection type, this may not even be reasonably feasible technically. According to the information received by the Finnish Transport and Communications Agency during the operation of the working group, this would be a laborious change for telecommunications operators. The change would have a cost impact that could affect the whole customer base. However, the actual costs incurred by the telecommunications operator are not known to the Finnish Transport and Communications Agency. It can also be noted that in some other countries such an option for an exception would seem to already exist. Nevertheless, when taking account of what has already been stated on information security and the effect of the restrictions on customers, it seems justified to consider that in principle the hindrances due to the potential change are greater than the benefits. The matter can be reassessed in connection with the next update of the Regulation, for instance.

Restriction on the application of the regulation to email relay service and secondary email relay service

The Finnish Transport and Communications Agency evaluated the options of keeping the application restrictions in their previous form or removing them from the Regulation. As a result of the assessment, the application restrictions have been partially removed from the Regulation as unnecessary.

Firstly, in the assessment of the Agency, there are no grounds to exclude incoming traffic that endangers the information security of systems used to provide secondary email relay services from the scope of the filtering obligation. In principle, applying the filtering obligation to other incoming malicious traffic is also justified. The previous regulation already made customer-specific exceptions possible based on agreement, and this will also be possible in the future. Secondly, there are grounds for also applying the obligation on filtering outgoing malicious traffic to the email relay service as a rule, so that the information security of this traffic, too, is ensured.

According to the information received by the Finnish Transport and Communications Agency, the filters used in the email relay service as well as the secondary relay service are in many cases currently the same that the telecommunications operator already uses otherwise. In any case, the Regulation is flexible concerning the methods that can be used for filtering out malicious traffic in different kinds of services. As a result, it is no longer necessary to include the same limitations of the scope of application in section 26 of this Regulation as in the previous regulation.

According to this and the previous regulation, the telecommunications operator providing email services must offer its customers as the primary alternative a secure connection between the customer and the electronic mailbox and between the customer and the outgoing email server. In the previous regulation, this obligation did not apply to the email relay service. In practice, this has meant that it has not been necessary to offer an encrypted connection to those users of an internet access service that are customers of another email service provider but who have wanted to use port 25 to send

email. In that case, they have been required to use the outgoing SMTP traffic email server of the telecommunications operator acting as the internet access service provider due to the filtering of the port (section 14.1 of the previous regulation, section 21.1 of this Regulation). The use of TLS encryption without authentication in port 25 is technically possible as such; however, in the understanding of the Finnish Transport and Communications Agency, in practice offering this option varies at the moment. Offering the encryption would support the Regulation's goals of promoting the information security of communications services and safeguard the confidentiality of electronic communications. As a result, it has been evaluated whether the limitation of the scope of application should be removed so that the encryption of the connection should also be offered when using port 25 for the email relay service.

When a customer uses the services of another email service provider with the email application on the terminal device, the filtering of port 25 does not prevent the customer from using the server of the customer's own email service provider to send email via port 587 or 465, for example. This means that a customer who wishes to use encryption can in any case use the server of the customer's own email service provider instead of the proxy server, if using a port other than port 25 is possible. In contrast, in the understanding of the Finnish Transport and Communications Agency, the filtering of port 25 prevents the implementation of an ordinary email server with a consumer connection in practice, unless the SMTP server of the customer's own internet access service provider is used as a proxy server (relay) for sending the messages. As a result, the Finnish Transport and Communications Agency finds that in the future it will be justified to require telecommunications operators to offer an option of encrypting the connection when using the email relay server, too. This is estimated to only cause minor costs due to making the necessary changes to the settings for those service providers who do not yet offer this option.

Obligations on communication to customers

Chapter 6 on communication to customers in the previous regulation has been removed from the Regulation. According to the assessment of the Finnish Transport and Communications Agency, the goals of the obligations in question are achieved appropriately already by applying the regulations at the level of the Act and Decree, and therefore there is no need to issue any more detailed mandatory regulations on the matter.

The Government Decree on Information to be Provided Before Drawing up a Communications Service Agreement (96/2021) contains provisions on providing information about the measures taken by the service provider if information security is at risk or in case of information security threats or vulnerabilities (section 1, paragraph 6). This essentially corresponds to section 21 of the previous regulation, which contained a general obligation to provide information on information security measures. In addition, the provisions of the Government Decree can also be considered to cover section 23 of the previous regulation on specific obligations to inform related to an email service concerning the principles of email traffic filtering. In addition, information must be provided on the processing of traffic data related to filtering under section 138, subsection 2 of the AECS. With regard to the email address management practices, it is found that providing the information within the scope of application of the obligation is currently a part of normal customer service practices.

Section 22 of the previous regulation on specific obligations to inform related to an internet access service applied to providing information on the information security risks related to the use of the connection and the related measures available to the customer. As an example, the explanatory notes mentioned offering an internet access service through an unencrypted WLAN connection, in which case the telecommunications operator must provide information on the specific risks to the confidentiality of communications related to the use of the connection. As far as is known, no publicly available

communications services are offered extensively through WLAN connections. In addition, the encryption of HTTP traffic and the use of VPN connections becoming more common limits the information security risks due to the lack of encryption of a WLAN connection somewhat. Insofar as an information security risk can affect a telecommunications operator, the instructions provided by the telecommunications operator to the user are provided for in section 246, subsection 3 of the AECS. According to the section, a subscriber shall maintain equipment or a system to be connected to a public communications network in accordance with instructions from the telecommunications operator so as not to endanger the information security of the public communications network or service. Furthermore, section 274, subsection 2 of the AECS provides for the obligation of the telecommunications operator to provide information on the measures available for combating the threat when the telecommunications operator informs subscribers or users of an information security breach involving the service of the telecommunications operator or a threat of it.

The Finnish Transport and Communications Agency has moved most of Chapter 6 of the previous regulation into recommendations in Chapter 7 of the Annex to these explanatory notes.

V. Preparatory work of the Regulation

The Finnish Transport and Communications Agency started preparing for the regulatory amendment by conducting a survey among telecommunications operators and other members of the public on their experiences and development ideas in the summer of 2022.[10] DNA Plc, Elisa Corporation, Telia Finland Oyj, Erillisverkot Group and Huawei Technologies Oy (Finland) Co. Ltd as well as a private individual responded to the survey. The responses were used in drawing up the draft of the Regulation.

In January 2023, the Finnish Transport and Communications Agency asked telecommunications operators to appoint participants to a working group for the regulation. Representatives from the following parties came forward and were appointed to the working group: Digita Ltd, DNA Plc, Elisa Corporation, FiCom ry, Finnet-liitto ry, Ikaalisten-Parkanon Puhelin, Karjaan Puhelin Oy, Line Carrier Oy, Telia Finland Oyj, Telia Inmics-Nebula Oy and Ålands Telekommunikation Ab. The working group met eight times in 2023. Drafts of the Regulation and the explanatory notes were discussed in the meetings of the working group.

The consultation was held […].

VI. Comments received through consultation

[to be completed during the processing]

VII. Changes and assessment of the impact of the Regulation

This Chapter describes the key amendments to the Regulation and their impact.

Chapter 1 of the Regulation

- After this, the goals of the Regulation are only described in the explanatory notes.

[10] Teletoiminnan tietoturvasta annetun määräyksen (67 A/2015 M) ajantasaistaminen: Kysely kokemuksista ja kehitysideoista (Updating the Regulation on information security in telecommunications operations (67 A/2015 M): A survey of experiences and development ideas), Doc. no Traficom/16241/09.09/2022: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=e80c3ac0-6941-4bba-bdcf-62c826646465&proposalLanguage=da4408c3-39e4-4f5a-84db-84481bafc744.

- The scope of application of the Regulation has been changed so that the application restrictions on email relay service and secondary email relay service have been removed from the Regulation. In addition, the expansion of the scope of application of the obligation to prevent interference that was already found in the previous regulation to include public authority communications was further extended to also cover communications services related to official communications.

- The definition of malicious traffic has been supplemented in the definitions, so that it more clearly covers the same situations in which section 272 of the AECS enables measures related to the processing of communications to implement information security.

- Instead of open mail servers, the matter being defined was changed to open mail relays so that the definition would correspond to the concept used in the obligations of the Regulation.

- The definitions of text and multimedia message services that are used in the new Chapter 5 have been added to the definitions.

Chapter 2 of the Regulation

- The section 'Consideration of information security issues' has been expanded compared to the previous regulation. The aspects to be taken into account correspond to the division into eight information security domains followed in ENISA's guidelines. Each aspect is specified in the new sections that take advantage of the security goals defined by ENISA for each domain, taking into account, however, the fact that security goals are also partially provided for in other regulations of the Finnish Transport and Communications Agency. In this regard, the update of the Regulation was caused by a need to update the Regulation and take account of the new architecture changes and use cases of 5G networks in particular.

  Even though the Regulation no longer uses the original division in accordance with the previous regulation into administrative information security, personnel security, security of hardware, software and data communications, security of information material and usage as well as physical security as is, the Regulation is still intended to cover all of these aspects.

  The greater detail of the Regulation nevertheless causes some extra work for telecommunications operators, especially if they must implement and document new measures. The relative impact is the greatest for the small telecommunications operators, where the material produced by ENISA may not have been used before on a large scale. Meanwhile, it is also true that specifying the Regulation provides clearer guidance than before for telecommunications operators in implementing the necessary information security measures, which simplifies the specification of the required measures and therefore also the application of the Regulation to some degree.

  It is estimated that the amendment will have a clear impact on strengthening information security, because the Regulation provides clearer guidance than before for implementing the specified information security goals. As for the implementation of the information security goals, materials such as the information security controls specified by ENISA can be used; it is easy to combine them with the obligations in accordance with the Regulation, which also supports documentation.

  In addition, the amendment promotes the effectiveness and predictability of the monitoring and inspection activities of the Finnish Transport and Communications

Agency, when the implementation of the Regulation can be supported with the clearly defined information security goals and controls by ENISA.

- The obligation to keep the results of the risk management process has been extended from the previous one processing period to the three most recent processing periods. The earlier documentation for one processing period has not been sufficient to confirm the continuity of risk management. In the ISO/IEC 27005 standard, the requirement applies to two processing periods. Because keeping the results of more processing periods does not cause significantly more extra work, the requirement has been extended to three processing periods in the Regulation.

- Managing the information security risks related to subcontracting and supply chains has been raised to the level of the Regulation as a particularly important set of issues. In addition, matters such as maintaining threat information have been included in the Regulation as new issues.

- Procedures for following the mobile network standards have been included in the Regulation as a new requirement. The obligation requires telecommunications operators to adopt procedures that ensure the implementation of security functions described by the standards in the 4G and 5G networks of the telecommunications operator. However, the Regulation allows an option to not implement a function described in the standards, if the telecommunications operator has a justified reason to do so and the risks have been managed in other ways. This allows telecommunications operators to choose specifying and documenting compensating measures as an alternative to implementing the security functions of the standards.

  The obligation itself is not estimated to cause any significant additional costs to the mobile network telecommunications operators, because the aim is compliance with the standards in question in purchases and by the equipment manufacturers in any case. Taking the procedures and security functions into account and potentially not implementing them and documenting the compensating measures still causes some costs. As a result of the documentation obligation concerning the procedures, the telecommunications operators must include the monitoring of the standards in question as a part of their documentation and other processes, such as configuration management.

- Identifying the customer to ensure information security has been added to the Regulation as a new item.

  It is estimated that the companies that follow the best practices in the field will not incur any significant additional costs, because this involves measures that any telecommunications operator should follow in any case. However, the obligation emphasises the need for continuous development. If the company's practices have not been at a sufficiently high level before, the specific obligation supports the monitoring of the practices and highlights the need of these companies to develop their practices.

- The section on the protection of the management network and management connections has been specified. A requirement on drawing up operating principles and procedures has been added to the section in addition to a requirement on the assessment and management of risks related to the terminal devices used for management.

Chapter 3 of the Regulation

- The first subsection of the section 'Prevention of and protection from interference in interfaces' has been expanded so that it also applies to the prevention of interference in all other communications networks instead of only public communications networks. The second subsection has been expanded to include application interfaces, and it has been clarified that the obligation applies to both communications networks and services.

- The section 'Protecting interconnection interfaces and filtering the traffic' has been expanded compared to the previous regulation. The section mainly discusses the protection of the BGP routing protocol, which was discussed mainly with regard to route advertisements in the previous regulation. The most important procedures based on ENISA's recommendations have been added as aspects of the obligations.

  The Regulation includes more detail than before, and this causes extra work for telecommunications operators in some respects. Most of the obligations have been already taken into account at least to some degree, and in fact the Regulation mainly reinforces existing practices. The greater detail included in the Regulation than before guides telecommunications operators to implement the necessary protection and filtering measures with regard to BGP routing.

  It is estimated that the changes will promote and maintain the security of the BGP routing protocol. Because the most important security features based on ENISA's recommendations have been added as aspects of the Regulation, it is also considered that this will make the implementation of the Regulation easier. The use of ENISA's recommendations as the basis will also facilitate the inspection activities of the Finnish Transport and Communications Agency as well as the monitoring and development of the security features related to the BGP routing protocol.

- A new obligation on the protection of mobile network interfaces has been added to the Regulation. The life cycle of mobile network generations is very long; for instance, the SS7 signalling protocol, originally drawn up in the 1970s and developed for a very different threat environment in its time, is still in use. Later, efforts have been made to prevent the security deficiencies of signalling protocols with instructions and recommendations to combat known weaknesses.

  It is estimated that the obligation will not cause additional costs to telecommunications operators, if the procedures of the telecommunications operator are already compliant with the recommendations and best practices in the field. Along with the changes in the architecture of the 5G network, the importance of protecting different application interfaces is also emphasised, and new interfaces that should be taken into account in particular include the security of key functionalities, such as slicing and edge computing. For slicing, it is important that unauthorised access to both the resources and the management interface of the slice is prevented. It is also important to strengthen the radio interface access control as needed with slice-specific access authentication. It is estimated that protecting the management user interface and the radio interface according to the best practices will not cause any additional costs to the telecommunications operators.

Chapter 5 of the Regulation

- Filtering text and multimedia message traffic has been added to the Regulation as a new issue. As a rule, the obligation is not estimated to require any significant new investments from telecommunications operators.

Chapter 6 of the Regulation

- The restrictions on the scope of application concerning email relay service and secondary email relay service have been removed from the Regulation as unnecessary. The changes promote information security, but it is estimated that they will not have any significant impact on the activities of telecommunications operators. Depending on the practices of the telecommunications operator, they may not require changes to the previous practices. In some cases, changes may need to be made to the settings of the email service.

Removed obligations

- Chapter 6 of the previous regulation on communication to customers has been removed from the Regulation (see: 'Other implementation options'). The matters discussed in the chapter have been moved to the Annex to these explanatory notes, which has been supplemented in general.

DETAILED GROUNDS AND APPLICATION INSTRUCTIONS

Chapter 1 Scope of application and definitions

This chapter explains Chapter 1 of the Regulation, i.e. the scope of application and definitions of the Regulation.

1. Scope of application

1.1 General scope of application of the Regulation

The Regulation applies to public telecommunications operations. Therefore, the Regulation is binding for all telecommunications operators regardless of what type of service they provide. The Regulation also applies to telecommunications that are of minor significance and therefore do not have a telecommunications notification duty referred to in section 4 of the AECS.

Pursuant to section 3, paragraph 27 of the AECS, telecommunications operator means a network operator or a communications service operator offering services to a set of users that is not subject to any prior restriction.

Network service is defined in section 3 of the AECS, meaning service a telecommunications operator provides comprising a communications network in its ownership or for other reasons in its possession for the purposes of transmitting or distributing messages. A telecommunications operator offering a network service is also referred to in the AECS as a *network operator*. Under the Act, a *communications network* means a system comprising cables and devices joined to each other for the purpose of transmitting or distributing messages by wire, radio waves, or by other electromagnetic means. Communications networks used to provide communications services to a set of users that is not subject to any prior restriction are referred to as *public communications networks* in the Act. The communications networks primarily used for transferring or transmitting television and radio programmes or other material conveyed in identical form to all recipients are *mass communications networks* according to the Act.

According to section 3, paragraph 37 of the AECS (in Act 1207/2020), a *communications service* means a service consisting wholly or mainly of the conveyance of communications in a communications network, a transmission and broadcasting service in a mass communications network, and an interpersonal communications service. The Regulation applies to both interpersonal communications services based on numbers as well as those independent of numbers.

The requirements of the Regulation have been divided under five topics:

- Chapter 2 lays down general information security requirements on telecommunications operations for all communications networks and services.
- Chapter 3 focuses on the information security measures for interconnection, application and customer interfaces.
- Chapter 4 contains specific requirements concerning the information security of internet access services.
- Chapter 5 contains specific requirements concerning the information security of SMS and MMS message services.
- Chapter 6 addresses specific requirements of email services.

The Regulation *is not be applicable to activities other than public telecommunications operations*. Network or communications services or content services provided to a limited set of users do not constitute public telecommunications operations. Examples of content services outside the scope of the Regulation are website content, discussion forums, and the contents of television and radio programmes.

Therefore, the Regulation does not apply to *communications providers* other than telecommunications operators, i.e. *corporate subscribers* and *other communications providers*.[11] The Regulation does not impose obligations to parties such as corporate subscribers. The Regulation does not apply to cases such as the management of an internal communications network of a company or organisation, because the set of users in this case is subject to a prior restriction, and it does not constitute public telecommunications operations. Corporate subscribers are *subscribers* as referred to in the AECS. Even if the telecommunications operator providing the service is not responsible for an internal communications network or service, it is responsible for the service it provides to the subscriber.

1.2 Application of the Regulation to public authority networks and communications services related to public authority communications

Even though the Regulation otherwise only applies to telecommunications operations, section 15.1 of the Regulation applies to public authority networks and communications services related to public authority communications when they are interconnected with a public communications network or a publicly available communications service, i.e. the network or service of a telecommunications operator. In other respects, the Regulation does not apply to public authority networks.

Pursuant to section 3, paragraph 39 a of the AECS (in Act 52/2019) a *public authority network* means a communications network built for the needs of government measures and state security, national defence, public order and security, border security, rescue operations, maritime rescue operations, emergency response centre operations, immigration, health care and social welfare emergency services, rail transport safety or civil defence. An example of such a public authority network is VIRVE.

Communications service related to public authority communications refers to a service by a *provider of a communications service related to public authority communications* referred to in section 3, subsection 39 c of the AECS, i.e. an information and communications technology service in time-critical mobile broadband communications by the authorities.[12]

[11] According to section 3, paragraph 36 of the AECS, a communications provider means a telecommunications operator, corporate subscriber or other party that conveys electronic communications for other than personal or comparable customary private purposes (hereinafter other communications provider). *Corporate subscriber* means, according to section 3, paragraph 41 of the AECS, an undertaking and an entity which subscribes to a communications service or a value-added service and which processes users' communications, traffic data or location data in its communications network.
[12] In accordance with its general scope of application, the Regulation also applies to network service related to public authority communications that is considered a part of public telecommunications operations (HE 226/2018 vp, p. 49).

The Regulation does not impose obligations on local networks that do not constitute public telecommunications operations. Depending on their implementation method, they may also be under an obligation provided for in the AECS. If the local network is connected to the public communications network, information security must also be ensured in the design and use of local networks.[13]

2. Definitions

This chapter details the definitions of the Regulation. The Regulation does not redefine concepts that have been defined in the AECS. The definitions have been drawn up to avoid conflict with the definitions provided for in the Act.

2.1 Customer interface

In this Regulation, a customer interface means an interface through which the communications network, terminal or application of a customer of the telecommunications operator is connected to a public communications network. Customer terminals include modems, switches and computers owned and managed by the customer. A customer interface is also known as a User to Network Interface (UNI interface).

2.2 Open mail relay

Open mail relay means an email relay system that a third party is able to use for relaying email messages without authorisation. In this Regulation, a relay system refers to email servers or web proxy servers or software installed to a web server that can be used to relay email messages.

2.3 Malicious traffic and spam

In the Regulation, malicious traffic means electronic messages that jeopardise the information security of communications networks or services connected to them as well as information systems, at which actions may be targeted in the manner referred to in section 272, subsection 1, paragraph 2 of the AECS in order to safeguard the possibilities of the sender or recipient of the message for communications, or messages that are used to prepare for payment fraud referred to in Chapter 37, section 11 of the Criminal Code to be implemented on a wide scale via communications services. The concept is referred to in sections of the Regulation on matters such as text and multimedia message services as well as email services in which obligations on the filtering of malicious traffic are set. The aim is for the concept to cover all situations in which the processing of messages and traffic data can be processed under section 272 of the AECS in order to ensure information security.

Information security means the administrative and technical measures taken to ensure that data are only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data and information systems can be used by those who are entitled to use them. Depending on the case in question, an electronic message may refer to an IP packet, email or SMS message or control traffic between network elements, for example.

Therefore, malicious traffic can be traffic caused by denial-of-service attacks, spamming or the spreading of worms. The harmfulness of malicious traffic must be considered from the perspectives of both the service provider and the customer. In practice, this could mean that safeguarding the availability of a communications service may require actions to both ensure the capability of the service provided by the service provider and

[13] Finnish Transport and Communications Agency: Ohje paikallisten matkaviestinverkkojen kyberturvallisuudesta ja riskienhallinnasta. (Instructions on the cyber security and risk management of local mobile networks.) Traficom Research Reports 8/2023, p. 19–20, https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohje-paikallisten-matkaviestinverkkojen-kyberturvallisuudesta-ja-riskienhallinnasta.

to maintain the service level provided to the user. The type of malicious traffic that is prevented depends on the applicable obligation and the situation in which it is applied (such as which communications service is involved).

2.4 Filtering

Filtering means preventing or restricting the malicious traffic defined above. Examples of filtering are rejecting outgoing traffic from customer interfaces that uses forged source addresses, limiting the capacity reserved for certain types of internet traffic either in specific interfaces or on the basis of the application protocol used in the traffic, or preventing the transmission or reception of email messages.

