Council of the
European Union

Brussels, 3 March 2015
(OR. en)

6738/15

CIS 3
CSC 54
CSCI 12
CYBER 11

INFORMATION NOTE

From:	The inter-institutional CERT-EU Steering Board
To:	Delegations
Subject:	CERT-EU mandate, service catalogue and information sharing and exchange framework

1. On 25 February 2015, the inter-institutional CERT-EU Steering Board agreed on a new mandate for CERT-EU and its service catalogue (see Annex I). It also approved a CERT-EU information sharing and exchange framework (see Annex II).

2. Delegations are reminded that the mandate of the CERT-EU Steering Board can be found in doc. 12992/14, page 6.

MANDATE OF CERT-EU

A. MISSION AND TASKS

1. CERT-EU's mission is to enhance the security of the information and communications technology (ICT) infrastructure of all EU institutions, bodies and agencies (its 'constituents'). It supports incident prevention, detection, mitigation and response by acting as the cyber-security information exchange and incident response coordination hub for its constituents.

2. CERT-EU's tasks are to provide to its constituents the services described in its service catalogue and to liaise as appropriate with Member State CERTs on matters relevant for protecting constituents' ICT infrastructure. It also cooperates with non-EU CERTs, international organisations, commercial entities and individual experts on such matters as set out in Section C. below. It performs these tasks by collecting, managing, analysing and sharing information with constituents on threats, vulnerabilities and incidents on unclassified ICT infrastructure, and by coordinating responses to incidents at inter-institutional and constituent level, including by providing or coordinating specialised operational assistance.

3. CERT-EU may provide assistance for incidents on classified networks when invited by the constituent concerned.

4. CERT-EU encourages information sharing among constituents on vulnerabilities, threats and incidents, in line with general principles agreed by the Steering Board.

5. CERT-EU will draw up a document describing its incident handling process for constituents.

6. CERT-EU may undertake any activities going beyond this mandate with the prior approval of the Steering Board (where appropriate under the urgency procedure). It will not engage proactively in intelligence-related activity, in particular with the purpose of attributing attacks.

B. SERVICE PROVISION

7. CERT-EU provides CERT services to all constituents based on a service level arrangement (SLA) specifying the services to be provided and each constituent's contribution for these services. The core services set out in CERT-EU's service catalogue (annexed) comprise:

(i) announcements and advisories;

(ii) alerts and warnings;

(iii) incident response coordination (remote or on site);

(iv) incident response and analysis (remote or on site);

(v) artefact analysis and actions;

(vi) development of security tools;

(vii) intrusion detection and log management services;

(viii) vulnerability assessment and penetration testing; and

(ix) cyber threat intelligence (including information from paid subscriptions and unpaid non-public sources).

8. CERT-EU provides the following basic services to constituents which have not yet entered into an SLA:

(i) announcements and advisories;

(ii) alerts and warnings;

(iii) incident response coordination (remote); and

(iv) cyber threat intelligence (information from unpaid non-public sources).

9. CERT-EU makes information available to its constituents via non-public channels. CERT-EU may make cyber security information which is in the public domain available via its publicly accessible website, or in any other manner.

10. CERT-EU may seek the Steering Board's approval to modify the service catalogue in response to constituents' needs, within the boundaries of its mandate and taking into account its resources.

C. INTERNAL AND EXTERNAL COOPERATION

11. CERT-EU develops synergies with the European Union Agency for Network and Information Security (ENISA) and the European Cybercrime Centre (EC3) at Europol to build on complementarities and synergies in:

    (i) developing cyber-security awareness raising and training programmes;

    (ii) developing cyber-security risk assessment tools;

    (iii) developing alerts or advisories concerning important vulnerabilities or threats;

    (iv) leveraging best practices in cyber-security;

    (v) sharing threat intelligence; and

    (vi) organising exercises.

    CERT-EU may seek the Steering Board's approval for the development of other synergies with ENISA and EC3.

12. CERT-EU may enter into SLAs to provide services to other European-level public bodies with the prior approval of the Steering Board.

13. CERT-EU, acting in accordance information sharing and exchange principles approved by the Steering Board, may cooperate with non-EU CERTs, international organisations, commercial entities and individual experts to exchange technical information on vulnerabilities and threats and on responding effectively to cyber incidents affecting constituents.

