Source: CEPIS LSI/CEPIS Council

Version for Publication
27.02.2014

CEPIS LSI SIN

Document for:

Decision	
Discussion	
Information	x
Publication	x

Assisting EU citizens with reliable ICT security information

CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote high standards among Informatics Professionals in recognition of the impact that Informatics has on employment, business and society. CEPIS – which represents 35 Member Societies in 32 countries across greater Europe – has agreed on the following statement:

1. Background

Nowadays European citizens of all ages are used to sharing sensitive personal and non-personal (*i.e.* not traceable to a person) information online for both personal and professional reasons. However, they often lack awareness of the important security risks inherent in sharing such information. Almost on a daily basis, Europeans are confronted with (news of) ICT security breaches and the practice of large-scale data collection by ICT service providers (especially by means of applications and/or social media networks like Facebook) and operating system designers (like Apple, Microsoft, and Google through the use of respectively iOS, Windows, and Android) as well as state agencies and bodies.

Traditionally, actors involved in ICT security breaches and the practice of illegal data collection are criminals and criminal organisations. However, according to computer crime experts even governmental organisations are involved in ICT security breaches. Nowadays it is very difficult to distinguish between the “good guys” and the “bad guys” with respect to ‘legally’ breaching ICT security. [1] ICT crimes related to online banking and (illegally) obtaining valuable sensitive personal and non-personal online information from citizens and companies demonstrate the clear need for ICT security in general. An adequate level of ICT security is of the utmost importance for the protection of the European citizen’s data and interests.

The average European citizen is often lacking the knowledge and means to take effective countermeasures against ICT security risks. Security companies, banks, and governments in most cases do have the resources to set up agencies as well as effective security checks and balances to deal with these matters. The average citizen, however, does not have access to dependable ICT security information.

ICT and ICT security products are usually developed by (large) commercial entities with limited governmental oversight and next to no control by the public. These companies possess information about their products and the required ICT security measures for their products. Mostly, ICT development and the development of the required ICT security measures are carried out in isolation from the average European citizen as well as from European governments. Citizens and governments do not have a say in this. [2] Non-ICT experts (average citizens) do not possess nor can they access (fast) enough reliable (non-technical and 'digestible') information about what to do in a specific emergency situation with regard to general or specific ICT security threats. They do not know where to obtain trustworthy ICT security information [3], notwithstanding the efforts already made by the European Commission for an adequate European and national ICT security policy and budget with respect to the protection of the legitimate interests of the European citizen in this respect. We refer to the establishment in March 2004 of the European ENISA Agency and its work [4] as well as the Cyber Security Strategy for the European Union and the Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union [5]. However, regarding the availability of reliable ICT security information for the average citizen, CEPIS believes that there is still some work to be done within the European Union, which fits well into the afore-mentioned European framework.

2. Concerns

Today, the European citizen still does not have access to reliable – in the sense of dependable and/or trustworthy – information on ICT security risks (and incidents). For the sake of clarity, we would like to distinguish between two types of security risks, for which reliable security information is necessary for the citizen: (1) operational ICT security weaknesses (*i.e.* ICT security breaches caused by 'insufficient' management) and (2) design vulnerability of, *e.g.* operating systems, software, applications, social media networks or ICT services (*i.e.* they are designed in such a way that there are privacy or security issues). [6]

Examples of type (1) risks include the Sony case of April 2011, in which the hacking of the Sony PlayStation Network resulted in stolen personal data and credit card details of millions of online gamers. Other hacking incidents followed with a peak in June 2011, in which personal data of over one million customers were exposed. [7] The same happened in the Netherlands with data of the customers of the ICT service provider KPN being compromised. In January 2012, several hundreds of KPN servers used to store customer data used in online services were hacked. Personal data of KPN customers were via another website exposed by the hacker. [8]

In these cases ICT security information is needed by ICT service providers in order to protect the data of their customers when they get hacked. The citizen should also be aware of the implications of such activities and should somehow be notified and provided with relevant reliable information, even if it is of a non-technical nature, *e.g.* about the reliability of an institution like a bank or an ICT-services company.

Examples of type (2) risks include iOS, Windows, Android, and, as already mentioned, Facebook. In these cases better ICT security will not protect the user/citizen against the vulnerabilities inherent in the design of the operating system, platform or application, because the user is driven into giving away sensitive personal data and often too much of it. For instance, all kinds of personal information are gained through the use of mobile (smart)phones or tablets and the user has no realistic choice than to give away these data. The user has to agree to something when she or he does not really know what it actually means. iOS, Windows, and Android are designed in a way that they can only work properly by gathering and transferring all this information away from the user while the user is conditioned to agree to the respective terms and conditions. The user can, in fact, only accept this or decide not to use the mobile (smart)phone or tablet. In these cases, there is no real lack of information, because to some degree this information is available; but not always in a way the user understands. The mobile (smart)phone or tablet does what the user has agreed to but the user does not really understand the technicalities. The designers of the operating systems or software consider this a service and not an ICT security threat or weakness. The difference between type (1) and type (2) risks is that type (1) risks involve unwanted weaknesses, which for instance the operator or ICT service provider does not wish for in the first place, while design vulnerabilities are desired for the collection of personal data.

