



Securing data in cyber space

March 2014





Table of Contents

1.1	ENISA comments following large-scale data compromise activity	1
1.2	Emerging cybersecurity trends	1
2.	Cloud Computing and privacy	3
3.	Cryptography	4
4.	Data Breach Notification Schemes	4
5.	Cloud computing and EU policy.....	5



About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the European Union, 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

Udo Helmbrecht, Steve Purser, Evangelos Ouzounis, Demosthenes Ikononou, Louis Marinos, Andreas Sfakianakis, Dimitra Liveri and Marnix Dekker.

Contact

For contacting the authors, please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2014

Reproduction is authorised provided the source is acknowledged.

Securing data in cyber space

1.1 ENISA comments following large-scale data compromise activity

As specified in its mandate, “(ENISA) shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet ... requirements of network and information security ... thus contributing to the proper functioning of the internal market”¹.

In this paper, ENISA states its position with regard to recent discussions on the relationship between cybersecurity and data compromise. That ENISA should comment on these discussions is a consequence of the fact that they refer to potential “.. unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems”². Such discussions clearly have an affect on the internal market: they cast doubt on the trustworthiness of digital services and products, such as services related to Cloud computing, and in particular, privacy^{3,4}.

Commenting on the implications of disruptive actions, European Commission Vice President, Commissioner Neelie Kroes said, “If businesses or governments think they might be spied on, they will have less reason to trust the Cloud, and it will be Cloud providers who ultimately miss out.”⁵

Fuelled by the regular headlines on state data surveillance, a very serious debate is taking place in the areas of cybersecurity, data protection and privacy. This debate is necessary to reinforce trust in protection measures, understand the trade-offs between security and privacy, and thus maintain the level of confidence in the relevant services and products. As network and information security (NIS) and digital surveillance have diametrically opposed objectives, these developments have obvious consequences for cybersecurity: many voices refer to the failure in protecting data in cyber space, while others, for example, security experts, see it as proof of a long known threat. Regardless of the view taken, it is a fact that the cybersecurity community needs to digest these revelations and reassess their purpose and scope. All this is of paramount importance to the European Union and is being followed closely by EU bodies. These include the Commission, the Fundamental Rights Agency (FRA), Europol, the European Union Institute for Security Studies (EUISS) and the European Defence Agency (EDA), each looking from their particular viewpoints. ENISA is following these developments carefully with a view to supporting the Commission and the Member States in implementing suitable counter-measures to these evolving threats.

1.2 Emerging cybersecurity trends

Within its activities related to the identification of emerging trends in cybersecurity⁶, ENISA has identified the following developments that have partly materialised or are expected to materialise in the short term. These trends are related to threats, risks and impacts following the revelation of massive state digital surveillance activities, and are based on information published in the media.

¹ REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 21st May 2013, Art. 1, 1.

² REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 21st May 2013, Art. 1.3

³ http://www.afr.com/p/technology/us_surveillance_threatens_confidence_bIQTKSP3qAKwQLsrDCeMYJ, accessed 27 July 2013.

⁴ <http://www.it-business.de/cloud-computing/weiteres/articles/411076/index3.html>, (text in German) accessed 27 July 2013.

⁵ http://europa.eu/rapid/press-release_MEMO-13-654_en.htm, accessed 27 July 2013.

⁶ REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 21st May 2013, Art. 3.1.(d). ii)

From these developments and our experience in data analysis we predict the following trends in cybersecurity:

- Revival of the privacy, trust and data protection debate at the level of States/EU-Member States^{7 8}.
- Increased uneasiness about large service and infrastructure providers, especially the ones involved in the recent revelations⁹. This might have an impact on competitiveness¹⁰.
- Increase in popularity of information security/privacy-enhancing platforms, products and services^{11,12}.
- Increase in development of new information security/privacy-enhancing platforms, products and services.
- Cybercriminals/cyber-terrorists adapting their strategies and tactics on the basis of known surveillance activities of nation states, for example, by increasingly using information security and anonymity technologies^{13,14}.
- Existing information security controls and strategies being revisited and new security controls possibly arising and being introduced, especially in the area of critical systems (i.e. critical information infrastructure protection - CIIP)¹⁵.
- Increased media appetite to look into these cybersecurity¹⁶ events in more depth.
- Increased awareness of politicians regarding the topics of data protection, trust and lawfulness of digital surveillance¹⁷.
- Debates regarding the completeness, effectiveness and impact of existing or newly issued regulations in all relevant areas (i.e. cyber security, electronic communications, internet, privacy, critical infrastructure protection, etc.) are to be expected^{18,19,20}.

ENISA's ongoing work will continue to assess these current or expected developments. As well as focusing on threats emerging from these trends, ENISA's activities will also include following relevant policy and technological developments, observing market reactions, identifying proper protection

⁷ https://www.nytimes.com/2013/06/18/opinion/global/viviane-reding-protecting-europes-privacy.html?_r=0, accessed 27 July 2013.

⁸ <http://www.reuters.com/article/2013/06/07/europe-surveillance-prism-idUSL5N0EJ31S20130607>, accessed 27 July 2013.

⁹ http://www.huffingtonpost.com/bennet-kelley/the-economics-of-prism-an_b_3469350.html, accessed 27 July 2013.

¹⁰ <http://www.forbes.com/sites/richardstiennon/2013/06/07/nsa-surveillance-threatens-us-competitiveness/>, accessed 27 July 2013.

¹¹ http://www.huffingtonpost.com/2013/06/14/privacy-apps-services_n_3444217.html, accessed 27 July 2013.

¹² <https://www.youtube.com/watch?v=JY3EXVdyiM>, accessed 27 July 2013.

¹³ <http://security.blogs.cnn.com/2013/06/25/terrorists-try-changes-after-snowden-leaks-official-says/>, accessed 27 July 2013.

¹⁴ http://www.washingtonpost.com/world/national-security/us-officials-worried-about-security-of-files-snowden-is-thought-to-have/2013/06/24/1e036964-dd09-11e2-85de-c03ca84cb4ef_story.html, accessed 27 July 2013.

¹⁵ https://www.networkworld.com/news/2013/061713-prism-doesn39t-have-cios-in-270921.html?source=nww_rss, accessed 27 July 2013.

¹⁶ https://www.computerworld.com/s/article/9240084/Digital_surveillance_programs_in_other_countries_trigger_controversy, accessed 27 July 2013.

¹⁷ <http://www.wort.lu/en/view/time-to-wake-up-viviane-reding-on-the-prism-scandal-s-violation-of-human-rights-51c80a5fe4b02fa5029bed7e>, accessed 27 July 2013.

¹⁸ https://www.techdirt.com/articles/20130622/22485623584/leaked-document-shows-eu-approach-to-cybercrime-is-completely-misguided.shtml?goback=.gde_60173_member_253111479, accessed 27 July 2013.

¹⁹ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf, accessed 27 July 2013.

²⁰ <http://www.infosecurity-magazine.com/view/33052/the-effect-of-prism-on-europes-general-data-protection-regulation/>, accessed 27 July 2013.

requirements, supporting relevant stakeholders, etc. If asked to do so, ENISA will provide advice on how to respond to these threats in specific situations or with particular stakeholders in mind.

Apart from these trends, the concerns of industry and consumers need to be taken into account. These concerns are related to the trust of existing digital services and products and might affect the relevant market segments. Privacy concerns related to Cloud Computing appear to be one of the most prominent areas regarding protection requirements.

2. Cloud Computing and privacy

Given that it is highly probable that the Cloud computing business model may be adversely affected by the current debate, emphasis has to be put on available mitigation measures to manage this risk. In work already conducted, ENISA has pointed out the risks related to foreign states' national interests and the interception of data transfers over the internet in its Cloud Risk Assessment²¹, with a forthcoming update to this currently under review. When it comes to the threat of data being accessed with the cooperation of a Cloud provider, a possible mitigation action would be to ensure that encryption is used when data are transmitted and/or stored. Note that in such a scenario, the way in which the cryptographic keys are managed is critical and the challenge will be to find solutions that offer the required level of security at a reasonable cost

Currently, customer-controlled and customer-side encryption can only be applied in a limited number of cloud use cases. It is a topic of research to create new cryptographic algorithms which are more compatible and which could address more cloud computing use cases. Certain products aim to provide "per record" or "per data field" encryption, for certain (Software-as-a-Service) applications, while preserving at least some level of the other functionality usually offered by SaaS applications, such as searching or indexing. Such products, however, usually require the hosting of an appliance at the customer's site, which reduces some of the advantages of Cloud computing. At the same time, there are doubts about the actual strength of the protection such products offer.

When implementing cryptography within the Cloud, there will necessarily be a trade-off between security and flexibility of service. For example, it will often be necessary to distribute cryptographic keys to platforms before they can be used to support cryptographic operations. But this requires knowledge about which platforms are likely to be used in the future and preparation of these platforms beforehand, which is to some extent antagonistic to the idea of scalability upon demand.

Before moving data to the Cloud, public administrations and businesses should therefore perform a thorough analysis of the threats and risks involved, and weigh them against the envisaged benefits. ENISA's Cloud Risk Assessment can be used as a starting point for many of these analyses, but it is recommended that users take their decisions based on an individual, rather than a generic risk analysis. From a customer point of view, ENISA's report on service level agreements (SLAs)²² highlights the indispensable clauses that can't be left out from a service level agreement related to Cloud computing services.

ENISA has long recommended a European Cloud, both to protect data, and because of the potential economic benefits.²³ From the European perspective, the Commission has taken the issue of Cloud computing deployment very seriously, even before the latest developments. After publishing the

²¹ <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment>, accessed 27 July 2013.

²² <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts>, accessed 27 July 2013.

²³ <https://www.enisa.europa.eu/media/press-releases/enisa-clears-the-fog-on-cloud-computing-security-1>

European Cloud Strategy²⁴ the European Cloud Partnership²⁵ was established, with representatives from the private and public sectors who work together on making Cloud a safe solution for European SMEs and governmental agencies. The proposal for the NIS Directive²⁶, which extends to Cloud providers, will become a safeguard to European citizens and businesses.

3. Cryptography

The use of cryptographic techniques has been identified as a key element for privacy. In 2011, ENISA launched a study on the use of cryptographic techniques in the EU, with the aim of identifying the relevant documents setting requirements/specifications related to authentication, integrity and confidentiality of information at national and international levels (even beyond the EU)²⁷. ENISA, for its part, has recommended that:

- Organisations must pro-actively review their encryption specifications and solutions, updating them in line with changing circumstances. Clear procedures for the withdrawal of compromised algorithms, or those that are too weak, must be included in the policies; and
- There is a need for specialised personnel for the deployment of best practices/guidelines with strong security/cryptography knowledge. Many of the cryptographic solutions audited and tested are poorly deployed; in many cases the deployment teams for systems/services handling unclassified information are lacking cryptographic expertise.

During 2013, ENISA has been working towards creating a framework for a multiannual activity in the area of cryptography. In this respect, the recommendations for the use of algorithms, parameters and key lengths need to be updated based on newly discovered vulnerabilities.

4. Data Breach Notification Schemes

EU-wide data security best practices should be developed in the context of preventing data breaches. Article 4 of the ePrivacy directive and Article 32 of the proposed Data Protection Regulation²⁸ also mention technical measures which have an impact on the notification procedure in the case of data breaches. Further technical description is needed to translate into actions the legal provisions for “Such technological protection measures [as] shall render the data unintelligible to any person who is not authorised to access it” and achieve a common understanding across the EU. Such work is also useful in the context of secure electronic signatures²⁹.

²⁴ <https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy>, accessed 27 July 2013.

²⁵ <https://ec.europa.eu/digital-agenda/en/european-cloud-partnership>, accessed 27 July 2013.

²⁶ <http://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced>, accessed 27 July 2013.

²⁷ https://www.enisa.europa.eu/activities/identity-and-trust/library/the-use-of-cryptographic-techniques-in-europe/at_download/fullReport, accessed 27 July 2013.

²⁸ European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, accessed 27 July 2013.

²⁹ A 2010 report to the European Commission, CROBIES : Study on Cross-Border Interoperability of eSignatures deals with this area http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=974. Reference is made to the possible involvement of ENISA in the process of establishing the lists of algorithms and parameters for secure electronic signatures in the associated “Algo Paper”, available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=978, both accessed 14 August 2013.

5. Cloud computing and EU policy

The proposal for an NIS Directive³⁰, published a year ago by the Commission, extends the provisions of Article 13a of the Telecom package to other critical sectors. Article 14 of the NIS directive imposes incident reporting obligations on Cloud providers. These provisions will ultimately increase the transparency about security and resilience of cloud computing, paving the way for a new era in Cloud security.

The Commission also published a European cloud computing strategy aiming to increase the uptake of Cloud computing in the EU. ENISA, together with industry, actively supports the implementation of this strategy. A pillar of this strategy is the European Cloud Partnership Steering Board, set up to execute part of the EU's cloud strategy. The ECP steering board recently published a vision, called 'Trusted Cloud', on 21, March, 2014³¹. ENISA endorses this vision, which focusses on how to accelerate the adoption of Cloud, and how Europe can become a trusted region for Cloud computing.

³⁰ <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>, accessed 27 July 2013.

³¹ European Commission initiative 21, March 2014, on Trusted Cloud Partnership, please refer to http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935 and http://europa.eu/rapid/press-release_IP-14-296_en.htm



ENISA

European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu