European Crime Prevention Award (ECPA)

Annex I – new version 2014

Please complete the template in English in compliance with the ECPA criteria contained in the RoP (Par.2 §3).

General information

1. Please specify your country.

Portugal

2. Is this your country's ECPA entry or an additional project?

3. What is the title of the project?

CHAOS (Cyber Health and Awareness Operational System) The project name was inspired by the Greek mythology that mentions Chaos as the first divinity in the Universe, therefore, the oldest conscience from all divinity consciences.

4. Who is responsible for the project? Contact details.

Name: José Carlos Martins Job Title: Coordinator Email: jc.martins@cncs.gov.pt Phone: +351 962 880 095

5. Start date of the project (dd/mm/yyyy)? Is the project still running (Yes/No)? If not, please provide the end date of the project.

Start date: 07/10/2014 (the beginning of National Cyber Security Centre) Status: still running

6. Where can we find more information about the project? Please provide links to the project's website or online reports or publications (preferably in English).

Until now, the project website doesn't exist, because the project is under development, although some links regarding tools and procedures used in this project are available:

CNCS Website - Alert Service:

http://www.cncs.gov.pt/cert-pt-2/security-alerts/index.html

Incident Handling Automation Project:

https://www.enisa.europa.eu/activities/cert/support/incident-handling-automation

IntelMQ:

https://github.com/certtools/intelmq/

CVE Search:

https://github.com/wimremes/cve-search

ContactDB:

https://github.com/certtools/contactdb

Security Ratings Platform:

http://www.bitsighttech.com/security-ratings-platform

Please give a **one page** description of the project (**Max. 600 words)**

CHAOS focuses on prevention and improvement of the health of Portuguese cyberspace through communications and alerts to reduce the cyber-attacks surface and support entities with the technical and procedures information.

Therefore, the CHAOS platform in National CyberSecurity Centre is being developed to prevent vulnerability exploits in Public Administration, Critical Infrastructures and important systems available in Portuguese cyberspace. The platform will support multiple tasks, like sending alerts of vulnerable systems detected in cyberspace and new found software and hardware vulnerabilities, recommendations to improve the security of systems and infrastructures, and monitoring the systems and networks in each entity to generate periodically a "reliability indicator" at a national, sector and entity level.

In order to achieve these goals, the project has the following steps:

1. Networks, domains and systems identification and map them to the correspondent entities. Insertion of collected information into an open-source tool named ContactDB;
2. Present and apply a "Maturity Model" to improve the reliability of technical teams responsible for monitor, prevent and respond to incidents at each entity. In this step, each entity should follow the model to achieve technical capabilities to correctly monitors and protect their networks and systems;
3. Collect and process data feeds (compromised systems, vulnerable systems, indicators of compromise) from multiple sources using an open-source tool named IntelMQ developed by CNCS;
4. Correlate information from step 1 and 3 and generate automated reports mentioning the possible vulnerable systems;
5. Based on found vulnerable systems, intersect vulnerabilities with CVE database using an open-source tool named CVE-Search to manually create reports and recommendations with technical details to fix the vulnerability and prevent future systems compromise;
6. Monitor the "reliability indicator" generated by a commercial tool named Security Ratings Platform from BitSight Company to evaluate the effectiveness evolution of the project;
7. Generate "reliability indicator" evolution reports at a national, sector and entity level.

The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.

8. How does the project contribute to crime prevention and/or to the reduction of crime or the fear of crime? (**Max. 150 words**)

The approach of this project is using proactivity procedures thereby trying to be one step ahead of cyber criminals. To achieve these goals, awareness, procedures, technical information should be available to all entities in cyberspace. Some examples are the following:

- Automated alerts of found vulnerabilities in software and hardware that majority of entities use;
- Automated feed reports collection and process to be send to entities. These reports contain information regarding compromised systems, vulnerable systems and indicators of compromise;
- Apply a "Maturity Model" to improve the reliability of technical teams responsible for monitor, prevent and respond to incidents at each entity.

9. How is the project contributing to raising citizens' awareness of crime prevention? (**Max. 150 words**)

The initial phase of this project is dedicated for State institutions, critical infrastructure and entities, which will have direct impact on citizens and society security. The effects from this phase reflect into continuous improvement in technology systems from evolved entities through a gradual maturity process regarding cyber security in each entity.

As an example, the botnets, spam and phishing indicators decrease will be the result of the resilience from prevention improvements.

I. The project shall have been evaluated and have achieved most or all of its objectives.[1]

10. What was the reason for setting up the project? What problem(s) did it aim to tackle?

The increasing of cyber-attacks to entities which operates in Portugal along with advanced campaigns. Awareness and proactivity are one of the steps to improve the process of decreasing the national indicators.

