EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SECURITY SUPERVISION UNDER THE EECC

JANUARY 2020

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

CONTACT

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Eleni Vytogianni and Marnix Dekker, ENISA

ACKNOWLEDGEMENTS

We are grateful for the valuable input received during interviews, discussions and meetings with different telecom experts, telecom security experts, both in the public and in the private sector. For this project we have worked with Ernst & Young Business Advisory Solutions S.A. and the Athens Cybersecurity Team, under tender ENISA S-COD-19-T07.

LEGAL NOTICE

COPYRIGHT NOTICE

CATALOGUE NUMBER TP-02-19-765-EN-N ISBN 978-92-9204-304-9 DOI 10.2824/ 647924

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The EU's electronic communications landscape has changed dramatically over the last decade. Consumers have largely switched from traditional electronic communication services, like telephony and SMS, to number independent interpersonal communications services the so-called "over-the-top" (OTT) communications services like Skype and WhatsApp offering voice calls, video calls, sharing of photos, etc. Consumers nowadays require high-quality internet connections for consuming online content, social media, streaming content and therefore they need fast and reliable internet connections.

In December 2018, the new set of telecom rules called the European Electronic Communications Code[1] (abbreviated as EECC) was published and it entered into force. The EECC updates the existing EU telecom package of 2009 and paves the way for the roll out of fibre, very high capacity networks and next generation mobile networks (5G), which will create jobs and growth, enable new application scenarios like internet of things (IoT) and new business models. EU countries have to transpose this EU directive into national law by the end of 2020.

An important part of the EECC is consumer protection and security of electronic communications. Article 40 of the EECC contain detailed security requirements for electronic communication providers and article 41 empowers the competent authority with respect to the implementation and enforcement of these requirements. As with Article 13a, the security requirements in the 2009 telecom package, ENISA will support EU Member States with the implementation of Article 40, to ensure there is an effective, efficient, and harmonized approach to security supervision across the EU.

With this paper, ENISA aims to support EU countries with their transposition, by analysing the main changes to the security requirements and the security supervision under the new rules.

The principles of security supervision under the new rules (Article 40 and 41 of the EECC) are a continuation of the old rules (Article 13a and Article 13b of the Framework directive[2]). However, we see seven important changes in the new rules, which adapt, extend or in some cases clarify the old rules:

1. Under the EECC, more communication services are in scope, particularly the so-called Over-The-Top (OTT) communications services like Gmail, WhatsApp e.g.
2. There is a definition of security, security incidents and security measures.
3. Providers should implement state-of-the-art measures, as well as encryption and end-to-end encryption, when needed.
4. Providers should promote encryption and encryption software, where needed, and inform subscribers about threats.
5. Incident notification parameters are clarified, specifying factors of significance, such as economic and societal impact,
6. The authorities for electronic communications should be able to get support from the national CSIRT and collaborate with other authorities, such as the national authorities for the NIS Directive and data protection authorities.

EUROPEAN ELECTRONIC COMMUNICATIONS CODE (EECC)

- **Article 40** contains detailed security requirements for electronic communication providers and
- **Article 41** empowers the competent authority with respect to the implementation and enforcement of these requirements

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN
[2] Directive 2002/21/EC as amended by Directive 2009/140/EC, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

7. The national telecom authorities have the power to require providers to take measures to mitigate significant threats and to impose a time-limit on the implementation of those measures (even before actual incidents occur).

Based on these seven changes, we propose three key areas where work needs to be done by the national authorities as well as ENISA.

1. The existing security measures framework needs to be reviewed and updated to reflect the state-of-the-art, good practices in the EU Member States, and the new provisions in the EECC.
2. A common threshold and reporting model should ideally be developed to allow for harmonized national reporting thresholds and a consistent EU-wide implementation of mandatory incident notification and annual summary reporting. This model should take into account the OTT communications services.
3. A common approach to cross-border security supervision is needed, not only because the European telecom market is increasingly interconnected and interdependent, but also because the EECC brings a number of global communication service providers in scope.

For the latter it is important to communicate and share good practices with other groups of national authorities, such as the working group of authorities for the Digital Service Providers under the NIS Directive and the group of authorities for the Digital infrastructure sector under the NIS Directive.

In the coming period, ENISA will be preparing for these changes. We have started the adaptation of the Cybersecurity Incident Reporting and Analysis System[3] (CIRAS). We are also reviewing the Article 13a guideline on security measures, which is used by many countries as the basis for supervision of the security requirements for the electronic communication service providers. ENISA looks forward to working closely with BEREC and the competent authorities for supervision of Article 40 of the EECC.

