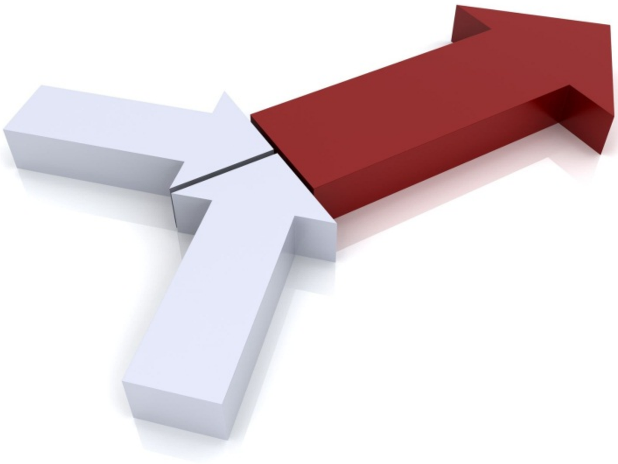
European Network and Information Security Agency



CERT Operational Gaps and Overlaps

Report, December 2011

Contributors to this report

The report production was commissioned to Deloitte (Belgium).

Editor: Agris Belasovs (ENISA)

Contributor: Marco Thorbruegge (ENISA)

Acknowledgements

We wish to thank all the 20 CERTs that responded to the initial survey and the following teams for providing additional input during later interviews:

- CERT Bulgaria
- CERT-BUND
- CERT.GOV.PL
- Danish GovCERT
- IRISS-CERT
- mtCERT
- TF-CSIRT

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of expertise for the European Union (EU), its Member States (MS), the private sector and Europe's citizens. As an EU agency, ENISA's role is to work with these groups to develop advice and recommendations on good practice in information security. The agency assists MS in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. In carrying out its work programme, ENISA seeks to enhance existing expertise in MS by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

Contact details

For contacting ENISA for general enquiries on CERT-related matters or this report specifically, please use the following details:

- Email: cert-relations (at) enisa.europa.eu
- Internet: http://www.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 ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. 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.

Reproduction is authorised provided the source is acknowledged.

Contents

1 Executive summary

This document analyses the operational gaps and overlaps of national/governmental CERTs and provides some reccomendations. Recommendations made in this report represent the results of the analysis of input gathered from the relevant external stakeholders (European CERTs) and give additional ideas for ENISA experts to consider when planning future ENISA activities.

Recommendations made in this report in no way indicate that ENISA has commited itself in any way to undertake any specific activity or recommended action. Decisions on implementing specific recommendations are subject to the normal process of planning ENISA's activities, which takes into account the priorities of different stakeholders, required and available resources, etc.

After initial desk research, a survey was held with the EU national /governmental CERTs to determine which services are provided, which are required, and where the CERTs themselves see the most opportunities for improvement. This consultation also provided the opportunity for the participating stakeholders to share individual views in the comment fields. Several surveys responses were followed up afterwards with interview calls in cooperation with ENISA, during which the context in which the answers were given was further explored and further in-depth discussions were held. The output from the study was condensed into 17 recommendations:

- Aggregation of announcements and alerts & warnings
- Stimulating and providing means to centrally exchange information on alerts & warnings among CERTs
- Providing CERT communications channels
- International incident coordination
- CERT membership services
- Support to malware analysis services
- Industry partnerships
- European institutions CERT
- Providing specialised training
- Joint tool development
- Single point of contact for the national/governmental CERT community
- Closed CERT-community contacts directory
- Incident classification and reporting standardisation
- Harmonisation of legal framework for information sharing and international incident handling
- CERT process guidance
- Cooperation with bodies such as TERENA
- Guidance and direction on detected trends

For each of the recommendations, this report includes an overview of the observations which led to the recommendation, the detailed actions recommended, and the perceived support basis from the CERT community as well as compatibility with ENISA's mandate.

Based on the input collected from the stakeholders and our professional judgement, we believe the following **five key recommendations** should be considered by ENISA first:

1. Guidance and direction based on observed trends
2. Harmonisation of legal framework for information sharing and international incident handling
3. Providing specialised training
4. Industry partnerships
5. Providing CERT communication channels

2 Introduction

2.1 Target audience

The primary target audience for the recommendations in this document are ENISA's CERT experts and the CERT community (for information).

2.2 Report objective

Under its mandate ENISA has been tasked with analysing how CERT cooperation can be further facilitated on a European level, by examining operational needs and whether overlaps exist. This activity is framed as part of WPK 1.4 'Support CERT (co)operation on European level' in its Work Programme 2011[1].

The purpose of this study is to identify actions that ENISA could undertake to support and facilitate CERTs in dealing with operational gaps and overlaps. It should be however noted that ENISA does not commit to undertaking any of the recommended actions, but will consider these recommendations when planning future work in this area taking due account of available resources.

In this context, the key objectives of this study and report are to:

- Analyse the operational activities that the national/governmental CERTs carry out in order to provide essential services to their constituencies. The following activities are considered as essential:
    - Incident Handling (including cooperation with external stakeholders);
    - Alerts & Warnings (also referred to as dissemination of NIS relevant information);
    - Artifact handling.
- Investigate how ENISA can support and facilitate the operations of others (in this case the CERTs) by their own activities, taking into account that ENISA does not have an operational role by mandate, but may be very well suited to support operative tasks of the Member States and other stakeholders in agreement with them.
- Derive suggestions for future activities by ENISA that could:
    - complement and facilitate, on the European level, activities carried out by national/governmental CERTs (gaps);
    - streamline and facilitate, on European level, activities carried out by national/governmental CERTs (overlaps).

2.3 Context

We live in a world where the risks relating to cyber attacks are ever-growing, and where threats from unknown sources are dynamic and constantly evolving. Reports on significant security incidents are more prominent in the media than ever before, illustrating that there is an increasing need for the

[1] ENISA's work programme 2011: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011

effective and efficient management of cyber security. Computer Emergency Response Teams (CERTs)[2] play an increasingly important role in this as they are responsible for collecting information about and coordinating the response to cyber security incidents.

Certain ICT systems and networks form a vital part of the economy and society of Europe and its Member States. For this reason, they are generally regarded as Critical Information Infrastructures (CIIs) as their disruption or destruction could have a serious impact on vital societal functions. More specifically, CIIs are those systems that provide the resources upon which all functions of society depend; for example telecommunications, transportation, energy, water supply, health care, emergency services, manufacturing and financial services, but also essential governmental functions. Because of this, every single country that is connected to the Internet has an interest in implementing capabilities to respond effectively and efficiently to information security incidents, and to protect these essential functions from a national security perspective.

Initially CERTs were set up mostly to provide security incident management services for particular private sector or academic constituencies. However, an emerging need for national and governmental CERTs has presented itself to support incident management across a broad spectrum of sectors within a nation’s borders. Moreover, national/governmental CERTs have become a key component in the implementation of cyber security and Critical Information Infrastructure Protection (CIIP) at national level.

The aim of a national/governmental CERT, from a cyber security perspective, is to protect national and economic security, the ongoing operations of a government, and the ability of critical infrastructures to continue to function. Many Member States have recognised the need for a national/governmental CERT and are currently implementing such a capability. ENISA’s CERT expert group is actively supporting the Member States that are ramping up such capabilities by organising information sharing meetings, sponsoring specific training for CERT staff and also publicising reports which aim to help start up or organise a CERT’s operations. This activity is driven by ENISA’s mandate to support CERT (co)operation on European level.

Internet communications and cyber attacks are not bound by the physical frontiers of a nation and as a consequence not all security incidents can be handled locally by one CERT. International cooperation between the CERTs of different Member States may be required and it is recognised that a lack of efficient international cooperation is currently limiting the effectiveness of the CERT community as a whole. ENISA’s work programme for 2011, WPK 1.4, states that ‘ENISA will focus on how cross-border collaboration (of CERTs and other stakeholders) can be reinforced (with regard to incident response coordination and other issues)’.

In combining both the support to the CERT operations and the enhancement of CERT cooperation, ENISA is looking for current operational gaps and overlaps in the different national/governmental CERT organisations. While ENISA is not mandated to have an operational role, this report will investigate how ENISA can support and facilitate the operations of others by their own activities. In order to maximise the gains for the CERT community and constituency as a whole, this report will focus on what are considered to be essential CERT services.

[2] It should be noted that in general the terms CERT and CSIRT (Computer Security Incident Response Team) are often interchanged, where the first is actually a registered trademark of Carnegie Mellon University.

3 Methodology used

As a first step in this project desktop research was performed on the operational activities that the national/governmental CERTs in Europe carry out to support their constituency. During the desktop research phase, some potential gap or overlap candidates were identified (see 4.5 Initial Desk Research Conclusion).

As a next step in the project a survey was sent out to the different stakeholders who were jointly identified by ENISA and Deloitte. The survey polled the current services provided by the different services, the degree in which they cooperated with other CERTs in providing those services and furthermore on the cooperation they have with ENISA.

The structure of the survey was:

- Part 1: General questions on CERT mandate and team;
- Part 2: Questions on the services provided by CERT, considering the following three service categories:
    - Proactive services;
    - Reactive services;
    - Security quality management services.
- Part 3: Questions on services context;
- Part 4: A number of additional specific questions on three important services:
    - Alerts & Warnings;
    - Incident Handling;
    - Malware and artifact analysis.
- Part 5: Questions on cooperation and communication, at national and international levels.

Following the survey based on preliminary analysis of the survey results a one-hour follow up interviews were organised with selected stakeholders who had provided answers in response to the survey. The interviews were mainly focused on clarifying existing written answers and on validation of recurring ideas in the survey. The most common recurring ideas were:

- ENISA to help in the resolution of current hurdles in the legal framework
- Continuation of ENISA's efforts in the CERT process formalisation area. All interviewed stakeholders were also aware of the existing documentation such as the 'Baseline Capabilities' document series[3] published by ENISA
- The creation of a common malware hash database
- The aggregation of announcements by a central body for later distribution to the CERTs
- Industry partnerships where ENISA or another central body could act as a single point of contact. By joining forces, the CERTs could possibly have more leverage over large software vendors to request early warnings regarding software vulnerabilities.

And as a final step in the project analysis of all the gathered information was performed and results documented in the form of the report. This report represents the final result of the work carried out as part of this project.

[3] Baseline capabilities for national/governmental CERTs: http://www.enisa.europa.eu/act/cert/support/baseline-capabilities

4 Operational activities in essential services for national/governmental CERTs

4.1 Introduction

In this chapter the results of the desktop research, which was initial step of the project, are provided.

At the core of the service portfolio of most CERTs is typically the reactive incident handling capability. Around this core service, most CERTs offer a number of other services, both reactive and proactive or more supporting services. Some of these services are considered optional for national/governmental CERTs and others have become essential to the service offering, for example the provision of alerts & warnings with regard to current attacks, vulnerabilities, intrusion alerts, viruses, etc.

In order to structure the operational activities and services rendered by national or governmental CERTs, several service taxonomies were considered in the execution of this study of which the three most important are highlighted below.

Firstly, the widely recognised CERT Coordination Center (CERT/CC)[4] has created a broadly accepted and widely used overview of CERT service categories and services. However the overview is already several years old and does not specifically define what services are essential or what activities are particular to national/governmental CERTs. Furthermore, the activities that constitute a service have not been well defined. Certain services have overlapping activities but the CERT/CC overview does not fully reflect this.

The CERT CC services overview is shown in Table 1.

[4] CERT Coordination Center (CERT/CC): http://www.cert.org/certcc.html

Reactive services	Proactive services	Security Quality Management Services
➡ Alerts and Warnings ➡ Incident Handling • Incident analysis • Incident response on site • Incident response support • Incident response coordination ➡ Vulnerability Handling • Vulnerability analysis • Vulnerability response • Vulnerability response coordination ➡ Artifact Handling • Artifact analysis • Artifact response • Artifact response coordination	➡ Announcements ➡ Technology Watch ➡ Security Audits or Assessments ➡ Configuration and Maintenance of Security Tools, Applications, and Infrastructures ➡ Development of Security Tools ➡ Intrusion Detection Services ➡ Security-Related Information Dissemination	➡ Risk Analysis ➡ Business Continuity and Disaster Recovery Planning ➡ Security Consulting ➡ Awareness Building ➡ Education/Training ➡ Product Evaluation or Certification

Table 1: CERT/CC Services overview

Furthermore, Deloitte's operational Cyber Security Incident Management framework considers a broad array of possible services delivered to the constituency (based on the proactive and reactive services described by CERT/CC).

This framework includes the most essential reactive services such as incident handling, alerts and warning, as well as other reactive services such as vulnerability handling and artifact handling. Furthermore, it pays specific attention to the capability management activities required in setting up and running a CERT. The framework of services is depicted in Figure 1.

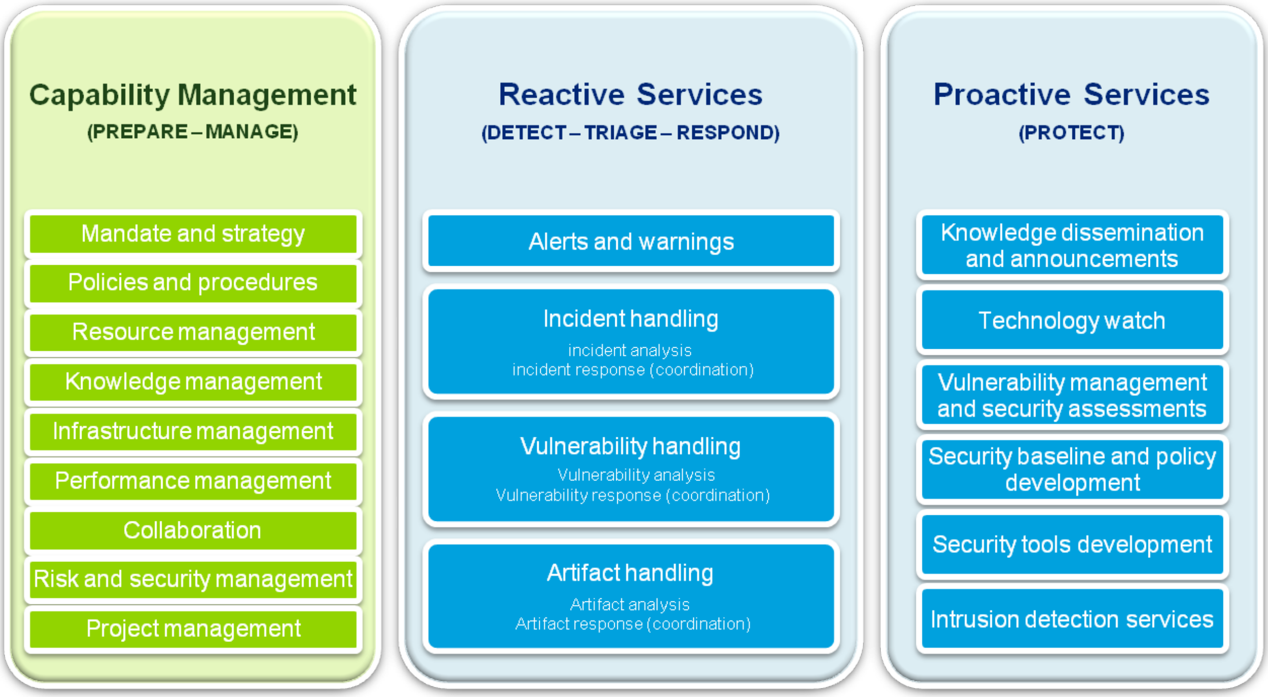

Capability Management
(PREPARE – MANAGE)
Mandate and strategy
Policies and procedures
Resource management
Knowledge management
Infrastructure management
Performance management
Collaboration
Risk and security management
Project management
Reactive Services
(DETECT – TRIAGE – RESPOND)
Alerts and warnings
Incident handling
incident analysis
incident response (coordination)
Vulnerability handling
Vulnerability analysis
Vulnerability response (coordination)
Artifact handling
Artifact analysis
Artifact response (coordination)
Proactive Services
(PROTECT)
Knowledge dissemination and announcements
Technology watch
Vulnerability management and security assessments
Security baseline and policy development
Security tools development
Intrusion detection services

Figure 1: Operational cyber security incident framework

Finally, prior ENISA work regarding CERT baseline capabilities regarding CERT services portfolios was also considered in structuring the stakeholder consultation and results presentation regarding operational activities.

