Insider Threats in Critical Infrastructure Organizations - Discovery and Protection

Ivan Gaidarski[1,2][0000-0002-4979-445X]

[1] Institute of Robotics "St. Ap. and Gospeller Matthew", Bulgarian Academy of Sciences
[2] Acad. Georgi Bonchev Str., Bl. 2, PO Box 79, 1113 Sofia, Bulgaria
ivangaidarski@ir.bas.bg

Abstract. In this article, we examine what constitutes critical infrastructure and the nature of internal threats to its information assets. We discuss innovative methods for detecting internal threats, measures to combat and mitigate them, and preventing the leakage of sensitive information. We examine the causes of internal threats - intentional actions or negligent behavior of employees with access to critical resources (insiders), as well as gaps in the organization's IT security policies. Security measures include defining information sensitive to the organization, measures to detect internal threats, stop the leakage of sensitive information, analysis of user behavior, risk assessment and profiling, and analysis of information flows in the organization. We also present methods for protecting against leakage of sensitive data through a holistic approach that covers data both inside and outside the organization. We examine user activity monitoring systems and data leakage monitoring systems for data leakage prevention (DLP).

Keywords: Critical Infrastructure, Insider, Threats, Data Leak Prevention, DLP

1. Introduction

The life of the modern people is highly dependent on the modern civilization achievements – electricity grids, telecommunications, railways and roads, gas and water transmission networks. These assets and services rely on the seamless operation of large-scale infrastructures and facilities, which are known as Critical Infrastructure (CI). CI can be described as Infrastructures of significant national importance, which enable society and the economy to function [5].

CI refers to various assets, services, systems and processes, technologies, facilities, essential to the safety, security, health and economic well-being of the society and citizens, as telecommunications, electrical power grid and plants, transportation facilities as roads and railroads, water distribution systems, healthcare services, security, banking and financial systems and many more [2].

Here are some definitions from some major international organizations:

Research Paper
DOI: https://doi.org/10.46793/BISEC25.086G
Part of ISBN: 978-86-89755-40-4

EU: According to the EU Directive 2008/114/EC, critical infrastructures can be defined as assets, systems, or parts thereof, essential for the maintenance of vital societal functions, health, safety, security, economic, or social well-being [1].

NATO: Physical or virtual systems and assets under the jurisdiction of a state that are so vital that their incapacitation or destruction may debilitate a state's security, economy, public health or safety, or the environment [8].

International Telecommunication Union: The key systems, services, and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these [7].

International Organization for Standardization: Organizations and facilities that are essential to the functioning of society and the economy as a whole. The standard elaborates that a failure or malfunction of such organizations or facilities would result in sustained supply shortfalls, make a significant impact on public security, and have other wide-ranging impacts [6].

CI can be stand-alone or interconnected geographically across local territories or national borders. The CI elements are dependent from each other, for example all communications depend from electrical power, the electrical distribution himself is dependable from the communications, roads and etc.

CI assets are so crucial to the society, that their malfunction will have critical impact on security, national economy, national public health or any combination of these [3]. There are many possible threats to the CI, such as extreme weather (storms, hurricanes, heavy snow), accidents (accidental, intentional, human errors), natural disasters (earthquakes, flooding, fires), pandemics (plague, HIV, smallpox), technical faults (software errors, human factor, equipment faults), malicious attacks (direct or remote), external and internal cyber threats.

Some of these threats are unavoidable and unpredictable (natural disasters or extreme weather), but their effect can be mitigated, if pro-active measures (monitoring and control of key parameters) and appropriate afterward procedures are taken, to ensure the normal operations after the failure event. A failure event can be defined as a negative incident, which can impact the normal functioning of the infrastructures or it's subsystems [3].

If we take a look to the CI as s system, one of the basic requirements is that the system should continue to operate even after one or more of its components have failed.

Due to deregulation purposes, one of the most vital requirements of CI is they should have various autonomous subsystems. So, even one or more of subsystems have failed, the system can continue to operate normally. The different CIs are interconnected and potential damage to one infrastructure can lead to cascading failures in others, which can have serious and unpredictable consequences [4].

To achieve the continuous work of CI, a systematic approach must be performed. Such is for example the holistic approach, which ensures the protection of all of the system (CI) components and grants the normal operation after potential failure. The holistic approach includes risk assessment of the security (confidentiality, integrity, authenticity, availability) level of all assets (physical and cyber) in all layers of the system.

