TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 65, Issue Special IV, December, 2022

# DRAFTING A SECURITY CONCEPT FOR MIDDLEWARE INTEGRATION ENVIRONMENTS IN THE MANUFACTURING ENTERPRISE

**Dorin-Vasile DEAC-ȘUTEU, Alina Bianca POP, Aurel Mihail ȚIȚU**

***Abstract:*** *Enterprise application security is a system of people, procedures, and technologies that ensures the security of an application by continuously measuring observable threats to all application assets. This framework protects an application by preventing unauthorized access to sensitive information. A first step in determining the security posture of applications used by the organization is to conduct an intelligence-gathering mission to understand how people work within the organization, what processes they use, and what technologies support the people and processes. This step should enable the development of a model, and IT management should develop a list of monitoring and performance indicators, develop the methodology for monitoring these indicators, and present the interpretation of the information to the organization's management to make timely decisions about possible risks.*
***Key words:*** *IT technology, security, processes, vulnerability detection, public sector.*

## 1. INTRODUCTION

Since the rapid growth of digital information and its increasing importance, conditions are now ripe for new information security risks to emerge. These risks include the following: leakage, theft, loss, misrepresentation, falsification, destruction, copying and blocking of information; as a result, the organization suffers damage.

Today, information risk assessment and management techniques are used as a methodical framework for information protection.

This study proposes a comparative approach to cloud and local security concepts, information risk analysis and the use of SWOT analysis techniques to identify and analyze risks in knowledge-based organizations.

The study is part of a broader research on manufacturing solutions for equipment and machinery used for activities carried out in the public sector, in particular for the provision of services of local and area interest (e.g., snow clearing in extreme conditions), the use of information technology for command, control, tracking, and equipping and interfacing with smart devices.

As providing the necessary Hardware &Software IT infrastructure for these processes requires major investments, cloud solutions are an alternative to consider. This development is already being addressed at government level, where several projects for cloud solutions are already underway. And security issues, in addition to data storage activities, are the most debated topics when talking about the cloud environments.

We intend, based on scientific sources, to identify issues such as internal weaknesses and external threats to defend against information privacy threats (privacy, accessibility and integrity breaches) and use external opportunities to develop them.

The use of a communication network offers several immediate benefits, including the sharing of tasks and responsibilities, data protection, information sharing and data transfer. If any of the network components fail, the network itself must continue to function as normal and the functions previously performed by the failing components must be taken over by other components. There is a need for tools to simplify network administration and maintenance, as the complexity and scale of network components will increase the level of

difficulty associated with these tasks. This aspect of the service is facilitated by the availability of remote network diagnostic and maintenance capabilities. A set of defined communication standards and formats for data representation and transfer is called protocols. These protocols are the basis for communications between equipment in a network that is both physically and logically coupled.

Cyber events are increasingly seen as a potential source of global risk and top the list of the most important business issues for 2019-2021 (Fig. 1.) [1].

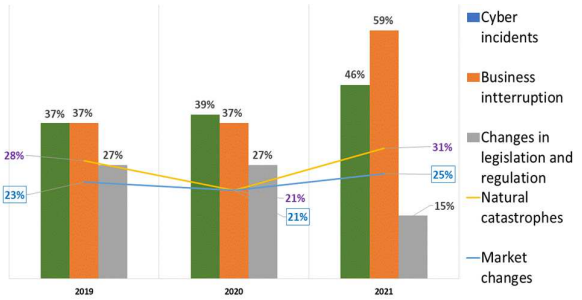


**Fig. 1.** Main threats to businesses [authors' conception]

The conclusions of the report [2] demonstrates that external occurrences such as DDoS assaults, phishing campaigns, and malware/ransomware account for most losses (85%) in the value of claims evaluated, followed by internal hostile conduct (9%), which is uncommon but can be expensive.

Especially nowadays, because of the Covid-19 pandemic, businesses now conduct their operations differently, and more employees are choosing to work from home, which has increased the risk of cyber disasters [3]. As a result, the security of communication networks is a priority and needs to be continuously improved [4].

## 2. CURRENT STATUS

Communicating information remotely has become important due to the increase in the number of smart devices and the fact that each of these devices stores information gathered from different sources. As a result, computer networks have emerged. Computers, laptops, printers, phones, personal digital assistants, and other electronic devices can now be integrated

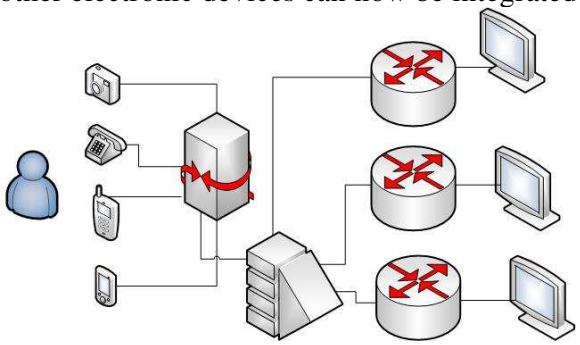

**Fig. 2.** Network component clients to businesses [authors' conception]

into a communication network due to the expansion of the types of devices that can be connected to a network (Fig. 2.).

The security of a computer network can be compromised by natural disasters, technological failure, human error, and fraud. The first three types of threats are unintentional. But according to the latest analysis [5], half of the incident costs are attributed to deliberate destruction, a quarter to accidents, and a quarter to human error (Fig. 3.).

As most companies have embraced remote working, access control has become sophisticated, needing on-premise and cloud solutions to provide access to internal resources regardless of location. Work is hampered when employees don't have the right level of access to view and/or change papers, slides, and other files on a network drive. Users soon need a system administrator to assign suitable credentials.

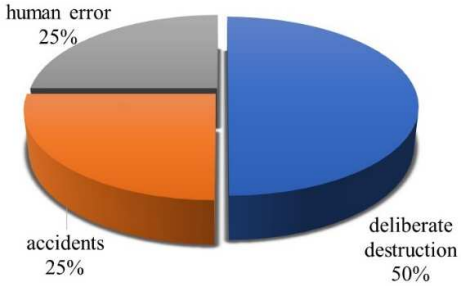


**Fig. 3.** The True Cost of Cybersecurity Incidents [authors' conception] [5]

In information security, this is letting a user to enter a network with a username and password and access the data, computers, equipment, or software they need to complete

their job. Comparative analysis of the most relevant aspects of how access to resources is granted are noted in figure 4.

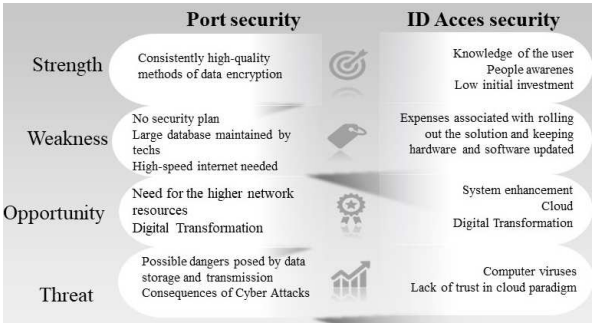


**Fig. 4.** SWOT analysis for possible ID access [authors' conception]

Security standards recommend making frequent backups of data, mirrored disks, regardless of the physical medium through which it is made or the details of the information transmission network [6]. Thus, communications security is crucial for confidential financial, banking, military, government, and other confidential information [4]. Vulnerabilities in networks and communication systems can cause substantial losses. These concerns require a detailed investigation of risks and vulnerabilities to find security solutions, strategies, methodologies, and procedures [7].

Depending on the importance of the information, the public or private nature of the communication network, and the terminal used certain security policies are developed which, based on security analysis, best express the principles underlying a given security strategy, implemented through various specific measures, with appropriate techniques and protocols [8]. For a complete security study, all internal and external, hardware and software, human and mechanical elements, types of networks, transmission topologies and settings, communication protocols, applications operated, security threats, and costs must be addressed.

All layers have network vulnerabilities, requiring layer- and network-specific security measures. This shows that two components of network security need to be prioritized:

- The integrity and physical or logical availability of the network, despite hardware or software failures, interruptions, or attempts to interrupt communications;
- Individuals have the right to control what information about them is stored in files or databases on the network and who has access to it. The network is responsible for preventing illegal attempts to steal or manipulate information.

Cyber security attacks rarely involve a single computer. Most threat actors today target networks and large enterprises, not personal computers. Specific security weaknesses have been identified in both (wired and wireless environments). When attackers can gain access to the network they want to attack, their task becomes relatively simple. Ethernet LANs are extremely vulnerable to attack because the switch ports are left open by default. Layer 2 Dos attacks and address spoofing are examples of possible attacks.

The network is obviously secure if the administrator has control over it. The user can use the port security function to gain full control over the switch ports.

A port can be secured in two steps:

- Set a maximum for the number of MAC addresses that can be learned from a single switch port; if more than the maximum can be learned from a single port, the required measures will be implemented;
- If unauthorized access is discovered, the user is required to either stop all communication by selecting one of the two options provided or generate a log message that clearly identifies the location of the intrusion.

## 2.1 Zero trust security

In 2010, John Kindervag of Forrester Research released the Zero Trust concept for security architecture [9]. The basic principle of Zero Trust is that to properly assess cyber risk, we must first assume that our internal network has already been infiltrated, but we are unaware of this. This assumption leads us to the conclusion that internal connections must first be validated before they can be trusted.

The phrase "Zero Trust" is based on the concept that trust is a vulnerability, therefore security should be characterized by "Never trust, always verify".

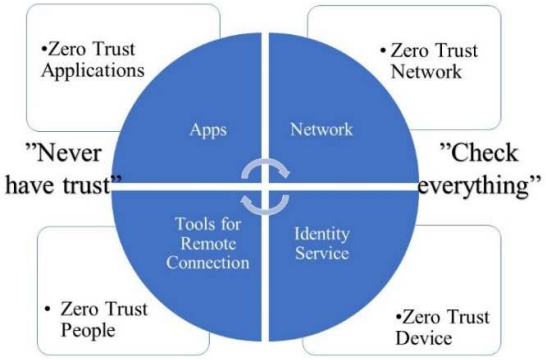


**Fig. 5.** Zero Trust Network guideline [authors' conception]

Mobile technologies and cloud migration are making it harder to define a company's network boundary. SaaS apps, IaaS, remote users, IoT devices, and more regularly send data, giving potential attackers more entry points to critical information.

Zero Trust principles (Fig. 5.), enhance an organization's security by eliminating perimeter-based defenses and relying on strict authentication at each access point. No device, user, system, or workload is trusted by default within a Zero Trust security architecture, regardless of location.

Thus, the conventional way of thinking about trust and distrust is redefined by the special approach of Zero Trust.

Both the ability to react quickly and the ability to limit the consequences of a security breach are essential qualities that a security system should possess. This makes it possible to use a strategy known as 'defense in depth, which works to eliminate potential breaches for a single destructive attack.

Collaboration between cybersecurity specialists, management, and administration /operations teams are recommended to support a successful Zero Trust architecture.

## 2.2 Costs associated with maintaining security

There is widespread agreement among industry professionals that the question is not "if" a business will fall victim to a breach or cybersecurity attack, but rather "when".

Cyber security incidents are costly (Fig. 6.). In the 2020 Cost of a Data Breach study published by IBM [10] the global average cost of cybersecurity breaches in the United States

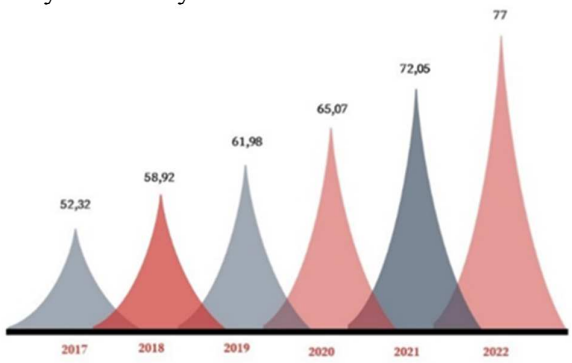


**Fig. 6.** Cost of information security services from 2017 to 2022, USD bn [11]

between August 2019 and April 2020 was $8,640,000.

According to IDC's analysis of global network security spending [12] global investment in network security hardware, software and services was $143.5 billion in 2021. The total amount spent globally on network security will grow at a compound annual growth rate (CAGR) of 9.41% between 2019 and 2024, ultimately reaching $189.2 billion [12].

Cyber security has taken on an even greater level of importance, with small and medium-sized organizations at particularly high risk of data breaches and cyber-attacks during the pandemic [13].

"Covid-19 could influence remote working". Before the pandemic, 5% of full-time office workers worked from home. The new normal could be 20-30%, depending on jobs and sectors. Employment will not depend so much on location [16]. Post-pandemic, there is a growing interest in "remote", permanent work, (Fig. 7.) [17].

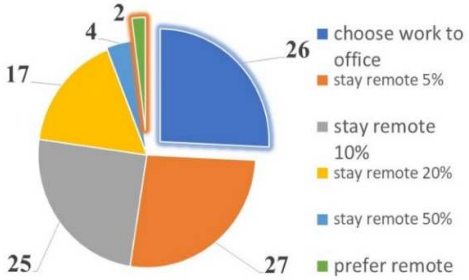


**Fig. 7.** Share of office vs. remote work [authors' conception]

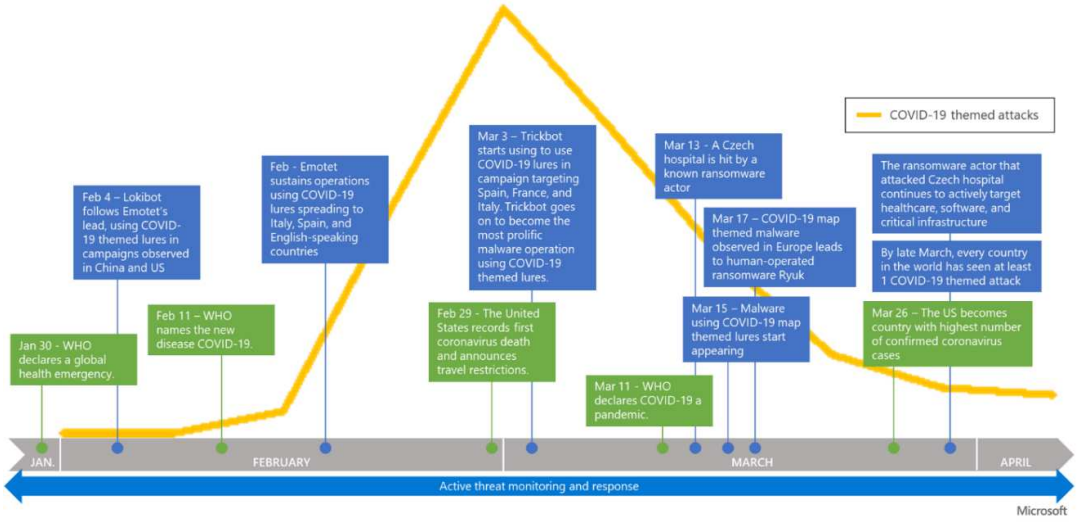


**Fig. 8.** Trend of COVID-19-themed attacks [15]

This is because more people now work from home, making it impossible for organizations to apply uniform security practices and difficult or impossible to know exactly what users are doing (Fig. 8.).

The COVID-19 outbreak has hastened the shift to "work-from-home" arrangements, making the workplace more susceptible to cyber threats. The number of COVID-19-themed internet and email attacks and Remote Desktop Protocol (RDP) attacks continues to rise.

