COUNCIL OF THE EUROPEAN UNION

Brussels, 6 June 2012

10578/12

CSCI 20
CSC 34

NOTE

From:	The General Secretariat
To:	Delegations
Subject:	Information Assurance Security Guidelines on Network Defence

1. The Council Decision on the security rules for protecting EU classified information[1] states that "The Security Committee may agree at its level security guidelines to supplement or support this Decision and any security policies approved by the Council." (cf. Article 6(2)).

2. The CSC approved the attached Information Assurance Security Guidelines on Network Defence on Friday 25 May 2012.

[1] Council Decision 2011/292/EU, OJ L 141 of 27.5.2011, p. 17.

This page intentionally left blank

IA Security Guidelines on Network Defence

IASG 4-01

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'), are designed to support implementation of the CSR and the Information Assurance Policy on Network Defence[2] (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.

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

4. When EU classified information is handled in national structures, including national CIS, the Member States will use these security guidelines as a benchmark.

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. 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.

7. 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.

[2] Doc. 8408/12

II. NETWORK DEFENCE

8. The Information Assurance Policy on Network Defence (IASP 4) defines Network Defence as a set of measures, processes, and activities to enable early detection of cyber threats to and vulnerabilities of CIS and to enhance their resilience to cyber attacks, so that attacks can be detected and rapid response can be implemented, to minimise the damage caused and to assess the actual impact of breaches of security.

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. Network Defence measures should include

    (a) security assurance measures of a preventive nature

    (b) security operation and maintenance measures; and

    (c) security restoration measures.

11. 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[3]) to keep up to date with new threats, new modes of attack and new protective methods.

12. 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.

13. 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[4].

---

[3] 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.

[4] 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

14. 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.

15. These guidelines are grouped into measures which provide:

(a) security assurance: those 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 (digital certificates, smart card..)
  - security measures for virtualised environments
- 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[5];
  - intrusion detection and prevention;
- awareness and training of users with standard or elevated privileges [6] in secure use of CIS, as well as in detecting and reporting unusual behaviour:- "the human firewall";

(b) security operation and maintenance: those 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;

---

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

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

– detection of unexpected system behaviour (security information and event monitoring); and
– review of rule sets.

(c) security restoration[7]
– 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

(d) management commitment.

III. SECURITY ASSURANCE

III.1. Design And Development

16. 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, or to enable isolation of the compromised sections in order to minimise and limit the impact. This is especially important if the functionality provided by the CIS is of critical importance in a crisis or emergency.
17. While checklists, included in risk management toolkits, of potential 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. Established and documented risk management methods must be used to reproducibly create such lists.
18. To build resilient CIS, single points of failure[8] in the system must in addition be actively identified and eliminated in the design phase.

---

7 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.

8 Such points of failure can be personnel, buildings, electronic devices, software packages, communication lines used by the CIS and its supporting infrastructure such as operators, alarm systems, access control systems, etc.

19. Should it not be feasible to completely remove the point of failure, mitigating measures must be included in the design to reduce the risk associated from such failure to an acceptable level.

20. In order for as much 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.

21. The methodology to be used to identify risks and mitigate them in the CIS design phase must be documented and agreed, subject to periodic revision, by the (security) management of the organisation.

22. Once risks affecting the resilience of a system have been identified, they must be handled by the risk analysis methodology chosen by the organisation.

23. In order to guarantee security of the CIS, it must be built using secure components.

24. 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.

25. The configuration of such components must be fixed using tested secure standard builds which 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 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.

26. The result of this initial configuration and testing exercise flows into the accreditation data set used by the SAA in accreditation of the CIS[9].

[9] Doc. 8420/12.

III.2. Provision of Technical Protection

27. Tools and methods are usually divided, for historical reasons, into device-oriented and boundary- oriented solutions.

Device-oriented tools

28. In order to ensure resilience against common security deficiencies, where technically feasible and justified after risk assessment, protection packages[10] must be deployed, updated, and configured correctly on all fixed and mobile[11] components of the CIS.

29. 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[12] as described below. The solutions must complement one another and be compatible with CIS monitoring systems.

Boundary-oriented tools

30. 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] as well as Information Assurance Guidelines on Data Separation [2] cover 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.

31. 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[13] as well as intrusion detection and prevention systems.

---

10 e.g. antivirus, full disk encryption.

11 Usb sticks, mobile phones, smart phones, tablet PCs, etc, which could be connected to fixed CIS components.

12 e.g. SIEM, GRC products.

13 See glossary Guard, Gateway.

32. 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

33. Intrusion detection systems (IDS) search for patterns of attack in network traffic and system log files respectively. Network Intrusion detection sensors (NIDS) and host intrusion detection sensors (HIDS) are sensors which reside both on network boundary devices and individual CIS components respectively. They feed the central monitoring and reaction system which produces alerts to which the IA Operational Authority (IA OA) and NDM must respond.

34. Intrusion prevention systems (IPS) use the same type of sensors as IDS and are additionally able to react immediately against the source of malfunction without human intervention, thus blocking or mitigating the severity of the disruption to service. This results in the IPS being considerably faster than IDS and thus more effective at blocking or mitigating attacks. As many routine events require routine responses, such solutions provide standard rule sets to kick start the IPS.

35. The IPS must be tuned and customised to the CIS as it is quite common for the built-in rule-set to block desired functionality while failing to detect anomalous behaviour which could be a security incident. The rule set of any such toolkit used must be therefore be checked and modified by the NDM personnel in an ongoing exercise.

36. The process for generating rules must be defined and the persons authorised to do this identified. It is also important that decisions as to what sensors to deploy, where and the reasons for doing this are documented for further reference. To ensure minimum disruption of service and maximum benefit from the use of IDS/IPS, sensors must initially be deployed only on a small number of CIS components which are

    (a) important or critical to the business of the organisation using them;

    (b) well known to the support teams; and

    (c) physically easily reachable.

37. During the learning phase, the configuration of the security management tool itself must be recorded frequently so that its performance can be linked to specific configurations.

38. As experience is gained in the use of the IPS, the number of monitored items as well as the number of rules invoked must be adapted and increased for maximum effectiveness and efficiency.

III.3. Awareness Training of Users

39. 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[14] staffed 24x7, with the persons handling the calls able to call in experts if preliminary investigation does not exclude a security incident.

40. 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[6], 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.

41. 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;

    (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.

---

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

IV. SECURITY OPERATION AND MAINTENANCE

IV.1. Configuration and Change Management

Configuration Management

42. Configuration management is essential to good systems management and is thus also required for Network Defence. It involves both version control of deployed products as well as control of the settings of the products deployed.

43. Automated toolkits[15] 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.

44. 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.

45. 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.

Management of requests for change and exceptions

46. 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 changes 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. . While 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

[15] e.g. ITIL™ toolkits

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 the last three 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.

47. 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

48. Network Defence must include a process for obtaining and evaluating security alerts from:

a) "feeds" about newly discovered or zeroday[16] 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[17] which report ongoing malfunction or attack:

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

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.

49. 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.

50. Trained personnel who know the functional purpose and technical details of the CIS must evaluate, score and disseminate alert information with trusted partners such as IA operational authorities, other Network Defence experts, CERT members, etc.

51. 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.

52. 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.

53. 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 46.

IV.3. Ongoing Event Logging, Monitoring and Consolidation

54. 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.

---

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

55. 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. Such a collection also simplifies incident investigation and response.

56. 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.

57. All events of potential security relevance, whether related to hardware, software or system performance, are therefore best exported to a read-only dedicated device such as a "log server" or consolidator, preferably without filtering but with conversion of the different log file entries to a common record format. Access to the log server 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.

58. For monitoring large numbers of near-simultaneous events, consideration should be given to the use of visualisation techniques interpreted by trained personnel.

IV.4. Network Discovery, Mapping And Monitoring

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

Vulnerability assessment

60. Here this term refers to the technical, usually tool-assisted, testing of a CIS[19] performed prior to release to its 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.

---

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

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

61. 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[20] and additional manual testing for false negatives

62. 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[21] responsible for checking and fixing the reported weaknesses;

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

    (f) generation of work tickets for fixing;

    (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.

63. The design of the scan process must be performed on dedicated testing environments 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.

64. 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.

65. As outlined above, after checking the output for false positives, work tickets must be generated by the platform experts to support teams to remove or mitigate the vulnerabilities discovered and treat the resulting risks.

---

[20] A false positive is an alert about a problem or vulnerability which turns out to be untrue when checked manually, a false negative is a failure to detect an existing weakness or vulnerability.

[21] Security experts in network device and server operating systems and specific layered products.

Full security evaluation

66. A black-box, and/or white-box approach to VA-scanning supplemented with manual checking 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".

67. 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.

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

Infrastructure[22] vulnerability analysis

69. Prior to any scanning, the tool must be updated with the most current lists of vulnerabilities.

70. 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.

Application vulnerability analysis

71. 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.

72. 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.

---

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

Other aspects

73. 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

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

75. 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 76 is considered necessary.

IV.5. Generation of Security Alerts and Warnings

76. A central IT tool for consolidating, correlating, analysing and reporting the collected security events able to facilitate efficient and timely reaction to security incidents and preferably[23] should be used.

77. 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.

[23] The need for such a tool depends on the risk assessment for the CIS as well as on other considerations, e.g. when the tool is used for several CIS.

78. 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.

79. 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 outlined later in paragraph 91.

IV.6. Implementation considerations

80. 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?

81. Rules must be modified or created to reflect the above, their justification documented and the configuration stored off-line at a secure location as a historical record over time.

82. 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.

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

    (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.

84. 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.

IV.7. Rule set Review

85. In order to maintain the security of a CIS, revision and 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. Such rule sets are for example:

- "Role" or "profile" templates used by the CMDB,
- access control lists (ACLs),
- routing tables,
- firewall rules,
- IDS/IPS configuration,
- SIEM configuration,
- (incoming) content filtering rules, egress filtering rules, etc.

V. SECURITY RESTORATION

V.1. Incident investigation and digital forensics

86. 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.

87. Having set up a CIS to monitor, record and report unexpected behaviour, it will generate alerts about potential breaches of security. As it must be assumed that all incidents may be security-related, the integrity and authenticity of the data collected must be preserved and an unbroken "chain of custody" guaranteed in case action needs to be taken against identified perpetrators.

88. Alerts about malfunction or incidents must first be analysed to determine whether they are indeed security incidents or not. If a security incident cannot be excluded, investigators trained in digital forensics must be called in.

89. The generic security incident investigation process must:

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

    (b) determine the course of and cause of malfunction (the source of attack);

    (c) trigger incident response processes; and

    (d) inform affected parties.

90. The data recorded by CIS components and security monitoring tools will provide the bulk of information used in investigation a security incident. 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:

    (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?

91. In order for the information to be usable for potential subsequent action against perpetrators of the incident, especially when cross-border events are involved, investigators must be aware of the regulatory and legal restrictions valid in the jurisdiction responsible[24]

92. Because of the very powerful nature of security testing and incident investigation tools and owing to legal restrictions on their use, specific mandates must be given to the handlers who use such tools and techniques. This is required both to ensure that only authorised personnel can use such tools, as well as to protect the handlers from criminal prosecution and disciplinary action.

93. In the context of CIS handling EUCI, all personnel involved in investigation must be in possession of suitable 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, the incident information is to be classified at least as RESTREINT UE/EU RESTRICTED, but may be classified at the level of CIS.

V.2. Incident Response and Corrective Action

94. Once security events have been reported and confirmed, documented and agreed processes must be initiated. Corrective actions must be formalised and implemented in a manner commensurate to the risk posed by the alert or reported security event.

95. As far as possible, repetitive events should provoke standard reactions, to relieve experts of the task of reacting to and analysing routine events and situations. Standard response processes must be documented and always available, either in the form of hardcopy or softcopy stored in dedicated CIS-independent devices[25]. Scripts or executables of this type run with the required rights and privileges but do not require the first responders[26] invoking them to have high[6] rights or privileges on the CIS.

96. The use of such automated response procedures or programs must be restricted to authorised users, and their use must be audited and logged. 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 preserve evidence.

---

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

[25] They may also be stored on-line but must also be off-line.

[26] Helpdesk, network and operations control centres, etc.

97. Following any incident, the IA operational authority and the NDM must review the Network Defence measures and propose changes to prevent the incident from reoccurring. Changes made to an accredited CIS must also be reviewed by the SAA to determine whether the system requires re-evaluation.

V.3. Business Continuity and Disaster Recovery Planning

98. 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. BCP is part of the risk management process and involves identifying threats that can impact an organisation's operations adversely and providing technical or conventional workarounds to maintain a (potentially reduced) level of services considered important by the CIS business owner during incidents and failures. The business owner of the CIS must thus contribute in the BCP process.

99. 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.

100. BCP and DR plans should be tested at least yearly in order to gain experience in using them.

101. International standards[27] for developing and using such plans must be referred to. The CIS Business owner – for accredited CIS together with the SAA – must approve business continuity and disaster recovery plans.

V.4. Information sharing and escalation mechanisms

102. Network Defence must provide for secure methods of sharing information about potential and actual security weaknesses, attacks, etc. with trusted partners in order to:

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

---

[27] 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.

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

103. 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 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.

104. 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.

105. 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[28] 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.

106. 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.

[28] Such persons must not only possess suitable personnel security clearance 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.

VI. MANAGEMENT REVIEW

107. Network Defence activity requires significant effort to set up from scratch. The 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.

108. 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.

109. 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.

110. 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?

111. 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
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
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	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)
SSO	Single Sign-on

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 (WI-FI)	Trade mark of the WIFI alliance: class of wireless local area network (WLAN) devices based on the standard IEEE 802.11

For more terminology, please see IA Glossary [3]

REFERENCES

1 INFOSEC Policy on Interconnection of CIS (TECH-P-05)

2 Information Assurance Guidelines on Data Separation (to be published)

3 Information Assurance Glossary (to be published)