11. Was the context analysed **before** the project was initiated? How, and by whom? Which data were used? (**Max. 150 words**)

[1] For more information on evaluation, see Guidelines on the evaluation of crime prevention initiatives (EUCPN Toolbox No.3): http://www.eucpn.org/library/results.asp?category=32&pubdate

Since Portuguese National CyberSecurity Centre (CNCS) starts, prevention and awareness were strategic goals at National level. To achieve these goals internally, CNCS creates this project that includes multiple human resources and some systems that are now up and running, collecting information regarding vulnerable systems and vulnerabilities advisories.

12. What were the objective(s) of the project? Please, if applicable, distinguish between main and secondary objectives. (**Max. 150 words**)

Main objective is:

- Decrease the number of vulnerable systems in cyberspace with direct impact on prevention and cyber-crime decrease.

Secondary objectives:

- Raise the awareness of entities which have information systems
- Automate report tasks
- Create a vulnerability central system
- Clean-up network information provided by Whois service from RIPE

13. Did you build in internal goals to measure the performance of the project? If so, please describe at what stage of the project and how you measured whether the project was moving in the planned direction. (**Max. 150 words**)

According to levels of indexes and classifications identified by CNCS (low, medium, high) it is intended that all State entities and critical infrastructures will be at medium level in a first phase.

14. Has there been a process evaluation? Who conducted the evaluation (internally or externally?) and what where the main results? (**max. 300 words) -** *for more information on process evaluation, see EUCPN Toolbox No.3, p.9-10 & part 2 - section 2A*

The evaluation is made by us using an external tool named Security Ratings Platform from BitSight Company. The tool has historical evolution charts to evaluate the decreasing & increasing of vulnerable systems. By now we have charts available for more than twenty entities and results are still being evaluated.

15. Has there been an outcome or impact evaluation? Who conducted the evaluation (internally or externally?), which data and evaluation method where used and what were the main results? (**Max. 300 words**) - *for more*

information on outcome or impact evaluation, see EUCPN Toolbox No.3, p.7-9 & part 2 - section 2A

The objective is to measure the increased level of systems and infrastructures security at national level which will reflect directly in quality services provided by entities to citizens.

II. The project shall, as far as possible, be innovative, involving new methods or new approaches.

16. How is the project innovative in its methods and/or approaches? (**Max. 150 words**)

Our approach is flexible, generic and can be implemented by any organization that has the same needs like other National Cyber Security Centres. The tools used are open-source and improve the automation in multiple tasks which will replace man power used in last years.

III. The project shall be based on cooperation between partners, where possible.

18. Which partners or stakeholders were involved in the project and what was their involvement? (**Max. 200 words**)

Stakeholder: Portuguese National CyberSecurity Centre Commercial Partners: BitSight IntelMQ tool partners: ENISA, CERT.AT, CERT.CZ, ContactDB tool partners: CERT.AT, CIRCL.LU

IV. The project shall be capable of replication in other Member States.

19. How and by whom is the project funded? (**Max. 150 words**)

Portuguese National CyberSecurity Centre

20. What were the costs of the project in terms of finances, material and human resources? (**Max. 150 words**)

Duration of project will be 2 years The following values are annually described: Human resources (operation and maintenance): 2 FTE Cost per human resource (FTE): €24.000 IRD (Investigation Research and Development): 0.30 FTE Internal Infrastructure Costs: €40.000

External Infrastructure Costs: €20.000

Logistic: €5.000

21. Has a cost-benefit analysis been carried out? If so, describe the analysis, including how and by whom it was carried out and list the main findings of the analysis. (**Max. 150 words**)

No. Since the project is still running, costs haven't been evaluated.

22. Are there adjustments to be made to the project to ensure a successful replication in another Member State?

No need for adjustments.

23. How is the project relevant for other Member States? Please explain the European dimension of your project.

Cyber security awareness and prevention of vulnerable legit systems being use to crime are at the moment a priority in terms of national security for any Member State according to European Union Cyber Security Strategy.

Please provide a short general description of the project (abstract for inclusion in the conference booklet – **max. 150 words**).

CHAOS focuses on prevention and improvement of the health of Portuguese cyberspace through communications and alerts to reduce the cyber-attacks surface and support entities with the technical and procedures information.

Therefore, the CHAOS platform in National CyberSecurity Centre is being developed to prevent vulnerability exploits in Public Administration, Critical Infrastructures and important systems available in Portuguese cyberspace. The platform will support multiple tasks, like sending alerts of vulnerable systems detected in cyberspace and new found software and hardware vulnerabilities, recommendations to improve the security of systems and infrastructures, and monitoring the systems and networks in each entity to generate periodically a "reliability indicator" at a national, sector and entity level.