In addition to the broad services and operational activities assessment, particular focus was given during this study to the following essential services, which are described below:

- Incident handling
- Alerts & Warnings
- Artifact analysis

4.2 Incident Handling

In describing the operational CERT activities regarding incident handling, reference is often made to the NIST Incident Handling Guide[5] (publication SP800-61 revision 1). This guidance document describes computer security incidents as ‘violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices’. The publication describes how such a CSIRT (computer emergency incident response team) should be organised, in which phases incidents should be handled and what types of incidents can occur.

The NIST guide also indicates that it is fairly rare for a team to perform incident response only. Teams might also offer alerts and warning services, vulnerability assessments and intrusion detection, among other services. The coexistence of these services in the different CERTs should be taken into

[5] NIST Computer Security Incident Handling Guide: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

account when determining the operational activities which support these services and how different services might be supported by common activities.

However, regarding the specific operational activities of incident handling, NIST identified four main phases:

- **Preparation:** Incident response methodologies typically emphasise preparation – not only establishing an incident response capability so that the organisation is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks and applications are sufficiently secure. By doing this, it will attempt to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments.
- **Detection and Analysis:** Detection of security breaches is necessary to alert the organisation whenever incidents occur. Proper analysis is needed to rule out false positives and to determine impact and containment strategies. This step includes the classification of the incident.
- **Containment, Eradication and Recovery:** When an incident has been detected and analysed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. Most incidents require containment, so it is important to consider it early in the course of handling each incident.
- **Post-Incident activity:** One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned.

These four phases can be broken down further into operational activities supporting the incident handling service lifecycle (taken from NIST SP800-61), as described below.

- **Preparation**
    - Maintaining a contact database with other CERTs (see **Figure 2**) for the different parties with whom communications might be required). This includes the maintenance of incident reporting facilities.

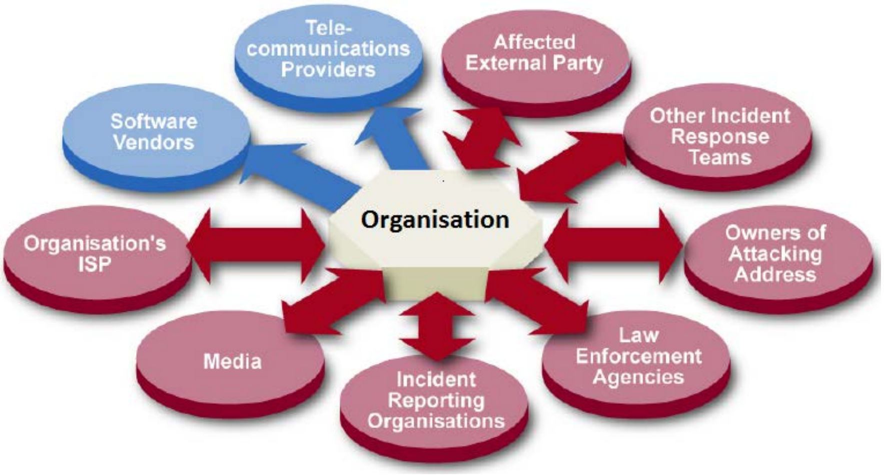

Tele-communications Providers
Affected External Party
Software Vendors
Other Incident Response Teams
Organisation
Organisation's ISP
Owners of Attacking Address
Media
Law Enforcement Agencies
Incident Reporting Organisations

Figure 2: Communications during an incident (From: NIST SP800-61)

-
    - Having the appropriate hardware and software standby for taking disk images, gathering log evidence, capturing network traffic, etc.

    - Maintaining a useable knowledge base of past incidents.
    - Maintaining network diagrams and lists of critical assets.
- **Detection and Analysis**
    - Maintaining and monitoring of the event and incident detection systems (including the configured filters, correlation patterns, sensors, etc.). These can include:
        - Operating system, service and application logs;
        - Network device logs;
        - Network-based, host-based, wireless, and network behaviour analysis IDPSs;
        - Antivirus, antispyware, and antispam software;
        - File integrity checking software;
        - Third-party monitoring service of an organisation's public services such as DNS or FTP.
    - Monitoring of so-called indicators:
        - Information on incidents at other organisations;
        - General threat-level indicators such as the SANS Internet Storm Center or the US Department of Homeland Security threat indicator;
        - Vendor-issued alerts on detected vulnerabilities or attacks occurring in the wild.
    - Analysis of incidents:
        - Initial analysis to determine scope, impact on systems and networks and origin;
        - Compare system and network behaviour vs. profile information to easier detect deviations from the expected behaviour;
        - Verify logs and audit trails;
        - Consult event correlation systems to determine possible impact or attack trail;
        - Consult the existing incident knowledge base (and update if necessary) (including online antivirus vendor databases, exploit databases and/or hoax information);
        - Use of Internet search engines for research on attacks/scans on unusual ports;
        - Use of network protocol analysers (e.g. Wireshark and Tshark, tcpdump);
        - Creation of a diagnosis matrix or 'cheat sheet' for less experienced staff;
        - Escalation to vendor or other specialised team.
    - Incident documentation;
    - Incident prioritisation;
    - Incident notification (see also Figure 2).
- **Containment, Eradication and Recovery**
    - Planning & coordination of containment strategy;
    - Planning & coordination of eradication strategy;
    - Planning & coordination of recovery strategy;
    - Information gathering using:
        - Knowledge bases;
        - Forensics/malware databases;
        - Monitor possible attacker communication channels;
        - Incident databases;
    - Attempting attacker identification;

  - Responding to the incident, aligned with the chosen strategy. Particular response activities include:
    - Taking action to protect systems and networks affected or threatened by intruder activity;
    - Providing solutions and mitigation strategies from relevant advisories or alerts;
    - Looking for intruder activity on other parts of the network;
    - Filtering network traffic;
    - Rebuilding systems;
    - Patching or repairing systems;
    - Developing other response or workaround strategies;
    - Legal actions against attacker:
      - Escalate information about incident/attacker to local authorities;
      - Escalate information about incident/attacker to international authorities (e.g. Europol).
  - Coordination with involved sites;
  - Re-evaluation of security incidents;
    - Downgrade incident severity/priority
    - Consideration of legal issues.
- **Post-Incident activity**
  - Lessons learnt documentation
  - Identification of possible organisational/tooling/staff skill improvements

4.3 Alerts & Warnings

Often there is some confusion between the alerts & warnings service, which is considered to be a reactive service, and the Announcements service, which is considered to be a proactive service. This was also confirmed during the execution of the study when interacting with stakeholders.

Alerts & warnings[6] involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any **short-term** recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CERT itself or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency. This clearly contrasts with **announcements**,[7] which inform constituents about new developments with **medium- to long-term impact**, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

The alerts & warnings service consists of the following activities:

[6] Alerts and Warnings service description: http://www.enisa.europa.eu/act/cert/support/guide/appendix/csirt-services#Alerts_and_Warnings

[7] Announcements service description: http://www.enisa.europa.eu/act/cert/support/guide/appendix/csirt-services#Announcements

- Definition of systems and networks of interest (i.e. systems and networks for which the constituency is interested in receiving alerts & warnings);
- Detection of:
  - intruder attacks;
  - security vulnerabilities;
  - intrusion alerts;
  - computer virus/malware;
  - hoaxes.
- Distribution of alerts & warnings to interested constituents;
- Providing any short-term recommended course of action for dealing with the resulting problem.

4.4 Artifact handling

A third essential service for CERT operations relates to artifact handling. An artifact[8] is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

The term ‘artifact handling’ was coined by CERT/CC in their description of possible CERT services. CERT/CC makes a clear distinction between artifact analysis, artifact response and artifact response coordination.

However, these terms are not encountered in practice. The different CERTs mostly refer to it as malware analysis. This indicates that there is a strong focus in practice on analysing the effects of malware, rather than creating signatures or coordinating response strategies with the software vendors. For the purposes of this document, the terms artifact and malware are interchangeable.

Artifact handling involves:

- Receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorised or disruptive activities;
- Gathering and validating information from anti-malware vendors (verification whether the malware type has been discovered and analysed);
- Review of the artifact in a sandbox environment:
  - Analysis of the nature, mechanics, version, and use of the artifacts:
    - Network profiling;
    - System profiling;
    - Reverse engineering;
    - Analysis in a honeypot environment.

[8] Artifact handling service description: http://www.enisa.europa.eu/act/cert/support/guide/appendix/csirt-services#Artifact_Handling

  - Developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts;

- Coordination with other interested parties, mainly by communicating an information bulletin and a hash of the malware.

4.5 Initial Desk Research Conclusion

In this chapter, the incident handling, alerts & warnings and malware and artifact analysis services were dissected into their typical activities, although delivery of these services can vary from one CERT to another.

During the desktop research phase, some potential gap or overlap candidates were identified:

- Currently, each CERT distributes **alerts and warnings** inside its constituency, based on the information it gathers either from internal systems or from other sources such as vendors or other CERTs. Distributing this information to the larger audience (outside current constituency) would not require a lot of additional resources. It has become clear that the distribution mechanisms can be considered to be duplicate work, as well as the development of the portal which hosts alerts & warnings.
- It is clear that **incident handling** can prove a complex process. As CERTs mature their operations, they will seek more repeatable processes. Further process guidance and formalisation assistance could be of considerable help to those CERTs that wish to advance their maturity.
- Furthermore, **international incident handling** can be burdened by the difference in legal frameworks which may impede collaboration between the different CERTs.
- **Analysis of malware** requires many specific tools, and not all tools available today are tailored to the needs of the CERTs. A common approach towards the development of such a toolkit could benefit the CERTs.

These candidate recommendations were verified during the survey and interviews carried out with the different stakeholders. Although not all points are considered to be purely operational gaps or overlaps, they are discussed in more detail in section 6, where gaps/overlaps and the relevant recommendations are considered (this section will go beyond the scope of the three services mentioned in this chapter).

Furthermore, for a given CERT providing the discussed services, some touch points between the services themselves have been identified. These items are potentially interesting for larger CERT teams, where dedicated team members work on separate services in isolation. There might even be overlaps within the teams as well.

- During the preparation phase of the incident handling service, the CERT organisation will, with the help of the constituency, **define the critical assets** to protect and make sure that the characteristics of these assets are accessible and known to the CERT staff. This step provides very useful information for the definition of the systems and networks of interest for the **alerts & warnings**.
- The **event monitoring** which is done during the incident detection phase can also provide relevant input for the **alerts & warnings** service. An example of this is a widespread attempt at port-scan systems of the constituency on an unknown TCP port.

- When the CERT team receives **incoming warnings** from the security feeds they are subscribed to and if this alert is deemed relevant, CERT staff should look at the **incident detection** systems to make sure that specific events which are congruent with the behaviour described in the incoming alert will trigger a relevant alert.

5 Analysis of the services offered

5.1 Introduction

The aim of this project was to develop recommendations on current gaps and overlaps in the operational aspects of the services provided by national/governmental CERTs, in order to complement and facilitate the current operations of the CERTs on a European level. A second objective was to investigate how ENISA can support the CERTs in their activities under ENISA's current mandate.

In order to collect adequate stakeholder inputs on these topics, a survey was made of the different services provided by a number of European national/governmental CERTs, as well as potential improvement areas. In particular, the survey aimed to determine which services are most commonly provided and where the CERTs themselves see the most opportunities for reducing overlaps and opportunities where ENISA could possibly support them. The survey also gave participants the opportunity to enter their personal views in open comment fields.

All (de-facto) national governmental CERTs were invited to participate in the survey, and 20 responses were received. This chapter presents the most important results of the survey and will provide insights into which services ENISA can impact the most by taking over certain tasks and/or by filling existing voids, as well as how ready the CERTs are to cooperate with other bodies for certain services.

5.2 Services provided

At the close of the survey, mainly CERTs responsible for governmental constituencies responded. The answers to this question were not mutually exclusive: the governmental CERTs can also have other constituencies but the mere fact that they are responsible for the governmental networks and systems validates the relevance of these answers to the objectives ENISA wants to attain (supporting national/governmental CERTs). This is shown in Figure 3.

