Workshop on Cyber Security Training

Sharing Best Practices for EU-wide Network & Information Security

27 February 2014

Representation of the State of Hessen to the EU

European Security Round Table sprl
Rue d'Arlon 51, 1040 Bruxelles
Tel.: +32 (0)2.640.63.92 - Fax: +32 (0)2.646.61.93
www.security-round-table.eu - info@security-round-table.eu

Agenda

14:00

Welcoming Remarks & Opening

Friedrich von Heusinger, Director of the Representation of the State of Hessen to the EU
Florent Frederix, Trust & Security Unit, DG CONNECT, European Commission

14:15

Panel I: The Challenge of Homogenous Cyber Security Trainings

Marco Thorbrügge, Head of Unit for Operational Security, ENISA
Wolfgang Röhrig, Programme Manager Cyber Defence, EDA
Yves Vandermeer, Chair, E.C.T.E.G and Detective Chief Inspector, Federal Computer Crime Unit, Federal Police, Belgium
Ilias Chantzos, ICSPA Enterprise Member and Senior Director Government Relations, EMEA & AJP, Symantec

15:30

Coffee Break

16:00

Panel II: How to Get Cyber Security Trainings Right?

Susanne Sondergaard, Senior Analyst, RAND
Ray Genoe, Cybersecurity/Cybercrime Analyst & Training Officer, Centre for Cybersecurity and Cybercrime Investigation, UCD School of Computer Science and Informatics, Dublin
Ralf Kaschow, Director, CyberAkademie
Christian Van Heurck, Coordinator, CERT.be

17:15

Drawing Recommendations

Christoph Raab, Chairman, European Security Round Table

Presentation

Why this workshop?

Being one of the most prominent German regions in the field of cyber security, the Representation of the State of Hessen to the EU hosted this workshop with the aim to discuss the development of European cyber security trainings. The participants shared their thoughts and views in order to identify the main motives for creating such trainings and to propose some concrete steps forward. It was recalled that the increasing European reliance and dependence on cyber space requires the protection of online activities and critical infrastructures in the EU. In particular, the sharp increase of cyber incidents risks and cyber-attacks calls for establishment of new capabilities, both in the private and the public sector. In this context, cyber security trainings are of vital importance for the strengthening of Information and Technology (IT) competencies and skills in companies and in public administrations. Although some efforts have already been made to develop such training interventions, there is a strong need for greater coordination across the EU and across sectors involved in order to ensure their availability and quality. With this workshop, the European Security Round Table (eSRT), ICSPA and the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE) together with ENISA and EDA, launched a common initiative to identify challenges and best practices across sectors, and organise training interventions across the EU.

Panel I: The Challenge of Cyber Security Trainings

Current Efforts

The discussion first addressed the existing efforts in the field of development of IT skills and competencies[1] and promotion of good practices. Several public and private entities already provide cyber security trainings to their relevant departments. Some public authorities have established working groups and certain agencies provide guidelines for ensuring good practices[2]. Therefore, there are initiatives to bring together experts from several EU Member States and sectors in order to provide efficient trainings to public administrations and relevant stakeholders.

Limitations

However, these efforts have limitations: trainings remain limited because of a shortage of skilled professionals capable to training others, and because the area is still perceived as relatively new. Moreover, trainings are most effective when tailored to a specific audience. Nevertheless, the identification of different audiences and their specific requirements in this emerging area has just begun.

Speakers also pointed out that the lack of funding limits the success of cyber security trainings. Even today, whilst cyber security is featuring prominently on the political agenda, some leaders think that cyber security can be achieved at no or low cost, or that investing in technology is sufficient. On the one hand, existing funds are not efficiently distributed. Some countries, for instance, allocate all resources to the private sector and thus prevent public administrations from building up cyber security capabilities. On the other hand, certain companies such as SMEs or public departments do not have enough money to pay the costs of cyber trainings. Certain cybercrime units, for example, have had difficulties to pay for a multiple day seminar.

Interoperability is another limitation. The range of languages and backgrounds (education, experience) among professionals and potential participants constitutes a challenge to the creation of common standards.

These challenges are not exhaustive, but certainly form a strong incentive to discuss the establishment of common European standards and modules facilitating the development of cyber security trainings across the EU.

What is Needed?

Cyber security training and education has to be embedded in the bigger picture. Training and education is also related to personnel development, recruitment and retention of personnel. Regarding the shortage of skilled professionals, particularly in the public sector, there is a need to find incentives to encourage young talents, professionals or students, to consider a career in the cyber security area.

The guarantee of reusable IT skills could be one. Potential IT professionals need to be sure that they will be able to use their skills in various sectors. In the discussion the absence of synergies between the military and civilian sectors was mentioned: young professionals are not willing to engage in the military sector because their skills are not always compatible with and recognizable for the civilian sector, which prevents them from reusing their skills after a military career[3]. This problem exist across various sectors, and needs a common approach by civilian and military stakeholders. Therefore, there is a need to generally consider the extent to which the skills developed in one sector are transferable and recognised in others. Standardisation and accreditation is one way in which you can make it more transparent and easy to compare existing skills and qualifications.