D. REPORTING

The head of CERT-EU reports regularly to the Steering Board on CERT-EU's activities.

computer emergency response team CERT-EU for the EU institutions, bodies and agencies

SERVICE CATALOGUE

Introduction

This Service Catalogue sets out core services available to the EU institutions, bodies and agencies (the CERT-EU constituents). It provides an overview of CERT-EU services and specifies information to be shared between CERT-EU and the 'Beneficiary' to start operational cooperation. Where appropriate, it provides links or references for useful documents and webpages. The services are based on the typical CERT services as documented by ENISA[1] and CERT/CC[2].

For each service / product, constituents will find

- Summary description: a few words describing the service / product
- Service access: key information for accessing or triggering the service
- Cooperation: suggestions in case constituents would like to develop specific cooperation with CERT-EU.

It is understood that CERT-EU can make available to other parties cyber-security tools it has developed as part of these services, as long as this does not require additional funding from the institutional budget of CERT-EU. The Steering Board is informed.

Background

The EU institutions, bodies and agencies have set up a Computer Emergency Response Team (CERT-EU) in September 2012 after the successful completion of a pilot phase of one year. Its constituency is composed of all the EU institutions, bodies and agencies, 60 organisations with close to 75.000 end users. CERT-EU's mission is to support the European institutions, bodies and agencies to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery.

General information

Contact

CERT-EU

Address: CERT-EU - Rue Montoyer, 34 - 1049 Bruxelles

Phone: +3222990005

Website: http://cert.europa.eu

Email (general information): cert-eu@ec.europa.eu

Email (incident response): reports@cert.europa.eu

Constituent (info required)

- ✓ Physical / postal address
- ✓ Contact person name / phone / email
- ✓ Functional mailbox for alerts and incident response

Security & Privacy

CERT-EU

PGP KeyID: 0x46AC4383

PGP FP: 9011 6BE9 D642 DD93 8348 DAFA 27A4 06CA 46AC 4383

Data Protection: CERT-EU complies with EC Regulation n°45/2001

Privacy Statement: http://cert.europa.eu/cert/plainedition/en/cert_privacy.html

Constituent (info required)

- ✓ PGP KeyID
- ✓ PGP FP
- ✓ Data protection notification (reference)

Services categories

CERT services require a financial or resources contribution and are subject to a service level agreement (SLA).

- ✓ Minimum requirement: Financial or resources contribution and SLA detailing conditions and mutual obligations of 'service provider' (CERT-EU) and 'beneficiary'
- ✓ General access conditions: as described in the SLA.

The following basic services are provided to EU constituents that have not yet entered into an SLA:

- Announcements and advisories
- Alerts and warnings

[1] https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/possible-services

[2] http://www.cert.org/incident-management/services.cfm

- Incident response coordination (remote)
- Cyber threat intelligence (based on information from unpaid non-public sources).

✓ Minimum requirements: none

✓ General access conditions: functional mailbox (FMB), PGP key, IP/ASN range.

CERT SERVICES

1. Announcements and advisories

This service includes, but is not limited to, vulnerability warnings and security advisories. Such announcements 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.

This service also includes White Papers and Green Papers to take stock of lessons learnt in past incidents and to recommend approaches to prevent future problems.

Finally this service also provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include

- reporting guidelines and contact information for CERT-EU
- archives of announcements
- documentation about best practices
- general computer security guidance and checklists
- information that can improve overall security practices.

Service access

➢ Specific products: Advisories, CERT-EU White Papers and web portal (http://cert.europa.eu).

➢ Channel: Website and Email distribution.

2. Alerts and warnings

This service involves disseminating information that describes an immediate threat or an on-going intruder attack, specific security vulnerability in your infrastructure, intrusion alert, targeted malware and providing any short-term recommended course of action for dealing with the resulting problem. The alert or warning is sent as a reaction to the current problem to notify constituents of the activity and to provide generic but constituent specific guidance for protecting their systems or recovering any systems that were affected. Information may be created by CERT-EU or may be redistributed from vendors, other CERTs or security experts, or other parts of the constituency.

Service access

➢ Specific products: Alerts

➢ Channel: Email distribution

➢ Information required: FMB (where alerts should be forwarded to), PGP key, ASN/IP range, Internet domains owned, email address domain.

Cooperation

➢ Constituents are encouraged to notify CERT-EU with feedback on this service so as to improve it and to feed in information about alerts.

3. Incident response support and coordination (remote or on-site)

CERT-EU assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation on a best effort basis. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as described above. CERT-EU provides guidance remotely so that site personnel can perform the recovery themselves.

CERT-EU also provides advisory support to the better coordinate the response effort among parties involved in an incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CERTs, and system and network administrators at the site. The coordination support may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. The support work may involve notification and collaboration with an organization's legal counsel, human resources or public relations departments. It could also include, with the consent of the affected party, engaging with law enforcement.

Service access

- Incidents should be reported to reports@cert.europa.eu
- The following minimum information should be provided in the initial message: name of victim organisation, local incident response contact details (email address, phone), date/time of detection, type of incident, actions taken
- Further information may be asked in the procedure.

4. Incident response and analysis (remote or on site)

The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. CERT-EU helps to analyse the affected systems and conduct the acquisition of the systems. Incident response support can be provided by telephone or email (see above). Or in case of need CERT-EU team members would travel to the site and perform the response activities in alongside the local team.

CERT-EU may use the results of vulnerability and artefact analysis to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. CERT-EU correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Sub-services that may be offered as part of incident analysis are

- **Forensic evidence collection**: CERT-EU supports the local team or carries out the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports via memory forensic analysis; and checking for Trojan horse programs and toolkits.
- **Tracking or tracing**: CERT-EU supports the tracing of the origins of an intrusion or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, and what other systems and networks were used as part of the attack. This work might be done alone but usually involves working with relevant public authorities, Internet service providers, or other involved organisations.

Service access

- SLA
- Data protection notification and privacy statement.

5. Artefact analysis and actions

CERT-EU performs or supervises the performance of a technical examination and analysis of artifact found on a compromised system. The analysis might include identifying the file type and structure of the artefact, comparing a new artefact against existing artefacts or other versions of the same artefact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artefact. This service also involves sharing and synthesizing analysis results and response strategies pertaining to an artefact with other researchers, CERTs, vendors, and other security experts. Activities also include maintaining a constituent archive of known artefacts and their impact and corresponding response strategies. CERT-EU determines the appropriate actions to detect and remove malware from a system based on identified malware, as well as actions to prevent malware from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

Service access

- SLA
- Data protection notification and privacy statement.

6. Development of security tools

This service involves the provision of specialised tools to improve detection or remediation. This can include developing tools or scripts that extend the functionality of existing security tools to detect artefacts, to cross-correlate logs and to summarise the state of health of the infrastructure. It can also include tools to automatically handle suspicious documents, email, links etc. Finally it can also include tools to automatically handle incoming feeds of abuse and malevolence monitoring.

Service access

- SLA.

7. Intrusion detection and log management services

CERT-EU makes available a network intrusion detection device in the form of an appliance or software application to be installed in the network of the constituent with the purpose of detecting suspicious or anomalous events potentially related to targeted attacks and produce reports to a management station. CERT-EU uploads specific rules and indicators of compromise during on-going incident and maintains the database of rules and indicators for continuous operation. It reviews the resulting logs, analyses and initiates a response for any events that meet their defined threshold, or forwards any alerts according to a pre-defined service level agreement or escalation strategy.

CERT-EU also makes available tools and services to facilitate log management and correlation using a multi-tier index for searching into past events or for detecting events in real-time using rules applied to log files from multiple sources.

Service access

- SLA
- Technical information for IDS installation.

8. Vulnerability assessment and penetration testing

This service provides an analysis of the constituent's information systems using tools and techniques to identify cyber security vulnerabilities. This service uses ethical hacking techniques to test selected information systems and networks of the constituent to assess vulnerabilities. Depending on the needs and preferences of the constituent, this service can be limited to the internet accessible parts of the constituent's information systems, or include all or part of the constituent's information systems and networks. A vulnerability assessment report is provided to the constituent that reviews and classifies the vulnerabilities and makes suggestions for effective countermeasures and, upon request, makes suggestions for improved objectives for the cyber security infrastructure.

CERT-EU can also support security awareness raising at senior management level by presenting the vulnerability assessment report, in order to improve prevention and to obtain support for the improvement plan resulting from the review. This service could also involve the provision of brief on-site awareness raising sessions for the staff of the constituent (all staff or high-level management). The sessions include an overview of the threat landscape, the techniques deployed by adversaries and guidance to increase the IT security hygiene of the organisation.

Service access

- SLA.

9. Cyber threat intelligence

CERT-EU provides a cyber-threat intelligence service which consists in disseminating actionable information on targeted or other relevant attacks. This enables constituents to ***detect*** if they have been affected by similar threats, ***prevent*** the occurrence of corresponding attacks on their IT infrastructure, ***react*** appropriately in case of attack, and ***report*** to CERT-EU to assist other constituents to counter the threat. In terms of classical CERT services, it is a mix of alerts and warnings, and announcements, while it also contributes to risk analysis.

Service access

- Specific products:
  CIMBL (CERT-EU identified malicious blacklist): dissemination of relevant indicators of compromises – technical data to feed IT security tools (IDS, IPS, mailguard, firewalls, etc.)
  CITAR (CERT-EU identified threat assessment reports): dissemination of threat assessment report – tactical data concerning threat actors, their campaigns, motives, tactics/techniques/procedures and courses of action to defeat them
  Cyber Security Brief: monthly overview of the most relevant threats presented in an easy to read, high-level fashion
  Detection rules adapted to the specific infrastructure of the clients (SIEM, IDS)
- Email distribution
- Information required: FMB, PGP key
- More information: see 'CIMBL-User-Manual'.

Cooperation

- Constituents are encouraged to notify CERT-EU if they become aware of any specific threats or attacks.

CERT-EU INFORMATION SHARING AND EXCHANGE

I. GENERAL PRINCIPLES

1. CERT-EU will provide constituents with all relevant information on general and specific cyber-security threats, vulnerabilities and incidents, as well as on possible counter-measures.

2. Institutions, bodies and agencies (the 'constituents') will provide CERT-EU with all relevant information on cyber-security threats, vulnerabilities and incidents, and possible counter-measures.

3. Information will be shared or exchanged with the consent of the information provider. Information provided by constituents or CERT-EU may be marked (using the Traffic Light Protocol and possible additional markings) to indicate the extent to which it may be shared. Unmarked information will be considered as shareable according to CERT-EU's judgement. Constituents and CERT-EU will handle shared information in line with these markings.

4. CERT-EU may cooperate and exchange information on cyber-security threats, vulnerabilities and incidents, as well as on possible counter-measures, with Member State CERTs.

5. CERT-EU may cooperate and exchange information with any other parties as described below.

6. CERT-EU will share information on specific incidents with law enforcement authorities only in agreement with the competent services in the constituent affected by an incident.

7. CERT-EU will keep records of all information shared with constituents and exchanged with other parties. It will provide written reports to the Steering Board on information sharing arrangements with other parties. Constituents may request CERT-EU to provide details of information shared with other parties.

II. INFORMATION SHARING BETWEEN CONSTITUENTS AND CERT-EU

8. When CERT-EU becomes aware of a threat, vulnerability or incident affecting or potentially affecting a constituent, it will alert the relevant constituent by providing all relevant information (including the level of criticality) as soon as practicable so that protective or remedial measures can be implemented.

9. Constituents will provide information on significant cyber-security threats, vulnerabilities and incidents affecting it as soon as practicable to CERT-EU. Regarding incidents, information will include all relevant technical details. Non-technical information may be shared with CERT-EU at the discretion of the impacted constituent.

10. Where appropriate, CERT-EU may organise and coordinate information sharing directly between constituents to address a cyber-security incident.

III. INFORMATION EXCHANGE WITH MEMBER STATE CERTS

11. CERT-EU will gather from Member State CERTs information on general and specific threats to constituents and on tools or methods (including techniques, tactics and procedures), best practices and general vulnerabilities for dissemination to its constituents.

12. CERT-EU may exchange information on tools or methods (including techniques, tactics and procedures), best practices and general threats and vulnerabilities with such CERTs.

13. CERT-EU may exchange incident-specific information with such CERTs in accordance with paragraph 3.

IV. INFORMATION EXCHANGE WITH OTHER THIRD COUNTRY CERTS

14. CERT-EU may cooperate and exchange information with other non-EU CERTs on tools/methods (including techniques, tactics and procedures), best practices and general threats and vulnerabilities.

15. CERT-EU will seek advice from the Steering Board on cooperation or information exchange with other non-EU CERTs (including in frameworks where such CERTs cooperate with Member State CERTs) going beyond such exchanges.

V. INFORMATION EXCHANGE WITH OTHER PARTNERS

16. CERT-EU may exchange information with other partners (i.e. commercial entities or individual experts) to gather information on general and specific threats, vulnerabilities and possible counter-measures.

17. CERT-EU will seek approval from the Steering Board on formalised cooperation or information exchange with other partners.

18. CERT-EU may provide information from a constituent, particularly in the event of an incident, to other partners who can contribute to its analysis, in accordance with paragraph 3. CERT-EU will ensure that legally verified non-disclosure arrangements or contracts are in place with the relevant partner.