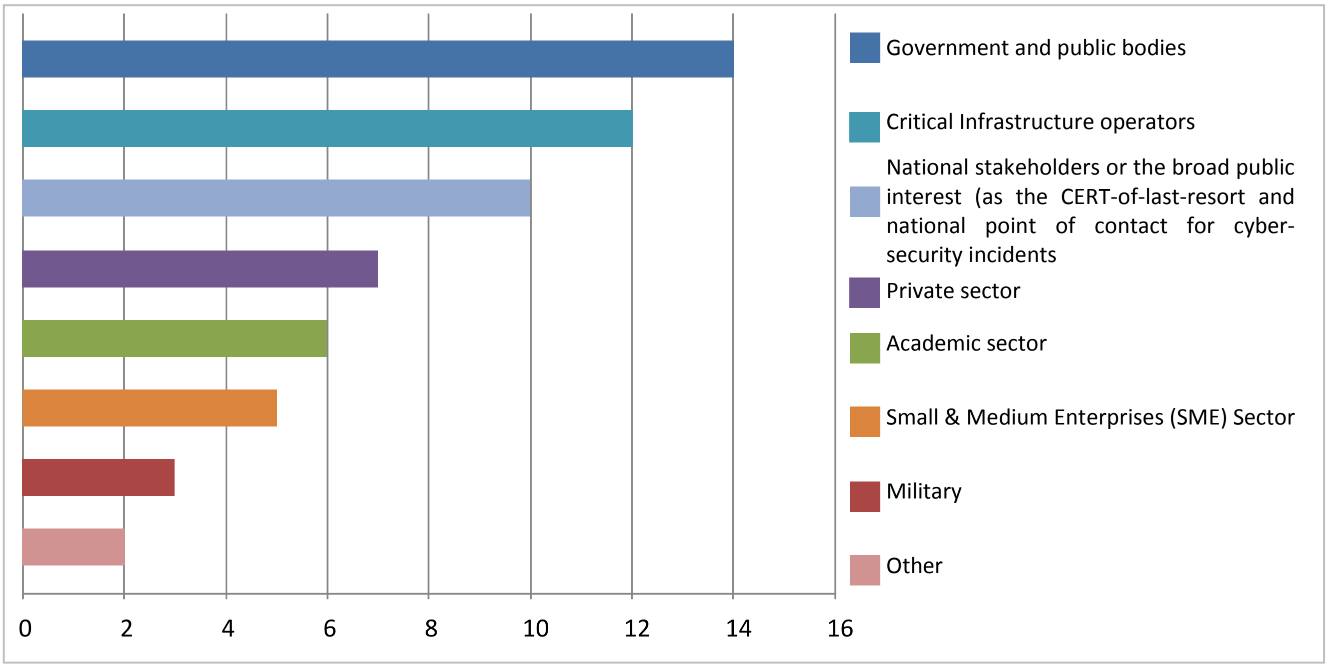


Figure 3: Constituency distribution

Numbers on the horizontal axis show the number of responding CERTs claiming to belong to the specific category (note: CERTs could choose more than one category).

Figure 4 indicates that the announcements service is offered by the most CERTs, followed by incident handling services. Alerts & warnings are performed by the majority of the respondents while only 40% of the respondents provide artifact handling services.

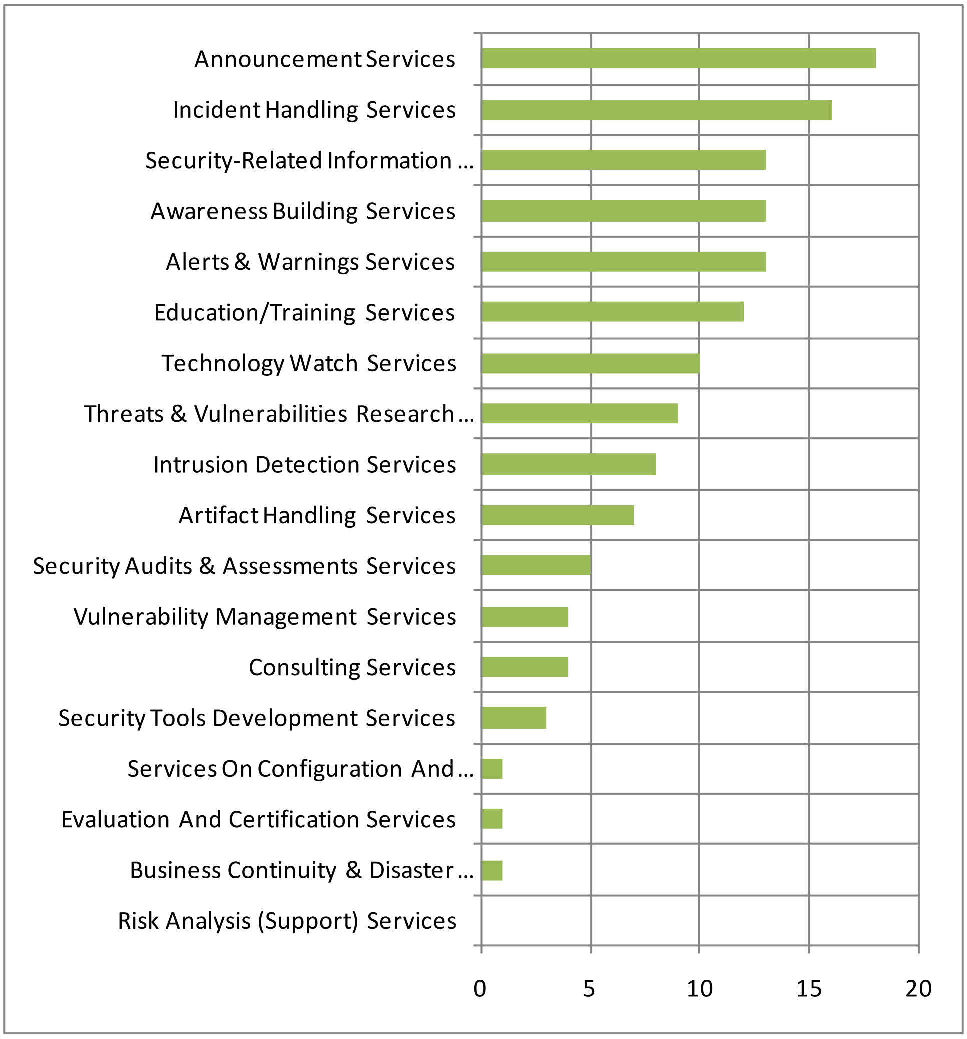


Figure 4: Services provided by the survey respondents

When the CERTs were asked to indicate which services were considered to be the most important (according to the constituency they serve), they named incident handling and alerts & warnings as the most important (shown in Figure 5).

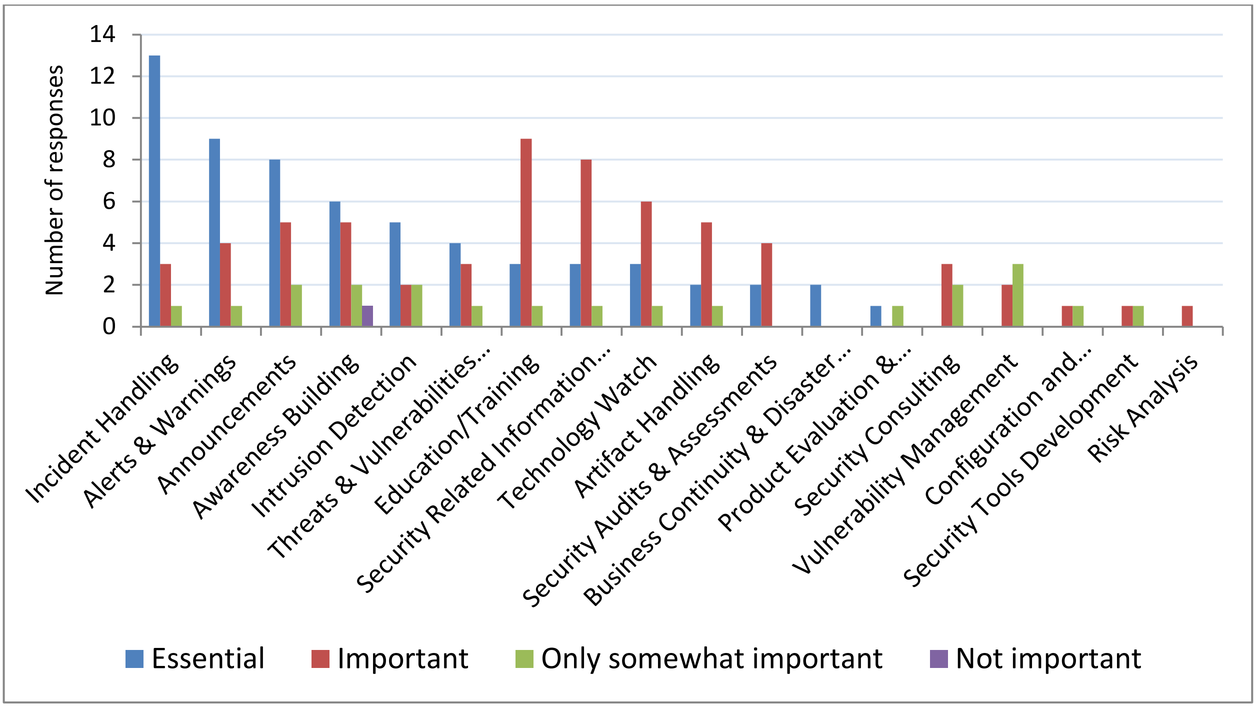


Figure 5: Services perceived as essential or important

This aligns with ENISA's perception as detailed during the scoping of this project. Announcement services are in third place and as they are the most provided service by the respondents (see Figure 4), this gives an opportunity for ENISA to support the CERTs in this activity.

The third service in which ENISA was specifically interested, artifact handling, is considered by the constituency to be rather important but is not in the top of the services. While this statement has not been verified, it is possible that the constituents do care for artifact handling but only within the scope of an incident occurring.

5.3 Synergies

When considering what services might be supported by ENISA, it is imperative for the success of such an initiative that the CERTs themselves are convinced of its usefulness. Without the buy-in of the CERTs, the consolidation of specific services on a central European level would probably not improve the CERTs' operations.

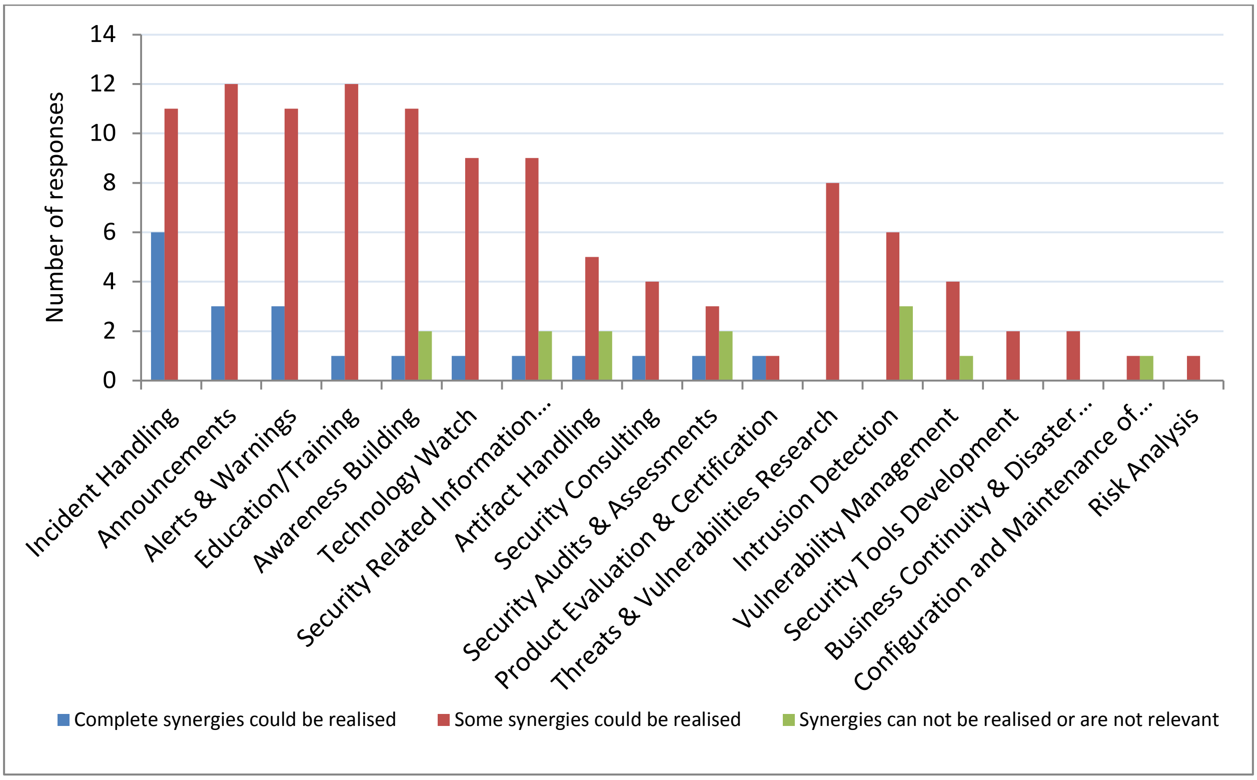


Figure 6: Services eligible for synergies

Based on the survey responses from the national /governmental CERTs, Figure 6 indicates that incident handling and alerts & warning services provide the most opportunity for at least some synergies with other CERTs or with central bodies (also note that none of the respondents indicated that there are no synergies possible).

This observation, combined with the fact that these two services are also considered to be the most essential services provided by the CERTs, implies a favourable context for ENISA to further support the CERTs in their operational tasks. Announcement services are also considered to be both very important and suitable for synergies. Artifact handling seems to provide some possible synergies, although there is no consensus on this, and two respondents out of 20 even oppose the idea of synergies in this area.

Figure 7 shows the current collaboration between the respondents and other European CERTs.

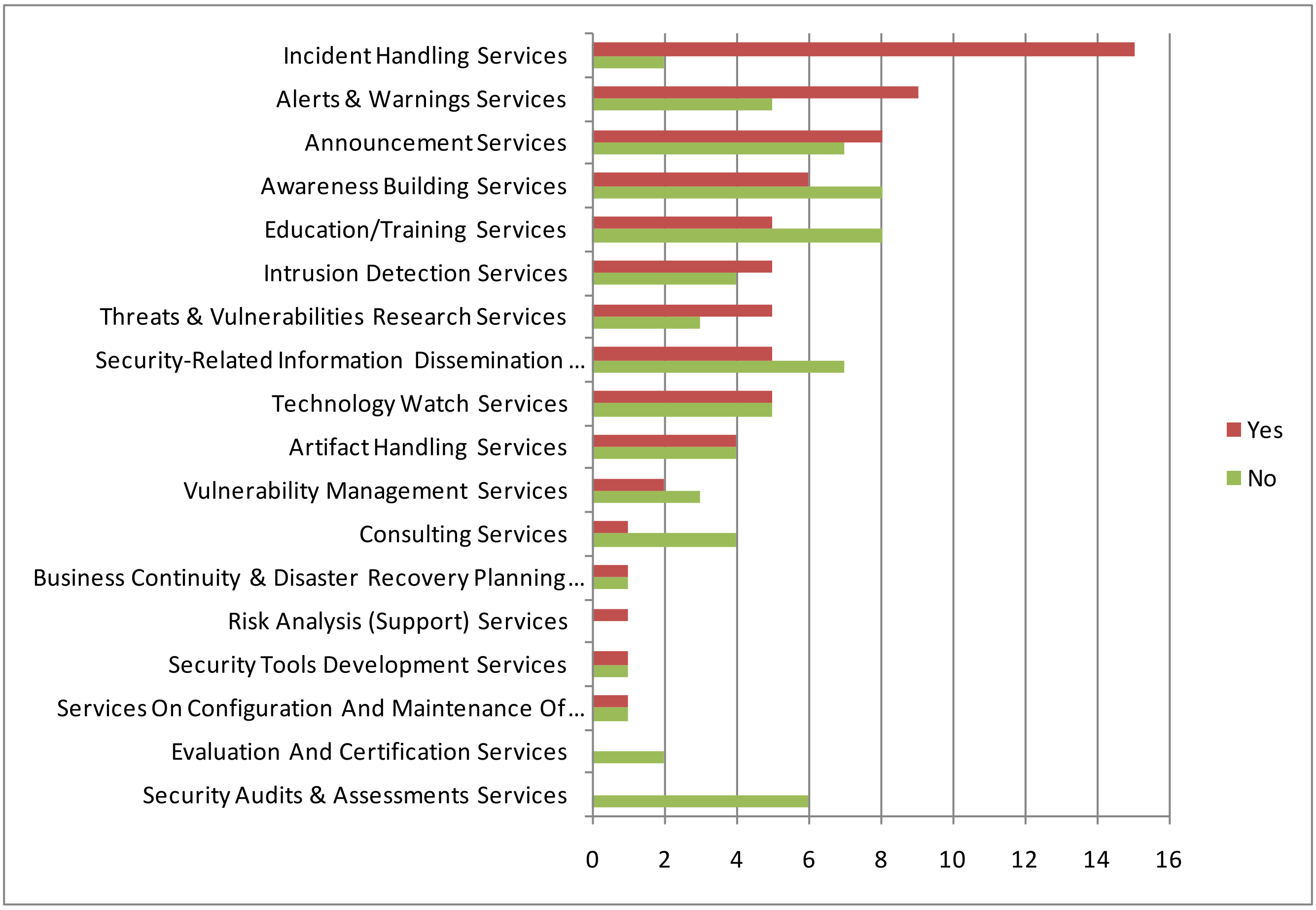


Figure 7: Current collaboration with other CERTs

It is interesting to compare the difference between their current collaboration on services and the services the respondents deemed eligible for synergies (Figure 6):

- Incident handling: Recognised as the service which is the most eligible for synergies, incident handling also appears to be the service on which the CERTs cooperate the most;
- Announcements: While 15 out of 20 respondents acknowledged the potential for synergies, only half of them actively cooperate on providing this service;
- Alerts & warnings: About the same number of respondents believe in the eligibility for cooperation compared to the announcements service, while more respondents are already cooperating;
- The same phenomenon is noticed for artifact handling.

Figure 8 shows the dependencies the respondents assessed they have on third parties in the provisioning of the different services.

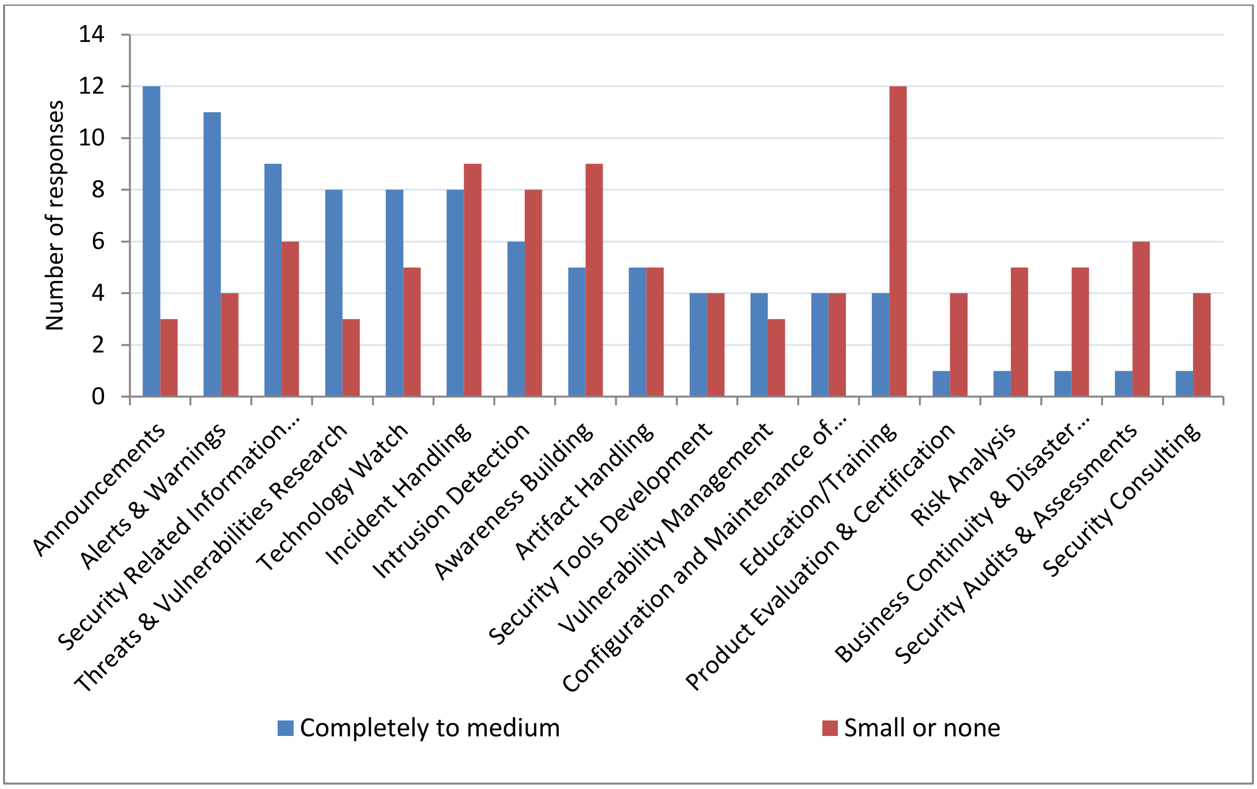


Figure 8: Dependency on third parties

The graph shows that the respondents consider announcements, alerts & warnings and to a lesser degree incident handling as services that depend on third parties, which reveals that they not only see the opportunity to cooperate with others on these services but also the necessity.

Special note was made of the threats and vulnerabilities research service, for which they consider themselves highly dependent on third parties. This seems logical, as it is something which is only provided by a couple of CERTs and requires dedicated resources and very specific skills.

This could indicate that CERTs may be interested in a central party that possesses these specific skills and that they can entrust with this task.

5.4 Maturity

In the survey, the different CERTs were also asked to assess the maturity of the different services they offered.

Figure 9 shows that the respondents have the most confidence in their announcement services and indicate decreasing maturity when the graph is elapsed clockwise.

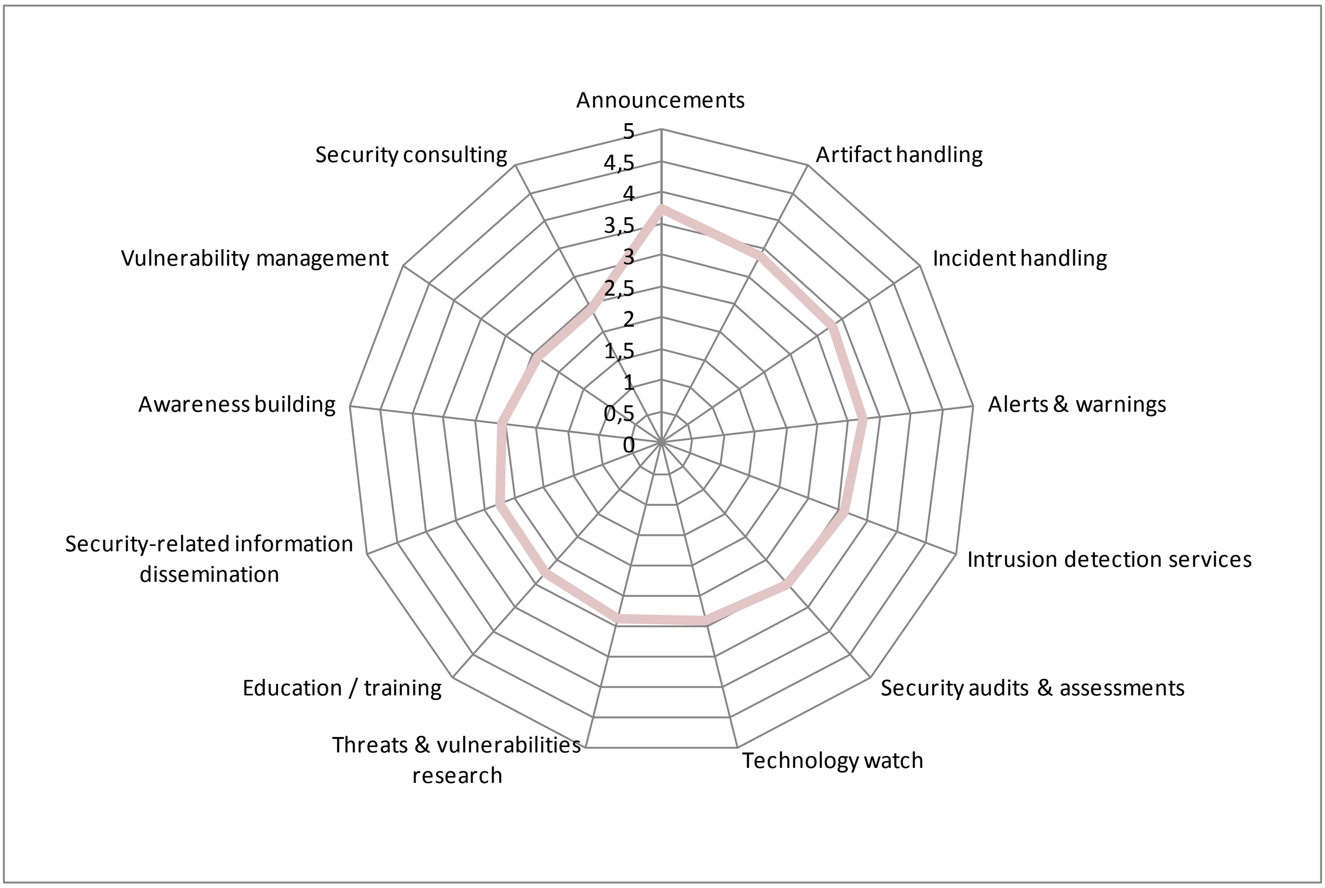


Figure 9: Self-assessment of service maturity

The purple line represents the collective data from all responses. Please note that the graph only contains answers for which five or more responses were given in order not to skew the results.

6 Gaps and overlaps

6.1 Introduction

The objective of this chapter is to zoom in on the recommendations following the analysis of the desktop research, CERT survey and clarifying interviews; and to point out to ENISA if there are possibilities to support and help the pan-European national/governmental CERT community from an operational services perspective.

During the analysis of the different CERT services, the survey responses and the interviews with the different stakeholders, many CERTs indicated areas of improvement, mainly in the inter-CERT cooperation. Many obstacles exist today, despite the different initiatives taken by organisations such as FIRST[9], TERENA[10] and ENISA itself.

Following analysis of the CERT survey, the recommendations highlight future activities by ENISA that could:

- complement and facilitate, on European level, operational activities carried out by national/governmental CERTs (gaps)
- streamline and facilitate, on European level, operational activities carried out by national/governmental CERTs (overlaps).

Each of the proposed recommendations needs to be considered in terms of the ENISA mandate, CERT gap/overlap and community readiness.

- ENISA does not have an operational role by mandate, but may be very well suited to support operative tasks in agreement with the Member States and other stakeholders. The 'ENISA mandate' characteristic verifies for each of the recommendations whether the proposed suggestion is covered by the current ENISA mandate or not.
- The 'CERT gap/overlap' characteristic specifies if the analysis based on the CERT survey pointed out that this recommendation is seen as a gap or overlap
- The last characteristic is the 'community readiness', which is a feasibility score out of three stars based on opinions, positions and ideas arising from survey results to provide an indication to ENISA of whether the community feels comfortable and is willing to work with ENISA on the suggestion.

The characteristics outlined above are indicators enabling ENISA to draw up a 'roadmap' of how to approach the CERT community with activities that can be complemented by ENISA or activities where the work of ENISA could contribute to avoiding redundancies.

The recommendations will be structured as follows:

[9] Forum of Incident Response and Security Teams: http://www.first.org/

[10] Trans-European Research and Education Networking Association: http://www.terena.org/

<table>
<tr><th colspan="3">Summary of recommendation</th></tr>
<tr><td>Gap or overlap</td><td>CERT community acceptance 🟦🟦</td><td>ENISA mandate support 🟦🟦🟦</td></tr>
<tr><td colspan="3"><i>Observation</i>
This part of the text will describe the different observations made which support the recommendation made. Observations will be based on the analysis of the essential services, results from the survey and the input gathered during the interviews.</td></tr>
<tr><td colspan="3"><i>Recommendation</i>
Based on the observations, this section will detail one or more recommendations. Every recommendation will receive a score indicating the support of the CERT community for such an initiative.</td></tr>
<tr><td colspan="3"><i>Mandate support</i>
Finally, a statement will be made on whether or not the recommendation is supported by ENISA's mandate.
ENISA's initial mandate is defined in regulation EC/460/2004.[11] This mandate has been extended as-is until September 2013 by regulation EU/580/2011 [12] while the Commission's proposal for ENISA's mandate[13] is debated further.
To align as closely as possible to the current and future objectives of ENISA, the mandate support section will be based both on the objectives of ENISA's mandate publication and the Commission's proposal dated 30 September 2010.</td></tr>
</table>

6.1.1 CERT community acceptance

This report aims to give a sense of how the CERTs surveyed perceived the identified gaps and overlaps and possible initiatives by ENISA. Rather than prioritising the different recommendations, we propose the notion of community acceptance as an indicator for its feasibility.

[11] Regulation (EC) No 460/2004: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[12] Regulation (EU) No 580/2011: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:165:0003:0004:EN:PDF

[13] COM(2010) 521 final: http://www.coe.int/t/DGHL/STANDARDSETTING/T-CY/Proposal%20new%20regulation%20ENISA.pdf

Every recommendation will be rated according a three-scale scoring system, for which a legend is provided below:

🟦	**'Low degree of acceptance'**: The recommendation is supported by a few stakeholders only. Other stakeholders may not see the relevance of the idea, or may even oppose it.
🟦🟦	**'Medium degree of acceptance'**: The recommendation is supported by several stakeholders and would not, according to the input gained during the survey and interviews, cause a large degree of resistance in the CERT community. However, some stakeholders have indicated that they are neutral towards the idea or may not see its relevance.
🟦🟦🟦	**'High degree of acceptance'**: The recommendation received a large degree of support among the stakeholders and no stakeholder opposed the idea.

6.1.2 ENISA mandate support

The ENISA mandate support score indicates to what degree the recommendation is supported by the current ENISA mandate.

Every recommendation will be rated according to a three-scale scoring system, as shown below:

🟦	**'No mandate support'**: The recommendation is not supported by ENISA's mandate. For the recommendation to be implemented, a large change in the mandate may be required.
🟦🟦	**'Partial mandate support'**: The recommendation is supported by ENISA's mandate to a certain degree but not completely. For the recommendation to be implemented, a small change or additional nuance in the mandate may be required.
🟦🟦🟦	**'Complete mandate support'**: The recommendation is completely supported by ENISA's current mandate and requires no changes in the mandate for it to be implemented.

