Council of the
European Union

Brussels, 5 June 2015
(OR. en)

9650/15

CSCI 31
CSC 135

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Information Assurance Security Guidelines on Network Defence

Delegations will find attached the Information Assurance Guidelines on Network Defence as approved by the Council Security Committee on 4 June 2015.

This page intentionally left blank

IA Security Guidelines on Network Defence

IASG 4-01

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'), are designed to support implementation of the CSR and the Information Assurance Policy on Network defence[1] (IASP 4).

2. These guidelines describe minimum standards to be observed for the purpose of network defence of communication and information systems (CIS) and interconnections between them. The security authority having created a Network Defence Management (NDM) structure, the document describes the network defence measures and processes required in some detail. The guidelines also require provision of escalation and information procedures as well as methods to invoke mutual assistance in dealing with incidents.

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 these security guidelines as a benchmark when EU classified information is handled in national structures, including national CIS.

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

6. Network defence measures are needed owing to the increasing complexity and interdependence of CIS, the widespread availability of powerful attack toolkits, the increasing involvement of criminal and intelligence organisations with access to extensive resources, as well as the increasingly frequent, cross-border, targeted and sophisticated nature of current attacks on CIS, as well as organisational or architectural changes such as the use of outsourced services, virtualisation of physical components and deploying systems as cloud services.

[1] Doc. 8408/12

7. Network defence nowadays includes the capability of co-operation between Security Authorities across organisational and national boundaries.

8. While the physical security aspects of facilities housing a CIS, accurate and up to date CIS documentation, choice of vendors, choice of products and the security of personnel providing and supporting network defence measures are all crucial to the level of security a CIS can provide, these guidelines do not go into detail regarding such aspects of network defence.

II. NETWORK DEFENCE

9. For network defence to be effective, trained personnel must be made available to design, implement, and regularly review the measures and processes required to achieve and maintain a degree of security commensurate with the importance and sensitivity of the CIS in the face of an ever changing threat and vulnerability scenario.

10. While these guidelines reflect good security practice at this time, the constant disclosure of vulnerabilities and weaknesses in CIS components, as well as of new methods of attack and defence for communications and information systems require network defence management (NDM[2]) to keep up to date with new threats, new modes of attack and new protective methods.

11. These guidelines require that network defence measures are implemented not only at the level of the individual CIS but also that they should be merged into a central network defence capability within an organisation.

[2] The term network defence management refers to a structure and roles which may be assigned to persons holding other roles provided there is no conflict of interest.

12. The measures must be based on and integrated into the ongoing risk management process and the security accreditation strategy of each CIS. The measures set out in these guidelines must be adapted by the NDM and IA Operational Authority for the CIS in question. Network defence measures must themselves be robust and should not be interdependent[3].

13. Network defence measures also include methods to communicate with affected users, management, etc. They need to take into account all architectural aspects of a CIS: hardware, firmware (embedded software), software, processes and personnel.

14. Measures which dissuade would-be attackers should be also integrated into the design of the CIS. Such measures can be technical, such as the use of multiple authentication methods or, if applicable, several different encryption products. Dissuasion can also be, for example, widely advertising the capability of the organisation to respond to attacks. These guidelines are grouped into measures which provide:

    a) security assurance measures of a preventive nature: which ensure that CIS are built securely and have features which enhance detection and response to attack and provide resilience to disturbance whether accidental or malicious:

        – design and development aimed at building CIS which are able to detect, repel and survive disturbances such as:

            - system hardening
            - internal segmentation
            - filtering of various kinds
            - use of strong authentication (e.g. digital certificates, smart card)
            - security measures for virtualised environments

[3] i.e. there is no link between different measures so that failure of one measure does not result in compromise of the CIS because other measures compensate for the absence of one or more others

– provision of technical protection:

  - ingress filtering against malicious content, e.g. malware protection packages, firewalls, content filters, as well as egress filtering against information leakage and other illicit outgoing content[4];

  - intrusion detection and prevention;

  - design features which enhance resilience, i.e. which enable the CIS to minimise the impact of attempted or successful attack;

b) awareness, education and training of users with standard or elevated privileges [5] in secure use of CIS, as well as in detecting and reporting unusual behaviour:- "the human firewall";

c) security operation and maintenance measures: which ensure that the security of the CIS is maintained and monitored

– configuration and change management;

– alert management, patch management;

– network discovery, mapping and monitoring to detect unauthorised changes;

– assessment of the vulnerability of components of the CIS to known avenues of attack;

– detection of unexpected system behaviour (e.g. using Intrusion Detection and Prevention Systems, preferably centralised reporting to a Security Information and Event Monitoring solution); and

– review of rule sets.

[4] Consider internal boundaries of the CIS, especially in virtualised environments, to/from mail system, etc.

[5] A user who can change system parameters or modify the work of others is considered to have elevated privileges.

d) security restoration[6] measures: which ensure that should a security incident occur, the CIS is returned to a secure and functional state

- processes for forensic investigation and follow-up in compliance with regulatory and legal constraints, especially in cross-border incidents;
- incident response processes
- contingency, business continuity, and disaster recovery processes; and
- relevant documentation and information sharing.

and

e) management commitment.

III. SECURITY ASSURANCE

III.1. Design and Development

15. CIS design or architecture must be performed in a way that, as far as possible, a system is still able to provide the required functionality even in the event of inadvertent misuse or malicious attack. This is especially important if the functionality provided by the CIS is of critical importance in a crisis or emergency. If it is more important to protect the information handled by the CIS than to ensure its availability, its design should facilitate isolation of compromised sections in order to minimise and limit the impact.

16. CIS must be so designed as to take into account potential known sources of failure. Established and documented risk management methods must be used to reproducibly create such lists. While checklists[7] of potential vulnerabilities, weaknesses and causes of failure in CIS, the buildings housing them, etc. must be used in order to ensure that known sources of failure are covered during the analysis, used alone they are insufficient to describe all potential sources of failure which must be avoided or mitigated when (re-)designing CIS.

---

[6] Measures which enable rapid recovery of the CIS from incidents while preserving evidence for potential later use against malicious perpetrators and using lessons learnt to further improve the ability of the CIS to resist disturbance.

[7] Such as those built into risk management application packages

17. In order for resilience to be built into a CIS to a degree proportional to its importance in the eyes of the CIS business owners and users, an exercise must be conducted which determines what are the consequences of different kinds of failure or event on the functionality of the CIS. This exercise is best done in a team involving technical experts as well as non-technical users. The consequences of simultaneous multiple failures should also be considered in the CIS design phase.

18. To build resilient CIS, single points of failure[8] in the system must be actively identified and eliminated in the design phase. The use of multiple redundant components should be balanced against the risk due to the increased attack cross-section of the final system.
If a CIS or group of CIS depends on the availability of external services, e.g. power and cooling, network connectivity, etc., such services must be designed to be multiple-redundant either simultaneously in real time or as contingency measures to be implemented in case of loss of service. Should it not be feasible to completely remove the single point of failure, mitigating measures must be included in the design to reduce the risk associated from such failure to an acceptable level.

19. The methodology to be used to identify risks and mitigate them in the CIS design phase must be documented and approved, subject to periodic revision, by the (security) management of the organisation. Once risks affecting the resilience of a system have been identified, they must be handled by the risk analysis methodology chosen by the organisation.

20. Secure CIS must be built using secure components. The security requirements for such components should be derived and documented to meet the desired level of security for the CIS e.g. in the SSRS. In procurement, tender and contract clauses must specify minimum requirements for the security level of hardware and software components and where appropriate, for the maturity and the security and software engineering capability of suppliers.

8 Such points of failure can be for example communication lines, personnel, buildings, electronic devices, software packages, alarm systems, access control systems, etc.

21. The configuration of such components must be fixed using customised tested secure standard builds. Sets of standard build recommendations for various CIS components are available from vendors and special interest groups on security in government and industry. Their indiscriminate use can, however, interfere with the required functionality of the CIS. Risk management must be performed to determine which features of such standard builds must be implemented and which can be omitted in the interests of functionality without compromising CIS security. Such customised standard builds must then be documented, tested regularly against vulnerabilities and weaknesses, and revised as needed, to ensure the security of the CIS over its entire lifetime. The result of this initial configuration and testing exercise flows into the accreditation process.

III.2. Provision of Technical Protection

22. Tools and methods are usually divided into device-oriented and boundary-oriented solutions.

Device-oriented tools

23. In order to ensure resilience against common security deficiencies, where technically feasible and justified after risk assessment, protection packages[9] must be deployed, updated, and configured correctly on all fixed and mobile[10] components of the CIS.

24. Products should be used which provide for central management and monitoring ('enterprise grade'), and which can generate real time alerts. Ideally they should report to a central security monitoring and reaction system[11] as described below. The solutions must complement one another and be compatible with CIS monitoring systems.

---

[9] e.g. antivirus, full disk encryption.

[10] USB sticks, mobile phones, smart phones, tablet PCs, etc. which could be connected to fixed CIS components.

[11] e.g. Security Information and Event Management (SIEM), Governance, Risk, and Compliance (GRC) products.

Boundary-oriented tools

25. Boundary protection is a key component of the measures which defend the CIS. They include various "services" aimed at intercepting malicious content before it crosses the CIS boundary, whether in the incoming or outgoing direction. The interconnection policy [1] covers such aspects. The boundary can be a fixed physically identifiable border in isolated CIS. In those with interconnection capabilities, the boundary is to be based on trust: the limit up to which a uniform degree of protection and security policy apply, anything beyond that being considered "partly trusted" or "untrusted". In segmented CIS with different security zones and/or in the event that CIS are implemented using virtualisation technologies, internal borders at which such tools can be deployed will exist but these may not be evident as physical boundaries. The Information Assurance Guidelines on Data Separation [2] should be consulted on this subject.

26. Current boundary protection services include: cryptographic gateways, filtering by network address, protocol and application, mail and web content filtering, data loss prevention systems, "data diodes", guards and/or security gateways[12] as well as intrusion detection and prevention systems. Filtering is facilitated if the set of communication protocols used by a CIS or set of CIS is limited by design.

27. The tools chosen must be complementary to one another so that filtering rules which cannot be implemented on one device can be placed on others. The tools should also be able to feed their output to a central security monitoring, analysis and reaction system as described below.

Intrusion Detection and Prevention

28. Separate guidelines have been produced regarding the deployment of intrusion detection and prevention systems (IDPS) which is only outlined here:

    a) the need for IDPS and an estimate of its extent and severity shall be established based on the estimated threat scenario to which the CIS is exposed, its security requirements, its technical features and the volume and nature of the information it handles;

[12] See glossary Guard, Gateway.

b) the nature of the IDPS sensors, their location and number must be planned and their effectiveness tested prior to scale up and large-scale use of IDPS;

and

c) the IDPS must be constantly tuned by trained personnel in order to adapt to the security threats and technical features of each supported CIS.

III.3. Awareness Training of Users

29. Raising awareness to what could be accidental or malicious disturbance of CIS functionality must be part of network defence. The methods of contacting support for handling security events must be communicated and ideally the contact point[13] staffed 24x7, with the persons handling the calls able to call in experts if preliminary investigation does not exclude a security incident.

30. Such a program involves:

a) alerting users to currently observed attacks or indications of malware activity;

b) suggesting methods to improve user behaviour for different target audiences such as unprivileged users, technical staff, privileged user, developer, security staff, etc.; and

c) enhancement of and review of the perceived value of security to their work for staff at all levels. Users, especially those with managerial or political duties, must be addressed in an appropriate manner to show how network defence measures can improve continuity, security, and quality of service.

31. The level of security awareness of all CIS support staff must be maintained at a high level, for example by:

a) continuous professional education in the use of security features and toolkits;

[13] The contact point is usually staff who perform round the clock support e.g. in a network operations centre.

b) testing of the knowledge of security features of the operating systems and layered products and custom applications supported; and

c) job rotation to ensure that should a key person become unavailable, others are on hand with the required knowledge.

IV. SECURITY OPERATION AND MAINTENANCE

IV.1. Configuration and Change Management

Configuration Management

32. Configuration management is required for network defence. It involves creating an inventory of CIS components, version control of deployed products as well as control of the settings of the products deployed.

33. As a rule, automated toolkits[14] are to be used to populate and maintain the configuration management data base (CMDB) in real time and keep historical records of the assets making up the CIS for correlation with other sources of security information. The configuration of such CMDB tools themselves must also be documented separately as a function of time.

34. While in small CIS, manual maintenance of its CMDB over time can be achieved by piecing together the initial set-up and subsequent change records, this is prone to human error and intervention is needed when undocumented changes are discovered.

35. Besides the inventory of physical and soft assets, the actual settings of configuration variables of hardware, firmware, operating systems and layered products making up the CIS need to be defined. The variables and their settings must be selected on the basis of best practices and the desired configuration documented. Where technically feasible and justified, role-based (user profile) configuration management tools should be preferred and the tool settings monitored.

[14] e.g. ITIL™ toolkits

Management of requests for change and exceptions

36. Network defence must provide for an effective and efficient process to manage requests for changes and requests for exceptions or variance from established standards and security policies. While change requests could be considered a special kind of alert, they are usually managed by a dedicated process which ensures that such requests do not lower the security level of a CIS. Although problems and incidents often require "on the fly" changes to a CIS, such emergency changes must also be subsequently documented by a "request for change" and evaluated for impact as with regular change requests. Changes can be of a routine type which do not need risk-assessment every time they are submitted and can be "pre-approved" for security purposes once the initial risk assessment has defined a framework for their execution. Other change requests, however, always require the submitter to reflect on whether the change could result in a change of the security posture of the CIS. They must be submitted well ahead of time to enable their potential impact on security to be assessed and contain the following details, of which at least a, d, e and f below are required for security:

    a) the difference between the original and the changed CIS;

    b) an informed opinion as to whether the proposed change is technically justified;

    c) the measures which ensure service levels during and after the change;

    d) a back out plan in case the CIS does not perform properly after the change;

    e) acceptance by the CIS business owner of the resulting risks, service interruptions and his approval for the change to take place at the requested date and time; and

    f) evaluation of a need for reaccreditation or renewed testing.

37. For requests for exceptions (variance) at least the following must be documented:

    a) the difference between the standard solution and the requested variation;

    b) what alternatives have been tested, if any;

c) the business reason why the standard cannot be followed;

d) what mitigating factors reduce the risk of the deviation from security policy, guidelines or standards;

e) the period for which the exception (variance) is being requested;

f) an informed opinion as to whether the proposed variation is technically justified; and

g) acceptance by the CIS business owner of the resulting risks and his approval for the variation to be implemented at the requested date and time.

IV.2. Alert Management, Patch Management

38. Network defence must include a process for obtaining and evaluating security alerts from:

a) "feeds" about newly discovered or zeroday[15] vulnerabilities, attacks, etc. provided by vendors of operating system (OS) and layered products, security product vendors and other security organisations;

b) security monitoring tools of various kinds[16] which report ongoing malfunction or attack:

c) recommendations of vendors, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), other NDM teams supporting similar infrastructures, security experts and security researchers (hackers) issuing bulletins; and

d) planned modifications to the CIS.

39. Rapid and effective methods must be in place for screening alerts, determining their relevance to the CIS and the urgency for corrective action to be taken.

---

[15] Zeroday vulnerabilities are those which are made public on the same day as a fix is published by a vendor.

[16] e.g. IDPS, malware-protection 'antivirus' packages, data loss prevention systems, identity management and access control products, security information and event monitoring (SIEM), spam filters, etc.;

40. Trained personnel who know the functional purpose and technical details of the CIS must evaluate, score and prepare information about these alerts for distribution as appropriate.

41. Alerts received must be fed rapidly to these experts for timely evaluation of their potential relevance and urgency using their knowledge and the information stored in the CMDB. While many such alerts arrive with a severity rating such as a Common Vulnerability Scoring System (CVSS) score, specific workarounds and business constraints present in a particular CIS may justify assigning a lower or higher rating to the alert.

42. Processes must be established for internal information of management and users, as well as for alerting and exchanging information with trusted partners such as IA operational authorities, other network defence experts, emergency response team members, etc. Personnel trained in handling such alerts[17] are to be entrusted with the communication of such information.

43. A documented decision must be taken as to whether

    a) the alert represents a potential or real security problem and needs to be acted on with an assigned level of urgency,

    b) needs no action because the product or version affected is not in use, other workarounds are in place, or

    c) corrective action conflicts with business requirements for the CIS.

44. In the event that a decision is taken to harden the CIS by applying workarounds or patches, a change request must be prepared and submitted as outlined in paragraph 36.

[17] Authorised spokespersons of the security authority

IV.3. Ongoing Event Logging, Monitoring and Consolidation

45. When routinely monitoring a CIS, as it is not known up front which information could be needed later for investigation into security incidents, it is necessary to record as much information as possible and archive it, within legal and regulatory constraints, while analysing a subset of events of high relevance to the security and performance of the CIS for real-time or near-real-time alerting. To minimise the effort required to follow events from various sources and generate a security 'picture' of the CIS in real time, a central collection of security events is considered key to network defence measures. The individual CIS components must be configured to collect events of potential security relevance and generate log files. Usually events generated by different CIS components are, however, stored in different record formats. Log files stored on CIS components may also be corrupted or destroyed by malfunction or attack.

46. All events of potential security relevance, whether related to hardware, software or system performance, are therefore best immediately copied or exported to a dedicated device such as a "log server" or consolidator, preferably with technical restrictions allowing the source devices only to write to the log server, without filtering but with conversion of the different log file entries to a common record format. Such a collection also simplifies incident investigation and response. Access to the collection of security events must be monitored and limited to the minimum number of security administrators[18]. Analysis of log files should be performed on systems other than the log server. See also below paragraph 63 - 68.

    The Information Assurance Guidelines on Intrusion Detection and Prevention Systems [5] go into further detail on this topic. For monitoring large numbers of near-simultaneous events, consideration should be given to the use of visualisation techniques interpreted by trained personnel.

[18] To avoid conflict of interests, the security administrators should not be privileged users of the systems being monitored.

IV.4. Network Discovery, Mapping And Monitoring

47. In order for the security of CIS to be maintained, it must be set up for continuous security assessment and monitoring.

Vulnerability assessment

48. Here this term refers to the technical, usually tool-assisted, testing of a CIS[19] performed prior to its release to production, to determine whether it has known weaknesses and vulnerabilities. Such testing must be repeated after changes to the CIS, when a security incident has occurred and/or corrective action has been taken to fix discovered weaknesses. Should the threat scenario to which a CIS is exposed change, it is also necessary to perform Vulnerability analysis to detect weaknesses against the feared threat. Vulnerability analysis is also performed routinely during the lifetime of a CIS.

49. It includes both the "scanning" of the CIS and any interconnections it may have using tools, as well as manual checking of tool findings for false positives and additional manual testing for false negatives.

50. As VA-scanning can be disruptive, measures to avoid disruption include:

    a) careful scan design and testing;

    b) notification and change management (during the learning phase);

    c) scanning - automatically, with manual fill-in as needed;

    d) identification of platform experts responsible for checking and fixing the reported weaknesses;

    e) checking for 'false positives' by the platform experts;

    f) generation of work tickets for fixing;

[19] Also known as pen-testing, vulnerability analysis or VA-scanning.

g) fixing of what can be fixed;

h) implementing and documenting workarounds of what cannot be fixed; and

i) acceptance of residual risk by the CIS business owner.

51. The design of the scan process must be performed on dedicated testing environments representative of the production CIS to determine the speed of the tools used, potential negative impact on CIS services and/or conflicts with other network defence measures. Tools used for scanning must be configured by experts but scanning itself may be delegated or performed automatically. The tools (attack machines) must be physically and logically protected and access to them restricted to the minimum number of experts. The output of the tools, its interpretation and handling must also be done by experts knowledgeable of the tool and its target CIS.

52. Details of the results must be handled as sensitive information as they reveal avenues of attack of the CIS scanned. Such VA-scan results must be handled by a minimum of persons. VA scan output of CIS is to be classified at least at the level of the CIS scanned.

53. As outlined above, after experts have checked the VA-scan results for false positives, work tickets must be generated by the NDM to support teams to remove or mitigate the vulnerabilities discovered and treat the resulting risks.

54. Such scanning also permits detection of devices or services which are different from the entries in the configuration management database.

Full security evaluation

55. A black-box, and/or white-box approach to VA-scanning supplemented with manual checking[20] may be performed. During black box testing, the scan is carried out without any knowledge of the architecture of the CIS, or with only an absolute minimum such as the range of network addresses for the CIS. During white box testing, details of the architecture as well as login parameters for CIS users of different levels are used to investigate its security in more depth. Such VA-scanning can also be performed from different network points external or internal to the CIS under study. It is always advisable to perform white box testing to ensure that the systems are internally resilient to the level of "state of the art".

56. Vulnerability Assessment can also target either the entire CIS or only special services offered by the CIS such as its interconnectivity, especially web and email if present.

57. The resilience of CIS users to social engineering techniques is nowadays also considered necessary when determining the security level of a CIS.

Infrastructure[21] vulnerability analysis (VA-scanning)

58. Prior to any scanning, the tools must be updated with the most current lists of known vulnerabilities.

59. In large networks, scans must be designed and so performed at such times as to capture the maximum amount of active devices of the CIS while minimising the likelihood of service interruption. Depending on the purpose, VA scans can be designed to include or omit password cracking and/or denial of service attacks.

---

20 This involves verifying the output of automatic tools by manually attempting to exploit the vulnerabilities and weaknesses reported by automatic toolkits, as well as attempting attacks not included in the automatic tools..

21 Layered products and operating systems/embedded software/firmware of servers, workstations, network devices, printers, scanners and other peripherals, etc…

Application vulnerability analysis

60. Network defence requires that applications be created securely and custom code checked for absence of known weaknesses. This is typically done using a combination of automated and manual methods. Most tools for automated application vulnerability scanning must, however, currently be supplemented with human intervention to ensure testing of all parts of the application.

61. While code review can be assisted by tools which detect programming errors, source code review requires experts in the programming language and/or frameworks used to ensure that logical and programming errors are absent. As applications often make use of shared libraries, compilers or interpreters which can be either in the operating system or add-on layered products, the security of such resources should also be regularly reviewed.

Other aspects

62. Beyond the technical audit of the CIS, procedural aspects regarding use of the CIS must be evaluated to identify potential risks and define countermeasures, e.g. to track information flows such as addition, access or processing of stored data, etc., in order to detect any unexpected or unauthorised processing which affects the integrity and authenticity of the information in the CIS.

Log file Management

63. All CIS events of potential security relevance are to be exported to a central “log server” or consolidator without pre-filtering.

64. These log file collections must be analysed at different intervals: daily, weekly, and monthly, using search and evaluation patterns of increasing complexity to detect events of different degrees of sophistication. For network defence to be most effective, a monitoring system as described in paragraph 46 is considered necessary.

Generation of Security Alerts and Warnings

65. A central IT tool should be used for consolidating, correlating, analysing and reporting the collected security events able to facilitate efficient and timely reaction to security incidents.

66. The central tools must not only collect and analyse events but are also able to initiate alerts about and actions against detected "attacks". Such tools must be customised by knowledgeable personnel to reflect the functional and security needs as well as "expected behaviour" of the CIS. The choice of tool must be dictated by the complexity, size and importance of the CIS to be monitored. Tools which check the security of the CIS against legal or regulatory requirements and issue compliance reports should be used. The tools must be resilient to disruption and unauthorised interception, and must be configured for maximum efficiency and effectiveness, reusing rules and component profiles across different CIS.

67. Such central tools are preferably a comprehensive source of security alerts, able to act independently of other services such as intrusion prevention systems, system and network device monitoring interfaces, help desk calls, etc. The alerts may be standard responses or messages to human operators able to take action to investigate and correct the "event". The central tools form part of the alert management process as described above and where technically feasible, must be the central location for triggering "standard reactions" to reported security events.

68. Depending on the geographical distribution of the attack and of the CIS itself, the central tools must conform to legal and regulatory constraints to enable the information collected to be used in action against identified perpetrators of breaches of security, even in different legal and regulatory systems as mentioned in 14.d).

IV.5. Implementation considerations

69. When deploying such a system, consideration must be given to the features of the CIS:

    a) Where is the important or interesting information stored, who accesses it, how is it protected, etc.?

b) In case of an incident, what kind of information will most likely be needed from the tool?

c) Which devices are most likely sources of security-relevant information?

d) Which parts of the CIS would cause most damage and disruption if compromised?

e) How many personnel resources are trained and available to work on the product?

70. Rules must be created or modified to reflect the above, their justification documented and the configuration stored off-line at a secure location as a historical record over time. As described in paragraph 74, these rule sets must be periodically reviewed. Such rule sets are for example:

- "Role" or "profile" templates used by the CMDB,
- access control lists (ACLs),
- routing tables,
- firewall rules,
- IDPS configuration,
- SIEM configuration,
- (incoming) content filtering rules, egress filtering rules[22]

71. When choosing such a tool, the ease of creating and modifying rules and reports as well as methods available which guarantee the integrity, accuracy and confidentiality of the information collected must be given high importance. The speed of analysis of input data and report generation must also be evaluated when selecting a solution.

72. The deployment of such a tool consists of the phases: test and experimentation, piloting, field testing, and scale up.

[22] e.g. rules set on mail, web content, data leak prevention, or web application firewall products

a) The test or experimental phase must use a dedicated test environment, with devices which easily can be restored to their original configuration in case of corruption. The test environment should be located physically close to the personnel performing the NDM function to enable manual checking of any anomalies detected by the system, the verification of reported events and the results of corrective action.

b) The piloting phase should be performed on a scale model of the final CIS with the desired set of components. The aim is to check the functionality of the monitoring tool and determine its performance under stress such as during a simulation of a massive barrage or when detecting a stealthy attack.

c) The field testing phase must be carried out on a representative segment of the production CIS after obtaining authorisation from the CIS business owner, to cover any potential impact on service. The aim of field testing is to determine the impact on service and to test various "response mechanisms" to simulated attacks. It involves a migration of the pilot set-up to production. It should concentrate on components which are most likely to be attacked and/or cause service disruption when attacked.

d) The scale up phase involves expanding the number of sources of security events, adding new rules and new standard response processes.

73. On the other hand, rushed deployment of such tools must be avoided as it can lead to overload of the persons monitoring the tools with large amounts of irrelevant information and the exercise falling into disrepute.

74. In order to maintain the security of a CIS, revision and management review of rule sets which are part of its network defence measures must be carried out regularly, as a minimum every 12 months, preferably every 3 months or more frequently, to determine whether they are necessary and sufficient for the data traffic needs of the CIS concerned.

V. SECURITY RESTORATION

Incident investigation and digital forensics

75. In the context of a network defence program, an incident investigation process common to all CIS in an organisation must be set up using reference works publicly available on this subject.

76. Separate guidelines [4] describe the requirements for incident handling of CIS in greater detail than in this document. These requirements are only outlined here:

a) analysis of the alert or unexpected events to determine whether they are security incidents or not;

b) analysis of the security incident to determine whether there is a prepared response to it or not, and if yes, triggering of a limited number of audited attempts to resolve the incident using the prepared procedure ;

c) if not successful, escalation of security incidents to the incident response team (IRT/CSIRT/CERT) which has the mandate and established documented processes to perform such tasks, as well as forensic and other toolkits, and personnel trained in their use;

d) collection of evidence in a forensically sound manner;

e) if there is a service degradation, initiation of business continuity processes to be able to provide services, possibly at a reduced level, until normal service can be restored;

f) initiation of service restoration processes to restore normal service in the shortest possible time;

g) information sharing with the Security Authority, affected users, management, peer organisations, other emergency response teams and external parties, by authorised persons according to established procedures as described in paragraph 42;

VI. MUTUAL ASSISTANCE

77. When the NDM discovers a threat[23] or actual attack on CIS, it must decide whether it can be dealt with internally as a technical matter, whether non-technical action is required, whether assistance from external[24] experts needs to be requested to react to the attack, or whether other measures, e.g. of a political or diplomatic nature, are required to deal with the threat or attack.

78. Beyond the ability to detect and react to unexplained and unexpected malfunction of CIS due to malicious or accidental activity, network defence requires criteria to be set up by which the criticality of a malicious attack can be categorised according to its impact on the security or essential interests of the entity using the CIS, the EU itself, its member states and/or partners.

79. While it is at the discretion of each NDM to define its own criteria, the Annex gives an example of how attacks can be rated.

80. When the NDM or emergency response team handling the CIS security incident considers it necessary to request outside assistance, it will follow established and approved processes and arrangements by which the organisation can request such assistance from other EU entities, Member States and/or partners, in order to defend CIS against and/or to respond to threats or attacks, especially those of a cross-border or cross-organisational nature.

81. Due to the need for speed when dealing with attacks, it is essential to test network defence measures and procedures by holding regular 'network defence' crisis management exercises, at least every 24 months or after any revision of such measures and procedures.

---

23 Threat in this context is a potential avenue of attack to the CIS

24 e.g. other NDM or emergency response (CSIRT/CERT) units, cybercrime units of law enforcement agencies, vendor support, etc.

VII. MANAGEMENT REVIEW

82. Network defence activity requires significant effort to set up from scratch. NDM personnel and the Information Assurance Operational Authority (IA OA) must be able to demonstrate progress in the security posture of a CIS. Regular reviews of the efficiency and cost-effectiveness of the security measures in place must therefore be held even when no incidents happen. Typically this will be performed at least yearly.

83. Each organisation must determine what is important for its daily work and prioritise measures being suggested internally and externally to the own organisation to find what fits their goals and needs. This results in the Security Authority being able to discuss with the NDM, SAA and IA OA of the CIS, whether the network defence measures in place are significantly reducing the severity and number of security incidents affecting it.

84. As indicated earlier, the threat scenario to which a CIS is exposed changes over time due to internal and external developments. Such changes may necessitate a change in the network defence measures used to protect the information in a given CIS.

85. Typical questions which need to be answered are e.g.:

a) What are the business benefits for current and alternative efforts?

b) Which measure(s) should we pursue to achieve a desired benefit?

c) How do we spend a given budget to obtain the greatest benefit from available resources?

d) Which effort should be implemented first to maximise benefit?

86. The occurrence of an incident is also an indication that the network defence measures need adjustment. After major incidents or after a series of repeated incidents of minor nature, a review of the procedures and technical measures implemented for network defence must therefore be performed. Lessons learnt have to be translated into recommendations which can be long term/ middle term/ short term and impacting many levels. These recommendations must be part of a follow-up program of management.

GLOSSARY

ACL	Access Control List
CERT	Computer Emergency Response Team, a team of experts trained to handle computer and network security incidents in a forensically sound manner.
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.
CMDB	Configuration Management Data Base
CSIRT	Computer Security Incident Response Team, a team of experts trained to handle computer and network security incidents in a forensically sound manner.
Attack	Any accidental or malicious misuse of information technology to alter, disrupt, deceive, degrade, or destroy a target computer or network, or the data and/or programs contained or processed in a computer or network used by the victim organisation. The targeted computer or network may not necessarily be owned and operated by the victim organisation, it may simply support or be used by the victim CIS.
Network defence	The set of all technical and non-technical measures allowing an organisation to defend its CIS against attack
Gateway	Technology (software and hardware) that transforms content, protocol or security information from one format to another to enable interoperability, at a boundary between networks with different security policies; cf. Guard
GSC	General Secretariat of the Council of the EU
Guard	Technology (software and hardware) used to control transfer of information at a boundary between networks of different security levels; cf. Gateway

IA	Information Assurance
IA OA	Information Assurance Operational Authority
IDS/IPS (IDPS)	Intrusion detection system / Intrusion prevention system software packages
ITIL	Information Technology Infrastructure Library - an approach to Information Technology Service Management - registered trade mark of the UK Government's Office of Government Commerce
NDM	Network defence Management is an organisational structure to implement network defence measures and ensure their correct implementation.
SAA/SAB	Security Accreditation Authority / Security Accreditation Board
SIEM	Security Incident (Information) and Event Manager (Monitor)
SPAM	in information technology: unwanted and/or malicious email or advertising; originally a brand name for canned processed meat (luncheon meat)
TCP/IP	transmission control protocol/internet protocol
TTP	Trusted Third Party: a reliable organisation which checksums and signs the contents of a collection of evidence or data.
VA	Vulnerability assessment
V-LAN	Virtual Local Area Network - a set of ports defined on a network switch with specific network access control rules set either on the device or via a “firewall”
Vulnerability	A weakness of a device or CIS which can be exploited by a threat to cause malfunction and/or damage to the target or to its user(s)

Weakness	A configuration or software error which can be exploited by a threat to cause malfunction and/or damage to the target or to its user(s)
WIFI	Trade mark of the WIFI alliance: class of wireless local area network (WLAN) devices based on the standard IEEE 802.11

REFERENCES

1. Information Assurance Security Policy on Interconnection of CIS IASP 3 (doc. 6467/15)

2. Information Assurance Security Guidelines on Data Separation IASG 5-07 (doc. 10821/14)

3. Information Assurance Security Guidelines on CIS Security Incident Handling IASG 4-03

4. Information Assurance Security Guidelines on Intrusion Detection and Prevention Systems in CIS IASG 4-02

EXAMPLES OF CRITERIA FOR RATING ATTACKS

1. Impact assessment of security threat[23] or attack:

Affected Community	Impact	Duration	Rating
All EU, its Member States and its partners	Unable to perform critical functions	>1 day	CRITICAL
All EU, its Member States and its partners	Unable to perform important functions	>1 day	IMPORTANT
Parts of the EU, its Member States or its partners	Unable to perform critical functions	>1 day	IMPORTANT
All EU, its Member States and its partners	Unable to perform critical functions	<1 day	IMPORTANT
Parts of the EU, its Member States or its partners	Unable to perform critical functions	<1 day	MEDIUM
Parts of the EU, its Member States or its partners	Unable to perform important functions	>1day	MEDIUM
A single department (unit), member state or partner	Unable to perform critical functions	>1 day	MEDIUM
All EU, its Member States and its partners	Some functionality is not available	>1day	LOW
Parts of the EU, its Member States or its partners	Unable to perform important functions	<1day	LOW

A single user, department (unit), member state or partner	Unable to perform important functions	>1 day	LOW
A single user, department (unit), member state or partner	Some functionality is not available	>1 day	LOW
All EU, its Member States and its partners	Some functionality is not available	<1 day	VERY LOW
Parts of the EU, its Member States or its partners	Some functionality is not available	<1 day	VERY LOW
A single user, department (unit), member state or partner	Some functionality is not available	<1 day	VERY LOW
etc.	etc.	etc.	etc.

2. Outside assistance may be needed when the threat or attack

a) is the action of terrorists;

b) is the action of a government;

c) can affect other EU organisations, Member States, agencies or partners

d) threatens critical EU or Member State infrastructure; or

e) threatens or damages the security and/or interests of the EU, its Member States or partners.