The average European citizen is not (completely) aware of the repercussions and the intrusiveness of ICT security threats with respect to his or her personal life and does not know to which reliable source to turn for reliable (non-technical and 'digestible') information regarding general or specific ICT security threats. It is not clear where in Europe to get reliable consumer ICT security information. Another concern is that the clients (contractors and users) of ICT companies who want to solve a specific ICT security problem and who are not aware of their privacy rights might give away too much personal information without an existing need to do so. A last concern is that some data collectors might not (sufficiently) protect the collected consumer data, because they are not aware that the collected data is personal data in the legal sense. Therefore, extension of existing consumer protection and data protection legislation might be required.

CEPIS would like to ask the European Commission as well as EU Member State policy makers to take (legal) action in order to ensure the average European citizen has access to the necessary reliable ICT security information regarding general or specific ICT security threats, *e.g.* by making the publication and distribution of this type of information mandatory, in order to take effective (preventive) countermeasures. This should be done with respect for the legitimate interests of the parties involved. First steps will be taken with the enactment of art. 15 of the mentioned Proposal of the European Commission for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (see footnote 5).

The European Agency ENISA has already undertaken solid work on some issues mentioned in this statement under the topic of education and awareness. ENISA could potentially co-ordinate the actions, which are further required to assist European citizens with reliable ICT security (risk) information. However, performing the required tasks alone is perhaps too large an undertaking for ENISA. In our view, these tasks would be best suited to a large agency, which has direct contact with citizens on the topics set out in this statement. ENISA may, according to its new Regulation (see footnote 4), upon request by Member States or EU bodies, provide advice in the event of breaches of security or loss of integrity. ENISA's mandate is extended in this respect. According to its mandate, ENISA may also support Member States, at their request, and at the request of the Union's Institutions to organise awareness-raising and other outreach activities to increase network and information security and visibility.

One of the key tasks in terms of assisting EU citizens with reliable ICT security information is a national (and European) overview of the relevant institutions from which to obtain such information. ENISA has been doing this task with its Who-is-Who Directory on Network and Information Security (NIS) for several years now. It contains information on NIS stakeholders, such as national and European authorities and NIS organisations, contact details, websites, and areas of responsibilities or activities. [9] However, this Directory does not contain an evaluation of the organisations involved nor the content they provide. Defining the complete information that Europe's citizens need to be properly assisted is very complex. One way to structure this body of work could be through the appointment of a European body for instance ENISA. As a first step the focus could be on type (1) and type (2) security risks. In a second phase, European Member States could take this work further in their local NIS landscape, culture, and language. Another actor that could potentially contribute to this work is the recently launched European Cybercrime Centre (EC3), the European focal point in the fight against cybercrime. The EC3 can provide analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community. However, EC3's remit, as an extension of Europol, is organised online crime, child sexual exploitation online, and critical infrastructure and information systems. At present it is not aimed at "consumer" issues. The Cyber Security Strategy for the European Union states that the European Commission will examine in 2013 how major providers of ICT hardware and software could inform national competent authorities on detected vulnerabilities that could have significant security implications. This examination could also take the present statement into consideration.

CEPIS considers such action is in the best interest of the European ICT community itself because the ICT company-client relationship could be seriously compromised if the European citizen is left ill-equipped to counter the mentioned ICT security risks.

3. Recommendations

In particular the following points should be on the research agenda of European and domestic policy makers:

1. The European citizen should be better protected against ICT security threats by more awareness-raising and much better availability of ICT security information in order to

adequately assess a general or specific ICT security risk situation. [10]

2. The European citizen should be assisted with reliable (non-technical and 'digestible') ICT security (risk) information by a reliable, preferably independent, body, *e.g.* a European trusted party or Agency in order to get reliable ICT security information regarding general or specific ICT security threats. The citizen should know what to do in a specific risk situation.
3. A European body, *e.g.* ENISA should structure the landscape to give direction for Member States. Member States need to address this at national level. Citizens should be better informed about data flows, especially about data flows in clouds, to better understand, whether or not their data are remaining within the European data protection regime.
4. Providing ICT security information regarding general or specific ICT security threats should be in conformity with European intellectual property legislation and the commercial interests of the involved ICT companies.
5. The information gathered with the consent of the clients (contractors and users) of ICT companies and other relevant parties requesting reliable ICT security information regarding general or specific ICT security threats should be used, stored, and deleted according to European data protection legislation.
6. The information gathered with or without consent of ICT companies and other relevant parties regarding general or specific ICT security threats should be used, stored, and deleted according to European data protection legislation.
7. The European Commission and (European and national) policy makers should examine the need for mandatory publication of ICT security related information by ICT companies and other relevant parties in order to help the average European citizen as well as European Member States to counter serious general and specific ICT security threats.
8. The principle of proportionality should be paramount when making ICT security-related information by ICT companies and other relevant parties available to ICT experts and non-ICT experts and *vice versa*, even with respect to non-personal information. [11]