6.2 Recommendations

6.2.1 Aggregation of announcements and alerts & warnings from external sources

Aggregation of announcements and alerts & warnings from external sources		
Overlap	CERT community acceptance 🟦🟦	ENISA mandate support 🟦🟦

Observation

Announcements and alerts & warnings are deemed to be very important services by the CERTs surveyed (announcement services being the most provided service, according to Figure 4).

It was observed that less than 40% of the CERTs currently collaborate on announcements and less than 30% on alerts & warnings. When polled about the possibilities, the majority of the respondents believe that synergies are possible both for announcements and alerts & warnings, as explained in section 5.3.

Furthermore, it became clear that the CERTs are sourcing their announcement information from a common set of sources (vendor websites, mailing lists such as Full Disclosure or even the announcement feeds published by other CERTs).

Recommendation

ENISA could research and propose an information intelligence framework which it could provide as a service to the CERT members on a pan-European basis and consisting of the following sources:

- Open-source such as US-CERT,[14] SANS ISC,[15] NVD;[16]
- Commercial sources;
- Own sources by using the CERT information nodes in the Member States.

ENISA could parse and present this information in an aggregated feed to the different CERTs that wish to make use of it. The feed could either be offered within the closed user group of pan-European national/governmental CERTs or it could be decided to make the information portal publicly accessible. ENISA does not commit to undertaking any of the recommended actions, but will consider these recommendations when planning future work in this area taking due account of available resources

An open and interoperable feed of this information that is configurable would be a bonus to stimulate interactions amongst the community members. The feed would allow CERT community members to automatically capture it as intelligence feed and feed it as an automatic

[14] US-CERT: http://www.us-cert.gov/
[15] Internet Storm Center: http://isc.sans.org/
[16] National Vulnerability Database: http://nvd.nist.gov/

Aggregation of announcements and alerts & warnings from external sources

input within the local security operations of the CERT to create value and increase the efficiency and effectiveness of their CERT services as a whole.

An important factor in the success of such an initiative is the detail of the information provided, the format and applicability to the assets in each CERT's constituency. Any problems could be overcome by providing a standardised reporting format for the different announcements and by providing the possibility for the CERTs to filter on the incoming messages. Furthermore, the information should provide independent disclosure and vendor neutrality by including as many objective sources as possible. The completeness of information should be ensured by including as much coverage as possible about one vulnerability instead of only the vendor-issued bulletin. Furthermore, information should be focused on the constituencies of the European CERTs, as opposed to the focus of sources such as DHS and US-CERT on their constituency.

One interviewee was rather pessimistic about the success of such an initiative and indicated that the CERTs would be wary of such an initiative for two reasons:

- The supposed unwillingness of the CERTs to divulge their sources of information. Some of the information sources might be underground channels. The presence of multiple CERTs or non-trusted parties could alert the users of such channels, effectively reducing the value of the information disclosed on those platforms. The CERTs would therefore continue to scrape these sources individually.
- The CERTs currently have the responsibility of gathering and filtering vulnerability and threat information for the different constituency systems, based on their own judgement. While relying on central feeds is an interesting option, it does not relieve the CERTs of accountability for gathering correct information. Clearly, this issue is something that can only be resolved by building trust among the CERTs in the completeness and accurateness of such a service.

However, these reservations should not be considered as major obstacles towards implementing such a recommendation. The CERTs that wish to do so can still rely on their own sources which they do not want to divulge and continue scraping their own sources while subscribing to the central feed. When they see that such a central feed can be relied upon, they might increase their dependence on such a feed.

Alternatively, it was mentioned that the different CERTs can continue to source information from each other while reducing their own efforts by making arrangements for following specific information sources. For example, a certain CERT might be appointed by a group of CERTs to watch all Microsoft-related announcements on the vendor website and to publish them in a standardised format to the other members of the group. This way, each CERT still possesses all necessary information on security announcements while duplicate efforts are reduced.

Finally, one stakeholder indicated they used the WARP platform in the past, when it was offered as a managed service by the British government. For a fixed fee, they provided a collaboration platform based on SharePoint with specific workflows and tools for CERT activities such as request tracking for incidents. In addition, as part of the service the users of the WARP received vulnerability feeds which were harvested by dedicated staff from the usual channels such as vendor websites or mailing lists. As such, the stakeholder only had to invest time in identifying issues local to the constituency. This service was discontinued and it was suggested that ENISA

Aggregation of announcements and alerts & warnings from external sources
could investigate hosting an independent WARP platform, given enough interest from the community. Not only would this be beneficial to the community, it could also help encourage the formation of smaller CERTs by providing a cost-effective way to start providing services. To avoid duplicated efforts current relevant activities of CERT-EU[17] should be taken into account when considering implementation of this recommendation.
Mandate support Based on the ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted task: *(e) Contribute to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users by, inter alia, promoting exchanges of current best practices, including on methods of alerting users, and seeking synergy between public and private sector initiatives* Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted task: *(c) Assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data* In line with these mandated tasks, ENISA will assist in the collection of timely and objective data by disseminating the most relevant announcements, alerts & warnings for the European constituency to the different CERTS. By doing this, ENISA can help the national/governmental CERT community (and their constituents) in assessing the risks for their constituency. However, the mandate is rather vague about the degree to which ENISA can assist the Member States in their day-to-day operations of collecting information.

[17] The EU Institutions CERT: http://cert.europa.eu/

6.2.2 Stimulating and providing means to centrally exchange information on alerts & warnings among CERTs

Stimulating and providing means to centrally exchange information on alerts & warnings among CERTs

Gap	CERT community acceptance 🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

Currently, information sharing is only done in clusters of CERTs that trust one another and mostly on an informal basis (an email to a select number of recipients, for example). Traffic Light Protocol[18] is a mechanism often used to indicate the severity of the alerts and the distribution chain to use for alert bulletins.

The respondents agree that trust is the foundation required to distribute such alerts and, even then, certain details cannot be shared depending on the situation. The formation of trust is an informal and typically slow process which means that clusters of CERTs share this information based on long-standing relationships, perhaps complemented by personal contact between two staff members.

Because of this, respondents see a benefit in a single point of contact which can distribute alerts and warnings in a less trusted but known community (for certain alerts, such as the GREEN alert as described above).

Recommendation

ENISA, currently already involved in community-forming activities for the CERTs, can play a role as a central dissemination point for alerts & warnings. Such a distribution mechanism could possibly provide both a secure channel to the different CERTs and a centralised, pre-validated address list of the different CERTs.

The key to the success of this initiative would indeed be the trust that the different CERTs place in this community and the degree to which they are prepared to share information with the community. However, CERTs will not be prepared to divulge to ENISA which CERTs they trust the most or indicate which CERTs are trusted less than others (for obvious political reasons).

The interviews revealed that trust is only a part of the equation; the other part is the fact that CERTs may be keener on sharing information when they see that they will receive interesting information in return. By sharing incident information, they will add to the collective knowledge of the community while gaining access to the ENISA dataset for themselves. The overall goal should be to stimulate the security incident information exchange and build a foundation from which members of the national/governmental CERT community can constructively and

[18] Traffic Light Protocol description: https://www.enisa.europa.eu/act/cert/support/incident-management/browsable/incident-handling-process/information-disclosure#Traffic%20Light%20Protocol

Stimulating and providing means to centrally exchange information on alerts & warnings among CERTs

cooperatively learn from one another. Such an initiative can be technically supported via a central portal or mailing list, as described in the next recommendation (section 0).

ENISA will have to play a role in ensuring that the information sharing relationships with the different CERTs in the community are, and remain, bidirectional Should the CERTs be more comfortable with sharing and exchanging specific information in an anonymous manner (as with the NEISAS model[19] approach), ENISA can further facilitate the bidirectional relationship by provided anonymisation. In this case, ENISA will distribute information to the community without mentioning the originating CERT.

Another ENISA initiative could be to suggest a common alerting concept for the CERT community. In case of a disaster or a major cyber attack the national/governmental CERTs have to use a communication medium to inform and help their constituency with the next steps. This is done very much with the focus on local initiatives. In this case, ENISA could leverage from existing smart incident notification and alerting mechanisms within the CERT community and other commercial initiatives. It is important for ENISA to learn from existing techniques and then increase the maturity of other CERT members in the community by leverage and offering these techniques to a broader set of members.

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted task:

> *(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues*

Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted tasks:

> *(b) Facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents;*
>
> *(c) Assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data;*
>
> *(g) Support cooperation between public and private stakeholders on the Union level, inter alia, by promoting information sharing and awareness raising, and facilitating their efforts to develop and take up standards for risk management and for the security of electronic products, networks and services*

ENISA has the mandate to stimulate and help the community in information sharing practices

[19] National & European Information Sharing & Alerting System: http://www.neisas.eu/

Stimulating and providing means to centrally exchange information on alerts & warnings among CERTs

between the members of the community to ensure reliable and actionable data is exchanged in a structured, open, trustworthy and secure way.

6.2.3 Providing CERT communications channels

Providing CERT information channels

Gap	CERT community acceptance 🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

When respondents were asked about their current communication channels within the community, they agreed unanimously that communications are currently both trust-based and email-driven. The respondents indicated their preference for contacting their peers directly via personal addresses and after a trust relationship has been built (during previous collaborations or meetings). A typical example mentioned of information to be shared relates to alerts & warnings which can be distributed to the CERT community, in addition to their own constituency.

One particular case was observed where a respondent indicated his awareness of mailing list set up by ENISA for the CERT community but was advised against using it for information exchanges with the community at this stage.

Recommendation

For security information to be exchanged productively between multiple parties (i.e. members of the CERT community), secure and trusted communications channels are essential. While these methods are not technologically advanced, stakeholders feel very comfortable communicating over PGP-encrypted email and IRC; they do not consider new secure communications channels a priority.

Such information sharing channels can vary from a closed mailing over secure web portals to custom-designed collaboration platforms that can support standardised CERT workflows. One stakeholder indicated that simplicity is key in crisis communications: he saw no value in new technology or tooling but did mention the possibility for ENISA to store up-to-date PGP keys to facilitate encrypted communications between the CERTs.

Furthermore, the platform should be specific to the needs of the national/governmental CERTs and not limited to that group: it should be open to any CERT wishing to participate. This contrasts with the EGC, which already provides a forum for the governmental CERTs and in which the members are highly trusted. As the EGC no longer accepts applications (in order to maintain the current level of trust, which disappears as soon as there is one member in the group who is not trusted), ENISA can provide value to the community with an alternative forum.

For those CERTs that wish to use it, ENISA can host information channels or even help in

Providing CERT information channels

designing a pan-European collaboration platform to help the community work together. It is acknowledged that TF-CSIRT[20] already provides such a means of communication for the European CERT community, but ENISA could provide a channel for non-accredited CERTs as well.

Such a platform should at least have the following characteristics:

- It should not be a data triage tool that sits close to the information sources, but an overarching environment used to build up an interactive repository of relevant security information (possibly incident-related), to share amongst the whole national/governmental CERT community.
- Distribution of such information could be supported by the traffic light protocol.[21] By allowing such input into the collaboration tool, the information could be disseminated automatically to the desired community members.
- By sharing information with the community, the CERTs will have the opportunity to prove their willingness in sharing information and this could result in stronger cohesion within the CERT community.
- As more information is added over time, the collaboration platform will structurally improve the capability and risk awareness of the community.

The collaboration platform should be built around a modular, scalable, robust and secure concept. Some key capabilities of a good collaboration platform concept should be: data management and integration, feeds and alerts, ticket management, fine-grained access control and flexible data import.

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted task:

> *(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues*

Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted tasks:

> *(b) Facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents;*
>
> *(c) Assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data*

[20] TF-CSIRT: http://www.terena.org/activities/tf-csirt/

[21] Traffic Light Protocol description: https://www.enisa.europa.eu/act/cert/support/incident-management/browsable/incident-handling-process/information-disclosure#Traffic%20Light%20Protocol

Providing CERT information channels
ENISA has the mandate to facilitate cooperation between the different Member States in preventing, detecting and responding to network incidents. Within this mandated task, it should be feasible for ENISA (given enough community acceptance), to operationally support such a cooperation.

6.2.4 International incident coordination

International incident coordination		
Gap	CERT community acceptance 🟦	ENISA mandate support 🟦🟦🟦

Observation

Respondents indicated they are experiencing difficulties when handling international incidents. Currently, there is no body that can take up central coordination of the incident handling or contact central bodies in the name of several CERTs (as Interpol does in the case of the police). The root causes of the difficulties are a lack of trust in each other's capabilities and the fact that the national legal frameworks on incident handling and information sharing in the different Member States are dispersed and unclear. Currently the CERTs exchange or receive information that is either informal or limited to bilateral or limited multilateral exchanges. One stakeholder indicated that CERTs do not share information unless specifically authorised by management and a legal counsel, out of fear of making errors; this is an obvious sign that the legal frameworks are unclear.

The situation is aggravated because constituents might be unwilling to share information internationally because they fear it will make them appear incapable of handling the attack or bring the fact that they have been targeted by an attack to the attention of an international crowd. Certain items related to national security are legally prohibited from being shared with incident handlers.

When asked about the feasibility of a central European body which could step in when international cooperation was needed, the community answered with a strong 'no'. However, when probed for more details, it appeared that the CERT community might show less resistance to activities that are less comprehensive.

Recommendation

As indicated, the general idea of a central body which would oversee international information security incidents and coordinate/manage the information exchange between the different CERTs was met with resistance. It stands to reason that if national security information cannot be shared with other Member States, the CERTs would not be prepared to share that type of information with a central body either. Furthermore, the CERTs feel that whoever contributes to the community and responds to incidents will prove themselves trustworthy enough to communicate directly with the other CERTs without the need for a central body.

Activities which were deemed acceptable by the stakeholders were:

- Dissemination of information on international incidents involving many (4+) Member States. Currently, information is only shared in one-on-one relationships between the different CERTs that trust one another. This recommendation is similar to 0 but applies to incident information. Dissemination can be done via communications channels as described in recommendation 0.

International incident coordination

- Improvement of collaboration between national and private bodies within the EU: ENISA is currently already doing this by participating in initiatives such as EFMS and EP3R.

Mandate support

This recommendation is not supported by ENISA's current mandated tasks as described in Regulation (EC) No 460/2004. However, based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted task:

> *(b) Facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents*

The Commission's proposal clearly contains the cross-border dimension and explicitly includes activities regarding the response to information security incidents. However, given the community's resistance to a coordinating/managing body, ENISA should investigate how it can support international information security incident response in a way that is acceptable to the community.