[3] https://resilience.enisa.europa.eu/article-13

1. INTRODUCTION

ENISA will support the national authorities for implementation of Article 40 of the European Electronic Communications Code (EECC)

In December 2018, the EU adopted a new set of telecom rules, the European Electronic Communications Code[4] (EECC). An important part of the EECC is consumer protection and security of electronic communications. Article 40 of the EECC contains specific security requirements for electronic communication providers. As with Article 13a of the Framework Directive[5] in the past, ENISA will support the national authorities for Article 40 of the EECC, particularly on the technicalities and details of security supervision, to ensure there is an effective, efficient, and where possible harmonized approach across the EU. Article 40 of the EECC brings important changes with respect to Article 13a. In this paper, we analyse these changes and their meaning for security supervision by the national competent authorities.

This work follows up on almost 10 years of close and fruitful collaboration between ENISA and the national competent authorities on the implementation of Article 13a. This collaboration has resulted in several technical guidelines on Article 13a, which carry the consensus of the entire Article 13a Expert Group.

We should underline however that this paper is an ENISA paper and that it is not a guideline produced by the ENISA Article 13a Expert Group. For the EECC it is too early to discuss or reach consensus about more detailed aspects of security supervision, because most EU Member states are in the process of transposing and competences still need to be assigned.

We based our analysis on interviews with experts from public and private sector, including experts from providers, national authorities, industry associations, telecom consultancy firms, etc.

Throughout this document, we discuss examples of electronic communication services. These examples are merely for the sake of illustration and we underline that this paper does not aim to define which services are in scope of the EECC. Member States will transpose and interpret the EECC provisions. It is the role of BEREC to enhance the consistent application of the provisions of the EECC across Member States. The EECC is a directive, meaning that EU countries will have to transpose this into national law by the end of 2020. In this document, we refer to the EECC provisions as “new rules” and those of the Framework Directive as “old rules” even if they are still applicable.

1.1 TARGET AUDIENCE

- Experts in national ministries, telecom and other national authorities
- Experts in the electronic communications sector (providers, industry associations, etc).

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN
[5] Directive 2002/21/EC as amended by Directive 2009/140/EC , https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

2. POLICY CONTEXT

The European Electronic Communications Code, the EECC, is an EU directive, meaning that EU countries will have to transpose the new rules into national legislation. The deadline for this transposition is December 2020. It is important to see the changes it brings and the main provisions.

December 2020 is the deadline for the transposition of the EECC Directive into national legislations of EU Member State.

2.1 OLD RULES

The new EECC replaces four EU directives. In this paper, we refer to these directives as the "old rules", although they are of course currently still in place.

- The Framework Directive, which is based on the Framework Directive 2002/21/EC as amended by Directive 2009/140/EC.
- The Access Directive, which is based on the Access Directive 2002/19/EC and amended by Directive 2009/140/EC.
- The Authorisation Directive is based on the Authorisation Directive 2002/20/EC and amended by Directive 2009/140/EC.
- The Universal Service Directive is based on the Universal Service Directive 2002/22/EC and the Citizens' Rights Directive 2009/136/EC.

These rules were last modified in 2009 as part of a wider EU telecom reform, which included also the e-privacy directive, addressing privacy in electronic communications and the BEREC regulation, establishing the Body of European telecom regulators.

2.2 MAIN PROVISIONS OF THE EECC

The new EECC replaces four EU directives. In this paper, we refer to these directives as the "old rules", although they are of course currently still in place.

The main provisions of the EECC are:

- **Clear and inclusive rules**: the same rules will apply all over Europe with a vision of an inclusive single market;
- **Higher quality of services**: the Code will foster competition for investments, in particular in next generation networks - 5G, meaning higher connection speeds and higher coverage;
- **Competitive prices**: by multiplying the offers available and bringing more capacity, the prices are expected to go down;
- **Consumer protection**: the Code proposes a regulatory approach, which allows all actors, from traditional telecom operators to online players, to provide interpersonal communication services with the same level of protection for the end-user. That means that, 'electronic communications services' will also cover services provided over the internet such as messaging apps and email (also known as 'over-the-top' or 'OTT' communications services).

2.3 SECURITY REQUIREMENTS IN THE EECC

Security is one of the general objectives of the EECC, as outlined in Article 3 of the EECC:

Article 3 General objectives

[…] (d) promote the interests of the citizens of the Union, […] by maintaining the security of networks and services, by ensuring a high and common level of protection for end-users through the necessary sector-specific rules

Most of the security requirements are contained in Article 40 and Article 41 of the EECC. Although the EECC uses many of the same principles of security supervision that existed in the old rules, the EECC also brings several changes in security supervision. We will look at the changes in more detail in the next section.

For the sake of reference we quote Article 40 and Article 41 in full below.

Article 40 Security of networks and services

1. Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services.

The European Union Agency for Network and Information Security ('ENISA') shall facilitate, in accordance with Regulation (EU) No 526/2013 of the European Parliament and of the Council (45), the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market.

2. Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.

In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:

(a) the number of users affected by the security incident;

(b) the duration of the security incident;

(c) the geographical spread of the area affected by the security incident;

(d) the extent to which the functioning of the network or service is affected;

(e) the extent of impact on economic and societal activities.

Where appropriate, the competent authority concerned shall inform the competent authorities in other Member States and ENISA. The competent authority concerned may inform the public or require the providers to do so, where it determines that disclosure of the security incident is in the public interest.

Once a year, the competent authority concerned shall submit a summary report to the Commission and to ENISA on the notifications received and the action taken in accordance with this paragraph.

3. Member States shall ensure that in the case of a particular and significant threat of a security incident in public electronic communications networks or publicly available electronic communications services, providers of such networks or services shall inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users. Where appropriate, providers shall also inform their users of the threat itself.

4. This Article is without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC.

5. The Commission, taking utmost account of ENISA's opinion, may adopt implementing acts detailing the technical and organisational measures referred to in paragraph 1, as well as the circumstances, format and procedures applicable to notification requirements pursuant to paragraph 2. They shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(4).

Article 41 Implementation and enforcement

1. Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to issue binding instructions, including those regarding the measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and time-limits for implementation, to providers of public electronic communications networks or publicly available electronic communications services.

2. Member States shall ensure that competent authorities have the power to require providers of public electronic communications networks or publicly available electronic communications services to:

(a) provide information needed to assess the security of their networks and services, including documented security policies; and

(b) submit to a security audit carried out by a qualified independent body or a competent authority and make the results thereof available to the competent authority; the cost of the audit shall be paid by the provider.

3. Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance and the effects thereof on the security of the networks and services.

4. Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to obtain the assistance of a Computer Security Incident Response Team ('CSIRT') designated pursuant to Article 9 of Directive (EU) 2016/1148 in relation to issues falling within the tasks of the CSIRTs pursuant to point 2 of Annex I to that Directive.

5. The competent authorities shall, where appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities, the competent authorities within the meaning of Article 8(1) of Directive (EU) 2016/1148 and the national data protection authorities.

2.4 ROLE OF ENISA

Article 40 of the EECC asks ENISA to facilitate harmonization on the security aspects.

The European Union Agency for Network and Information Security ('ENISA') shall facilitate, in accordance with Regulation (EU) No 526/2013 of the European Parliament and of the Council (45), the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market.

This paper is a first step towards harmonized implementation of the EECC across Europe. It follows up on a decade of ENISA support of and collaboration with the EU's telecom regulators in the Article 13a Expert Group.

3. SECURITY SUPERVISION

The principles of security supervision under the new rules (Article 40 and 41 of the EECC) are a continuation of the old rules (Article 13a and Article 13b of the Framework directive). Under the new rules, as with under the old rules:

- Communication providers have to assess risks, take appropriate security measures and report significant incidents to national authorities (Article 13a of the Framework directive, Article 40 of the EECC).
- The national telecom authorities should have powers to supervise this, to enquire about measures in place, and to investigate cases of non-compliance by providers (Article 13b of the Framework directive, Article 41 of the EECC).

This means that for the new rules national authorities can build on the experience and practice developed under the old rules.

There are also some changes for security supervision, which adapt, extend or in some cases clarify the old rules. In this section, we analyse the seven most important changes:

1. More services in scope: Under the EECC more communication services are in scope, particularly the so-called Over-The-Top (OTT) communications services like for example Gmail, WhatsApp, and Skype.

2. New definitions of security and security incidents: The EECC provides definition of security, including also aspects like the confidentiality of communications. The EECC also provides a security baseline and a set of minimum-security measures.

3. State-of-the-art measures and (end-to-end) encryption: The EECC requires that providers implement state-of-art measures, as well as encryption and end-to-end encryption, where appropriate.

4. Promote encryption and inform subscribers about threats: The EECC requires that providers promote the use of encryption and encryption software with subscribers and that they inform subscribers about potential threats.

5. Clarification of incident notification parameters: The EECC clarifies the impact criteria for mandatory breach reporting, specifying the factors, such as economic and societal impact, and clarifies that reporting must be done without undue delay.

6. Collaboration with national CSIRT and authorities: The EECC requires that national telecom authorities have the power to get support from the national CSIRT, and that they collaborate with law enforcement authorities, national authorities for the NIS Directive and the data protection authorities.

7. Mitigating significant threats: National telecom authorities have the power to require providers to take measures to mitigate significant threats and to impose a time limit on the implementation of those measures (even before actual incidents occur).