Moreover, the standardisation of professionals' profiles and skills would permit the distribution of academic modules across the EU, while still adapting to certain local features. When stressing the need to reach a common level of skills, a common academic background and a common terminology, a reference was made to the creation of "cyber ERASMUS" [4].

Finally, there is a need to raise awareness on cyber security in schools, companies and public administrations, irrespective of the level of hierarchy[5].

Panel II: Get Cyber Security Trainings Right

Target Audience

In the second panel, the discussion moved to the concrete features of high quality training interventions. The first point which was addressed was the attention that should be paid to the target audience[6]. In order to be relevant and to obtain empirical results, both the training sponsors and the trainers/ organisers should know who they target and what the main characteristics and expectations of their audience are in view of the expected skills or competencies developed through training courses/classes. The expected learning outcomes should be clear. Moreover, they should include an evaluation of the impact of the training. What difference should cyber security trainings make?

Filling the gaps

Existing efforts should serve as an example and starting point for the identification of the main characteristics which ought to shape training interventions. What works? What should be improved? Which gaps can be identified?

Currently the majority of training courses are designed for specialists in order to develop very specific and primarily technical competencies and skills. However, not only specific sectors and departments should have access to training interventions aimed at raising threat awareness and the development of basic response skills. The first gap identified is thus the absence of trainings for a large part of public administrations and employees.

A second gap pertains to the lack of a European cyber security expert and trainer database. Such a database would facilitate access to IT professionals and promote the sharing of experiences and best practices. Creating a common pool of experts would go along with the logic of mutual recognition between cyber security trainings instead of inefficient competition. The various trainings should not juxtapose but complement each other.

As an example of an empirical training provider, the Centre for Cybersecurity and Cybercrime Investigation of the UCD School of Computer Science and Informatics (Dublin) gave some feedback on cyber exercises[7]. The Centre aims to target various sectors such as cybercrime units, the energy sector and the banking sector. However, it faces the problem that not all members of the targeted audience have the resources to participate physically in cyber security trainings. This raises the need to consider appropriate training formats for the training audiences, taking into account both the effectiveness of the format and the resources required to deliver and participate.

Communication

Communication should also be part of training interventions[8]. Firstly, communication should be *about* trainings. Along with their visibility, cyber security trainings should be promoted in professional environments. Not only IT departments should be aware of cyber incidents risks, managers and employees should also be informed about these threats. The need for cyber security trainings should be recognised at all management levels and in all departments.

Those participating in the workshop expressed a preference for interactive training sessions with ample opportunities to engage with real-life examples in order to bring the learning to life.

Finally, organisations should support the transfer of knowledge obtained during the training into the work environment, e.g. by providing participants the opportunity to apply the skills developed during the training, offer refresher trainings, and stimulate continuous professional development to keep the acquired skills up-to-date. Furthermore, both the format and the content of training interventions should be continuously reviewed and updated to ensure their validity and relevance in light of the evaluation of new technologies and attack vectors.

Recommendations

- **Cross-border synergies *vs.* localization**: Find the right balance between the broad and standardized distribution of cyber security trainings across the EU, and the adaptation of these trainings to specific local/national needs.

- **Education on IT security**: awareness raising should start at an early age and focus on security, a matter that must be part of IT trainings and, more generally, of IT education.

- **Accessibility**: Cyber security trainings should be open to a general audience (with different levels of knowledge and from different sectors), and it should be easy to apply for training sessions.

- **Matter of change**: cyber security trainings should be up-to-date in their content and professionals' certifications must complt with the evolution of IT technologies, habits and threats.

- **Interoperability** : the identification of common standards, certifications, scenarios and terminology should be promoted through the facilitation of best practices exchange and the adoption of existing private sector standards by the public sector. An example of an interaction initiative would be the introduction of a "cyber Erasmus", both between different member states as well as different sectors, in order to boost IT skills, employability and a common understanding across physical and mental borders.

- **Private & public sectors**: the private and public sectors should identify opportunities for closer collaboration and trust building in order to define the European cyber security trainings' requirements and standards together.

Further Information

[1]: The increasing reliance of the EU on the Internet and critical infrastructures potentially introduces further vulnerabilities and detrimental impact of a cyber attack. Consequently, both private and public organisations need to have the skills to operate securely and efficiently in this environment.

[2]: **Florent Frederix** named different types of efforts: drivers licences for Network and Cyber Security, voluntary programmes for IT education, cyber security Master programmes or private programmes provided by industries. **Marco Thorbrügge** also mentioned the existence of tailored consultancy services for CERTs setups and the development in 2008 of a training material from BP-Guide (teacher and student handbook). The B-CCENTRE also referred to the network of Cybercrime Centres of Excellence for Training, Research and Education established in the EU.

[3]: This challenge presented by **Wolfgang Röhrig** raises the question of IT certifications. A corollary limitation is the lack of cross-sectorial certificates that, in this example, could be an additional incentive to join the military sector.

[4]: The idea of a cyber ERASMUS would depend on the definition of common students profiles by the European Commission according to **Yves Vandermeer**."It is not the paper that makes the guy". Moreover, he stressed that a pumping system would be needed to motivate people for trainings. How can we motivate students?

[5]: **Ilias Chantzos** stressed the necessity to raise awareness at an early age, in school. Cyber security trainings have to be normalised in a way that everybody feels involved and concerned. Cyber security and data protection issues are not someone else's problem. All sectors and departments, all levels of the hierarchy, should have basic reflexes to tackle cyber incidents and know what to do or who to call in case of emergency. As **Ralf Kaschow** explained later, if one person opens wrong email attachment at the wrong moment, the whole company can be affected.

[6]: **Susan Sondergaard** identified through RAND's pan-European training needs analysis of military cyber defence four target audience categories: the ICT users, the cyber defence specialists, the senior decision makers and the practitioners engaged with e.g. advice to seniors. She recognised that the audiences are somewhat overlapping and change along the career paths. She pointed out the need to understand the specific training needs of each target audience to make sure design of training interventions is relevant and appropriate.

[7]: **Ray Genoe** explained that the UCD Centre provides capacity building courses for industry, law enforcement and academia, and has recently developed e-learning courses with the aim to address the problem of budgetary issues for the police. One of the courses focuses on training development. The main topics are data forensics, corporate cyber crime, cyber security research, telecommunications, incident response, incident management planning, etc.

[8]: It was stated in both panels that not only IT skills were needed in the establishment of Cyber Security Trainings but also communication skills. If you want to be good in cyber security trainings you need personal skills and communication skills as well as the technical knowhow, in order to clearly communicate and to attract a maximum number of participants. Experts and specialists are not only "geeks". According to **Christian van Heurck**, this would increase the quality of the trainings. Specialists should be able to motivate participants and explain people what to expect from the trainings.

Participants

Last Name	First Name	Function
Božič	Gorazd	Team Manager - SI-CERT
Chantzos	Ilias	Senior Director Government Relations - Symantec
Dahno	Michelle	CERT-RENATER
Dragostinov	Todor	Chief Expert - CERT-Bulgaria
Encutescu	Sorin	National security Counsellor & Cyber Security Adviser - Office of the Prime Minister of Romania
Frederix	Florent	Trust & Security Unit, DG CONNECT, European Commission
Genoe	Ray	Cybercrime/Cybersecurity Analyst & Trainer - UCD Centre
Hargis	Monica	Program Manager - Strategy Analytics
Heuré	Jeanne	Event Manager - eSRT
Ivanova	Maria	Expert - CERT Bulgaria
Jakimavicius	Tomas	Counsellor - Permanent Representation of Lithuania to the EU
Kaschow	Ralf	Director - Cyber Academy
Lamont	Kristof	ATM Cyber Security Expert -EUROCONTROL
Lendl	Otmar	Team Leader - CERT Austria
Leonard	Rauch	Program Assistant - ATA
Mennens	Ann	Manager - B-CCENTRE
Mifsud	Charles	Team Leader – CSIRT Malta
Nitoi	Mihai	Counsellor - Permanent Representation of Romania to the EU
Nogueras	Antonio	Head Air Traffic Management Security Unit - EUROCONTROL
Perhoc	Darco	Assistant Director - Croatian National CERT
Pierangelini	Erminio	Military Attaché - Permanent Representation of Italy to the EU

Participants

Last Name	First Name	Function
Raab	Christoph	Chairman - ESRT
Röhrig	Wolfgang	Programme Manager Cyber Defence - European Defence Agen-
Rotariu	Mihai	Technology of Information consultant - CERT-RO
Rozentāle	Līga Raita	Counsellor Cybersecurity - Permanent Representation of Latvia
Salm	Kusti	Adviser - Permanent Representation of Estonia to NATO
Slezák	Henrich	System Engineer - CSIRT.SK
Smeaton	Rob	Action Officer, CIS Directorate - EEAS, EUMS
Sondergaard	Susanne	Senior Analyst - RAND
Szep	Tamas	Deputy Leader of Duty Team, IT Engineer - GovCERT-Hungary
Tafra	Tamara	Attaché Cyber Issues - Permanent Representation of Croatia to
Thorbrügge	Marco	Head of Unit for Operational Security - ENISA
Tofan	Dan	Technical Director - CERT-RO
van der Wel	Matthijs	Director Incident Response - DataExpert
Van Heurck	Christian	Coordinator CERT.be - Belnet / CERT.be
van Wijk	Wout	EU Public Affairs Manager - Huawei
Vandermeer	Yves	Chair, Detective Chief Inspector - E.C.T.E.G, Federal Police
von Heusinger	Friedrich	Director - Permanent Representation of the State of Hessen to

European Security Round Table

Rue d’Arlon 51
1040 Brussels

Tel: +32 (0) 2 640 63 92
Fax: +32 (0) 2 646 61 93