Filtering also refers to removing from communication any malicious software that impairs information security, e.g. removing malware from email messages.

In addition to the above, filtering may also refer to other technical measures to control traffic that compromises information security.

2.5 Email service

Email service means the transfer, transmission and reception service of electronic mail messages that uses internet name services, i.e. DNS services in the transmission of messages. Figure 1 is a diagram of an email service, the different functions and the protocols to be used between functions.

An email submission service means a service in which a customer sends a message via the mail submission agent (MSA) of the service provider. A transmission service means a service in which an email message is received, (processed) and forwarded to a destination agreed with the customer. A delivery service means a service in which the customer's email messages are received by a mail delivery agent (MDA) and delivered to the customer's electronic mailbox.

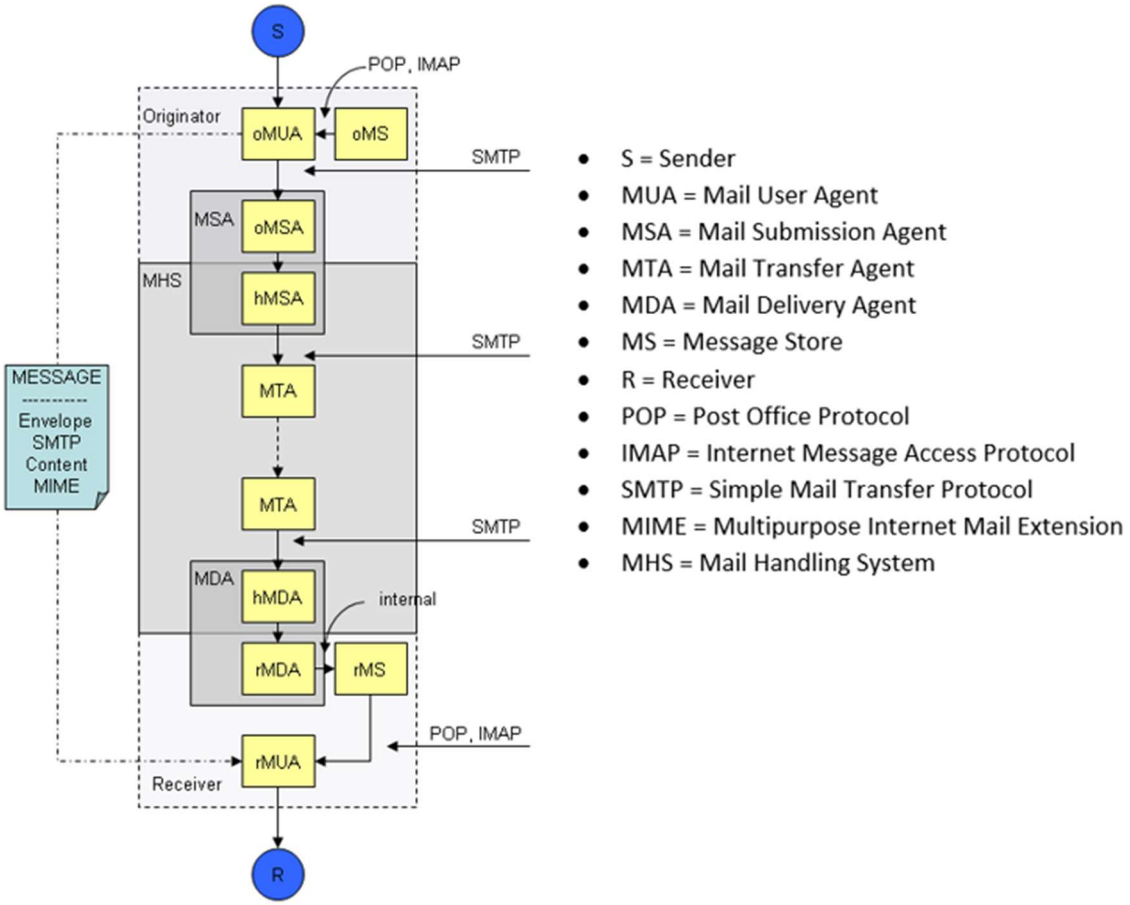

Figure 1. A diagram of an email service.

Outgoing email traffic refers to email messages sent by customers that are transferred via the mail submission agents (MSA) of the service provider to the mail transfer agents (MTA).

Incoming email traffic, on the other hand, means incoming email messages that are transferred via the mail delivery agents (MDA) of the service provider to the electronic mailboxes of customers (MS).

The scope of application of the Regulation also includes the *email message relay service* and *secondary email relay service*, which have not been defined separately in the Regulation.[14]

Email relay service means a service provided by a telecommunications operator engaged in email services in which the telecommunications operator forwards or redirects messages through its own email servers (so-called message redirection service).

The obligations concerning email also apply to a secondary email relay service, i.e. an email proxy server backing up the customer's own email service. In such a service, the customer's primary MX record(s) refer to the customer's own email server(s). In this case, the customer's incoming email traffic goes through the secondary email proxy servers of the email service provider only when the customer's own servers are unavailable. In principle, the obligations on filtering incoming email traffic also apply to such

[14] See section 'Other implementation options' on changes to this Regulation with regard to the scope of application of certain obligations.

a service, but the Regulation reserves an opportunity to agree otherwise on the matter with the customer.

2.6 Component of a communications network or service

Communications network or service component refers to a network element, device or information system comprising a communications network or service or utilised by a communications network or service. The concept is used in several regulations of the Finnish Transport and Communications Agency.

Communications network or service components include mobile switching centres, base station controllers, base stations, text message centres, DSLAMs, name servers, network access control servers, switches, routers, SIP application servers and intelligent network components. Communications network or service component does not refer to transmission links or network element parts such as mobile switching centre CPUs. Telecommunications terminal equipment are not communications network or service components, either.

A component of a communications network or service can also be implemented in a virtualisation environment (see Chapter 6.6 of the explanatory notes).

2.7 Interconnection interface

In this Regulation, an interconnection interface means a connection interface between telecommunications operators' communications networks or services. This is also known as a Network to Network Interface (NNI interface).

2.8 Text and multimedia messaging services

In this Regulation, a *text messaging service* means a transmission service for short messages (SMS message) containing alphanumeric characters and special characters or in binary format via a short message centre of the mobile network.

In turn, in the Regulation a *multimedia messaging service* means a service for transmitting short messages that contain multimedia objects, i.e. MMS messages such as images, sound, video and edited text via the multimedia message centre of the mobile network.

Chapter 2 General information security requirements

This chapter explains the requirements concerning all communications networks and services of a telecommunications operator laid down in Chapter 2 of the Regulation. In addition, section 10 of the Regulation includes specific requirements for mobile network telecommunications operators.

3. Consideration of information security issues

3.1 Aspects of information security

Information security is an essential element of the quality of communications networks and services provided by a telecommunications operator. The consideration of the various areas of information security in telecommunications is important in all stages of the life cycle of communications networks and services: in coordinating, implementing and maintaining the service as well as in terminating the service. To make the consideration of information security an everyday routine, it is justifiable to require a telecommunications operator to establish the processes and procedures that it will follow in the implementation of information security measures.

Information security measures and the documents that describe the measures must take several matters into consideration. Section 3.1 of the Regulation lists the topics to be taken into account that correspond to the division of eight security domains used in ENISA's guidelines on information security measures under the European Electronic Communications Code Directive (EECC).[15] The aspects to be taken into account include:

1) information security and risk management;
2) personnel security;
3) information system and telecommunications security as well as physical security;
4) information secure operations and change management;
5) detection and management of situations that disturb or threaten information security;
6) continuity management;
7) monitoring, testing and information security assessments; and
8) maintaining threat awareness as well as providing information to users and subscribers.

Minimum requirements on the different aspects will be set later in sections 4–9 of the Regulation, which in turn take advantage of the security objectives defined by ENISA for each security domain. Requirements related to the aspects are also set in other regulations of the Finnish Transport and Communications Agency, and this Regulation does not set detailed obligations on all aspects. In fact, the more detailed requirements related to aspects 5–6 as well as partially to aspects 7 and 8 are set in the Regulation on disturbances in telecommunications services, which includes requirements on matters such as detecting information security breaches and recovery procedures as well as submitting notifications related to information security breaches. Aspect 5 includes information security breach management procedures, detection of information security breaches as well as the procedures for processing notifications related to information security breaches.[16] As for aspect 6, it refers to ensuring the continuity of telecommunications operations in case of various serious disruptions, which includes e.g. procedures for restoring operations in case of serious disruptions as well as backups.[17] The monitoring referred to in aspect 7 includes, in addition to what has been stated in section 8 of the Regulation, the monitoring of events significant to information security by means of logging in particular.[18] In addition to maintaining the threat awareness of the telecommunications operator as discussed in the Regulation, aspect 8 covers informing users and subscribers of information security threats so that they can deploy necessary protective measures, thereby also promoting the information security of communications networks and services.[19] Recommendations concerning the aspect related to informing users and subscribers are issued in section 7 of the Annex to these explanatory notes.

The Regulation sets the most important information security objectives and measures for most of the different aspects of information security, but in principle it does not set any detailed requirements on how or by implementing which information security measures (controls) these different matters should be taken into account in all situations. The appropriate measures for implementing information security vary somewhat by telecommunications operator, based on matters such as the scope of the activities

[15] ENISA Guideline on Security Measures under the EECC, 4th Edition, July 2021 (hereinafter also ENISA GL).
[16] ENISA GL SO18–SO20. Among other things, aspect 5 covers the coordinated first response function in case of an information security breach, maintenance of a contact point for notifications as well as abuse functions, meaning a function intended as a contact and service point in cases related to information security breaches of customers and external interest groups in connection with the provision of internet services.
[17] ENISA GL SO21–SO22.
[18] ENISA GL, SO23.
[19] ENISA GL, SO29.

as well as the networks and services offered and the different kinds of threats related to them. The information security measures must be commensurate with the seriousness of threats, level of technical development to defend against the threat and costs incurred by these measures (AECS, section 243, subsection 3).

The matrix of 5G information security measures[20] drawn up by ENISA includes both general controls suitable for all telecommunications operations that are based on e.g. the ISO/IEC 27000 series of standards as well as technology-specific controls that are based with regard to the 5G network on the TS 33.501 standard by 3GPP, among other things. The matrix can also be used in implementing the obligations of the Regulation. The minimum requirements related to the topics of the Regulation have also been discussed in the other regulations of the Finnish Transport and Communications Agency or elsewhere in legislation, in addition to which there may also be telecommunications operator specific requirements due to agreements on ensuring the information security of telecommunications operations. In terms of section 3.1 of the Regulation, the essential requirement is that the telecommunications operator must identify the requirements that are relevant to its operations and the procedures that best serve their implementation. It is also possible to use other, equally effective measures instead of the information security controls mentioned as examples in these explanatory notes.

3.2 Information security documentation

Section 3.2 of the Regulation requires the telecommunications operator to have documents on how it implements the general requirements of Chapter 2 of the Regulation on information security in its operations. The documents create a basis for systematic information security development and management and help with allocating investments in information security. The documentation also helps the Finnish Transport and Communications Agency verify, where appropriate, that the telecommunications operator meets its obligations in terms of safeguarding information security.

As the Regulation does not specify the different documents that the telecommunications operator must have, this is left to the discretion of the telecommunications operator. The important thing is that the documentation is up to date and it can be used to verify that all aspects of information security within the scope of the documentation obligation as well as the more detailed obligations have been taken into account in the operations of the telecommunications operator.

4. Information security and risk management

4.1 Information security policy and operating principles

Section 4.1.1 of the Regulation requires the telecommunications operator to draw up appropriate information security guidance documents that include an information security policy as well as the operating principles that specify it. In the information security policy, the top management of the telecommunications operator commits to implementing information security and defines the intention and principles of information security for ensuring the information security of the communications network and service components and other objects to be protected related to telecommunications operations. When drawing up information security guidance documents, the telecommunications

[20] ENISA 5G Security Controls Matrix, May 24, 2023, https://www.enisa.europa.eu/publications/5g-security-controls-matrix.

operator can rely on publicly available information security standards or ENISA's recommendations, for example.[21] Requirements on the information security policy and information security management systems in general have also been presented e.g. in the standard ISO/IEC 27001.

The Regulation requires (section 4.1.1 and parts of section 3.2) that the telecommunications operator reviews its information security policy and the operating principles that implement it regularly and maintains (updates) them as needed. In accordance with the Regulation, the changes in the operating environment, the security incidents detected, training and predictable changes in the information security threat environment must be taken into account in the review. In practice, when assessing any changes to the information security policy or operating principles that may be required due to the incidents detected, it would be good to take into account whether the matter involves an intentional violation or if the incident is due to lack of training, for example, because this affects the practical measures that are reasonable for the telecommunications operator to implement due to the incident.

4.2 Risks

A risk is the combination of the likelihood of a negative factor or event and its effects.[22] In the Regulation, an information security risk means an accidental or deliberate event that compromises the confidentiality, integrity or availability of telecommunications operations. An information security risk differs from an information security threat in that its likelihood and effects have been assessed.

For instance, information security risks may arise from the following:

- human error
- gaps in or non-compliance with the instructions provided to the personnel
- theft or vandalism
- flaws and malfunctions of equipment, systems or software
- malware spread
- destruction of data
- fire or flood
- errors and neglect on the part of a subcontractor or a member of a partner network.

Risk management is a process that aims at identifying risks, reducing their likelihood and/or impact to an acceptable level and maintaining the achieved level. The purpose of risk management is to protect the organisation and its ability to perform its operations, taking into account economic factors.

The objective of risk management requirements is to ensure that the telecommunications operator is aware of the consequences of the potential realisation of the risks and knows whether the risk-mitigating measures are adequate. The objectives of risk management include:

- speeding up recovery after information security problems
- reducing the costs and damage caused by information security problems
- helping in allocating investments that improve the information security of telecommunications
- improving the quality and productivity of telecommunications
- optimising, in terms of finances, the management of risks related to telecommunications operations

[21] E.g. ENISA GL and ENISA 5G Supplement to the Guideline on Security Measures under the EECC, 2nd Edition, July 2021.
[22] Vocabulary of Comprehensive Security, TSK 50, Helsinki 2017.

- preventing the realisation of risks.

The contingency planning obligation of telecommunications operators is provided for in Chapter 35 of the AECS.

Identifying and addressing risks

Section 4.1.2 of the Regulation requires the telecommunications operator to identify and manage the risks related to its telecommunications operations and their continuity. Risk management means that the telecommunications operator assesses the information security risks and processes them, meaning that it implements appropriate risk controls and approves the potential residual risks while ensuring that repeated assessments produce comparable results. As a result of addressing the risks, the telecommunications operator determines an acceptable risk level for its operations and takes appropriate measures (through controls, i.e. various measures that mitigate the risks or their consequences) to implement it. This means that practical risk management requires the determination of responsibilities and schedules. In addition, an appropriate owner that reviews and approves the residual risks must be specified for risks. The authorisation to approve residual risks must be granted at the level of the telecommunications operator's organisation in accordance with the approved information security policy.[23]

The Regulation does not impose an obligation to comply with a specific risk management standard; instead, operating models on different levels can be applied depending on the scope and nature of the telecommunications operations. Examples of standards and publications in which risk management has been discussed include the following: ISO/IEC 27005 and NIST 800-30 Risk Management Guide. Risk management models vary from company to company, and there is no single model that would suit every purpose.

The Regulation requires risk management as a continuous process. In accordance with this, risks and their management methods must always be assessed when the situation changes, such as a part of the purchasing and deployment process of new services, in connection with changes (regarding change management, see 7.2), or after a potential risk has been realised.

For a mobile network telecommunications operator, it is crucial to take special account of the internal and external threats to the components of the 5G networks and services, some of which are new. The Regulation requires the telecommunications operator to have a risk management process with the aim of managing and mitigating the risks caused by the threats to the assets in question, among other things. In addition, there are grounds for paying special attention to the risk assessment of virtualisation environments and edge computing units, for instance.

Documentation of the process and its results

According to section 4.2 of the Regulation, in order to monitor the continuity of risk management and compliance with the requirements, the telecommunications operator must keep the documented results of the risk management process for at least three years or for the three most recent processing periods, whichever storage period is the longest. If there are fewer than three processing periods during the three years, this means that the documentation must be stored longer than three years, while if there are more than three processing periods during the three years, all of their documentation must be stored.

[23] ENISA GL SO2, 5G Security Control Matrix: M07–M013, SO2-001, SO2-003–SO2-005 and ISO/IEC 27005:2018: 8 and 9.

Documenting the risk assessment and keeping the previous results provides valuable information on the approach to similar risks during previous processing periods. For example, the result of assessing the risks may be the processing of new threat information that may nevertheless not lead to changing the risk assessment.

4.3 Information security roles and responsibilities

According to section 4.1.3 of the Regulation, the telecommunications operator must specify the appropriate information security roles and the related responsibilities in accordance with the information security policy and the operating principles used to implement it.

Clearly defined and documented information security roles and responsibilities known to the whole personnel enable systematic implementation of information security and an information security management structure that supports implementing information security in daily work. Depending on the telecommunications operator's scope of operations and the nature of the different information security roles, the responsibility may be a part of the person's overall job description. Where applicable, support for the implementation can be found in the measures and information security controls in accordance with ENISA's guidelines.[24] In particular, in practice it is justified to identify clearly the obligations related to ensuring the information security of key parts of the communications network and other major targets to be protected.

According to the Regulation, the telecommunications operator must also prevent the creation of combinations of responsibilities and tasks that endanger information security as far as possible by separating conflicting tasks and responsibility areas from each other, such as requesting, approving and granting access rights.[25] The creation of such combinations of responsibilities and tasks can be allowed temporarily, if the risks related to the situation have been assessed and the appropriate management measures have been taken. However, for example, if the operator in question is small, it may not be possible to entirely separate all conflicting tasks in practice; in that case, the risks due to the activities should be managed in other ways, such as by technical monitoring and logging the measures.

It is appropriate to document the areas under the responsibility of a single individual or one key persons and to review the risks detected in connection with the situation.

Section 5.1.2 of the Regulation provides for the information security skills and training of the personnel.

It is good to note that a review of the responsible persons and the relationships between information security roles must be carried out regularly as a part of maintaining the information security policy and operating principles required by section 4.1.1 of the Regulation. In practice, changes in the operating environment, changes in personnel and any incidents detected should be taken into account when implementing this in practice (see also sections 4.1.3, 5.1.3 and 5.1.4 of the Regulation).

4.4 Supplier relationships

Supplier relationship management is an integral part of the telecommunications operator's risk management. For example, insufficient risk management with regard to the subcontracting chains of the key parts of the communications network or other functions important to information security may lead to endangering the information security of the whole communications network or service.

[24] ENISA GL SO3, 5G Security Control Matrix: M014–M018, SO3-001 and ISO/IEC 27002:2022: 8.8.
[25] Correspondingly, ISO/IEC 27002:2022: 5.3.

Section 4.1.4 of the Regulation requires the telecommunications operator to draw up specifying measures and risk management processes to manage the risks in the supply chain. The section corresponds to SO4 in accordance with ENISA's guidelines, and the measures specified by ENISA and the information security controls that support them can help with its implementation where applicable.[26]

Therefore, in practice the requirement of the Regulation means that the telecommunications operator must have procedures in place for ensuring that third parties, such as equipment, software and service providers as well as interconnection partners and other partners, comply with the level of information security required by the telecommunications operator. In practice, the telecommunications operator should specify appropriate information security requirements for agreements with third parties. The requirements ensure the realisation of the telecommunications operator's information security policy or other instructions. For example, the telecommunications operator can require that the products, services and operations of the supplier comply with appropriate security standards.

The operating principles concerning supplier relationships should identify the procedures for ensuring information security in supplier relationships and the procedures related to the monitoring of suppliers, as well as the management of any residual risks that the supplier's own measures have not reduced to the level approved by the telecommunications operator.

The operating principles should include maintaining a register of the agreements with suppliers that can be used to review the agreements regularly, if necessary, to ensure that the information security requirements are up to date, for example.

The telecommunications operator should specify appropriate procedures for protecting the data to be transferred or processed for supplier relationships (see also section 6.1.4 of the Regulation) as well as the obligations on the confidentiality of data.[27]

The realisation of information security requirements in the operations of the third party should also be monitored. This can be done through audits, for example, or by means such as requiring regular, independent reporting on the supplier's information security management methods and their effectiveness.

In addition, the operating principles should include the monitoring of security incidents due to the actions of third parties and e.g. methods for ensuring that the software components supplied by the third party are authentic and unaltered.[28]

In accordance with section 4.1.1 of the Regulation, the telecommunications operator must regularly review and update its specifying measures, taking account of the changes in the operating environment as well as the incidents detected in the operation of the suppliers.

5. Personnel security

5.1 Reliability of the personnel

According to section 5.1.1 of the Regulation, the telecommunications operator must perform appropriate checks in order to ensure the reliability of their personnel within the framework of the applicable legislation, if this is necessary with regard to the duties and responsibilities of the person. The section corresponds to SO5 in accordance with ENISA's guidelines, and the measures specified by ENISA and the information security

[26] ENISA GL SO4, 5G Security Control Matrix: M019–M026, SO4-004 - SO4-014 and SO4-016 - SO4-048.
[27] ISO/IEC 27002:2022: 5.20.
[28] Concerning methods, see for example: NIST, Defending Against Software Supply Chain Attacks (April 2021).

controls that support them, for instance, can help with its implementation.[29] The telecommunications operator must define the operating principles and procedures for implementing the background check of people in advance, because the telecommunications operator must document how it takes the requirement into account and draw up an information security policy and the related targeted operating principles (sections 3.2 and 4.1.1 of the Regulation).

The telecommunications operator must carry out an appropriate background check on the persons selected in the recruitment process, if this is considered necessary with regard to the person's duties. When implementing background checks, the applicable legislation concerning data protection in working life and personal security clearances must be taken into account, such as the Security Clearance Act (726/2014) and the Credit Information Act (527/2007).

The background checks should be in proportion with the identified risks and the classification of the data being processed. The background check process must also be applied to agency contract workers and external suppliers, when this is justified in connection with the risks related to the use of such personnel. If an acceptable level of risk cannot be achieved by the means of a background check process, the telecommunications operator should have procedures for the management of the residual risks. If the residual risks cannot be reduced to an acceptable level, the person should not be assigned to the task in question. Residual risks can be managed by means such as access control or by implementing separate supervision.

When carrying out background checks and specifying the scope of the checks, attention should be paid especially to the roles in which the person has physical or logical access to the critical parts of the mobile network or other key communications network, or other important targets to be protected.

The obligation is also related to the obligation in accordance with section 5.1.3 of the Regulation to manage the risks due to changes in the duties of the personnel. When a person transfers into such a role within the telecommunications operator, the telecommunications operator must assess whether the previous background check is sufficient and, if necessary, carry out a background check that corresponds to the role. In any case, the background checks should be repeated at appropriate intervals as needed, taking account of the periods of validity of the security clearances.

If necessary, the telecommunications operator must review and update the targeted operating principles and procedures drawn up in order to implement the background check, taking account of the changes in the operating environment and threats as well as the security incidents detected, as section 3.1 of the Regulation requires in practice.

5.2 Information security skills of the personnel and their development

According to section 5.1.2 of the Regulation, the telecommunications operator must have procedures for ensuring the sufficient information security skills of the personnel and maintaining them. The telecommunications operator must provide its personnel information security training that can be either general or focused on a specific task as needed. Monitoring the participation in trainings is justified. General information security training should take account of issues such as preventing the spread of malware and aim especially to develop and maintain the awareness of personnel and their ability to act to prevent phishing.[30]

[29] ENISA GL SO5 and 5G Security Control Matrix: M027–M030 and SO5-001. See also ISO/IEC 27002:2022: 6.1.
[30] ENISA GL SO6 and ISO/IEC 27002:2022: 6.2, 6.3, 6.6 and 8.7. See also https://www.kyberturvallisuuskeskus.fi/en/news/tips-identifying-suspicious-websites.

The personnel of the telecommunications operator must be made aware of the information security policy and targeted measures as well as their goals and effect on their own duties.[31]

In practice, the content of information security training should be regularly reviewed and updated, taking account of the changes in the operating environment, the results of assessments and any security incidents detected.

In order to verify the information security skills of the personnel, the telecommunications operator can implement procedures for testing the information security skill level of the personnel. In addition, the telecommunications operator can implement methods for its personnel to report any information security threats, breaches, risks or development targets they have observed; the reports can be anonymous. The telecommunications operator can use these measures to build its own information security culture.

5.3 Changes in and the end of employment relationships

According to section 5.1.3 of the Regulation, the telecommunications operator must have documented procedures for managing the information security risks due to changes occurring in the personnel or their duties.[32]

In practice, the procedures include the telecommunications operator giving its personnel an orientation to their duties and the changes in said duties, and the telecommunications operator removing, if necessary, any unnecessary access rights, access permits, identity cards and devices in connection with changes in the personnel or their duties without delay.

Section 5.1.2 of the Regulation provides for the information security skills of the personnel and ensuring that the personnel are aware of the operating principles, especially the ones related to their own duties.

In practice, due to section 3.2 of the Regulation, the telecommunications operator must ensure that the operating principles and procedures related to the changes in the personnel or their duties are up to date by taking account of the changes in the operating environment and any incidents detected.

5.4 Actions by personnel that violate the information security policy

The telecommunications operator must have a documented procedure for addressing situations in which an employee violates the telecommunications operator's operating principles or procedures on information security. In practice, the procedure must describe how to handle situations in which an information security breach is caused by personnel acting in violation of the information security principles, for instance.[33] The procedure should also include assessing potential measures for avoiding incidents in the future.

An information security breach or a threat thereof must be reported to the supervisory authority as well as the users and subscribers in accordance with the applicable legislation.

[31] 5G Security Control Matrix: M004 and ISO/IEC 27002:2022: 5.1.
[32] ENISA GL SO7 and ISO/IEC 27002:2022: 6.2, 6.5, 6.6.
[33] ENISA GL SO7 and ISO/IEC 27002:2022: 6.2, 6.4, 6.5, 6.6.

6. Information system and telecommunications security as well as physical security

6.1 Access management

Appropriate logical, physical and administrative access control mechanisms for accessing the communications network and information systems of the telecommunications operator must be in place, and they must be maintained carefully throughout the life cycle of the user identity.[34]

The Regulation requires the telecommunications operator to specify and document targeted operating principles and procedures that take account of the requirements on the information security of access control and ensure only authorised access to the communications network or service components as well as the data processed in connection with the telecommunications operations. The interest groups that the telecommunications operator has authorised to participate in access control must also be informed about the access control requirements.

In practice, the operating principles describe at least the rules concerning access control and identity management as well as the principles of granting and managing access rights.

The access control rules are implemented by specifying access rights and limitations in accordance with the requirements. An access right can be granted to a person or a technical or logical object, such as a machine, device or service. The starting point of access control should always be the principle of least privilege. Separation of the tasks related to applying for access rights and granting them should also be taken into account (see also section 4.1.3 of the Regulation).[35]

There are several different ways to implement access control, which can also be used to automate and facilitate it. In role-based access control, the access rights are based on user roles, in which case it is particularly important to ensure that conflicting information security roles and responsibilities have been separated from each other in accordance with section 4.1, item 3 of the Regulation. For example, dynamic access control can also be used to restrict access with regard to time or only a specific part of the data and protect components critical to the continuity of the communications network and services.

A unique identity enables individual identification and management of users. By default, identity management aims to use personal identities. If this is not technically possible or if its costs are not reasonable for an individual system, in practice procedures for identifying users in a sufficient way by means outside the system (such as by using a jump host) should be implemented and documented.

The operating principles must be documented in accordance with section 3.2 of the Regulation.

Requirements related to changes in personnel are also discussed in Chapter 5.3 of the explanatory notes.

6.2 Protecting the integrity of networks and information systems

The Regulation requires the telecommunications operator to ensure the integrity of the terminals and information systems used by its networks, services and personnel and protect them from viruses, insertion of malicious code as well as malware that could

[34] ENISA GL SO11.
[35] ISO/IEC 27002:2022: 5.15, 5.16, 8.2.

change the functions of the systems.[36] The operating principles required by this obligation must be documented in accordance with section 3.2 of the Regulation.

The protection, management and monitoring of networks and services as well as the devices implementing them are important for protecting the systems and application data from being endangered via the network. For this purpose, the telecommunications operator should have controls to strengthen the information security of the network and protect the services connected to the network from unauthorised use.

Appropriate management, use and protection of the terminal devices used by the personnel of the telecommunications operator in their work is important, because if terminal devices are used contrary to the instructions or if there are deficiencies in the use, they may become exposed to malware and phishing and act as an access route to the network or data of the telecommunications operator.[37]

In practice, the targeted operating principles and instructions of the telecommunications operator should specify the information security management methods related to the environments of different classification levels for terminal devices in accordance with the information security policy and describe the responsibilities of the personnel for implementing the management methods. Requirements related to the training of personnel are discussed in section 5.2 of the Regulation.

Protection against malware can be implemented by means such as restricting access rights according to the principle of least privilege, hardening systems, appropriate security update installation practices, information security awareness training for personnel, and malware detection and patching of software.[38]

Vulnerability management is supported by asset management that is sufficiently accurate and comprehensive as well as based on automation, if possible, and that contains the necessary information on the software dependencies (hierarchy, systems), the software provider, the name and version of the software, as well as information on the persons responsible for the software.[39] Procedures concerning asset management are provided for in section 7.1.3.

The security functions of mobile network components are also discussed in section 10 of the Regulation.

The zero trust principle is an information security model in which the access of systems and users is limited only to the necessary resources and the risks of unauthorised access are minimised.[40] The model also forces repeated authentication and authorisation between entities. The model assumes that an attacker is always present, meaning that as a rule, no component or system is reliable. There are grounds for applying this information security model to the traffic in the network of the telecommunications operator especially when components important for continuity are involved and the model is suitable on a technical level.

[36] ENISA GL SO12.
[37] ISO/IEC 27002:2022: 8.1.
[38] ISO/IEC 27002:2022: 8.7.
[39] ISO/IEC 27002:2022: 8.8.
[40] NIST - Zero Trust Architecture - SP.800-207, https://csrc.nist.gov/publications/detail/sp/800-207/final.

Lateral movement is a concept that refers to the movement of an attacker inside the network that is under attack after gaining a foothold in one of the systems in the network. Restriction of this movement can be implemented by means such as dividing the network into different areas according to trust levels.[41]

Dedicated targeted operating principles and instructions should be drawn up on the division of networks into different network areas, zones or segments according to the different trust levels as well as the separation of network areas from each other either physically or logically (such as with virtual dedicated networks). Network areas should be separated from the public network whenever possible. One purpose of the separation is to make it more difficult for an attacker to move between different network areas inside the network, if the attacker manages to gain a foothold in one area. The zero trust principle described earlier also supports this way of thinking.

In practice, the criteria used to separate networks into different network areas should be based on an assessment of the security requirements of each network area. The separation can be implemented e.g. by aiming to separate the network layers transporting user, control and management traffic from each other by using the methods mentioned above. Traffic and access between network areas can be allowed, but in that case, it should be ensured that control has been arranged between the network areas with an option to restrict traffic so that only the traffic necessary for the operations is allowed. Traffic filtering and control can be implemented using e.g. firewalls, routers, application gateways or separate intrusion prevention systems (IPS) and intrusion detection systems (IDS).[42]

The operating principles should take account of disabling or removing services and protocols that are unnecessary for the connections and logical and physical interfaces of the network. Logical and physical interfaces are gateways through which network devices communicate with external devices and systems. The services and protocols offered via the interfaces enable different kinds of functionalities, and the more such protocols and services are active at the same time, the greater the risk that they will also be exploited in potential attacks.

6.3 Protection against denial-of-service attacks

According to section 6.3 of the Regulation, the telecommunications operator must protect the systems critical to communications networks and services against denial-of-service attacks. The protective measures must be scaled in accordance with an up-to-date risk assessment. This means that the risk assessment must be based on up-to-date threat information; maintaining it may include, for instance, exchange of information with different cooperation networks and real-time monitoring of different sources by using the appropriate tools. Maintaining threat information is discussed in section 9 of the Regulation.

A denial-of-service attack is an attack that aims to prevent the use of a network resource or a service located in the network. Usually, denial-of-service attacks are carried out either by overloading the targeted service/network traffic with extra traffic or taking advantage of a vulnerability in the target. Nowadays a large share of denial-of-service attacks are distributed, which means that the attack comes from several devices at the same time. This makes it possible to use a larger traffic volume to overload the targeted service, for instance. There are often devices behind distributed attacks that have been hijacked to be used in attacks without the knowledge of their owners.

[41] Information security now! Lateral movement — what you need to know (parts 1 and 2), https://www.kyberturvallisuuskeskus.fi/en/news/lateral-movement-what-you-need-know-part-one and https://www.kyberturvallisuuskeskus.fi/en/news/lateral-movement-what-you-need-know-part-two.
[42] ISO/IEC 27002:2022: 8.22.

The implementation methods of denial-of-service attacks vary. In most cases, the attack overloads the target with a large traffic volume, resulting in the use of the network resource being prevented or a reduction in the service level. One example of a commonly used denial-of-service attack type is a SYN flood, which is based on the three-way handshake in the TCP protocol. In the attack, the attacker sends large numbers of TCP SYN packets to the target without sending any ACK packets, and as a result, the targeted server or device fills up with incomplete connections and becomes unable to receive new contact requests.

A denial-of-service attack can also be targeted at the application level. In that case, the attacker targets the application itself, exploiting vulnerabilities or commonly known issues. Such attacks may not need a large traffic volume to work, which makes detecting them more difficult. One example of such an attack is an HTTP flood, in which the attacker sends the intended target enough HTTP requests to prevent other users from using the target. It may be difficult to tell these HTTP requests apart from those sent by real people, and as a result, detecting such attacks may be challenging.

Along with new technologies and methods, the targets, number and type of denial-of-service attacks change constantly. For example, attacks targeted at the different interfaces of the 5G network create new challenges for service providers. The 5G network enables a device frequency that is many times higher than that of the previous network generations, and the number of potential IoT devices (Internet of Things, IoT) used for denial-of-service attacks is expected to grow. The increase in the number of devices and their potentially variable level of information security require taking the risks into account and preparing for them.

Typical ways of mitigating the impact of denial-of-service attacks include packet scrubbers that distribute network traffic, or the use of SAV (Source Address Validation) methods such as ACLs (Access Control Lists), that make possible to specify IP prefixes to be rejected in network traffic, among other things.[43] The impact of denial-of-service attacks can also be mitigated by properly configured hardware, such as firewalls and load balancers. IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) systems that operate either separately or integrated into a firewall help detect and prevent denial-of-service attacks.

6.4 The use of encryption and cryptography

The confidentiality, authenticity and integrity of data are protected by the use of cryptography. The appropriate use of encryption prevents and minimises the impact of information security incidents on users, networks and services. The Regulation's obligations on encryption correspond partially to the obligations on telecommunications operators imposed in the regulation of the Swedish PTS (Post- och telestyrelsen) and its application guidelines.[44]

According to the Regulation, the telecommunications operator must draw up and maintain procedures in accordance with the targeted operating principles on encryption (encryption policy). The operating principles must include at least the implementation methods of encryption and when and in what situations it is possible to not use encryption. The operating principles must also include general information on the functioning, type and strength of the encryption methods used. In addition, the operating principles must include descriptions of the protection level required by the data as well as which encryption method is suitable for encrypting which type of data.[45]

[43] NIST - Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation, p. 27–28, https://csrc.nist.gov/publications/detail/sp/800-189/final.
[44] Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster, PTSFS 2022:11, Chapter 10, https://www.pts.se/sv/dokument/foreskrifter/telefoni--internet/ptsfs-202211---foreskrifter-och-allmanna-rad-om-saker-het-i-nat-och-tjanster/.
[45] ENISA GL SO13, 5G Security Control Matrix: M071, M073 and M074.

There are different kinds of risks associated with different data types that vary depending on the type of data and the threat level of the environment. In fact, the telecommunications operator should always assess the need for encryption, the encryption level and the appropriate encryption procedures required by the data on a case-by-case basis. The passwords, encryption key materials and other secret information used for authentication in particular should always be encrypted, if it is technically possible. Encryption solutions and protocols that are suitable for the situation and provide sufficient protection should always be used for encryption. When assessing the need for encryption, it can be considered e.g. whether it is sufficient that one part of the traffic is encrypted in certain situations. For example, it is possible that a sufficient level of information security can be achieved by encrypting the control traffic, in which case there is no separate need to encrypt user-level traffic. In addition, the risk assessment can take account of the various information security risks caused by the transfer method of the traffic. The assessment is also affected by factors such as the opportunities of different parties to access the traffic and whether the traffic travels over the internet, in a network of trusted partners or only in the telecommunications operator's own network, for example, as well as the ability and need of the telecommunications operator to detect malicious traffic.

According to the Regulation, appropriate encryption must always be used when data are stored or when they are transferred, if this is appropriate, technically possible and proportionate in light of the nature of the data. If data are encrypted while they are moved or stored, a method offering sufficient protection with regard to the classification and performance requirements of the encrypted data should be selected. As for the encryption method, its uses, algorithms and key strengths should be taken into account. The requirements of the encryption method used should be up to date throughout the life cycle of the system. If implementing encryption is not possible, the telecommunications operator must justify it in the operating principles it maintains. If encryption is not used for the storage or transfer of data, in practice the telecommunications operator must draw up a risk and impact assessment on the matter as a part of implementing the requirements of section 4.1.2 of the Regulation and describe it in the operating principles.[46]

Using other protection methods to compensate for the deficiencies of encryption methods may be challenging, and therefore the telecommunications operator should pay attention to the selection and safe use of encryption solutions.[47] Particular attention must be paid to the selection and use of encryption protocols used to protect the components critical to the continuity of the communications network or service, as well as the protection of components that contain or process sensitive data.

For example, at least version 1.2 of the TLS encryption protocol or later should be used for encrypting telecommunications. TLS protocol versions 1.0 and 1.1 are obsolete, and therefore they should no longer be used.[48]

6.5 Protection and management of the encryption key materials and secret information used for authentication

Section 6.1.5 of the Regulation requires that the telecommunications operator must have appropriate operating principles and procedures for the protection and management of encryption key materials and secret information used for authentication. This is important, because if they were to end up in the wrong hands, this could endanger

[46] ENISA GL SO13, 5G Security Control Matrix: M072.
[47] Correspondingly, Katakri 2020 – Information security auditing tool for authorities. I-12, p. 89, https://um.fi/information-security-auditing-tool-for-authorities-katakri.
[48] IETF RFC 8996, Deprecating TLS 1.0 and TLS 1.1, https://www.rfc-editor.org/rfc/rfc8996.

telecommunications security and the effectiveness of access management procedures, among other things.

Therefore, in practice the telecommunications operator must ensure that the encryption key material or secret authentication information, including the encryption key material used for authentication, is not disclosed and that it is protected from alterations and loss. This means that encryption keys must only be available to the intended users and processes. The encryption key material and secret authentication information as well as the devices used to create, store and archive encryption keys should be protected in accordance with the best practices and standards of information security.[49] The use of encryption in protecting the encryption key material and other secret information used for authentication is also justified.

The operating principles and procedures related to the management of encryption keys must be designed, implemented and described. Therefore, in practice the telecommunications operator must have practices for the use, protection and service life of encryption keys. The operating principles should also specify the different roles, responsibilities and monitoring throughout the life cycle of encryption keys, including the use, backup and restoration of private keys.[50]

6.6 Hardening the virtualisation environment

Section 6.1.6 of the Regulation requires that communications network and service components implemented in a virtualisation environment must be implemented so that only the functionalities and access rights necessary to their operation are permitted. In other words, the Regulation requires the hardening of virtualisation environments. The telecommunications operator must have documented operating principles and procedures for hardening virtualisation environments (section 3.2 of the Regulation).

Virtualisation means a process in which a functionality is simulated by creating a virtual calculation environment for it in order to separate the functionality from the physical resource in its background.[51] A *virtualisation environment* consists of different components and systems. As a rule, virtualisation architecture involves the following components and systems: Physical devices, virtualisation level, virtualisation management level and individual virtualised systems, as well as operative and telecommunications operations support systems. The more components and different suppliers are used to support virtualisation, the more likely it is that the virtualisation environment contains vulnerabilities that threaten information security as well as functionalities that are unnecessary for the essential use of the system and may also prove to be information security threats. Several different suppliers create challenges for vulnerability management and monitoring, and therefore it is particularly important to disable or remove unnecessary features.

[49] ENISA GL SO14, 5G Security Control Matrix: M075.
[50] ENISA GL SO14, 5G Security Control Matrix: M076 and M077.
[51] Virtualisation hides the physical resource from other systems, applications and users. In virtualisation, the same physical resource such as a server, memory or processor in the background can act as several logical resources, or if there are many physical resources, they can be presented as a single logical whole thanks to virtualisation. Virtualisation can be applied in several different areas, such as servers and computing power, network, storage space, operating system or applications. Virtualisation can be realised in different ways. The first method is to create a virtual machine, which has been created programmatically to emulate a foreign operating system. Several virtual machines can be established on a single physical device; they use the resources of the host machine to run software and functions. In case of virtual machines, a hypervisor (virtualisation platform) creates and runs virtual machines. The hypervisor is responsible for allocating the resources of the host machine to the virtual machines. Another method for implementing virtualisation is the use of containerisation. Containers differ from virtual machines in the sense that virtual machines virtualise the whole operating system, but containers only virtualise the software and dependencies needed by the container. Software intended for the purpose is used to run and create containers.

Hardening, in contrast, means in this case that the communications network and service components are installed and maintained so that they only use the *necessary functionalities and access rights* for their operation. Limiting functionalities by means such as removing unnecessary applications and services reduces the vulnerability area of systems.

The telecommunications operator itself can specify the methods and techniques it uses to implement the requirements of the Regulation. Some actors that the telecommunications operator should take into account when selecting an implementation suitable for its own operations are presented below:

- In general, appropriate tools related to configuration management should be used to implement and maintain a hardened installation.
- Restricting access rights is one hardening method. Here, the principle of least privilege should be followed, meaning that rights are granted only according to what is absolutely necessary. The number of users that have system administrator rights should also be limited. In addition to the above, it is often reasonable to limit access to and editing rights of sensitive files, such as different kinds of settings files.
- Components and systems integral to the realisation and generation of a virtualisation environment, such as hypervisors and host operating systems, should be kept up to date with regular updates and security fixes. To implement this, software essential for the realisation and generation of a virtualisation environment can be scanned regularly, for example, to make it possible to detect any vulnerabilities related to them. Updates can be taken care of with regular update practices, such as monthly patching/update days. In addition, the telecommunications operator should have its own processes for situations in which critical vulnerabilities of the system appear. For these kinds of vulnerabilities, updates and security fixes should be applied as soon as possible.
- In practice, virtualised network functions and components should be classified and separated into administrative areas based on how high a risk is involved in the component or function. As far as possible, administrative areas should also be separated from each other. At minimum, the aim should be to ensure that the traffic between them can be controlled in some way. This can be implemented by means such as dividing the different workloads into separate segments based on their information security needs and risk classification and connecting these segments into different administrative areas. The risk can be assessed based on the type, features and role of the host. It should also be noted that in some critical systems, physical separation may be necessary.[52]
- As far as possible, the virtual environment management layer must be separated from management areas with a lower trust level, such as operative infrastructure, the telecommunications operator's own intranet, the internet, as well as user networks and the networks of other operators. The separation can be implemented either physically or logically. Physical separation can be implemented by not running the management layer functions on the same physical platforms as the functions of other layers, for example. As for logical separation, it can be implemented by means such as using separate virtual machines for the management components and functions or by network layer separation by using VXLANs, VLANs or traffic encryption.
- Access to the management layer should only be allowed by means such as using multi-factor authentication, which is implemented by creating another authentica-

[52] ENISA 5G Security Matrix: SO12-018 and ENISA NFV security in 5G: BP-T16, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices.

tion factor locally, for example. A time limit or timeout can also be set for management access. Using personal credentials for management is justified. In addition to personal credentials, credentials intended for emergencies or exceptional situations can be used, if the use of personal credentials is not possible. The use of these credentials should be limited to only previously documented use cases. In addition, the use of the credentials must be controlled sufficiently with means outside the target system, taking the risks related to the matter into account.