3.1 MORE SERVICES IN SCOPE

Under the EECC, more communication services are in scope, particularly the so-called Over-The-Top (OTT) communications services, such as Gmail, WhatsApp, and Skype. The EECC aims to protect consumers, irrespective of the chosen communication tool, focusing on the functionality (electronic communication), rather than on the underlying technology or implementation choices. Article 2 gives the definition of electronic communications services in scope:

Article 2 Definitions

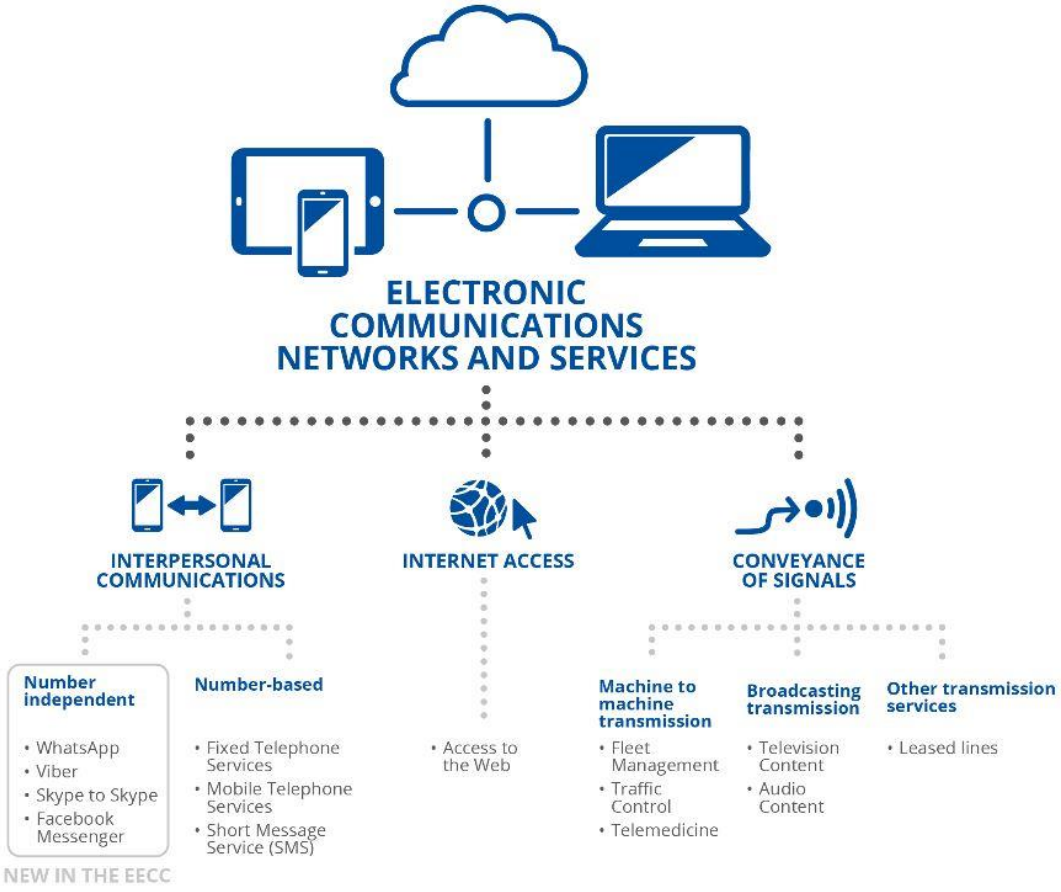
[…] (4) 'electronic communications service' means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:
(a) 'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;

(b) interpersonal communications service; and

(c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;

This means that under the EECC there are three main service categories. The picture below shows examples of services for the sake of explanation. Especially for the new services in scope, we show some examples of the most popular OTT communications services.

Figure 1: Examples of services in scope



Note that some applications or software can offer functionality in terms of services, which may fall under different categories. This is the case when the application/software offers number independent interpersonal communication and a functionality, which enables communication with numbers in national or international numbering plans.

Under the old rules: *The EU telecom rules currently in place normally cover traditional telecommunications like the Public Switched Telephone Network (fixed or mobile), SMS, fixed and mobile internet connections, broadcasting platforms (like television, or satellite), and the email services offered by telecom providers[6].*

3.1.1 Interpersonal communications services

An important new term introduced by the EECC is "interpersonal communications service". This category includes all services that allow direct and interactive communications between a finite number of persons, determined by the sender of the communication. See preamble 17.

> *(17) Interpersonal communications services are services that enable interpersonal and interactive exchange of information, covering services like traditional voice calls between two individuals but also all types of emails, messaging services, or group chats. Interpersonal communications services only cover communications between a finite, that is to say not potentially unlimited, number of natural persons, which is determined by the sender of the communication.*

This definition excludes services like linear broadcasting, video on demand, websites, social networks, blogs, exchange of information between machines, etc.

Note that some of the interpersonal communications services were already in scope under the old rules like for example mobile telephony or SMS.