References

[1] According to for instance Nissim Bar-El, founder and CEO of the Israeli ICT security company Comsec, who is now hired by banks and insurance companies for the protection against cyber-attacks. His message in a Dutch TV interview for KRO Brandpunt of April 28, 2013 is clear: the worst is yet to come. According to him the budget for the fight against cyber-attacks should be considerable higher than today and in the hands of the Prime Ministers of the Member States. ICT service providers are mainly forced by the state to collect the data on the basis of legislation, while operating system designers and state agencies as well as some application designers collect the data because they want to. The activities of Edward Snowden, an American computer specialist and a former CIA and NSA employee, made this more public. He intentionally disclosed classified details of several top-secret United States and British government mass surveillance programs to the press. See: http://en.wikipedia.org/wiki/Edward_Snowden

[2] For more information concerning the developments with respect to legal and security issues in Europe see: Kai Rannenberg, Marko Hölbl, Eleni Kosta, Les Fraser, and Joop Verbeek, 'Legal and Security Issues in Informatics', in Robert McLaughlin, Fiona Fanning, and Nello Scarabottolo (guest editors) (2009), UPGRADE, The European Journal for the Informatics Professional, http://www.upgrade-cepis.org, Vol. X, issue No. 4, Monograph –

20 Years of CEPIS: Informatics in Europe today and tomorrow (published jointly with Novática), Brussels: CEPIS, August 2009, p. 15-18.

[3] ICT experts, on the other hand, are not always able to provide non-ICT experts with the necessary information regarding general or specific ICT security threats. The required data are not (fast enough) at their disposal. Another point is that ICT companies are reluctant to give away ICT security information. These issues fall outside the scope of the present statement. Where we speak about ICT security information, one can, according to the context, also speak of ICT security risk information. That is sometimes more clear.

[4] See for instance the ENISA Work Programme for 2013:
http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013
and also its new Regulation: The European Commission Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)(14358/10):
http://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/viv75rdmr3zl?start_00g=10;
For the last changes of the ENISA mandate see:
http://register.consilium.europa.eu/pdf/en/13/st05/st05921.en13.pdf;
On April 16, 2013 this legislation was voted in the European Parliament.

[5] See: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security and
http://www.europarl.europa.eu/document/activities/cont/201207/20120712ATT48826/20120712ATT48826EN.pdf;
Related: A Digital Agenda for Europe, COM(2010)245, May, 2010.

According to art. 15 section 2 of the Proposal Member States shall ensure that the competent authorities have the power to require market operators and public administrations to: (a) provide information needed to assess the security of their networks and information systems, including documented security policies; (b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.
On the basis of art. 6 of the Proposal Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority"). In particular Chapter three of the Proposal is interesting for the present statement as it describes the cooperation between the competent authorities and as part of that the information sharing. Part of this partly secured information sharing could be the information sharing meant in the present statement.

[6] A third type of ICT security risk information could involve information regarding the question if an ICT device is working properly or not. The citizen has the feeling that his device is hacked or not working properly and would like to obtain reliable information about this. For instance in Germany the *Bundesamt für Sicherheit in der Informationstechnik* (abbreviated BSI - in English: Federal Office for Information Security, but more often known as German Information Security Agency (GISA)) is the German government agency in charge of managing computer and communication security for the German government and is able to handle such information needs. However, for other countries there could be a need for this third type of ICT security risk information also.

[7] See: http://nakedsecurity.sophos.com/2013/05/13/sony-hacking-

suspect/?utm_source=feedly&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+ and:
http://www.informationweek.com/security/attacks/sony-hacked-again-1-million-passwords-ex/229900111

[8] See: https://www.security.nl/artikel/46554/1/KPN-hacker_krijgt_100_uur_taakstraf_.html

[9] See: http://www.enisa.europa.eu/publications/who-is-who-directory-2011

[10] ENISA and the European Commission have already worked with the US Department of Homeland Security to produce a report on November 30, 2012 on "Involving Intermediaries in Cyber Security Awareness Raising''. In focus were mechanisms for cross-border cooperation, as well as for public-private collaboration and information exchange. The report was one of the results of an EU-US workshop held earlier that year. See: http://www.enisa.europa.eu/media/news-items/new-enisa-report-with-us-homeland-security-2013-cyber-security-awareness-raising

[11] The principle of proportionality ensures that the processing of a person's personal data is limited to cases where there is a direct connection with the initial purpose of the processing. The information must not only be useful, but also necessary to whoever is processing a person's data. The data being processed must not be excessive in relation to the aim pursued.