To prevent the spread of COVID-19, several companies have been forced to implement rules on working from home (Fig. 8). However, remote working increases the risk of cyber

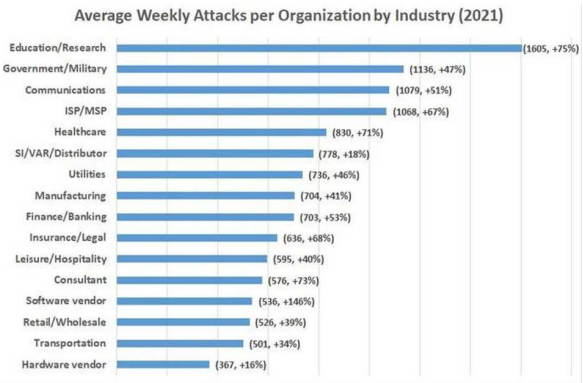


**Fig. 9.** Cyber-attacks per organization by Industry in 2021 [14]

including intrusions, man-in-the-middle attacks, and spear phishing [15].

After the COVID-19 epidemic, internet penetration and smartphone use increased spear phishing attempts, (Fig. 9), which require endpoint and virtual private network security measures and prevention procedures to prevent them [15].

Permanent remote hiring could complement firms' cost-cutting strategies [17], to counter potential business disruption caused by COVID-19 [18].

## 3. HUB SECURITY CONCEPT FOR INTEGRATED IT SERVICES

"IT Security" Information is essential to the functioning of any organization. This involves documents, personal information, or intellectual property that must be protected from external access. IT security is the process of protecting both the information and the technologies used to store it, i.e., both physical and cyber security.

Cybersecurity protects all information held in cyberspace and accessible via the internet or system network. Cyber security is responsible for detecting malicious websites, links, email attachments, and other media used for hacking, phishing, theft, infiltration, and network damage.

National, regional, and municipal authorities define, organize, finance, and monitor integrated public services. The Internal Market, Competition and State Aid, Free Movement, Social Policy, Transport, Environmental Health, Consumer Policy, Trans-European Networks,

Industry, Research into Economic and Social Cohesion, Trade and Development Cooperation, And Taxation Are All Areas in Which the European Union Is Competent. The Treaty gives the Community numerous powers and obligations to ensure that all EU citizens have access to high-quality services of general interest [19].

Social assistance and social protection are national, regional, and local responsibilities. It is well known that communities generate collaboration and coordination. Modernizing social security systems is a key objective for the European Commission.

There are three categories of services of general interest in terms of Community activity and Member State participation [19]:

- Network operator services such as telecommunications, postal services, electricity, natural gas, and transport.
- Other economic services, such as waste management, water supply, and public broadcasting, are not subject to full EU regulation.

Today, business-to-business (B2B), and organization-to-organization connectivity is becoming increasingly prevalent. Although B2B integration was originally used by IT organizations, as the use of IT devices has grown and organizations have started to digitize, B2B integration has become mainly about merging, automating, and optimizing business processes that reach outside the company firewall. While these processes differ greatly from organization to organization, one thing they all have in common is that integrating these external business processes gives the organization a sustainable competitive advantage.

Examples of such benefits include real-time visibility, increased automation, increased inventory efficiency, and improved satisfaction levels among customers. Organizations that contribute to the provision of an integrated service of local and regional interest are targeted in the circumstances examined in this study.

Organizations have found that having good software solutions isn't enough in times of healthcare constraints. They can use the most feature-rich software within their own firewall (or in the cloud) but cannot effectively manage end-to-end public service delivery without a proper B2B connection and associated capabilities. Although B2B integration got its start when large companies demanded a way to collect business information, it swiftly progressed to the adoption of Electronic Data Interchange (EDI) standards and, later, other, more recent technologies such as XML, JSON, and others. Currently, it is a default requirement that every new program provides an API solution that allows integration with other applications. This would ensure that there is transparency and continuity in the provision of information in the public space.

The primary connections will be made with GPS systems (Fig. 10) that are responsible for managing information pertinent to the organization's operations. These GPS systems include Google Map, Google Street, Apple Maps, and Waze, among others.

These systems will provide real-time data on traffic, congestion, or GPS location, i.e., selection and mapping of information that is of interest to the user, such as an example of this would be an example of:

- Information on work that is intended to be done by diverse business agents (roads, gas, power), as well as information on unplanned interventions;
- Data transferred from the platforms of specialist providers, depending on the selection of user-defined vehicle characteristics, the presence or implementation schedule of new electric vehicle filling stations (cars, motorcycles, and scooters), availability check, and reservation;

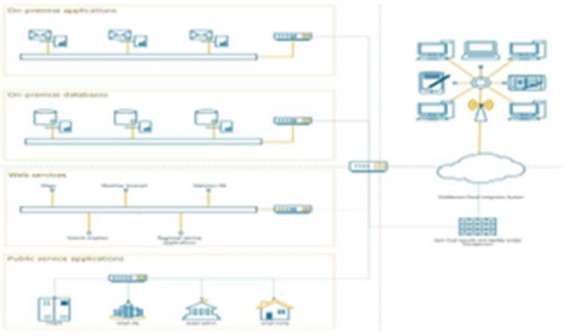

**Fig. 10.** HUB concept for integrated services of local and regional interest [authors' conception] [20]

- Data on the existence of health limitations, a history of collected information, and a list of travel advice;
- Information on the conditions for participating in hobbies, suggestions for chances to go trekking or view animals, or information on the likelihood of traversing potentially hazardous places.

## 4. CONCLUSIONS

Once linked to the internet, any device, in any situation, is vulnerable to cyber security dangers, so this action is important. Cybercrime can move from a single device to a whole organization's network via non-tangible techniques. If an infected personal device is connected to a company's network or computer systems, it can infect other systems, increasing cyber-attack risk.

Best practice guidelines for strengthening security begin with tight authentication and permission of each resource. Rather than depending on implicit trust, this often requires multi-factor authentication.

- measuring and monitoring the security of all resources to maintain data integrity and limit cyber-attacks;
- regular collection of data from different sources: network infrastructure and communications;
- security must be assessed for each piece of hardware connected to a network;
- the highest level of security will be required for all communications, regardless of network location, as proximity does not imply trust.

Users will request per-session access to resources with limited privileges. Access and information resources must be safeguarded by a dynamic, open, and flexible security policy.

With cyber threats within and outside the security perimeter, Zero Trust security is necessary to secure company data everywhere.

Spending more on cybersecurity or deploying the most popular security solution is not the most proactive option. The frequency and severity of historical attacks, breaches, and damage can be studied.

After-the-fact cybersecurity spending is more expensive than planning before.

The study is part of a larger research project on ideas for modernizing public sector equipment and machinery, especially for local and area services (e.g., snow removal in difficult conditions), and equipping and interfacing with smart devices.

Cloud solutions offer an alternative to investing in hardware and software infrastructure for these operations. Several cloud-based government projects are already underway. Cloud security, along with data storage, is a hotly disputed topic.

## 5. REFERENCES

[1] Barometer, A. R. *Global risks*, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, January 2020

[2] Global, A. *Cyber risk trends 2020*, https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2020.html, 2020

[3] Shevchenkoa, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Negodenko, O. *Cybersecurity Providing in Information and Telecommunication Systems*, Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021) Kyiv, 2021, http://ceur-ws.org/Vol-2923/ paper 34.pdf, January 2021

[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*, 16 April 2018, https://doi.org/10.6028/NIST.CSWP.04162018

[5] Pelzer, L.M., *The True Cost of Cybersecurity Incidents: The Problem*, https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem, 2021

[6] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of network and information security within the Union*, https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 2016

[7] C.I.O. Council, *CIO Handbook*, https://www.cio.gov/cio-handbook/, 2021

[8] I. 27001, *Information technology - Security techniques - Information security management systems*, https://www.iso.org/standard/54534.html, July 2022

[9] C. Point, *Check Point Enterprise Security Framework, CESF,* https://www.checkpoint.com/downloads/products/checkpoint-enterprise-security-framework-whitepaper.pdf, 2020
[10] IBM, *Cost of a Data Breach Report 2020*
[11] Sava, J.A. *Worldwide information security services spending from 2017 to 2022*, https://www.statista.com/statistics/217362/worldwide-it-security-spending-since-2010/, April 2022
[12] IDC, *IDC's Worldwide Security Spending Guide Taxonomy, 2021: Release V1, 2021*, https://recordtrend.com/network-security/it-is-predicted-that-the-global-investment-in-network-security-related-hardware-software-and-services-will-reach-143-5-billion-us-dollars-in-2021-from-idc/, February 2021
[13] Verizon, *Data Breach Investigations Report*, https://www.verizon.com/business/ resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf, 2022
[14] Brooks, C. *Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know*, https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=58310b837864, June 2022
[15] M. 3. D. T. I. Team, *Exploiting a crisis: How cybercriminals behaved during the outbreak*, June 2020
[16] Levanon, G., *Remote Work: The Biggest Legacy of Covid-19*, https://www.forbes.com/sites/gadlevanon/2020/11/23/remote-work-the-biggest-legacy-of-covid-19/?sh=2e182dfd7f59, November 2020
[17] Arligton, V., *Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently*, https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2, April 2020
[18] Dinha, F., *The Hidden Cost of Remote Work*, https://www.forbes.com/sites/forbestechcouncil/2021/03/30/the-hidden-cost-of-remote-work/?sh=639e2fd66947, March 2021
[19] C. CEMR, *European Charter of Services of General Interest at Local and Regional Level*, https://www.ccre.org/img/uploads/piecesjointe/filename/charter_sgi_RO.pdf, March 2009
[20] Deac-Suteu, D.-V., Titu, M.-A., Stanciu, A., *The Reference Architecture of An Integrated Service Middleware Hub in The Environment of Knowledge-Based Organizations*, ECAI, Cluj Napoca, 2021.
[21] Microsoft, *Evolving Zero Trus*, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT. November 2021
[22] Puiu A. *Playtech - How to find out all devices connected to your wireless network*, https://playtech.ro/2017/cum-afli-toate-dispozitivele-conectate-la-reteaua-wireless/, March 2017

## DEFINIREA UNUI CONCEPT DE SECURITATE PENTRU MEDIILE DE INTEGRARE MIDDLEWARE ÎN SECTORUL PUBLIC AL UE

*Securitatea aplicațiilor de întreprindere este un „sistem de resursă umană”, proceduri și tehnologii care asigură securitatea unei aplicații prin măsurarea continuă a amenințărilor observabile la adresa tuturor activelor aplicației. Acest cadru protejează o aplicație prin prevenirea accesului neautorizat la informații sensibile. Un prim pas în determinarea poziției de securitate a aplicațiilor utilizate de organizație este efectuarea unei misiuni de culegere de informații cu scopul de a înțelege modul în care angajații lucrează în cadrul organizației, ce procese utilizează și ce tehnologii sprijină utilizatorii și procesele. Acest pas ar trebui să permită dezvoltarea unui model, iar conducerea IT ar trebui să elaboreze o listă de indicatori de monitorizare și de performanță, să dezvolte metodologia de monitorizare a acestor indicatori și să prezinte interpretarea informațiilor conducerii organizației pentru a lua decizii în timp util cu privire la posibilele riscuri.*

**Dorin-Vasile DEAC-ȘUTEU,** Sc.D. Student**,** University POLITEHNICA of Bucharest, Faculty of Industrial Engineering and Robotics, 313 Splaiul Independenței, 6th District, Bucharest, Romania, E-mail: fam.deac@gmail.com,
**Alina Bianca POP,** "Technical University of Cluj-Napoca", 62A Victor Babeș Street, 430083, Baia Mare, Romania, bianca.bontiu@gmail.com,
**Aurel Mihail ȚÎȚU,** Professor, Lucian Blaga University of Sibiu, 10 Victoriei Street, Sibiu, Romania, E-mail: mihail.titu@ulbsibiu.ro