Council of the
European Union

Brussels, 14 March 2016
(OR. en)

7049/16

CSCI 17
CSC 72

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Information Assurance Security Guidelines on CIS Security Incident Handling

Delegations will find attached the Information Assurance Security Guidelines on CIS Security Incident Handling as approved by the Council Security Committee on 11 March 2016.

This page intentionally left blank

Information Assurance Guidelines on CIS Security Incident Handling

IASG 4-03

TABLE OF CONTENTS

I. PURPOSE AND SCOPE

1. These guidelines, agreed by the Council Security Committee in accordance with Article 6(2) of the Council Security Rules (hereinafter 'CSR') [1], are designed to support implementation of the CSR.

2. These guidelines describe minimum standards to be implemented for the purpose of handling of incidents affecting the security of CIS or of the information handled by CIS. The document defines responsibilities and procedures to implement the ability to identify and handle security incidents which affect CIS in its constituency/ies.

3. The Council and the General Secretariat of the Council (GSC) will apply these security guidelines in their structures and CIS.

4. Member States should use security guidelines as a benchmark when EU classified information is handled in national structures, including in national CIS.

5. EU agencies and bodies established under Title V, Chapter 2, of the TEU, Europol and Eurojust should use these security guidelines as a reference for implementing security rules in their own structures.

6. In this document any unusual behaviour such as unexpected, unexplained or unplanned changes in the functionality of CIS or a breach of policy is called an event, irrespective of whether it affects the security of the CIS or of the information it handles.

7. As incidents affecting CIS could affect the security or essential interests of the EU, its Member States and partners, information which could identify the affected CIS and the potential impact of an incident may need to be classified until investigation determines that it can be released. This does not exclude rapidly exchanging sensitive but unclassified alerts with partners, e.g. information about attack detection and mitigation which is not linked to any CIS.

[1] Council Decision 2013/488/EU, OJ L274 of 23.09.2013, p.1.

II. OVERVIEW

8. As indicated by the information assurance network defence policy IASP 4 and guidelines IASG 4-01, among other measures, network defence management (NDM) needs to have, or have access to a specialised team of experts whose core task is to respond to 'computer' security emergencies or incidents - the incident response team (IRT)[2]. In the context of security incidents affecting CIS, the core services provided by this team are

   (a) incident handling;

   (b) incident analysis;

   (c) incident response support;

   (d) incident response coordination; and

   (e) issuing notifications and alerts to members of its constituencies about new threats vulnerabilities and weaknesses of CIS components and advice for their mitigation.

   An IRT may offer additional services such as advising CIS designers on security measures[3].

9. The set of services needed by the NDM needs to be defined and documented. This document will list the services which the local IRT is able to provide and highlight areas where external assistance may be required. This document needs to be regularly revised as part of the management review of the effectivity and efficiency of CIS Network Defence measures, in order to adapt the IRT's role to the developing security requirements and changing threat scenario to which the managed CIS is/are exposed. As an IRT as a rule will not have all the resources and expertise to be able to deal with all kinds of incidents, it needs to establish procedures to involve internal experts and/or request external assistance as needed. External assistance of a technical nature will typically be requested from institutional or other public- or private-sector CERTs, but may also be requested from law enforcement, through diplomatic channels, etc. The incident response operating procedures for a specific CIS must be included in the accreditation process of that CIS.

[2] This team is also often called a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT), though other names are also used.

[3] cf. ENISA "Possible services that a CSIRT can deliver"

10. The Computer Emergency Response Team of the EU institutions, bodies and agencies (CERT-EU) acts as the cyber-security information exchange and incident response coordination hub for its constituents. In accordance with its mandate (cf. Annex I to doc. 6738/15) it may provide assistance for incidents on classified networks when invited by the constituents concerned.

11. The overall process for handling incidents consists of a planning phase and an operational phase. The operational phase can be further subdivided into

    (a) a detection phase which receives events which could be security-related;

    (b) an assessment and decision phase;

    (c) a response phase where the cause of the security incident is removed and the CIS restored to a secure state;
    and

    (d) a remediation (lessons learnt) phase which may require modifying the network defence measures of the CIS to prevent or minimise the likelihood of recurrence.

12. While not part of incident handling, for effective handling to be possible, the CIS must have been set up to provide information about events which could be security incidents.

13. The planning phase of incident handling requires the role of the IRT to be defined, the IRT to be staffed, incident detection, analysis and response tools to be chosen, members of IRT staff to be trained in their use, and procedures for routine incident analysis and resolution being established. Further the planning phase includes setting up information exchange methods with partners and procedures for requesting internal and external assistance.

14. The general procedure is initial checking to exclude that the suspected incident is in fact normal or expected behaviour, failing which IRT members are called in to determine the cause of the events and trigger Business Continuity Plans (BCP) or Disaster Recovery (DR) plans[4] to restore service, while preserving evidence in a forensic manner for legal or disciplinary action against identified perpetrators as applicable, and technical information needed to improve network defence measures for the victim CIS.

[4] BCP and DR plans are not performed by the IRT but by the business owners and "operations support" of the CIS.

15. The first operational step in incident handling is the collection of information and elimination of false positives (events which are not security incidents) as follows:

(a) first responders check whether planned changes, normal behaviour, etc. could be the reason for triggering the alert about an event, without investigating the event themselves[5]; the event should however still be reported to the IRT, to avoid missing information which can be useful in refining event detection and alerting methods;

(b) if the event cannot be proven to be due to planned, expected or normal behaviour, first responders call the designated point of contact for the IRT and request the IRT to start investigations;

(c) if the IRT finds that the events are not security-related, it hands the event over to support teams for restoration of service.

16. Security Incident handling is initiated when the reported event is found or suspected to be security-related, the IRT declares a CIS security incident and proceeds as follows:

(a) restricts distribution of information about the incident;

(b) estimates the impact of the incident on the security of the CIS and the data it handles;

(c) analyses the incident to determine the cause;

(d) recommends measures to contain the damage caused by the incident and mitigate the impact or eliminate the cause;

(e) if service is impacted, requests that business continuity plans be implemented until normal service can be restored;

(f) reports regularly to the Security Authority via NDM.

[5] unless they have been forensically trained

17. The Security Authority decides what and how to communicate internally and externally and authorises requests by IRT/NDM for mutual assistance/external help if needed.

18. Follow up and remediation:

    (a) After incident resolution, IRT requests that procedures to restore normal service (disaster recovery if needed) are started.

    (b) When no advantage is to be gained from further investigation, IRT stops forensic activity, reporting and documenting the incident and any modifications make to the CIS during incident handling according to established procedures.

    (c) Following incident resolution, IRT consults NDM to update network defence measures of the organisation and together with the Information Assurance Operational Authority (IAOA), the security operating procedures of the affected CIS as required.

    (d) The reported or recommended modification of the CIS and its network defence measures should be notified to the SAA.

19. Speed is essential when dealing with potentially malicious disturbances of computer and communications networks. Incident handling processes must be prepared in anticipation of disruptive events of accidental or malicious nature. Before incidents happen, incident handling exercises should be scheduled by the NDM and rehearsed by the IRT at a frequency commensurate with the criticality of the CIS and the impact its disruption would have on the work of the organisation making use of it, typically every six months.

20. While some incidents affecting CIS can be predicted and responses to them prepared in advance, incident handling processes must be able to handle unforeseen events.

21. Incidents affecting CIS should be processed according to general incident handling procedures affecting any communicating and information systems of an organisation except that, as described in paragraph 36, all details of the events and measures concerning the incident should be classified unless further investigation determines they can be disclosed.

22. Communications about any incidents affecting CIS must be controlled and Security Authority of the organisation to which the CIS belongs will decide what and how to distribute such information as described in paragraph 47. External announcements may not be handled by any other than the Security Authority or its authorised spokespersons/liaison officers.

23. The IRT will report its findings to the Security Authority which coordinates sharing of information about the events. If a CIS Security Incident of sufficient importance and severity is reported, upon request by IRT/Network Defence Management, the Security Authority will consider requesting external assistance of a technical or other nature, if applicable and needed invoking the solidarity clause of the Treaty of the Functioning of the European Union, Title VII Article 222.

III. INCIDENT ANALYSIS

24. Having set up a CIS to monitor, record and report its behaviour, it will generate alerts about events which could be breaches of security. As it must be assumed that all events are due to incidents which may be security-related, the integrity and authenticity of the event data collected must be preserved and an unbroken "chain of custody" guaranteed.

25. Events can be of any kind: slow or different response of the CIS to user input, unavailability of all or some services offered by a CIS, theft of CIS components, break-in to facilities housing CIS, discovery of malware or eavesdropping tools, policy violations, malfunction of the CIS, inability to reach point of presence of a CIS (e.g. due to natural disasters, civil or other disturbance), etc. Unusual events which could be incidents are also often reported through alerts sent by intrusion detection and prevention systems (IDPS) or other network defence components which monitor the CIS, but may also be received from partner organisations, the media, members of the public and other sources of external information.

26. Not all events are incidents. Nor do all incidents affect the security of the CIS or the information it handles, or the security or vital interests of the EU, its member states and partners.

27. Unusual events or alerts which could be incidents are usually detected by or reported to "first responders". The first responders must rapidly determine whether the events are normal or expected behaviour of a CIS (for example after completing a planned change order).

28. First responders are often members of ‘operations support’ who monitor network and computer systems 24x7, or members of the ‘help desk’ who handle user requests for problem solving and/or new or modified services. First responders must be aware that they need to treat all abnormal behaviour as a potential incident affecting security. First responders must also be aware of the need for confidentiality when any incident affecting CIS is discovered or reported. First responders must therefore avoid actions which could destroy information (evidence) required for forensic investigation. In most organisations, the task of first responders is primarily to check whether planned changes, “expected” behaviour, etc. of CIS could explain the observed events, in order to determine whether the reported events could be due to a security incident or not.

29. Security incidents which the IRT has classified as "minor" should be first handled by the first responders using prepared procedures described in the ANNEX to these guidelines. Note that all use of such procedures must be audited and the related incidents always reported to the IRT.

30. If it cannot be established that the events are not related to security, or if the prepared procedures are unsuccessful, first responders must escalate the event to the IRT of the organisation.

31. While it is customary to record all events reported by the CIS, the analysis of such data is to be performed routinely even in the absence of confirmed security incidents, typically by automated tasks which run at different frequencies, e.g. continuously, daily, weekly, monthly and yearly. Such tasks should be of increasing thoroughness. Thus events which are continuously monitored typically are those due to security incidents which are highly likely to occur, while the less frequent and more in-depth analyses of event data aim at detecting less likely and/or more stealthy attacks on the CIS. In any case, IRT must be authorised to access the entire set of stored event data.

IV. SECURITY INCIDENT HANDLING

32. The generic process used by the IRT must:

    (a) collect, correlate, and analyse information about the event;

    (b) trigger incident response processes;

    (c) inform affected parties; and

    (d) if possible, determine the course of and cause of the incident.

33. The data recorded by CIS components and security monitoring tools will provide the bulk of information used in investigation a security incident. Other methods such as forensic analysis of storage media[6] of CIS components may also provide useful information. The procedure (digital forensics) must gather and analyse data in a reproducible and consistent manner to ensure that the evidence is as free from distortion or bias as possible, and to be able to reconstruct a record of what has happened. It must answer the 6 Ws in as great detail as possible, albeit it is difficult for (e) and (f) below:

    (a) What happened?

    (b) When did it happen? What is the timeline of the incident?

    (c) Where did it happen? Which CIS/computers were affected?

    (d) How did it happen? Which exploit was used against which vulnerability?

    (e) Who did it? Who was the threat agent?

    (f) Why? What were the motivations of the threat agent?

[6] This is not always possible e.g. if the amount of data to be searched is so large that its analysis is impossible or would take an inordinately long time.

34. Investigators must be aware of the regulatory and legal restrictions valid in the jurisdiction(s) responsible[7], especially when cross-border events are involved.

35. Because of the very powerful nature of forensic, security testing and incident investigation tools and owing to legal restrictions on their use, specific mandates must be given to the incident handlers, to ensure that only authorised personnel can use such tools and to protect the handlers from criminal prosecution and disciplinary action.

36. In the context of CIS handling EUCI, personnel involved in investigation should be in possession of suitable security clearance. When investigating security incidents, details of the event, its investigation and the response thereto must be handled as sensitive information. If CIS handling EUCI are involved, information identifying a specific CIS or vulnerabilities thereof will be classified at the level of CIS. Sanitised information about a vulnerability, attacks, detection and protection methods should be handled as sensitive and may be exchanged with partners.

IV.1. Incident Response and Corrective Action

37. The IRT to which the potential security incident is reported must be qualified and trained. It must consist of, or be able to call in, experts in the forensic examination of the hardware, firmware and software components of the CIS affected and of other electronic devices [8] which could be instrumental in clarifying the nature and cause of the incident, as well as enforcement officers empowered to take action against identified perpetrators as appropriate.

38. Key to the effectiveness of the IRT is basic training of its members and their continuous professional education such as attendance of specialist seminars, participation in training for methods and tools used by the IRT and for the security features of components of the supported CIS, certification of team members in their special area of competence, etc.

[7] i.e. tools must be chosen and validated so that, when used by qualified personnel according to validated, documented procedures, the information collected is acceptable as evidence in legal or disciplinary proceedings.

[8] e.g. cameras, smartphones, storage media, etc.

39. IRT operating procedures must be established at least for:

(a) criteria for rating the impact (seriousness) of the incident[9], or whether it is not an "incident" at all;

(b) methods for the forensic investigation of the CIS itself and its components and for validating such methods;

(c) methods for determining whether the incident is a result of technical factors in design and implementation, failure due to wear and tear, or whether the cause is accidental or malicious personal action;

(d) procedures, roles and responsibilities of IRT and other investigative bodies should the incident be the result of actions of persons or groups of persons;

(e) criteria for informing affected or interested partners in and outside the EU, and if needed to call for concerted action to defend against the incident and/or to take concerted action;

(f) the nature and frequency of reporting on incident response activity;

(g) reporting and command lines between the IRT, the organisation's Security Authority and senior management, the IAOA of a CIS and support staff responsible for maintaining and running CIS;

(h) methods and procedures to be observed for obtaining and distributing unclassified and classified information about incidents affecting the security of CIS from and to IRT teams, which can be inter-institutional, those of other entities and/or Member States;

(i) procedures to follow when communicating information about CIS security incidents between members of the IRT and its assistants, to other parties in the organisation, member states, other affected organisations, other IRTs, end-users, the general public, the press, law enforcement, etc.

[9] e.g. as outlined in the Annex to the Information Assurance Security Guidelines for Network Defence of CIS: IASG 4-01.

40. Incidents involving Controlled COMSEC Items or Cryptographic products require special treatment specified in the Instruction Manual Crypto And COMSEC Material Management (TECH-I-01), such as the involvement of personnel holding the required authorisation to handle such items.

41. Available EU expert knowledge regarding the establishment and tasks of a team of experts for emergency response, for example in ENISA, should be the basis for the structure and functioning of the IRT supporting one or several CIS.

42. The IRT initiates investigations in a forensically sound manner to establish with certainty whether the incident affects security, in which case it is treated as a CIS security incident.

43. If it is determined that there is no security impact, the incident is not categorised as a CIS security incident and handed back to the operations support teams for

    (a) implementation of business continuity plans (BCP) if service is impacted;

    (b) restoring full service up to the implementation of disaster recovery (DR) measures; and

    (c) modifying operating procedures as needed to reduce the likelihood of repetition of the observed events.

44. For the reasons mentioned in paragraph 21, details of CIS security incidents and any items of information which could disclose security weaknesses of CIS or attacks on them are classified. It is prohibited to record any details regarding CIS security incidents using unclassified systems, including those for recording problems and requests deployed in the context of service management frameworks. Details of the CIS affected or the nature of the events reported cannot be entered into any problem tickets created for the purposes of service delivery management. For such purposes, it is strongly recommended to disclose only that another team has been tasked with resolving the problem, in any 'work ticket' entered into service delivery management systems for problem and request handling.

45. Once CIS security incidents have been reported and confirmed, corrective actions must be implemented in a manner commensurate to the risk posed by the alert or reported security event. The IRT will call in any experts required and lead a forensic team to investigate the incident. The forensic team will evaluate the importance of the incident and co-ordinate activity in finding the cause, putting business continuity plans into action in the interim and restoring normal service. The IRT will determine whether the availability, integrity and/or confidentiality of CIS or of the information handled by CIS have been compromised. If this is the case, the IRT may need to trigger the BCP for the CIS to maintain services required until full service has been restored, or DR plans to restore full service.

46. As outlined above, the IRT will report on its findings to the Security Authority of the organisation or its delegate via the NDM on a regular basis.

47. The Security Authority will authorise communication as needed with partners of the EU, affected users, the person(s) discovering the incident, and the general public at its own discretion, preferably via experts trained in such matters as in paragraph 49 below. Where appropriate, the Security Authority will report incidents which can or could significantly compromise the security and/or essential interests of the EU, its Member States or partners to the Council Security Committee.

48. The Security Authority will decide, upon request of the NDM, whether it is necessary to request outside help of technical or any other nature at the disposal of the EU, its Member States and partners. In case this is requested, the Security Authority of the organisation will decide whether its IRT will continue to lead the investigation or whether another investigative body should take over.

49. For the purposes of referred to in paragraphs 22, 48, 55 and 39(i), external communications should be carried out by trained spokespersons or liaison officers authorised to deal with the press, law-enforcement agencies, the general public, etc.

50. At regular intervals during the investigation, for prolonged investigations at least weekly, the IRT to which the incident was first reported will determine whether to continue with investigations or to stop the work if no further gain is to be expected.

51. Records must be kept of all, even minor, incidents affecting CIS, preferably in secured redundant locations. This is needed to determine whether certain incidents keep recurring, whether there are combinations of incidents which happen simultaneously, etc. If such patterns or recurrence is discovered, while each incident still needs to be handled in isolation, the root cause for repeated incidents or patterns of incidents which frequently occur together, etc. must be sought by an in-depth problem resolution process independent of the individual incident handling process.

52. The security operating procedures and network defence measures for the CIS must be reviewed after any security incident and changes recommended to the IAOA of the CIS to reduce the likelihood of repetition (risk).

53. The SAA must be informed of any changes made to the CIS or to its network defence measures.

IV.2. Information sharing and escalation mechanisms

54. Incident response procedures must provide for secure methods of sharing information about potential and actual security weaknesses, attacks, etc. with partners in order to

    (a) increase situational awareness of the NDM to threats and vulnerabilities beyond those affecting the own CIS; and

    (b) inform management, partners and users of progress in investigations and service restoration efforts following incidents.

55. Documented escalation processes must be established to ensure that management and potentially affected internal and external parties are informed. The persons authorised to initiate external communications with external partners, law enforcement agencies, etc. must be identified in such procedures and authorised by the Security Authority.

56. The mechanisms must be such that there is no delay in sharing such information and that the content thus shared is truthful, reliable and protected to ensure the appropriate level of confidentiality and integrity. Participants in network defence information exchange mechanisms should therefore agree to commit their organisation to exchange and share information about potential or actual modes of attack as well as about breaches of security they become aware of or are experiencing themselves and commit to help one another in case any participant experiences breaches of security of inadvertent or malicious nature.

57. Once a breach of security has been verified and prioritised, information must be shared among the participants of the network defence effort and a course of action proposed to enable others to make suitable corrective or defensive changes in the security measures. Multiple-redundant secured means of communication must be established for this, since standard means of communication may not be available during an incident.

58. Alerts can also be used to notify participants in the network defence information exchange mechanism about new vulnerabilities or new attack methods being used against CIS. Such bulletins are regularly issued by CERT and CSIRT networks. In order for this to work, only authorised personnel[10] are allowed to introduce items into the information sharing mechanism. Every participant must nominate a trusted introducer and back-up personnel. These should establish relationships of trust e.g. in face to face meetings.

_____

[10] Such persons must not only possess personnel security clearance as required and need to know but also be expert at analysing alerts and researching various sources to determine the nature of the weakness being exploited, the potential impact and potential responses in a timely manner.

V. GLOSSARY

BCP	Business continuity planning (BCP) or contingency planning describes the set of measures and workarounds invoked during an outage of a CIS to ensure availability of the required business service, potentially at a reduced level, until full service is restored. International standards[11] for developing and using such plans must be referred to. The CIS Business owner, together with the SAA where applicable, must approve business continuity and disaster recovery plans.
DR	A disaster recovery (DR) plan describes the set of measures taken to restore full service after an outage. Disaster recovery typically requires that system backup, original software distributions and set-up guides, configuration guides, as well as spare or redundant hardware are readily available, possibly at a different location.
CERT	Computer Emergency Response Team – the term is often used for CSIRT teams too - see below.
CERT-EU	CERT-EU is the Computer Security Incident Response Team set up by the EU institutions, bodies and agencies to support them in protecting themselves against intentional and malicious cyber-attacks which could hamper integrity, availability or confidentiality of their IT assets and harm the interests of the EU. When invited by the constituent concerned, CERT-EU may provide assistance for incidents happening in their classified networks. The scope of CERT-EU's activities covers prevention, detection, response and recovery. See ST 6738/15 for details.
CIS	Communications and Information System.
CIS business owner	Represents the interests of the entity or entities who will benefit from the functionality provided by the CIS, and is thus in a position to define which level of risk is acceptable.

[11] ISO/IEC 27031 Information technology -- Security techniques -- Guidelines for information and communications technology readiness for business continuity,
ISO/IEC 24762:2008 Guidelines for information and communications technology disaster recovery services.

CSIRT	Computer Security Incident Response Team, often called a CERT. This function forms part of the Network Defence Management structures supporting the CIS.
Event	Any unexpected, unusual or deviant behaviour of a CIS.
Security Incident	A security incident is declared when the analysis of an event shows that the security of the CIS and/or of the information it handles and/or stores has been compromised by the event.
Forensic	Suitable for presentation in a tribunal or court of law. This requires the use of validated (proven) documented investigation methods, their use by appropriately trained experts, and accurate recording of the process and its results, in a manner which preserves a chain of custody, to guarantee that the evidence has not been modified or tampered with by the methods used or since its collection.
NDM	Network Defence Management - the management and support structures which provide network defence for one or several CIS, of one or several organisations.

ANNEX

Handling Of Minor Security Incidents

1. Incidents which are to be dealt with as an operational task must be reviewed by the IRT and classified as "minor".

2. The handling of frequent minor security incidents must as a rule be performed by first responders but must always be reported to the IRT which will analyse their potential impact in isolation and in relation to other incidents and sources of security information.

   Examples of such incidents are

   (a) loss of configuration of device(s);
   (b) inability to access (CIS) network resources;
   (c) problems with storage device(s) such as FDD, Disk arrays, …;
   (d) problems with backup/restore;
   (e) out of date patch levels of software;
   (f) out of data malware definitions and detection (engine) software;
   (g) absence of a memory-resident module required;
   (h) application crash;

   etc.

3. Minor incidents are to be first treated using a documented service-restoration processes defined by or in conjunction with the IRT. Such a process should as far as possible be automated, for example as a standalone executable which restarts missing services. However, see 6 below.

4. The use of such automated response procedures or programs must be restricted to authorised users, usually first or second level support personnel, and their use must be audited and recorded either by automatic logging or by documentation of their use in a hardcopy or electronic log book. The response processes should contain checks and balances so that, if the incident cannot be speedily resolved by the standard response mechanisms, experts can quickly intervene to limit damage and collect further evidence.

5. In any case, such prepared procedures should not be used if a problem is widespread or is affecting many different CIS or components of CIS in a short time.

6. The prepared procedure should be capable of being started by an unprivileged account, for example those held by first level support for the CIS, but 'business' users of the CIS should not be able to use such prepared procedures, access to the procedures being preferably limited by technical measures.

7. The prepared procedure should also ensure that forensically relevant information is not corrupted or deleted in the attempt to restore the missing service, e.g. by creating a 'memory dump' prior to starting the attempt to restore a missing process.

8. Alternatively, if the CIS has automatic monitoring capabilities which can detect such common security incidents, the monitoring solution could be used to trigger prepared procedures ensuring that checks and balances are built into the procedures to prevent abuse of such a mechanism which can itself cause a security incident.

9. Further, if one or at most two successive attempts at using the prepared procedures does not eliminate the problem successfully, all further attempts to use the prepared procedure must be stopped, upon which the security incident is escalated to the IRT supporting the CIS as described in paragraph 30 of the main document, e.g. if isolating a malware-infected device from the CIS and running an antivirus scan does not succeed in eliminating a malware infection.