6.2.5 CERT membership services

CERT membership services		
Gap	CERT community acceptance 🟦	ENISA mandate support 🟦🟦

Observation

One respondent explicitly discussed the need for a new type of accreditation/affiliation system, other than the currently existing services from FIRST and TERENA (Trusted Introducer[22]).

First of all, the benefits of both existing instances are perceived as positive (they both offer a closed directory with contacts for all accredited/affiliated CERTs and all members enjoy a mutual degree of trust because the criteria for membership of these schemes demand a level of trustworthiness). However, it was indicated as being a handicap of the FIRST and TI schemes that they focus mainly on the organisational and operational maturity level. Therefore, it was suggested that a new accreditation scheme should be created and give a more technical skill-based indication of the capabilities of the different members.

Furthermore, the fee to join the existing schemes is perceived as a financial burden to the members, to such a degree that some consider it unfeasible to join both current schemes at the same time.

Recommendation

We recommend that ENISA investigates how the gap of technical accreditation can be filled and whether this is considered useful by the whole of the CERT community. If a new accreditation type could enhance cooperation between the different CERTs, it would certainly be commendable to do so. It was suggested that a common set of accreditation criteria be agreed on a European basis to assess specific technical skills such as the ability of staff to do technical assessments, and the presence of certain core skills.

This would as well help to weed out the 'minimal' CERTs that consist only of a phone number and an email address merely to comply with Europe's Digital Agenda,[23] which indicates that 'by 2012 a well-functioning network of CERTs at national level covering all of Europe should be established'.

Another possibility for ENISA is to support the existing schemes. TERENA recently launched the Trusted Introducer certification service, which has stronger requirements compared to the accreditation. Part of the certification system will be a credit scheme (similar to CISSP[24] or CISA[25] certifications for individuals) which requires regular training. ENISA could discuss with TERENA

[22] Trusted Introducer for Security and Incident Response Teams: http://www.trusted-introducer.org
[23] A Digital Agenda for Europe, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF
[24] CISSP - Certified Information Systems Security Professional: https://www.isc2.org/cissp/
[25] Certified Information Systems Auditor (CISA): http://www.isaca.org/CISA

CERT membership services

possibilities to contribute to these certification efforts, as they could provide ENISA with a valuable interface to the CERT community. It can be envisaged that ENISA would assist in the certification audits or help in meeting the criteria required for certification.

If ENISA wishes to develop a proper accreditation/certification scheme, it should align with the existing schemes and provide a way of achieving dual certification, i.e. enabling CERTs to be certified with ENISA and another scheme while only having to comply with one set of requirements.

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted task:

> *(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues*

Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted tasks:

> (c) *Support cooperation among competent public bodies in Europe, in particular supporting their efforts to develop and exchange good practices and standards*

In line with the mandate on cooperation facilitation and support, ENISA can provide such a membership scheme to the CERT community in Europe and enhance the building of trust and ease of contacting each other. However, the mandate mainly refers to the development of methodologies and good practice while the recommendation is mainly about building a reference framework in which equally mature CERTs can meet and build trust (and afterwards exchange such methodologies and good practices). Therefore, it is concluded that only limited mandate support exists.

It must be clarified that this could only be considered as a future service provided by ENISA if the Member States specifically ask for it.

6.2.6 Support to malware analysis services

Support to malware analysis services		
Gap	CERT community acceptance 🟦🟦	ENISA mandate support 🟦

Observation

Different CERTs have different tools and techniques to analyse malicious code (i.e. malware). Although the service is rather new, it seems that the CERT community could benefit from ENISA’s interaction to help bring all members up to the same level as the more mature members.

Malware prevention is a very time-sensitive activity: new malware strains are constantly appearing and as soon as the authors detect that end-point protection systems have identified these strains and possess signatures or other techniques to identify the malware, they evolve the malware strain. This time-sensitivity even reduces the cooperation abilities of the different CERTs, as they are unaware of which CERTs are analysing what kind of samples and where the threats are occurring.

In addition to the problems during analysis, preparatory tasks such as building virtualised infrastructures to create sandboxes for system and network profiling of suspected malware samples also appear to be tasks done by many of the CERTs individually, thus duplicating one another’s efforts.

Recommendation

ENISA could research and investigate how to overcome duplicated efforts in building virtualised infrastructures to create sandboxes. It could be considered too operational task for ENISA to offer the community a malware and artifacts handling service, where ENISA is hosting the sandbox (similar to http://www.sunbeltsecurity.com/sandbox/), which would allow the community to leverage an existing, mature and fully supported environment at a low cost. Managing an operational service with Service Level Agreements attached to it might become too complex and too resource-heavy for ENISA, at least currently.

Several CERTs (independently) communicated the idea of a common database of malware hashes which could be consulted by them, indicating who had spotted certain malware hashes, what actions were taken at the time and, more importantly, indicating when a certain malware specimen has been discovered and is currently being investigated by a certain CERT. Indicating this to other CERTs could further foster cooperation in the malware domain and allow for the creation of trust relationships between the CERT malware expertise in the CERT community. Team Cymru’s current hash database[26] already provides an inventory of known malware

[26] Team Cymru Malware Hash Registry: http://www.team-cymru.org/Services/MHR

Support to malware analysis services

instances and could be expanded to provide an oversight of malware instances under review (although not all stakeholders would be prepared to share that information).

It was suggested that to overcome the potential unwillingness of CERTs to share (targeted) malware information, ENISA could provide automated means for distribution of specific SNORT rules to the CERT community which they can activate on their IDS systems. CERTs would then be requested to call the originating CERT in case that specific SNORT rule fired for more information and perhaps to start joint analysis – this would enhance cooperation between the CERTs and would provide a more anonymised way for the different CERTs to share information on malware. Furthermore, individual CERTs indicated they have privileged relationships with anti-malware vendors (such as Symantec, F-Secure, etc.) because they are part of a larger body for national security. For the smaller CERTs, centralising a hash database might provide them with an opportunity to get early and/or privileged information from the vendors when requesting it through a central body representing the national/governmental CERT community of Europe. This recommendation aligns closely with the recommendation on industry partnerships (see 6.2.7).

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted tasks:

> *(a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission;*
>
> *(f) assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products*

Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted tasks:

> *(b) facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents;*
>
> *(c) assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data*

Both the current and proposed future mandates support the cooperation of CERTs, facilitated by ENISA in the analysis of current security risks. However, the development of tools or hosting of services to such an end is not described in the mandate.

It must be clarified that this could only be considered as a future service provided by ENISA if the Member States specifically ask for it.

6.2.7 Industry partnerships

Industry partnerships		
Overlap	CERT community acceptance 🟦🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

Of the different CERTs surveyed, only a few have good relationships with the software and hardware industry. Those that do are eligible to participate in specific vendor programmes which supply the CERTs with early warnings on discovered vulnerabilities in the software or upcoming patches. A clear link was discovered between the CERTs that are organisationally part of a national security organisation and those that have privileged contacts with the industry. As a consequence, such information appears to be available to only some of the CERTs on the basis of individual partnering agreements, while such information is useful to the CERT community as a whole.

One stakeholder mentioned that their entitlement to the early notifications was part of an enterprise agreement their parent organisation had with the vendor. Such enterprise agreements often comprise the purchase of software licences, maintenance, patches, upgrades and technical support. The same conclusion was drawn as for the privileged information: these agreements are based on individual contracts with each CERT instead of a common agreement.

Recommendation

ENISA can reduce the administrative burden of maintaining contacts with the main vendors and distribute received information through, for example, a joint cooperation platform to the different CERTs and their constituencies. Instead of the current individually agreed contracts, ENISA could (in agreement with the CERTs) represent the European national/governmental CERT community as a single point of contact with the most important software and hardware vendors. Agreements regarding the distribution of early information could be created between ENISA and the different vendors, after which ENISA could distribute to the different CERTs in a closed distribution system (as opposed to distributing this to the broad public). By doing this, ENISA could build additional trust between itself and the different CERTs but most importantly, jumpstart the smaller CERTs that do not have the necessary footprint, constituency or parent organisation to qualify for a privileged relationship with those vendors.

A variation on this idea was proposed by one of the interviewees: instead of ENISA focusing on all the software vendors, ENISA could facilitate an agreement with the different CERTs where each CERT would start to focus on different vendors. In this case, one CERT would specifically monitor all publicly available sources and use its relationship to gather all information on Microsoft and distribute this to the other CERTs to the extent allowed by their agreement with Microsoft (possibly through ENISA), while another CERT would for example focus on Cisco or VMWare. This would significantly reduce the individual effort made by the CERTs in mining this information while they would all still have access to the same information. This would require additional cooperation between the CERTs and could possibly help in building additional trust

Industry partnerships

between the different national/governmental CERTs. It is noted that not all vendors will appreciate the dissemination of information to the other CERTs with whom they have no relationship. It should therefore be verified to what extent information can be shared and which agreements should additionally be put in place. ENISA can certainly play a role in the negotiation of such agreements.

A special case to be mentioned is the relationship with anti-malware vendors. Several CERTs have good, informal relationships with the anti-malware vendors which they have created by submitting unknown malware samples, for which they request in return some information on ongoing investigations by the vendors. ENISA could centralise the contacts with those vendors and possibly integrate them in a central malware hash repository (see section 6.2.6). Further investigation will be needed to verify whether this trust in a specific CERT can be transferred to ENISA and thus to all the European national/governmental CERTs. The vendor would clearly require that ENISA carefully selects the organisations to which information is distributed.

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted task:

> *(f) assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products*

In the Commission's proposal for ENISA, COM(2010) 521 final, no specific task has been identified which outlines cooperation with industry.

The current mandate actively advocates dialogue with the industry. When looking at the proposed future mandate, there is no apparent trace of task (f) to be found.

6.2.8 European institutions CERT

European institutions CERT		
Gap	CERT community acceptance 🟦🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

A few respondents indicated they see a need for a CERT for the European institutions. This task was suggested to be fulfilled by ENISA. The CERTs were not aware of the current initiative (published in June 2011) in which ENISA already participates in the EU-CERT pre-configuration team.[27]

During the survey it became clear that the CERTs do see a role for ENISA involved in building a CERT for the EU institutions but they do not specify how they envision this – either as a supporting body or as the organisational host of the EU institutions CERT.

Recommendation

ENISA should continue looking into supporting efforts to set up an operational incident response capability which would have the EU institutions as constituency, similar to NATO's NCIRC (NATO Computer Incident Response Capability) which protects NATO's information assets locally and abroad in the theatres.

To this end, ENISA is already present in the EU-CERT pre-configuration team launched recently.

One stakeholder identified additional tasks for such a European CERT, such as a focus on threats at the European level, threats against critical (pan-European) network infrastructure, relationship building amongst Member State CERTs and also research into attack trends and security tools, techniques and processes.

Mandate support

In the Digital Agenda for Europe adopted in May 2010 (see IP/10/581, MEMO/10/199 and MEMO/10/200), the Commission committed itself to establishing a CERT for the EU institutions, as part of the EU's commitment to a reinforced and high-level EU Networking and Information Security Policy in Europe.

In August 2010 the Commission asked four cyber-security experts known as the 'Rat der IT Weisen' to make recommendations on how to set up such a CERT. Their report was finalised in November 2010, which was too late for it to be referenced in the Commission's proposal for ENISA.

While the current mandate of ENISA does not mention the creation of a European CERT or

[27] Cyber security: EU prepares to set up CERT for EU Institutions: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/694

European institutions CERT

assistance to the European institutions, the proposed mandate for ENISA specifies:

> *(i) Assist the Member States and the European institutions and bodies, at their request, in their efforts to develop network and information security detection, analysis and response capability*

This task statement, in combination with the statement in the Digital Agenda, is to be interpreted as a clear commitment towards the establishment of such a EU CERT. Including ENISA in the pre-configuration team is an acknowledgement of ENISA's role as expertise provider in information security, but its further role in the deployment of the EU Institutions CERT capability has yet to be defined (the task description only says 'assist in developing', not hosting).

With regard to the recommendation that ENISA focuses on European threats and researching techniques and tools, the current mandate provides clear support for this:

> *(a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission*

6.2.9 Providing specialised training

Providing specialised training		
Gap	CERT community acceptance 🟦🟦🟦	ENISA mandate support 🟦🟦

Observation

Echoing the observation made in section 6.2.5 regarding accreditation, one respondent indicated that the current TRANSITS-I[28] training provided by TERENA is not of sufficient technical depth (this training as well as more technical TRANSITS-II[29] course is already supported by ENISA, both financially and by providing exercise material). Current training is considered too focused on the operational aspects of CERT activities while not providing its participants with learning opportunities on detailed technical tasks such as malware reverse engineering.

Furthermore, the results from the survey indicated that training and education is considered the most important improvement made by the majority of the CERTs, indicating the significance of training activities for the CERT community.

Recommendation

ENISA already partially fills this void by supporting TRANSITS trainings and also by facilitating the pan-European incident response exercises which are aimed at the different CERTs, amongst others, because of their role in CIIP. These exercises are of strategic importance in enhancing the security and resilience of CIIs, in particular by focusing on flexible strategies and processes for dealing with the unpredictability of potential cyber attacks. ENISA should continue facilitating these exercises across national boundaries as they require a central body for coordination and communication. It has been noted that these exercises are also vital for building trust between the different CERTs that participate in the activities, as they have an opportunity to witness the level of maturity and standards by which other CERTs operate.

ENISA should also investigate how further technical training opportunities could be organised (and how to inform the community of such training events). ENISA should have a thorough look at the existing market offer on technical training, such as the SANS 504 'Incident handling' and SANS 610 'Reverse Engineering Malware'. Such training materials can be purchased in bulk and distributed to the CERTs requiring them (with a substantial discount). ENISA could also consider hosting training at ENISA premises with a professional trainer. Not only would this reduce the training fee compared to regular training, it would also provide an excellent opportunity for CERT staff to get acquainted and build trust relationships.

Furthermore, it was suggested that ENISA creates a training matrix for junior handlers, senior handlers, analysts, managers, etc., which should indicate the levels of training required for those

[28] TERENA, TRANSITS-I courses: http://www.terena.org/activities/csirt-training/transits-i/

[29] TERENA, TRANSITS-II courses: http://www.terena.org/activities/csirt-training/transits-ii/

Providing specialised training

positions within the CERTs. These skill matrices also exist within TF-CSIRT and FIRST and should be aligned.

ENISA could even license training courses from CERT/CC or SANS or work together with bodies such as TF-CSIRT to create additional training.

As a final note, one interviewee pointed out the current focus on technical training, while soft skills are an absolute requirement for some of national/governmental CERT staff when they need to communicate with their constituency or senior government members on the importance issues. ENISA could look into creating soft skills training, tailored to CERT staff.

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted task:

> *(b) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues*

Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted task:

> *(i) Assist the Member States and the European institutions and bodies, at their request, in their efforts to develop network and information security detection, analysis and response capability*

ENISA currently fulfils the cooperation facilitation task by running the pan-European exercise in which a number of CERTs take part. The development of a training matrix could be considered as the development of a common methodology towards staffing CERTs but providing training is not specifically included in the mandate.

