sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVIII No 1 2022

METHODOLOGY FOR DEVELOPING RESILIENT INFORMATION SYSTEMS IN CYBER CONFLICT ENVIRONMENT

Veselina ALEKSANDROVA GAGAMOVA*, Anna GUNCHEVA*, Violeta VASILEVA**

***"G.S. Rakovski" National Defence College, Sofia, Bulgaria**
****Artshare, Estarreja, Portugal**
v.gagamova@rndc.bg, guncheva67@gmail.com, violeta.vasileva@artshare.pt

Abstract: *Successful cyber defence in the challenging cyber conflict environment depends on many factors but a crucial one is the use of a resilient system for cyber defence which is highly interoperable with those of partner countries and organisations. This paper presents a methodology of developing information systems capabilities resilient and interoperable in cyber conflict environment. The applied approach for defining the system design of information infrastructure is based on NATO models. For the architectural configuration, the NATO Technical Reference Model is applied and the NATO Common Operating Environment Component Model (NCOECM) is used for defining the information infrastructure components of the system design. NATO Technical Reference Model defines system services necessary for the information infrastructure of organizations. Functionalities needed by users and based on system services are also identified using reference models like workstations, servers, terminals and others, which are connected in an integrated information infrastructure. By implementing the proposed methodology a model of architectural configuring of an information infrastructure component has been developed – the Security Information and Event Management (SIEM) Server functional configuration.*

Keywords: Cyber Conflict Environment, methodology, NATO models

1. Introduction

Various models and architectural configurations could be used to define information infrastructure of Information Systems of the organizations in Cyber Conflict Environment. For the architectural configuration NATO Technical Reference Model (NTRM) is applied and for the system design defining of Information infrastructure components the NATO Common Operating Environment Component Model (NCOECM) is used. NATO Technical Reference Model (NTRM) is related to the necessity of materializing twelve system services. Eight functional configurations possess such capabilities, for example, terminals, active network devices, workstations and servers, which are practically the main elements of information infrastructure of a Security Operation Centre (SOC). The components model defines the services content. These configurations must have available functional capabilities at different levels: networking, infrastructural and others belonging to basic services and applications.

As a whole, the methodology for developing resilient information systems in cyber conflict environment includes building the architecture of informational

DOI: 10.2478/kbo-2022-0024
© 2015. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

infrastructure of cybersecurity systems such that are used in SOC, Security Emergency Response Team (SERT) or Security Incident Response Team (SIRT). Resilient information systems have the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents [7]. They also have to be able to continue to operate while under attack, and to rapidly recover operational capabilities for essential functions after disruptions [8]. Such systems should be developed in the information infrastructure of the SOC in order to ensure successful functioning and protection in cyber conflict environment.

Informational infrastructure comprises a unity of its components, the relations among them, the principles and rules that govern their design and development. Security Information and Event Management (SIEM) server as a component of cybersecurity informational systems should be architecturally configured by implementing the proposed methodology. For that purpose a model of an information infrastructure component (SIEM server) could be developed with a specification of its technical and software configuration by using of the two main NATO references models NATO Technical Reference Model (NTRM) and NATO Common Operating Environment (NCOE) Component Model (NCM) [1].

The architectural description includes all the products defining the architecture. Architectural development requires modelling which helps us understand the connection between the requirements, on the one hand, and the architectural concept, on the other hand. The requirements must be presented in a chart format according to NATO C3 Technical Architecture Implementation Handbook (NC3TA-IHB) [2]. Although the NC3TA-IHB is primarily developed for the implementation and maintenance of NATO C3 Systems, it should also provide equal benefit to national project and procurement staff and their contractors, in order to promote the widest possible opportunities for interoperability. The NC3TA-IHB identifies in Annex A the templates that need to be filled out by project managers and architects but does not provide a methodology how to do this. It is up to the project managers and architects to choose appropriate methodologies that fit their needs. There is a need for a methodology to fill out the NC3TA templates from Annex A. A proposal for such methodology is presented by the authors. As an example of the application of such a methodology, the report presents the development of the functional configuration of SIEM server.

2. Description and Concept Models for Architectural Configuration of the Organization of the Components of the Information Infrastructure of Systems in Cyber Conflict Environment

For achieving resilience of Information Systems in Cyber Conflict Environment it is necessary the development of cybersecurity systems for organizations to be in such a way that they are interoperable. Therefore, the application of NATO models would assist the development of organizations' cybersecurity systems.

2.1. Models for Describing the Components of the Information Infrastructure of Cybersecurity Systems

For the description of the components of the information infrastructure of the organizations the NATO Technical Reference Model (NTRM), the NATO Common Operating Environment (NCOE) Component Model (NCM), service taxonomy model and others are used [1].

In order to achieve interoperability between management and governance systems in the Cyber Conflict Environment, reliance is placed on the implementation of a set of measures, including policy, directives, guidance and supporting documents. One of the main models of system compatibility is

the NATO Technical Reference Model (NTRM). It is a model for describing the information environment, defining applications data and information infrastructure components data. It also defines the service areas (capabilities that are grouped by function) as well as their interfaces. The structure of the Technical Reference Model considers the separation of data from applications as well as applications from software configuration. The model is designed to separate applications and the external environment from the platform. This allows for application compatibility and independence from external devices (for example, disks, networks, etc.). For this purpose, the model defines the Application Program Interfaces and the External Environment Interfaces.

In general, the NATO Technical Reference Model (NTRM) is the basis for defining the Component Model of the Common Operational Environment (NCOE).

The NATO Common Operational Environment (NCOE) Component Model (NCOECM) visualizes with concrete examples the functionalities of the information environment components defined by the NTRM. The main elements of the NCOE component model (see Figure 1) are the services divided by levels:

- Network Services - provide the connection between the platform and the physical environment of the network infrastructure;
- Kernel Services - include operating system, windowing software, security services, management services and some more;
- Infrastructure Services - directly support the information flow between systems;
- Common Support Application Services – they share data processing and networking services. They also provide interoperability between different applications for different organizations;
- Application Programming Interfaces - can be launched from applications or services if needed;
- Support Services - include training, management, storage and security services.

These components, defined as groups of services, are the basis for configuring the building blocks of each information infrastructure platform, listed in the next part of the paper. This is achieved by applying the methodology of architecture configuration.

2.2. Methodology of Architecture Configuration of the organization of the Components of the Cybersecurity Systems Information Infrastructure

The methodology for architectural configuration of the organization of the components of the information infrastructure includes two steps:

- development of a functional configuration of the whole system, consisting of functional configurations or components and related functional interfaces.
- architectural configuration of components of the information infrastructure, by developing the respective Functional, Technical and Software Configuration (FC, TC, SC) for each component, in this way filling out the NC3TA Compliance Templates from Annex A of the NTRM model.

First of all, the development of the architecture is related to defining the requirements for the realization of the necessary capabilities of the system, or functions that the system performs, through the appropriate “Functional configuration”. The single FC consists of a logical arrangement of functional components, which together constitute the information infrastructure and provide a single set of services to users, such as functionalities.

The second step of the methodology for building the resilient information infrastructure is to define the organization

of the components of the information infrastructure of the system.
The development of the architecture is related to the definition of the requirements for the realization of the necessary capabilities of the system, or functions that the system performs, through the appropriate "Functional Configuration". The definition of functions related to the implementation of system design of system components is done by developing "Technical Configuration" and "Software Configuration".
There are connections and relationships between the three architectural configurations. Functional configurations are made up of applications, basic services and functional interfaces between them. Technical configurations are a collection of components and standards that interact with other technical configurations through Interoperability Profiles, and software configurations are a physical collection of software products and segments that provide software interfaces with other software configurations.
All configurations are a type of model for a component of the organization's infrastructure and as such these three configurations represent a common template for architectural configuration. It can be used to develop any element of the information infrastructure. Therefore, for each component of the organization of the information infrastructure of the cybersecurity system, architectural configuration is performed developing respectively: The Functional Configuration representing a particular functionality, the Technical Configuration representing the technical solution and the Software Configuration containing the relevant product solutions.
Functional configurations present as functions the capabilities in terms of system functionality. They are shown with a graphical representation of functional blocks that should be built to meet the requirements of the capabilities of the information system. For example, a component may appear in several functional configurations (e.g. operational system, general purpose components, security components, management, monitoring, etc.). Functional configurations represent the necessary services, such as functional interfaces, and they must be presented as interoperability profiles containing standards that implement these functional services. Examples of functional configurations can be personal workstations, a server or a server system and others, i.e. they are the devices in the infrastructure. The interfaces between them are represented by arrows in the graphical representation of the functional configuration.
Technical configurations represent a technical transformation of functional configurations.
The software configuration represents the software products needed to implement the technical configuration. The components and standards included in the technical configurations are presented as products of the software configurations.

3. Defining the Organization of the Components of the Information Infrastructure of the Cybersecurity System

For the effective functioning of the Computer Security Incident Response Team (CSIRT) [3], it is necessary to provide the following components of the information infrastructure of the cybersecurity system in organizations:

- technological equipment with the relevant sensors for monitoring the communication and information infrastructure;
- intrusion detection and prevention systems - IDS / IPS / IDPS [6];
- systems for processing and analysis of computer incidents - Security Information and Event Management (SIEM) to support

the actions of the team in reading a large number of registered events from cyber defence sensors [4], [5];

• video surveillance systems, Next Generation Firewalls;

• trained and highly qualified personnel in the field of cyber defence;

• software for cyber forensics;

• a web server with cyber awareness information service.

The various components (platforms) of the information infrastructure of the cybersecurity system are considered as functional configurations. According to the methodology of architectural configuration of the components of the information infrastructure, for each of the components the following configurations have to be developed, which represent a different aspect - functional, technical and software. For each of the three configurations a graphic and tabular design need to be developed according to the templates [2, pp.49 – 67, Annex A] of the NTRM Concept.

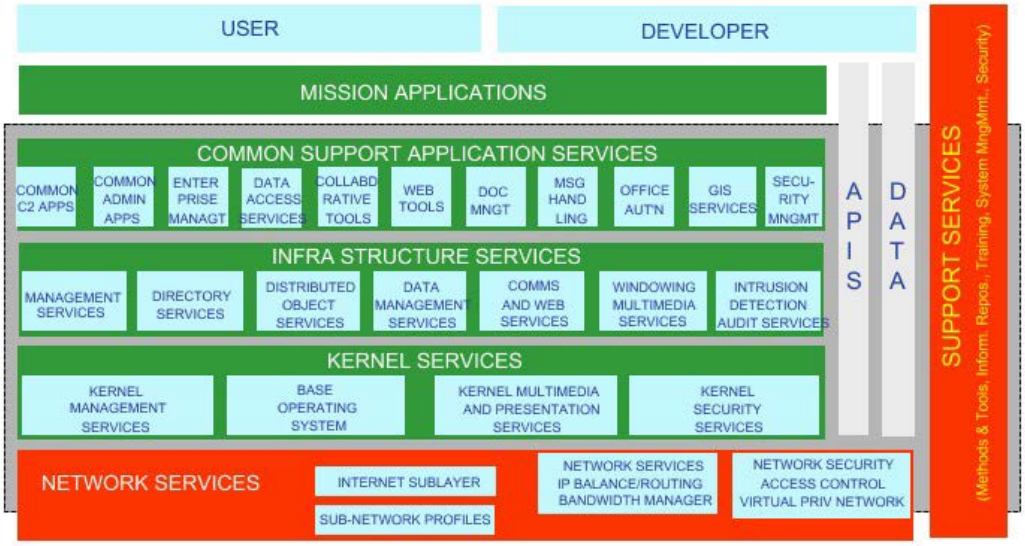


Figure 1: The NCOE Component Model Structure
Source: [1, p.18, Sec. 3.3, Figure 3.2.]

4. Implementation of the Methodology for Architectural Configuration of a Server for Processing and Analysis of Computer Incidents - Security Information Event Management Server

Functional configuration of the Security Information Event Management (SIEM) server is shown in graphical form, Figure 2 Functional configuration is built through the five layers of services: application services; common support application services; infrastructure services; kernel services; network services.

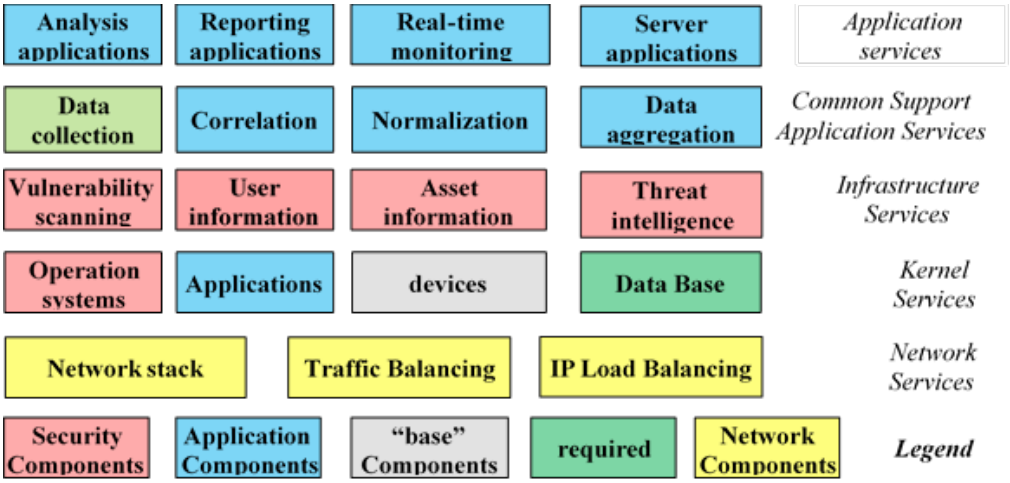


Figure 2: Graphic Representation of SIEM functional configuration according to NCOECM

At the level of functional configuration, the SIEM architecture has been developed. It will be presented in more detail with the technical and software configuration.

A technical configuration is a transition from a technical view to software configurations that define specific segments and their component and software products. The software configuration presents the software for executing the technical configuration.

5. Conclusions

To develop the architecture of an organization's computer incident response center, a proposal is offered to use NATO models to architecturally configure the components of the information infrastructure of cybersecurity systems.

In order to develop the capability for providing information services in building a Resilient Information Systems in Cyber Conflict Environment, the minimum configuration of the cybersecurity system of the organizations involved in the process must include automated workstations for users, administrators and a system of servers to provide the system services.

It can be concluded that the authors have presented Methodology for Developing Resilient Information Systems that includes architecture configuration and system design of its components in a specific way - by using NATO models. Various tools have been used, such as figures and textual explanation. This presentation of the information infrastructure is not very popular among developers' teams, especially in the field of Resilient Information Systems design. We hope that the topic would be interesting because the defining of the information infrastructure and its software configuration could successfully be used to improve the design of such systems in order to meet the challenges of Cyber Conflict Environment.

References List

[1] Allied Data Publication 34 (ADatP-34) NATO C3 Technical Architecture, Volume 2 Architectural Descriptions and Models, Version 6.0, ISSC NATO Open Systems Working Group, NC3TA-Vol2- v6.xml.

[2] NATO C3 Technical Architecture Implementation Handbook (NC3TA-IHB), Version1, ISSC NATO Open Systems Working Group, AC/322(Sc/5) N268, 2002.

[3] How To Setup Up CSIRT and SOC Good Practice Guide, European Union Agency for Cybersecurity (ENISA), 2020, ISBN 978-92-9204-410-7 - DOI 10.2824/056764. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc (accessed on Jan. 8, 2022).
[4] What Is SIEM?. Splunk.com. Available from: https://www.splunk.com/en_us/data-insider/what-is-siem.html#overview (accessed on Jan. 8, 2022).
[5] What is SIEM? SIEM Defined, Explained, and Explored". Forcepoint.com. Available from: https://www.forcepoint.com/cyber-edu/siem (accessed on Jan. 8, 2022).
[6] Jeff Petters, IDS vs. IPS: What is the Difference?, Inside Out Security Blog / Data Security, March 29, 2020, Varonis.com. Available from: https://www.varonis.com/blog/ids-vs-ips (accessed on Jan. 8, 2022).
[7] NISTIR 8323 under Resilience from PPD 21 Available from: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil), National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Resource Center, Glossary, under Information System Resilience, Available from: https://csrc.nist.gov/glossary/term/information_system_resilience (accessed on May 30, 2022).
[8] NIST SP 800-30 Rev. 1 under Information System Resilience, National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Resource Center, Glossary, under Information System Resilience, Available from: https://csrc.nist.gov/glossary/term/information_system_resilience (accessed on May 30, 2022).