3.1.2 Number independent interpersonal communications services

Interpersonal communications are sub-divided into "number-based" interpersonal communication services, i.e. services, which connect to the public switched telephone network, and "number-independent" interpersonal communication services, which do not connect to the public switched telephone network and do not use conventional telephone numbering. The number dependent interpersonal communications services are well known: mobile telephony, fixed telephony, SMS, VOIP, etc.

The number independent interpersonal communications services, which are often referred to as "Over-The-Top" (OTT) communications services, are services like Viber, WhatsApp, Slack, Gmail, Outlook, Skype-to-Skype etc., which are provided over internet connections, on top of more traditional networks. The OTT communications services are new in scope and this means that competent authorities will be supervising a new group of providers. Often, they are multinational companies, providing communication services in multiple countries or even across the globe.

The most popular OTT communications services operate globally and have hundreds of millions of subscribers, sometimes billions of subscribers across the globe. Note that the use of a mobile phone number for authentication or as identifier does not make an interpersonal communications service 'number-based'. A good example is WhatsApp, which uses mobile phone numbers as identifiers but does not connect with publicly assigned numbering resources for the communication itself. This is clarified in recital 18.

> *(18) […] The mere use of a number as an identifier should not be considered to be equivalent to the use of a number to connect with publicly assigned numbers and should therefore, in*

6The ECJ jurisprudence has clarified what constitutes an electronic communications service. See case C-142/18 Skype Communications Sarl v IBPT.

itself, not be considered to be sufficient to qualify a service as a number-based interpersonal communications service.

Note that many websites offer end-users some kind of an interpersonal and interactive communication functionality. The EECC makes an exception if the functionality is 'minor' and 'purely ancillary', and that it cannot be used without the principal service, and that it is in reality, barely used by the end-user.

3.1.3 Supervision regime for over-the-top services

In general, the security provisions in the EECC for number-based and number-independent interpersonal communications services are the same. Both are subject to (normal) ex-ante, supervision, and are required to provide information, submit to security audits and be subjected to investigation of non-compliance by the competent authorities. This is similar to the security supervision regime in the NIS Directive for the Operators of Essential Services (OES) [7].

However, there are some exceptions for the OTT communications services. The EECC outlines that, because these providers of OTT communications service do not exercise actual control over the transmission networks, there may be fewer risks for these providers, and certain security measures may not be needed, if justified on the basis of a risk assessment. See recital 95.

(95) […] independent inter personal communications services, […] are also subject to appropriate security requirements in accordance with their specific nature and economic importance. Providers of such services should thus also ensure a level of security appropriate to the risk posed. Given that providers of number -independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. Therefore, where justified on the basis of the actual assessment of the security risks involved, the measures taken by providers of number-independent interpersonal communications services should be lighter. […]

The EECC also exempts providers of number independent interpersonal communication services from the 'general authorisation' requirement, and possible related notification requirements at Member States level.

3.1.4 Emergency access via over-the-top services

Under the EECC the number based interpersonal communications services should provide the end-user access to emergency services, beyond just the traditional voice communication services. See recital 20

(20): Technical developments make it possible for end-users to access emergency services not only by voice calls but also by other interpersonal communications services. The concept of emergency communication should therefore cover all interpersonal communications services that allow such emergency services access.

For citizens, access to emergency services is an important function of communication networks and services. Access to emergency services is an important factor when assessing the significance of security incidents, and such outages can have a significant impact on economy, society, increase risks for public safety, potentially putting lives at stake.

[7] The supervision regime in the NIS Directive for Digital Service Providers (DSPs) on the other hand is 'light-touch' (ex-post supervision only).

3.2 DEFINITION OF SECURITY AND SECURITY INCIDENTS

The EECC provides a definition of security, clarifying for example that it includes also aspects like the confidentiality, authenticity, integrity and availability of communications.

Article 2 Definitions

(21) 'security of networks and services' means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services;

The definitions in the EECC clarify that security measures to be taken by providers should protect not only the continuity of services, but also the confidentiality of the communications, the metadata, etc.

Under the old rules: *In the 2009 telecom rules, a definition of security was lacking in the Framework directive, which led to some discussions and divergence.*

3.2.1 Security incident definition

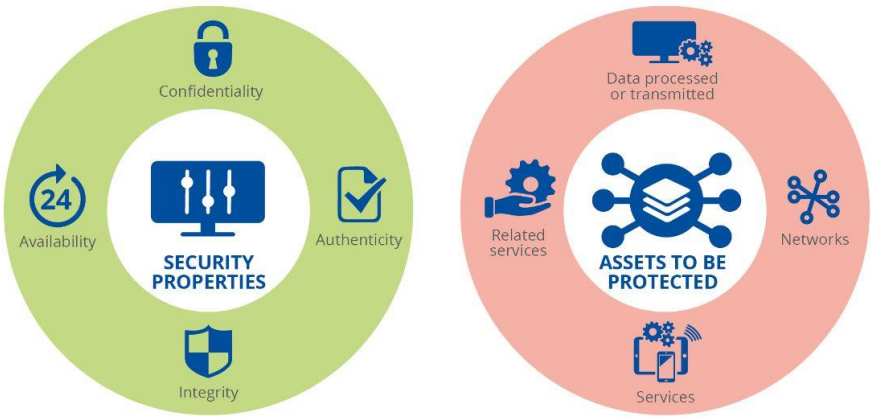
The EECC also includes a definition of a security incident, which was lacking in the 2009 telecom rules.

Article 2 Definitions

[…] *(42) 'security incident' means an event having an actual adverse effect on the security of electronic communications networks or services.*

This definition of security incident in the new rules is aligned with the definition in the NIS Directive and consistent with industry standards and good practices.

Figure 2: Security incident, properties and assets affected



This means that, considering the definition of security, security incidents can include not only network outages but also other types of incidents, like for example breaches of the confidentiality of communications.

Events, which reduce the redundancy of a network or service, such as for instance when one of two redundant submarine cables breaks, could fall under the definition of an incident because they reduce the ability of the system to protect itself.

Newly discovered security vulnerabilities (like, for example, Heartbleed) may become security incidents, if there is an actual effect on the security of the networks and services. It does *not* mean that all such vulnerabilities fall under mandatory breach reporting, which requires there to be a significant impact on the networks or services.

Under the old rules: *In the 2009 telecom rules, a precise definition of security incident was lacking, which led to discussions and some divergence in interpretation.*

3.2.2 Security baseline

The EECC also defines a security baseline, a set of technical and organizational security measures, which need to be taken by providers, as a minimum.

Article 40 requires providers to take appropriate security measures:

> ***Article 40 Security of networks and services***
>
> 1. *Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services.*

Recital 94 details which aspects security measures should take into account, as a minimum.

> *(94) […] Security measures should take into account, as a minimum, all the relevant aspects of the following elements: as regards security of networks and facilities: physical and environmental security, security of supply, access control to networks and integrity of networks; as regards handling of security incidents: handling procedures, security incident detection capability, security incident reporting and communication; as regards business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; as regards monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and service testing, security assessments and compliance monitoring; and compliance with international standards.*

In this way, the EECC provides a starting point for a security supervision framework

Table 1: EECC Security baseline

Measures	Description
Security of networks and facilities	• Physical and environmental security • Security of supply • Access control to networks • Integrity of networks
Handling of security incidents	• Handling procedures • Security incident detection capability • Security incident reporting and communication
Business continuity management	• Service continuity strategy and contingency plans • Disaster recovery capabilities

Monitoring, auditing and testing	• Monitoring and logging policies • Exercise contingency plans • Network and service testing • Security assessments and compliance monitoring • Compliance with international standards.

Under the old rules: *The national authorities in the Article 13a expert group agreed, in a consensus process, about a minimum set of security measures, which goes beyond the measures listed in the EECC. This Article 13a guideline covers the above-mentioned security measures enumerated in the EECC and lists 25 high-level security objectives, divided in 7 security domains[8]. For each security objective, there are examples of technical measures and possible evidence, which should be considered by national authorities when assessing compliance.*

3.3 STATE-OF-THE-ART MEASURES AND ENCRYPTION

The EECC requires that the security measures taken by providers are state-of-the-art and to include encryption, where appropriate, to mitigate the impact of security incidents on subscribers, other services, etc.

> ***Article 40 Security of networks and services***
>
> […] *Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services.*

Recital 97 clarifies that where necessary, encryption and end-to-end encryption should be mandatory and turned on by default:

> *(97)In order to safeguard security of networks and services, and without prejudice to the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences, the use of encryption for example, end-to-end where appropriate, should be promoted and, where necessary, encryption should be mandatory in accordance with the principles of security and privacy by default and by design.*

The latter provisions are in line with industry good practices. For example, a popular messaging particular and significant threat of a security incident a closer look at the security and technology behind some of these services.

3.4 PROMOTE ENCRYPTION AND INFORM ABOUT THREATS

Article 40(3) and Recitals 96 explain that it is the responsibility of the provider to inform subscribers about significant security threats and how they can protect themselves, for example by using specific software or encryption. Recital 97 mentions that end-to-end encryption should be promoted.:

> *(96) Providers […] should inform users of particular and significant security threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies. […]*

:

[8]Article 13a Technical Guideline on Security Measures
https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

(97) […] the use of encryption for example, end-to-end where appropriate, should be promoted and, where necessary, encryption should be mandatory in accordance with the principles of security and privacy by default and by design.

This is a new provision that builds on Art 4(2) ePrivacy Directive[9] but considerably amended and modernised. It expands the duty of care providers have regarding the security and privacy of their subscribers.

***Under the old rules**: The 2009 telecom rules only make it mandatory for a provider to reach out subscribers when there was an actual significant incident and if the authority mandated the provider to do so.*

3.5 CLARIFICATION OF INCIDENT NOTIFICATION PARAMETERS

The EECC specifies parameters that, where available, should be taken into account when determining the significance of a security incident and in this way puts the basis for harmonized incident reporting thresholds across the EU. In addition, the EECC clarifies that reporting must be done without undue delay.

Article 40 Security of networks and services

[…] 2. Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.
In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:

(a) the number of users affected by the security incident;

(b) the duration of the security incident;

(c) the geographical spread of the area affected by the security incident;

(d) the extent to which the functioning of the network or service is affected;

(e) the extent of impact on economic and societal activities.

The provisions about cross-border information and annual summary reporting to ENISA remain unchanged.

Where appropriate, the competent authority concerned shall inform the competent authorities in other Member States and ENISA. The competent authority concerned may inform the public or require the providers to do so, where it determines that disclosure of the security incident is in the public interest.

Once a year, the competent authority concerned shall submit a summary report to the Commission and to ENISA on the notifications received and the action taken in accordance with this paragraph.

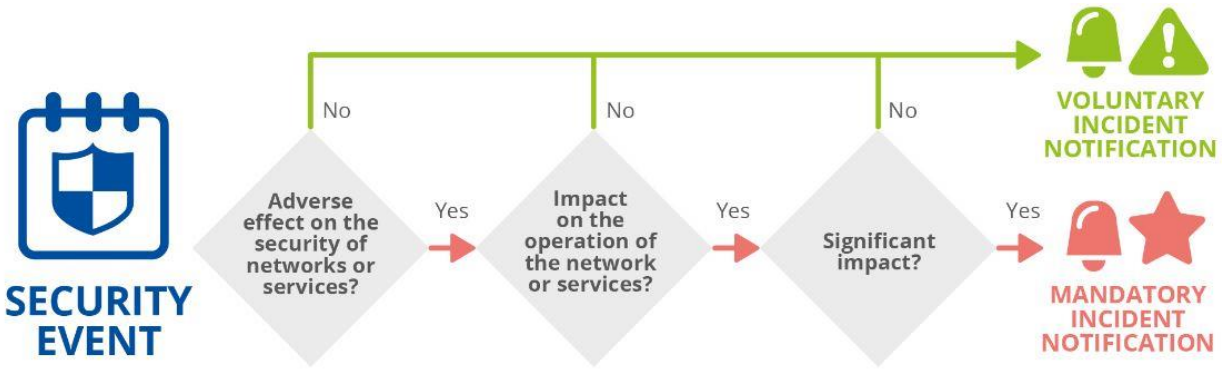
In the past, the national telecom authorities in the Article 13a group and ENISA have discussed EU-wide thresholds, in particular for an efficient and consistent implementation of annual summary reporting across the EU. The experience is that a threshold using absolute numbers of subscribers is difficult to use across the EU because of the differences in size of the EU

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN

countries. A common EU-wide threshold model should be flexible enough to work for countries of all sizes.

The EECC uses a two-step definition to determine which security incidents fall under mandatory notification. The EECC first gives a broad definition of a security incident, including a wide range of security events. The threshold for reporting is defined more strictly in terms of the impact on the *operation* of the networks and/or services.

Figure 2: EECC two-step definition for incident mandatory notification



Under the old rules: *Previously the legislation did not list detailed criteria to consider when an incident should be considered significant. Each country also derived their own national thresholds. The Article 13a expert group did reach agreement about thresholds for EU-wide annual summary reporting. For the sake of reference, we report these EU-wide annual summary thresholds (see also the Article 13a guideline on incident reporting[10]):*

- duration more than an hour, and the percentage of users affected is more than 15%,
- duration more than 2 hours, and the percentage of users affected is more than 10%,
- duration more than 4 hours, and the percentage of users affected is more than 5%,
- duration more 6 hours, and the percentage of users affected is more than 2%, or if it
- duration more than 8 hours, and the percentage of users affected is more than 1%.
- or the product of duration and number of users exceeds 1 million user hours

3.6 COLLABORATION WITH NATIONAL CSIRT AND AUTHORITIES

The EECC in Article 41 asks member states to give the national competent authorities the power to get assistance from national CSIRTs and requires them to consult and cooperate with other national authorities, like law enforcement, authorities for the NIS Directive, and data protection authorities.

Article 41 Implementation and enforcement

[…] 4. Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to obtain the assistance of a Computer Security Incident Response Team ('CSIRT') designated pursuant to Article 9 of Directive (EU) 2016/1148 in relation to issues falling within the tasks of the CSIRTs pursuant to point 2 of Annex I to that Directive.

5. The competent authorities shall, where appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities, the competent

[10] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

authorities within the meaning of Article 8(1) of Directive (EU) 2016/1148 and the national data protection authorities.

Under the old rules: *Under the old rules there was no such provision. Nevertheless, in most countries there is close collaboration between the competent authorities for telecommunications, national cybersecurity agencies, and national CSIRTs.*

3.7 MITIGATING SIGNIFICANT THREATS

Under Article 41 of the EECC national telecom authorities shall have the power to require providers to mitigate significant threats and to impose that measures should be taken within a time limit (even before actual incidents occur). Article 41 defines the supervision powers of national competent authorities:

Article 41 Implementation and enforcement

1. Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to issue binding instructions, including those regarding the measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and time-limits for implementation, to providers of public electronic communications networks or publicly available electronic communications services.

2. Member States shall ensure that competent authorities have the power to require providers of public electronic communications networks or publicly available electronic communications services to:

(a) provide information needed to assess the security of their networks and services, including documented security policies; and

(b) submit to a security audit carried out by a qualified independent body or a competent authority and make the results thereof available to the competent authority; the cost of the audit shall be paid by the provider.

Most of this is similar to the old rules. It describes 'normal' preventive, ex-ante supervision. Part 1) however contains an additional provision regarding significant threats and measures to mitigate those threats, to prevent incidents from occurring. This part (Article 41(1)) enhances clarity regarding the binding instructions competent authorities can give.

Under the old rules: *Under the old rules, Article 13b of the Framework directive stipulated the supervision powers of competent authorities. In the EECC it is clearly specified that already a significant threat is enough basis for the competent authority to instruct providers to take mitigating measures. In the past, in some countries the authorities only had the power to request information after a suspicion or a reason for such information requests or audits, for example when presented with evidence of an incident or evidence of non-compliance.*

4. CONCLUSIONS AND OUTLOOK

Security supervision under the new rules, the EECC, is in its principles similar to the security supervision under the old rules. However, there are several changes, which adapt, extend or clarify the old rules. Therefore, once the EECC is transposed into national legislation, the national competent authorities, i.e. those national authorities who will be assigned the relevant competences (for Article 40 and Article 41 of the EECC), as well as ENISA, will have to adapt the current guidelines, procedures and tools.

We see three key areas where work is needed. In each area, we outline potential next steps for the coming 2-3 years:

ENISA and national competent authorities will work together to adapt the current guidelines, procedures and tools.

1. **Review and update the existing security measures framework:** The EECC clarifies the security requirements and requires state of the art measures and encryption where needed. National authorities will need to develop a new security framework for assessing the conformity of providers with the new rules. ENISA, with the support of the Article 13a Expert Group, aims to review the current Technical Guidelines for Security Measures and start the process of extending the guidelines to align with the EECC.

2. **Develop harmonized reporting thresholds and a new incident reporting guideline**: ENISA will work with the national authorities to develop a harmonized reporting approach by defining the parameters for measuring the impact of an incident and the thresholds for the reporting. This work will be based on the current technical guidelines but it will go further to cover not only outages, but also all kind of security incidents and the various aspects of their impact (economical, societal etc). The aim is to agree on thresholds that will take into consideration the size, the population and the specific characteristics of every country.

3. **Develop a cross-border approach to security supervision:** The supervision of the OTT providers brings new challenges to the national authorities. Incidents affecting the OTT communications services will be mostly cross-border and collaboration between the Competent Authorities will be required to allow for effective and efficient supervision. ENISA will focus on helping the Competent Authorities to agree on cross-border collaboration procedures for supervision. Communication with other similar groups such as the NISD DSPs group will help to learn more about supervising (multinationals with global services) across borders.

In parallel, ENISA has started the work of rebuilding the CIRAS reporting tool, which is used for annual summary reporting as well as cross-border information about incidents between national authorities, to make it fit for the EECC. The work should be ready in the next months, in time for the next round of annual summary reporting. Currently CIRAS contains around 1000 incident reports, which are publicly accessible, going back to 2012 when annual summary reporting started in earnest[11].

In this period of transposition of the new rules, it is important to share good practices and collaborate with other national authorities in other EU countries, to avoid unnecessary divergence. As stipulated in the EECC, ENISA will support the EU countries to ensure there is a

[11] There is a publicly available visual frontend which can be used for a custom analysis of all the past telecom security incidents https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/visual-tool

harmonized approach, where possible. This work will start as in earnest when the EECC competences for Article 40 have been assigned.

We look back at a decade of successful collaboration with the national authorities on the implementation of Article 13a, in the Article 13a group, and we look forward to continue working with the member states, national authorities and the private sector, towards an efficient and effective implementation of the new EECC.

TP-02-19-765-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-304-9
DOI: 10.2824/ 647924