To perform a holistic approach, the protection measures toward the different subsystems must include all possible vectors of attacks and take into account all of the possible threats and vulnerabilities. Developing methods and measures for quickly detecting, isolating, and recovering the faulted subsystems is from extremely importance. It can be achieved with development of a common framework for modelling the behavior of CI subsystems and for designing methods and measures for intelligent monitoring, control, and security of the CI and it's subsystems [21][22][23][28][29][33],[34],[35].

In this article we take a look at the discovery and protection from insider threats, as one of the components of the holistic approach for CL protection. Due to the unpredictable nature of the internal threats, the usage of innovative methods of protection are necessary, such as cyber threat intelligence, behavior analysis, consumer behavior analysis, risk assessment and profiling, analysis of information flow and definition of organization-sensitive information. We look at the causes of insider threats, such as negligent behavior of insiders, e-identity theft and malicious users. We also present holistic approach for protecting sensitive data that covers data both inside and outside the organization. Systems for cyber threat intelligence, user activity monitoring and Data Leak Prevention (DLP) are discussed.

2. Internal threats to critical infrastructure security.

To deliver their services and conduct the normal operations, the CI systems and subsystems are highly dependent from information and communication technologies – the so-called Critical Information Infrastructure (CII). Potential disruption to the CII could have significant impact to the ability of CI to perform its essential mission. In order to provide effective protection and assurance of the resilience of CI, a security plan and policies must be developed, part of Critical Information Infrastructure Protection (CIIP) program. These policies are part of the cybersecurity program, which is designed to protect against all forms of cyber threats by strengthening and securing CII's networks and services.

There are many legislative regulations and Information Security standards which regulate the measures, taken in organizations, for example ISO 27000 [11][12], ISACA's COBIT [13], NIST 800 Series [14], sector-specific regulations as the Gramm-Leach-Bliley Act (GLBA) [15] for the financial sector, Sarbanes-Oxley Act (SOX) [16][17] for US public companies, Health Insurance Portability and Accountability Act (HIPAA) [18] and Payment Security Industry (PCI) Data Security Standard (DSS) [19] for credit card operators. As they incorporate the most important aspects of IS, these standards and regulations are only sets of recommended and good practices. Most common practice are single actions to solve certain tasks as incidents (leakage, attack on infrastructure, loss of information, etc.) or new challenges - for example recently adopted regulation EU GDPR [20] for protection and processing of personal data of EU Citizens.

The cases in which the IS are approached methodically and all requirements of the standards are satisfied, are not very common.

Cyber incidents can take many forms of malicious activity, such performed by botnets Denial-of-Service attacks, malware infections, phishing, ransomware attacks or identity theft and they can affect the ability of the CI objects to perform its normal operations [7].
The threats can be External, with the vector of attack outside to inside and Internal, with vector of attack inside to outside direction.
When we talking about External threats, we assume that the attack to the assets comes from an external source – for example a hacker attack. The attack must be stopped and not to be allowed to the penetrator an access to the resources of the organization. A typical example of IT Security solution, which are used against external attacks are the classic firewalls.
Protection from Internal Threats means, that the assets must be protected in Inside-Out direction. These attacks are typically performed by insiders - persons with legal access to the resources of the organization. The assets must be protected in such way, which makes the leakage or export of the sensitive data of the organization or CI object impossible. Combating these threats requires unconventional approaches. The typical solutions from Internal threats are the Data Loss Prevention (DLP) solutions - for example Acronis Device Lock [24], Netwrix Data Loss Prevention [25].
Many organizations do not understand the causes of the Internal Threats incidents and how to detect and prevent them, as they are virtually unpredictable.
An incident caused by an Internal Threat occurs when an insider, employee, partner or provider with authorized access to an organization's sensitive information, intentionally or accidentally misuses that access, resulting in negative consequences. There are many causes for the rise of the internal threats – Table1.

Table 1. Causes and countermeasures of the internal threats.

Causes and actors	Countermeasures
Negligent behavior of insiders, accidentally sharing sensitive data, opening malicious phishing emails, using illegitimate software.	Security awareness program and compliance with IT Security regulations and personal responsibility. Regular security audits.
Third parties - external consultants and suppliers, with authorized access to of the organization's resources, which not follow the internal security policies.	An effective counteraction measure is the monitoring and recording of all external actions. Regular security audits.
Too many and too strict IT security policies, implemented in an organization may be the	Continuous training, maintaining open dialogue, seeking feedback and proactive sharing of good

root cause of insider-related incidents, creating too many barriers to the usual daily work of the employees, and can lead to so-called “Security Fatigue effect”.	practices with employees. Adopting policies and solutions with transparency of daily activities - principle of non-intervention.
Electronic Identity Theft. The reasons can be using of weak passwords, lack of a policy for changing them periodically, the lack of strict rules for their formation, as well as the use of the same passwords to access different resources.	Adoption of a strict policy for the passwords, two-factor identification (2FA), as well as additional biometric identification through fingerprints, scan of the iris, retina or face.
Malicious users - persons with privilege access, for example technicians could use their level of access to the organization sensitive data.	Understanding the true intentions of the users is very important to combat internal threats effectively.

Depending from their source, the internal threats can be divided into several groups:

1. Human threat – They can be completely intentional or unintentional by mistake. To identify that threats, it is very important to classify the different types of users and profile them by the risk they carry for the organization [23].

The following categories of users may be identified:

- External vendors
- Privileged users
- Employees with access to sensitive data

2. Employee’s activities – the most common vector of internal threat. The employees may take actions that harm the sensitive information and the critical IT systems of the organization, due to negligence, carelessness or malice intentions.

3. Business applications - The usual applications used by employees - accounting systems, invoicing systems, CRM systems and CAD applications, can be a serious source of risks, because of their access to sensitive data.

The modern cloud services, communication applications, peer-to-peer file sharing (torrents) are a direct source of high risk for the organization.

3. Discovery of internal threats

Organizations with serious attention to the IT Security, invest hard in human and IT resources, to ensure the security of their infrastructure - virtual private networks (VPN), firewalls, intrusion detection and prevention systems (IDS and IPS), monitoring systems as database activity monitoring (DAM), security information and event management (SIEM) systems.

The traditional IT security systems are target toward the external sources of threats, ignoring the fact that insiders - have direct and legal access to sensitive data and critical systems. The insiders easily can overcome the traditional IT security systems and the security of the organization's sensitive information is completely dependent on their goodwill. There is a need for new and unconventional methods of protection, such consumer activity monitoring systems and Data Leakage Prevention (DLP) systems, which are based on new methods for detecting threats, such as user behavior and activities analysis, risk assessment and analysis and profiling and analysis of information flow and definition of organization-sensitive information.

3.1 User behavior analysis

By monitoring the everyday behavior of the individual users, we can create a profile of the users, according to the risk that he carries for the organization. This type of profiling requires preliminary classification of the various actions in daily work and we must take into account the specifics of the different roles that employees have in the organization, the IT security policies, compliance with different standards and regulatory mechanisms, business documentation and etc. By analyzing the user behavior we can detect a behavioral anomaly, show negligence or intend hostile actions. A different type of suspicious behaviors can be distinguished:

- Non-typical access to files, systems or other IT resources;
- Access to systems outside of normal hours of the day or days of week;
- Perform unusual operations or infrequently used commands;
- Generate larger than usual reports;
- Access to systems from unusual client machines or from outside;
- Performing an unusual number of actions compared to normal.

3.2 User activities analysis

Monitoring of the user day-to-day activities can discover possible hostile acts to the security of the organization. The analysis can detect abnormalities in the normal daily activities of the users. Some of these activities can be:

- Visiting unauthorized websites that may install malware on systems.
- Installing remote access applications for home office mode;
- Uploading sensitive data to cloud services;
- Sharing sensitive data with other people via email, cloud apps, flash drives, and more;

- Using an application that process sensitive data;
- Opening phishing emails thus giving access to the internal network to hostile actors;

A special attention must be paid to the untypically privileged user actions:

- Escalating privileges for Unix or Linux users' workstations;
- Changing admin passwords;
- Making changes to configuration files that can cause system fail;
- Execution of malicious code leading to denial of critical services (DOS);
- Creating unauthorized local or remote accounts (VPN or SSH).

3.3 Risk assessment and profiling

By analyzing the data for user behavior and activities, we can create risk profiles of the users and the assess the risk they carry for the IT Security of the organization. We must take into account not only the information about their actions and behavior, but also the good business practices, the compliance with regulations and regulations.