However, it is noted that ENISA has already been supporting the TRANSITS training for some time without anyone questioning the relevance in relationship to its mandate. Based on article (i), providing training on request can be interpreted as providing assistance in developing information security detection, analysis and response capabilities. It can be concluded that the recommendations on training curriculum development or joint training organisation can be included in the future proposed mandate only if such training activities are requested by the Member States.

6.2.10 Joint tool development

Joint tool development		
Overlap	CERT community acceptance 🟦	ENISA mandate support 🟦

Observation

Many expensive manual investigation and human manipulations are currently performed within the national/governmental CERT community with regard to the following services: alerts & warnings, announcements and incident handling.

From an operational perspective, automation can happen in different steps from information capturing, event processing, automatic report or ticket creation up to automatic response actions.

The CERTs were polled about the different domains where such automations would be desired. They indicated they see the most potential for detective tools and malware analysis tooling; less than half of the participants see potential in information exchange tools (as shown in Figure 10).

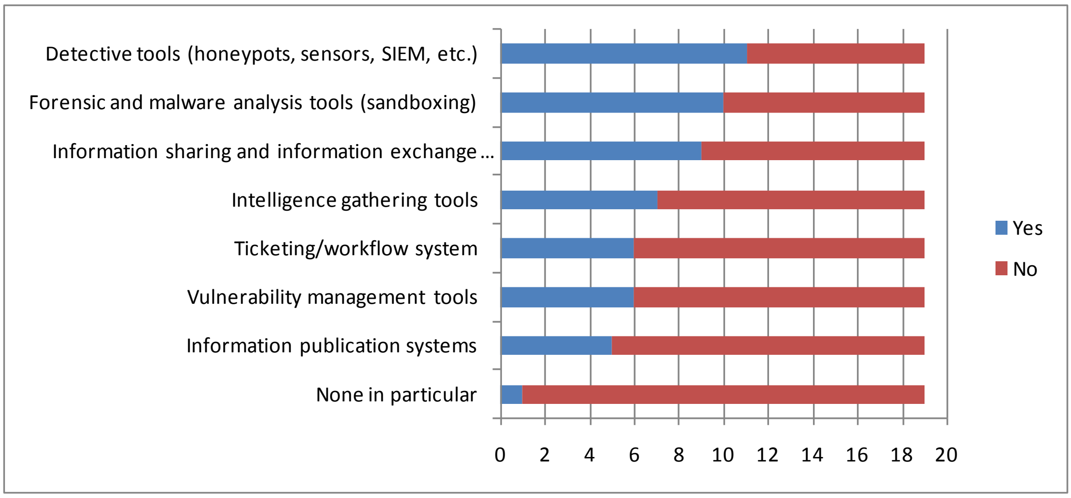


Figure 10: Tools and technologies that need to be advanced in the short term

Because certain tooling domains appear to be of common interest to more than half of the stakeholders, it would be sensible to consider joint design or development efforts for such tools, to the extent where the CERT can standardise on their requirements.

Recommendation

ENISA could research and provide advice how the CERT community could enhance their

Joint tool development

operations with the introduction of certain automations. Some automation suggestions include:

- Deployment of a common sensor network or honeypot network. It should be noted that actions have already been taken in this area by EU-funded projects such as ecsirt.net[30], Wombat[31], NoAH[32] and Lobster[33] – although the CERT community may not be aware of this as they consider this to be technology which needs to be advanced in the short term.
- Defining standard formats for automated processing of information intelligence sources.
- Tools for automatic ticket creation and follow-up.
- Tools to obfuscate sensitive data when sharing information.
- Automated information dissemination as a response action. An example can be an auto-generated ticket if port scanning attempts on a certain port exceed a predefined threshold.
- Central alerts & warning as a response action.
- Information exchange to central collaboration platform as a response action.

Mandate support

The mandates (both current and proposed) contain no reference to development initiatives which can be taken up or led by ENISA.

The current mandate however references the task:

> *(h) advise the Commission on research in the area of network and information security as well as on the effective use of risk prevention technologies*

In its task as a research advisor, ENISA could link interesting development initiatives to the policy makers and their research funding (such as the FP7 programme). By helping to secure funding ENISA can intervene as a guide in the progress of the development project, but in the mandate there is no support for software development activities.

[30] The European CSIRT Network: http://www.ecsirt.net/
[31] The WOMBAT project: http://www.wombat-project.eu/
[32] European Network of Affined Honeypots: http://www.fp6-noah.org/
[33] LOBSTER Project: http://www.ist-lobster.org/

6.2.11 Single point of contact for the national/governmental CERT community

Single point of contact for the national/governmental CERT community		
Gap	CERT community acceptance 🟦	ENISA mandate support 🟦🟦

Observation

As mentioned several times already, the national/governmental CERT community is a disparate group of different organisations with sometimes different objectives and constituencies. Currently, there is a clear focus on enhancing cooperation by promoting trust between the different organisations but this will only facilitate communications between the members of the community, not between the members and third parties. The survey and interviews indicated that ENISA could play a role in representing the CERT community as a whole to such third parties, but only on the condition that it would not affect the ability of the different CERTs to communicate directly between them.

Recommendation

With respect to being a single point of contact, ENISA could potentially play a role in the following scenarios:

- Supporting the CERTs in communicating with law enforcement officials both on a local and pan-European level;
- Communicating with the national/governmental CERT community during the course of a pan-European cyber security incident;
- In cases of major flash threats or where communication and coordination is needed with non-EU parties where the community requires multilateral interaction with the non-EU party;
- Representing the national/governmental CERT community in communication with private industry peers (recommendation 6.2.7);
- ENISA is already the point of contact for the CERT community and policy makers, the European Commission and other legal bodies.

Furthermore, one stakeholder indicated that ENISA is uniquely positioned as a contact point for the CERT community when specific technical knowledge is sought during incident resolution by indicating the expertise/specialties of each CERT in a specialised, closed directory. Mutual cooperation between the CERTs based on these skill sets could enhance the level of mutual trust and recognition of skills.

Mandate support

The current mandate does not foresee activities where ENISA can act as the single point of contact for the mentioned stakeholders. However, the proposed mandate contains two tasks which specifically assign ENISA the central role of a dialogue facilitator (which is not the same, but approximates to the role of a single point of contact):

Single point of contact for the national/governmental CERT community

> *(h) Facilitate dialogue and exchange of good practice among public and private stakeholders on network and information security, including aspects of the fight against cybercrime; assist the Commission on policy developments that take into account network and information security aspects of the fight against cybercrime;*
>
> *(j) Support Union dialogue and cooperation with third countries and international organisations in cooperation where appropriate with the EEAS, to promote international cooperation and a global common approach to network and information security issues*

As a side note, the aspects of the fight against cybercrime is explicitly mentioned; this also aligns with current activities of ENISA (ENISA's work programme for 2011 contains a specific study topic on the interfaces between the CERTs and law enforecement).

6.2.12 Closed CERT-community contacts directory

Closed CERT-community contacts directory		
Overlap	CERT community acceptance 🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

Multiple directories exist for CERT contacts. One example is CERT inventory[34] hosted by ENISA. In addition to that, TERENA (which is EU-focused) and FIRST (which is US-focused) offer separate directories of their accredited/affiliated members (Trusted Introducer also includes listed members for which no fee is required and whose data is published publicly). The accredited/affiliated CERTs have access to a more comprehensive, private directory with administrative, technical and management contact details. The multitude of directories can lead to confusion when there are multiple versions of the data and can pose an administrative burden when members need to update the data.

A stakeholder mentioned the current, rather confusing landscape and indicated their desire to see a simplified directory for use by the CERTs, independent from the accreditation/affiliation status with certain schemes. As an example, it was indicated that it is quite difficult for a non-FIRST member to contact CERTs in the US.

Recommendation

ENISA could organise and host such a centralised directory for the CERTs that wish to participate. It is clear that the success of such an initiative depends on the buy-in of the community as a whole. Furthermore, it should be aligned with the FIRST and TF-CSIRT directories.

According to the community, this directory should be for the use of the CERT community itself and should include sensitive details such as emergency contacts and mobile phone numbers. The directory should therefore be closed. Furthermore, ENISA can further promote the use of RFC2350 standard on contact information.[35]

A subset of those data can be made available to the broad public, which would make sense given ENISA's role in raising awareness of cyber security for all European citizens.

The surveyed CERTs mostly think this is a valuable idea, but indicated that it is relatively easy to identify communications means for other CERTs.

[34] CERT Inventory: http://www.enisa.europa.eu/act/cert/background/inv

[35] Expectations for Computer Security Incident Response: http://www.ietf.org/rfc/rfc2350.txt

Closed CERT-community contacts directory

Mandate support

This task is mainly supported by the current mandate task:

> *(c) enhance cooperation between different actors operating in the field of network and information security, inter alia, by organising, on a regular basis, consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies*

Particular attention is paid to ‘establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies’ which can be interpreted as facilitation of the communications between the different CERTs.

6.2.13 Incident classification and reporting standardisation

Incident classification and reporting standardisation		
Gap	CERT community acceptance 🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

The majority of the stakeholders indicate that they see value for the CERT community in a standardisation effort regarding incident classification and reporting. One stakeholder has already made such an effort within its local constituency.

Another stakeholder mentioned the relationship between the need for standardised reporting and the European Commission's Telecom Package, which requires service providers to report all significant incidents to their regulator.

It should be noted that only one respondent strongly disagreed that there is a need for such an effort. This respondent felt that such an attempt would not be useful because of the differences in mandate, constituency and definitions of what exactly the criteria are for identifying an incident. It was also noted that definition of such standards is very hard, because of a lack of consensus in the community.

Recommendation

ENISA could suggest an incident information exchange classification standard, in cooperation with the community, to provide common ground for documenting security incidents in a structured and repeatable manner. Such a standard could take into account parameters such as attack vector or the ease of remediation. Inspiration can be sought in the CVSS[36] (Common Vulnerability Scoring System). Having a common way of looking at the indicators will not only guide others but also help them be prepared in case of new incidents. Paramount to the success of such an initiative is consensus on the criteria according to which incidents are classified and the fact that those criteria must be objective.

As a next step, the framework should give the CERT community a means by which high severity incidents (i.e. Red, Amber) can be anonymously reported and shared with the community.

The overall goal should be to stimulate the security incident information exchange and build a foundation from which the national/governmental CERT community can constructively and cooperatively learn from each other.

Practically, ENISA could provide a CERT incident template and make it available to the community. The local CERTs could then document and complete each incident in the same, structured way. This would allow statistical reporting over time within the operational CERT context, as well as accelerating interoperability between the incident ticketing databases of the

[36] http://www.first.org/cvss/

Incident classification and reporting standardisation

different CERTs. It would promote consolidation to allow ENISA to build a pan-European trend historical incident database.

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted tasks:

> *(a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission;*
>
> *(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues;*
>
> *(g) track the development of standards for products and services on network and information security*

Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted task:

> *(b) Facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents;*
>
> *(f) Support cooperation among competent public bodies in Europe, in particular supporting their efforts to develop and exchange good practices and standards*

Both in the current and proposed mandate, there is ample support for initiatives which try to enhance the exchange of information between the CERTs (tasks (d) and (g) as well as (b) and (f)) and to establish good practices and standards. Furthermore, task (a) can support ENISA in building a historical database on incidents to analyse current and emerging risks at the European level.

6.2.14 Harmonisation of legal framework for information sharing and international incident handling

Harmonisation of legal framework for information sharing and international incident handling		
Gap	CERT community acceptance 🟦🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

There was consensus between the stakeholders that the current legal framework in Europe is a major hurdle in the way of further cooperation between the different CERTs in handling international incidents. The current legal environment seems not only to be different across the different European Member States but also unclear to the CERT staff. One case was noted where CERT staff were unable to share information (which potentially could have resolved the incident) with another European CERT. This was because, due to the complex environment, CERT incident handlers are more inclined to keep information to themselves unless they are positive they can share information, rather than considering information sharing to be the default scenario unless restrictions would apply. The same legal framework and hurdles apply both to incident handling and information sharing (alerts & warnings) based on incidents or other events which took place inside the constituency.

Recommendation

ENISA is uniquely positioned to assist the Commission, where called upon, in the legal (and technical) preparatory work for updating and developing national/governmental CERT community legislation in the field of network and information security.

Feedback from the stakeholders indicates that ENISA's guidance documentation in the CERT domain is very much appreciated and well used by the CERTs (e.g. the Baseline capabilities documents[37]). Given the authority that ENISA has among the CERTs, guidance documentation on legal implications of information exchange and international incident handling would be considered very useful by the community. In this respect already this year ENISA has launched a project on the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe[38].

Another suggested activity for ENISA is to support the dialogue with countries which are the source of most cyber attacks.

[37] Baseline capabilities for national/governmental CERTs: http://www.enisa.europa.eu/act/cert/support/baseline-capabilities

[38] A flair for sharing - encouraging information exchange between CERTs: http://www.enisa.europa.eu/act/cert/support/legal-information-sharing

Harmonisation of legal framework for information sharing and international incident handling

Mandate support

While the current mandate does not address the legal framework for information sharing, it became abundantly clear during the survey and associated interviews that this is one of the most pressing issues regarding the sharing of information in the CERT community (which in turn is a goal of the current mandate). The Commission and ENISA have become aware of this issue, which is reflected in the following task of the proposed mandate (specifically mentioning ENISA's task in developing and updating Union legislation):

> *(a) Assist the Commission, at its request or on its own initiative, on network and information security policy development by providing it with advice and opinions and with technical and socio-economic analyses, and with preparatory work for developing and updating Union legislation in the field of network and information security*

Furthermore, liaising with international organisations and third countries (as recommended for the 'wild' countries) also fits within the proposed mandate:

> *(k) Support Union dialogue and cooperation with third countries and international organisations in cooperation where appropriate with the EEAS, to promote international cooperation and a global common approach to network and information security issues*

6.2.15 CERT process guidance

CERT process guidance		
Gap	CERT community acceptance 🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

Although half of the surveyed CERTs acknowledges that more process formalisation and support is required to further advance their services, further guidance by ENISA for the development and alignment of CERT processes is only supported by a minority of them. When requested, the respondents indicate that ENISA current study work in the CERT area is known and appreciated.

One stakeholder referred to the difference between the US-CERT and CERT/CC. While US-CERT is mainly involved with security vulnerability information dissemination, has a more operational nature and is incident-focused, CERT/CC provides for process and procedure guidance, develops best-practice manuals and training and can provide general advice on major threats such as Stuxnet. The stakeholder indicated that ENISA should select a course similar to CERT/CC instead of the operational, incident-oriented focus of US-CERT.

