Adapted SANS Cybersecurity Policies for NIST Cybersecurity Framework

Vladimir Dimitrov [0000-0002-7441-253X], Kalinka Kaloyanova [0000-0003-0222-7607], Milen Petrov [0000-0001-7701-8362]

Faculty of Mathematics and Informatics, Sofia University St. Kliment Ohridski
5 James Bourchier blvd., 1164, Sofia, Bulgaria

{cht, kkaloyanova, milenp}@fmi.uni-sofia.bg

Abstract. Cybersecurity Framework has been developed by NIST as a framework for improving cybersecurity in critical infrastructures, but soon it has been found out that it is applicable for any organizational type.
The Framework Core defines a set of five activities (functions) for cybersecurity achievements. The functions are subdivided into categories and the last ones in subcategories. Finally, informative references are supplied as examples of applicable standards and specifications.
The framework can be used to plan cybersecurity activities in the organization: Current Profile of the organization has to be developed and then Target Profile as a plan to achieve a particular cybersecurity level.
The problem with the NIST Cybersecurity Framework adoption in non-English speaking countries like Bulgaria is the informative references. They are in English and are appropriate for staff with technical background. On the other hand, plans (Target Profile) have to be approved by the senior management – it must be in Bulgarian. Therefore.
Another problem with NIST Cybersecurity Framework adoption is that only a few standards and specifications can be used as informative references in Bulgaria. These are mainly international standards, specifications, and EU directives.
SANS offers a set of template policies organized around the NIST Cybersecurity Framework. These policies refer to a minimal set of informative references. In such a way, the policies can be translated into Bulgarian for the senior management and the informative references can remain in English for the technical staff.

Keywords: Cybersecurity, Cybersecurity Framework.

1 Introduction

The growing number of cybersecurity incidents affects different parts of today's life. It is a necessity for the government and industry to address all cybersecurity aspects both at the national and international level. Although many institutions work in that area, a particular implementation of a framework that meets all cybersecurity challenges at a national level is a complex task for many countries.

Most of the recommendation/guidelines in cybersecurity were announced by US institutions – the National Institute of Standards and Technology (NIST), U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Escal Institute of Advanced Technologies (SANS Institute), the National Centers for Academic Excellence in Cyber Defense (CAE-CD).

The EU center, which provides expertise in the cybersecurity domain, is the European Union Agency for Cybersecurity (ENISA) [6]. This institution presents information in the languages of the EU countries, including Bulgarian [7].

In Bulgaria, the Cybersecurity Act (2018) was announced to meet the requirements of the European Parliament Directive 2016/1148 [3].

This paper discusses main principles of the most used framework in cybersecurity – the NIST Cybersecurity Framework and the SANS policies, associated with the framework's subcategories, and their adaption in Bulgaria.

2 NIST Framework for improving critical infrastructure cybersecurity

In 2013, NIST started an initiative to design a cybersecurity framework for critical infrastructures, following the next design criteria [1,8]:

- "Identify security standards and guidelines applicable across sectors of critical infrastructure
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach
- Help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Enable technical innovation and account for organizational differences
- Provide guidance that is technology-neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services
- Include guidance for measuring the performance of implementing the Cybersecurity Framework
- Identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations"

NIST has been selected to do this job because it is a non-regulatory federal agency promoting innovation and industrial competitiveness in the USA. The agency has long collaboration history and strong connections with industry and academia. The framework nevertheless has been developed in collaboration with all stakeholders.

In 2014, NIST published Framework Version 1.0. The leading idea was the framework to be useful for strengthening cybersecurity in critical infrastructures,

but it has appeared to be designed in enough industry-independent manner to be applicable in any other area. Something more, it is applicable for organizations of any type and size.

In 2018, NIST released Framework Version 1.1. This version is currently the last one. This version is translated into Bulgarian and a reference to it is available at the NIST site [14].

The Framework Core consists of Functions, Categories, Subcategories, and Informative References [9].

The Framework Core defines a set of five activities (functions) for cybersecurity achievements: Identify, Protect, Detect, Respond, and Recover – see Fig.1. The role of the Functions is to organize the main cybersecurity activities. Further, the Functions are subdivided into Categories, which can be detailed into Subcategories. Finally, Informative references are supplied as examples of applicable standards and specifications.