- For third parties, the need for management connections and granting access rights should be assessed on a case-by-case basis and the principle of least privilege should be followed in granting rights. Especially when access to systems and their parts is granted via remote connections, it should be ensured that the connections and the measures carried out are logged appropriately, and in addition, other audit measures should also be considered to ensure that no unauthorised changes are made to the network and information systems.

- If the container technology is used in the virtualisation environment and the implementation of the network functions, it is important to ensure that sufficient information security controls are deployed for them, too. The separation of the containers from each other can be achieved by e.g. running the containers as runtime processes in specified namespaces. Limiting the running of containers with privileges to a minimum and ensuring that elevating the rights is not permitted, for example, can act as additional controls. The rights of containers run with privileges are usually inherited from the host machine, in which case extensive rights may allow access to sensitive information. They may also allow making malicious API calls that may enable an attacker to expand its intrusion by lateral movement within the clusters.

- In virtualised environments, containers and other components should have unique identifiers to help with detecting and preventing potential lateral movement.[53] In addition, different kinds of policies and group definitions can be used to limit the resources visible to containers and how much resources (CPU, memory, storage space, network) they are allowed to use and how new directories can be linked to containers. It is also reasonable to restrict the running of processes within containers with root rights. The best practices and methods for information security controls of the most common container technologies, such as Kubernetes and Docker, can be for example found in the security guides of the Open Web Application Security Project (OWASP) organisation that aims to improve the security of software.[54]

6.7 Physical security

Section 6.2 of the Regulation imposes an obligation on the telecommunications operator to draw up appropriate operating principles and procedures for ensuring the physical security of information systems, devices, data and premises. The telecommunications operator must also take care of the environmental conditions of the devices. This means that the telecommunications operator must take care of the appropriate protection of data, devices, equipment facilities and other facilities used in telecommunications operations against physical threats. The threats against which protection is needed are related to unauthorised access and environmental factors in particular, such as fire or water damage.[55]

[53] NSA - Security Guidance for 5G Cloud Infrastructures - Part I: Prevent and Detect Lateral Movement, p. 8, https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_I_508_Compliant.pdf.
[54] OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/.
[55] The section is based on the information security objective SO9 in accordance with ENISA GL, and measures recommended by ENISA can be used in its implementation.

The Regulation of the Finnish Transport and Communications Agency on resilience of communications networks and services and of synchronisation of communications networks provides for e.g. the physical protection of equipment facilities and documenting the protection (section 17 of the Regulation). However, the regulation in question is not a comprehensive regulation on physical security, and therefore the necessary considerations related to physical security are also covered by this Regulation on information security in telecommunications operations. In fact, the obligation in accordance with section 6.2 of the Regulation also applies to the cases in which the Regulation on resilience of communications networks and services and of synchronisation of communications networks mentioned above does not impose any specific access control or other requirements, and it also covers facilities used for working or data storage in addition to the equipment facilities.[56]

If necessary, the operating principles and procedures must take the importance of the target to be protected into account, such as if a critical part of the communications network is involved. Other factors that must also be taken into account in the risk assessment include the location of the facilities and the safety of the environment, for instance. In practice, matters processed as a part of drawing up the operating principles and procedures include at least access control, the structural protection of devices and equipment facilities, burglar alarms, as well as the monitoring of environmental conditions and the use of fire extinguishing systems, for instance. Access should only be granted to a limited number of personnel, whose reliability and information security skills have been ensured. Correspondingly, the access of the personnel of third parties in particular must be restricted and specifically monitored.[57]

7. Information secure operations and change management

The aim of the obligations of section 7 of the Regulation is to establish a chain of traceability for hardware and software, among other things. The complexity of software environments makes traceability especially important. In order to gain confidence in the information secure operations of software environments, it is important to know when and what changes have been made and who has made them.

7.1 Information secure use of the communications network and service

In accordance with section 7.1.1 of the Regulation, the telecommunications operator must have operating principles and procedures for the use of the communications network or service components, i.e. operation.[58] With regard to operational procedures, the requirement can be implemented by means such as documenting the responsibilities for the operation of network and information systems and supplementing this by also describing the most important practices for the operation and management of systems. The practices and responsibilities should be reviewed regularly and updated as needed, especially if there have been changes in the environments or if an earlier event has shown that there are gaps or deficiencies in the practices.

7.2 Change management

In accordance with section 7.1.2 of the Regulation, the telecommunications operator must have change management procedures that reduce the likelihood of information security incidents caused by the changes or, if necessary, restore the state before the change or other functioning state, which refers to a rollback procedure. In this context, changes refer to all changes with an impact on information security that may affect

[56] Section 17.3 of the Regulation on resilience of communications networks and services and of synchronisation of communications networks requires that the communications network or service components are physically protected in such a way that they cannot be easily accessed by unauthorised persons.
[57] 5G Toolbox: TM06, p. 25.
[58] ENISA GL SO15.

things such as software, hardware, configurations and interfaces. The change management procedures may be in proportion with the information security risks caused by the change, affected by the type and extent of the change.

With regard to change management procedures, the requirement can be implemented by documenting predefined procedures for implementing changes.[59] The documentation should include a description of the need for changes, preliminary testing, production testing and deploying the change to production, as well as approval procedures for each stage. When it comes to change management procedures, it is justified to take special care of the measures referred to in sections 6.1.2 and 6.1.7 of the Regulation that are used to harden components by removing unnecessary access rights and services. Section 8.1 of the Regulation applies to testing.

The procedures for reverting a change that has failed or interrupting a change by restoring a version or configuration that is known to function should also be planned. The change management procedures should cover the whole development life cycle of the systems.[60]

Provisions on change management can also be found in section 9 of the Regulation of the Finnish Transport and Communications Agency on disturbances in telecommunications services. The obligation in question is not focused on taking care of information security specifically, however.

7.3 Asset and configuration management

According to section 7.1.3 of the Regulation, the telecommunications operator must have appropriate operating principles and procedures for the management of assets and component configurations.[61]

Among other things, the management of assets such as equipment and software support vulnerability management and the prediction of risks and dependencies. Configuration management is important for restoring the correct settings, if necessary, and detecting unauthorised changes. It is also good to note that it is important to keep the operating principles and procedures up to date after changes and events that threaten information security.

The procedures should include appropriate measures to prevent and correct unauthorised or unintentional changes in configurations, if the configuration is incorrect. Configuration management can be implemented by means such as using specialised tools and keeping an event log of the changes. In fact, asset and configuration management is an integral part of the change management procedures referred to in section 7.1.2 of the Regulation. Before implementing changes, procedures for restoration to a previous version should be specified (see also Chapter 7.2 of the explanatory notes), and old versions of software should be archived as a precaution together with the necessary information, which includes e.g. the details of configurations and the parameters used.[62]

With regard to configurations, the requirement of the Regulation can be implemented with a configuration management database (CMDB), for example; it is used to manage information on the telecommunications operator's hardware and software assets. CMDB makes it possible to keep a record of diagrams describing the network structure, components and software versions, and manage the mutual dependencies of the communications network and service components.[63]

[59] ENISA GL SO16, 5G Security Control Matrix: M84.
[60] ISO/IEC 27002:2022: 8.32.
[61] ENISA GL SO17.
[62] ISO/IEC 27002:2022: 8.19.
[63] ENISA GL SO17, 5G Security Control Matrix: M88

In addition, as the diversity of the telecommunications operator's software environment increases, the monitoring and management of software vulnerabilities should be systematic and centralised. Vulnerability management can be implemented by means such as a software bill of materials (SBOM) based on a proactive classification of the communications network components and vulnerabilities based on various sources of information, which makes identifying vulnerabilities and reacting to them faster and easier.[64]

It should be noted that the Regulation of the Finnish Transport and Communications Agency on critical parts of a communications network imposes an obligation on telecommunications operators to identify the critical parts of a communications network and the communications network and service components used in them. In addition, the Regulation of the Finnish Transport and Communications Agency on resilience of communications networks and services and of synchronisation of communications networks provides for an obligation to document information on all communications network and service components classified by priority.

8. Testing and information security assessments

Section 8 of the Regulation provides for testing and information security assessments.

8.1 Testing the information security of the communications network and service and carrying out security assessments

Section 8.1.1 of the Regulation requires the telecommunications operator to have appropriate and up-to-date operating principles and procedures for testing the information security of the components of communications networks and services and, if necessary, carrying out security assessments based on the risk assessment. The procedures are also an important part of change management (section 7.2 of the Regulation), and they should be in proportion with the type and extent of the changes.

Testing primarily means testing the functions related to information security. The testing should verify at least the validity of the security functions as well as the security of the software development and configurations.[65] Using automated testing tools in the testing is justified, even if it may be appropriate to make an exception to this with minor or otherwise small-scale telecommunications operations, for example. Implementing special security assessments through information security scans and penetration tests, for instance, should be done when it is necessary based on a risk assessment.

Testing and security assessments are important before deploying new components and software and before making software changes, so that disturbances and the creation of holes in the information security can be avoided.[66] In addition, testing and security assessments should be carried out after a change to verify that the change has not caused damage to information security. There may be reason to implement testing and security assessments throughout the life cycle of the components, so that potential unauthorised or unintentional configuration changes as well as vulnerabilities in the components can be detected. This provides information on the state of information security of the network and services.

It is important to carry out testing and a security assessment before the deployment of new components as well as during use. A preliminary assessment can include, among other things, a check of how the component is hardened, whether the component has

[64] See NIST - Guide to Enterprise Patch Management Planning.SP.800-40r4, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf, SBOM at a Glance (ntia.gov), https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf and the National Cyber Security Centre Finland: Managing vulnerabilities with SBOM, https://www.kyberturvallisuuskeskus.fi/en/news/managing-vulnerabilities-sbom.
[65] ISO/IEC 27002:2022: 8.29.
[66] ENISA GL SO25–SO26.

known information security vulnerabilities, and whether the component has been updated to the latest appropriate software version. Testing and security assessments during use can be implemented by means such as scanning components in the network in case of devices and software versions that contain known vulnerabilities. This requires using vulnerability databases generated by third parties and comparing the results of the security assessment with them. The CVE (Common Vulnerabilities and Exposures) database is one such option, as an example. The results of the security audit should be documented in order to maintain knowledge of the status of information security of the network. The results should include information on which components were assessed, what was assessed and by whom, the results of the assessment and potential further measures.[67]

8.2 Information security assessments

Section 8.1.2 of the Regulation requires the telecommunications operator to have appropriate operating principles and procedures for monitoring the realisation of its information security policy and operating principles as well as the information security requirements on its operations.[68]

A regular inspection of compliance with the requirements supports the security of the operations and the realisation of all aspects of information security, when the measures taken by the telecommunications operator in order to implement the requirements are reviewed regularly in ways specified by the telecommunications operator in advance.

The assessments should consider the realisation of compliance with the requirements in relation to not just the information security policy, operating principles and procedures defined by the telecommunications operator for itself, but also the realisation of applicable statutory obligations and regulations related to information security. In addition, they can review compliance with the applicable standards. Here, standards refer to the standards that the telecommunications operator is required to follow, or that it has committed to following as a part of its information security and information security risk management procedures.

Such an information security assessment can be carried out as a review implemented as a self-assessment or through internal or external independent information security audits, depending on the case. The assessment methods used should be defined in the operating principles and procedures, i.e. how the compliance is assessed, the frequency of assessments, the recording and implementation of corrective measures, and the focus of the reviews or audits. They can also specify whether the assessments are implemented as preventive measures or possibly also after serious information security incidents or significant changes.

According to the Regulation, the results of the latest assessment must be stored at minimum.

9. Maintaining threat information

Section 9 of the Regulation requires the telecommunications operator to have appropriate procedures for collecting threat information related to the information security of communications networks and services and assessing the threats. The purpose of this obligation is to ensure that the telecommunications operator maintains continuous, up-to-date threat information on the threats against the communications network and service components. The operating principles and more specific procedures must include a

[67] ENISA GL SO26.
[68] ENISA GL SO27 applies to compliance with statutory obligations and standards. See also ISO/IEC 27002:2022: 5.36 that applies to compliance with the information security policy and operating principles, rules and standards on information security.

review of the strategic, tactical and operative levels. Up-to-date, evaluated threat information acts as an important starting point for the processing of information security risks.

The telecommunications operator can proactively mitigate or remove the impact that identified internal and external threats have on information security risks by maintaining a continuous awareness of the current threat situation.[69] As the threat environment changes constantly, it is essential to use threat information in the continuous assessment of information security risks. In addition, completely new information security risks to the communications network and service components can be identified when the threat information changes.

When applicable, the collection of threat information should include at least the threats against the supply chains of software and devices, the impact of denial-of-service attacks on the operation of the communications network or service components, the effects of ransomware and other malware, the vulnerabilities of components, monitoring the threats related to BGP routing and the threat of manipulation of employees.[70]

See also Chapter 7.3 of the Annex to the explanatory notes (Providing information on vulnerable customer devices).

It is recommended that telecommunications operators also send information on denial-of-service attacks to the notification interface of the Finnish Transport and Communications Agency. The aim of using the notification interface is to collect information on denial-of-service attacks in order to improve the overall level of information security. With this information, the Finnish Transport and Communications Agency can help telecommunications operators react rapidly to threats and disturbances related to denial-of-service attacks, for instance. Collecting data also promotes the generation of a long-term situational picture.

10. Compliance with standards

New generations of mobile communications networks expand the network services to cover different aspects of society, making them an increasingly essential part of the operation of society and other critical infrastructure. The new service-based interface architecture of the fifth-generation mobile network makes it possible to open the network functions to third parties and creates new operating and service models. Older network generations are also in use at the same time; of them, the 4G network in particular will be used in parallel with the 5G network for a long time. At the same time, the management of interfaces and opening them up increase the complexity as well as the threat area. In that case, it is especially important to take all security functions of the network devices into account and utilise them as fully as necessary in the operations of the telecommunications operator.

Section 10.1 of the Regulation requires a mobile network telecommunications operator to have the appropriate procedures in place for ensuring that all necessary security functions of the 4G, 5G and IMS systems in accordance with the technical specifications of Annex 1 to the Regulation are realised.

The realisation of security functions means not only that the communications network and service components used support the functions in accordance with these standards,

[69] ENISA GL SO28. See also ENISA 5G Matrix: M138–M144 and SO29-001–SO29-003, ISO/IEC 27002:2022: 5.6, 5.7 and 8.8), 3GPP TS 33.501, cl. 5.10.1 as well as the ENISA Report: Cyber Threats Outreach in Telecom, Chapter 4, https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom.
[70] See ENISA Threat Landscape for Supply Chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, ENISA Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 and ENISA Threat Landscape for 5G Networks Report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

but also the deployment of the functions in the communications network of the telecommunications operator. The procedures must also ensure the permanence of security functions in connection with software updates and the implementation of new functions.

3GPP draws up its technical specifications and standards as releases; their adoption may sometimes take a long time and progress by stages online. The functions specified in a later version can sometimes also be implemented and adopted partially in a situation in which the communications network or service component is otherwise still implementing the previous version. As a result, out of the versions of technical specifications, the version approved by 3GPP that corresponds to the version of the functionality implemented by the telecommunications operator in the network must always be studied.

The telecommunications operator may choose not to implement the safety requirement referred to in subsection 1 if implementing it is not appropriate for the purpose, taking account of its significance to the information security of the communications network or service in the case in question as well as the other related measures to ensure information security (section 10.2 of the Regulation). Grounds for the non-implementation of a security function in accordance with the standard may include e.g. implementing an alternative security function that sufficiently mitigates the risk caused by the threats identified. For example, the lack of a security function in a device, software or a part thereof, the logical or physical location of the device and a need related to network management or detection may justify not implementing an optional security function either temporarily or, if necessary, permanently in a manner required by the risk assessment. The risk assessment must take account of the threats against both the telecommunications operator and the user of the communications service.

According to section 10.3 of the Regulation, the telecommunications operator must maintain a description of the procedures with which it ensures that the security requirements of the standards are taken into account. It is also required that not implementing a specific safety function or mechanism on the grounds in accordance with section 10.2 is documented separately. The purpose of this requirement is to enable the monitoring of the obligation and verifying the grounds for applying the exception after the fact.

The Regulation does not require the telecommunications operator to test independently whether the implementation of all functions complies with the standard; instead, appropriate procedures could include requirements on the equipment supplier concerning the issue and taking appropriate measures to monitor that they are realised, for example. When possible, the telecommunications operator can also take advantage of the information security certification of the component in accordance with the EU Cybersecurity Act as a part of the procedures when it becomes available,[71] or an assessment of the component in accordance with the NESAS scheme[72]. In addition, the procedures must also ensure that security functions are deployed and maintained appropriately as a part of the configuration management of the components.

11. Information material

In order to ensure that important information relevant to telecommunications is only available to those who have the right to access it, the telecommunications operator must have in place a classification system, classification criteria and a processing procedure related to the classification for the information material considered relevant for its telecommunications operations.

[71] ENISA Securing EU's Vision on 5G: Cybersecurity Certification, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification.
[72] GSMA Network Equipment Security Assurance Scheme (NESAS), https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

User access management in accordance with the classification of the information materials is also an integral part of the classification and processing of information materials.

User access management is discussed in section 6.1.1 of the Regulation.

The telecommunications operator must determine a set of information material classification criteria that is appropriate for its own operations. An example of the classification of the materials is: public, confidential and secret.

In addition, the telecommunications operator must determine how it processes (protects) the materials belonging to the different classes.

The classification and the related processing procedures must be documented (see section 3.2 of the Regulation). Matters to be considered in the determination of the classification and its documentation include the following:

- general principles of assessing the security class and confidentiality of information material and in keeping the material secret
- the rights to process and alter the materials and the distribution of the rights to access and alter the information material
- determination of the confidentiality class
- publicity of data or a document, including the right to speak publicly of the matter concerned
- document properties: paper, watermark and other marks
- storage and encryption
- printing and copying
- backup copies
- sending and receiving, distributing and moving
- documentation of the processing of the data and the document
- document archiving, processing or the termination of processing rights, destruction of data and the document.

12. Identifying the customer to ensure information security

Section 12 of the Regulation requires the telecommunications operator to have operating principles and procedures for identifying the user or subscriber that are sufficiently reliable for the purpose before essential changes affecting the information security of the communications service are made to the customer's service or confidential information is disclosed to the user or subscriber. The identification procedure can be adjusted so that it is proportionate to the risk level of the activity from the perspective of the changes made to the service or the confidential information disclosed. When assessing the risk level, the special characteristics of the user or subscriber, such as potential non-disclosure of data restrictions, must be taken into account in addition to assessing the customer event. For example, the operating principles and procedures could specify sufficient identification procedures based on risk with regard to different types of service changes and customer information.

The operating principles and procedures that have been drawn up should be included in the training programme of personnel involved in customer service. Section 5 of the Regulation imposes an obligation on the telecommunications operators to ensure the information security skills of the personnel and organise information security training regularly, and the requirements on the information security skills of the personnel and their development are discussed in section 5.2.

In *e-services,* the use of strong electronic identification in accordance with the Act on Strong Electronic Identification and Electronic Trust Services (617/2009), for instance,

can be considered a reliable method of identifying a user or subscriber. An alternative reliable method for identifying a user or subscriber can be the use of two-factor authentication with e.g. a mobile application, taking the risk level into account. For a *visit in person,* checking the identity document of the user or subscriber can be considered a reliable method. Reliable identity documents include e.g. a Finnish passport, personal identity card or driving licence as well as foreign documents of comparable reliability, such as a passport or personal identity card granted by another state in the European Economic Area. A document must not be accepted if the telecommunications operator is not sufficiently certain that the document truly belongs to the person who presents it, or if there is reason to suspect that the document is false.[73] In *telephone calls,* too, the customer must be identified using a sufficiently reliable method. Based on a risk assessment, a customer can be identified over a telephone call sufficiently reliably by using a list of questions with answers that are not known to outsiders, for example. In addition, strong electronic identification or a mobile application can be used over the telephone, when possible.

Essential changes to a communications service that affect its information security can be considered to include at least changing the SIM card of the subscription, reopening the subscription (disclosing the PUK code), downloading or activating an eSIM as well as terminating the subscription.[74] Essential changes also include changing the forgotten password of an email account or opening a locked user account. Among other things, traffic data related to the user or subscriber, such as information included in a detailed itemised invoice, or information stored in an email or instant message service, are considered confidential information. The telecommunications operator must not make essential changes to the service or disclose confidential information, if the user or subscriber of the service has not been identified at a sufficient level.

13. Documentation of IP addresses

Section 13 of the Regulation requires the telecommunications operator to ensure that the IP addresses assigned to it and advertised by it are carefully documented by entering the networks to the database of the internet address registry (IR) that allocated them or another appropriate internet address registry. This is important, because telecommunications operators can use this information to create automatic route filters (prefix lists), for example. The purpose of prefix lists is to ensure that the telecommunications operator advertising the routes only advertises the address spaces it manages. Appropriately documented IP network resources also make the maintenance of routing information as well as the investigation of disturbances and information security breaches much easier.

Telecommunications operators must report the networks managed by them to the WHOIS database of the appropriate internet address registry (IR). In connection with the Regulation, the networks managed refer to network areas owned by the telecommunications operator or ones it has delivered to customers. This information is logged and maintained in accordance with the address registry's guidelines. Information to be logged includes the IP address space, the telecommunications operator’s contact information, the administrator's contact information, the abuse and IRT contact information and the network AS number, from which the IP addresses in question can be found. RIPE NCC, the European Regional Internet Registry, has a dedicated field for registering abuse contact information.

The telecommunications operator must specifically ensure that the documentation of the IP networks used by that operator is up to date. If the telecommunications operator

[73] On approving a document granted by a party other than a Finnish authority, see KHO 2017:19 (in Finnish), https://www.kho.fi/fi/index/paatoksia/vuosikirjapaatokset/vuosikirjapaatos/1486031131275.html.
[74] See On procedures related to countering SIM swapping: SIM-ENISA Countering SIM-Swapping, p. 17–20, https://www.enisa.europa.eu/publications/countering-sim-swapping.

is a source of route advertising for PI (Provider Independent) network address spaces that belong to other organisations, the correctness of the information related to these address spaces must be verified at the time when the route advertising is activated. Similarly, if a telecommunications operator maintains a Local Internet Registry (LIR), lending IP address space to third parties, the veracity of the address information must be checked when the network address space is registered.

In practical terms, the documentation requirement means that telecommunications operators are not allowed to advertise undocumented IP address spaces to other telecommunications operators, unless otherwise expressly agreed.

14. Management network and management connection traffic

The telecommunications operator must have appropriate operating principles and procedures on network management and management connections that ensure the realisation of an assurance level in accordance with the risk assessment in order to minimise information security threats (section 14.1 of the Regulation). The Regulation requires the telecommunications operator to protect the management traffic of communications network or service components (section 14.2 of the Regulation). Management traffic means traffic that the telecommunications operator uses to monitor and manage its network devices. The purpose of the obligation to protect management traffic is to ensure that no unauthorised tampering of the components of the communications network or service takes place.

The operating principles must include at least the requirements related to protecting management traffic, the hardening requirements on terminal devices used for network management, as well as access control principles depending on how central the communications network and service components are.

In practice, management traffic may be protected either physically by isolating the traffic in designated cables or logically by using encryption to isolate the traffic. Encrypting the management traffic by using a method suitable for the situation is needed especially if there are no other ways to ensure that monitoring or hijacking the traffic has been prevented. Unencrypted management traffic may reveal information or characteristics of the components of the communications network or service.

In addition, the telecommunications operator must use appropriate procedures for assessing the information security threats caused by the terminal devices used for network management and managing the risks caused by them (section 14.3 of the Regulation). Special attention must be paid to the protection of terminal devices used for the management of communications network and service components, because if email and internet services, for example, can be used on the same terminal device, the management network is also targeted by information security threats through these services.

A dedicated, hardened workstation can be used in some situations, in which case the possibility of using functions other than those necessary for network management is removed from the terminal device. Based on an overall assessment, other procedures can also be used in risk management, in which the risks caused by the terminal device have been managed in other ways. The starting point of the Regulation is that terminal devices used for network management must not be connected directly to the management network systems; instead, the use of the management network should be implemented through virtual termination, a carefully monitored jump host, or with a remote desktop -based solution. Two-factor authentication, antivirus or a VPN connection should not be considered sufficient by themselves. When transferring necessary files from one terminal to another, the risk of malware shall also be taken into account, e.g. by ensuring the use of reliable sources only and safeguarding information security (integrity) using all appropriate methods.

Without exception, the principle of least privilege should be applied to the access control of the management network connections, and user authentication should be done by using at least two authentication factors. Sending the authentication factor via a text message should not be considered a primary method. In addition, suitable procedures should be implemented and documented for mitigating the residual risks related to ensuring the information security of the management connection. The procedures may include e.g. restricting connections to only specific IP addresses, allowing management connection events based on need, limiting the duration of events, real-time monitoring and logging the management connection events.

Requirements related to user access control are also discussed in section 6.1 of the Regulation.

Recommendation

The Finnish Transport and Communications Agency recommends that the telecommunications operator maintain a log of the previous six months concerning the changes made to the settings of its network devices in order to detect and trace potential unauthorised changes in the settings of the network devices. The Agency also recommends that the indications of the time of events and observations to be logged include a separate entry for the time of the event and that of the observation. It is recommended that at least the date of the observation be logged, but in system logs concerning the event, the precise time should also be reported, including the time zone (such as "UTC+2") and the potential offset of the clock and its direction compared to the official time. The time stamps of technical system logs should preferably be indicated in an ISO 8601-compatible format.[75]

Chapter 3 Specific requirements for the interfaces of communications networks and services

This chapter explains the requirements concerning the information security of interconnection, application and customer interfaces laid down in Chapter 3 of the Regulation.

15. Prevention of and protection from interference in interfaces

15.1 Prevention of interference

The network or service of the telecommunications operator must not interfere with other communications networks or services. The obligation laid down in section 15.1 of the Regulation obviously prohibits intentional interference, but the requirement is still primarily intended to prevent unintentional disturbances – caused by a configuration error, for instance – from spreading from one network to another. Disturbances spreading over an interconnection interface may create loops in the network, misdirect traffic or simply create congestion in some part of the network or service due to extra traffic. At worst, the service may be rendered altogether unavailable.

Because the impact of these disturbances may be significant, it has been considered necessary to impose on obligation on telecommunications operators to prevent their communications network or service from interfering with the services of other communications networks. This despite the fact that in section 15.2 of the Regulation, an obligation to protect themselves from these disturbances has also been imposed on telecommunications operators.

[75] A recommendation with comparable content has been issued in section 9.2 of the explanatory notes to Regulation 66 A/2019 M on disturbances in telecommunications services.

The obligation is not targeted at any one technology or protocol level, but rather the telecommunications operator must evaluate the threats caused by the technologies and services used in the interconnection interface, and subsequently implement all the protection mechanisms required for preventing disturbances from spreading.

Mechanisms that prevent loops from forming in the interconnection interface can be considered to represent a necessary protection mechanism. For instance, calls can be forwarded a maximum of five times in circuit-switched telephone services, after which the call will be disconnected. With regard to interconnection of internet access services, this means the telecommunications operator not sending traffic over the same logical interface in the interconnection interface that it has already received over the interface in question.

Even though the Regulation otherwise only applies to public telecommunications operations, it should be noted as provided for in the scope of application of the Regulation that the obligation in accordance with section 15.1 of the Regulation on preventing interference also applies to public authority networks and communications services related to public authority communications insofar as they are interconnected to a public communications network or a publicly available communications service, i.e. the network or service of a telecommunications operator. In other words, a network operator maintaining and providing a public authority network or a communications service related to public authority communications is under an obligation to ensure that the components of its communications network or service will not cause interference to public communications networks. The party in question must have in place appropriate mechanisms for preventing such interference.

Chapter 6 of these explanatory notes includes recommendations on the information security of Ethernet interfaces.

15.2 Protection from interference

According to section 15.2 of the Regulation, a telecommunications operator must protect its own communications network and services from malicious traffic from interconnection, application and customer interfaces by applying the required protection mechanisms to its networks.

Compared to the interconnection interfaces between communications networks, threats to customer interfaces are even more varied. For instance, insofar as the internet access service is concerned, the telecommunications operator must ensure that customers are unable to eavesdrop on other customers' traffic or cause denial-of-service attacks targeting these customers. The nature and severity of the threats together with the required protection measures vary according to the service provided and the technology used.

The malicious traffic mentioned in the obligation refers to traffic harmful to the telecommunications operator's own communications network or service that may at worst jeopardise the functionality of the telecommunications operator's communications network or service.

The obligation is not targeted at any one technology or protocol level, but rather the telecommunications operator must evaluate the threats caused by the technologies and services used in different interfaces, and subsequently implement all the mechanisms required for protecting its communications network and service. These mechanisms include filters based on the source or target address, the protocol used, message content, or the number of messages.

The aforementioned protection mechanisms can also be implemented at the control level, in which case the filtering of messages is not necessary. It may therefore be

sufficient, at least with regard to certain threats, for telecommunications operators to simply protect the control level of the devices processing the traffic in question in their network, while conveying traffic in the normal fashion via their network. If a telecommunications operator carries out protection at the control level instead of filtering, it must obviously implement the required mechanisms in all the necessary network elements.

Below are some examples of threats and the protection mechanisms required for them. It should be noted that the examples are not exclusive, and telecommunications operators must evaluate the required measures themselves:

- Bitstream customer interface: For example, the network operator should filter the customer port's incoming and outgoing BPDU (Bridge Protocol Data Units) messages and manufacturer-specific L2-level control protocol messages at the customer interface Ethernet DSLAM (Digital Subscriber Line Access Multiplexer) or the subsequent edge switch.
- VoIP interconnection and customer interfaces: The problem is discussed in more detail in RFC 5390[76] and 6404[77]. Protective measures that may be necessary include restrictions based on source addresses or the number of call attempts. Such mechanisms can be implemented with SBC, for example[78].

16. Shutting down unnecessary ports, services and protocols

Switching off services and protocols in the components of the communications network or service that are unnecessary for the operation of the communications services and the systems of the telecommunications operator is crucial because when the communications network or service component is running less software, it also has fewer vulnerabilities available to potential attackers. In addition, filtering unnecessary routing protocols or other control traffic in the management interfaces also reduces the possibility of traffic distributed over the interface interfering with the operations of the telecommunications operator's network, as an example.

The requirement applies to the communications network or service components both in the interconnection and customer interfaces (i.e. not to customer terminals, including modems, switches, computers, etc. owned and managed by the customer). The requirement is not targeted at any one technology or protocol level, but rather the telecommunications operator must evaluate the unnecessary physical ports, telecommunications ports (such as TCP and UDP protocol ports) or services at the device level and possibly also port level, and disable them. In contrast, the obligation does not apply to the telecommunications ports used in the traffic of the customer connection of the internet access service in general.

In some devices this issue may have been taken into account in the default settings, or the device manufacturer may have provided commands that can be used to switch these types of services off all at once. Telecommunications operators must find out the correct procedure for each device, since unnecessary services and protocols cannot be assumed to have been sorted out by default.

Examples of how the obligation may be complied within terms of different network elements are listed below. It should be noted that the examples are not exclusive, and telecommunications operators must evaluate the required measures themselves:

[76] IETF RFC 5390, Requirements for Management of Overload in the Session Initiation Protocol, https://tools.ietf.org/html/rfc5390.
[77] IETF RFC 6404, Session PEERing for Multimedia INTerconnect (SPEERMINT) Security Threats and Suggested Countermeasures, https://tools.ietf.org/html/rfc6404.
[78] IETF RFC 5853, Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments, https://tools.ietf.org/html/rfc5853.

- Bitstream customer interface (PE router): This means services such as FTP, HTTP, NTP, finger, or bootp not being switched on at the customer interface of the PE router's customer ports. Similarly, routing protocol or proxy ARP messages from customer ports should not be processed at the control level. However, traffic can be distributed via the network.
- Outgoing mail server (MSA): The outgoing mail server is a device or virtual server in the customer interface via which outgoing emails are sent from. This type of server does not handle routing or other network-level control protocols. In order to reduce vulnerability risks, no unnecessary services should be running in this network element. In MSA's case, these may potentially include FTP and HTTP servers.

17. Protecting IP interconnection interfaces and filtering the traffic

Information security of the routing protocol

BGP (Border Gateway Protocol), a key internet backbone network routing protocol, does not have integrated security by default, which exposes it to configuration errors and attacks. BGP is an interconnection protocol that organisations can use to connect their own network to the rest of the internet to send traffic to the right destination on the one hand and to receive traffic to destinations in the organisation’s own IP addresses on the other hand.

Due to the above, the Finnish Transport and Communications Agency has considered it necessary to impose obligations to improve the information security of routing. The obligations imposed by the Regulation are mainly based on ENISA’s recommendations for protecting the BGP routing protocol.[79]

The networks of operators connected to the internet are called autonomous systems (AS). Every autonomous system has its own unique numerical identifier (Autonomous System Number, ASN), with which the AS in question is known on the internet. Internet Assigned Numbers Authority IANA and the Regional Internet Registries (RIR) operating under it distribute the internet ASNs. Each autonomous system controls one or more sets of specific IP addresses and is connected to several other AS systems, which it notifies about the address series it manages with the BGP protocol. This network is used to guide the network traffic consisting of data packets to the right target, i.e. the operator that manages the destination addresses.

The BGP protocol was designed more than 25 years ago, and at the time, simplicity, ease of deployment, reliability and flexibility became its operating principles, which has resulted in the protocol still being used today. The size and role of the internet was much smaller then, than it is now, and routes were exchanged among only a small group of operators who knew and trusted each other, so that emphasising the security perspective was not considered necessary. Therefore, BGP is primarily based on trust in the authenticity of the received information. The routing nodes, or routers, publish information on data transfer paths or routes to other routers, and the other routers trust the information received and distribute it further without checking. As the use of the internet has become more common and services have moved online, the number of operators has grown exponentially, and as a result, configuration mistakes and human error allow even extensive disturbances to occur. There may also be malicious actors among the parties exchanging routes with each other that want to falsify route information for their own purposes, such as stealing traffic and the data it contains, aiming

[79] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp.

to cause outages in certain services, or guide traffic to the wrong place for scamming purposes.[80]

Route hijacking is one of the most common issues related to the security of BGP. In route hijacking, one routing node starts to advertise wrong information on routes to the neighbouring nodes directly connected to it, or alternatively it advertises owning IP addresses that in reality belong to a different party. BGP in itself does not contain a check for advertisements, and therefore such wrong information can easily spread to a large part of the internet over a short period of time, causing traffic to be routed incorrectly and potentially preventing access to and use of services.

BGP also faces other information security threats in addition to route hijacking. The TCP/IP protocol is used to establish a BGP session between two parties. The attacker may, for instance, attempt to alter authentic BGP peer-to-peer communication by inserting false BGP messages into the messaging between the BGP partners with the aim of breaking up or changing the connection to disrupt, hijack or rewrite internet traffic.

Incorrect source IP addresses

IP packets directed to a telecommunications operator's network (i.e. to its subscribers) may include an incorrectly defined source address, falsified either by mistake or on purpose. Receiving IP packets from another telecommunications operator with a source address that belongs to the telecommunications operator itself and is managed by it or that belongs to a private (non-public/non-routing) IP address space is not a regular situation – unless separately agreed – and involves a significant risk to information security. In addition to what has been mentioned above, there are also other addresses that should never be included in internet routing. These include e.g. IP prefixes that the Regional Internet Registries (RIR) have not distributed for use yet, as well as IP prefixes intended for special use.

IP spoofing, or falsifying the source IP address, is also often used in denial-of-service attacks. In IP spoofing attacks, the attacker falsifies its own network address so that the target of the attack believes that the packets originate from a reliable source. The purpose of IP spoofing is to conceal the attacker's identity. The lack of filtering of IP packets sent using a falsified sender address enables sabotage targeting other internet users without the possibility of discovering the perpetrator's identity. The purpose of the requirements concerning falsified source addresses is to significantly reduce the problems caused by attacks using falsified IP source addresses and network failures.

17.1 Detecting routing deviations

Routing deviation refers to an abnormal and often also sudden change in the accessibility and topology information of the network that may have a negative impact on the transmission of internet traffic. Detection of routing deviations is important in order to maintain a situational awareness of changes that could damage the telecommunications operator’s own network areas. The importance of detection, which makes it possible to react to incidents, is emphasised especially because attacks against the BGP protocol may have a major impact on the flow of network traffic. In addition, monitoring and detection enable analyses over a longer period of time, which can be used to plan proactive measures to maintain the security of network traffic.

The Regulation requires the telecommunications operator to have the ability to detect deviations in the visibility of its own routes. With regard to its own routes, it should be possible to observe at least how the routes advertised by the telecommunications operator are shown outside the telecommunications operator’s own environment (i.e. around the world), so that it would be possible, for instance, to detect a situation in which

[80] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP).

another party starts to advertise a competing route to the networks in question either by accident or with malicious intent. To implement the detection, things such as public routing information servers can be used, such as the information gathered by the Routing Information Service[81] of RIPE NCC.

The telecommunications operator should also monitor and control BGP network traffic incoming from other network areas and outgoing from the telecommunications operator's own network areas, so that the telecommunications operator can maintain knowledge of both the stability and resilience of its own network areas as well as the protection of privacy and information security of its subscribers.

17.2 Protecting BGP sessions

The Regulation requires the telecommunications operator to protect BGP sessions used to exchange routing information with routing neighbours whenever possible. The protection of BGP's TCP sessions can be implemented with the options described in the IETF specification RFC 5925,[82] for example. As for the spoofing of BGP sessions, it can be prevented by means such as using a Generalized TTL Security Mechanism (GTSM[83]). GTSM uses either the Time to Live (TTL) of an IPv4 packet or the hop limit of IPv6 to check if the packet was sent by the node next to the connected link, i.e. the neighbour with which the BGP session was established. The GTSM solution has been described in the IETF specification RFC 5082[84].

The aim of the obligation on protecting sessions is to prevent terminating BGP sessions through man-in-the-middle attacks or inserting falsified data into sessions.

Deploying the protective measures mentioned above requires configuration changes in the routers of the traffic exchange partner in addition to the local routers. A telecommunications operator can also have traffic exchange partnerships with parties other than other telecommunications operators, and in such cases, it may not be possible to agree on the deployment of protections. If so, the telecommunications operator must in any case enable the protection of BGP sessions and aim to promote the deployment of protective measures for its part, but if it is not possible to agree on a specific measure with the traffic exchange partner, the protection in question naturally cannot be implemented.

17.3 Filtering invalid source addresses

The Regulation requires the telecommunications operator to filter traffic containing an incorrect IP source address towards its communications network, unless otherwise agreed. Special filters should be installed in the routers, reducing the number of IP packets using falsified addresses sent to and from the network.[85]

This requirement only applies to source addresses relevant to the telecommunications operator's network, meaning that the telecommunications operator does not need to check the other source addresses distributed with an IP packet's payload in connection with VPN tunnelling, for example.

[81] RIPE NCC, https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris
[82] IETF RFC 5925, The TCP Authentication Option, https://tools.ietf.org/html/rfc5925
[83] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), p. 12 (TTL Security (GTSM)
[84] IETF RFC 5082, The Generalized TTL Security Mechanism (GTSM), https://tools.ietf.org/html/rfc5082
[85] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP). See also MANRS Actions for Network Operators, Action 2. Version 2.5.2 – 17 May 2021, https://www.manrs.org/netops/network-operator-actions/.

Filtering procedures must be performed at the technically appropriate level of specificity in the interconnection interface. The solution options to be used and factors to be considered are detailed in the IETF specifications RFC 2827[86] and RFC 3704[87].

Address spaces to be filtered out may include bogon prefixes, meaning address spaces reserved for non-public use (RFC 6761[88]) or special purposes and not intended to be used openly on the internet. Other address spaces to be filtered out may include networks that are so far not made available by IANA or local internet address registries.[89]

Bogon filtering may be carried out by using BGP routing tables as provided by trusted parties to which the changes to the use of address spaces are made centrally to the filter identifier list. The default bogon lists delivered with devices are outdated and should not be used.

In some exceptional cases, a telecommunications operator may agree with another telecommunications operator that a part of the telecommunications operator's address space is temporarily routed from the other's network. This procedure must be planned and executed with careful consideration, using methods suitable to the interconnection interface conditions. The primary responsibility for the blocking of traffic using false source addresses lies with the telecommunications operator that distributes the traffic.

In interconnection traffic between telecommunications operators, a situation in which the telecommunications operator receives route advertisements from another telecommunications operator but does not advertise them further is not considered a situation that would involve false source addresses. In that case the route advertisements do not correspond to the routing information of the telecommunications operator, but interconnection traffic between telecommunications operators can still be transmitted.

17.4 Filtering route advertisements

Pursuant to the Regulation, from the route advertisements received from IP interconnection interfaces, the telecommunications operator must reject by default the ones belonging to the operator's own blocks or to those provided by the telecommunications operator to one of its customers and that cannot be expected to be advertised by other telecommunications operators. The Regulation allows exceptions from this standard provision, if separately agreed.

The telecommunications operator must reject route advertisements where the ROA (Route Origin Authorization) does not correspond to the ROA information submitted to the RPKI (Resource Public Key Infrastructure) database.

No telecommunications operator should advertise routes including network address blocks controlled by another telecommunications operator or its customer, or more specifically their sub-blocks, without a separate agreement. For example, certain multihoming solutions may require such an agreement.

Unauthorised advertisements may mean directing traffic intentionally or unintentionally to the system of an external operator. In order to protect against risks associated with unauthorised advertising, a telecommunications operator receiving route advertising must filter out false advertising, such as the address blocks belonging to other telecommunications operators or their customers, as well as address blocks that should not be

[86] IETF RFC 2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, https://tools.ietf.org/html/rfc2827.
[87] IETF RFC 3704, Ingress Filtering for Multihomed Networks, https://tools.ietf.org/html/rfc3704.
[88] IETF RFC 6761, Special-Use Domain Names, https://tools.ietf.org/html/rfc6761.
[89] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), p. 11 (Bogon Filtering).

found in internet routing. Potential solution options for filtering have been described in the IETF specification RFC 7454[90].

Recommendation

The Finnish Transport and Communications Agency recommends that the telecommunications operator implement the technical and operative capability of filtering BGP AS paths. Path filtering is a method that can be used to accept or reject prefixes, the origin or route of which passes through a specific AS. This method can be used to e.g. reject prefixes that originate from a private AS, unless the AS in question is the customer of the telecommunications operator. Further information on the filtering of BGP AS paths can be found in the IETF specification RFC 7454[90].

17.5 Verifying route advertisements

The Regulation requires the telecommunications operator to create ROAs for the IP prefixes that the telecommunications operator owns or delivers to its customers. It must also be ensured that the ROAs are signed and published in the appropriate internet address registry.

One of the factors that significantly reduce the security of BGP is that the authenticity of route advertisements is not usually checked at all, because in principle, it is trusted that the information on routes received from the autonomous system acting as the route exchange partner is true. Normally this is in fact the case, but advertisements may also contain intentional or unintentional errors. However, solutions have been developed for verifying routing information, of which the best known and most commonly used is RPKI. With RPKI, autonomous systems can verify the route advertisements they own. Technologically, this is implemented by creating ROAs that are verified with a digital signature. The ROA states which autonomous system is authorised to create and advertise routes for certain groups of IP addresses. In order to verify the route advertisements, the routers must be configured to check the routing information with RPKI and carry out measures on the routes that do not pass the check. The simplest way to create and sign ROAs is to use the trust chains in the local internet registries. For Finland, the local internet registry is RIPE NCC; its website has comprehensive instructions for creating, managing and signing ROAs, as well as verifying route advertisements on routers[91].

In validating the BGP route advertisements, the validated RPKI information of routers participating in the BGP routing is compared to the arriving route advertisements. Validated RPKI information refers to the ROA information of RPKI-validated servers (RPKI Validator). The information on the status of ROAs comes to the RPKI-validated servers from the RPKI repository, which is managed by the regional internet registry.

This validation process has three possible end results: "Valid", "Invalid", and "NotFound".[92] The results "Valid" and "Invalid" mean that the ROA exists and it either corresponds to an RPKI-validated ROA in the RPKI database, or that these criteria are not met. "NotFound" means that the ROA has either not been created, or that it has not been published in the RPKI database.

Network areas that are not within the scope of the internet address registry system as well as areas for which creating an ROA is technologically impossible can be excluded from the scope of requirements on ROAs.

[90] IETF RFC 7454, BGP Operations and Security: https://tools.ietf.org/html/rfc7454. See also MANRS Action 1 and ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP).
[91] RIPE NCC, RPKI, https://www.ripe.net/manage-ips-and-asns/resource-management/rpki. See also ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), measure 7.
[92] IETF RFC 6811, BGP Prefix Origin Validation, https://tools.ietf.org/html/rfc6811.

In addition to the measures mentioned above, the telecommunications operator can use the BGPsec extension to the BGP protocol to improve the security of routing. IETF has described the BGPsec extension in RFC 8205[93] and RFC 8206[94]. BGPsec makes it possible to ensure cryptographically that every AS along the network traffic route has authorised the advertisement of the route to the next AS.

18. Preventing the falsification of IP addresses (IP spoofing) in the customer interface

In distributed denial-of-service attacks, fake source addresses are often used to complicate the identification of the attacker. An external network not involved in the attack or a randomly selected target network address may be spoofed as the source of traffic. Fake source addresses may also be randomly selected addresses from address spaces reserved for non-public use or a special purpose. The purpose of the requirements concerning the filtering of IP traffic with invalid source addresses is to minimise the problems caused by attacks using falsified IP source addresses.

As a milder alternative to filtering, the customer may also be contacted for the purpose of solving the situation. The basis of this option is the provision of the AECS pursuant to which the telecommunications operator may prevent or restrict the delivery of messages to a customer's terminal device in order to prevent information security threats and disturbances to communications networks or their associated services. As a milder alternative to traffic restriction measures, the telecommunications operator may find out the identity of the user causing an information security threat or disturbance and contact the user or the user's representative in order to eliminate the threat or disturbance.

18.1 Filtering

To block traffic with falsified source addresses, the telecommunications operator providing customer interfaces must filter any traffic from a customer interface to the communications network with a source address that is not assigned to the customer interface in question. If necessary, the telecommunications operator must be able to identify the customer interface from which the traffic with falsified source addresses is coming.

Traffic may be filtered e.g. by comparing the source address of each packet received at the interface to the list of valid address spaces and rejecting each packet with an address that does not belong to the listed address spaces.

In the case of ADSL connections, filtering can take place in the DSLAM network element, in the terminator of the DSL network connections, or the backbone network router. The appropriate filtering point depends on the network device technology and filtering capacity and the telecommunications operator's filtering practices.

18.2 User identification

Information security requires that the telecommunications operator must be able to identify a customer connection that has used a certain IP address on the basis of traffic data saved in the DHCP log, if necessary. Identifying the customer connection is necessary to allow the information security measures to be targeted at the correct customer interface, even if its IP address had changed.

According to FICORA's previous interpretation (Reg. No. 387/64/2009), the telecommunications operator may, if necessary, use traffic data both in the situations defined in

[93] IETF RFC 8205, BGPsec Protocol Specification, https://tools.ietf.org/html/rfc8205.
[94] IETF RFC 8206, BGPsec Considerations for Autonomous System (AS) Migration, https://tools.ietf.org/html/rfc8206.

section 272, subsection 1 of the AECS and when undertaking any of the measures currently referred to in subsection 2 of that section. FICORA's interpretation is that the telecommunications operator may use the traffic data not only to perform the actual measure referred to in section 272, but also to complete the necessary preparatory steps of the measure. Such preparatory steps may include the identification of a customer that has used a certain IP address on the basis of traffic data saved in the DHCP log.

19. Protecting the interfaces of the mobile network

The new use cases of the 5G network and the architectural solutions required by them have added new interfaces to the communications networks of telecommunications operators, through which network control can also be handed over to third parties for purposes such as the partial management of a communications network slice or edge computing unit. The signalling protocols of previous network generations are still widely used, maintaining connections between different network generations. As a whole, this increases the threat surface, the management of which requires telecommunications operators to protect interfaces comprehensively by implementing the obligations of this Regulation as well as actively monitoring and implementing the recommendations of different interest groups based on its own threat and risk assessment.

19.1 Signalling interfaces

In mobile networks, signalling means the steering of control plane and user plane traffic of the different elements of the mobile network as desired. As networks develop, the amount of and need for signalling has grown further. New functionalities are added to the communications network, and new signalling interfaces are created between them. The old Signalling System 7 (SS7) was already used in the 2G and 3G networks It has been used for purposes such as routing calls within a telecommunications operator or from one operator to other, for exchanging roaming information or notifying subscribers of the available features. Originally, the design of SS7 did not take the importance of information security sufficiently into account, which allowed SS7 to be misused. For example, a potential attacker could inject SS7 traffic into the mobile network and receive information that the attacker should not be able to access, or monitor network functions without permission. Attacks can also be used to map the mobile network with different scanning methods used within the network. Depending on the network structure and the location of the attacker, the attacker can map the structure of the core network, the radio access network or the IMS.[95] The information gathered during mapping can be used to target the next stage of the attack and choose a suitable method.

In 4G networks, the Diameter protocol replaces the SS7 used in 2G and 3G networks. Similarly, in 5G networks Diameter has been mainly replaced with HTTP/2 JSON. A common feature of these protocols is that potential attackers take advantage of a normal functionality of the core network, such as by pretending to be an HLR/HSS element of the network, and the attack may be used to find out the location of the end user in the network or determine the network structure. Another attack method involves creating denial-of-service situations in the network by exploiting certain signalling messages. This makes it possible to consume network resources or target the attack directly against a specific user. This should be taken into account in protecting different types of application interfaces in particular.

According to section 19.1.1 of the Regulation, in its mobile network interfaces the telecommunications operator must monitor the information security of signalling interfaces

[95] Rao, S. P. – Chen, H. Y. – Aura, T., Threat modeling framework for mobile communication systems. Computers and Security 125 2023, 103047, p. 1–23.

and design, implement and maintain information security management measures of the signalling interface based on up-to-date threat information and risk assessment.

Signalling protocol attacks can be prevented or mitigated by means such as filtering signalling messages. With a dedicated Signalling Firewall (SigFW) operating at the edge of the network, signalling messages can be filtered in the application layer already before they reach the targeted network element and affect its operation. In network elements that process signalling, too (SS7's Signal Transfer Point, STP; Diameter Agents, DRA, DEA; 5G's Security Edge Protection Proxy, SEPP), different levels of traffic filtering can be implemented depending on the technology. In general, security can be improved by hardening systems, i.e. by disabling unnecessary functions of the network elements.

SEPP is a mandatory security function specified by 3GPP that improves the security between 5G networks by implementing authentication, authorisation and encryption in the N32 interface, among other things.[96] By ensuring the appropriate design, implementation and maintenance of the SEPP functionality, it is possible to hide the communications network architecture and filter the incoming and outgoing traffic, among other things. In addition, it is possible to aim at encrypting the data to be transmitted as comprehensively as possible to ensure the security of data transfer between 5G networks.

Recommendations

The SS7 protocol is still widely used, and therefore also maintaining and developing its security in the future is justified. The Finnish Transport and Communications Agency recommends that the Common Nordic Recommendations on SS7 Security Issues drawn up in 2015 be implemented as widely as possible to achieve a comprehensive protection and detection capability.[97]

In order to ensure the security of the Diameter protocol, the Finnish Transport and Communications Agency recommends that the recommendation on the Diameter protocol drawn up and maintained by the GSMA should be followed; implementing its measures will help telecommunications operators to protect themselves against most of the known threats.[98]

19.2 Mobile network slicing

Network slicing means the logical separation of mobile network services that makes it possible to offer optimised and targeted services for different use cases. As the development of the 5G network advances, the following use cases have been specified:

- enhanced Mobile Broadband (eMBB), Vehicle to X (V2X)
- Ultra-Reliable Low Latency Communication (URLLC)
- massive Machine-Type Communication (mMTC)
- High-Performance Machine-Type Communications (HMTC).

The recommended features of the slice types described above and features related to the quality of the service have been specified in a publication by the GSMA.[99] The recommended features and values have been derived from a technical specification by 3GPP,[100] and GSMA has found that they meet the minimum requirements of the slice types in question. When a use case other than the ones mentioned above is involved, the telecommunications operator offering the slice can define its features more freely

[96] National Cyber Security Centre Finland, 5G Security Architecture, p. 33–34, https://www.kyberturvallisuuskeskus.fi/en/publications/5g-security-architecture.
[97] Common Nordic Recommendations on SS7 Security Issues, 18 December 2015.
[98] GSMA, FS.19 - Diameter Interconnect Security.
[99] GSMA, Official Document NG.116 - Generic Network Slice Template.
[100] 3GPP TS 23.501.

together with the Network Slice Customer (NSC). For example, this may involve a private network implemented with the slice (Public Network Integrated Non-Public Network, PNI-NPN).

Protecting the management connection

The Regulation (section 19.219.1.2) requires the mobile network telecommunications operator to protect the management connection of the slice so that unauthorised creation, change or removal of the slice is prevented and that the features of the slice or the data of the subscribers or users are not disclosed without authorisation. The aim of protecting the management connection is to prevent the attacker from using services subject to a charge without authorisation or creating a network slice that can be used to prevent services or monitor the customers of the communications network. The attacker may also attempt to carry out a man-in-the-middle attack by editing the slice in order to reroute the traffic.

In protecting the slice management connection, particular attention should be paid to situations in which the slice has been implemented as a service (Network Slice as a Service, NSaaS) and the customer (NSC) has been granted unique access rights to the network functions and data. In that case, it should be ensured through careful specifications, limitations and monitoring that the customer is only able to access the previously agreed data. In order to ensure information security, the traffic can be routed via an NEF function (Network Exposure Function), which controls the disclosure of data related to the features of 3GPP's core network outside the 3GPP domain, for instance, and validates and authorises all incoming message traffic from the outside.

Slice-specific authentication of access rights

The Regulation (section 19.1.3) requires the telecommunications operator to implement Network Slice Specific Authentication and Authorization (NSSAA) for the terminal devices using the slice based on the risk. In addition to the primary 3GPP authentication, the slice-specific access right authentication and authorisation must be implemented using identification information other than that used for the primary authentication. This must be done if it is necessary considering the information security threats related to the use of the slice and the technical possibilities of implementing access right authentication and authorisation.

The slice-specific access right authentication and authorisation between the terminal device and the AAA server (Authentication Authorization and Accounting Server) is implemented with the NSSAAF (NSSAA Function) that acts as a proxy server. NSSAAF sends the AAA server information about the slice (Single-Network Slice Selection Assistance Information, S-NSSAI) as well as the identifier of the terminal device (Generic Public Subscription Identifier, GPSI). Identifiers for the 3GPP area must not be sent to external network areas.

3GPP Release 17 introduces a new function for the access control of the network slice (Network Slice Admission Control, NSACF), which enables better management and use of the slices. The function makes it possible to monitor and control the slice-specific number of registered terminal devices and PDU (Protocol Data Unit) sessions. The security function can mitigate risks especially in a situation in which the slice management right is outside the 3GPP domain. For analysis and further processing, the information sent to the holder of the slice (Application Function, AF) is transmitted using the NEF functionality.[101]

The Regulation has taken into account that there may not necessarily be a need for special slice-specific access right authentication and authorisation if, for instance, there

[101] 3GPP, Network Slicing Security for 5G and 5G advanced systems, https://www.3gpp.org/technologies/slicing-security

are no unusual information security threats related to the use of the slice. Therefore, the Regulation also takes account of the fact that the terminal device used may limit the possibilities of implementing further measures, although even in such a situation, there must not be any uncontrolled information security risks generated.

If slice-specific authentication is not carried out, unauthorised terminal devices may use the resources of the slice or gain information on the network's characteristics without having the right to do so. An unauthorised terminal device can be any ordinary device that may have completed the primary authentication successfully with 3GPP identifiers, but does not have the access rights necessary for the use of a specific network slice.[102]

19.3 Edge computing in the communications network

The new use cases of the communications network and especially the mobile network set performance and reliability requirements, and the systems of the communications network are brought closer to the end user in order to meet them. In that case, the user's traffic can be directed to the service's resources via a shorter route, or the service may even be implemented locally within the edge computing unit. The edge computing environment characteristically consists of the software and devices of several different entities that makes it possible to develop versatile new operating methods and services and offer them to users. Typically, the physical devices, hypervisors and applications of the environment are implemented by different parties. Together with third-party applications and different kinds of virtualisation solutions, the telecommunications operator's network functions create a whole that is disunited and exposed to vulnerabilities, especially if no special attention is paid to the matter. It must also be taken into account that due to its location, the edge computing unit may be more exposed to physical influence (attacks) than the more centralised network functionalities of the telecommunications operator.

Hardening the software components that implement virtualisation in accordance with the hardware manufacturer's instructions should be taken into account in the implementation and maintenance of the edge computing environment, also considering the risks related to the location of the environment's physical systems. In that case, the connection between applications, the NEF function and the edge computing environment must be implemented securely to ensure the security of the edge computing units as well as the rest of the communications network by implementing mutual, repeated authentication and identification and ensuring the implementation and permanence of the security features of the NEF function throughout their life cycle. Special attention should be paid to an arrangement in which the edge computing unit is controlled by a third party from outside the 3GPP system. To ensure the security of the edge computing unit, security measures critical to slicing and virtualisation, such as slice-specific access and authentication management, should be implemented in addition to comprehensive vulnerability management and hardening the virtualisation environment.

Chapter 4 Specific requirements for internet access services

20. Separation of traffic in internet access services

According to section 20.1 of the Regulation, the telecommunications operator must separate the traffic of its customers, ensuring that the users of various subscriber connections cannot have unauthorised access to each other's traffic. The telecommunications operator must ensure that an unauthorised re-routing of traffic between subscriber connections is not possible.

[102] ENISA GL SO11, 5G Security Control Matrix: SO11-010.

Internet access connections based on shared capacity between subscribers have been used in networks of housing corporations, for instance. In such networks, the internet access available in the housing corporation is shared between the users in the housing corporation by using network equipment belonging either to the building or to the telecommunications operator. Similar shared capacity network models are often used in MAN networks that provide an open access to all users within the range of the network.

Subscriber traffic may be separated either physically by isolating the traffic in designated cables or logically by using connection-specific VLANs or traffic encryption to isolate the traffic. Another way to keep subscriber traffic separate is the port isolation function of DSLAMs or switches, particularly when the group VLAN ID is used.

Unencrypted WLAN networks are commonly used particularly in locations with a large number of moving subscribers. The encryption of WLAN connections is technically possible, but the encryption, particularly the management of encryption keys, would make the provision of the service significantly more complex. For this reason, section 20.2 of the Regulation includes a special exception that makes it possible to provide unencrypted WLAN connections without traffic separation at the radio interface. If possible, users should be informed of the risks related to using unencrypted WLAN connections. WLAN connections refer to wireless local area network connections defined in the IEEE standard 802.11.[103]

21. Directing of outgoing email traffic from consumer subscriber connections

According to section 21 of the Regulation, the telecommunications operator must prevent unlimited outbound SMTP traffic from consumer subscriber connections other than through servers intended for outgoing SMTP traffic. However, the Regulation also makes it possible to deviate from the restriction, in which case the telecommunications operator must inform the subscriber about the risks associated with the matter and be able to react quickly in case of possible interference related to it.

Unlimited outbound SMTP traffic (port 25) from a connection to the internet enables malware to send junk email. Allowing outbound email traffic only via the telecommunications operator's designated outgoing SMTP traffic servers is an efficient way to curb junk email generated by malware. This does not affect users' communication possibilities significantly, because email can be sent through the outgoing mail server of the telecommunications operator providing the internet access service by using authenticated mail submission[104] or webmail interfaces. However, the filtering measure on port 25 restricts the realisation of email servers in consumer subscriptions.

The provision establishes the best practices of email submission operations described in IETF document RFC 5068.[105]

The Regulation also allows unlimited traffic, if necessary. Allowing unlimited SMTP traffic means that traffic going to communications port 25 reserved for SMTP traffic may be sent outside the telecommunications operator's network from the network space assigned by the telecommunications operator to the consumer connection.

Some consumer customers may have a reasonable need for direct SMTP traffic from the consumer connection to anywhere beyond the telecommunications operator's network. Such need arises, for example, when a consumer customer manages SMTP traffic through their own server. The Regulation allows making exceptions from the filtering of

[103] IEEE, 802.11 standard, https://standards.ieee.org/ieee/802.11/7028/.
[104] IETF RFC 6409, Message Submission for Mail, https://tools.ietf.org/html/rfc6409.
[105] IETF RFC 5068, Email Submission Operations: Access and Accountability Requirements, https://tools.ietf.org/html/rfc5068.

port 25 for such situations, for example. Exceptions are made at the discretion of the telecommunications operator, because the Regulation does not include an obligation for telecommunications operators to make customer-specific exceptions to filtering. For example, subscription type specific technical limitations may restrict making such exceptions.

Blocking unlimited SMTP traffic means blocking the traffic going to communications port 25 from the network space assigned by the telecommunications operator to consumer connections via other servers than those designated for outbound SMTP traffic by the network operator.

The blocking of unlimited SMTP traffic provided for in the Regulation must not affect email traffic using other communications ports, such as email protocols with user identification or encryption. In particular, it must be ensured that blocking does not affect traffic to Mail Submission service port 587 described in IETF document RFC 6409[104]. This allows the customers of a telecommunications operator providing an internet access service to send and receive secure, authenticated traffic to and from an email system administrated by another email service provider.

Pursuant to the Regulation, the telecommunications operator may make an exception and allow unlimited SMTP traffic to go through other servers than servers intended for outgoing SMTP traffic. In this case, the telecommunications operator must inform the subscriber about the risks associated with open traffic. The telecommunications operator must also be able to react quickly in case of interference.

22. Obligation to filter malicious traffic in an internet access service

The requirements of section 22 of the Regulation impose an obligation to filter malicious traffic in internet access services and maintain documentation on the filtering measures in use.

The Regulation obliges the telecommunications operator to maintain a technical capacity to temporarily filter out malicious traffic in internet access services (for the definition, see section 2.3). Indeed, the purpose of the Regulation is to ensure that the telecommunications operator has up-to-date processes, procedures and systems in place that enable it to start temporarily filtering out malicious traffic as quickly as possible. Such technical ability to filter out involves both the ability to first detect malicious traffic and then filter it out, if necessary. However, it should be noted that the requirement in this section also relates to the Regulation of the Finnish Transport and Communications Agency on disturbances in telecommunications services and its section 4 laying down provisions on the ability to detect situations that may disturb information security.

Filtering out traffic may help in limiting the impact of the denial-of-service attacks that use a certain kind of management traffic to overload network systems. In addition, it is possible to limit malicious traffic to a certain port.

It should be noted that pursuant to section 272, subsection 4 of the AECS, the measures shall be implemented with care, and they shall be commensurate with the seriousness of the disruption being combated. Such measures shall not limit freedom of speech, the confidentiality of a message or the protection of privacy any more than is necessary for the purpose of attaining the goals set for the measures. Such measures shall be discontinued if the conditions for them specified in legislation no longer exist.

In addition to the general filtering ability obligation set in section 22 of the Regulation, section 26 of the Regulation lays down specific requirements concerning the filtering out of malicious email traffic.

Protecting the systems and services of the telecommunications operator from denial-of-service attacks is also discussed in section 6.1.3 of the Regulation.

22.1 Technical capability for filtering

The telecommunications operator must equip its communications network with a system that enables the detection of malicious traffic. The system must be able to monitor the traffic in the communications network when necessary and with an appropriate sampling accuracy.

Because of the high volume of traffic in public communications networks, it is often impossible to build a system that detects malicious traffic without a major impact on the network performance. In such cases, information may be gathered on the basis of samples of traffic, which means that only a certain share of the packets sent over the network are monitored. The sampling accuracy must be selected to allow a sufficiently accurate overview of the network traffic.

For example, the telecommunications operator may use an automatic management system that monitors traffic volumes or exceptional events in the network and sends an alarm to the monitoring system when predetermined limit values are exceeded. In addition, the management of information security events may use intrusion detection and prevention systems.

In a situation where the information security of a communications network or service is at risk, the telecommunications operator may have to use temporary measures to block traffic to a certain communications port or limit traffic to certain recipient addresses. The filtering measures have to be suspended as soon as the threat that jeopardises the information security of the communications network or service is over.

Technical capability for filtering means e.g. that the network elements of the telecommunications operator support the limitation of traffic volumes on the basis of protocols, addresses, ports and network interfaces. It must be possible to limit traffic volumes without unnecessarily risking the availability of the network. In addition, the technical capability requires that the network operation centre of the telecommunications operator is able to launch the necessary filtering measures.

22.2 Filtering rules and their documentation

When using various traffic filtering lists, it should be particularly ensured that the filtering rules are up to date to avoid incorrect and unnecessary filtering due to outdated filtering rules. For example, filtering must not prevent the appropriate use of allocated IP network resources.

Up-to-date documentation of the available filtering measures should be maintained to keep track of the filters in place in networks and services and monitor their appropriateness.

Traffic may be filtered to block malicious email traffic, prevent the capture of unused address spaces from route advertising or curb traffic related to a denial-of-service attack from the traffic source addresses. Because falsified but routable source addresses are also regularly used in denial-of-service attacks, the need for address filtering and its updating mechanisms should be considered carefully.

23. Disconnection of an internet access service connection

When traffic to or from a customer connection threatens the information security of a communications service, the situation should be primarily addressed by the means laid

down in section 22 of the Regulation, i.e. filtering out the traffic within the telecommunications operator's network, or other measures that are less severe than disconnection, such as contacting the customer. However, if such measures are not enough to bring the situation that relates to a customer connection and threatens information security under control, the telecommunications operator has the right to initiate measures to remove the threat caused by the infected terminal.

The established interpretation of the Finnish Transport and Communications Agency is that infected terminals connected to the telecommunications operator's network that e.g. send substantial volumes of junk mail or malicious traffic from the connection always threaten the information security of the services of the telecommunications operator. Therefore, under section 273 of the AECS, an infected terminal device can be grounds for disconnecting the device from the network.

Since the disconnection of the connection prevents the customer from using the connection, the disconnection process must be planned carefully, detailed instructions must be provided, and the interruption or restrictions to the use of the connection should remain as short as possible.

23.1 Disconnection situations

In this Regulation, disconnection of the service of a customer connection means e.g. that if traffic to certain communications ports threatens the information security of the communications service, these ports must be temporarily closed for the customer connection. Similarly, the telecommunications operator may have to limit the outgoing traffic of certain application protocols from the customer connection, if the traffic jeopardises the information security of the communications service. Reasons arising from the customer connection do not typically mean situations when the customer connection or the web service connected to the internet through the customer connection is under a denial-of-service attack and receives exceptionally large volumes of traffic.

In all information security measures and in the event of disconnection, attention must be paid to the fact that the traffic data in communications may only be processed in cases of information security violations or threats to communications networks and services. Therefore, the telecommunications operator does not have the right to process the traffic data to prevent e.g. the use of the connection in committing a crime that does not jeopardise information security. An exception to this rule is the preparation of means of payment fraud referred to in section 272, subsection 1, paragraph 3 of the AECS (see also Chapter 4 of the Annex to the explanatory notes).

23.2 Disconnection process

If possible, the customer should be contacted by phone, email or other means before the connection is disconnected from a public communications network. However, consultation of the customer must not unduly jeopardise the measures to ensure the information security of the service.

Disconnection measures must be carried out following a predefined procedure. The measures performed and, in particular, the reason for disconnecting the connection must be recorded for any subsequent investigation of the situation.

Disconnection instructions must include the necessary procedures for reconnecting the customer connection to the network once the telecommunications operator has decided that the information security threat to the communications service no longer exists. For example, if there is malicious traffic caused by malware, the connection may be reconnected to the communications network as soon as the customer contacts the telecommunications operator to report that the malware is removed from the system.

If the service operator and the network operator are two different companies, they must reach an agreement on the principles related to the practical implementation of the disconnection. Both parties must have the possibility to take the necessary steps to ensure the information security of their service or network. Disconnections and reconnections must be reported to the other party without delay.

In applying the measures, the particular circumstances arising from the type of subscriber connection may be taken into account. For example, if an information security issue is related to the data services of a mobile subscription, it is possible to block only the data services from the connection until the information security issue has been resolved.

If the customer connection is automatically controlled, the connection or its certain services are automatically disconnected from the communications network for half an hour, as an example, without any manual operations by the operator, usually when the limit values for malicious traffic are exceeded. When the connection is disconnected, it is possible to redirect customer traffic to a service that informs the customer of the reason for the disconnection and the measures that the customer can possibly take to repair their device. In addition, the customer may be provided a possibility to go to the necessary websites for installing virus protection and running the operating system updates. This approach reduces the need for more permanent disconnection of customer connections.

If an automatic system manages the closure and reopening of customer connections carried out for information security purposes, customers must be informed of the principles guiding the temporary closures and reopenings.

Chapter 5 Specific requirements for text and multimedia message services

24. Filtering text and multimedia message traffic

The Regulation (section 24) requires the telecommunications operator to have appropriate systems and procedures for filtering out traffic identified as malicious from the text and multimedia message services. This refers to both technical capabilities as well as predetermined processes and operating instructions. Telecommunications operators must be able to filter out malicious messages from both incoming and outgoing message traffic. Subsections 1 and 2 on the filtering obligation correspond to subsections 1 and 2 of section 26 on filtering email, but no special need to provide for filtering to safeguard the operation of systems related to the production of the service has been identified for SMS and MMS messages.

Filtering based on the sender and other traffic data of text and multimedia messages as well as the message content can be used to address especially situations in which the aim is to implement an extensive campaign of sending malware or phishing messages via text or multimedia messages.

Identifying malicious traffic can be based on e.g. the threat information shared by the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency or other telecommunications operators, messages sent by the telecommunications operator’s own customers or information received from other parties that is estimated to be reliable.

As a less severe method compared to filtering messages, the Regulation allows tagging messages suspected of being malicious with an identifier (e.g. by changing the sender ID or adding a text at the start of the message) or disabling any links contained in the messages, when this is technically possible. The measures mentioned above prevent

misleading the recipient without completely preventing the delivery of messages, such as if it is not sufficiently certain that the message is malicious when the measure is taken. The measures must affect the delivery of appropriate messages as little as possible.

For the SMS service, an SMS firewall can be used to implement filtering. For the MMS service, there may not be equally well established technical solutions easily available. In addition, developing new technical solutions may not be justified in proportion to the threat, when taking account of the relatively low usage of the service. As a result, section 24.3 of the Regulation includes an exception, according to which it is possible to not implement filtering based on content and traffic data with regard to the MMS service under certain conditions. In that case, the telecommunications operator is required to detect disturbances that endanger information security in other ways, and it must have the ability to react quickly to them. For example, the detection may include monitoring for an anomalous number of messages, which may indicate an infected terminal device. In that case, instead of filtering the telecommunications operator may use another method suitable for removing the effects of the information security incident that is as mild as possible, which may involve e.g. preventing the sending of MMS messages until the malware has been removed from the terminal device. The measures must be in accordance with section 272 of the AECS.

Chapter 6 Specific requirements for email services

This chapter explains the obligations laid down in Chapter 6 of the Regulation.

25. Contact information for email services and address resource management

The Regulation requires that the domains used in the provision of email services must include "postmaster" and "abuse" email addresses or other abuse contact information and that messages sent to these addresses are regularly monitored. The purpose of the requirement is to ensure that email services have a contact point for reporting any functionality or usage incidents to the service provider, regardless of the location of the reporter.

In addition, the Regulation requires that an email address released from a customer must not be transferred to another customer in less than six months. Messages are often sent to email addresses after the address has been terminated. If the released address would be made available to another user immediately or soon after its termination, the new customer could receive emails intended for the old customer. To maintain the confidentiality of email messages and prevent the abuse of email addresses, a terminated email address must be quarantined for six months before it may be released to be reserved again.

25.1 Contact information of the telecommunications operator providing email services

The telecommunications operator providing email services must ensure that the domains used in connection with the provision of email services include "postmaster" and "abuse" addresses or abuse contact information and that messages sent to these addresses are regularly monitored.

Due to the extensive distribution of the postmaster and abuse addresses, they often attract inappropriate messages. Therefore, the telecommunications operator must arrange the monitoring of such addresses to ensure that the processing of relevant messages sent to these addresses is not delayed because of the large volume of malicious

traffic. If the telecommunications operator has a large number of domains, the messages sent to the postmaster and abuse addresses of the domains held by the telecommunications operator should be redirected to appropriate contact points.

The telecommunications operator may also delegate the monitoring of the incoming messages to the party responsible for the domain. In other words, it is also possible to let the party responsible for the domain, on behalf of the telecommunications operator, to monitor the messages received at the postmaster and abuse addresses.

25.2 Reuse of an email address released from a customer

The telecommunications operator providing email services must not transfer an email address released from a customer to another customer before a period of six months has passed since the release of that email address. If the former holder of the email address wants to have the released address back within six months from the release of the address, it is possible to reassign the address. However, the right to have the email address back does not oblige, as such, the service provider to keep the messages contained in the email account after the account has been closed. Such an obligation may, nevertheless, arise from an agreement between the parties.

26. Specific obligation to filter email services

This section of the Regulation discusses the capability to identify malicious traffic and lays down the requirements concerning the filtering out of malicious traffic.

A significant share of email traffic may today be interpreted to be malicious. If malicious email messages are identified and filtered out as early as possible, the burden to the email system is reduced and the delivery of legitimate messages becomes smoother.

Indeed, the purpose of the requirements is to curb the volume of malicious traffic and spam going through the servers of telecommunications operators providing email services, which helps reduce the overload of the email system, prevents harmful effects to the system (in cases of denial-of-service attacks, for example), improves the reputation of the email servers of the telecommunications operator, and secures the delivery of legitimate messages. Filtering out malicious incoming messages prevents the content harmful to the customer's information security and to the communications networks in general from entering the customer's electronic mailbox and being opened. In addition, the processing of email messages becomes easier for customers when they do not need to pick out legitimate messages from spam. This helps improve the customer experience and usability.

There are several different methods to identify and process malicious email traffic. The Regulation does not lay down requirements as to which one(s) should be chosen, and the telecommunications operator providing email service has the option to select the methods that are the most appropriate for the service it provides.

As some email service customers may want to verify themselves that there is no incorrect filtering, email service providers also have the option to tag the incoming traffic identified as malicious instead of filtering it out. The Regulation also makes it possible to agree on a customer-specific basis that the email service provider will not filter or tag incoming traffic.

26.1 Identification of malicious email traffic

The identification of malicious email traffic is a prerequisite for all processing by the email service provider, such as filtering out and tagging. The telecommunications operator providing email services should therefore have in place up-to-date and reliable mechanisms for identifying malicious email traffic.

Identification of malicious email traffic and the consequent filtering out or tagging may be based on the identification mechanisms of malicious sources of email, heuristic filtering systems, virus filtering of outgoing traffic, identification of abnormal volumes of outgoing email traffic from a user account, or to the verification of the compliance of message headers with internet standards. Various identification mechanisms are discussed in more detail in Chapter 2 of these explanatory notes.

On the basis of email traffic sources, it is possible to identify a significant share of both the known legitimate email sources and the known malicious traffic sources. The identification may be based on the sender's network address, domain or outgoing mail server. The determination of harmfulness is based on previous information on the messages sent through this source or the analysis of the message content. The identification of legitimate sources helps in avoiding the filtering out of legitimate email traffic due to incorrect identification. As for the identification of malicious sources of email traffic, it helps in preventing the delivery of messages from these addresses or tagging the message as suspicious before it is delivered to the customer's electronic mailbox.

However, email service providers are able to identify only a certain share of malicious email traffic on the basis of email sources. For this reason, the service provider must have other methods available to identify malicious email traffic. Many of these methods may incur significant costs to the email service provider, however. Stricter identification criteria are also more sensitive to misinterpretation. Therefore, the telecommunications operator providing an email service may choose the mechanisms employed in its system from several different alternatives to identify a significant share of the malicious traffic while the delivery of legitimate messages is affected as little as possible.

Even a single method enables the identification of a large share of malicious email traffic. However, the results are usually better when several complementary methods are used simultaneously. All methods have their advantages compared to others, but unfortunately each method also has its problems. The email service provider must be aware of the pros and cons of the methods it uses and evaluate their consequences before deployment.

In addition to basic-level identification mechanisms that meet the above criteria and are available to all customers, the email service provider may also offer its customers more advanced and customised solutions for identifying and processing malicious traffic by e.g. a separate agreement.

26.2 Recommendations on the identification of malicious email traffic

Telecommunications operators providing email services are recommended to identify the sources of malicious email traffic in the SMTP handshake phase. In this way, a major share of malicious email traffic may be blocked even before it enters the email system. This may help in reducing significantly the overload caused by malicious email traffic to email servers.

It is recommended that several methods for identifying malicious email traffic should be used simultaneously. This helps in improving the accuracy of the identification of malicious email traffic, which also means that stricter filtering criteria may be chosen.

To avoid misinterpretations, the use of allow lists is recommended when the email service provider uses blocking and filtering methods.

26.3 Processing of incoming email traffic

The processing of incoming email traffic refers to operations that can be performed on the incoming customer email messages received through the mail delivery agent (MDA)

servers or proxy servers of the email service provider. Such operations include the identification of malicious email traffic and its sources, filtering out and tagging of traffic identified as malicious, and delivering the traffic to the customer.

The filtering of incoming email traffic means that the incoming email traffic to customers that is identified as malicious is prevented from entering the customers' electronic mailbox. By filtering out malicious email messages, it is possible to reduce the overload of email servers and the volume of malicious traffic delivered to customers' electronic mailboxes, which also makes it easier to identify legitimate messages. Consequently, this helps in preventing the negative consequences of malicious messages that may be created when customers open attachments contained in the messages or are redirected to sites containing malware when they follow a link in a message. The filtering of email traffic may improve the customer experience and the information security of the service.

Pursuant to the Regulation, an email service provider must tag or filter out from incoming email traffic any traffic identified as malicious by the mechanisms it uses to identify malicious email traffic or its sources. Instead of filtering out automatically all traffic identified as malicious, the email service provider may also redirect some or all of the messages identified and tagged as malicious to a separate, user-specific folder designated for malicious traffic, in which a certain number of messages may be kept available for a certain time to be checked by the user. The email service provider may also remove content identified as malicious from the messages before they are delivered to the customer.

The service provider may separately agree with the customer that traffic identified as malicious will not be filtered out or tagged as malicious. Therefore, the email service provider may not, by default, provide the service without filtering out or tagging the traffic identified as malicious, which means that this option cannot be included in standard agreements by default.

In spite of the exceptions mentioned above, the email service provider must always filter out from incoming traffic any email traffic identified as malicious that compromises the information security of the systems employed to provide the email service (usability included).

26.4 Processing of outgoing email traffic

The processing of outgoing email traffic refers to operations that can be performed to the outgoing email messages delivered through the Mail Submission Agent (MSA). Such operations include the identification of legitimate senders and the filtering out of outgoing email traffic identified as malicious and delivered through the Mail Submission Agent.

Pursuant to the Regulation, the telecommunications operator providing email service must filter out from outgoing traffic any traffic identified as malicious. For this purpose, the telecommunications operator may select the mechanisms to be used in its system from several alternatives (see e.g. Chapter 2 of the Annex to the explanatory notes). The objective is that a significant share of outgoing malicious traffic is identified and filtered out while the delivery of legitimate messages is affected as little as possible.

If the email service provider finds out that the terminal of any of its customers is used in delivering malicious email traffic, the service provider must filter out the outgoing malicious traffic from the customer or block the customer's email traffic entirely and, if possible, contact the customer.

27. Open relays for email

Open relays for email (for the definition, see section 2.2) are commonly used to deliver malicious email traffic.

By identifying email systems that function as open mail relays and blocking the use of third-party mail relays for message delivery, it is possible to curb the volume of malicious email traffic delivered.

The telecommunications operator providing an email service must ensure that the email systems administered by it will not function as open mail relays. Testing and a careful configuration of settings every time systems or services are deployed or modified are examples of maintaining the safety of the use of email systems.

The telecommunications operator should regularly test all the email systems it administrates to ensure that the systems are not functioning as open mail relays. If the operator does not have its own testing system, it can test its systems with public services available on the internet.

With respect to the mail submission agent of the internet access service connection, the above obligation means that sending unauthenticated email messages is possible only from the network of the telecommunications operator.

28. Connection between customer and email server

Interface between customer and email server means the interface between Mail User Agent (MUA) and electronic mailbox (MS) as well as the interface between Mail User Agent and Mail Submission Agent (MSA).

Securing the interface between MUA and MS and between MUA and MSA means the authentication of the customer and the encryption of the interfaces between the customer and the service.

Usernames and passwords are delivered between the customer and the email server. Securing the interface between the customer and the server prevents third parties from accessing this information, prohibits the abuse of the service and improves its information security. In addition, it helps to ensure that the customer messages remain confidential in the traffic between the customer and the server. A secure interface also provides customers with a secure way to use the email service independently of access networks and improves the confidentiality of the service as experienced by customers.

However, customers should be aware about the fact that securing the interface between the customer and the server does not always mean an end-to-end protection of the connection from sender to recipient.

Due to the usage of browser-based webmail services, it is justified to require that the interfaces must always be secure.

The telecommunications operator providing email services must offer its customers as the primary alternative a secure connection between the customer and the electronic mailbox and between the customer and the outgoing email server. The obligation also applies to other than browser-based email services.

The obligation means that the telecommunications operator must offer all its email service users an option to use a secure interface, and the use of a secure interface is presented to customers as the primary or the only alternative in the user instructions delivered and available to customers.

To identify legitimate users and establish a secure customer interface from the customer to the mail transfer agent, using the SMTP-AUTH protocol is recommended.[106] Between the customer and the electronic mailbox server, it is possible to use for this purpose IMAP or POP connections secured by SSL/TLS protocol (IMAPS/POPS).[107]

When port 25 is used to send or transmit email (relay), STARTTLS can be used to protect the connection also when the user is not authenticated.[108]

Customer interfaces of browser-based email services must always be secured. The recommended securing method for the transport layer is the TLS protocol.[109]

Chapter 7 Provisions on entry into force

This chapter explains Chapter 7 of the Regulation, i.e. the provisions on entry into force and transitional provisions.

29. Entry into force [and transition period]

[The Regulation enters into force three months after the Regulation is issued.]

[106] IETF RFC 4954, SMTP Service Extension for Authentication, https://tools.ietf.org/html/rfc4954.
[107] IETF RFC 2595, Using TLS with IMAP, POP3 and ACAP, https://tools.ietf.org/html/rfc2595 and IETF RFC 4616, The PLAIN Simple Authentication and Security Layer (SASL) Mechanism, https://tools.ietf.org/html/rfc4616.
[108] IETF RFC 3207, SMTP Service Extension for Secure SMTP over Transport Layer Security, https://tools.ietf.org/html/rfc3207 and IETF RFC 7817, Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols, https://tools.ietf.org/html/rfc7817.
[109] When using the HTTPS protocol, see IETF RFC 2818, HTTP Over TLS, https://tools.ietf.org/html/rfc2818.

ANNEX Other matters related to the subject matter of the Regulation

Various recommendations related to information security in telecommunications operations, the interpretations of the Finnish Transport and Communications Agency and background material of the themes covered by the Regulation have been compiled in this Annex.

1. Deceptive email addresses

Deceptive email addresses are created to make the other party believe that the owner of the address is another person or entity. Deceptive email addresses mean email addresses registered with the name, business ID or generally known maintenance address (such as postmaster, webmaster or customer service) of another person or company.

If the telecommunications operator providing an email service detects or is informed about a deceptive email address registered to its domain, it should tackle the problem. The telecommunications operator has the right to disable addresses that have been set up for deceptive purposes.

An email address may also be personal data of another person. Pursuant to the Personal Data Act, personal data should be correct, and the Act provides for an obligation to correct personal data if there are errors in it. The use of another person's personal data for commercial or other gain may also be punishable under criminal law.

The Finnish Transport and Communications Agency recommends that the telecommunications operator providing an email service not allow its customers to set up deceptive email addresses defined in RFC 2142[110] or corresponding addresses in the Finnish language related to the telecommunications operator's own domain name.

2. Identification mechanisms for malicious email traffic

This chapter presents a variety of well-known and commonly used mechanisms for identifying malicious email traffic.

2.1 Block lists

Block lists help in identifying and filtering out or tagging connections or email messages coming from known illegitimate email sources. A block list usually consists of network addresses that are sources of malicious email traffic.

A block list may also be a list of individual email addresses, domains or email servers used in spamming. A block list may be maintained by the email service provider itself or a third party or be personally defined by a user. Email systems commonly use centralised block lists maintained by third parties.

In selecting and using block lists, particular care must be taken to avoid any misinterpretation. Static block lists are often unreliable, because the sources of malicious email traffic change often and a wrong entry in a static block list may block legitimate email traffic for a long time. Removing entries from static block lists always requires manual effort. Dynamically maintained block lists, on the other hand, are updated quickly, and incorrect entries are regularly removed from such lists.

Compiling one's own block list is usually not recommended, because the contents of the list would change continuously. To secure the availability of email services, block lists

[110] IETF RFC 2142, Mailbox names for Common Services, Roles and Functions, https://tools.ietf.org/html/rfc2142.

that block large domains because of the behaviour of individual users should be avoided. Other block lists that should be avoided are the ones that do not state clearly the reasons why an entry is included in the list or do not have clear procedures for leaving the list, or if the use of the list is not recommended for major service providers.

When selecting a block list maintained by a third party, an email service provider should pay particular attention to the following characteristics of the list:

- Listing principles are published
- Leaving the list is simple, and there are clear instructions for it
- Contact details of the list administrator are published
- Entries to the list are not made on the basis of a single invalid message
- The list is updated regularly.

When using block lists, it should also be taken into consideration that lists may contain false information, and the use of a list may also block legitimate email traffic. When using a list maintained by a third party, the behaviour of the list must be constantly monitored. Because different lists usually contain different sources, the use of several lists at the same time usually yields the best results. The identification rate of malicious traffic to the mail delivery agent from different sources increases when different lists help in identifying mutually different malicious sources. Block lists may also be used in heuristic filtering to rate the harmfulness of an email source. In this case, an incorrect list entry does not mean that an otherwise legitimate message is filtered out.

When using block lists, an email service provider must have an effective mechanism for identifying the most important known legitimate sources of email. At the time of publication of this Regulation, this means the use of allow lists. An email service provider must enter its relevant partners and reliable domestic service providers to the list of addresses (allow list) that overrules the block lists used in the email system to minimise the impact of disturbances possibly caused by block lists.

2.2 Allow listing

An allow list is used to indicate that the reception of messages is permitted through certain network addresses, email servers or addresses that are known to be generally trusted senders of legitimate messages. Trusted senders may include known email service providers and partners.

The use of an allow list is practically unavoidable when other blocking or filtering measures based on the source of email are used. Allow lists help in ensuring that messages from trusted sources get through even if the messages would otherwise be filtered out due to e.g. an incorrect block list entry.

When using allow lists, it should be taken into consideration that malicious email traffic may be delivered even through trusted bodies, which means that even allow listed sources cannot be trusted unconditionally. In addition, it is also possible to spoof allow listed addresses on malicious email messages to improve the penetration of malicious email traffic. To avoid problems, the messages sent by the allow listed sources must also be monitored.

An allow list is often a rather static list of network addresses. The service provider must ensure that the listed entries are up to date to avoid problems caused by outdated information.

2.3 Track listing

A track list, also known as a greylist, is based on the way that software sending out malicious email traffic operate. Unlike ordinary email systems, such software does not attempt to resend the message even if its delivery fails. Track listing means automatic

statistical reporting of certain parameters (IP address/C class of the sender of incoming mail, SMTP sender and SMTP receiver) or a hash table formed from these parameters. The reception of a message from an unknown sender or sent with certain parameters is denied. When the source attempts to resend the message after a pause, the message is received. Later, messages from this source are received without delay.

The problem with track listing is the delay of legitimate email messages coming from previously unknown sources. In addition, track listing is based on the single delivery principle of malicious email traffic senders. If malicious senders start to reattempt the sending of their messages to circumvent track listing, it will no longer work. In addition, resending email messages causes more email traffic, which overloads both networks and email servers.

2.4 Reputation systems

Reputation systems are based on the previous submission history of the message source. Messages submitted by email sources (such as the SMTP sender and the IP address of the sender) are monitored, recorded and compared to the previous message history of the source. In recording and comparing the messages, attention is paid to whether the source sends legitimate or malicious email messages. Email sources may also be monitored on the basis of the volume of outgoing messages from the server. This information is used to determine the level of reputation of the email source judging by the points awarded on basis of the previous submission and message history of the sender. The level of reputation forms a basis for the decision on whether the message coming from the source is delivered to the recipient as usual, whether the message is delivered with lower priority, or whether the delivery is blocked.

The advantage with reputation systems is that their decisions are based on the long-term monitoring of sources, and messages are not filtered out on account of individual invalid messages. Reputation systems support well other filtering systems, and the use of a reputation system as part of heuristic filtering helps to reduce errors caused by other criteria. However, when using a reputation system, it should be kept in mind that the ratings of the system cannot necessarily respond to a quick flood of malicious traffic.

Reputation systems maintained by third parties collect from their own customers the information on which ratings are based. Extensively gathered information is then consolidated to a single database for rating purposes and to determine reputation levels.

2.5 Heuristic analysis

An email service provider may also determine the harmfulness of messages and filter them by using an analysis based on the content of the message, or use such methods in addition to systems that identify email sources when filtering out email messages.

The content of malicious email messages usually meets certain predetermined criteria. Methods of filtering on the basis of message content include comparing a checksum calculated from the message to known checksums calculated from malicious messages, or scanning messages for certain elements that suggest harmfulness, such as certain words, types of formatting, attachments, images or links. It is also possible to scan email messages for characteristics of legitimate messages. Content-based filtering may be combined with filtering methods based on block lists or other similar methods.

When several mechanisms are combined, each method either increases or reduces the number of points awarded to the harmfulness of the message. The decision on whether the message is malicious or not is made on the basis of total points. Following the analysis, the filtering software may either block the message, tag the message as likely to be malicious, or forward the message as it is.

2.6 Irregular traffic volume

To recognise irregular volumes of traffic, an email service provider should set limit values for normal use. If the volume of outgoing email traffic exceeds the limit defined as normal, the email service provider may temporarily block the customer's email traffic. In addition, the email service provider should, whenever possible, contact the customer to allow them to take the necessary steps to remedy the situation by e.g. cleaning an infected computer.

2.7 Other methods for improving the security and reliability of email

In addition to the mechanisms listed in the above chapters, email service providers may choose from numerous other methods for improving the security and reliability of email.

Methods intended for verifying the authenticity of the sender of the email message include Sender Policy Framework (SPF)[111] and Domain Keys Identified Mail (DKIM)[112] that help in verifying that the email message has been sent from the email server indicated by the domain name in the email address. In addition to these, the DMARC protocol can be used, and in fact its use is recommended for monitoring and determining how the messages sent under a domain name should be processed and which authentication methods the message should pass. DMARC also adds a reporting feature that can be used to monitor the passing and failing of transmissions.

SPF is implemented with a domain name system (DNS). A text-type name record is published in the DNS, and the authorised email servers allowed to send email under the domain name in question or a lower-level domain name are specified as its parameters. The mail transfer agent (MTA) confirms the origin of the received message from its return path header field together with the information published in the DNS and applies the specified processing practice to the message, and as a result, the message in question is either approved, rejected or quarantined. The weakness of SPF is that it only checks the return path header field and not e.g. the from header field, and therefore a malicious sender can still manipulate the message envelope and try to deceive the message recipient. This is possible, because a normal user usually only looks at the from field while the more detailed header fields are hidden by default. This weakness can be corrected by using DMARC, another email validation protocol, in addition to the SPF.

For emails, DKIM offers a method for cryptographically verifying the digital identity related to messages, typically the domain of the sender. In addition, the method aims to ensure that the contents of the message have not been altered after sending. The DKIM method is based on a combination of a digital signature and a key pair. A digital signature is added to the message header and encrypted with a private key, and in addition a public key is added to the DNS information of the sender domain name that the message recipients can use to decrypt the data. A DKIM signature alone does not significantly increase or decrease the non-repudiation of the message, but a signature added to the message is nevertheless important information for email reputation assessment systems and especially decision-making related to the message, and therefore DKIM should be used in connection with other methods that improve the reliability of email.

Like SPF and DKIM, the use of DMARC is also based on DNS, meaning that DMARC records are created in the DNS like other authentication protocols. DMARC can be used to specify that the message passing SPF and DKIM validation is mandatory. DMARC can also be used to ensure that the domain name shown in the From field visible to the user corresponds to the domain name used in the SPF and DKIM validation.

[111] IETF RFC 7208, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, https://tools.ietf.org/html/rfc7208.
[112] IETF RFC 6376, DomainKeys Identified Mail (DKIM) Signatures, https://tools.ietf.org/html/rfc6376.

Like other methods to control malicious email traffic, such methods involve a number of weaknesses that must be taken into account when implementing the methods. The weaknesses of DKIM have been discussed in e.g. RFC 4686[113]. Because email exchange services, online postcards and submission services by internet access service providers are against the operating principles of such mechanisms, they are best suited to the positive identification of sources.

Before any new mechanisms are introduced, email service providers should study carefully the operating principles of the method and the risks involved to avoid filtering out legitimate email messages. In many cases, the accuracy of individual mechanisms is uncertain, if the interpretation of the mechanism concerning the harmfulness of the traffic is unconditionally trusted. On the other hand, if several methods are used simultaneously as part of a rating system, it is possible to obtain very accurate filtering results with a small margin of error.

3. Prevention of malware traffic to domains or IP addresses used in updating the malware

In 2009, the agency known at the time as FICORA was informed of several hundred suspected cases of Conficker/Downanup worm infections in Finnish networks It was estimated that the number of computers infected with the worm around the world was several million. The network worm was inspected to discover how it was updated. After infection, the worm creates a number of random domains based on the date and tries to contact them in order to update itself. Some of the infected terminals could be identified by registering some of the domains used by the worm and monitoring the incoming traffic. Network administrators were then informed of the addresses of the infected terminals.

In its interpretation (Reg. No. 46/64/2009), FICORA found that telecommunications operators may significantly reduce the information security threat caused by worm infections by blocking traffic to the domains it uses to update itself. Blocking the traffic makes it considerably more difficult to update the worm and use the broken system. According to FICORA's interpretation, blocking traffic to the malware update domains may be considered to be a necessary measure to safeguard network services or communications services (currently referred to in section 272 of the AECS).

If the telecommunications operator wants to identify the infected terminals in its network, it is possible to block traffic by e.g. sending a modified response to the name server query of the infected terminal to the resolver name servers of the telecommunications operator. The IP address of the modified response may be e.g. an unreserved IP address from the telecommunications operator's own IP address space.

According to FICORA's interpretation, telecommunications operators had the right to save the source addresses of the traffic to domains used in updating the malware and identify the subscribers who use the source addresses. To identify the subscriber, the telecommunications operator was also permitted to process traffic data collected in another context. The collected traffic data were to be destroyed as soon as their processing was no longer justified. The traffic data could be disclosed to third parties only when the criteria specified in law were met.

In 2021, the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency recommended that telecommunications operators should filter out the IP addresses of the active command and control servers of the Flubot malware that was spreading into mobile phones.[114] In that case, the malware was using encrypted

[113] IETF RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail (DKIM), https://tools.ietf.org/html/rfc4686.
[114] FICORA #1157426 Suositus internetyhteyspalveluliikenteen suodattamisesta (Recommendation on filtering traffic in an internet access service), 8 June 2021.

DNS traffic, which meant that preventing traffic to the domain names used was not an effective filtering method.

4. Filtering SMS traffic to prevent malware from spreading

In 2021, the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency recommended that mobile network telecommunications operators filter SMS messages based on content to prevent the Flubot malware from spreading.[115] The malware attempted to spread by sending text messages containing links to malware with the aim of having the user install it on the phone.[116] The processing of message content based on such filtering could be implemented within the scope of section 272 of the AECS.

5. Filtering traffic to prevent preparations of means of payment fraud

In 2009, the agency known at the time as FICORA was informed of several cases where the network traffic of Finnish online banking customers had been redirected to network servers maintained by a third party without the customers knowing. This was done by modifying the DNS settings with malware installed on the user terminal: After the modification, the terminal uses the DNS servers defined by the administrator of the malware to resolve the IP addresses of domain names. It is likely that this was done with DNS changer type malware, such as Zlob.

FICORA's interpretation (Reg. No. 1952/64/2009) was that under provisions corresponding to section 272 of the current AECS, telecommunications operators were allowed to filter out traffic to domains specified on a case-by-case basis in order to prevent preparations of means of payment fraud referred to in Chapter 37, section 11 of the Criminal Code planned to be implemented on a wide scale via communications services. Filtering out is justified also from the perspective of detecting, preventing, investigating and committing to pre-trial investigation disruptions in information security.

Pursuant to the AECS, traffic data may only be processed to the extent necessary for providing and using a network service, a communications service or an added value service and for the purpose of ensuring information security. Infected terminals in the network of the telecommunications operator compromise the information security of the services provided by the telecommunications operator. Therefore, identifying terminals infected with malware may be considered necessary for providing the service and ensuring its information security.

FICORA's interpretation was that telecommunications operators were allowed to collect the source addresses of traffic to specified domains related to the case and identify the subscriber that uses the source address on the basis of the data saved in the DHCP log (or similar log).

6. Recommendations concerning Ethernet interface information security

This chapter discusses a few of the key information security problems related to Ethernet technology that impact the operation of communications networks and services, while also providing examples of protection against these problems. The provided examples deal with situations in which the telecommunications operator network has been

[115] FICORA #1176113 Suositus tekstiviestiliikenteen suodattamisesta (Recommendation on filtering text message traffic), 25 November 2021.
[116] Traficom, NCSC-FI issued a severe alert on malware being spread by SMS, https://www.kyberturvallisuuskeskus.fi/en/news/ncsc-fi-issued-severe-alert-malware-being-spread-sms.

implemented using a conventional switch solution. The problems do not therefore primarily apply to networks using MPLS or pseudowire tunnelling, for instance.

Even though no detailed obligations regarding the subject are laid down in the Regulation, the Finnish Transport and Communications Agency recommends that telecommunications operators also prepare for the threats mentioned in this chapter when implementing the necessary protection mechanisms.

6.1 Broadcast storms

A broadcast storm is created when too many multicast messages are sent to the network via the Network-to-Network Interface port. A broadcast storm may render the Network-to-Network Interface unusable, if the multicast messages fill up the interconnected network's capacity. Due to this, parties engaging in interconnection traffic must prepare for limiting the impact of broadcast storms. This can be done, for instance, by restricting the capacity allowed for distribution messages in the network.

The Finnish Transport and Communications Agency recommends that only switches supporting storm control filtering be used in interconnection traffic interfaces. This type of filtering enables users to reserve a specific portion of line capacity for unicast and broadcast traffic. Filter settings must be configured so as to prevent filtering from interfering with normal network traffic.

6.2 L2 control protocols

Operators can prevent loops from being created in their own L2 networks by utilising the Spanning Tree protocol (STP). The protocol may also lead to significant problems if misused. Many manufacturer-specific protocols such as the Cisco protocols CDP and VTP can also result in similar problems. At worst, a customer may intentionally or unintentionally crash the provided service or direct traffic via its own subscription without authorisation, which enables activities such as tapping and redirection of traffic. STP and manufacturer-specific protocols must be isolated by means of a control level.

6.3 VLAN hopping

Double Tag VLAN packets can be used to send denial-of-service traffic from a customer port via the switch's backbone network to VLANs behind other switches. This is possible since, in a native connection, the switch typically only removes the outermost VLAN identifier, in which event the other VLAN identifier is still left in the packet. Establishing a bidirectional connection is not possible, but this can be used to conduct denial-of-service attacks on the port of some other service or customer.

In order to avert the threat, the network operator must ensure that only VLANs used by the subscriber are allowed in the trunk port of the subscriber switch. In the Network-to-Network Interface, network operators must only allow the VLAN area agreed with the service operator. It is also recommended to keep the number of switches between routing devices and the customer to a minimum.

6.4 MAC address operation management and filtering

MAC address operation management and filtering are network protection methods that are necessary when protecting against interference of telecommunications traffic and errors caused by device failure. If a customer is able to fill the switch's MAC table, the switch will send all packets to every switch port, in which event every device connected to the switch will be able to view all customer traffic distributed via the switch. In switches and DSLAMs, the restricted size of the MAC table thus represents one of the known information security threats.

The severity of the above threat is, however, dependent on the technology used. The telecommunications operator may, for instance, reduce the risk of the above by utilising the Provider Backbone Bridging technology (802.1ah).[117] The problem can also be prevented by restricting the number of port-specific MAC addresses and by allowing traffic only to correct known MAC addresses. Preventing MAC tables from filling up from customer ports is not always possible in older or cheaper switches.

The aforementioned problem also applies to the dimensioning of the Ethernet network between the terminating router and customer terminal. NOs and SOs should thus be able to manage the number of active MAC addresses in a port-specific manner (subscriber switch or interconnection interface).

7. Recommendations on communication related to information security

7.1 Providing general information on information security risks and the protection methods available to the customer

Poorly maintained terminals and careless use of services compromise not only the information security of the customer's own terminal, but also the information security of other users and the services provided by the telecommunications operator.

It is recommended that telecommunications operators provide advance information for customers on the information secure use of the communications service or subscription. General information security communications by the telecommunications operator to customers improve the customers' awareness of general information security risks of networks and services. A significant share of the reported customer information security problems may be avoided if the customer has taken appropriate steps to ensure the basic information security of terminals and pays attention to information security threats when using the services.

Another objective of the information measures is to enable customers to protect themselves from subscription type specific information security threats. For this reason, the telecommunications operator should ensure that the customers are informed of subscription type specific information security risks and available measures to maintain information security before the subscription is enabled.

The telecommunications operator can use different methods for providing information. It can be arranged by means such as a login page for enabling the use of the connection or by guiding the customer to a specific web page. In addition to its own customer communications, the telecommunications operator can direct customers to the website of the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency.

In the provision of information, the emphasis should be on the means available to the customer or the user of a customer connection to ensure the information security of its terminal. Such means include traffic encryption, separation of user traffic, installation of a firewall before the computer is connected to the internet, anti-virus systems, and updating the operating system and other software.

If necessary, the communication should focus on subscription type specific information security risks, i.e. the specific risks caused by the technical implementation of the subscription. An example of such risks is the provision of an internet access service through an unencrypted WLAN connection. In such situations, the telecommunications operator must provide information on the specific risks to the confidentiality of communications

[117] IEEE Standards Association, IEEE Std. 802.1ah - Provider Backbone Bridges, https://www.ieee802.org/1/.

related to the use of the connection. Information security risks may also be connected to subscriptions in which users share the capacity.

Section 246, subsection 3 of the AECS also applies to instructing the customer. According to the section, a subscriber shall maintain equipment or a system to be connected to a public communications network in accordance with instructions from the telecommunications operator so as not to endanger the information security of the public communications network or service. Furthermore, section 274, subsection 2 of the AECS provides for the obligation of the telecommunications operator to provide information on the measures available for combating the threat when the telecommunications operator informs subscribers or users of an information security breach involving the service of the telecommunications operator or a threat of it.

7.2 General communication about information security measures

It is recommended that telecommunications operators provide the customers with advance information on what measures may result from any potential use of the public communications network or service that endangers information security.

In fact, under Government Decree on Information to be Provided Before Drawing up a Communications Service Agreement (96/2021), the telecommunications operator must provide the customer with information on the measures taken by the service provider if information security is at risk or in case of information security threats or vulnerabilities before drawing up a communications service agreement (section 1, paragraph 6). The telecommunications operator should also describe to its customers the general principles of intervening in such a use of the subscriber connection or services that compromises the information security of communications services. This means that the customer is informed e.g. about the fact that if an infected terminal is connected to the interface, the interface may be closed down temporarily.

7.3 Providing information on vulnerable customer devices

The users of communications services can play an important role in protection against information security threats related to communications networks and services.[118]

Section 274 of the AECS provides for the disturbance notifications of telecommunications operators to subscribers and users in a situation involving significant information security violations or threats to information security in the services of the telecommunications operator and of anything else that prevents or significantly interferes with communications services. Furthermore, under section 246, subsection 3 of the AECS, a subscriber shall maintain equipment or a system to be connected to a public communications network in accordance with instructions from the telecommunications operator so as not to endanger the information security of the public communications network or service.

Vulnerable customer devices are a threat to the information security of the communications networks and services of both the customer and the telecommunications operator. As the number of devices in 5G networks in particular multiplies, network controls should also be used to prepare for signal storms in a situation in which a large number of vulnerable customer devices is infected by malware. In addition, attention should be paid to updating vulnerable devices or removing them from the communications network.

The Finnish Transport and Communications Agency recommends that the telecommunications operator notify its customers if it becomes aware of a vulnerable terminal

[118] ENISA GL SO29 applies to informing users about information security threats as well as the measures available for the user for protection against them.

device of the customer, the vulnerability of which threatens the information security of the communications network or service of the customer or the telecommunications operator, even in cases when there is no legal obligation to do so. On a case-by-case basis, vulnerabilities that endanger information security can also be addressed through means provided for in sections 272 and 273 of the AECS as well as sections 22 and 23 of the Regulation.

7.4 Describing the filtering principles of an email service

Customers are entitled to receive information on the filtering principles used by the telecommunications operator providing an email service.[119]

The filtering of email traffic often gives rise to customer enquiries to the service providers, if legitimate email messages are filtered out by error or if e.g. the volume of malicious email traffic entering the customers' electronic mailboxes increases significantly. As the identification and filtering out or tagging of malicious email traffic is essential for maintaining the functionality and availability of the service, it is possible to avoid misunderstandings and unnecessary customer complaints by informing customers about the basic principles adhered to in filtering email traffic.

It is recommended that the telecommunications operator describe to the customers the general principles of filtering email. The purpose of the description is to provide customers with general information about the filtering methods used and their impact on customer traffic. However, the description of the filtering principles to customers must not compromise the information security of the communications service. The description does not need to be unnecessarily detailed or provide exact reasons why e.g. a single email message is identified as malicious traffic on the basis of its content. If block lists are used, the email service provider does not have to provide a detailed list of the block lists used in filtering, since they may vary depending on the situation.

7.5 Description of the administration of email addresses

The practices concerning the administration of email addresses vary between service providers. Defining the administration practices and describing them to customers helps in avoiding misunderstandings and providing quicker solutions to problems.

It is recommended that the telecommunications operator should describe to its customers its email address administration practices. The purpose of the description is to help customers understand how a new email address can be acquired, how the settings of the email service can be edited, and how an email address can be deleted.

[119] On the information to be provided on the processing of traffic data, see section 138, subsection 2 of the AECS. See also section 1, paragraph 6 of the Government Decree on Information to be Provided Before Drawing up a Communications Service Agreement (96/2021) mentioned above.