PPHS CYBERSECURITY STANDARD

FOR SMALL AND MEDIUM-SIZED ENTERPRISES AND PUBLIC INSTITUTIONS

POLISH PLATFORM FOR HOMELAND SECURITY

PPHS CYBERSECURITY STANDARD FOR SMALL AND MEDIUM-SIZED
ENTERPRISES AND PUBLIC INSTITUTIONS

TABLE OF CONTENTS

03

INTRODUCTION

Cybersecurity Standard was developed in order to indicate a model for determining, implementing, monitoring and improving the level of cyber security in small and medium-sized enterprises and public institutions. The standard derives mainly from existing and recognized standards, which were adapted to the specificity and functioning conditions of the above mentioned entities.

The Standard consists of four main stages:

1. Asset management (more in the Annex 1)
2. Risk management
3. Security control selection and its implementation
4. Security testing and auditing and constant improvement.

Stages were divided into tasks. Additionally, the 2nd stage was divided into 4 phases.

STAGE 1: ASSET MANAGEMENT

The organization should implement a comprehensive asset management framework. It is crucial that the entity identifies all the assets at its disposal. This will allow the organization to understand the requirements related to its protection and take appropriate measures to ensure its security. A register of the assets should be the outcome of the final stage .

It is necessary to identify what really needs to be protected in order to ensure cybersecurity in an organization. It is necessary to identify what really needs to be protected in order to ensure cybersecurity in an organization. Each organization is limited as for providing cybersecurity, so it is necessary to identify what is the most valuable to the entity, what is important in terms of liability, and consequently what needs to be protected as a priority. At this stage, those activities will help understand the (legal, business, regulatory, etc.) environment in which the organization operates - to recognize the requirements and adapt to them.

The final effect of this stage is the creation of an asset register. It is essential to carry out further risk management activities and to identify responsibilities which will ensure an adequate level of asset security. The stage consists of several tasks.

STAGE 1: ASSET MANAGEMENT

Task 1: Identification of the assets.

Assets are to be understood as all information resources of value to the organization and its environment. Not only are the assets basic resources such as databases, documents, files, but also everything that is related to them and affects them: people, processes, technologies (more in Annex 1). Assets must be protected throughout their life cycle: from their creation, through their collection, storage, processing, transfer, to their destruction. The identification of the assets themselves should be accompanied by the identification of additional data related to them: location, format, quantity, life span, etc. The impact of assets on the implementation of processes in the organization should also be taken under consideration. This will help to manage the assets more effectively and reduce the level of risk.

Task 2: Identification and assignment of each of the assets to the owner.

Each set of assets should be assigned to an owner. The owner is responsible for asset management, including security activities. Asset management is a process that does not end after a "one-time" execution. It must be repeated and improved over time. Therefore, it will also be the responsibility of the owner to regularly update asset management activities, including those directly related to security. Permanent cooperation between owners of different assets is required in order to maintain the stability of the organization.

It is worth emphasizing that the owner is responsible for daily asset management, but the final, strategic legal and business, etc. responsibility lies with the management of the organization.

STAGE 1: ASSET MANAGEMENT

Task 3: Determination of the requirements on asset protection.

The functioning of the organization is influenced by many factors, both internal and external. They are the context in which the entity operates. They result, among others, from legal obligations (e.g. personal data protection), business environment, etc. Context analysis allows to identify all additional requirements (e.g. legal) related to the protection of the assets which must be implemented.

Task 4: Determination of the asset value and classification.

The objective of the action is to recognize the value of previously identified assets and clearly communicate it to all stakeholders. The classification should take into account internal and external conditions of the organization. The basic classification can come down to a description such as "confidential" and "public". Additionally, the asset owner may describe how the loss of asset confidentiality, integrity and availability in terms of cybersecurity and other legal requirements such as data protection affected the entity.

STAGE 1: ASSET MANAGEMENT

Task 5: Identification of current safeguards. The organization should identify those safeguards that are already in use.

At this stage it is important to establish and document which safeguards have already been implemented and are being applied in the organization. Among others, this will allow to better understand the risks, avoid duplication of activities and help to plan the implementation of other safeguards. It is worth emphasizing that the notion of a safeguard should be understood broadly. It may include processes, technological and organizational solutions etc.

Task 6: Creation and maintenance of an asset register

This task consists in creation of a register. It's not a one-time operation. The register should be checked and updated at fixed intervals and whenever major changes are implemented in the organization or when any safety incident has occurred. Safety incidents should be recorded in a separate register.

STAGE 2: RISK MANAGEMENT

The organization should implement a process of risk management. One of the most important elements of this process is a risk assessment which will help to make appropriate decisions ensuring safety in the organization.

The main objective of this phase is to analyze the risks which can be faced by the organization and take appropriate safety measures. The process should be documented.

Every organization has limited (financial, human, physical) resources and should focus its activities on the risks, which are the most important for safety and legal requirements. Risk assessment allows you to understand the situation and implement the best strategy while maximizing the use of the organization's resources.

The stage was divided into 4 stages, each consisting of several tasks which are to be implemented in the organization.

STAGE 2: RISK MANAGEMENT

Phase 1: Risk identification

Task 1:. Identification of threats to the security of assets

The organization should identify all threats that may negatively affect the safety of the previously identified assets. The organization shall also identify the sources of threats. The objective is here to possibly precisely identify who or what and how can endanger the security of the organization the most. The sources of threats may be categorized as given in Annex 2.

Task 2: Identification of vulnerabilities.

Vulnerability is understood as a weakness of the assets or safeguards which are prone to face threats. The aim is to identify as many weaknesses as possible which may appear in different ways or under different conditions during the utilization of assets. It is important to be aware that a negative impact on the security of assets may, as a result, impede the achievement of the organization's objectives.

STAGE 2: RISK MANAGEMENT

Phase 2: Risk analysis

In order to perform a qualitative or quantitative risk analysis correctly, an organization must examine two elements: the probability of previously identified risks and the consequences of their occurrence. It is worth emphasizing that it is impossible to eliminate all risks connected with the functioning of the organization. However, risk analysis makes it possible to ascertain that decisions on security measures are based on an objective analysis.

Task 1: Assessment of the potential consequences of the risk that may occur

In this task, it is crucial that the organization assesses the consequences of the threat which would have a negative impact on information assets. It is important to realize that the consequences can be multidimensional; namely, they can affect many areas, so it is important to analyze them in the context of possible occurrences that can generate costs, losses. Among others, those occurrences are related to:

- Loss of information assets,
- Unauthorized access to information assets,
- Unauthorized change of information assets.

The above mentioned occurrences should be the basis for estimating the consequences regarding e.g.:

- Costs of downtime,
- Costs of incident investigation (including costs of computer forensics and consulting services),
- Costs related to crisis management - e.g. costs of incident management, informing clients about losses and negative consequences, etc.,
- Costs related to legal and regulatory sanctions,
- Costs related to lost opportunities, such as damaged reputation, lost potential clients, etc.

STAGE 2: RISK MANAGEMENT

Phase 2: Risk analysis

Task 2: Probability assessment of threat occurrence

Once the consequences are determined, the next step should be an analysis of the likelihood of exploitation. In this task, the previously indicated elements should be taken into account: sources of a threat, vulnerabilities, existing safeguards, their effectiveness on the basis of their actual functioning, etc. While assessing the probability, an organization should extract information from diverse sources, e. g.: its own and employee experience, history, statistics, expert reports, etc.

Task 3: Comparison of the risk analysis results with predefined acceptable risk levels

The organization should define acceptable levels of risk. They will help to assess which risks and at what level the organization is able to operate. Establishing acceptable levels of risk will then allow them to be compared with the levels of risk resulting from the risk analysis. When establishing an acceptable level of risk, a previously adopted classification, built on the basis of values assigned to individual assets, should be taken into account. It is a decision of the organization what level of risk they agree to accept. In this process, the management should be supported by the owners of the assets. Actions taken within this task will be significant at a later stage when the organization makes a decision on how to deal with the risk.

STAGE 2: RISK MANAGEMENT

Phase 3: Evaluation of the analyzed risk.

The organization should define acceptable levels of risk.

The organization may accept the risk when the outcome of the risk analysis (phase 2) is lower or equal to the acceptable level of risk assigned to the information asset. This decision shall be documented and confirmed with the signature of the organization's management. The risk shall then be regularly reviewed and it should be assured that it remains at an acceptable level.

However, if the risk level is higher, the organization should decide to take appropriate action in accordance with the agreed strategy.

STAGE 3: SECURITY CONTROL SELECTION AND ITS IMPLEMENTATION

The organization shall select and implement adequate safeguards which, while increasing safety, reduce the level of risk identified to an acceptable level.

There are four main (but not sole) categories of security controls:

- Personal (including training),
- Technical,
- Physical,
- Organizational.

All types of security measures are designed, among others, to prevent incidents, help to detect them and minimize the possible consequences.

Based on the results of the risk analysis, the owner of the information asset (if necessary following agreement of other entities) should decide which safeguards should be applied. The implementation of safeguards is to reduce the risk to an acceptable level.

When the organization decides to implement specific safeguards, the organization should take into account that the key to achieving its objectives is maintaining business continuity.

STAGE 4: SECURITY TESTING, MONITORING, AUDITING AND CONSTANT IMPROVEMENT

In order to stay abreast of the constantly evolving factors affecting safety, the organization should regularly improve, maintain and update its safety measures.

The implementation of security measures must never be regarded as a one-time action. It should be a process which should be monitored and repeated at regular intervals. Key elements of this process (such as risk estimation) should be reviewed, updated regularly and whenever there are major changes in the organization or serious security incidents and occurrences regarding security.

In addition, the organization should conduct security tests and audits. The owner of the asset plays an important role in this process as the person who assists the organization's management in supervising the proper implementation of all the above activities.

Activities undertaken in stage 4 should be documented.

ATTACHMENTS

Annex 1: Examples of information assets:

- Information: databases, documents and data files (customer, financial, employee data, product information, contracts, plans, system documentation, research information, training materials, operating procedures, etc.), audio and video records, encryption keys and certificates, data on the work and operation of the software, systems and people's activities, passwords and identifiers.
- Software: applications, system software, configuration data, software security, etc.
- Processes: accounting processes, HR processes, production processes, etc.
- Physical resources: computer hardware, telecommunication equipment, media, physical protection, etc.
- Services: processing and transmission services, power supply, data destruction, etc.
- People: employees, management, third parties, etc.

Annex 2: Example sources of risk categorization:

- Internal (employees with excessive privileges, untrained employees, employees with low awareness of security issues or with special authorizations, faulty or ineffective security measures).
- Enemy entities (np. hackers, hacktivists, criminals and organized crime groups, states engaged in hostile activities in cyberspace, terrorists).
- Environmental risks (e.g. fire, flood, earthquake),
- Business risks (lacks of utilities, equipment failure, supply chain risks, employees).

ATTACHMENTS

Annex 3: Key principles for implementing the Standard:

- The Standard must be recognized as an integral part of the strategy according to which the organization operates. Cybersecurity Management should be closely linked to the mission, objectives and processes within the organization.
- Cybersecurity should be considered in an organization as a part of the overall security system.
- A precondition for effective and efficient implementation of the Standard is obtaining support from the management level in the organization.
- A key element is the continuous awareness and communication of cybersecurity objectives and responsibilities to all entities involved, in compliance with their areas of operations and responsibilities.
- As cybersecurity is a part of general strategic approach it must receive proper funding and competences. The cybersecurity level should derive from risk assessment determined within the conditions and activities of the organization.
- All steps included in the Standard implementation cannot be considered as a "one time" task, but rather as a continuous process which will constantly help to improve and modify the applied solutions. When the objectives and the scope of activities in the entity change along with the threats connected with it, cybersecurity issues also evolve.
- The actions included in the Standard are constructed with a risk-based approach. This method helps to solve the problem of limited resources in the organization. It results from the fact that the entity is able to identify and secure their most valuable assets, while taking under the consideration the possible risk.

POLISH PLATFORM
FOR HOMELAND SECURITY

Polish Platform for Homeland Security

ul. Slowackiego 17/11
60-822 Poznań
www.ppbw.pl/en
tel.: +48 (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

European Funds
Smart Growth

Republic
of Poland

European Union
European Regional
Development Fund

The project “Cybersecurity – PPHS Standard for SME and public institutions” was financed by the European Regional Development Fund.