sciendo

Proceedings of the 5th International Conference on Economics and Social Sciences (2022), ISSN 2704-6524, pp. 881-895

The 5th International Conference on Economics and Social Sciences
Fostering recovery through metaverse business modelling
June 16-17, 2022
Bucharest University of Economic Studies, Romania

Cyber Security of National IT Applications and Critical Infrastructure for European Funds

Marius ȘTEFAN[1]

DOI: 10.24789788367405072-082

Abstract

Modernity is characterized by major transformations and evolutions, which have penetrated into the depths of all levels of human life, in all economic, political, and social spheres, thus significantly increasing the quality of human life.

These legacies of modernity have laid the foundations for an evolving present, characterized by a new model of society, in which production is being replaced by global information services, knowledge and technologies, called the information society. The post-industrial society focuses not on the production of goods, but on the use of services in particular, the evolution thus depending on the use of technology.

Thus, a hierarchy of knowledge occurs, so that the model of access to knowledge undergoes essential changes, the primary interest no longer targets the universal aspect, the concern becoming centred on the local-individual space, producing transformations between word and image, speech and personality.

The information society is the postmodern society, in which the old norms and ways of thinking are replaced by new technologies and new lifestyles. There is a transformation of civilization through three scientific and technological revolutions: traditional conventional crafts, the scientific organization of production, and the automation of the intelligent artificial future.

Starting from the increasing role of science in production processes, corroborated with the emergence of information technologies, the economy and society become focused on a new fundamental principle, namely theoretical knowledge.

The information society is a society in which the quality of life, as well as the prospects for social change and economic development, depend, to an increasing extent, on information and its exploitation. In such a society, living standards, working patterns, the education system, and the labour market are all markedly influenced by advances in information and knowledge. The theme of the information society is described by this phrase - the society based on theoretical knowledge, also being very well synthesized in the term of the information age.

[1] Bucharest University of Economic Studies, Bucharest, Romania, marius.stefan@mfe.gov.ro.

Keywords: e-Business; emerging technologies; digital transformation; digital culture and cybersecurity; security of critical infrastructure of national interest; European funds; development of the national economy.

JEL Classification: K24, F52, P48, L63.

1. Introduction

Technological developments in recent decades have radically changed the way people communicate with each other, the ways in which they have access to a wide range of services, starting with education and health and continuing especially with working methods.

For decades, the European Union, through its institutions at the Member States level, has been a guarantor of the principles underlying freedom and security (ENISA, 2020).

Respect for human rights, the rule of law, as well as solidarity, give the measure of a free European Union, which will ensure the increase of the quality of life of the citizens.

Public administration services can be simplified through the use of advanced information technology. The European Commission is trying to set its own example in this, through the procedures and tools it uses in its day-to-day work, in its links with Member States' administrations and its own decentralized agencies, which are marked by progress in computerization. The aim is to facilitate citizens' access to public information through new computer applications, as well as to achieve better communication between all levels of public administration across the Union, thanks to the high-speed connection.

The development of the European Information Society involves a considerable and ever-increasing financial effort, which cannot be fully assumed by the European Union and the governments of the Member States. Experience shows that the private sector is best able to take risks of exploitation, so on, and the development of new adaptable markets and holds the capital needed to make such investments.

The social dimension of the information society is undoubtedly one of the most important facets of the new model of society and must be treated with great care in order to minimize risks and maximize potential benefits.

Science has made possible the technologies on which the information society is based, and the needs of the scientific community have often led to innovation in information technology, today benefiting from the Internet and the World Wide Web.

Science is systematized knowledge, which also includes derived activities, such as scientific research, technological development, technology transfer, and innovation.

In the technological age, action plans and policies are being developed to meet the challenges, the most important technology being ICT, which allows information to be processed and conveyed in a revolutionary way.

We thus identify the key terms that dominate the world we live in today: information, communication, and knowledge. The information society is considered to be the ICT-based knowledge society. Information society technologies will evolve in the direction of being at hand in the process of knowledge, i.e., the storage, transmission, and generation of knowledge. Knowledge is the result of the process of information management.

Knowledge and scientific information are of enormous importance in the global information society (European Information Society, 2005), through: supporting innovation, promoting economic development, making decisions in an efficient and transparent way, especially at government level and especially for the fields of education and training.

In order to move towards the construction of the knowledge society, it is necessary to reduce the digital divide, which accentuates disparities in development, excluding groups and even countries, from the benefit of information and knowledge. The human capacity to assimilate and develop these innovations and services can change the paradigm of achieving the impossible for the future of man-made artificial intelligence.

The creation of the European information society cannot be achieved only by adopting decisions and action plans of decision-makers at EU or Member State level, an essential role being played by the final beneficiaries of ICT, i.e., economic actors-companies, consumers, citizens. It is necessary to understand the benefits and the risks involved in developing new technologies, as well as how ICTs can influence their daily lives. While decision-makers have a duty to explain the new model of society and to take into account the suggestions and needs of the beneficiaries in the development of information society policies.

The EU institutions, in particular the European Commission, through its programs, take on the role of coordinator and catalyst for investment in the European Information Society. Coordination is mainly achieved by stimulating cooperation at the European level in order to avoid duplication of funded projects with the same result.

2. History of Computer Applications for European Funds

Computer applications designed to manage European funds have been developed as a necessary measure to increase the absorption of European funds, by streamlining the management of document flows, using capabilities of computer applications and new technologies, as a computing technique, thus succeeding, first notable steps in the process of continuous computerization of the central public administration.

In the 2007-2013 programming period, at the level of 2010, the management of IT applications for European funds was carried out in a decentralized manner, each operational program having its own form of IT organization, which also included an IT application with program-specific features. POSDRU was a pioneer in the electronic submission of projects.

By means of a computer application, the excessive bureaucracy was reduced, eliminating the submission of hundreds of documents related to eligible projects and expenses. In the relationship between the project beneficiary and the Managing Authority, an electronic communication is established that will streamline the absorption process, but not without encountering difficulties or blocking stages in the evolution process, thus replacing thousands of deposited bookshelves with electronically uploaded files in an account for each project.

These security measures were initiated as a result of counteracting cyber incidents, consisting of cyber attacks on calls for calls / submissions of European projects through the computer application – by electronic mechanisms (bots) for automatic completion of project content, violating thus the established rules of deposit and thus not respecting the principle established for the contracting phase – first come – first served. Simultaneous submission of projects is a violation of applicable law, but also a form of cyber-fraud, which is why we tried to exploit the vulnerabilities of open source technology used by the application – PostgreSQL.

Noting at the level of the institution, the emergence of the need for cyber security, by securing the application, starting from the stage of transferring the hosting location of computer equipment to a more secure data center specialized in the field.

These IT events created the premises for the transfer of the development of IT services and applications for European funds from the private sector of expertise by contracting on the basis of public tenders, in the public environment of interinstitutional cooperation with the related specifics, based on protocol relations established by law.

The management of the equipment that stores and manages information about the submission, contracting, and implementation of projects financed from European funds outlines a character of strategic objective, of national importance manifested in this way through the well-defined collaboration between the institutions involved.

In order to develop and host computer applications, cooperation agreements will be defined with the autonomous institutions that have attributions in the field of information security in Romania.

Decisive transparency in the management process of the submission of projects related to European funds, such as evaluation, contracting, and their implementation, will always be much better, in electronic form, implicitly requiring a high degree of protection and cyber security; only in this way will be reduced drastically and beneficial the current high degree of excessive bureaucratization in public administration. Transforming governance into an efficient, automated activity, in which the result obtained prevails, especially in a sensitive area and with complex implications such as that of European funds.

The critical IT infrastructure of national importance, dedicated to applications with the role of managing European funds, is becoming more and more at the same time a topic of interest for possible cyber attacks, especially since 2016 when the attention of some organizations began to focus on government cyberspace. .

That is why, at the ministerial level, all the necessary resources have been concentrated, creating the premises for strategies to prevent and combat any cyber attacks, which could jeopardize the integrity of information such as European funds, which have an impact on the country's economy, causing damage on the possible interests of the country, stability, and development.

Thus, through financing programs, the guidelines were established in the future developments of infrastructure protection through the acquisition of specific security equipment. With the considerable contribution of state institutions working in the field of cyber security, as well as through sources of external funding from European funds, it was possible to develop a national system that includes all state institutions, aiming to achieve prevention and protection against cyber threats.

3. Literature Review

Security is a priority; through specific European programs, the capacity of operational cooperation is strengthened, with a desire for consensus on the values that underpin the EU's internal security.

Mutual trust and the exchange of information will increase the preventive nature of the actions of the authorities, thus establishing the Standing Committee on Operational Cooperation in Internal Security, at national and EU level (European Commission, 2021).

The system is a set of principles, rules, and forces which form an organized whole, which aims to put order in a field of theoretical thinking, regulating the classification of material in a field of science or making a practical activity work properly. The purpose is pursued by complying with a set of rules and values.

The state is outlined, as a way of ensuring the political existence, by the established order and the development of the community, the defense and guarantee of the territorial integrity as well as of its autonomy.

National security is that state of balance, legality, economic, social, and political stability which guarantees the existence and development of the sovereign, unitary, indivisible, and independent state, through order, rights, and civil liberties.

National security leads to the realization of constantly evolving values, guided by constitutional-democratic principles. The national interest becoming a fundamental thesis in the applied foreign policy.

Security policy is represented in the long-term organization and ensures security change and innovation.

Security strategies, thus succeeding in adopting measures that counteract threats that evade the state of security.

A strong nation is built on common norms and values, goals, and aspirations, of paramount importance to individual interests. Citizen protection is a vision, an integral and important part of the National Strategy for National Defense.

Information and communication technology have a complex impact not only on the economy and its efficiency, but also on all aspects of people's lives. For a reinvention of governance in the information society, the following concepts have been identified that should be met:

- increase the state's capacity to absorb European funds using new technologies;
- increase the capacity of government administrations in public policy, both at the national and European level;

- e-democracy – the internet can increase democratic participation in government, the citizen of the information society is active;
- the electronic citizen – the citizens of the new society / young people are attracted in the modern technological fields being the key actors of the future governments, the politics in the digital age is in continuous transformation;
- politics in electronic format – the manifestation of politics in digital form is becoming more visible through the significant increase of online election campaigns, the electronic state, and behavioural patterns;
- the electronic state – in the phenomenon of globalization fuelled by the digital integration of the markets of the new economy, it will be desired to rethink and redefine the concept of nation-state.

Thus, increasing the chance of creativity and innovation by profoundly transforming the behaviours and profiles of citizens, from the reactive to the proactive.

4. Methodology

The research was carried out at the level of the Ministry of European Investment and Projects, with the main aim of creating scientific and technological excellence, as well as gaining advantages in the field of security and resilience of systems, services, and critical infrastructure of national importance, as well as increasing cyber security culture in the central public administration and among contract users or civil servants, with the possibility of establishing within the institutional organization, at least 3 posts with specific tasks in the cyber field, in direct collaboration with the Security structure of the Ministry and in cooperation agreement National Cyber-int.

The period included in the analysis activity is between the years 2014-2022, comprising two programming periods of non-reimbursable financing from European funds, facilitated by the European Commission.

The two projects carried out by the Cyber-int National Center, to ensure cyber security at national level, constituting a security umbrella, on the critical infrastructure of national interest, which will be reinvented by the digital transformation generated using emerging technologies, have produced a considerable evolution. Emerging technologies and the integration of Machine Learning or Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects, as a development measure through innovation, having positive effects including on the development of the national economy by increasing the absorption of European funds in a cyber secure environment.

The Ministry of Investment and European Projects regularly contracts the services of a certificate authority to allow user authentication and control access to various resources, especially in the application MySMIS2014, the first government IT application with this level of security implemented since 2016. They can be managed with HSM solutions and authentication tokens. Thus, an extra layer of Security can be added by implementing a Dual Factor Authenticator system. Authentication solutions, their management and monitoring, and even administrators who may have various access privileges may also be useful. Access to the ministry's resources will be secured and endpoints, mobile or immovable, must contain advanced antivirus protection technologies.

Virtual Private Network traffic tunneling and Internet access monitoring are performed through ICIN 54 MIPE – Cyber-int and STS. The encryption of the storage spaces that manage the used applications is performed at STS by securely hosting the equipment in the specially organized data center.

Critical systems must be completely separated from the rest of the network to create an area independent of attacks that may enter the organization. This is the area covered by the security equipment within ICIN 54 MIPE, which will benefit this year from an upgrade of capabilities, through refurbishment. Access should be granted only to people who use the system, and the connections will be encrypted by technologies such as data diodes, zero-trust, etc. Updates are performed through dedicated servers and well-defined policies to prevent access to the Internet Windows Server Update Services (WSUS).

5. Results and Discussions

The first step in the use of emerging technologies by integrating Machine Learning or Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects, was made within the projects financed from non-reimbursable funds, as a measure of development through innovation, of a critical infrastructure of national interest, by cooperation agreement with the National Authority in the field of Cyber-intelligence – Cyber-int National Center (Cloud Computing, Events, 2021). The security equipment used, offering advanced management capabilities, to realize the prevention, detection, and investigation of cyber security incidents, analyzing the risk generated by possible attacks, as well as automatic remediation of threats.

Raising awareness will be achieved by informing users, which is the first measure of protection against cyber-attacks. Human error can be avoided. This will close the way for hacker attacks, through good regular information, constant emails, courses, trainings, eliminating the possibility of further, much more serious problems, especially regarding information and data belonging to the state (National Cybersecurity Directorate, 2021).

In the near future, the public administration will evolve towards a different approach to the use of technologies, being transposed into future strategies, the need to use solutions in cloud, on-premises, or hybrid cloud environments, depending on available budgets and advantages or disadvantages. To streamline the activity or in the situation of permanent blocking of the procedures of new employees in the public administration, the subcontracting of services that allow access to these technologies is an efficient way to manage platforms, with a cost-benefit ratio for the benefit of the public institution, will relieve the care of the use of internal resources.

Public administration services can be streamlined using advanced information technology. The European Commission is trying to set its own example in this, through the procedures and tools it uses in its day-to-day work and in its links with

Member States administrations and its own decentralized agencies, which are marked by progress in computerization. The aim is to facilitate citizens' access to public information through new computer applications, as well as to achieve better communication between all levels of public administration across the Union, thanks to the high-speed connection.

The development of the European Information Society involves a considerable and ever-increasing financial effort, which cannot be fully assumed by the European Union and the governments of the Member States. Experience has shown that the private sector is best able to take risks in operating and developing new adaptable markets and has the capital to make such investments.

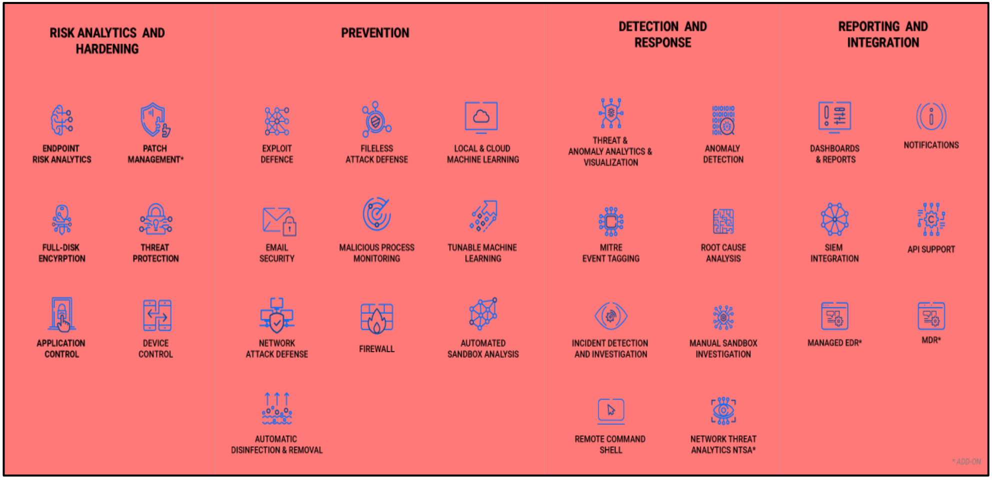
Integrating Machine Learning or Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects, could be seen in Table 1 below, while security levels could be observed in Figure 1.

Table 1. Integrating machine learning and artificial intelligence functionalities, at the level of the Ministry of European Investments and Projects

Implementation period	**Protected workstations**	**Increasing the degree of cyber protection**	**Automate responses to detected and remedied cyber attacks**	**Fixed vulnerabilities**	**Possible security risks**
2014-2017	250 to 450	200 Endpoints	About 50%	75%	25%
2020-2024	450 to 1700	1250 Endpoints	About 75%	99%	1%

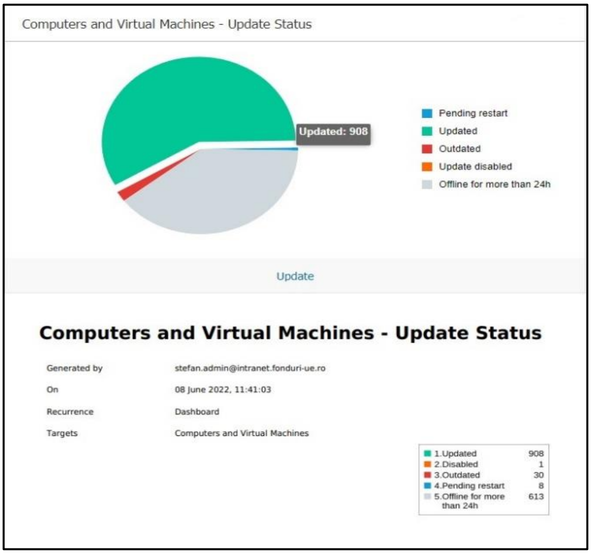
Source: Author' own research.

Figure 1. Security Layers



Source: www.bitdefender.com.

Figure 2. Centralized management of the antivirus solution update process (Bitdefender MIPE, 2022)


Computers and Virtual Machines - Update Status
Updated: 908
🟦 Pending restart
🟩 Updated
🟥 Outdated
🟧 Update disabled
⬜ Offline for more than 24h
Update

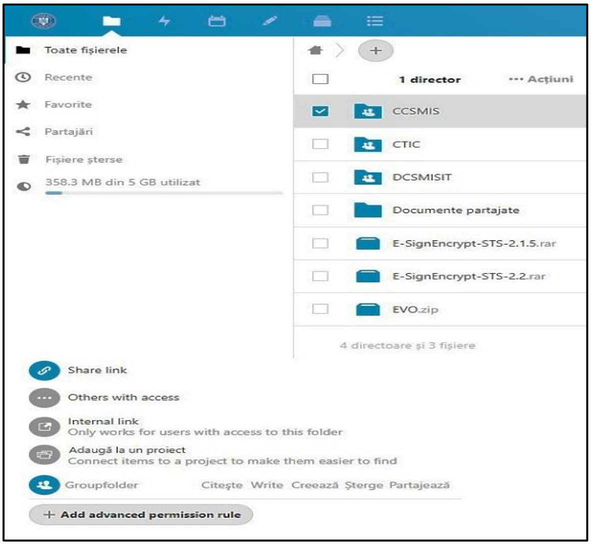
Computers and Virtual Machines - Update Status

Generated by	stefan.admin@intranet.fonduri-ue.ro
On	08 June 2022, 11:41:03
Recurrence	Dashboard
Targets	Computers and Virtual Machines

🟩 1.Updated	908
🟧 2.Disabled	1
🟥 3.Outdated	30
🟦 4.Pending restart	8
⬜ 5.Offline for more than 24h	613

Source: Central administration console – Bitdefender GravityZONE – Ministry of European Investments and Projects.

Figure 3. Cloud computing and services – private cloud solution (nextcloud MIPE, 2022)



Toate fișierele
Recente
Favorite
Partajări
Fișiere șterse
358.3 MB din 5 GB utilizat

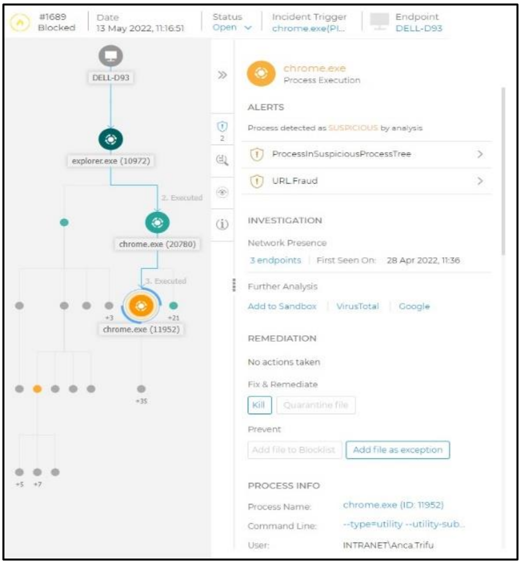
□ 1 director ··· Acțiuni
☑ CCSMIS
□ CTIC
□ DCSMISIT
□ Documente partajate
□ E-SignEncrypt-STS-2.1.5.rar
□ E-SignEncrypt-STS-2.2.rar
□ EVO.zip

4 directoare și 3 fișiere

Share link
Others with access
Internal link
Only works for users with access to this folder
Adaugă la un proiect
Connect items to a project to make them easier to find
Groupfolder Citește Write Creează Șterge Partajează
+ Add advanced permission rule

Source: Central administration console – Bitdefender GravityZONE – Ministry of European Investments and Projects.

Figure 4. Machine learning – cybersecurity incident investigation (Bitdefender MIPE, 2022).



#1689 Blocked | Date 13 May 2022, 11:16:51 | Status Open | Incident Trigger chrome.exe(Pl... | Endpoint DELL-D93

chrome.exe
Process Execution

ALERTS

Process detected as SUSPICIOUS by analysis

ProcessInSuspiciousProcessTree

URL.Fraud

INVESTIGATION

Network Presence

3 endpoints | First Seen On: 28 Apr 2022, 11:36

Further Analysis

Add to Sandbox | VirusTotal | Google

REMEDIATION

No actions taken

Fix & Remediate

Kill | Quarantine file

Prevent

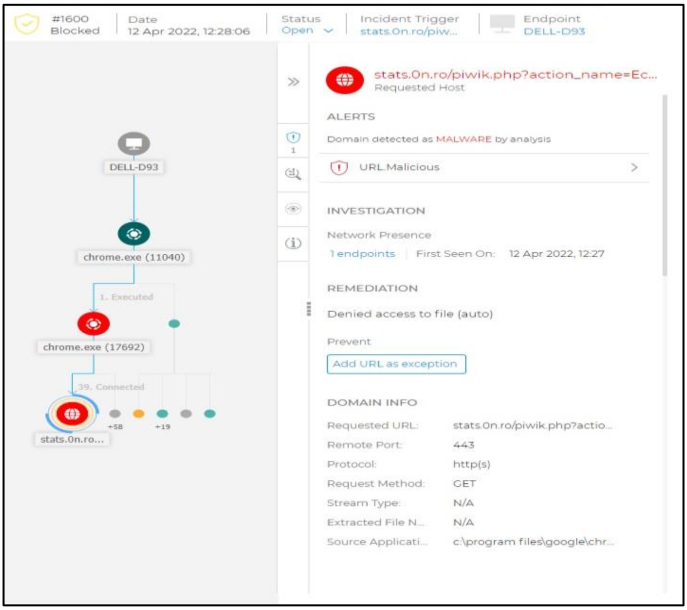
Add file to Blocklist | Add file as exception

PROCESS INFO

Process Name:	chrome.exe (ID: 11952)
Command Line:	--type=utility --utility-sub...
User:	INTRANET\Anca.Trifu

Source: Central administration console – Bitdefender GravityZONE – Ministry of European Investments and Projects.

Figure 5. Machine learning – automatically blocked cyber threat investigation (Bitdefender MIPE, 2022).



#1600 Blocked | Date 12 Apr 2022, 12:28:06 | Status Open | Incident Trigger stats.0n.ro/piw... | Endpoint DELL-D93

stats.0n.ro/piwik.php?action_name=Ec...
Requested Host

ALERTS

Domain detected as MALWARE by analysis

URL.Malicious

INVESTIGATION

Network Presence

1 endpoints | First Seen On: 12 Apr 2022, 12:27

REMEDIATION

Denied access to file (auto)

Prevent

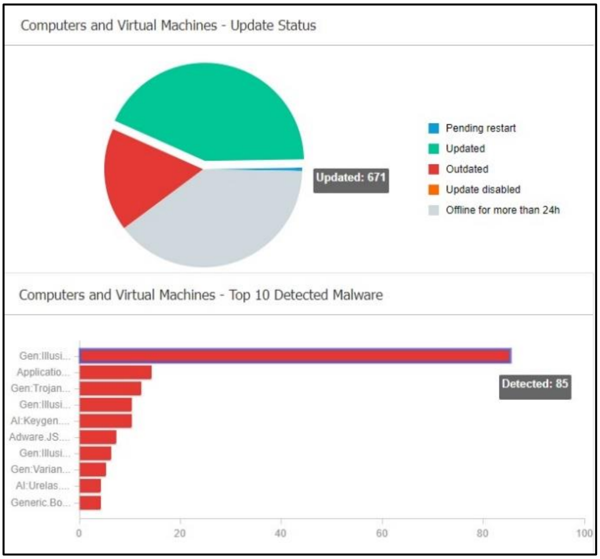
Add URL as exception

DOMAIN INFO

Requested URL:	stats.0n.ro/piwik.php?actio...
Remote Port:	443
Protocol:	http(s)
Request Method:	GET
Stream Type:	N/A
Extracted File N...	N/A
Source Applicati...	c:\program files\google\chr...

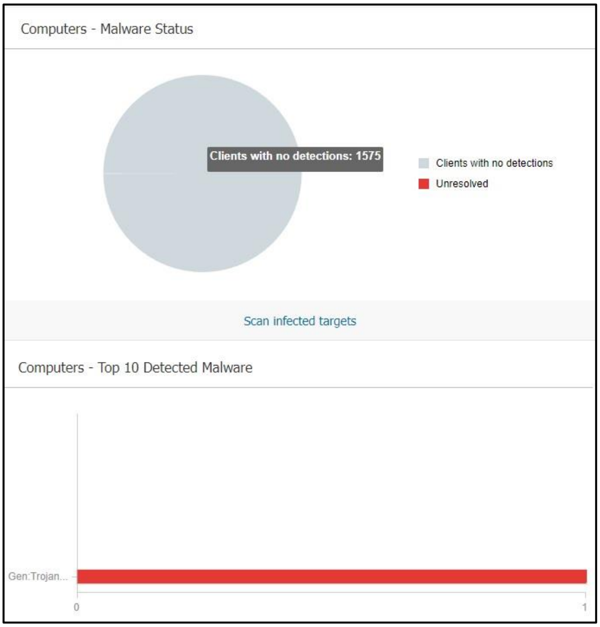
Source: Central administration console – Bitdefender GravityZONE – Ministry of European Investments and Projects.

Figure 6. Top 10 Vulnerabilities detected and blocked by the security solution (Bitdefender MIPE, 2022)



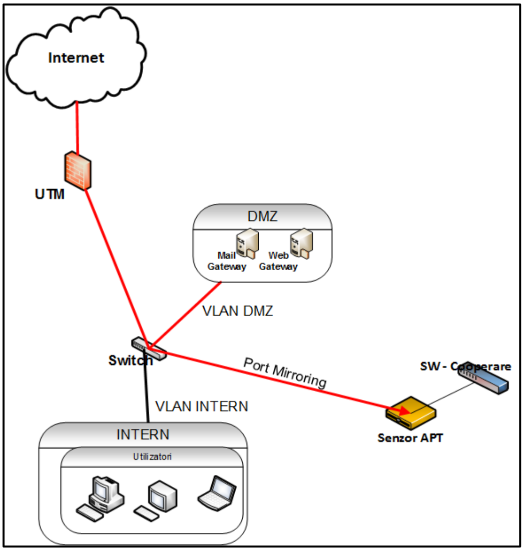
Source: Central administration console – Bitdefender GravityZONE – Ministry of European Investments and Projects.

Figure 7. Malware detection status in the MIPE 2022 internal network (Bitdefender MIPE, 2022)


Computers - Malware Status
Clients with no detections: 1575
Clients with no detections
Unresolved
Scan infected targets
Computers - Top 10 Detected Malware
Gen:Trojan...
0
1

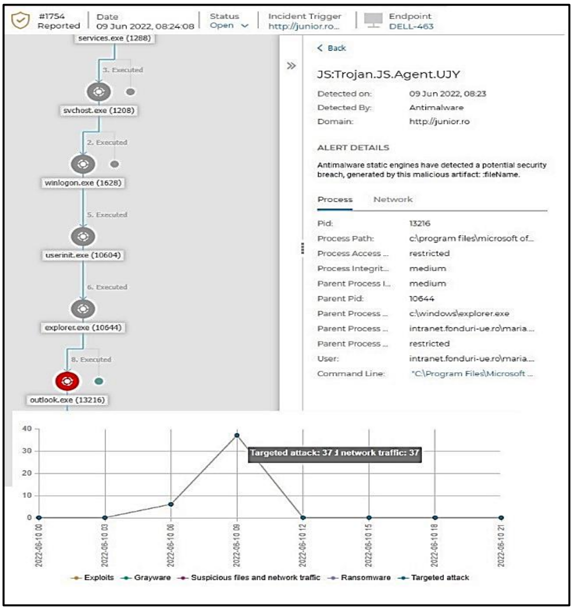
Source: Central administration console – Bitdefender GravityZONE – Ministry of European Investments and Projects.

Figure 8. Network scheme of cyber protection equipment related to critical infrastructure of national importance – ICIN – Țițeica



Source: The national system for the protection of IT/C infrastructures of national interest against threats from cyberspace.

Figure 9. Cyber attacks automatically countered according to the implemented security policies (Bitdefender MIPE, 2022).



#1754 Reported | Date 09 Jun 2022, 08:24:08 | Status Open | Incident Trigger http://junior.ro... | Endpoint DELL-463

< Back

JS:Trojan.JS.Agent.UJY

Detected on: 09 Jun 2022, 08:23
Detected By: Antimalware
Domain: http://junior.ro

ALERT DETAILS

Antimalware static engines have detected a potential security breach, generated by this malicious artifact: :fileName.

Process | Network

Pid: 13216
Process Path: c:\program files\microsoft of...
Process Access ... restricted
Process Integrit... medium
Parent Process I... medium
Parent Pid: 10644
Parent Process ... c:\windows\explorer.exe
Parent Process ... intranet.fonduri-ue.ro\maria....
Parent Process ... restricted
User: intranet.fonduri-ue.ro\maria....
Command Line: "C:\Program Files\Microsoft ...

Source: Central administration console – Bitdefender GravityZONE – Ministry of European Investments and Projects.

6. Conclusions

According to Article 3, letter f, L51 / 91, “harm to the interests of the country, as well as acts of destruction, degradation or rendering in a state of disuse blocking the absorption of European funds. In that case, according to Article 11 letter b – the direct beneficiary is the Minister of European Funds, who must be informed immediately in order to avoid such possible threats to the objectives of national strategic interest. (Information note of the Minister of European Funds 31.05.2018). As a dimension of information, counter-intelligence and security, the threat that consists in – blocking the absorption of European funds - falls within the provisions of Chapter 3 related to the National Strategy for National Defense 2015-2019.

The persistence in the vulnerability regarding the blockade of the absorption of European funds, being a real threat to the national security of Romania, due to the socio-economic implications and the obligations assumed as a member of the European Union, generates the need to capitalize the information for national security. European Funds, as well as by taking the necessary measures to address the shortcomings identified.

These data of national interest have an incidence in the current year – 2019, leading mainly to a non-fulfilment of the conditions established in the relationship with the European Commission, as an EU member state, of Romania.

As cyberattacks become more frequent, it is vital that organizations are equipped with the most effective tools and knowledge to prevent, detect and respond to cyber threats.

Thus, the identification and capitalization of these deficiencies, which constitute information for national security, will be done gradually, due to the degree of persistence manifested, as well as the permanent lack of sufficient and efficient resources, endowed with the necessary training to manage the computer system.

Therefore, it is necessary to create a global framework for security and trust in ICT. This strategic goal is aimed at creating scientific and technological excellence, as well as gaining advantages in terms of security and resilience of systems, services, and infrastructure, while meeting European privacy requirements (Regulation EU, 2016). The aim is to standardize networking and information security activities. The emphasis will be placed on ICT research in the field of public administration innovation, with a view to modernization and innovation, thus promoting an efficient type of governance, offering new services to citizens and economic agents, with the result of creating new public values.

Thus, making European citizenship a reality and providing support to citizens through innovative government services and active participation in decision-making. Everything happens thanks to a process called technology-based learning. The technology used efficiently, safely, with positive results for society, involves ensuring a high degree of security and awareness of the dangers of the virtual environment. Specialized security equipment is the specific technologies that ensure these activities without which the order and normality in electronic financial activity, especially in the institutional field, would be seriously endangered by attacks, intentionally aimed at the government's online environment, especially in the sensitive management of European funds.

Security solutions are needed, which bring real benefits to the institution once they are configured according to the needs of secure operation. Easy-to-use, intuitive management tools can optimize the time required to implement new policies, to make a correct monitoring and alerting. Also, the collaboration with the National Cyber-int Center offers stability and access to the necessary knowledge in the activity of implementing these systems for ensuring cyber security. Unified and integrated technologies offer a measurable advantage in results, benefiting from such consoles and tools adapted to the level of expertise, in accordance with the strategies built by the IT Security department. Cooperation with other institutions such as National Cyber-int Center, participation in seminars and conferences in the field, is an excellent tool for improvement, and especially a guide of good practices, assimilated to adopt the best decisions for the public institution.

The budget allocated to innovation in public administration will create and maintain such desirable stability, especially in critical areas, such as European funds. In industry and economics, the role of robotics and process automation will increase considerably, with changes related to technology bringing both benefits and vulnerabilities, especially in cyberspace. It will practically create a virtual parallel world, where the existence of the state, with everything it represents must be protected, so the environment will be safe and secure even for the individual. The consequences of competition in innovation produce major transformations, including in society, simplifying the complex life of modern man in the information society. Thus, constituting a national interest for the Government Strategy, the areas such as attracting European funds and ensuring cyber security, aiming at modernizing, and computerizing the public administration in Romania (ENISA, 2021).

Thus, it is necessary to create a global framework of security and trust in ICT, with an expansionist tendency toward process automation to achieve maximum efficiency. This strategic goal is aimed at creating scientific and technological excellence, as well as gaining advantages in terms of security and resilience of systems, services, and critical infrastructure of national importance, as well as increasing the degree of cyber security culture in the central public administration, with the possibility of establishing within the institutional organization, at least 3 positions with specific attributions in the cybernetic field, in direct collaboration with the Security Structure of the Ministry in question and in cooperation agreement with the National Authority in the field of Cyber-intelligence, following designation by SCND- Supreme Council of National Defense - Romanian Service of Information, through the National Cyber-int Center.

In this way, an important stage in inter-institutional collaboration will be fulfilled, to achieve the fundamental objectives of the country strategy, the field of funds becoming critical infrastructure through the implications inherent in the national economy, affecting all plans of society, from financial to economic, social-educational, up to the political one, with all the necessary risks assumed. But most importantly, the efficient management of infrastructure and applications for European funds, having a special importance in the much-needed process of increasing the quality of life, representing the first step towards knowledge, innovation, and development.

References

[1] Bitdefender MIPE (2022). Central administration console – Bitdefender GravityZONE – Ministry of European Investments and Projects.

[2] Cloud Computing, Events (2021). October 6, 2021 at 11:19 am. *Cloud Conference brings new technologies to the forefront - (clubitc),* https://www.clubitc.ro/2021/10/06/conferinta-de-cloud-aduce-in-prim-plan-noile-tehnologii/.

[3] European Commission (2022). *Jobs and the economy during the COVID-19 pandemic* https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/jobs-and-economy-during-coronavirus-pandemic_ro.

[4] European Commission – Brussels, 3.3. (2021). *One year since the outbreak of COVID-19: fiscal policy response*, https://ec.europa.eu/info/files/one-year-outbreak-covid-19-fiscal-policy-response_en.

[5] European Information Society (2005). Publisher: Foundation for European Studies.

[6] Ministry of European Investments and Projects.

[7] National Cybersecurity Directorate (DNSC) (2021). September 30 - *European Cybersecurity Month – ECSM*, https://cert.ro/citeste/comunicat-luna-europeana-a-securitatii-cibernetice-2021.

[8] Regulation EU (2016). / 679 – *on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC* (General Data Protection Regulation).

[9] The European Union Agency for Cybersecurity (ENISA) (2021). September 13 - *Methodology for a Sectoral Cybersecurity Assessment*, https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment.

[10] The European Union Agency for Cybersecurity (ENISA) (2020). April 15 - *Advancing Software Security in the EU,* https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework.

[11] The national system for the protection of IT/C infrastructures of national interest against threats from cyberspace, ICIN – Țițeica.

[12] www.bitdefender.com.