Discovering the high-risk users will allow to take special measures to them and a leakage or stealing of sensitive information can be prevented.

3.4 Analysis of information flow and definition of organization-sensitive information

To properly protect the sensitive information of organization, we need to identify it, by taking holistic approach to information that the organization owns, uses, processes or generates. That approach captures all the data both inside and outside the organization [22][23].

The process of analyzing the flow of information within an organization and the definition of sensitive information includes the following phases:

1. Creating a model of information flow in the organization.
2. Classification of the sensitive information in the organization.
3. Identification of critical activities and starting points.
4. Accepting a policy to prevent leakage sensitive information.

A model of the information flow can be created by monitoring the information flow through endpoints, servers, databases and networks, using specialized monitoring tools. For the classification of the data and to determine the sensitive information for the organization, we must take into account the regulatory requirements, the legal framework and the good practices. On that basis, we can determine the degree of risk of the activities performed by the different users and the critical points through which sensitive data can be leaked outside the organization. This will help the management to create and adopt an IT Security Policy to prevent leakage of sensitive information [21][22].

4. Protecting from Internal Threats

The next stage is the implementation of innovative security solutions for internal threats protection using the above methods, such consumer activity monitoring systems and data leak prevention (DLP).

4.1 Consumer activity monitoring and analysis systems

This type of solutions gives IT security teams provide an insider look at all user actions, thus giving the opportunity for real-time detection of dangerous or unauthorized activities and the ability to block the risky users. They allow quick identification who what, when and how accesses the sensitive data, systems and applications. Such solution for example is Proofpoint Insider Threat Management [23]. It significantly reduces the incidents related to internal threats and exposure to risks:

- Monitor user activity in applications and visited web pages, no matter how they are accessed – locally or remotely.
- Behavioral analysis and automatic risk assessment of the users;
- Alerts for risk activities or violations of rules;
- Monitor users for suspicious activity and violations of the security rules;
- Compliance with regulatory requirements - GDPR, PCI, SOX, HIPPA, NERC, FFIEC, FISMA and FERPA.

4.2 Data Leak Prevention systems (DLP)

DLP systems are data centric – they are focused on the data flowing through organizations in all three dynamic states:

- Static data - Data-At-Rest
- Transferred Data - Data-In-Motion
- Used Data - Data-In-Use

DLP systems are designed to prevent attempts to leak, modify, or destroy the sensitive data of the organization, without interfering with the normal business processes. DLP significantly reduces the leak of sensitive information, resulting from internal threats like human error, intentional action or outside breach. The main goal of DLP is to stop the data before it leaves the protected environment [24].

DLP solutions can provides useful information for the protected sensitive data:

- Identifying of the organization’s sensitive data;
- Discovery of sensitive data;
- Identification of the threats and risks to the data;
- Discovery of the possible leakage points;
- Violations of security policies and procedures.

DLP systems can be focused on servers, global communications or data channels of the organization. The DLP can control email servers, file transfers from file servers,

and Internet traffic filtering. DLP can be also focused on endpoints and local data channels – workstations, laptops, mobile devices - tablets and phones.
Controlled channels include all possible physical ports, personal emails, file transfer to cloud services and more – as Acronis Device Lock DLP, shown on Fig.1 [24].

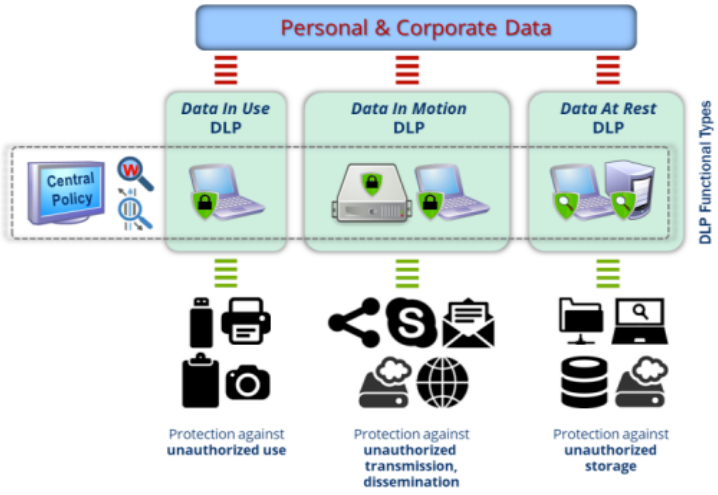

Fig. 1. Acronis Device Lock Endpoint DLP

The implementation of DLP in organization can effectively protect the sensitive information from Internal and External threats and additionally brings the following results – Figure 2 [21][22][23][26]:

