August 2013
Heraklion

Securing data in cyber space

ENISA comments following recent large-scale data compromise activity

As dictated 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 context ENISA is setting out its position with regard to recent discussions concerning the interplay between cybersecurity and data being compromised. Moreover, ENISA considers its involvement in these discussions to be a natural consequence of the fact that this debate concerns 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]. These discussions exert pressure 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 such 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 release the pressure on 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 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, and ENISA in particular, from a technical perspective.

Emerging cybersecurity trends

Within its activities related to the identification of emerging trends in cybersecurity[6], ENISA has detected 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. From

[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)*

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 revelations[9]. This might have an impact on competitiveness[10].
- 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 cybersecurity[16] events in more depth.
- Increased awareness of politicians regarding the topics of data protection, trust and lawfulness of digital surveillance[17].
- 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].

---

[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=JJY3EXVdyiM, 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.

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 requirements, supporting relevant stakeholders, etc.

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.

Cloud Computing and privacy

Given that it is highly probable that the Cloud computing business model may be adversely affected, 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 Assessment[21], 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, the only mitigation action possible would be to ensure that encryption is used when data are transmitted or stored.

In addition, to this, the owner of the information needs to have full control over the encryption[22]. Currently, customer-controlled and customer-side encryption can be applied only in Infrastructure-as-a-Service (IaaS) data storage services. Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) offering stronger encryption and full customer control would be the solution to this threat: however the cryptographic techniques required still remain a research topic. Other services are available for certain SaaS applications, which provide "per record" or "per data field" encryption, while preserving at least some level of the other functionality usually offered by SaaS applications, such as searching or indexing. Such services, however, usually require the hosting of an appliance at the customer's site, which sacrifices some of the perceived advantages of Cloud computing (in this case easy access from anywhere). At the same time, there are doubts concerning the actual strength of the protection such services offer.

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)[23] highlights the indispensable clauses that can't be left out from a service level agreement related to Cloud computing services.

---

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

[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] 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.*

ENISA has long recommended a European Cloud, both to protect data, and because of the potential economic benefits.[24] From the European perspective, the Commission has taken the issue of Cloud computing deployment very seriously, even before the latest developments. After publishing the European Cloud Strategy[25] the European Cloud Partnership[26] 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 Directive[27], which extends to Cloud providers, will become a safeguard to European citizens and businesses.

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)[28]. 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.

EU-wide data security best practices should be developed in the context of preventing data breaches. Article 4 of the ePrivacy directive and Article 29 of the proposed Data Protection Regulation[29] 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 signatures[30].

---

[24] https://www.enisa.europa.eu/media/press-releases/enisa-clears-the-fog-on-cloud-computing-security-1

[25] https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy, *accessed 27 July 2013.*

[26] https://ec.europa.eu/digital-agenda/en/european-cloud-partnership, *accessed 27 July 2013.*

[27] http://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced, *accessed 27 July 2013.*

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

[29] 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.

[30] *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*

Duty to report Cloud computing incidents

In the context of Cloud computing, the proposed new Cyber Security Directive[31] extends the provisions of the 2009 Directive to Cloud services. Like Article 13a in the telecom sector, Article 14 will impose incident reporting on Cloud providers. National competent authorities for Cloud providers will be established, thus enhancing Cloud security, privacy and resilience across the EU. ENISA is supporting the activities in the proposal, paving the way for a new era in Cloud security.

Clarifications are pending

In order to set the scope, purpose and practices behind state surveillance, and also to obtain clarity with regard to resulting protection requirements, several points must be addressed. This will lead to an understanding of the impact that large-scale digital surveillance capabilities can have on cybersecurity and privacy. Some of the pending clarifications are:

- The legal basis/bases for state surveillance should be clarified and discussed at EU and international level to enable a wider public understanding and debate of the issues.
- It should be clear under which conditions significant data collection and storage on individuals needs to be reported to public authorities.
- It should be clarified as to whether there are any restrictions on the lifetime of data pools collected for a specific purpose (such as avoiding a terrorist attack). Furthermore, possible practices for the enforcement of such restrictions have to be investigated.
- The minimum technical protection measures that are required from companies to protect data related to individuals should be discussed.
- There should be a debate on how the EU Member States can work together to make sure that techniques for protecting against casual eavesdropping are implemented by citizens by default without introducing unnecessary complexity.
- The feasibility of implementing technical measures for detecting eavesdropping based on traffic flows across the internet should be evaluated.
- Strategic research and development priorities addressing prospective requirements resulting from these developments need to be formulated.

While ENISA invites relevant EU authorities and bodies to elaborate on the above questions, the Agency will follow these developments with great interest and will continuously assess their impact on cybersecurity, and, when called upon, will contribute towards strengthening EU cybersecurity protection practices.

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.

[31] *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.*