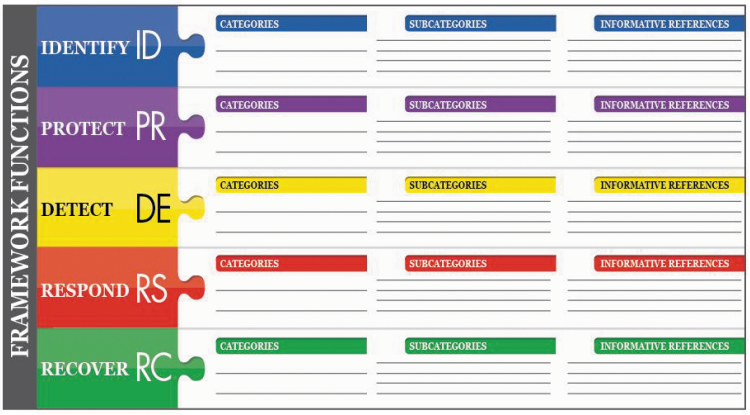

Fig. 1. NIST Framework Core Structure [9].

The framework can be used to plan cybersecurity activities in the organization. First, the Current Profile of the organization has to be developed. It is based on the current state of the art in the organization in terms of Framework Core. Then Target Profile has to be developed as a plan to achieve a particular cybersecurity level.

A problem with the NIST Cybersecurity Framework adoption concerns the informative references. They are written in English and have to be specific to the problem area.

On the other hand, the plans have to be approved by the senior management. The Target profile is a goal to be achieved – this is a strategic plan (policy). Therefore, the Target Profile has to be defined as a set of policies in the official country language.

Another challenge with NIST Cybersecurity Framework adoption is the small number of cybersecurity national standards and specifications that can be used as informative references in countries like Bulgaria. Usually, standards, regulations, and specifications are international, provided by EU and USA institutions.

3 SANS policies structured by NIST Cybersecurity Framework and security policy adaptation model

SANS offers a set of templates for policies organized around the NIST Cybersecurity Framework [10]. The SANS policies refer to a minimal set of informative references.

There are 27 SANS policy templates organized around NIST Cybersecurity Framework Functions, Categories, and Subcategories. A part of them are not classified in the framework – they are applicable in general, the others falls into several groups – networking, server, and application security, as listed below [13]:

Application Security

- Web Application Security Policy

General Security

- Acceptable Encryption Policy
- Acceptable Use Policy
- Clean Desk Policy
- Data Breach Response Policy
- Digital Signature Acceptance Policy
- Disaster Recovery Plan Policy
- Email Policy
- Ethics Policy
- Pandemic Response Planning Policy
- Password Construction Guidelines
- Password Protection Policy
- Security Response Plan Policy

Server Security

- Database Credentials Coding Policy
- Information Logging Standard
- Lab Security Policy
- Server Security Policy
- Software Installation Policy
- Technology Equipment Disposal Policy
- Workstation Security:For Health Insurance Portability and Accountability Act (HIPAA) Policy

Network Security

- Acquisition Assessment Policy

- Bluetooth Baseline Requirements Policy
- Remote Access Policy
- Remote Access Tools Policy
- Router and Switch Security Policy
- Wireless Communication Policy
- Wireless Communication Standard

Translation of these documents in Bulgarian will facilitate the adoption of the policies. It also helps to separate the use of the documents at different levels: the documents in Bulgarian – for the senior management, the original ones – with informative references in English – for the technical staff.

The SANS practice templates follow a predefined structure – Overview, Purpose, Scope, policy, Policy Compliance, Related Standards, Policies and Processes [13]. The Definitions and Terms section completes the list of sections.

Every institution could adopt these practices in a way that reflects its specific needs. Adaptation begins with the presentation of the overall goal of the institution or policy. The overall goal can be detailed into smaller sub-goals (tasks) that are associated with practices and resources.

Based on the experience, earned by working with NIST Cybersecurity Framework and SANS policies, has been created an initial version of *Security Policy Adaptation Model,* depicted in Fig. 2 below. Currently, the focus is mainly on security policies, practices, domains, resources, and security state profiles.

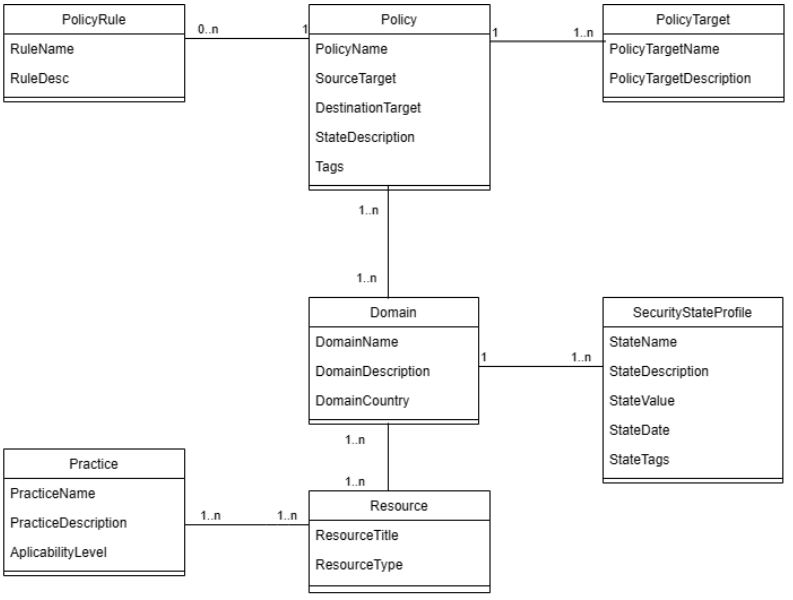

Fig. 2. Security Policy Adaptation Model.

The resources and practices identified according to the goals are closely related to the *Domain*. There could be different domains, which are included in specified model implementation, like universities, schools, research organizations, business companies, etc. The main properties, identified here represent the domain name, general description of the domain, the domain country (or region), and the language of policy – for policies, that need to conform to the national requirements.

To define different profiles for the same domain *SecurityStateProfile* is used. Profiles can be differentiated by language, or by other parameters. The most important property here is the State attribute, which is used for comparisons between the models. In the beginning, the possible values for this attribute are 'Source' and 'Destination'.

The Destination Profile (or also Target Profile) is a profile that has to be achieved in the future. Thus, it can be an advice and or recommendation, according to goals, what policies, practices, and resources need to be applied to achieve it.

Next, *Policy* describes the source and destination targets. In a separate entity, called *PolicyRules* are stored different policy rules options, available on different targets. Policies in *Policy* are related to earlier mentioned *SecurityStateProfile* via *Domain*. This will allow consumers of the model to compare different policies on different states – Source State, and Target (or desired) State. PolicyTargets Entity – which contains what are subjects to policy– generally those are assets or resources of the organization.

In *Practice* entity, in addition to the common name and description characteristics, an attribute that defined the level of applicability is added. It presents if the usage is too limited to the domain defined, or it can be widely adopted and used.

The identified resources that are represented with *Resources* entity, initially are defined with core attributes like title and bibliography information.

The presented model is only overviewed here. It could be not only detailed but also extended in different directions.

For example, Domains can be divided into smaller pieces, according to the needs of the stakeholder of the system, that implements the security policy model. Also, Risk assessments could be added using performance measures and performance indicators.

The model has to be further verified with real practices, resources, domains, and profiles. As cross entity aspect here is also NIST Framework, represented in *BestReferencePractices* entity, which defines attributes like, security state, reference models, functions, categories, and sub-categories.

4 Addressing cybersecurity in EU and Bulgarian documents

The EU Network and Information Security Agency – ENISA, was founded in 2004. Since then it provides expertise for EU member states, EU citizens, and the private sector. ENISA enables the development of recommendations and good practices in cybersecurity and supports the establishment of EU communities to address the challenges in this area.

ENISA defines cybersecurity as "the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment". The EU countries, on the other side, may use other definitions to clarify the meaning of cybersecurity, as well as to develop their own strategies for cybersecurity.

The National Cyber Security Strategy "Cyber Resilient Bulgaria 2020" provides "a modern framework and a stable environment for the development of the national cybersecurity system" [2]. It was announced in 2016. The strategy separates three phases "Initiating and Achieving basic cybersecurity capacity" (2016-2017), "Development – from Capacity to Capability" (2018-2019), and "Mature and Cyber Resilient Society"(2020). The strategic goals, implemented in the strategy, concerns cybercrime, security with privacy balance, citizen awareness, international cooperation, incident response capability, incident reporting mechanisms, research and development, training and educational programs. The role and the responsibilities of different institutions are noticed. A small vocabulary of basic items in cybersecurity completes the document.

In November 2018, a new Cybersecurity Act was promulgated in State Gazette in Bulgaria. It addresses European Parliament Directive 2016/1148 requirements for a high level of security for networks and information systems across the European Union. The Cybersecurity Act also outlines the authorities on the strategic and operational level, as well as their responsibilities [3].

Basic issues concerning vulnerability analysis and threat prevention in Bulgarian cyberspace are discussed in [11, 12 and 16], and a maturity-based approach for the Bulgarian cyber resilience roadmap is introduced in [17].

To answer to the impact of the COVID-19 pandemic and the growing potential of cybersecurity perpetrators, as well to the increase in the number of received signals for computer crimes and cyber incidents, in March 2021, the new, revised National Strategy for Cyber Security "Cyber Resilient Bulgaria 2023" was adopted to replace the "Cyber Resilient Bulgaria 2020" [15].