Recommendation

Given the oral support we received for ENISA's current activities in the CERT domain but a low degree of community perception of the importance of further process improvement, ENISA could maintain its current level of activity in this area but make sure enough resources and efforts are put in the development of collaboration between the CERTs by improving CERT process maturity, which is clearly perceived by the majority of the respondents as the most important topic for ENISA.

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted task:

> *(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues;*

Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted tasks:

> *(b) Facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents;*
>
> *(c) Assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data;*

CERT process guidance

> *(g) Support cooperation between public and private stakeholders on the Union level, inter alia, by promoting information sharing and awareness raising, and facilitating their efforts to develop and take up standards for risk management and for the security of electronic products, networks and services*

ENISA has the mandate to help the community in maturing their current way of operating, thereby enhancing information sharing practices and incident response capabilities.

6.2.16 Cooperation with bodies such as TERENA

Cooperation with bodies such as TERENA		
Overlap	CERT community acceptance 🟦	ENISA mandate support 🟦🟦

Observation

In researching the value placed by the CERT community on their cooperation with organisations such as FIRST and TERENA, it appears that the following activities (in order of importance) are considered to be the most important fruits:

- Knowledge and best practice sharing
- Networking with other senior technical staff and industry
- Knowledge dissemination from the different task forces organised within these bodies

Furthermore, it appears that TERENA has several activities which show parallels with ENISA's activities:

- Both TERENA and ENISA have published deployment guides for DNSSEC. The TERENA deliverable discusses the roll-out models in the research community both from a technological and a policy point of view[39] while ENISA published a document in cooperation with industry players but also national authorities[40]. As both projects were funded by the European Commission, further alignment of activities with the TERENA task force could be done to optimise joint spending effort.
- TF-CSIRT is a TERENA task force that promotes collaboration between CSIRTs at the European level, and liaises with similar groups in other regions, which is also a core goal of the ENISA CERT expert group.

One example of an already existing collaboration is the TERENA-organised TRANSITS training for CERT staff, which is sponsored by ENISA.

Recommendation

ENISA should further attempt to align agendas with bodies such as TERENA (and specifically the task forces) to optimise joint resource spending and to clearly identify which areas will be further researched by which entity.

Mandate support

The sharing of knowledge within the community and with bodies such as TERENA is heavily supported by the current mandate. This is shown in:

[39] DNS Security: http://www.terena.org/activities/dnssec/

[40] Good Practices Guide for Deploying DNSSEC: http://www.enisa.europa.eu/act/res/technologies/tech/gpgdnssec

Cooperation with bodies such as TERENA

> *(c) enhance cooperation between different actors operating in the field of network and information security, inter alia, by organising, on a regular basis, consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies;*
>
> *(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues;*
>
> *(e) contribute to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users by, inter alia, promoting exchanges of current best practices, including on methods of alerting users, and seeking synergy between public and private sector initiatives;*
>
> *(j) contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security;*

All these tasks support exchanging information between the actors in the field of network and information security and task (j) specifically mentions the sharing with international organisations such as TERENA.

6.2.17 Guidance and direction based on observed trends

Guidance and direction based on observed trends		
Gap	CERT community acceptance 🟦🟦🟦	ENISA mandate support 🟦🟦🟦

Observation

Although not specifically indicated by the survey, a stakeholder pointed out their vision of ENISA as a central body who should educate and guide the constituency on the risks and threats observed in the European cyber community. This is supported by the existing activities of ENISA, such as the publication on botnets.[41]

Recommendation

ENISA should ensure that its activities remain on the European level and are of use to the different European CERTs by making abstraction of the local CERT issues towards a higher geographical level. This can be done by analysing data from the different CERTs and comparing the origin and timelines of different alerts and warnings from the CERTs. Combining these insights with the agency's policy context, ENISA is uniquely positioned to see the bigger picture on European threats and issues.

Based on this information, ENISA should provide guidance on observed trends and help the CERTs by developing strategies to work together as a group to mitigate the threats. Guidance can take the form of the publication of reports, the creation of training, the organisation of workshops and other activities. The CERTs can then leverage the advice to implement their proper threat mitigation activities.

Mandate support

Based on ENISA's mandated tasks as described in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, this recommendation in is line with quoted tasks:

> *(a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission;*
>
> *(k) express independently its own conclusions, orientations and give advice on matters*

[41] Botnets: Measurement, Detection, Disinfection and Defence: http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

Guidance and direction based on observed trends

> *within its scope and objectives.*

Based on the Commission's proposal for ENISA, COM(2010) 521 final, this recommendation in is line with quoted tasks:

> *(a) Assist the Commission, at its request or on its own initiative, on network and information security policy development by providing it with advice and opinions and with technical and socio-economic analyses, and with preparatory work for developing and updating Union legislation in the field of network and information security;*

These tasks clearly outline ENISA's responsibility to use the collected information to analyse current and emerging risks, both at the request of the Commission as well as on its own initiative. These analyses should not be confined to the technical level: Socio-economic advice and preparatory work in developing Union legislation are also considered in scope.

6.3 Summary table of recommendations

Observation	Gap or overlap	CERT community acceptance	ENISA mandate support
Harmonisation of legal framework for information sharing and international incident handling	Gap	🟦🟦🟦	🟦🟦🟦
Guidance and direction based on observed trends	Gap	🟦🟦🟦	🟦🟦🟦
Industry partnerships	Overlap	🟦🟦🟦	🟦🟦🟦
European institutions CERT	Gap	🟦🟦🟦	🟦🟦🟦
Providing specialised training	Gap	🟦🟦🟦	🟦🟦
Closed CERT-community contacts directory	Overlap	🟦🟦	🟦🟦🟦
Incident classification and reporting standardisation	Gap	🟦🟦	🟦🟦🟦
CERT process guidance	Gap	🟦🟦	🟦🟦🟦
Stimulating and providing means to centrally exchange information on alerts & warnings among CERTs	Gap	🟦🟦	🟦🟦🟦
Providing CERT communications channels	Gap	🟦🟦	🟦🟦🟦
Aggregation of announcements and alerts & warnings from external sources	Overlap	🟦🟦	🟦🟦
Support to malware analysis services	Gap	🟦🟦	🟦
International incident coordination	Gap	🟦	🟦🟦🟦
CERT membership services	Gap	🟦	🟦🟦
Cooperation with bodies such as TERENA	Overlap	🟦	🟦🟦
Single point of contact for the national/governmental CERT community	Gap	🟦	🟦🟦
Joint tool development	Overlap	🟦	🟦

Table 2: Summary table of recommendations

6.4 Future role of ENISA

During the stakeholder interaction, it became clear that ENISA's work in the European national/governmental CERT ecosystem is noticed and appreciated by the different stakeholders.

Documents such as 'Baseline Capabilities for CERT'[42] are read in the community, as are more specific guides on starting up CERT activities.

When polled, only one stakeholder indicated they would like to see a reduction of ENISA's activities as regards the CERT community. This is shown in Figure 11.

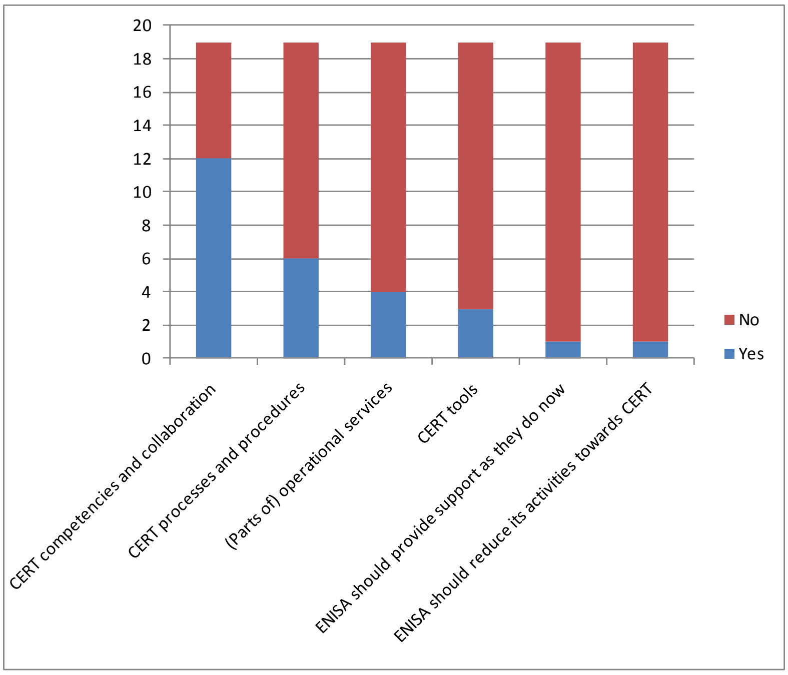


Figure 11: Future role of ENISA towards the CERT community

Out of the 19 respondents, there were an additional three who did not see the need for ENISA to increase its current involvement. This means that a vast majority of 15 stakeholders support the idea of ENISA taking up an additional role in the CERT community.

Out of the different possibilities presented, it appeared that **supporting the development of CERT competencies and collaboration** is by far the most preferred option. It is indeed in this domain that most of the recommendations apply. Other options, such as performing (parts of) operational services, seem to encounter major resistance by the stakeholders.

This leads to the conclusion that ENISA should be careful if launching activities which might be seen as operational and make sure to have the necessary buy-in from the CERT community first to ensure the success and uptake of the fruits of such activities.

[42] Baseline capabilities for national/governmental CERTs: http://www.enisa.europa.eu/act/cert/support/baseline-capabilities

7 Conclusion

During this study on the domain of possible operational gaps and overlaps in the existing CERT community, it became clear that the different CERTs have very disparate views of what activities can support them in their daily operations. This is not surprising, as every CERT has a different constituency, focal point, mandate, funding structure and therefore a different service offering. One constant throughout the study was the importance placed by the respondents on the incident handling, alerts & warnings and announcement services provided to their constituency. Their importance matched the request of ENISA to explore further into detail on those services as well as the artifact handling service.

As a result of the analysis of possible operational gaps and overlaps, the authors believe the recommendations below are the top considerations for the ENISA CERT expert group to consider implementing:

1. **Guidance and direction based on detected trends:** ENISA should continue its activities in observing information security trends and help the CERTs by developing strategies to work together as a group to mitigate the threats by providing guidance in the form of publications and workshops.
2. **Harmonisation of legal framework for information sharing and international incident handling:** ENISA is well positioned to assist the Commission, where called upon, in the legal (and technical) preparatory work for updating and developing national/governmental CERT community legislation in the field of network and information security.
3. **Providing specialised training:** ENISA should investigate how further technical training opportunities could be organised by creating skill development guides for CERTs, creating opportunities for the CERTs to attend private sector technical training at affordable prices and by bringing soft skills into the picture as important skill sets for CERT staff.
4. **Industry partnerships:** ENISA can help to reduce the administrative burden for each CERT of maintaining contacts with the main vendors. ENISA could distribute received information throughout a joint cooperation platform to the different CERTs.
5. **Providing CERT communication channels:** For security information to be exchanged productively between multiple parties (i.e. members of the CERT community), secure and trusted communications channels are essential. ENISA could investigate possibilities to provide such channels, which might serve as well as a platform to support implementing several other recommendations listed in this study (eg, central exchange of information on alerts & warnings, support to malware analysis services, industry partnerships, closed CERT-community contacts directory).

As a final note, as indicated in section 6.4, ‘Future role of ENISA’, less than half of the participants are comfortable with the idea of ENISA taking up operational activities with regard to the CERT community. For this reason ENISA will not implement directly the European institutions CERT, which is also one important recommendation of this report, but will support the pre-configuration team.

Several interviewed CERTs indicated they see ENISA’s role as representing the interests of the CERT community on a policy level, being an agency of the European Union as opposed to taking up operational activities.

The same expectations are reflected in the proposed mandate for ENISA, which focuses on the need for a more coordinated approach to cyber threats across Europe, transnational cooperation to respond to large-scale cyber attacks, building trust and improved information exchange among stakeholders.

As a final remark, if consideration is given to engaging ENISA in operational activities, we believe it is imperative to poll the CERT community again about the degree of acceptance on specific activities and to give the community the opportunity to indicate their requests or recommendations before implementing such a service. This will ensure awareness and buy-in from the community and avoid costly initiatives that are doomed to fail.

8 Annex I: ENISA's mandated tasks

This chapter provides an overview of the tasks for which ENISA is currently mandated, as well the tasks as outlined in the Commission's proposal on ENISA's mandate. These tasks are heavily referenced in the recommendations' mandate support sections and are listed here for the purpose of reference.

8.1 Current mandate (per regulation EC/460/2004)[43]

(a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission;

(b) provide the European Parliament, the Commission, European bodies or competent national bodies appointed by the Member States with advice, and when called upon, with assistance within its objectives;

(c) enhance cooperation between different actors operating in the field of network and information security, inter alia, by organising, on a regular basis, consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies;

(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues;

(e) contribute to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users by, inter alia, promoting exchanges of current best practices, including on methods of alerting users, and seeking synergy between public and private sector initiatives;

(f) assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products;

(g) track the development of standards for products and services on network and information security;

(h) advise the Commission on research in the area of network and information security as well as on the effective use of risk prevention technologies;

(i) promote risk assessment activities, interoperable risk management solutions and studies on prevention management solutions within public and private sector organisations;

(j) contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security;

(k) express independently its own conclusions, orientations and give advice on matters within its scope and objectives.

[43] Regulation (EC) No 460/2004: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

8.2 The Commission's proposal[44]

(a) Assist the Commission, at its request or on its own initiative, on network and information security policy development by providing it with advice and opinions and with technical and socio-economic analyses, and with preparatory work for developing and updating Union legislation in the field of network and information security;

(b) Facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents;

(c) Assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data;

(d) Regularly assess, in cooperation with the Member States and the European institutions, the state of network and information security in Europe;

(e) Support cooperation among competent public bodies in Europe, in particular supporting their efforts to develop and exchange good practices and standards;

(f) Assist the Union and the Member States in promoting the use of risk management and security good practice and standards for electronic products, systems and services;

(g) Support cooperation between public and private stakeholders on the Union level, inter alia, by promoting information sharing and awareness raising, and facilitating their efforts to develop and take up standards for risk management and for the security of electronic products, networks and services;

(h) Facilitate dialogue and exchange of good practice among public and private stakeholders on network and information security, including aspects of the fight against cybercrime; assist the Commission on policy developments that take into account network and information security aspects of the fight against cybercrime;

(i) Assist the Member States and the European institutions and bodies, at their request, in their efforts to develop network and information security detection, analysis and response capability;

(j) Support Union dialogue and cooperation with third countries and international organisations in cooperation where appropriate with the EEAS, to promote international cooperation and a global common approach to network and information security issues;

(k) Carry out tasks conferred on the Agency by Union legislative acts.

[44] COM(2010) 521 final: http://www.coe.int/t/DGHL/STANDARDSETTING/T-CY/Proposal%20new%20regulation%20ENISA.pdf

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu