Identification of assets in the process of privacy protection

Ing. Matúš Ivančo, prof. Ing. Tomáš Loveček, PhD.
Faculty of Security Engineering, University of Zilina, Zilina

***Abstract* — Currently, the issue of personal data protection is a topical issue, because of the expected approval of the Personal Protection Act in the Slovak Republic, which will be the transposition of GDPR. The paper provides a guidance on identifying of assets and interrelated or interacting activities in connection with the process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organization's broader risk management framework. In the context of a privacy risk management process, personally identifiable information will be considered as an asset. For the purposes of this article, the terms and definitions given in ISO / IEC 29100, ISO / IEC 29134, ISO / IEC 27000, ISO / IEC 27005, ISO Guide 73 will be used.**

***Keywords*:** privacy, identification, assets, processing of personal data, threats, risk

1 INTRODUCTION

The issue of the personal data protection is increasingly discussed subject at various national or international conferences. The obligation to deal with this issue no longer has arisen from law or technical standards, but rather from the need to provide sensitive (personal) information (e.g. IoT) to internal and external threats. The information and technological development of the company, in addition to the boom of classical information criminality (disruption of the basic attributes of information - accessibility, confidentiality, integrity), also has resulted in the development of methods of deep analysis and processing (e.g. Deep Learning) of Big Data, which represents a new, unresolved danger for the company. Information, from the point of view of the assets of the organization, becomes more valuable than other tangible or intangible assets. For this reason, it is necessary to pay attention to the protection of information, and in particular to information relating to a natural person (so-called personal data).

To ensure a sustainable security of information, it is necessary to introduce a systematic management mechanism that ensures correct treatment of the information used in the individual processes of the organization. Such guidance on the optimal mechanism for the handling of personal information (personal data) is provided in ISO / IEC 29 100: 2011 Privacy Policy. Regarding to the protection of personal data, the identification of the asset process transforms one of the initial steps in the information security management process.

2 ASSETS OF ORGANIZATION

In the process of risk management for information security, there are included identifying assets in the risk identification part, where the input for the Asset Identification process represents the range and limits of the risk assessment, the list of core components pertaining to owners, functions, locations, etc.

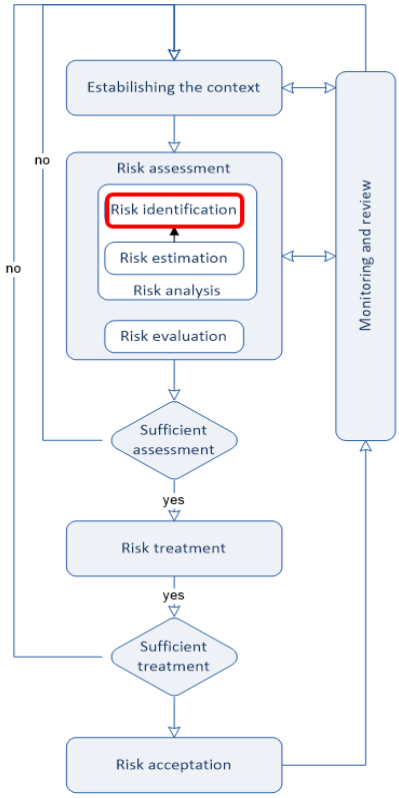

Figure 1: Information security risk management process [1]

Organization assets, whether business assets, employees or information, as well as company outputs, represent the value for the organization, next needed to be protected. Information and processing equipment assets should firstling be identified and the list of these assets should be updated on a regular basis. Each item in the asset list should be classified and assigned by the asset owner.

3 CLASSIFICATION OF ASSETS

The input of the asset identification process is defined by the scope and limits of risk management for information security. In order to determine the values of individual assets, they have to be identified. According to ISO / IEC 27005, the assets are divided as follows:

Primary assets include:

- Business activities and processes,
- Information.

Supporting assets, whose role is to ensure the integrity and connectivity of the primary assets:

- Hardware,
- Software,
- Networks,
- Locations,
- Organizations,
- Employees.

To assets into two groups (primary and supportive) enables us to understand the interrelationship between them and subsequently to create asset modules of the organization [2].

4 PRIMARY ASSETS

According to ISO / IEC 27005, business processes and information are further distributed as follows:

Business activities and processes, including processes:

- whose loss or limitation would not allow the organization to meet its main goals,
- which, if modified, can significantly affect the achievement of the main objectives,
- which are required to meet contractual legal or regulatory requirements,
- which contain secret processes (patented technologies).

Primary information is including:

- personal data are defined in the Privacy Act,
- information important to meet the organization's main goals,
- strategic information,
- Information requiring high financial costs, accumulation of storage, processing and transmission or requiring a considerable amount of time [1].

The fundamental difference between process and activity is primarily in the rate of generalization. In the term of the process, we understand any activity using resources and is managed to transform inputs to outputs. As follows from previous statement, the process is basically an activity or a sequence of activities that fulfill a predetermined goal.

The main input of each process or activity is information. On the basis of its character and content, the individual activities resulting in the desired output are subsequently performed.

From the point of view of the information security of the organization, they represent personal data, one of the most important components of the system that needs to be protected. Based on this knowledge, the regulation of European Parliament 2016/679 was issued in 2016. The regulation remarkably affects the whole process of information security management.

4.1 Classification of personal data

According to the regulation of the European Parliament 2016/679, the term personal information means *„any information concerning an identified or identifiable physical person. Identifiable physical person is a person who can be identified directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier, or a reference to one or more elements specific to physical, physiological, genetic, mental, economic, cultural or social identity of that person. "*

Among these specific identifying elements, we include in particular:

- **genetic data** - personal data concerning inherited or acquired genetic characteristics of a person and providing unique information on the physiology or health of that person
- **biometric data** - personal data resulting from specific technical processing related to the physical, physiological or behavioral characteristics of the natural person allowing to clearly identify the person
- **health data** - personal data relating to the physical or mental state of a person, including data on the provision of healthcare services [3]

5 SUPPORTIVE ASSETS

In order to ensure the processing of primary assets, it is necessary to identify support assets which threat directly affects the integrity of business activities and information. Different kinds of supporting assets can have occurred:

1. **Hardware** representing all processes supporting physical elements:
   - Data processing equipment:
     - fixed devices (PC, server),
     - portable devices (notebook, tablet, PDA),
     - peripheral devices (printer, removable disk drive).
   - Data carriers:
     - electronic media (CD, DVD, USB, HDD, SSD),
     - other media (paper, fax, slides).
2. **Software** representing all programs supporting the operation of hardware for data processing:
   - Operating system (Windows, Linux, OS X),
   - Service, management, or maintenance software (AMI, RiZone, Evis),
   - Software packages (Office 365, MySQL, Oracle),
   - Enterprise applications (Enterprise, Microsoft, Kros).
3. **Networks** representing a group of all telecommunication devices used to interconnect individual elements of the information system:
   - Communication interface (GPRS, Ethernet adapter),
   - Media and support (ADSL, FireWire, Bluetooth),
   - Active or passive transmission (router, switch, hub, bridge).

4. **Locations** shall include all places and physical means necessary for their operation:
   - Zones (access zones, security zones),
   - Compound (premises, building),
   - External environment (premises of other organizations, workers' homes),
   - Services (water supply, waste disposal, electricity supply),
   - Communications (telephone line, internal telephone networks),
   - Equipment (electricity, converter, air conditioning).
5. **Organizations** representing the entire organizational framework, consisting of all staff structures and procedures controlling the following structures:
   - Managing Authorities (Managing Authority, Organization Headquarters),
   - Organizational structure (security service, fire service, IT),
   - Project / System Organization (Information System Migration Project, New Application Development Project),
   - Suppliers / subcontractors / producers (purchasing services company, company management company).
6. **Employees** representing a group of persons involved in the information systems of the organization:
   - Managers (senior management, project managers),
   - Developers (enterprise application developers),
   - Operators and maintenance (system administrators, application operators),
   - Users (human resources management, finance, risk management) [1].

For the purposes of regulation No. 2016 / 679, processing means *"operation or set of operations with personal data or sets of personal data, such as retrieval, recording, arrangement, structuring, storage, reprocessing or alteration, searching, browsing, exploitation, transmission, or otherwise provided, regrouped or combined, limited, erased or destroyed, whether performed by automated or non-automated means."*

These processing operations are carried out by individual support assets.

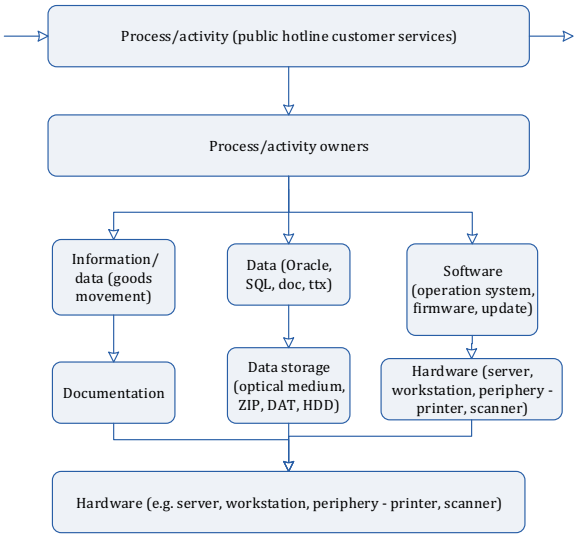

Figure 2: Dependence of organization's activities on assets [4]

6 LINKS BETWEEN PRIMARY AND SUPPORTIVE ASSETS

Defining links between asset types is an important part of the process of identifying primary and supporting assets. If we can't understand and describe their interrelationships and mutual links, we will not be able to evaluate the impact of individual identified threats using vulnerabilities in supporting assets.

One possible solution to the problem is to create asset modules. In the phase of its compiling, it is advisable to proceed from the process map of the organization. The asset module shows the linkage between specific primary and supporting assets with the purpose to realize a particular process, expressed as a primary asset. This approach is based on the knowledge that the information represents inputs or outputs of individual processes, and this information is accessible through specific software applications which data is stored on specific hardware devices located in specific areas and attended by specific owners. In this way, a certain dependency chain of specific assets is created. On its basis we know to accurately identify the likely vulnerable attack site and the amount of damage occurring after an attack [4].

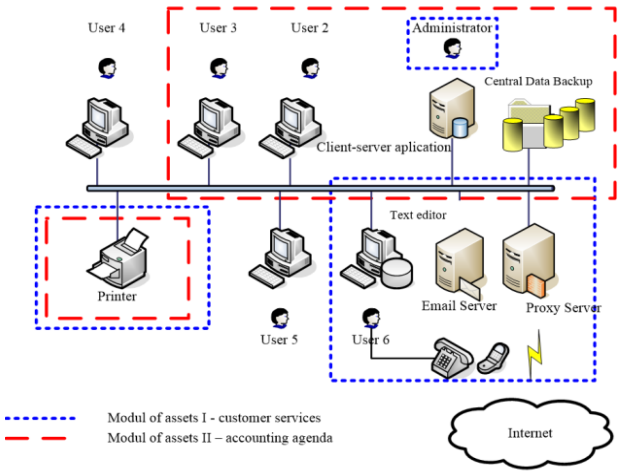

Figure 3: Example of creating modules of assets [4]

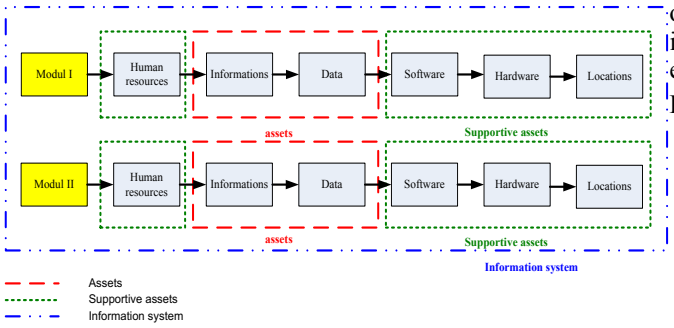

Figure 4: Example of information system in block diagram [4]

7 THREATS TO ASSETS

There is a high number of threats with effects on organization's assets, while they may differ in their source (hacker and water course), their form of expression (infringement of integrity, availability, confidentiality, or their combination), periodicity of occurrence (damaging code and an earthquake) or the extent of potential consequences. In general, we may divide threats into intentional and accidental, and further into external and internal ones.

Intentional threats are such threats, which source is a purposefully-acting natural person – attacker (organization's own employee, service-organization employee, strange person) with the aim to manipulate with organization's assets without authorization (e.g.: steal, misuse, damage, destroy, change). A motive or cause of such action may be profit, revenge, damage to interests/property, frequent staff migration, challenge, ego, rebellion, prestige, destruction of evidence, exploitation, political advantage, drawing attention of media, competitive advantage, economic espionage, curiosity or blackmailing.

Accidental threats are such threats which may arise independently from person's will. Their sources may be found inside or outside the organization. External accidental threats are such threats, which sources are found outside the organization and they operate from this space. They include environmental threats, technical threats and the so-called 'force majeure' threats. Force-majeure threats are to be understood as threats independent from person's awareness or acting (meteorite fall, deflection of the planet from Earth's axis). Environmental external threats are mainly disasters (sun eruptions, inundations, floods, fires, windstorms, landslides) where cumulated energies or masses are released excessively, possibly accompanied by destructive factors with negative impacts on assets. Technical external threats are mainly emergencies (explosion, fire) bringing about effects of destructive factors with a negative impact on assets. Internal accidental threats are threats; which sources are located inside the organization. Such threats may include social and technical threats. Internal accidental technical threats may be mainly crashes of technical devices forming a part of the organization, or technical failures of physical assets (Single Points of Failure). Internal accidental social threats are mainly represented by authorized persons who may, as a result of a lack of their knowledge (security awareness), forgetfulness or negligence, threaten the value of assets (blocking the access to a system after unsuccessful logins of an authorized person; unauthorized entry into an information system as a result of damaging security elements) [4].

Basic types of threats may be divided into:

- physical damage (fire, corrosion, freeze-up),
- natural disasters (climatic, seismic, floods),
- loss of basic services (air-conditioning breakdown or water supply malfunction, electric energy supply interruption),
- technical failure (device failure, overloaded network, maintenance error),
- threats to information (remote espionage, divulgement, forgery, wiretapping),
- threat to functionality (shortage of staff),
- unauthorized activities (unauthorized use of equipment, authorities, data processing, forgery),
- disruptions caused by radiation (electro-magnetic radiation, thermal radiation) [1].

8 CONCLUSION

The result of asset identification is a list of assets of the organization that provides the basis for the subsequent risk analysis impacting the assets. Without a thorough examination and knowledge of all information assets would be impossible to effectively protect the goals and mission of organization. For this reason, is necessary to introduce a systematic management mechanism for each organization to ensuring the correct handling of the information used in its individual processes. The importance of creating of given mechanism results from the growing threats of attacks on companies' personal data and their exploitation for commercial or criminal purposes. Each primary goal of organization is to ensure that its clients and employees are protected against threats that could harm their privacy. Therefore, the solution of this issue is currently considered to be one of the most important tasks of each organization.

REFERENCES

[1] ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management.

[2] ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council - Article 94 - Repeal of Directive 95/46/EC

[4] Kampová, K., Loveček, T.: Security systems - Managing security in organization. EDIS publishers, University of Žilina, 2007. ISBN 978-80-554-0615-2.

[5] ISO/IEC 29 100:2011 Information technology - Security techniques - Privacy framework

[6] ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment