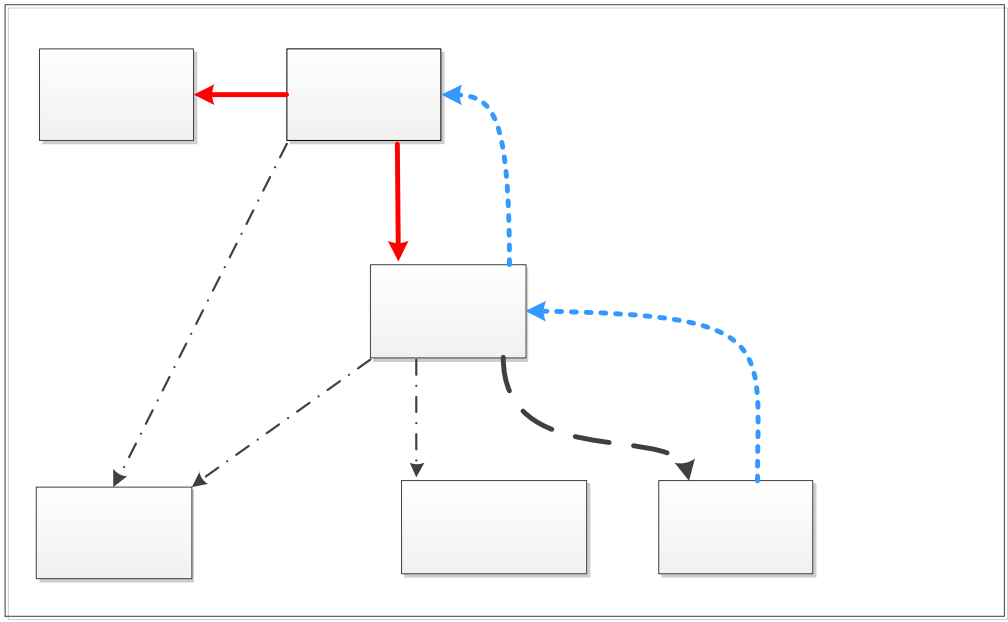

Cyber Incident Reporting in the EU

An overview of security articles in EU legislation

August 2012

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Marnix Dekker, Christoffer Karsberg, Barbara Daskala

Contact

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

1 Introduction

Reliable and secure internet and electronic communications are now central to the whole economy and society in general. Cyber security incidents can have a large impact on individual users, on the economy and society in general. We give five examples:

1. *In June 2012 6.5 million (SHA-1) hashed passwords of a large business-focussed social network appeared on public hacker forums. The impact of the breach is not fully known, but millions of users were urged to change their passwords and their personal data could be at risk.*
2. *In December 2011, the storm Dagmar affected power supplies to electronic communication networks in Norway, Sweden and Finland. As a result millions of users were without telephony or internet for up to two weeks.*
3. *In October 2011 there was a failure in the UK datacentre of a large smartphone vendor. As a result millions of users across the EU and globally could not send or receive emails, which severely affected the financial sector.*
4. *Over the summer 2011, a Dutch certificate authority experienced a security breach, allowing attackers to generate fake PKI certificates. The fake certificates, the result of the breach, were used to wiretap the online communications of around half a million Iranian citizens. Following the breach many Dutch e-government websites were offline or declared unsafe to visit.*
5. *In April 2010 a Chinese telecom provider hijacked 15% of the world's internet traffic through Chinese servers for 20 minutes, routing traffic to some large e-commerce sites, such as www.amazon.de and www.dell.com as well as the .mil and .gov domains, et cetera. As a result, the internet communications of millions of users were exposed (to eavesdropping).*

The large outages and large data breaches receive extensive media coverage, showing the importance of cyber security in society. Many breaches, however, remain undetected and if detected, are not reported to authorities and not known to the public. There is no overall view across the digital society of the incidents, the root causes or the impact for users.

Lack of transparency and lack of information about incidents makes it difficult for policy makers to understand the overall impact, the root causes and possible interdependencies. It also complicates the efforts in the industry to understand and address cyber security incidents. And finally, it leaves customers in the dark about the frequency and impact of cyber incidents.

Legislation can play an important role here. For some types of incidents[1], there is now an EU directive, which has been transposed in national laws obliging providers to report incidents to a national authority. In this paper we give an overview of different articles of EU legislation on cyber security incident reporting and prevention and we show how they are related. We conclude with some general remarks about incident reporting across the European digital society.

[1] *These are currently the security breaches and personal data breaches which occur related to the provision of public electronic communications networks and services. Public electronic communication networks and services are networks and services which offer or facilitate electronic communications to the public. Examples are fixed telephony, mobile telephony and internet access to the general public. Internal company networks, for example, are not in the scope of this legislation.*

2 Security articles in EU legislation

In recent years a number of EU Member States recognized the need for preventing cyber security incidents and they had started up, for example, voluntary or mandatory incident reporting schemes to create more transparency about cyber security incidents. In these countries often the focus was on the vital infrastructure for the digital society; the electronic communication networks and services.

Not all EU countries adopted legislation on security measures and incident reporting and there were big differences between the different national approaches. This had two main disadvantages:

- Cyber security incidents in one country may well have an impact across national borders. The Diginotar incident shows how national incidents can have a cross-border impact. This means that to improve security across the EU, all countries should agree on common principles.
- Furthermore, service providers often operate across EU countries, especially telecom companies and internet service providers. It is cumbersome for these providers to have to adapt their systems to different national requirements. A harmonized legislation across the EU avoids digital borders and allows for a level-playing field for providers across the EU market.

To address these issues, the EU countries, through the European commission (EC), have been working together on common EU wide legislation with the objective to have consistency and harmonization across the EU. In the following paragraphs we go over existing and proposed EU legislation on security measures, breach notification and incident reporting.

2.1 Article 13a of the Framework directive: *"Security and Integrity"*

The Telecoms reform passed into law in 2009, adds Article 13a to the Framework directive, regarding security and integrity of public electronic communication networks and services. Article 13a states:

- Providers of public communication networks and services should take measures to guarantee security and integrity (i.e. availability) of their networks.
- Providers must report to competent national authorities about significant security breaches.
- National authorities should inform ENISA and authorities abroad when necessary, for example in case of incidents with impact across borders.
- National authorities should report to ENISA and the EC about the incident reports annually.

Article 13a also says that the EC may issue more detailed implementation requirements if needed, taking into account ENISA's opinion.

The EC, ENISA, and the national regulators have been collaborating for the past 2 years to implement Article 13a and to agree on a single set of security measures for the European electronic communications sector and a modality for reporting about security breaches in the electronic communications sector to authorities abroad, to ENISA and the EC.

In May 2012 ENISA received the first set of annual reports from Member States, concerning incident that occurred in 2011. ENISA received 51 incident reports about large incidents, which exceeded an agreed impact threshold. The reports describe services affected, number of users affected, duration, root causes, actions taken and lessons learnt. While nationally incident reporting is implemented differently, with different procedures, thresholds, et cetera, nearly all national regulators use a common procedure, a common template and common thresholds for reporting to the EC and ENISA.

Despite the fact that this first set of incident reports is incomplete, as some countries had not yet fully implemented national incident reporting schemes, these reports already provide valuable insights into the types of threats facing the European electronic communications sector. The information from the incident reports is used, for example, as input to the European Cyber Security Strategy and the pan-European Cyber Security exercises. ENISA will publish a summary of the received annual incident reports in September 2012, and from spring 2013 annually.