5 Staff training and education

During the last several years, many of the leading universities launched programs to prepare students for future careers in the field of cybersecurity. Most of

the programs are for graduate students. CSEC2017 – Cybersecurity Curricular Guideline presents major curricula guidelines, which are the summary of the effort of these curricula present ACM, IEEE Computer Society, AIS SIGSEC, and IFIP WG 11[5].

The need for a large number of cybersecurity professionals forces other institutions apart from the universities also to work for cybersecurity training and certification. The Cybersecurity: A Generic Reference Curriculum, provided by NATO and PfP Consortium gives a broader view on cybersecurity [4]. Several other publications include the NICE Cybersecurity Workforce Framework, presented by the U.S. National Initiative on Cybersecurity Education (NICE), the Designation Program Guidance of the National Centers of Academic Excellence in Cyber Defense (CAE-CD), and the Designation Program Guidance IISP Knowledge Framework. The recommendations and the guidelines provided by these institutions present an extended vision of cybersecurity issues for non-technical experts and students, citizens, etc. However, they also leave room for more in-depth study by technical experts.

Considering the technical expertise of the last group, there is no need for all references to be translated. The technical staff should use the original references also because they will change rapidly following the changes in the technologies.

6 Conclusion

In this paper, some of the problems to adapting NIST Cybersecurity Framework via SANS Policy Templates as Target Profile are discussed. An approach for the adaptation of these frameworks is presented and a model for Security Policy Adaptation is introduced. These are initial results obtained in the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security". The research on the topic continues with the detailization of the model and providing resources. Possible areas of adaptation of the framework are universities, schools, local and governmental administration.

7 Acknowledgments

This research is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)" in Bulgaria.

References

1. Bulgarian Cybersecurity Association, https://bacs-bg.com/, last accessed 2021/04/02
2. Cyber Resilient Bulgaria 2020, http://www.cyberbg.eu/, last accessed 2021/04/17.

3. Cybersecurity Act (Bulgaria), https://www.mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf, last accessed 2021/04/02.
4. Cybersecurity. A Generic Reference Curriculum. https://pfp-consortium.org/index.php/pfpc-products/education-curricula/item/262-cybersecurity-reference-curriculum, last accessed 2021/04/08.
5. CSEC2017, Cybersecurity Curricula 2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Version 1.0, https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf, last accessed 2021/04/11.
6. European Union Agency for Cybersecurity (ENISA), (https://www.enisa.europa.eu/, last accessed 2021/04/02.
7. European Union Agency for Cybersecurity (ENISA)-BG, https://europa.eu/european-union/about-eu/agencies/enisa_bg, last accessed 2021/04/02.
8. NIST: History and Creation of the Framework. https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework, last accessed 2021/04/16.
9. NIST: Cybersecurity Framework, https://www.nist.gov/cyberframework, last accessed 2021/04/16.
10. Center for Internet Security, Multi-State Information Sharing & Analysis Center: NIST Cybersecurity Framework, SANS Policy Templates, https://www.cisecurity.org/wp-content/uploads/2019/08/NCSR-SANS-Policy-Templates.pdf, last accessed 2021/04/16.
11. Shalamanov V., Penchev G.: Academic Support to Cyber Resilience: National and Regional Approach, Computer and Communications Engineering. 13, No. 2: pp. 73-80 (2019).
12. Sharkov G., Papazov, Todorova K., Koykov G., Georgiev M., Zahariev G.: Cyber Threat Map for National and Sectoral Analysis, Computer and Communications Engineering. 13, No. 2: pp. 29-32 (2019).
13. SANS Security Policy Templates, https://www.sa.ns.org/information-security-policy/, last accessed 2021/04/12.
14. International Resources. Bulgarian Translation of the NIST Cybersecurity Framework V1.1, https://www.nist.gov/cyberframework/international-resources, last accessed 2021/04/16.
15. Cyber Resilient Bulgaria 2020, https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=5878, last accessed 2021/04/24.
16. Trifonov R., Nakov O., Manolov S., Tsochev G., Pavlova G.:New Approaches to the Investigations and Classification of Cyber Threats Challenged by the Application of Artificial Intelligence Methods, In: Proceedings of the Information Systems and Grid Technologies – ISGT 2020, Sofia, Bulgaria, 148-158, 2020, http://ceur-ws.org/Vol-2656/paper8.pdf, last accessed 2021/11/02
17. Sharkov, G.:Assessing the Maturity of National Cybersecurity and Resilience, Connections: The Quarterly Journal, vol. 19, issue 4, pp. 5-24 (2020).