- Reducing the sensitive information leak incidents (1);
- Limiting data leak channels (2);
- Improving compliance with the internal security policies, legal regulations and privacy directives (3);

Increasing the visibility of sensitive information, by the discovery function of the DLP (Data-in-Rest) (4);

4.3 Vulnerability Management

Vulnerability management systems identify, evaluate and report for security vulnerabilities in systems and applications in the organization. These systems maps, analyses, prioritizes and protects third-party apps against threats and attacks, by automated patch process or patchless mitigation. With the help of such systems the vulnerability exposure windows, which normally is 180 days can be reduced almost to zero [28].

4.4 Security Operation center

The Security Operations Centers (SOC) provides the information necessary for organizations to efficiently detect threats and subsequently contain them [28][29]. The SOCs gather information from different sources, as own sensors in the corporate network, import data from other security solutions like DLP, consumer activity monitoring systems, velnerability management systems or outside Threat Inteligence platforms [30]. SOC combine that data, analize it and show the correlation between different kind of security events, making possible to detect breaches and coordinate the appropriate response.

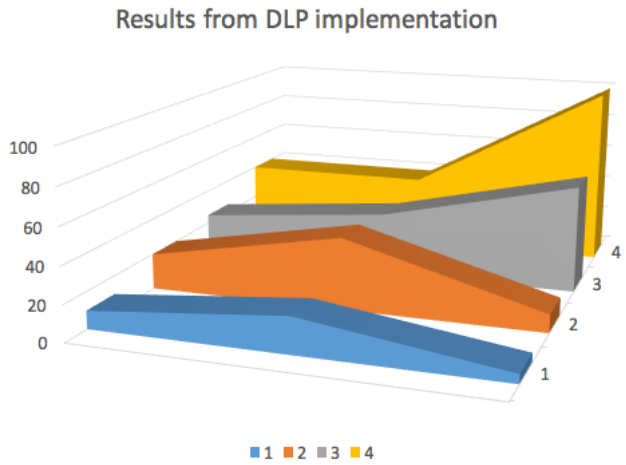

Fig. 2. Generalized results from DLP implementation

5. Conclusion

The modern challenges to the IT security of Critical Infrastructure require non-standard solutions based on entirely new principles. CI organizations need to develop a comprehensive, risk-based information security strategy to protect their sensitive information. Our holistic approach addresses the organizations data, profiling of the participants in the information process, based on what data they are using or processing, how and where they are using or processing it. With that approach, we can identify the the weak points in the organization and can take appropriate measures with the appropriate security controls as Data Leak Protection (DLP) systems, which can not only limit the data leaks, but improve the compliance with the internal security policies, legal regulations and privacy directives. in addition to cutting-edge security measures, a focus on the human factor in the organization is needed through proactive activities involving continuous training and enhancing security knowledge - Security Awareness Training.

Acknowledgments. This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. D01-74/19.05.2022.

References

1. EU Directive 2008/114/EC, Identification and designation of European critical Infrastructures, 2008, Available online via https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng, last accessed 2025/10/20
2. USA Patriot Act, Public Law 107-56, 2001. Available online via http://epic.org/privacy/terrorism/hr3162.html. last accessed 2025/10/20
3. Ellinas G., Panayiotou C., Kyriakides E., Polycarpou M., Critical Infrastructure Systems: Basic Principles of Monitoring, Control, and Security. In: Kyriakides E., Polycarpou M. (eds) Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems. Studies in Computational Intelligence, vol 565. Springer, Berlin, Heidelberg, 2015
4. Rinaldi, S.: Modeling and simulating critical infrastructures and their interdependencies. In: Proceedings of the 37th International Conference on System Sciences, 00(C):1–8 (2004), 2004
5. Garcia Zaballos A., Jeun I., Best Practices for Critical Information Infrastructure Protection (CIIP), 2016. Inter-American Development Bank (IDB) and Korea Internet & Security Agency (KISA), 2016
6. ISO (International Organization for Standardization). "Information Technology – Security Techniques – Information Security Management Guidelines Based on ISO/IEC 27002 for Process Control Systems Specific to the Energy Utility Industry." ISO/IEC TR 27019:2013
7. ITU (International Telecommunication Union). "Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts." ITU Study Group Q.22/1. Geneva, 2008
8. Schmitt, M. N., "Tallinn Manual on the International Law Applicable to Cyber Warfare." Prepared for the NATO Cooperative Cyber Defense Center of Excellence, Cambridge University Press, 2013
9. Polemi N., "Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains", Elsevier, ISBN: 9780128118184, 2017
10. Rhodes-Ousley,Mark. Information Security The Complete Reference, 2nd Edition, The McGraw-Hill, 2013
11. Hintzbergen, Jule, Kees Hintzbergen. Foundations of Information Security Based on ISO27001 and ISO27002. Van Haren, 2010
12. ISO 27001 official page: https://www.iso.org/isoiec-27001-information-security.html, last accessed 2025/10/20
13. IT Governance Institute. COBIT Security Baseline: An Information Survival Kit. 2nd ed. IT Governance Institute, 2007
14. NIST Special Publications (800Series): Available online via https://csrc.nist.gov/publications/sp800, last accessed 2025/10/20
15. Gramm-Leach-Bliley Act (GLBA): Available online via https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act, last accessed 2025/10/20

16. Anand, Sanjay. Sarbanes-Oxley Guide for Finance and Information Technology Professionals. Wiley, 2006
17. Sarbanes-Oxley Act SOX: Available online via https://www.sarbanes-oxley-act.com, last accessed 2025/10/20
18. Beaver, Kevin, and Rebecca Herold. The Practical Guide to HIPAA Privacy and Security Compliance. 2nd ed. Auerbach, 2011
19. PCI Security Standard: https://www.pcisecuritystandards.org/standards/pci-dss/, last accessed 2025/10/20
20. EU General Data Protection Regulation: Available online via https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, last accessed 2025/10/20
21. Gaydarski I, Minchev Z., (2017) Conceptual modelling of information security system and its validation through DLP systems, 9th International Conference on Business Information Security (BISEC-2017), 18th October 2017, Belgrade, Serbia
22. Gaydarski I, Kutinchev P, Andreev R, Holistic approach to data protection - identifying the weak points in the organization, International Conference “Big Data, Knowledge and Control Systems Engineering” BdKCSE'2017, 6th December 2017, Sofia, Bulgaria
23. Proofpoint Insider Threat Management, https://www.proofpoint.com/au/observeit-is-now-proofpoint, last accessed 2025/10/20
24. Acronis Device Lock DLP: https://www.acronis.com/en/support/protect/dlp/, last accessed 2025/10/20
25. Netwrix Data Loss Prevention: https://netwrix.com/en/products/endpoint-protector/, last accessed 2025/10/20
26. CYREX 2018: https://securedfuture21.org/cyrex_2018/cyrex_2018.html, last accessed 2025/10/20
27. Vicarius: https://www.vicarius.io, last accessed 2025/10/20
28. Dimitrov W., ICT Security Trends. Cyber Security. Avangard Prima, Sofia, 200 p. 2017, ISBN 978-619-160-766-2.
29. Dimitrov W., ICT Security Model. Cyber Security, Avangard Prima, Sofia. 2018, ISBN 978-619-160-950-5.
30. AT&T Cybersecurity https://cybersecurity.att.com, last accessed 2025/10/20
31. Fortra/ Digital Guardian DLP https://digitalguardian.com/, last accessed 2025/10/20
32. Trelllix https://www.trellix.com/en-gb/, last accessed 2025/10/20
33. Novakova Nedeltcheva G., Dimitrov W., Security dynamics - adaptation of ict infrastructure to cloud computing - threats and opportunities. International Scientific Journal Industry 4.0, 2:17–20, 2017.
34. Novakova Nedeltcheva G., Dimitrov W.. Security dynamics – adaptation of ict infrastructure to cloud computing – threads and opportunities. 2nd Intern. Conference High Technologies, Business, Society (HTBS) – 2017. Borovets, Bulgaria, 13-16 March 2017., 2017.
35. Dimitrov W., Dark data governance reduces security risks. BdKCSE’2016 – Big Data, Knowledge and Control Systems Engineering, 2016, December.