2.2 Article 4 of the e-Privacy directive: *"Security of processing"*

The Telecoms reform also changed the e-Privacy Directive, which addresses data protection and privacy related to the provision of public electronic communication networks or services. Article 4 of the e-Privacy directive requires providers to notify personal data breaches to the competent authority[3] and subscribers concerned, without undue delay. The obligations for providers are:

- to take appropriate technical and organisational measures to ensure security of services,
- to notify personal data breaches to the competent national authority,
- to notify data breaches to the subscribers or individuals concerned, when the personal data breach is likely to adversely affect their privacy, and
- to keep an inventory of personal data breaches, including the facts surrounding the breaches, the impact and the remedial actions taken.

Article 4 also says that the EC may issue technical implementing measures regarding the notification formats and procedures, in consultation with the Article 29 Working Party, the European Data Protection Supervisor (EDPS) and ENISA.

In 2011, ENISA started an expert group, including experts from national data protection authorities, industry, and EDPS, to draft recommendations for the technical implementation of Article 4.

2.3 Articles 30, 31 and 32 of the Data Protection regulation

The EC has proposed to reform the current European data protection framework (Directive 95/46/EC), and has proposed an EU regulation on data protection. The regulation regards organisations that are processing personal data, regardless of the business sector the organisation is in. Security measures and personal data breach notifications are addressed in Articles 30, 31 and 32:

- Organisations processing personal data must take appropriate technical and organisational security measures to ensure security appropriate to the risks presented by the processing.
- For all business sectors the obligation to notify personal data breaches becomes mandatory[4].
- Personal data breaches must be notified to a competent national authority without undue delay and, where feasible, within 24 hours, or else a justification should be provided.

[3] *In a number of countries, the competent body for notification about personal data breaches related to electronic communications networks and services is not the telecom regulator, but a data protection authority or other agency.*

[4] *This provision extends personal data breach notifications beyond the electronic communications sector.*

- Personal data breaches must be notified to individuals if it is likely there will be an impact on their privacy. If the breached data was unintelligible[5], notification is not required.

2.4 Article 15 of the e-Sig and e-ID regulation: "*Security requirements*"

The EC recently released a proposal for a regulation on electronic identification and trust services[6] for electronic transactions in the internal market.. Article 15 in this proposal introduces obligations concerning security measures and incident reporting:

- Trust service providers must implement appropriate technical and organisational measures for the security of their activities.
- Trust service providers must notify competent supervisory bodies and other relevant authorities of any security breaches and where appropriate, national supervisory bodies must inform supervisory bodies in other EU countries and ENISA about security breaches.
- The supervisory body may, directly or via the service provider concerned, inform the public.
- The supervisory body sends a summary of breaches to ENISA and the EC.

Article 15 is similar to Article 13a of the Framework directive (see References).

2.5 EU Cyber Security Strategy

The European Commission is developing a European Cyber Security Strategy. The roadmap for the strategy refers to Article 13a and mentions extending Article 13a to other business sectors. The Commission has indicated that there will be five main strands:

- Capabilities and response networks, for sharing information with public and private sector
- Governance structure including the national competent authorities, to address incidents and develop an EU contingency plan.
- Incident reporting for critical sectors like energy, water, finance and transport.
- Pre-commercial procurement of security technology and public-private partnerships to improve security across the single market
- Global cooperation, to address global interdependencies and the global supply chain.

A European Cyber Security Strategy is an important step to increase transparency about incidents, and ultimately to prevent them or limit their impact.

[5] *In the recommendation for the technical implementation of Article 4, unintelligible data is described as data that has either been encrypted (asymmetric or symmetric), or hashed.*

[6] *Trust service means any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.*

3 A model of security articles

In this section we show the overall picture of the different security articles discussed in Section 2.

3.1 General model

The diagram in Figure 1 shows the actions of the actors as described in the different security articles. In particular it shows the issuing of security measures to prevent breaches, as well as the reports about breaches.

We stress that this overall picture is not an exact description of the individual security articles, but intended as an overall view. We refer the reader to Section 3.2 for details about what is different across the different articles.

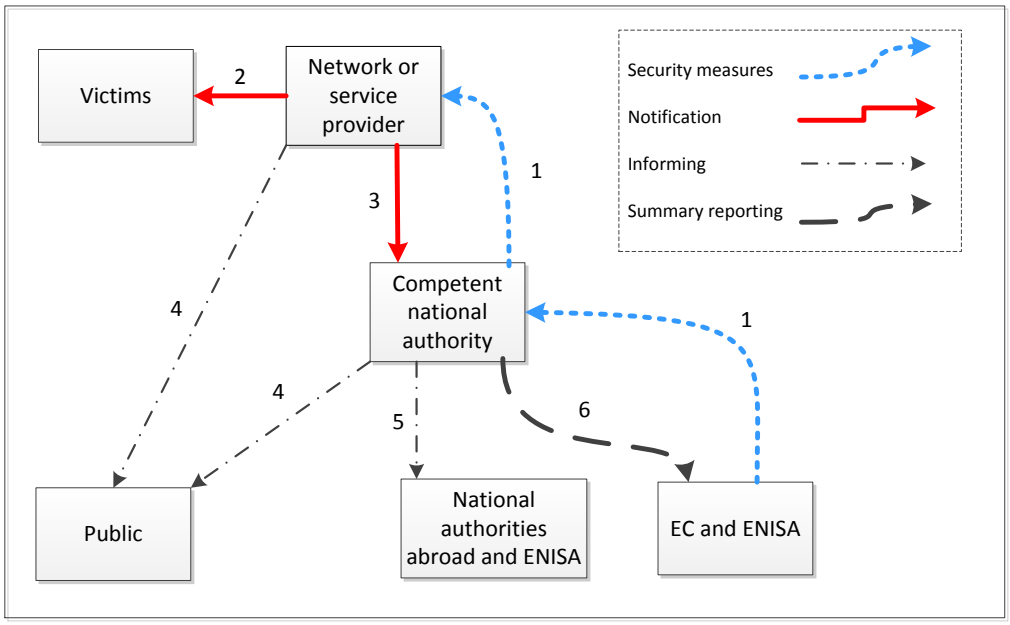

Figure 1: Overall view of actions and information flows

A simplification in this diagram is that we describe only one single national authority collecting breach notifications and incident reports. In practice multiple national authorities may be involved when dealing with security and privacy breaches. It is at the discretion of national governments to assign tasks to competent government bodies, depending on national circumstances. For example, in some countries security and privacy breaches regarding electronic communication services are all dealt with by the national telecom regulator acting as a single point of contact for the electronic communications sector. In other countries, the privacy breaches are reported separately to the data protection authorities, or to a national cyber security centre.

We go over the numbered arrows in the diagram, step by step:

1. *(blue dotted arrows) National authorities require providers to take appropriate technical and organisational security measures, taking into account the state of the art in security technology. To ensure that these security measures are taken, national authorities may audit providers, or ask them to do a self-assessment or undergo an audit. This step can be seen as one of the main objectives of this legislation, to ensure that appropriate measures are being taken, across the EU*[7].

At some point in time an incident is detected at a network or service provider. The incident may be a security breach, a personal data breach or both (e.g. a security breach resulting in a personal data breach). The provider starts to respond to the incident and if needed, the provider should contact technical experts or national computer emergency response teams (CERTs) to address the incident[8].

2. *(red arrow) The provider notifies users affected by the breach (victims)*
3. *(red arrow) The provider notifies competent national authorities about the breach. An initial quick notification is followed by more detailed incident reports at a later stage, containing impact analysis, root causes, actions taken, lessons learnt, et cetera.*
4. *(black dash-dotted arrow) When necessary the national authority informs the public. Alternatively, depending on the situation, the national authority may require the provider to inform the public.*
5. *(black dash-dotted arrow) Additionally, when relevant, the national authority informs authorities abroad and ENISA. For example, in case a breach has a cross-border impact.*
6. *(black dashed arrow) Later, on an annual basis, the national authority sends a summary report of the significant incidents to ENISA and the EC. The annual reporting gives feedback at an EU level about the effectiveness of EU legislation, to understand EU wide trends, and to provide a platform for discussing lessons learnt and agreement about a harmonized and consistent approach to improving cyber security across the EU.*

Finally, returning to the blue dotted arrows (1), past incidents, root causes, lessons learnt ex-post, are being discussed nationally and at an EU level, and the security measures are being adapted to improve the security of the networks and services.

[7] *Technical and organisational security measures are an important aspect in all the legislation discussed in Section 2*

[8] *Although out of scope of this paper, CERTs are crucial capabilities to be able to limit the impact of cyber security incidents and a key activity of ENISA is to support EU countries in setting up well-functioning CERTs and to foster collaboration and information sharing between the different CERTs.*

3.2 Commonalities and differences

The overall picture provided in Section 3.1 ignores some differences between the security articles. In the diagram below (Figure 2) we illustrate the commonalities and differences between the different security articles, by annotating the information flows with references to individual articles.

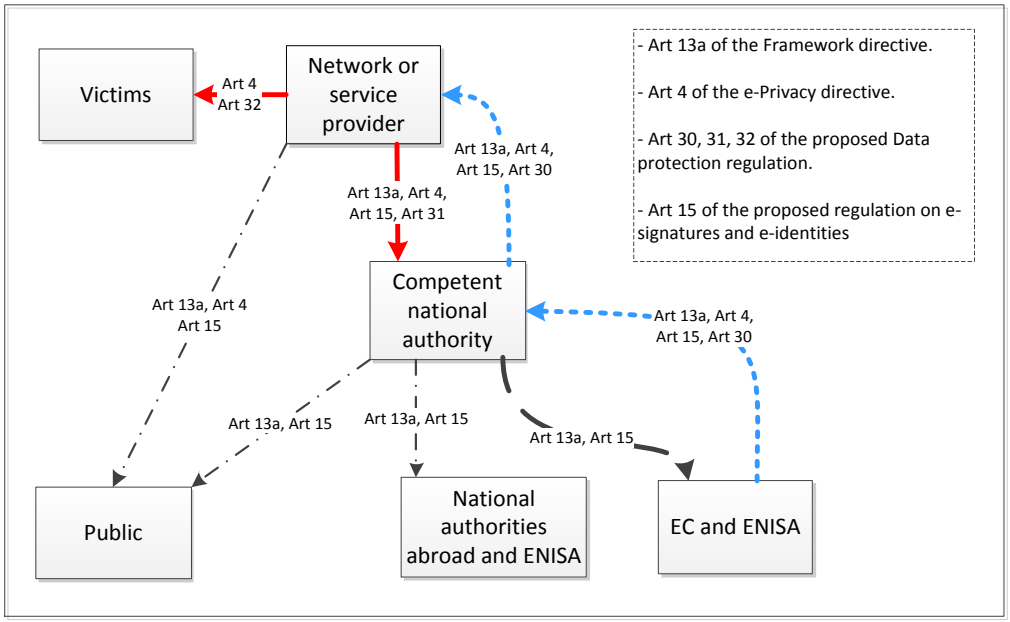

Figure 2: Commonalities and differences between the security articles

4 Conclusions

Security measures and incident reporting, implemented across the EU's digital society, are important to improve overall security. EU legislation plays an important role here as it allows harmonization across the EU member states. This in turn prevents weak links and unnecessary costs for providers operating cross-border. The European Commission, in collaboration with the EU Member States, has undertaken a number of legislative initiatives aiming to further improve transparency about incidents. Another important step is the proposed Cyber Security Strategy, which emphasizes incident reporting and the importance of exchange across the EU about incidents and how to address them. We conclude with some general remarks.

- **Regulatory gaps**: In the introduction we gave five examples of cyber incidents with a severe impact on the security or privacy of electronic communications. The 2nd incident, caused by the Dagmar storm, is in scope of existing incident reporting legislation and as such reported to authorities[9]. The proposed regulation on electronic trust providers would also cover the 4th incident[10]. But the remaining incidents (the 1st, 3rd, and 5th) are not clearly in scope or subject of debate between providers and the national regulator. It is important that national authorities and the EC discuss, agree, and clarify the scope of legislation on electronic communications and address these and other gaps. This can be done without necessarily changing the text of existing legislation, such as the telecom regulatory framework, but rather the interpretation of what the services are, because the landscape of electronic communications is continuously changing (from landline telephones and minitel in the past, to mobile phones, internet and VoIP).

- **Model security articles:** There is a lot of similarity between Article 13a of the Framework directive and Article 15 of the e-Signatures and e-Identities regulation. The former has been taken as a model for drafting the latter. Both articles combine security measures and incident reporting, at a national level and at an EU level. Consistency and standardization in the legislative texts allows for more easy governance by the member states, and more easy implementation by the providers. Furthermore, the combination of national reporting and EU reporting (present in both Article 13a and Article 15) allows national authorities room to adjust to national circumstances, while at the same time providing overview and feedback at an EU level, which allows Member States to optimize implementation and to ensure a harmonized approach across EU member states.

- **Governing security measures:** Mandatory breach reporting receives a lot of media attention and it is arguably the most visible part of the security articles discussed in Section 2. But the

[9] *The Dagmar storm caused power cuts which led to large outages which fall under Article 13a: To be precise in the article this would be called a breach of integrity of the networks affecting the continuity of supply of electronic communication services over these networks. The EC and ENISA received summary incident reports from three countries as part of Article 13a's annual incident reporting to ENISA and the EC.*

[10] *The Diginotar incident was a security breach at a Certificate Authority which would fall under the proposed Article 15.*

ultimate goal is to limit the impact of security and personal data breaches or prevent them altogether by making sure appropriate security measures are taken. This type of governance is crucial and not easy. In security much depends on the technical details of the implementation and these details are hard to capture in (high-level) legislation and subject to change. National authorities should exchange knowledge about an effective and efficient combination of high-level legal obligations and technical implementation requirements. For the latter it is important to adopt a bottom up approach (i.e. commonly agreed recommendations), taking into account the (changing) state of the art and the practical experiences of regulators and experts from the private sector.

As a second, but related point, the need to take "appropriate technical and organisational security measures" is mentioned in all the security articles discussed in Section 2. Although these articles are aimed at different providers and different types of breaches, there is still a large overlap[11] between the security measures that have to be taken. The competent national authorities should collaborate (nationally and at an EU level) to ensure that these security measures are implemented consistently and where there is an overlap, similarly, to allow providers to comply more easily, and to allow equipment vendors to adapt their products accordingly[12].

- **Optimizing incident reporting procedures:**
  - **Incident response versus incident reporting**: To prevent incidents from escalating Member states should encourage providers to quickly contact technical experts, incident response teams (like national CERTs), crisis coordination groups, and other organizations relevant in the response phase, should this be necessary. Member states should underline that incident response receives priority. The purpose of mandatory incident reporting to national authorities is supervision over whether or not providers comply with legal requirements, while the purpose of information exchange in the response phase, for example with a national CERT, is to tackle the incident. Member states should encourage transparency and trusted information sharing in the response phase and ensure that response processes are independent and not slowed down by legal reporting requirements. Member states should for instance ensure that incident reporting procedures are easy and quick to apply. [13].
  - **Exchange and sharing:** Over the past years CERTs have developed effective platforms for collaboration and information exchange. Beyond the response phase, however,

[11] *To give a simple example, access control to databases is an important measure under both Article 13a and 4.*

[12] *ENISA will address synchronization of Article 13a and Article 4 security measures, in collaboration with the national authorities, as part of ENISA's 2013 work program.*

[13] *For example by adopting a two-staged approach, where brief reports with impact estimates are sent within hours, while longer reports with exact figures are sent days after the incidents have been resolved.*

there is still little exchange of information about breaches between different national authorities. The EC should continue to support the working groups and platforms for exchanging information between national authorities, about breaches, about lessons learnt and best practices.

- **Granularity and tools**: An important aspect of the evaluation of existing legislation on incident reporting should be an analysis of costs and benefits. Both for national and EU level reporting it is important to review over time the thresholds for reporting, the type of information that is reported, the level of detail, and so on. If too few incidents are reported, then it will be difficult to draw meaningful conclusions about common root causes or trends. This would defeat the purpose of the legislation altogether and make the legislation cost ineffective. National authorities should analyse what is a good balance, taking into account the costs and benefits for providers as well as the national authorities. Providers and national authorities should investigate automated tools and computer interfaces to allow for cost-effective incident reporting at a sufficient level of detail, while avoiding the burden of manual and ad-hoc reporting procedures[14]. For example, one could distinguish between small and large incidents and use less reporting detail for the (many) smaller incidents.

For the sake of brevity we refrain from discussing a number of other related issues (including for example, common data models for incident reports, common impact assessment methods, severity classification of breaches, common risk assessment methods, et cetera), which are already being addressed in the different working groups for Article 13a and Article 4.

Concluding we would like to remark that in recent years a lot of progress has been made, in terms of addressing incidents and increasing transparency about incidents. The national authorities, for example, recently submitted to ENISA and the EC, the first Article 13a incident reports regarding severe incidents that occurred in 2011. The vast majority of national authorities use a single set of security measures and a common reporting template allowing for efficient collection and analysis. ENISA will publish an analysis of the 51 severe incidents in September 2012. From next year, every spring ENISA will collect annual incident reports and publish an analysis of the incidents of the previous year. For example, next spring 2013 ENISA will publish an analysis of the 2012 incidents.

We look forward to continuing our work with national authorities and the European Commission to support an efficient and effective implementation of Article 13a, Article 4, and the other security articles across the single digital market, and to support collaboration and information exchange between national authorities across the EU, to improve security across the EU's digital society.

[14] *In the context of Article 13a a number of countries are developing online reporting tools with interfaces to incident response systems of providers, and also ENISA is developing an automated tool for EU-level reporting which provides important functionality for national regulators.*

5 References

5.1 EU legislation and proposals

- Article 13a of the Framework directive of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf
- Article 4 of the e-Privacy directive, part of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/24eprivacy.pdf
- The electronic communications regulatory framework (incorporating the telecom reform): http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf
- Article 15 of the Regulation on electronic identification and trust services for electronic transactions in the internal market: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm
- Article 30, 31 and 32 of the proposed Data Protection regulation: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf The regulation is part of a wider reform of the data protection framework: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- Roadmap for a proposal on a European strategy for internet security: http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf
- The speech of EU Commissioner Neelie Kroes on the EU strategy for internet security: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204&format=HTML&aged=0&language=EN&guiLanguage=en
- The speech of EU Commissioner Cecilia Malmström on the EU Cyber security strategy: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/315

5.2 Related ENISA publications

- ENISA's Article 13a Guidelines on Incident reporting and Minimum security measures
- ENISA's Recommendations for the technical implementation of Article 4
- ENISA's 2009 paper on incident reporting shows an overview of the situation 3 years ago
- ENISA's 2011 paper on data breach reporting across the EU shows an overview of the different national approaches to personal data breach notifications.
- ENISA's paper on National Cyber Security Strategies shows commonalities and differences between national cyber security strategies across the EU.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu