PROJECT
Multi-tenant cybersecurity operations centre designed
as an open cloud service with machine learning elements

V21 – Available online awareness-raising materials and outputs

KPB7 – popularization activities
type educational materials
month of submission – M22

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

1 Introduction 4

2 Sub-objectives of the popularization activities 4

2.1 Sharing outputs and information through a web platform 4

2.2 Informing the lay public about the importance of cybersecurity and the potential of the INNOSOC project 5

2.3 Popularizing the topic and increasing digital literacy among students 5

3 Description of the segments for popularization activities 6

3.1 Professional public 6

3.2 General/lay public 6

3.3 Potential customers 6

3.4 Secondary school students 7

3.5 University students 7

4 Outreach methods and communication tools 7

4.1 Website 7
4.1.1 Activities carried out 8

4.2 Social networks 18
4.2.1 Basis of the communication strategy 18
4.2.2 Main communication tools 18
4.2.3 Content plan 19
4.2.4 Activities carried out 20

4.3 Popularization texts 37
4.3.1 Activities carried out 38

4.4 Audiovisual content 44
4.4.1 Activities carried out 45

4.5 Promotional materials 47
4.5.1 Activities carried out 48

5 List of sources 50

6 Annexes 53

Annex 1 – Article: Partners' meeting 15/7/2025 53

Annex 2 – Article: Foundations of the INNOSOC project: Interview with Ing. Michal Papučík 53

Annex 3 – Article: Interview with prof. Ing. Pavol Segeč, PhD.: Cybersecurity is no longer just a topic for large companies 54

Annex 4 – Article: Student event FRIčkovica – 8 October 55

Annex 5 – Announcement of the INNOSOC symposium 55

Annex 6 – Article announcing the winner of the iPad competition 55

Annex 7 – Article: Presentation of the INNOSOC project at the student breakfast 55

Annex 8 – Article on the presentation of the project at the Faculty of Applied Informatics, Tomas Bata University in Zlín 55

Annex 9 – Article on the presentation of the INNOSOC project at the Jozef Murgaš Secondary Technical School in Banská Bystrica 56

Annex 10 – Article: Cybersecurity: Basics and tips on how to protect yourself against online threats 56

Annex 11 – Article: Security Operations Center: what it is and how it protects your company? 58

Annex 12 – Article: Get to know the most common internet threats for young people: Options for prevention and protection..... 59

Annex 13 – Article: What the cloud is and what it is used for: Basic types and advantages of cloud storage 61

Annex 14 – Article: Computer security and data protection – principles and practical examples 62

Annex 15 – Interview with Ing. Michal Papučík..... 64

Annex 16 – Interview with prof. Ing. Pavol Segeč, PhD. 66

1 Introduction

The document contains a partially developed version of the proposed strategy for implementing popularization activities. The main objective of the strategy is to build awareness of the INNOSOC project as a European technology project of significance for cybersecurity and digital sovereignty. The project is to be perceived as an innovative, trustworthy and open tool for the prevention and management of cyber threats.

Emphasis will be placed on education, community interaction and support for the adoption of the technology not only among experts but also among young talents and the general public.

The expected target audience of the popularization activities can be divided into five basic segments:

- professional public,
- general/lay public,
- potential customers,
- secondary school students,
- university students.

Each of these segments is specific and requires an individual mix of communication channels for spreading awareness, as well as a specific communication message.

2 Partial objectives of the popularization activities

Given the wide range of targeted segments and, in particular, the different communication messages to be communicated to them, several sub-objectives of the popularization activities were defined.

2.1 Sharing outputs and information via a web platform

One of the main objectives of the popularization activities within the INNOSOC project is to build an open digital platform that will serve as a space for sharing the results, knowledge and outputs of the project. The information on the website will be intended for several segments. At the same time, however, it will be the core tool for sharing expert knowledge in communication with the professional public.

This platform will be publicly accessible and will give various target groups, from experts to laypeople, easy access to important information and materials. The project website will become the central place where final reports, technical documents, guides, methodologies, visualizations and research data will be published.

An important part will be the possibility of feedback and active interaction on the part of visitors, which will support two-way communication between the project team and the public. The platform will also be a place where new findings from experiments and testing will be published on an ongoing basis, with an emphasis on transparency and the usability of the results.

This approach reflects the principles of open science and allows the project outputs to be reused in science, development or teaching. The aim is to create an ecosystem in which research does not serve merely as a one-off output, but as a sustainable foundation for further development in the field of cybersecurity and cloud solutions.

2.2 Informing the lay public about the importance of cybersecurity and the potential of the INNOSOC project

Growing cyber threats have made it necessary to inform the general, lay public about suitable cybersecurity tools. It is therefore essential that the public be made aware of how the INNOSOC project contributes to the protection of the digital space precisely for those members of the public for whom existing solutions were financially unaffordable.

Given that the majority of the population obtains information online, we decided to use the website and social networks as the main communication channels as a priority. The website makes it possible to present the project's objectives, outputs, visualizations and news in a centralized, clear, comprehensible and educational way. Simplified language can thus be run in parallel with the professional language, which follows on from the previous partial objective.

Social networks, in turn, offer an interactive form of communication through which we can reach various groups of citizens and create a dialogue about internet security. Their strengths are the speed at which content spreads, visual appeal to the public and the possibility of involving the audience in campaigns, quizzes or discussions. Thanks to these tools, we can effectively spread awareness of the importance of cybersecurity, the risks of threats and the advantages of intelligent solutions such as those offered by INNOSOC. In this way, we seek to contribute to higher digital literacy of the public and, at the same time, to increase the societal impact of the project.

2.3 Popularizing the topic and increasing digital literacy among students

One of the sub-objectives of the INNOSOC project is to popularize the topic of cybersecurity and, at the same time, to increase digital literacy among secondary school and university students. The popularization activities will be carried out mainly through the project website and social networks, which will make it possible to reach students effectively in an environment that is close and natural to them. These digital channels will provide space for publishing popularization articles, guides, videos and short interactive posts that will explain, in an understandable and engaging way, the basic principles of cybersecurity, the threats of the digital world and the ways of addressing them.

A significant benefit of the project is also that it will enable the University of Žilina, specifically the Faculty of Management Science and Informatics (UNIZA FRI), to build a functional SOC solution as part of teaching, which will become a practical tool for developing students' skills. Teaching will take the form of project- and problem-based learning, thanks to which students will gain not only theoretical knowledge but also real experience in designing, testing and implementing security solutions in a cloud environment.

The aim is to significantly increase the number of students involved in practical teaching in the fields of cybersecurity and cloud computing and to motivate them to pursue further study or research activities in this field. Regularly publishing content on social networks, such as infographics, quizzes, previews of the development or interviews with experts, builds a relationship with students and increases their interest in the topic.

INNOSOC thus creates not only an educational and research infrastructure but also a lively and open communication channel with the student community. The project thereby also supports the emergence of new scientific research activities and meets the characteristics of a future solution with commercial potential that, already during its development, becomes part of the educational and awareness-raising environment.

3 Description of the segments for the popularization activities

Each of the segments of the popularization activities brings individual communication needs and scope for appropriate targeting.

3.1 Professional public

The professional public includes IT professionals, security analysts, researchers and academics who work in cybersecurity, the cloud or artificial intelligence.

This group is the primary recipient of the project's professional outputs, especially as regards technical documentation, research articles, algorithms and the architecture of the SOC solution. Thanks to the professional outputs, open-access publications and symposia, they gain an opportunity for professional discussion, feedback and the linking of research initiatives.

The INNOSOC project also offers this group the possibility of participating in the development through feedback mechanisms on the website. A significant benefit is access to open outputs that they can use in their own research or development. The project provides these target groups with a high-quality basis for scientific cooperation and innovation.

3.2 General/lay public

The general public consists of citizens without IT specialization who, however, increasingly face cyber risks in their everyday use of the internet and digital services.

The INNOSOC project aims to raise awareness of the importance of cybersecurity among this group as well. The website and social networks will serve as a tool for popularizing the topic by means of popularization articles, videos, infographics and animations.

The aim is to explain basic concepts such as "SOC", "anomaly", "cloud" and "AI" and to show how these technologies protect their everyday digital activities. Emphasis is placed on clarity, visualization and practical examples. The project also contributes to increasing digital literacy, which is in line with both European and national strategies. By activating this group, the INNOSOC project can achieve a broader societal impact and support informed digital behaviour.

3.3 Potential customers

The project's potential customers are mainly small and medium-sized enterprises (SMEs), larger companies and public administration organizations that face growing demands for the protection of IT infrastructure and data.

INNOSOC offers them an innovative SOC solution available as a service (SOCaaS) that is flexible, scalable and efficient. Customers will appreciate the advantages of the multi-tenant architecture, predictive monitoring and AI-based automated threat detection.

Direct sales via e-mail, telephone outreach and personal communication was chosen as the primary method for reaching potential customers. The outreach will, however, be supported by the existing popularization activities in the form of social networks and the website.

The project website will contain a section devoted to the commercial potential and possible uses of the solution. The aim is to build trust and prepare the market for the future deployment of the platform.

Successfully reaching customers also requires supporting outputs intended for popularization activities, such as brochures, leaflets, roll-ups and the like.

3.4 Secondary school students

This group represents future experts whose interest in the topics of security and modern technologies needs to be captured in good time.

Through social networks, blogs and short videos, the INNOSOC project will disseminate popular science content explaining the basics of cybersecurity, the principles of data protection and the role of artificial intelligence.

Emphasis will be placed on clarity, playfulness and the visual side in the form of infographics, quizzes and possibly gamified elements. The aim is to arouse interest in IT and cybersecurity as a potential study or career path. The activities may also include online competitions, involvement in popularization campaigns or workshops in cooperation with schools. In this way, the project wants to show these students that cybersecurity is not just for experts, but a topic that everyone can understand and that is indispensable nowadays.

3.5 University students

University students with a technical and informatics focus are among the main target groups of the INNOSOC project. The aim is not only to raise their awareness of security technologies but, above all, to involve them actively in development, testing and learning through project- and problem-based teaching.

The INNOSOC platform will provide a real SOC solution usable in practical teaching, through which students will gain valuable skills in cloud architectures, monitoring and AI-based threat detection. The popularization activities, conducted through the website and social networks, will provide them with technical content, tutorials, implementation examples and expert commentary on the solutions.

Space will also be created for feedback, discussion and involvement in competitions and final theses. The project thus contributes not only to increasing expertise but also to better preparing graduates for the needs of the labour market and further research.

4 Outreach methods and communication tools

An effective popularization campaign for the INNOSOC project requires targeted and differentiated communication across several target groups. For the content and message of the project to reach students, the professional public, the lay public and potential customers, several communication formats and channels must be used.

The basic principle is a combination of digital presence, professional and popular-science publications, and physical material for personal meetings and events. In this chapter, we present the individual communication tools that will be used within the project.

4.1 Website

The project website serves as the basic communication and information channel through which the main information about the project is conveyed to the public. Its main purpose is to present the objectives, professional focus and innovative character of the solution that the project brings in the field of cybersecurity and cloud technologies.

It serves to provide those interested with an overview of the research orientation, the benefits for practice and the connections with European digital initiatives.

The site also provides basic information about the partners involved, their roles and the context in which the project was created. It serves as an entry point where visitors can become acquainted with the project and then follow its further development – especially through regular content updates in the form of news or outputs.

The ambition for the future is for the website to grow and be supplemented with further sections: professional and popularization articles, downloadable documents, visualizations of the solution, research outputs, as well as calls for the involvement of the public or students. It is also linked to social networks, where news and popularization activities aimed at various target groups are shared. The website thus serves as an open and gradually developed platform that supports transparency, awareness and building interest in the topic of cybersecurity.

4.1.1 Activities carried out

4.1.1.1 Creation of the website

For the purposes of communication with the general public, the website INNOSOC was created. The website consists of 5 basic sections between which the user can navigate, namely:

- **Home,**
- **About the project,**
- **Outputs,**
- **News,**
- **Contact**.

On arriving at the website, the user can see a brief description of the project. The website contains the logos of the implementers, the project duration and the partners working on the project.

The "Home" section communicates the main objective of the project, the sub-objectives, the challenges that led to the project, as well as its benefits and the segments that will benefit from the project outputs.

The user can find out more about the project by clicking on the "About the project" section, where the project objective is described in detail, together with its identification data, such as the call code, investment name, component name, project code, place of implementation and implementation period.

All outputs in the form of project documentation, reports from experiments and testing, guides and the final report are also available on the website. All these documents will gradually be uploaded to the website and will be available for viewing.

Another section is "News", where blog articles and popularization articles will be published, as well as all news relating to the activities carried out, meetings, and published indexed articles and publications.

The last available section is "Contact", where the user has access to a form in case of questions.

To cover the popularization activities effectively, it was necessary to implement selected analytical tools on the website. The implementation of analytical tools on the INNOSOC project website is a key element for effectively measuring the impact of the popularization activities and optimizing the communication strategy. The analytical tools will enable the project team to make data-driven decisions on the further direction of the popularization activities and will also provide objective metrics for evaluating the success of the individual communication channels.

The basic analytical tool is Google Analytics 4, which provides a comprehensive overview of traffic, visitor sources, demographic characteristics of users and their behaviour on the website. Google Tag Manager serves as the central system for managing all tracking codes,

which will allow flexible and rapid adjustments without the need to intervene in the website code.

Google Search Console provides important information on the website's performance in Google search, including keyword positions and indexing errors. Ahrefs is used for comprehensive SEO analysis, backlink tracking and monitoring of positions for relevant keywords in the field of cybersecurity.

The analytical tools are implemented in compliance with the GDPR and include transparent information for users about data collection by means of cookie banners and a privacy policy. Google Tag Manager enables simple management of user consents and selective loading of tracking scripts based on the permissions granted.

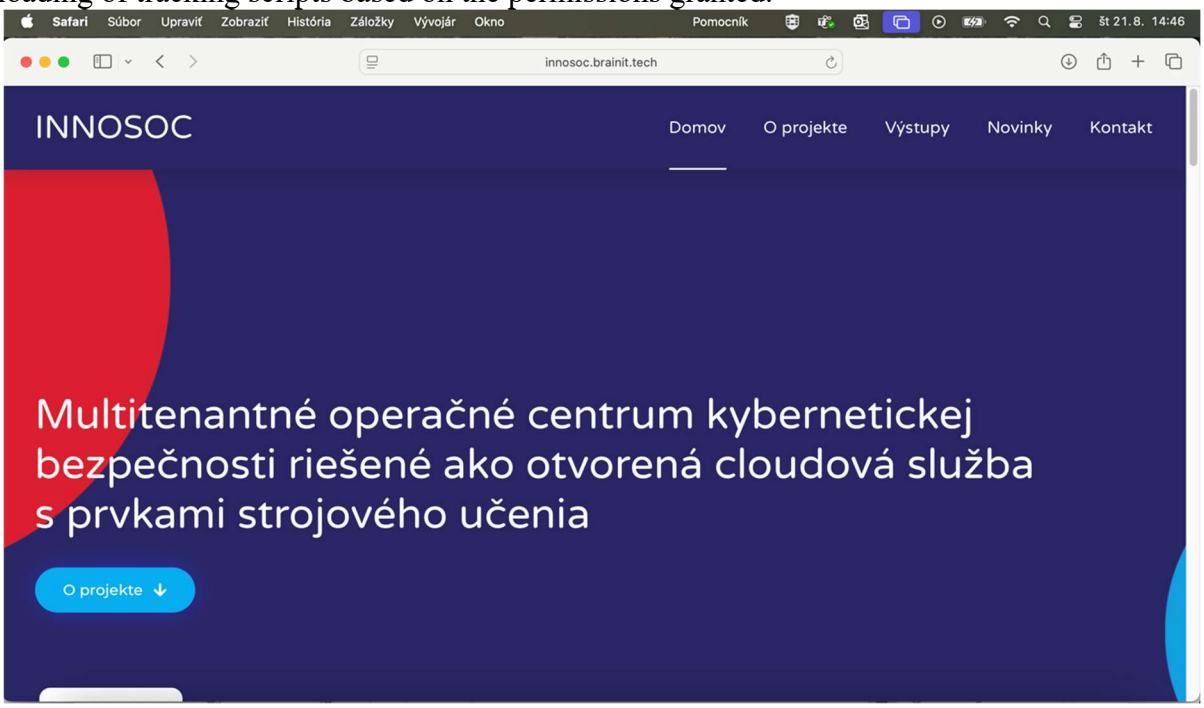


Figure 1: Preview of the INNOSOC home page, Source: (BRAIN:IT, 2025)

4.1.1.2 Article on the partner meeting

The aim of the blog post published on 28 July 2025 was to communicate the course of the meetings of the project partners, BRAIN:IT and the Faculty of Management Science and Informatics, University of Žilina, to the general public. The article on the meeting of 15/7/2025 communicates the current progress of work on the project, its further direction and the organizational activities for the following period, which were addressed at an online meeting.

The full text of the article can be found in Annex 1 – Article: Partner meeting 15/7/2025

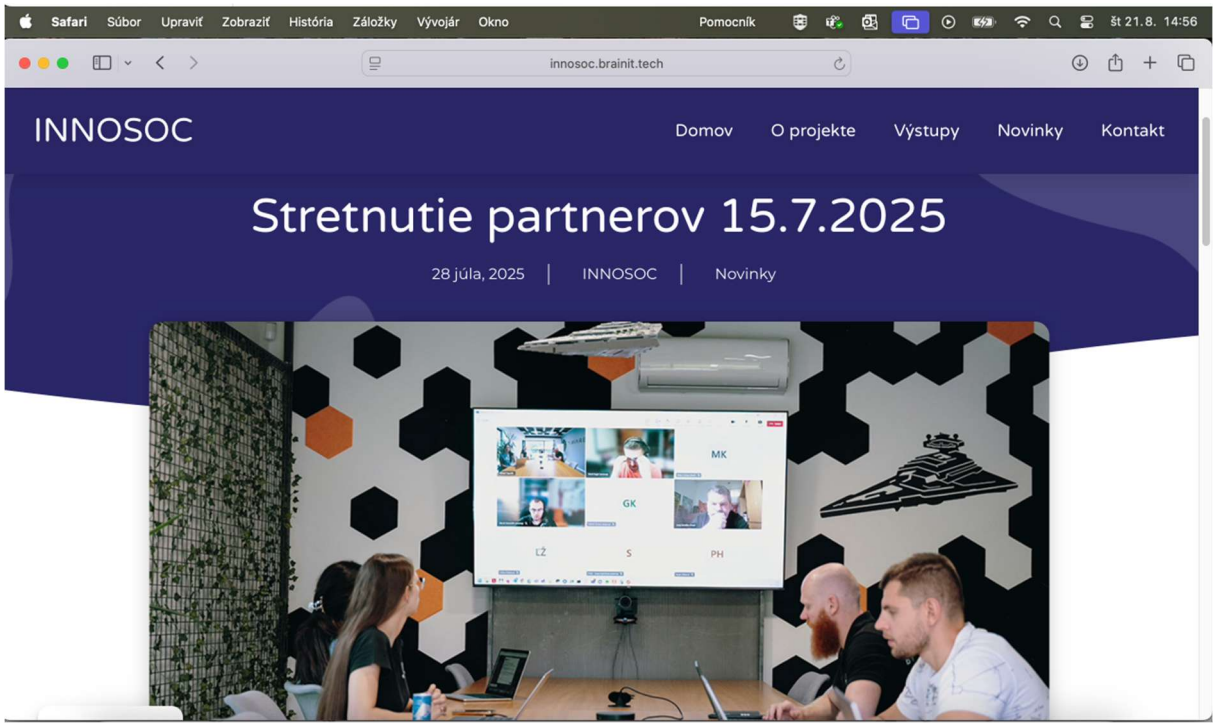


Figure 2: Article on the INNOSOC website: Partners' meeting 15/7/2025, Source: (BRAIN:IT, 2025)

4.1.1.3 Article on the interview with Ing. Michal Papučík

On 20 August, a short article was added to the "News" section communicating an information video, an interview recorded with the COO of BRAIN:IT, Ing. Michal Papučík. The video is embedded in the article by sharing it from the @INNOSOC channel on the YouTube platform. The blog article helps to distribute information about the interview to the wider public and at the same time to raise awareness of the basic information about the INNOSOC project.

The full text of the article can be found in Annex 2 – Article: Fundamentals of the INNOSOC project: Interview with Ing. Michal Papučík.

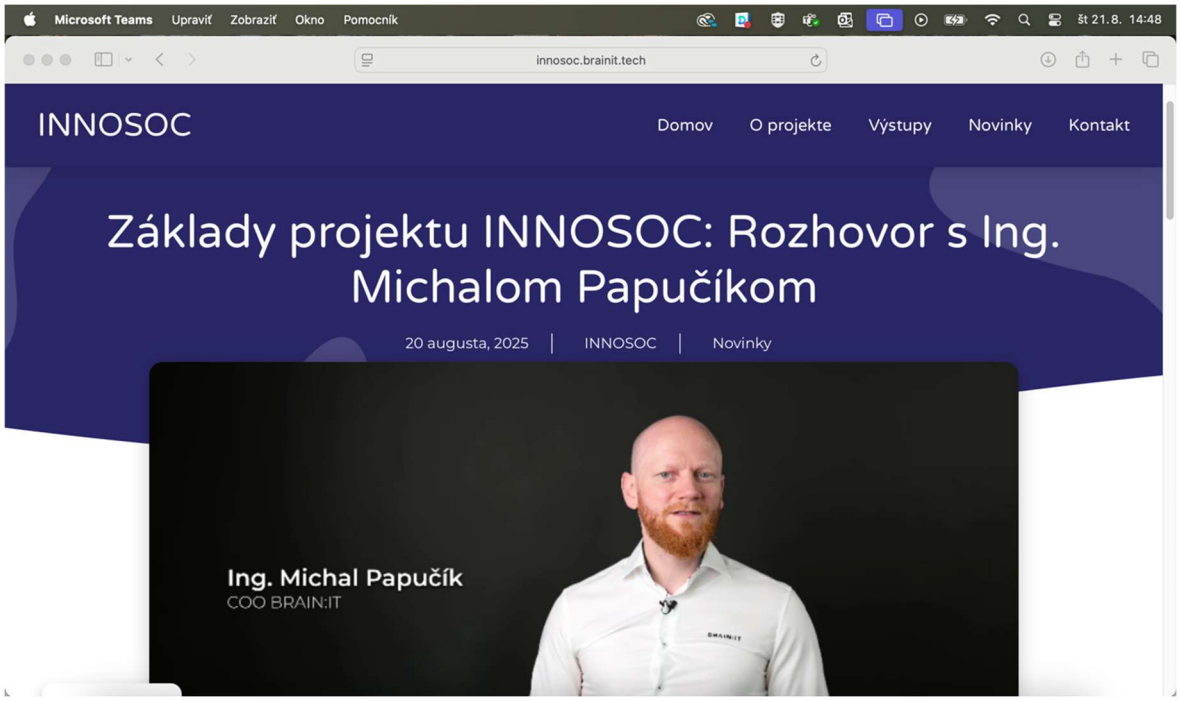


Figure 3: Article on the INNOSOC website: Foundations of the INNOSOC project, Source: (BRAIN:IT, 2025)

4.1.1.4 Article on the interview with prof. Ing. Pavol Segeč, PhD.

As part of the project, an expert interview was conducted and published on with prof. Ing. Pavol Segeč, PhD., head of the Department of Information Networks at the Faculty of Management Science and Informatics, University of Žilina (UNIZA), who acts as a key scientific researcher of the project. The aim of the interview was to explain the importance of cybersecurity in today's digital environment, to point out the growing cyber threats and to explain the role of the INNOSOC project in building systematic and centralized protection of organizations and educational institutions.

The content of the interview focuses in particular on:

- the importance of cybersecurity for organizations of all sizes in the context of growing digitalization,
- the role of the Faculty of Management Science and Informatics of UNIZA as the main project partner and provider of scientific research and development capacities,
- identification of the most common cyber threats, such as phishing, ransomware and advanced persistent threats (APT),
- explanation of the concept of the Security Operations Center (SOC) as a central element of protection, built on the pillars of people, processes and technologies,
- the impacts of the new NIS2 directive on requirements in the area of management and reporting of cybersecurity incidents,
- the practical operation of SOC systems based on the collection, correlation and analysis of large volumes of security data in real time.

The interview is a professional, presentational and awareness-raising output of the project that links the scientific research perspective with practical impacts on the security of organizations. At the same time, it serves as a tool for raising awareness of the importance of

cybersecurity and of the benefits of the INNOSOC project for both academic and applied practice.

The full text of the article can be found in Annex 3 – Article: Interview with prof. Ing. Pavol Segeč, PhD.: Cybersecurity is no longer just a topic for large companies.



Figure 4: Article on the INNOSOC website: Interview with prof. Ing. Pavol Segeč, PhD.: Cybersecurity is no longer just a topic for large companies, Source: (BRAIN:IT, 2025)

4.1.1.5 Article on the presentation of the INNOSOC project at the student event FRIčkovica

On 11 November 2025, an article was published in the "News" section on the presentation of the INNOSOC project at the student event FRIčkovica, which took place on 8 October 2025 at the Faculty of Management Science and Informatics of the University of Žilina. The aim of the project's participation in the event was to introduce students to the INNOSOC project, its main intentions, objectives and the problems addressed in the field of cybersecurity, as well as to raise awareness of the importance of research and innovation in this field.

As part of the activity, an information and presentation stand was prepared for students, through which the main outputs of the project, its benefits for both academic and applied practice and the opportunities to get involved in cybersecurity issues were communicated. The presentation also served as a tool for popularizing the topic of cybersecurity among young professionals and students of technical disciplines.

The activity is a popularization and dissemination output of the project, aimed at supporting education, building awareness of cybersecurity and strengthening the link between the research project, the academic environment and the student community.

The full text of the article can be found in Annex 4 – Article: Student event FRIčkovica – 8 October.

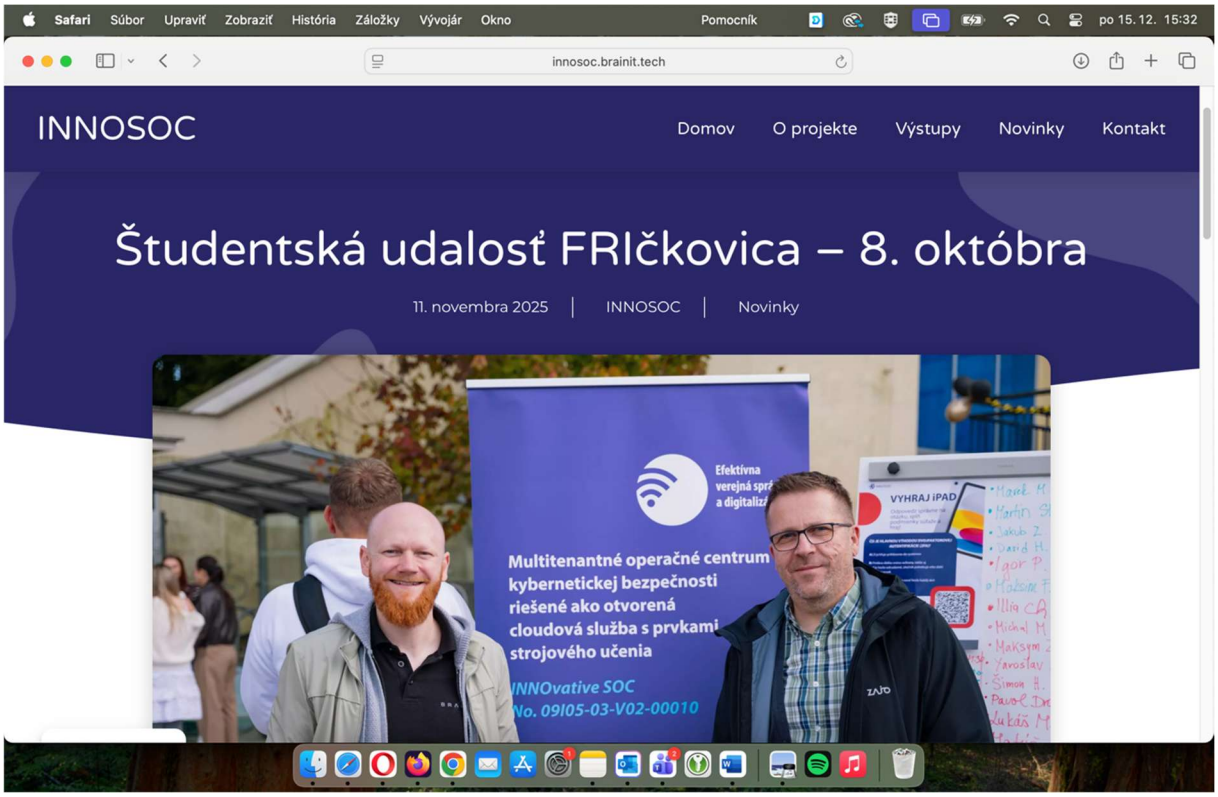


Figure 5: Article on the website: Presentation at the student event FRIčkovica, Source: (BRAIN:IT, 2025)

4.1.1.6 Information announcement of the INNOSOC project symposium

On 17 November, an announcement was published in the "News" section about the professional symposium on the topic Multi-tenant cybersecurity operations centre designed as an open cloud service with machine learning elements, which will take place on 19 December 2025 on the premises of the University of Žilina. The aim of the symposium is to present the current state of the INNOSOC project, its interim results and research findings in the field of cybersecurity and cloud security services. The event creates space for professional discussion between the academic community, researchers, students and other practitioners.

The full text of the announcement on the website can be found in Annex 5 – Announcement of the INNOSOC symposium.

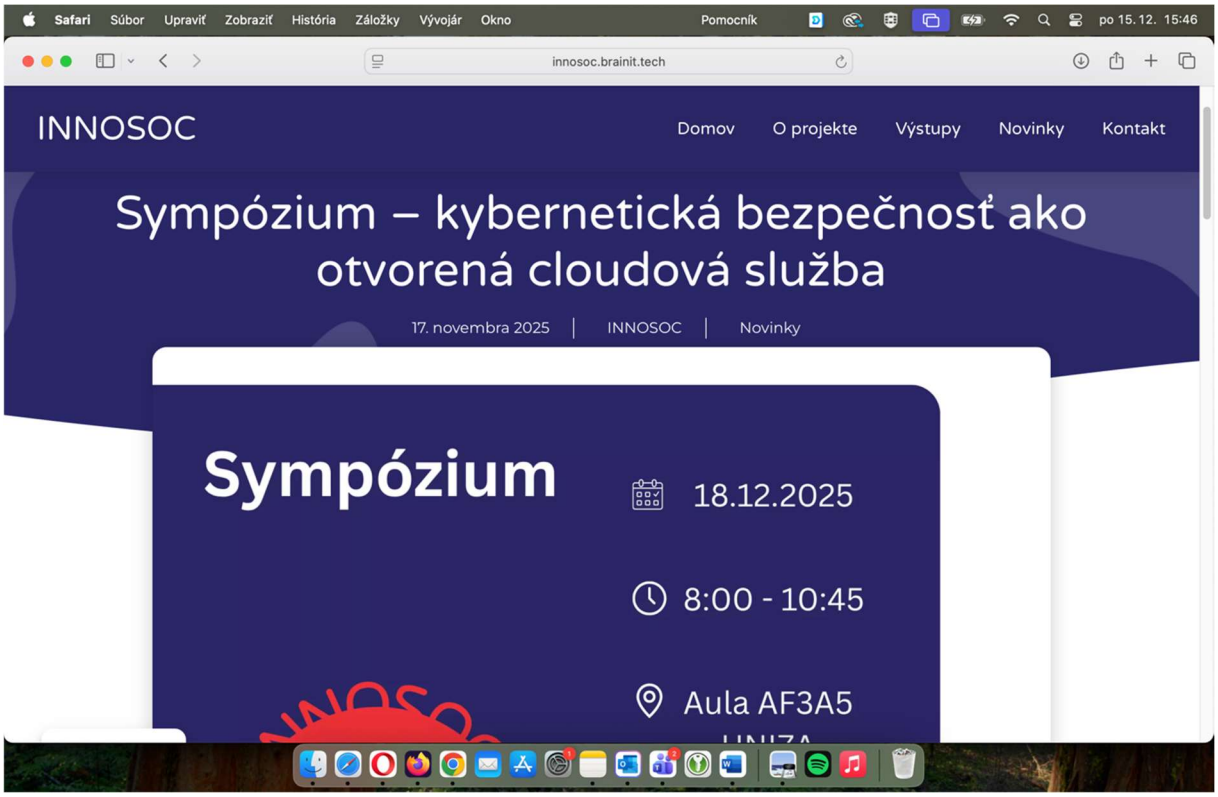


Figure 6: Article on the INNOSOC website: symposium, Source: (BRAIN:IT, 2025)

4.1.1.7 Article on the announcement of the winner of the iPad competition

On 24 November, an article was published announcing the winner of the iPad competition, which was organized through the Instagram profile @innosoc_.

The full text of the article can be found in Annex 6 – Article on the announcement of the winner of the iPad competition.

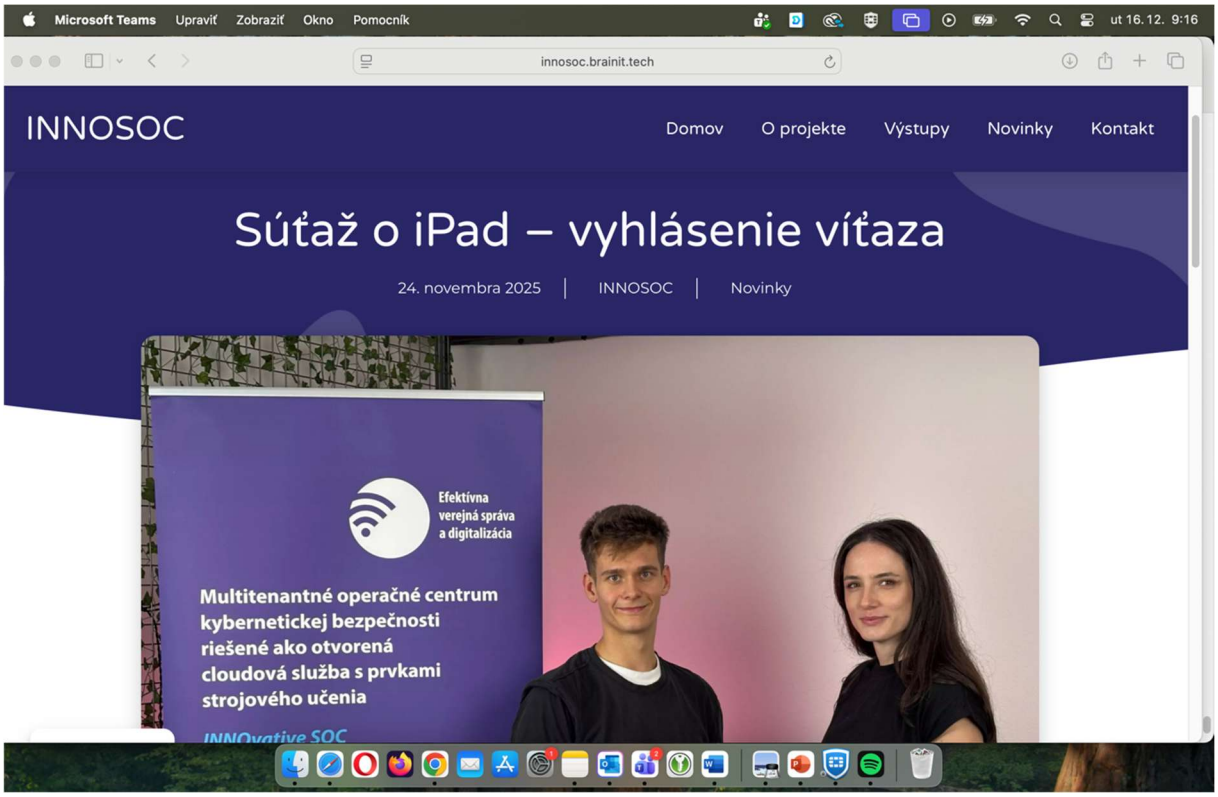


Figure 7: Article on the website: iPad competition, Source: (BRAIN:IT, 2025)

4.1.1.8 Article on the presentation of the INNOSOC project at the student breakfast

On 28 November 2025, an article was published communicating the presentation of the INNOSOC project during the student breakfast held at the Faculty of Management Science and Informatics of the University of Žilina on 4 November. The aim of the activity was to introduce the INNOSOC project informally to students of management and informatics disciplines and to acquaint them with the current state of the project, its outputs to date and the planned next steps. The presentation also communicated the key topics of the project, in particular the importance of cybersecurity in today's digital environment, the role of the Security Operations Center (SOC) and the benefits of using cloud technologies in protecting information systems.

The activity is a presentation, popularization and dissemination output of the project, aimed at raising awareness of cybersecurity, supporting students' interest in this field and strengthening the link between the academic environment, the research project and applied practice.

The full text of the article can be found in Annex 7 – Article: Presentation of the INNOSOC project at the student breakfast.



Figure 8: Article on the INNOSOC website: Presentation at the student breakfast, Source: (BRAIN:IT, 2025)

4.1.1.9 Article on the presentation of the project at the Faculty of Applied Informatics of Tomas Bata University in Zlín

On 9 December 2025, an article was published communicating the presentation of the INNOSOC project at the Faculty of Applied Informatics, Tomas Bata University in Zlín, on 20 November 2025. The INNOSOC project was presented to the students by Ing. Michal Papučík, who outlined the main objectives of the project, its focus and the way in which it responds to the challenges associated with the transition to a digital economy and the growing demands on cybersecurity.

The presentation focused in particular on:

- the link between the INNOSOC project and the current needs of the commercial and industrial sectors,
- the growing demand for modern IT services and qualified IT specialists,
- the importance of raising the level of cybersecurity in organizations,
- the basic principles, technologies and approaches used in the INNOSOC project.

The activity is a presentation, popularization and dissemination output of the project, aimed at disseminating the project results, strengthening cooperation between the academic environment and applied practice, and motivating students towards professional growth in the field of cybersecurity and information technologies.

The full text of the article can be found in Annex 8 – Article on the presentation of the project at the Faculty of Applied Informatics of Tomas Bata University in Zlín.



Figure 9: Article on the INNOSOC website: presentation of the project at Tomas Bata University in Zlín, Source: (BRAIN:IT, 2025)

4.1.1.10 Article on the presentation at the Jozef Murgaš Secondary Technical School in Banská Bystrica

On 12 December, an article was published in the "News" section communicating the presentation of the INNOSOC project at the Joef Murgaš Secondary Technical School in Banská Bystrica on 29 November 2025. The aim of the activity was to introduce the INNOSOC project to secondary school pupils, explain the basic principles of cybersecurity and raise awareness of the digital threats they may encounter in everyday life.

During the presentation, the pupils became acquainted in particular with:

- the main focus and objectives of the INNOSOC project,
- the areas addressed by the project,
- the most common types of cyberattacks today,
- the educational and academic institutions involved,
- the importance of cybersecurity for individuals and for society.

The presentation was delivered in an interactive form with an emphasis on actively involving the pupils in the discussion, which supported their interest in cybersecurity issues and the development of digital literacy.

The activity is a popularization, educational and dissemination output of the project, aimed at awareness-raising in the field of cybersecurity and motivating young people to behave safely in the digital environment.

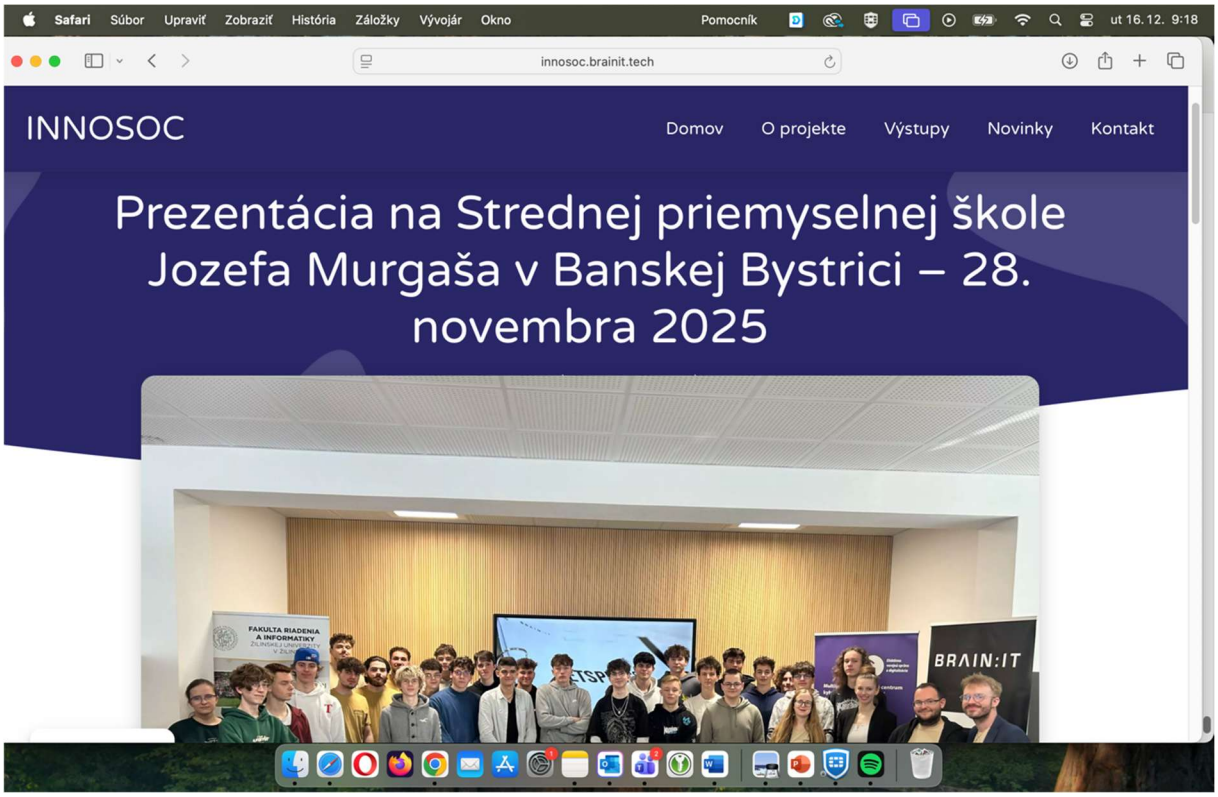


Figure 10: Article on the INNOSOC website: presentation at the Jozef Murgaš Secondary Technical School in Banská Bystrica, Source: (BRAIN:IT, 2025)

4.2 Social networks

Effective communication of the project outputs is essential not only for fulfilling its professional and research objectives but also for ensuring their societal and practical impact. Given the focus of the INNOSOC project – the development of an innovative multi-tenant security centre – a key aspect of promotion is targeted and trustworthy digital communication that reaches the right audience: from technical experts and public administration to the young generation of professionals and IT students.

4.2.1 Basis of the communication strategy

The target group of the communication is not only technology partners or customers. According to the "Project Description" document, important groups also include:

- small and medium-sized enterprises without internal IT departments,
- representatives of public administration (schools, municipalities, institutions),
- students and graduates in the field of informatics,
- technology enthusiasts and the community in the area of cybersecurity,
- the wider lay public interested in security in the digital space.

For this reason, communication channels with different levels of expertise, output formats and language style will be chosen. The content will be divided into categories according to the type of target segment, e.g. professional content for LinkedIn, visual and educational content for Instagram.

4.2.2 Main communication tools

Several platforms reflecting the diversity of the target groups may be used for promotion.

One of the main pillars of the project's communication strategy may be the LinkedIn profile of BRAIN:IT, which has more than 4,000 followers. It is a professionally oriented communication channel focused mainly on the B2B segment and the professional community. Through this profile, professional posts, posts presenting other supporting activities related to the INNOSOC project and knowledge acquired in the course of the project may be published. The aim is to reach corporate partners, the professional public and decision-makers in the fields of technology and public administration, thereby also strengthening the credibility of the project and its professional legitimacy.

Alongside the formal LinkedIn profile, another important tool is the Instagram account of BRAIN:IT with 1,000 followers. This channel has a visual and less formal focus, which makes it suitable for presenting the project activities and outputs and sharing knowledge acquired in the course of the project. This channel is oriented mainly towards the younger generation of professionals, the technical community, the wider public and informatics students and graduates, and it helps to build the brand and raise awareness of the project in the non-professional sphere.

At the academic level, the project may be communicated through the faculty's profiles, which already achieve a high level of interaction with the student community. The Instagram account @budmanazer, which has more than 900 followers, is a community-academic channel for followers drawn mainly from students and young professionals. The content will focus on the project outputs and sharing knowledge acquired in the course of the project. The aim is to activate the young target group and show them the project as an opportunity for personal and professional growth.

Reach into a technology-oriented audience is also provided by the Instagram profile @budfri with 1,900 followers. This profile targets students and graduates of the Faculty of Management Science and Informatics, as well as the wider IT community. The content may consist mainly of overviews of technical outputs and posts mapping the link between research and real-world practice. An important role of this channel is to strengthen professional awareness.

The communication strategy may also be complemented by the faculty's official LinkedIn profile Faculty of Management Science and Informatics, University of Žilina, which is intended for a more formal presentation of research and educational projects to the academic and scientific research community and which is followed by more than 2,000 users. Through this channel, official announcements on the progress of the project, summaries of research outputs, involvement in national and international initiatives, as well as examples of cooperation with industry may be published. The aim is to anchor the project in the context of the faculty's strategic innovations and to present it as part of its research portfolio.

A further complementary element of the communication strategy may be the creation of separate INNOSOC project accounts on Instagram and LinkedIn. These accounts could serve as central communication points for presenting all project activities across its life cycle – from the research intent through the development stages to the final implementations and demonstrations. The content of these profiles may be structured so that, in a chronological and thematically clear form, it captures the key implementation milestones, reports on ongoing progress, communicates results and presents the applicability of the solutions in various types of organizations. The Instagram profile may be visually oriented and geared towards fast and interactive communication with the public, whereas LinkedIn may serve as the project's professional noticeboard, with an emphasis on research, technological and legislative aspects. These channels may complement the communication of the project partners and will make it possible to preserve and present the project results even after its official completion.

4.2.3 Content plan

A complementary output of the promotion of posts on social networks will be the content plan, which serves to ensure consistent, timely and professional communication across all platforms.

This content plan will contain the following elements:

- Publication calendar
- Publication date
- Topic
- Distribution channel (IG, LinkedIn, @budfri...)
- Person responsible for creation, approval and publication
- Post status (draft – awaiting approval – ready – published)
- Links to media and assets (file name, location in the cloud, prepared QR code)

The Excel format enables efficient teamwork, task synchronization and retrospective tracing of published content, and will also provide an overview for internal reporting. Regular reviews make it possible to evaluate interactions and optimize the style of the outputs according to what works best.

4.2.4 Activities carried out

4.2.4.1 Creation of a page on the LinkedIn social network

For communicating and sharing information with the community of professionals, including researchers, experts, academics and other companies, a page named @INNOSOC was created on the LinkedIn social network. Communication on this social network is expected to target the professional public effectively. The page will also communicate longer professional posts and articles and will serve as a channel for communication with the professional public. The nature of this social network will ensure a high level of credibility.

The page contains a profile photo and a cover photo showing the logos of the implementers. The user can also learn what the project is about and who the project partners are, and can reach the website via a link.

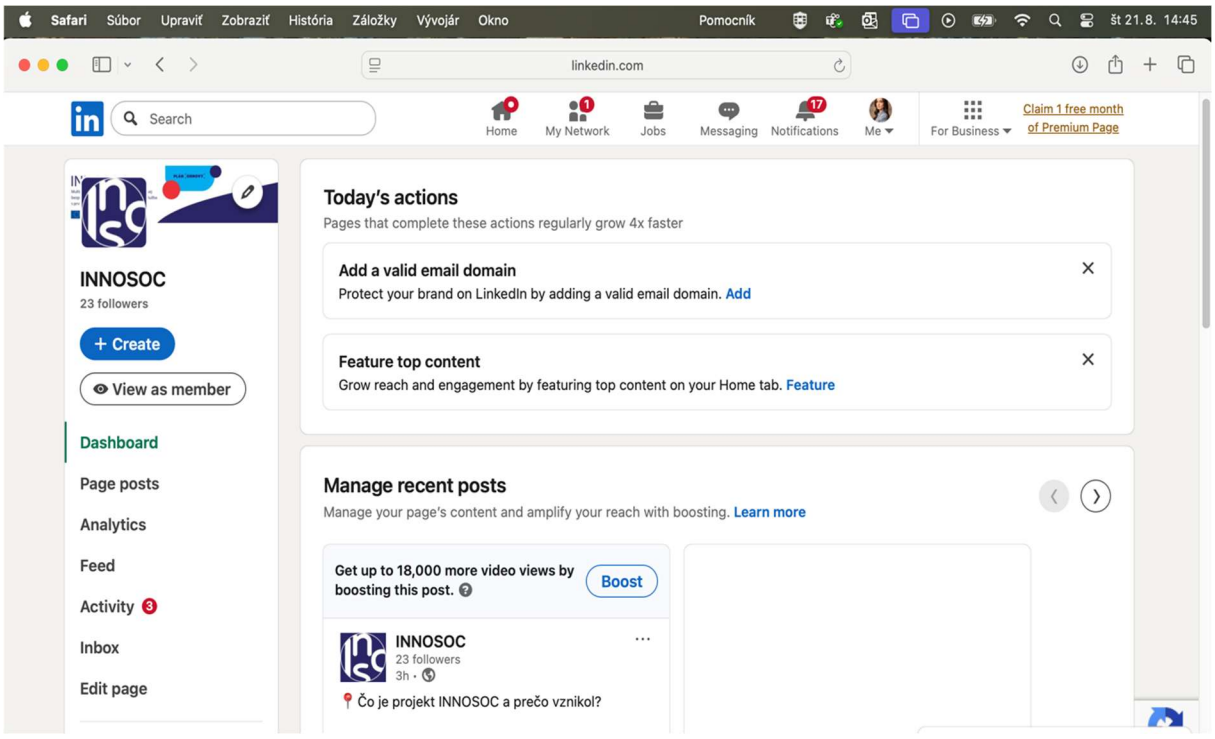


Figure 11: LinkedIn page for the INNOSOC project, Source: (BRAIN:IT, 2025)

4.2.4.2 Creation of a profile on the Instagram social network

For communicating with young students, young professionals and the general public, an Instagram profile named @innosoc_ was created. The Instagram profile was supplemented with a profile photo and a short description of the project, which introduces it to everyone who visits the profile. The profile also contains a link to the website.

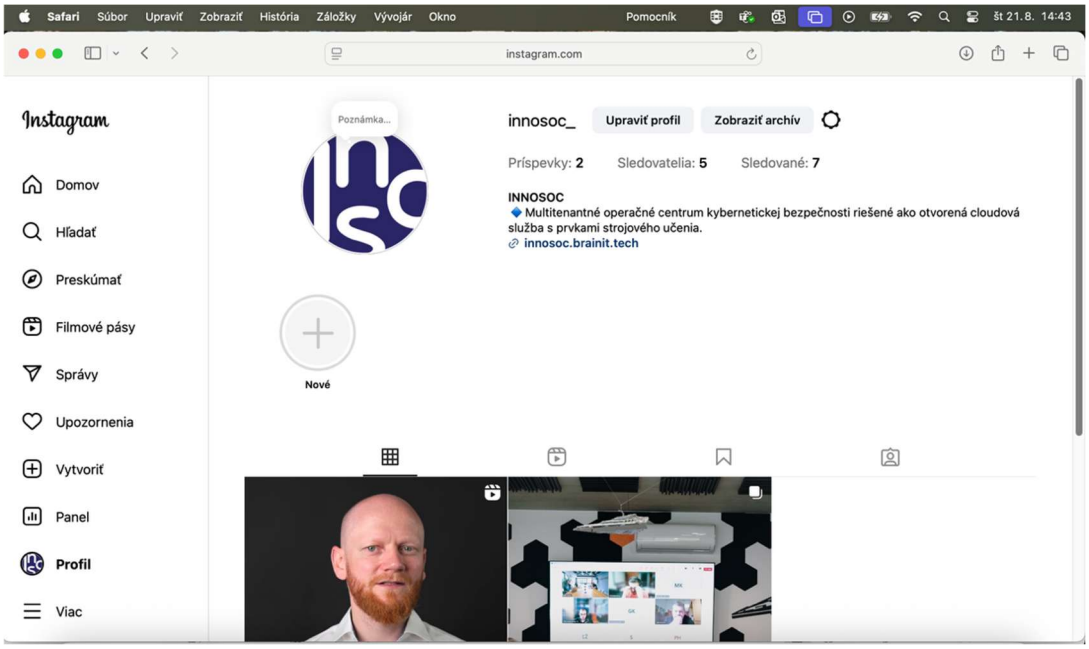


Figure 12: INNOSOC Instagram profile, Source: (BRAIN:IT, 2025)

4.2.4.3 Post communicating the availability of the INNOSOC website on Instagram @brainit.tech

The aim of the post on the Instagram profile @brainit.tech, published on 26 June 2025, was to initially communicate the existence of the INNOSOC project as industrial applied research. The post was published on the Instagram profile of the project partner BRAIN:IT, which has a large community base of young people, including secondary school and university students as well as young professionals. The post also draws attention to the newly created INNOSOC website.

The published content included:

- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic,
- visual graphics supporting the identity of the INNOSOC project.

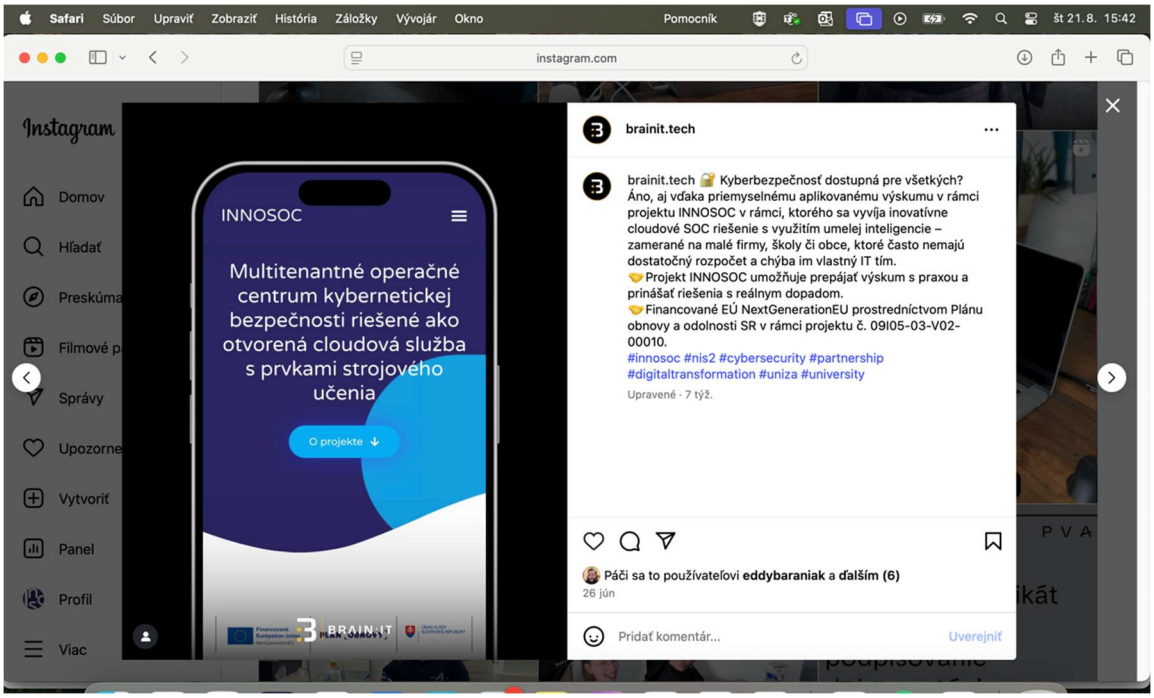


Figure 13: Post on the Instagram account @brain.tech, Source: (BRAIN:IT, 2025)

4.2.4.4 Post on the partner meeting of 15/7/2025 on Instagram @innosoc_

The aim of the post published on 28 July 2025 was to communicate the course of the meeting of the project partners, BRAIN:IT and the Faculty of Management Science and Informatics, University of Žilina. The post about the meeting of 15 July 2025 communicates the current progress of work on the project, its further direction and the organizational activities for the following period, which were discussed at an online meeting.

The published content included:

- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic,
- visual graphics supporting the identity of the INNOSOC project.

By publishing the post on the Instagram social network, the aim was to attract and reach secondary school and university students. The published posts can be seen in Figure 14.

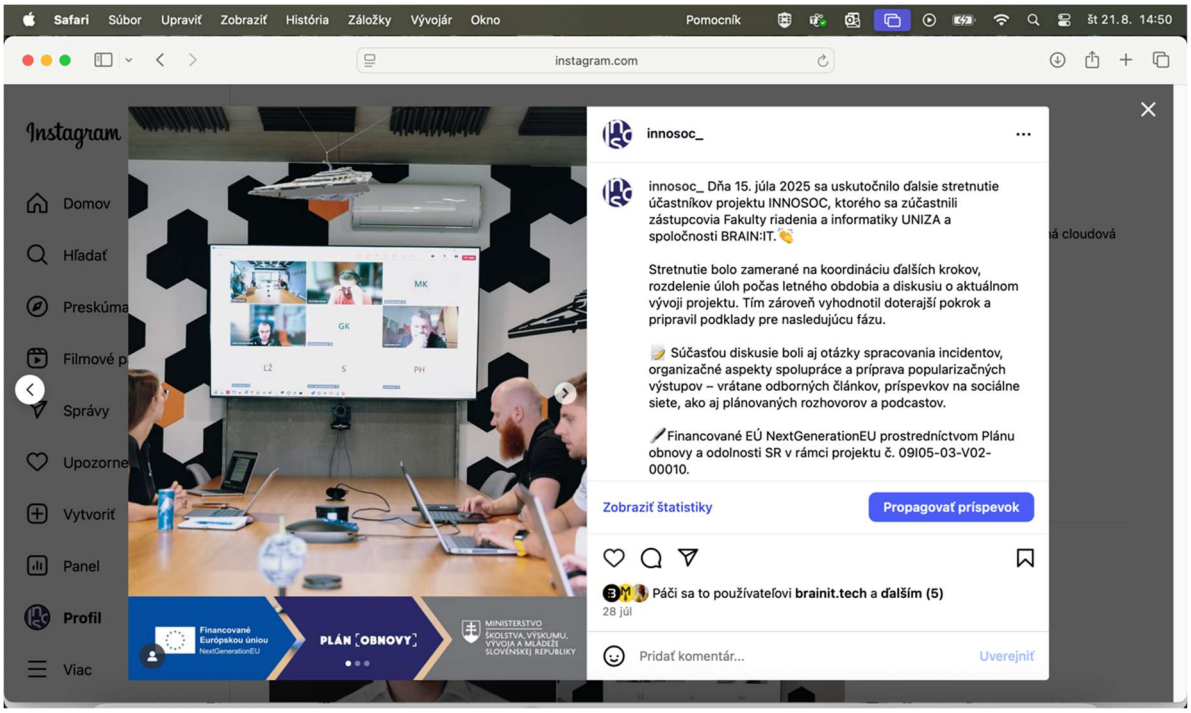


Figure 14: Post about the partners' meeting of 15/7/2025 on Instagram @innosoc_, Source: (BRAIN:IT, 2025)

4.2.4.5 Post on the partner meeting of 15/7/2025 on LinkedIn @INNOSOC

The aim of the post published on 28 July 2025 was to communicate the course of the meeting of the project partners, BRAIN:IT and the Faculty of Management Science and Informatics, University of Žilina. The post on the LinkedIn social network is aimed at reaching experts, researchers and the B2B segment. The post about the meeting of 15/7/2025 communicates the current progress of work on the project, its further direction and the organizational activities for the following period, which were discussed at an online meeting. Publishing on the LinkedIn social network creates a professional discussion.

The published content included:

- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic,
- visual graphics supporting the identity of the INNOSOC project.

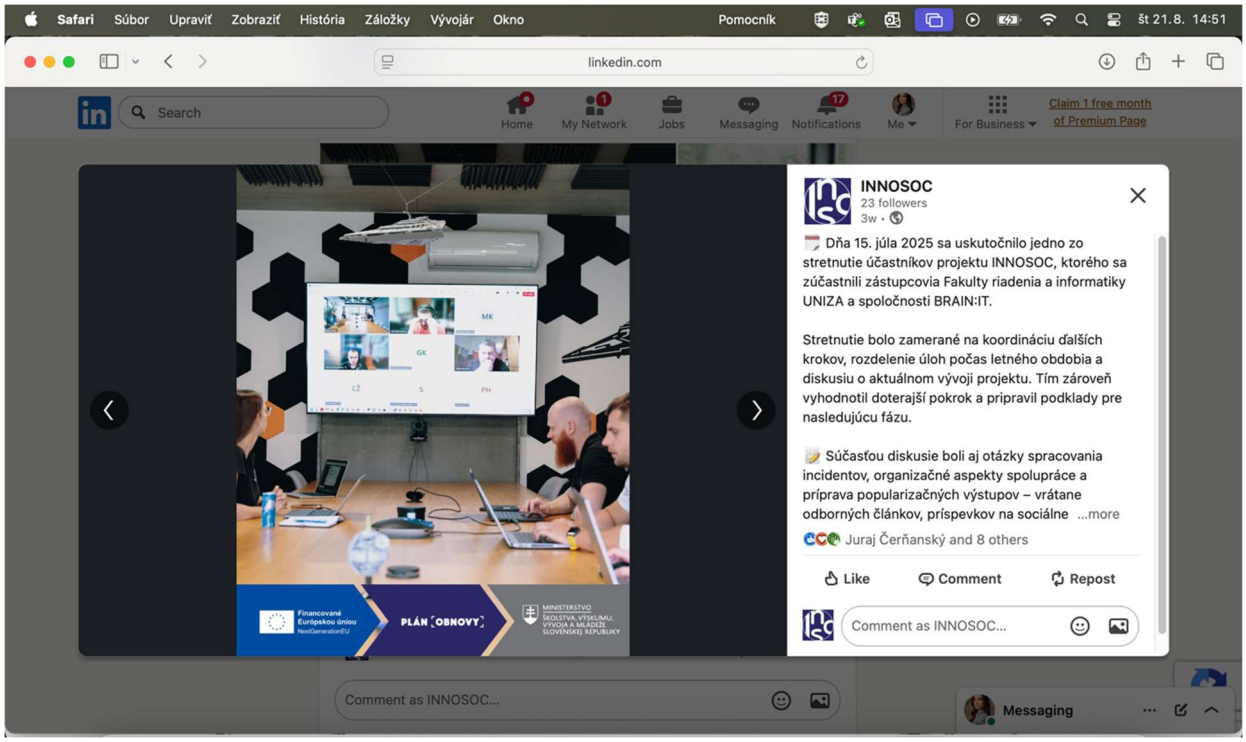


Figure 15: Post about the partners' meeting of 15/7/2025 on LinkedIn @INNOSOC, Source: (BRAIN:IT, 2025)

4.2.4.6 Post with basic information about the INNOSOC project on the Instagram profile @innosoc_ and the LinkedIn page @INNOSOC of 21/8/2025

On 21 August 2025, a short video was published on Instagram @innosoc_ and the LinkedIn page @INNOSOC. The video contains part of the interview recorded with Ing. Michal Papučík, the full version of which is available on the YouTube channel @INNOSOC. In this short published video, the audience and the general public learn basic information about the project, such as:

- What is the INNOSOC project and why was it created?
- What does the name INNOSOC represent?

The video is 54 seconds long, which makes it attractive to social media users. It is short, conveys the point concisely and, thanks to the added subtitles, allows wider sharing of information. The aim of the video is to raise awareness of the project and to explain its objective and significance to a wider audience, students and young professionals in an attractive way.

The published content included:

- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic,
- visual graphics supporting the identity of the INNOSOC project.

The transcript of the entire video can be found in Annex 15 – Interview with Ing. Michal Papučík.

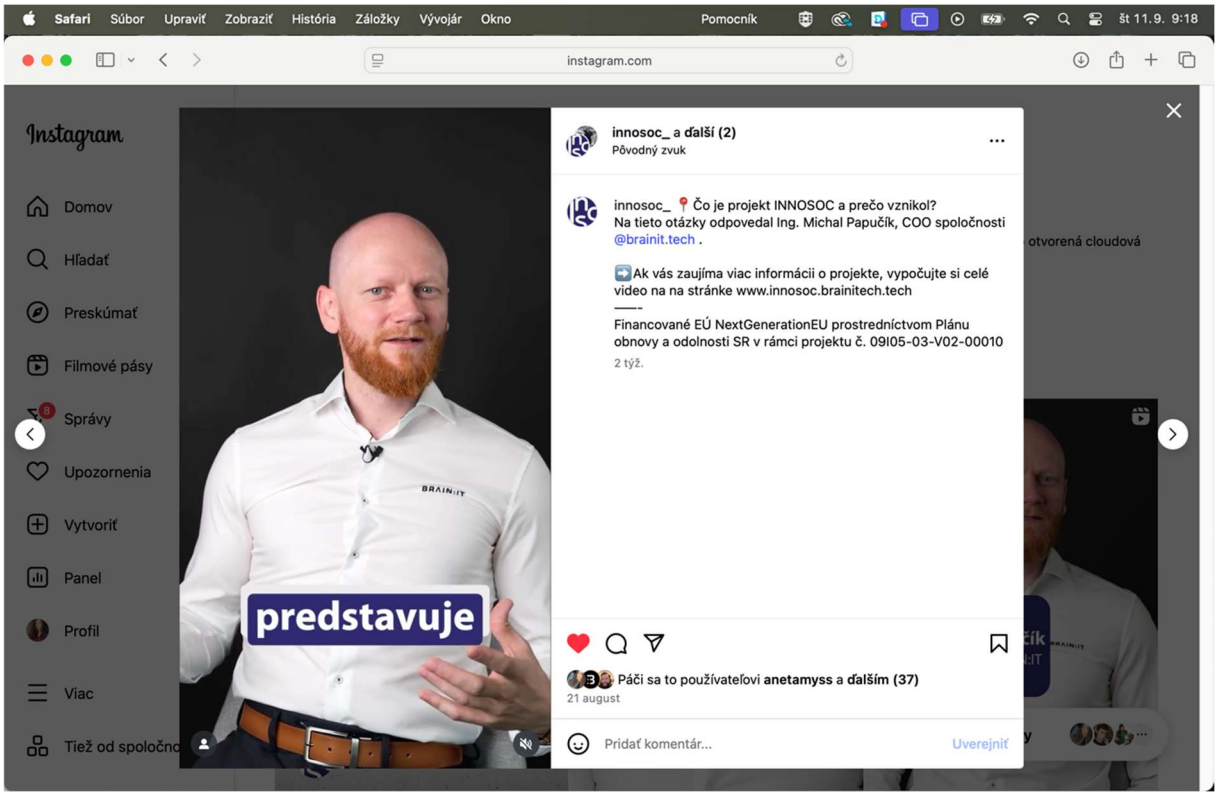


Figure 16 Short video post on Instagram @innosoc_ of 21/8/2025, Source: (BRAIN:IT, 2025)

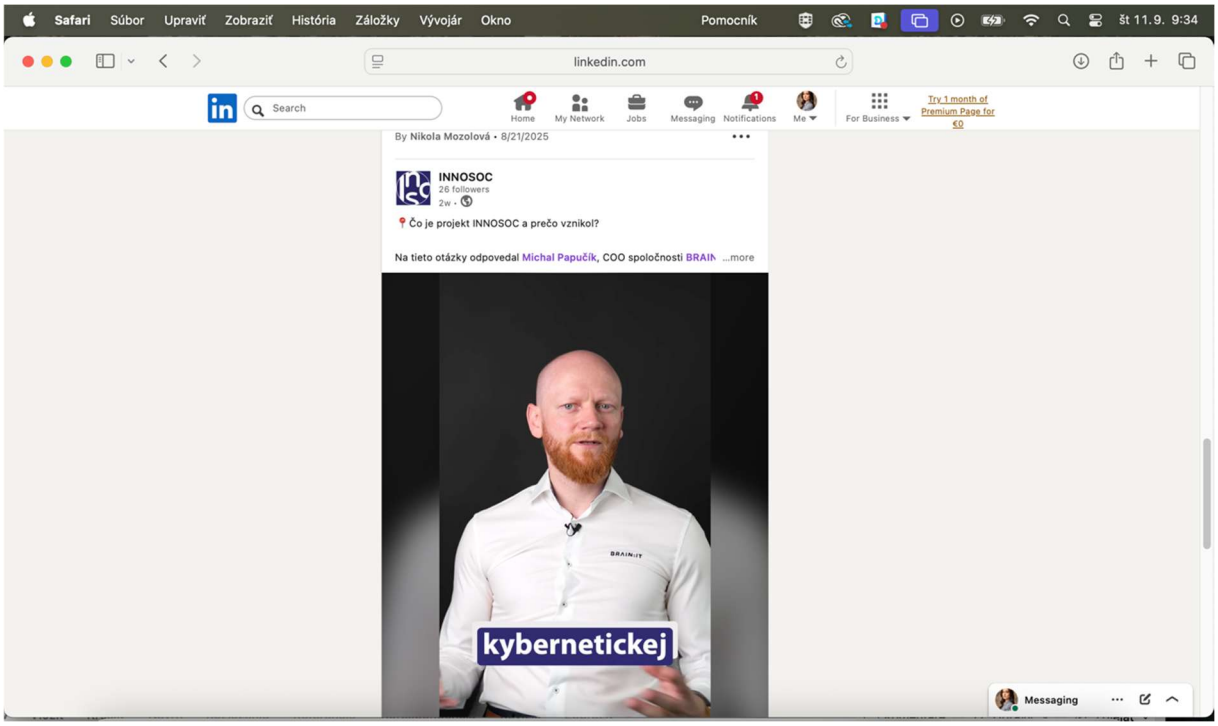


Figure 17 Short video post on the LinkedIn page @INNOSOC of 21/8/2025 , Source: (BRAIN:IT, 2025)

4.2.4.7 Post with basic information about the INNOSOC project on the Instagram profile @innosoc_ and the LinkedIn page @INNOSOC of 5/9/2025

On 5 September 2025, a post in the form of a short video was published. The video is 31 seconds long and contains part of the interview with Ing. Michal Papučík, which is published in full on the YouTube channel @INNOSOC. The video contains a brief explanation of the

project's objective. The video is edited into a format attractive for social media so as to engage the general public, students and young professionals.

The post published on Instagram @innosoc_ targets secondary school students and young professionals, while on the LinkedIn page @INNOSOC it targets university students, young professionals and the professional public.

The published content included:

- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic,
- visual graphics supporting the identity of the INNOSOC project.

The transcript of the entire video can be found in Annex 15 – Interview with Ing. Michal Papučík.

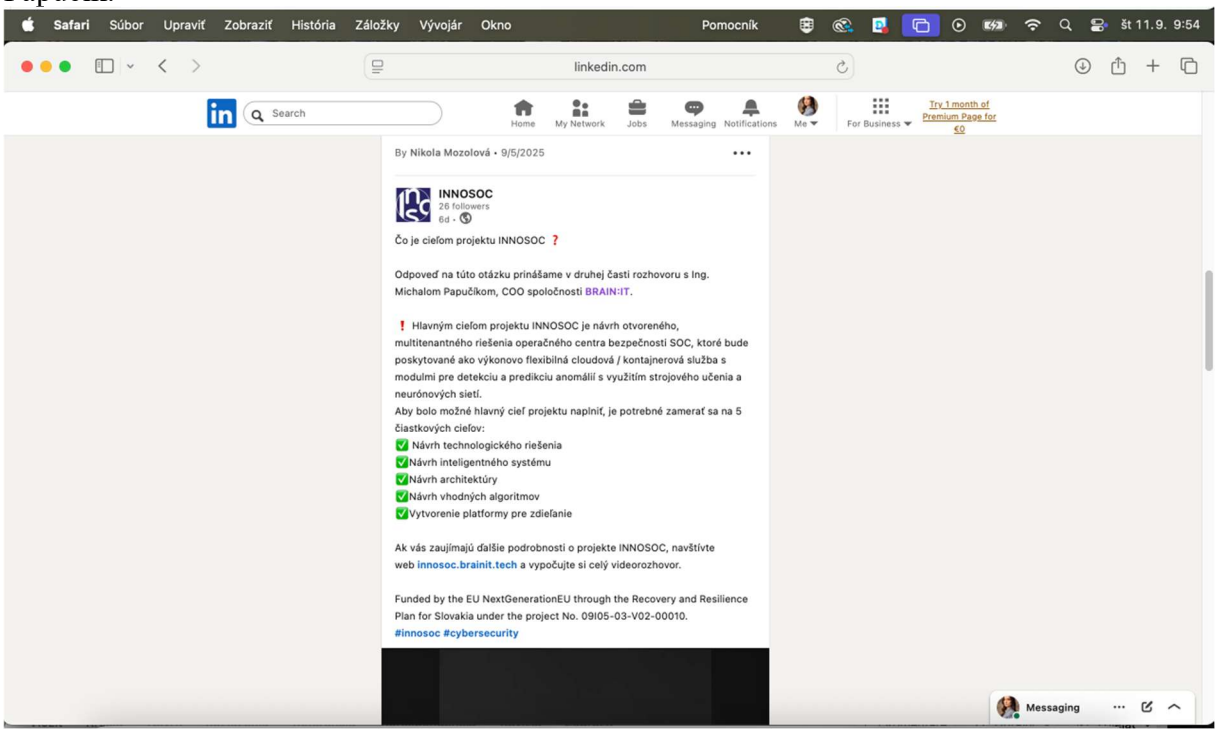


Figure 18 Short video post published on 5/9/2025 on LinkedIn @INNOSOC , Source: (BRAIN:IT, 2025)

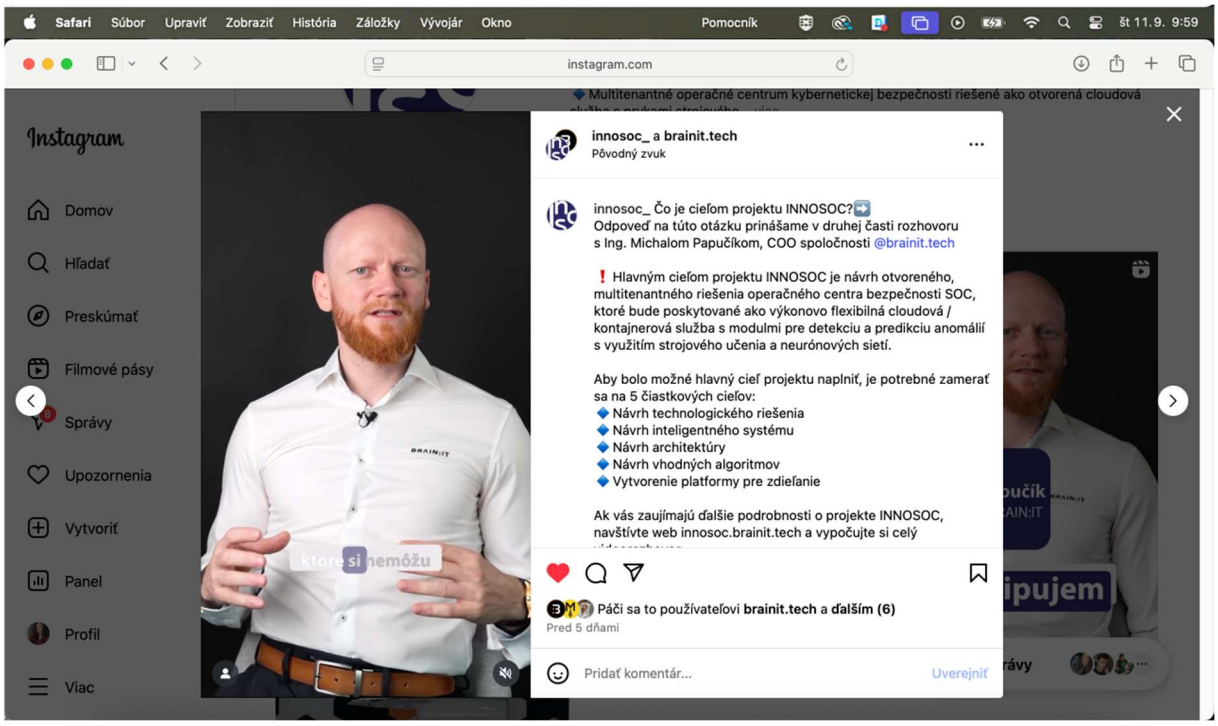


Figure 19 Short video post published on 5/9/2025 on Instagram @innosoc_ , Source: (BRAIN:IT, 2025)

4.2.4.8 Post in the form of a quiz on cybersecurity published on 8 September 2025

As part of cybersecurity education, a post in the form of a series of images was published on Instagram @innosoc_ on 8 September 2025. The post incorporates questions and options relating to cybersecurity and threats. The series of images offers a choice of options, giving the audience the opportunity to think and select the correct answer, which they can also verify in the post. The aim of the post is to educate and raise awareness of threats in the cyber world. The quiz questions follow up on the popularization article published on the LinkedIn page @INNOSOC and on the INNOSOC website, and the post also refers to the INNOSOC website, where the audience can read more.

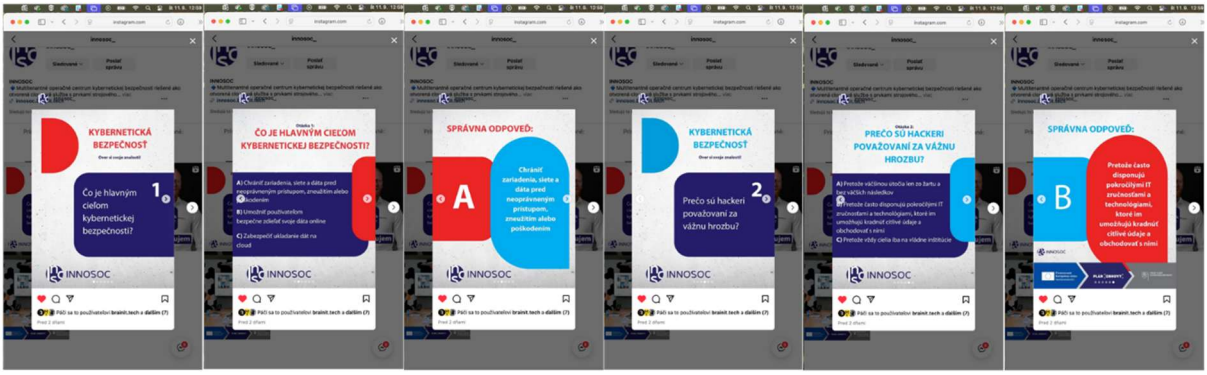


Figure 20 Quiz post on the topic of cybersecurity published on 9/9/2025 on Instagram @innosoc_, Source: (BRAIN:IT, 2025)

4.2.4.9 Post in the form of a quiz on cybersecurity published on 16 September 2025

As part of cybersecurity education, a post in the form of a series of images was published on Instagram @innosoc_ on 16 September 2025. The post incorporates questions and options relating to cybersecurity and threats. The series of images offers a choice of options, giving the audience the opportunity to think and select the correct answer. The aim of the post is to educate and raise awareness of threats in the cyber world. The quiz questions follow up on the popularization article published on the LinkedIn page @INNOSOC and on the INNOSOC website, and the post also refers to the INNOSOC website, where the audience can read more.



Figure 21: Post on the Instagram account @innosoc_: cybersecurity quiz, Source: (BRAIN:IT, 2025)

4.2.4.10 Informative post about the ongoing iPad competition on the Instagram account @innosoc_

On 3 October 2025, a post was published on the Instagram account @innosoc_ communicating the opportunity to win an iPad. The aim of the post is to increase young people's interest in cybersecurity issues. To enter the competition, each participant had to meet the following conditions, which were stated in the description of the competition post:

1. The participant had to answer correctly a question in the field of cybersecurity, which was communicated in the post visual as well as in the post description.

Wording of the competition question: "What is the main advantage of two-factor authentication (2FA)?"

Answer options:

a) It speeds up logging in to systems.

b) It adds another layer of protection, so even if the password is stolen, the attacker still needs another verification factor

c) It automatically generates a new password every day for additional protection.

2. The participant had to follow 4 Instagram profiles, namely @brainit.tech, @budmanazer, @budfri.sk and @innosoc_.

3. The participant had to tag 1 other person in a comment.

The published content included:

- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic,
- visual graphics supporting the identity of the INNOSOC project.

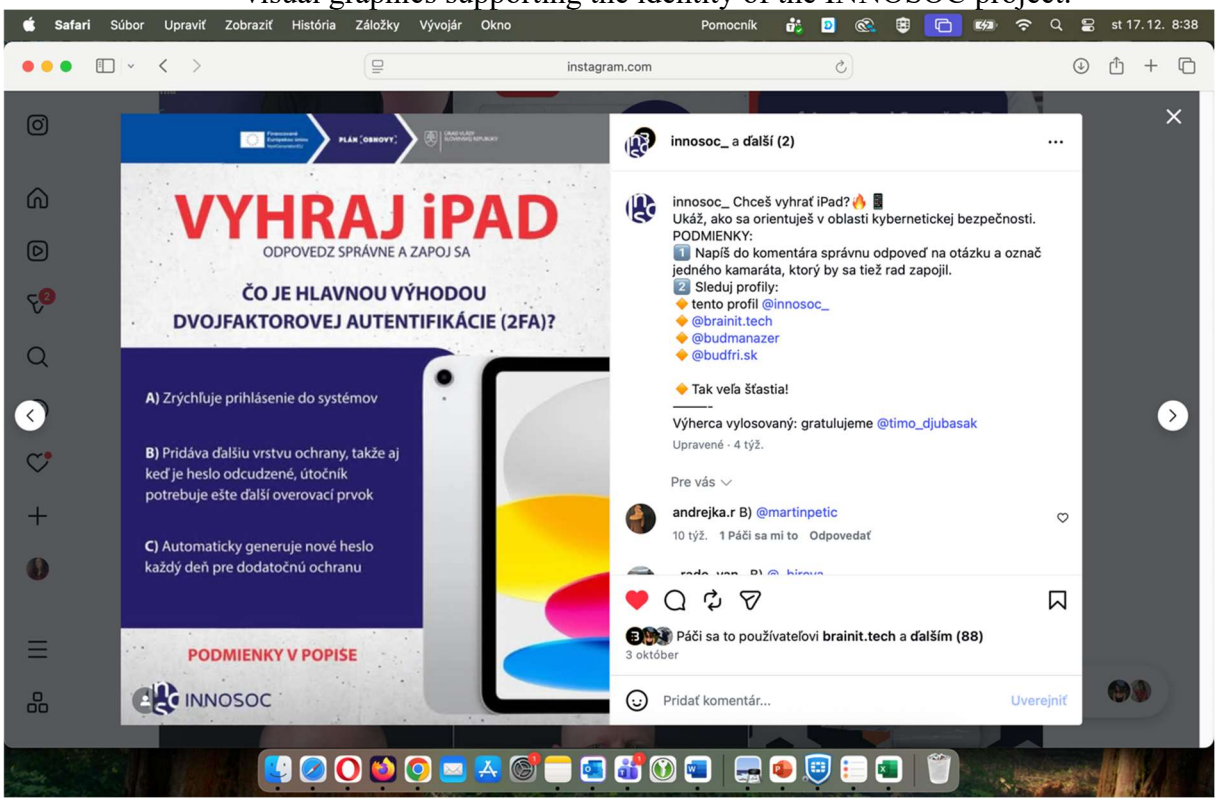


Figure 22: post on the Instagram account @innosoc_: iPad competition, Source: (BRAIN:IT, 2025)

4.2.4.11 Short video – interview with prof. Ing. Pavel Segeč, PhD.

On 17 October 2025, a short information video was published on the Instagram account @innosoc_ and the LinkedIn account @innosoc as an excerpt from the interview with prof. Ing. Pavel Segeč, PhD., who works on the project as a scientific researcher. The full-length interview is published on the INNOSOC YouTube channel. The short information video communicates why cybersecurity is a key topic. The short video is 1:02 minutes long and has been produced in a format attractive for social networks, with appropriate subtitles.

The published content included:

- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic,
- visual graphics supporting the identity of the INNOSOC project.

The full transcript of the interview can be found in Annex 16 – Interview with prof. Ing. Pavel Segeč, PhD.

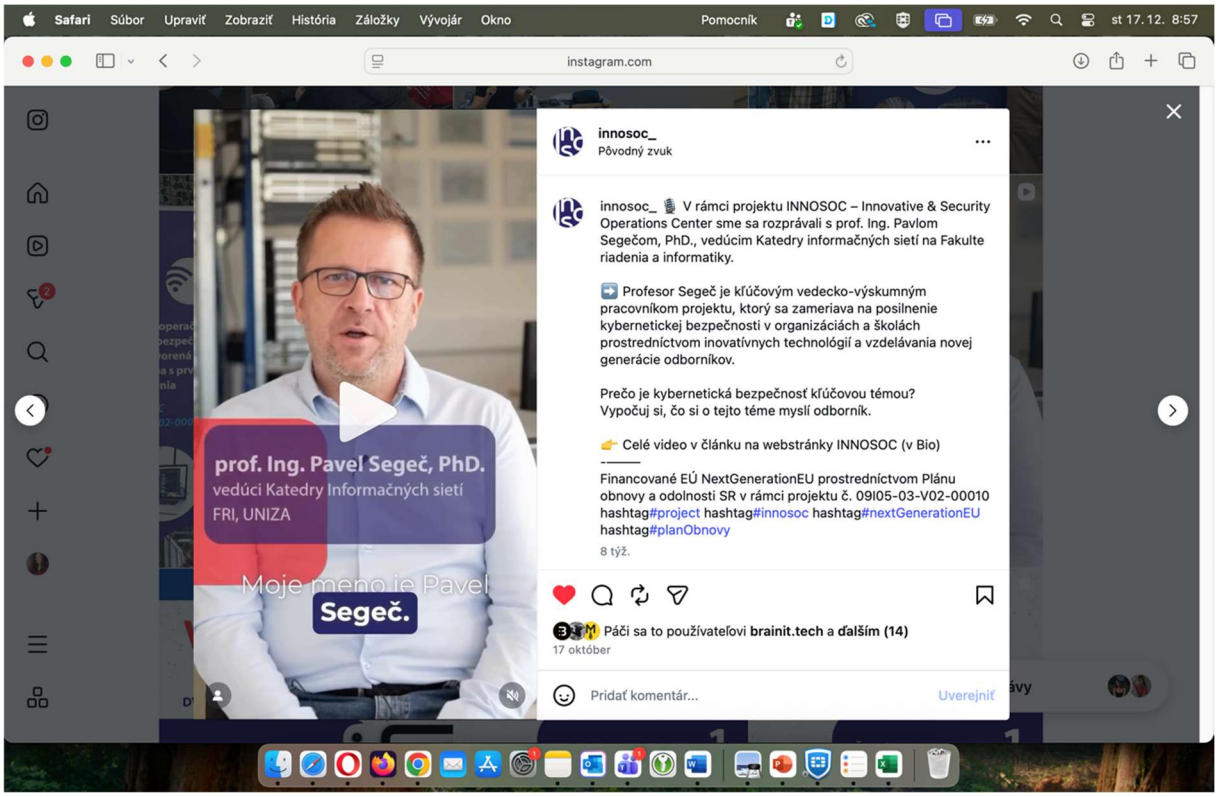


Figure 23: Short video on the Instagram account @innosoc_, Source: (BRAIN:IT, 2025)

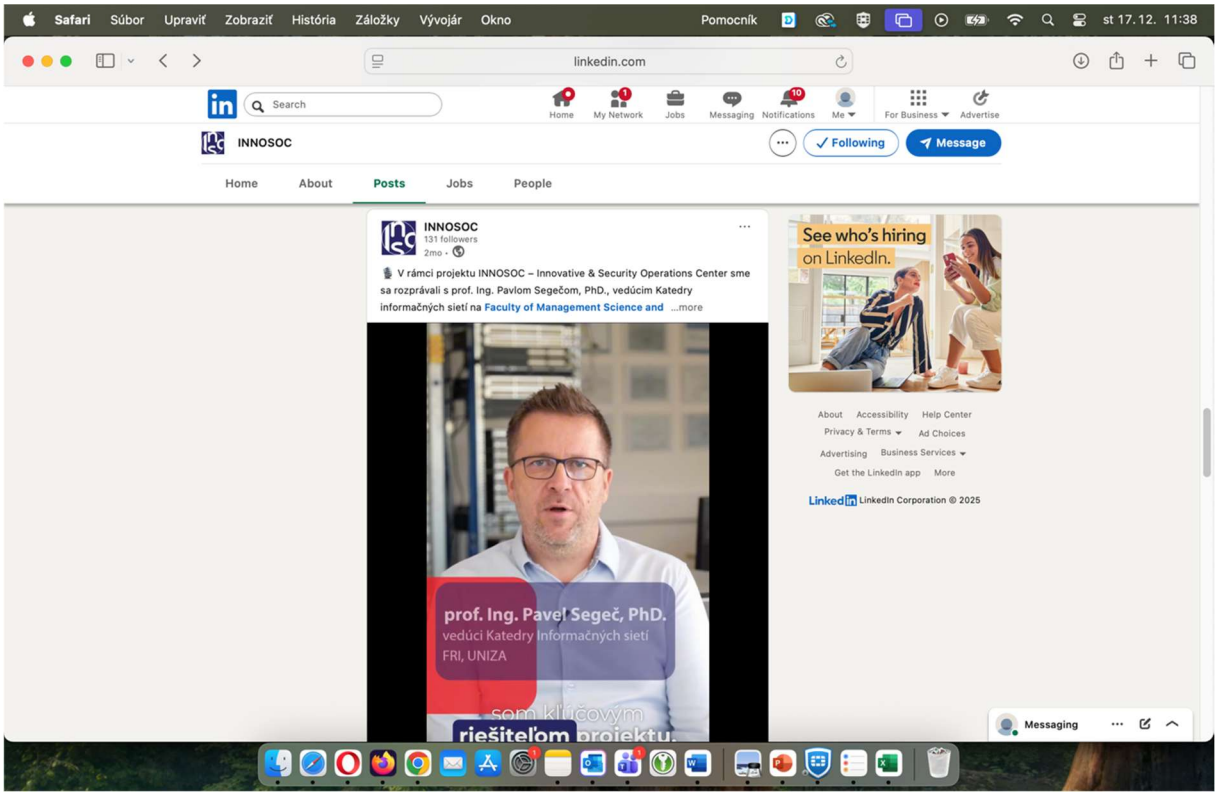


Figure 24: short video on the LinkedIn profile @innosoc: Interview with prof. Ing. Pavel Segeč, PhD., Source: (BRAIN:IT, 2025)

4.2.4.12 Informational post about the holding of the INNOSOC project symposium

On 18 November 2025, an informational and invitation post for the professional symposium on "Cybersecurity as an open cloud service" was published on the Instagram account @nnosoc_ and the LinkedIn account @innosoc.

The aim of the post was to inform the public, especially students and the professional and academic community, about the symposium, its topic, venue and time, as well as its link to the INNOSOC research project. The post also served to encourage attendance at the event and to spread awareness of the project's activities and outputs through social networks.

The published content included:

- basic information about the symposium (date, time, venue),
- the thematic focus of the symposium in the field of cybersecurity and cloud services,
- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic,
- visual graphics supporting the identity of the INNOSOC project.

The post represents a dissemination and popularization output of the project, aimed at communicating the results and activities of the INNOSOC project in the online space and at increasing its visibility among the target groups.



Figure 25: Post on the Instagram account @innosoc_: announcement of the symposium, Source: (BRAIN:IT, 2025)

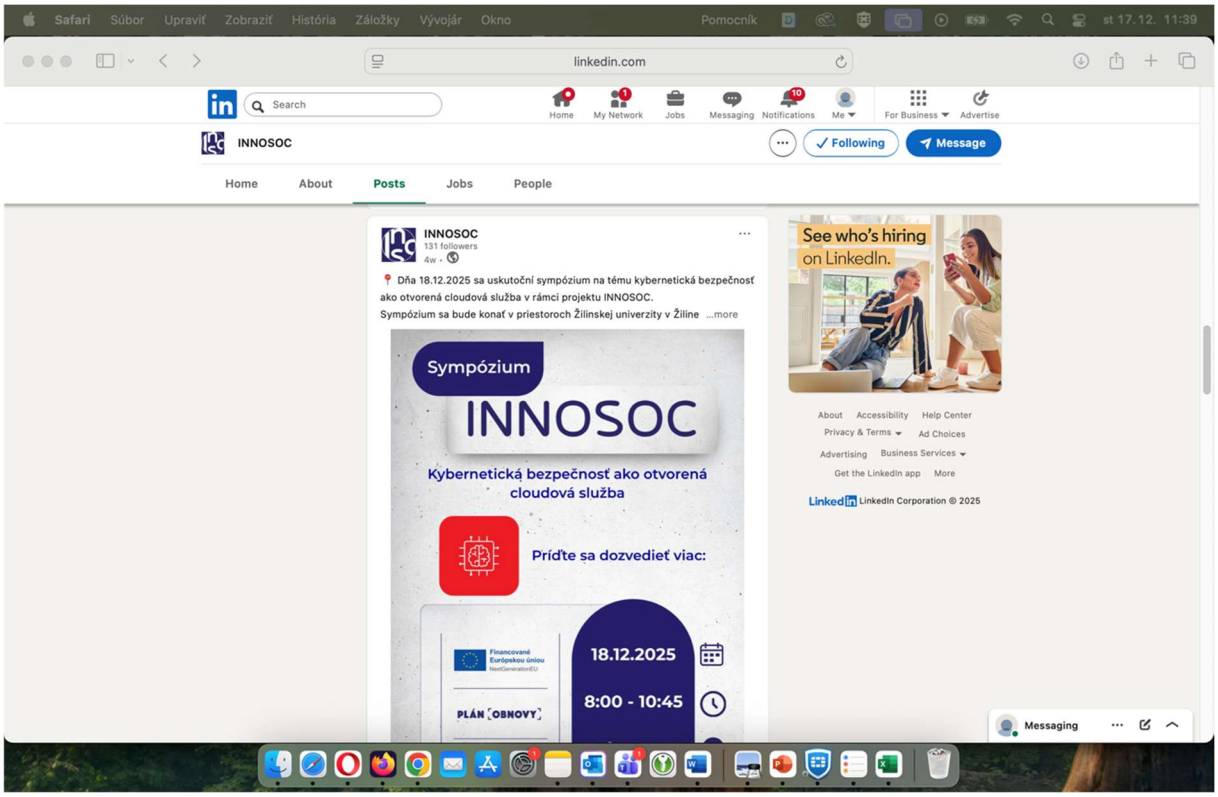


Figure 26: post on the LinkedIn profile @innosoc: announcement of the symposium, Source: (BRAIN:IT, 2025)

4.2.4.13 Post about the end of the iPad competition

On 24 November 2025, a post was published on the Instagram account @innosoc_ informing about the **end of the student iPad competition** and its winner.

The aim of the post was to support the involvement of young students in the activities of the INNOSOC project, to increase their interest in the topic of cybersecurity and to strengthen awareness of the project through an interactive form of communication on social networks.

The published content included:

- information about the end of the competition and its focus on fostering interest in cybersecurity,
- announcement of the competition winner and presentation of the prize-giving ceremony,
- visual material documenting the implementation of the activity,
- information about the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic.

The post represents a **dissemination and popularization output of the project** which contributed to the visibility of the INNOSOC project among the student community, supported interaction with the target group and increased the attractiveness of the project through educational and motivational activities.

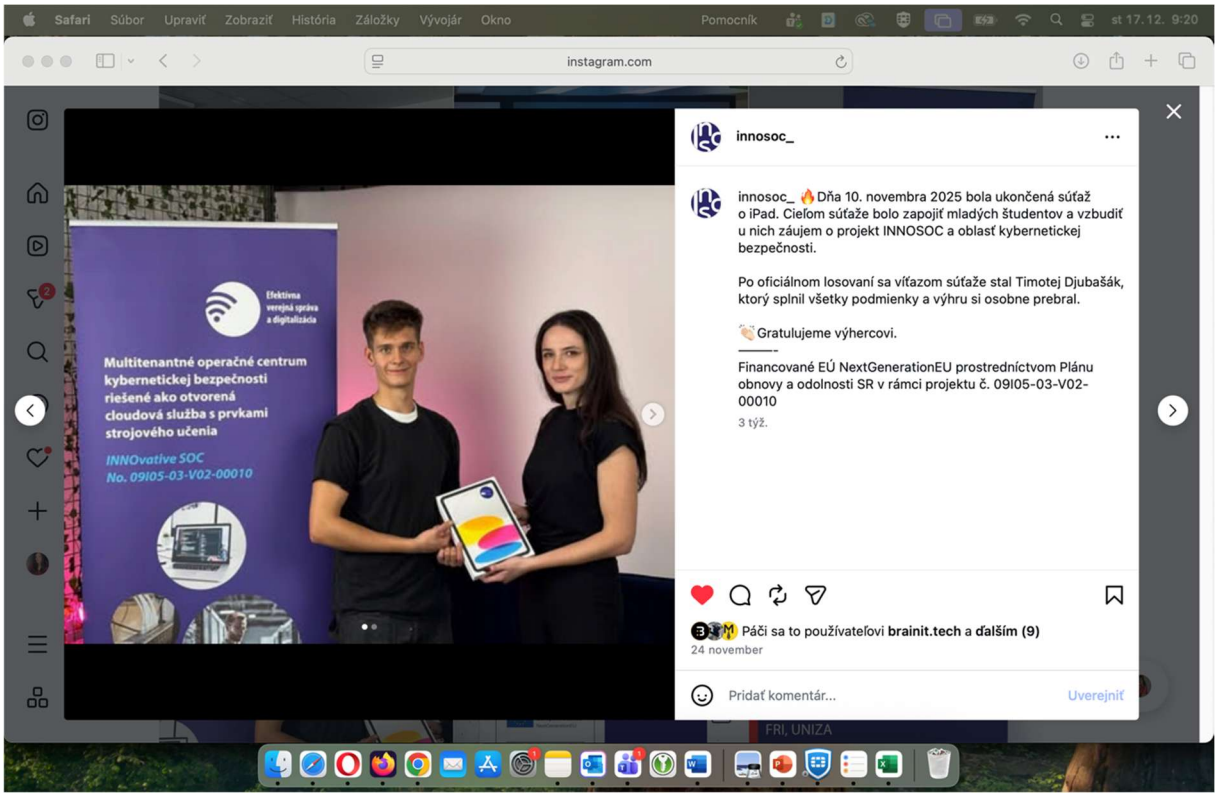


Figure 27:post on the Instagram profile @innosoc_: handover of the competition prize, Source: (BRAIN:IT, 2025)

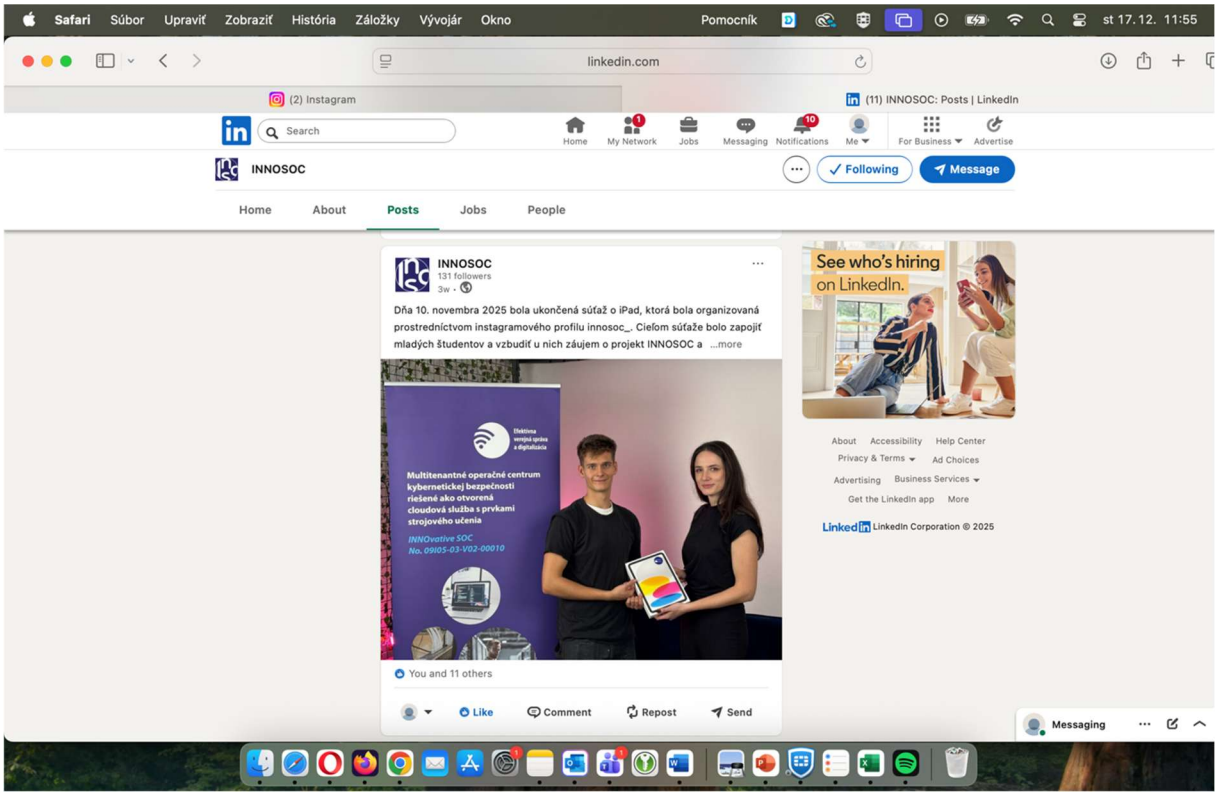


Figure 28: post on the LinkedIn profile @innosoc_: handover of the competition prize, Source: (BRAIN:IT, 2025)

4.2.4.14 Post about the presentation of the INNOSOC project at the student breakfast

On 28 November 2025, a post was published on the Instagram profile @innosoc_ informing about the student breakfast held on 4 November 2025 at the Faculty of Management Science and Informatics of the University of Žilina in cooperation with BRAIN:IT.

The aim of the post was to inform students about the informal presentation activity of the project, to raise awareness of the INNOSOC project among young people and to introduce them to the current state, outputs and further direction of the project in the field of cybersecurity.

The published content included:

- information about the student event and its informal character,
- presentation of the INNOSOC project to students of management and informatics programmes,
- communication of the importance of cybersecurity, the Security Operations Center and cloud technologies,
- visual documentation of the event supporting the visibility of the project,
- information about the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic.

The post represents a dissemination, popularization and recruitment output of the project, aimed at reaching the student target group, fostering interest in the topic of cybersecurity and strengthening the link between the research project, the academic environment and practice.

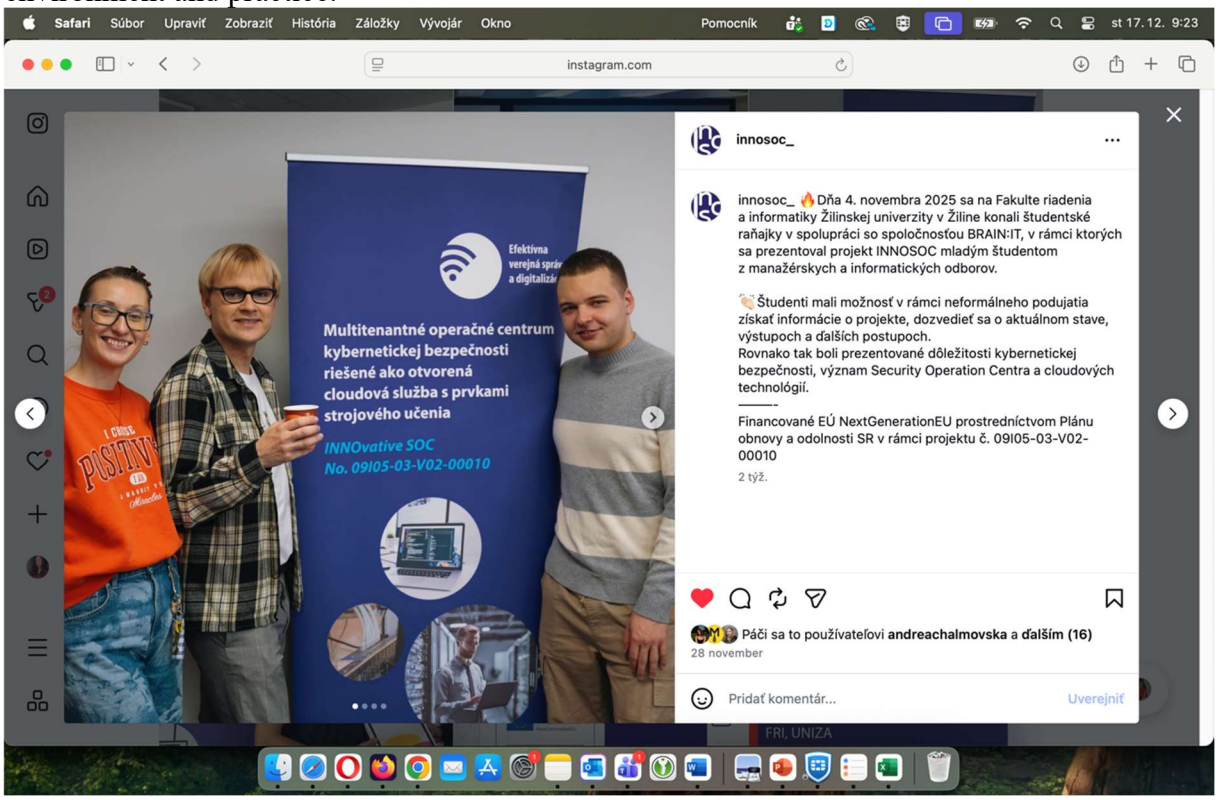


Figure 29:post on the Instagram account @innosoc_: presentation at the student breakfast, Source: (BRAIN:IT, 2025)

4.2.4.15 Post about the presentation of the INNOSOC project at Tomas Bata University in Zlín

On 10 December 2025, a post was published informing about the presentation of the INNOSOC project to students of the Faculty of Applied Informatics of Tomas Bata University in Zlín, which took place on 20 November 2025.

The aim of the post was to report on the presentation activity of the project carried out in the academic environment, to raise awareness of the INNOSOC project among students of

information technology study programmes and to explain to them the importance of cybersecurity in the context of digital transformation.

The published content included:

- information about the presentation of the project to students of applied informatics,
- introduction of the objectives, focus and benefits of the INNOSOC project,
- explanation of the importance of the Security Operations Center and modern IT security services,
- highlighting the need for IT specialists and the growing demand for experts in the field of cybersecurity,
- presentation of the principles and technologies used in the project,
- visual documentation from the lecture,
- information about the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic.

The post represents a dissemination, presentation and popularization output of the project which supports the link between the research project and the academic community, contributes to the dissemination of the project results and motivates students to take an interest in the field of cybersecurity and modern IT solutions.

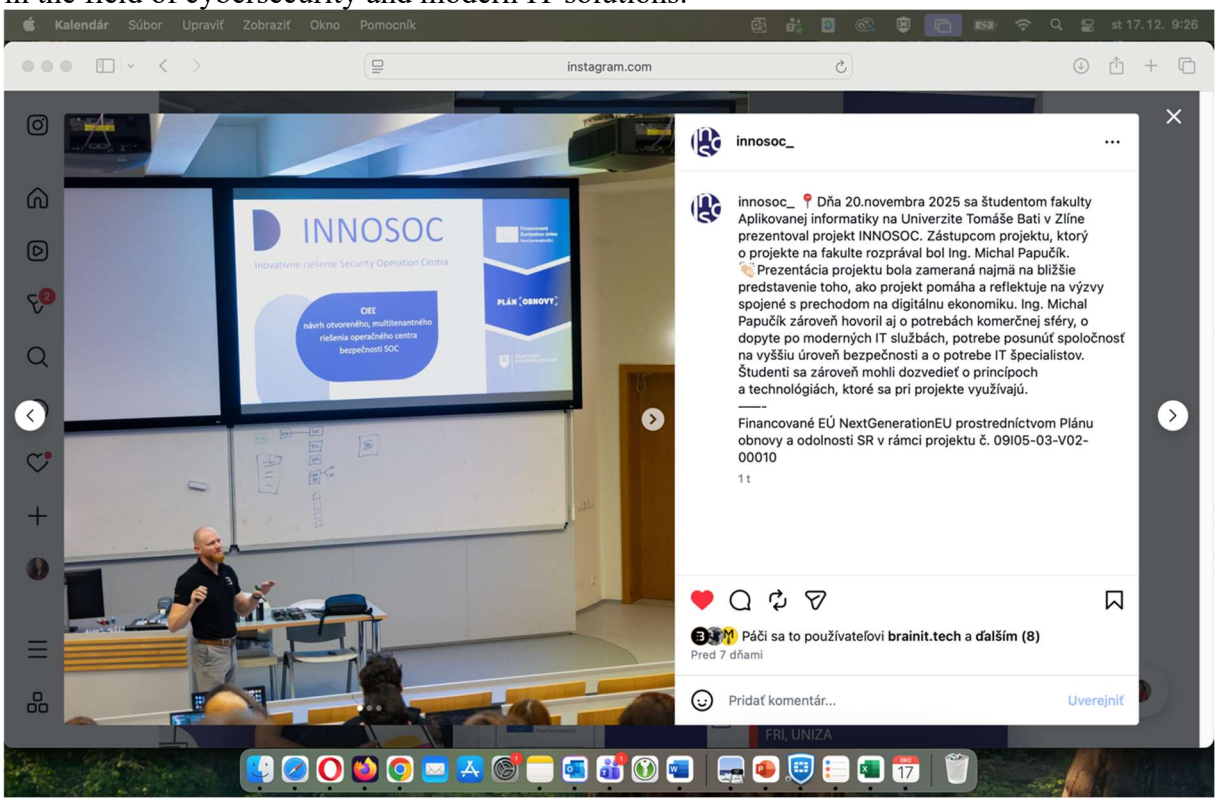


Figure 30: post on the Instagram profile @innosoc_: presentation at Tomas Bata University in Zlín, Source: (BRAIN:IT, 2025)

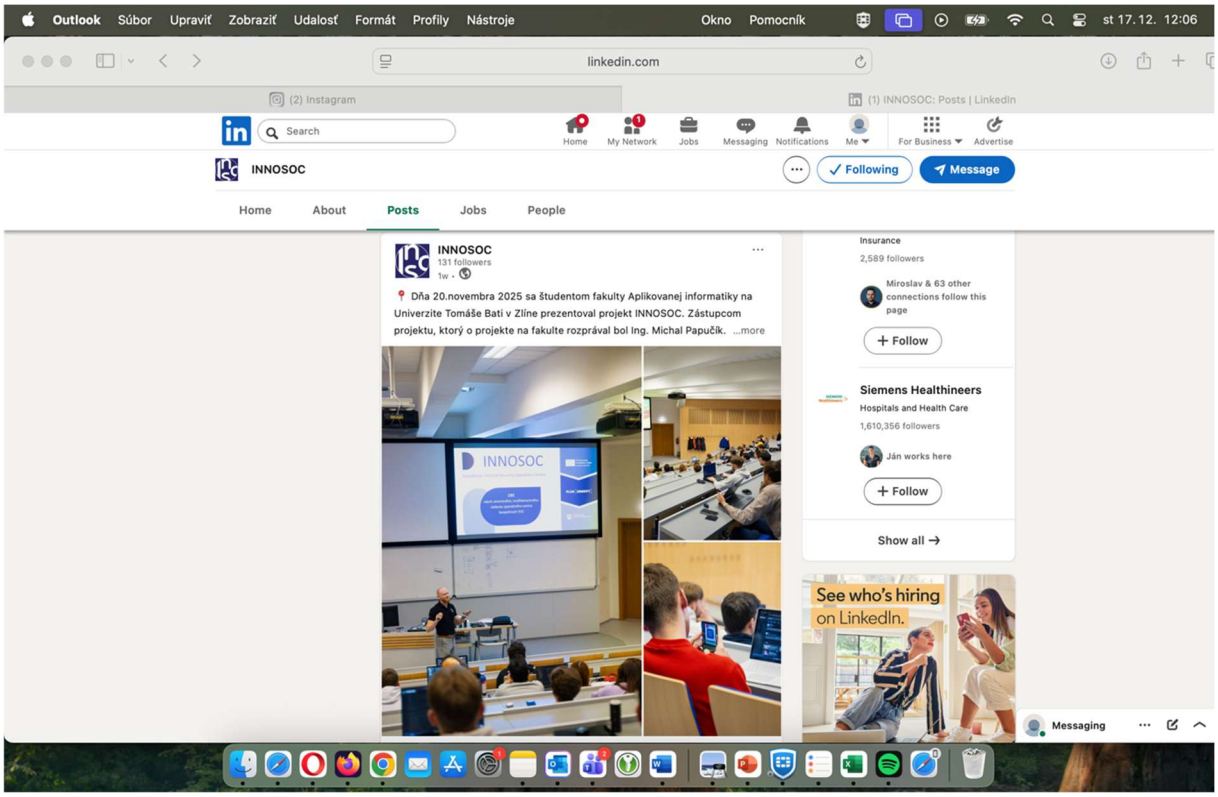


Figure 31:post on the LinkedIn profile @innosoc: presentation at Tomas Bata University in Zlín, Source: (BRAIN:IT, 2025)

4.2.4.16 Post about the presentation of the INNNOSC project at the Jozef Murgaš Secondary Technical School in Banská Bystrica

On 12 December 2025, a post was published informing about the presentation of the INNOSOC project at the Jozef Murgaš Secondary Technical School in Banská Bystrica, which took place on 28 November 2025.

The aim of the post was to inform the public about an educational activity aimed at raising awareness of cybersecurity among secondary school pupils and to explain to them the significance of the INNOSOC project in the context of protecting the digital space.

The published content included:

- information about the presentation of the project at the secondary school,
- introduction of the objectives and focus of the INNOSOC project,
- explanation of the importance of cybersecurity and current types of cyber attacks,
- presentation of the participating universities and project partners,
- the interactive nature of the presentation with active involvement of the pupils,
- visual documentation from the educational activity,
- information about the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic.

The post represents a dissemination, educational and popularization output of the project, aimed at reaching a younger target group, supporting digital literacy and building awareness of the importance of cybersecurity already at the level of secondary education.

The full text of the article can be found in Annex 9 – Article on the presentation of the INNOSOC project at the Jozef Murgaš Secondary Technical School in Banská Bystrica.

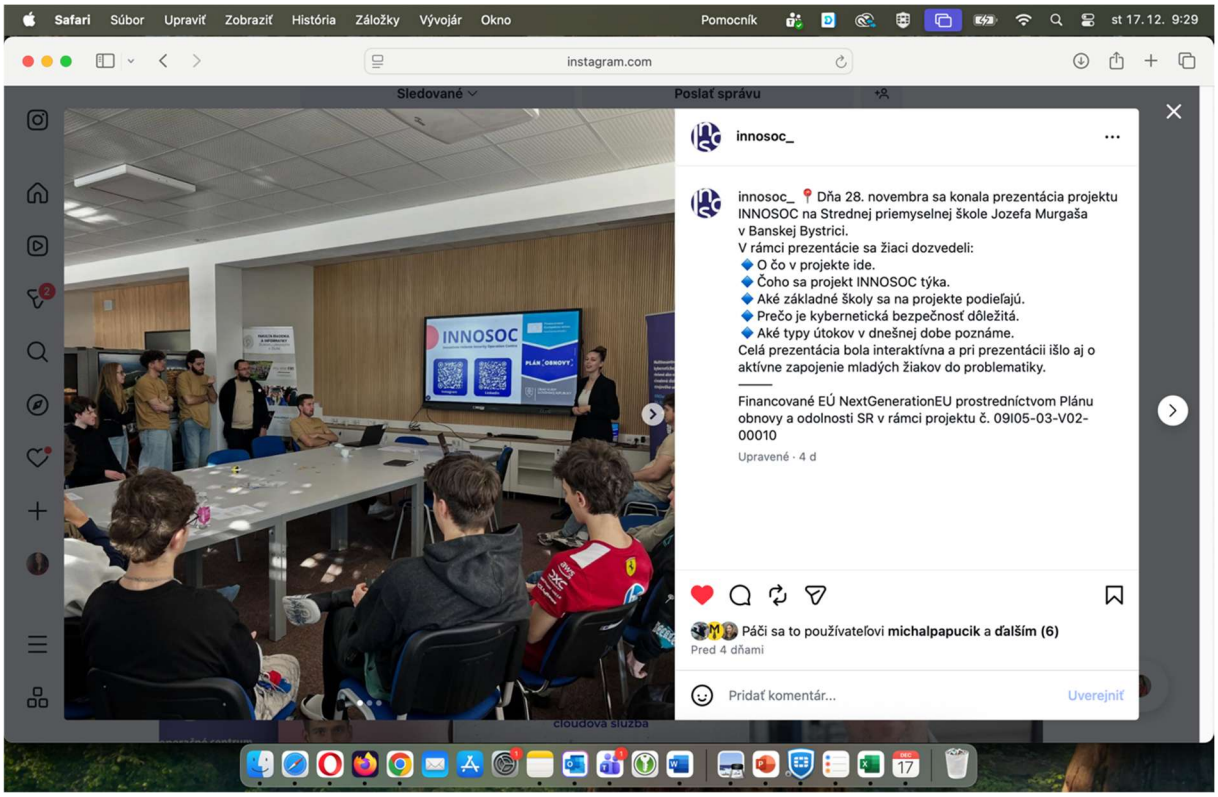


Figure 32: post on the Instagram profile @innosoc_: presentation at the Jozef Murgaš Secondary Technical School in Banská Bystrica, Source: (BRAIN:IT, 2025)

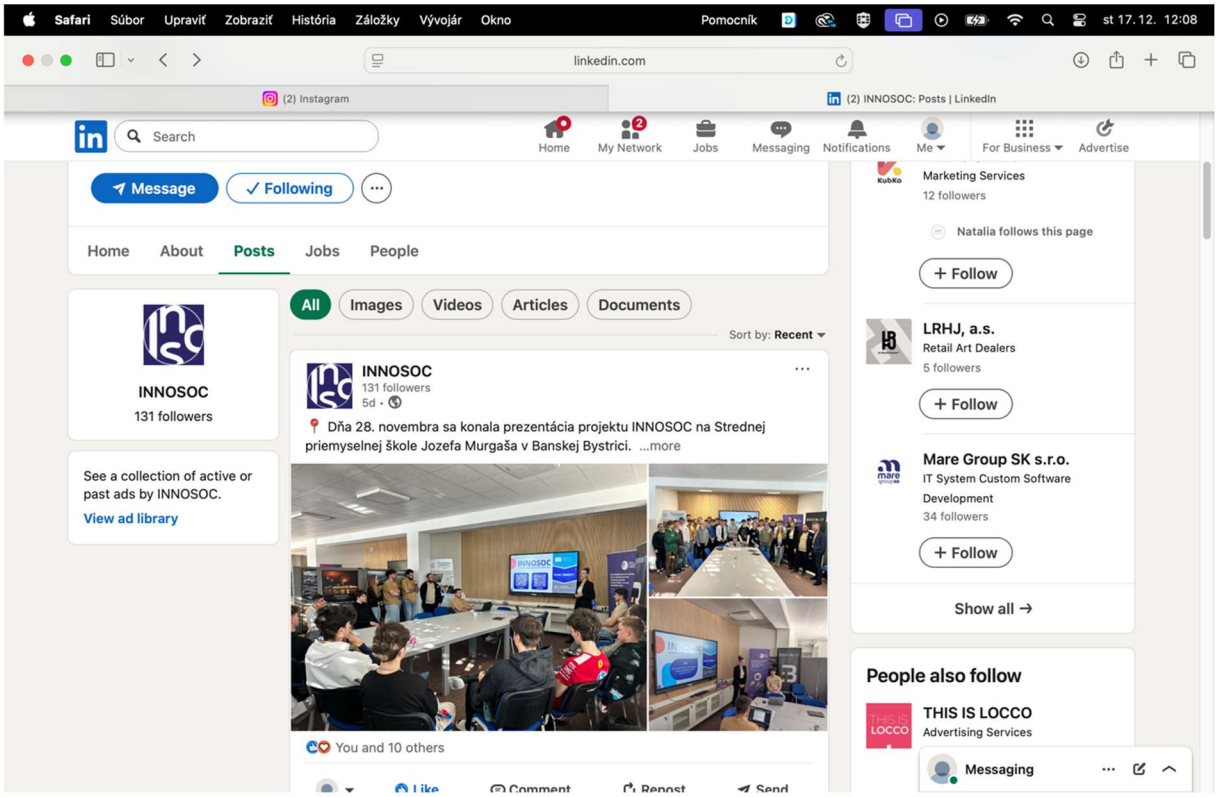


Figure 33: post on the LinkedIn profile @innosoc: presentation at the Jozef Murgaš Secondary Technical School in Banská Bystrica, Source: (BRAIN:IT, 2025)

4.3 Popularization texts

Popularization texts are a key tool for effectively conveying the expert knowledge and results of the INNOSOC project to a broad spectrum of target groups. Their main purpose is to transform complex technical information into an understandable and engaging form that will appeal not only to experts but also to the lay public, students and potential customers.

These texts will serve as bridges between the scientific research sphere and practical application, while taking into account the specifics of the individual target segments. For the professional public, the texts will contain technical details and methodologies, while for the general public they will be simplified and supplemented with practical examples and visual elements.

Popularization articles will be published primarily through the project website, where they will create a comprehensive source of information on cybersecurity, cloud technologies and the importance of SOC solutions. At the same time, these texts will be adapted for social networks in the form of shorter posts, infographics and interactive content.

Particular emphasis will be placed on the educational character of the texts, which will explain basic concepts such as "SOC", "multi-tenant architecture", "machine learning in cybersecurity" or "cloud services" in a way that is accessible to different levels of technical literacy. The aim is not only to inform but also to educate and motivate readers to take a deeper interest in cybersecurity issues.

The content strategy of the popularization texts will be based on the principle of gradually building awareness and trust. The texts will be structured into thematic units that will cover the basic concepts of cybersecurity, present the innovative solutions of the INNOSOC project and show their practical use in real scenarios. Each text will be supplemented with visual elements such as diagrams, infographics or illustrations that will make it easier to understand complex technical processes. The texts will also contain interactive elements such as questions for readers, quizzes or links to supplementary materials.

An important aspect of the popularization texts will also be their topicality and relevance to current trends in cybersecurity. The texts will be regularly updated with new knowledge gained during the implementation of the project, case studies of successful implementations and reflections on current cyber threats. This approach will ensure that the content remains attractive and useful for readers in the long term, while the project website will become a recognized source of information in the field of cybersecurity in Slovakia and in the wider European context.

Topics selected for the first popularization texts on the INNOSOC website:

- Cybersecurity: Basics and tips on how to protect yourself against online threats;
- Security Operation Center: what it is and how does it protect your company?;
- Get to know the most common internet threats for young people: Prevention and protection options;
- What the cloud is and what it is used for: Basic types and advantages of cloud storage;
- Computer security and data protection – principles and practical examples;
- Linking AI and cybersecurity in practice;
- Cyber attacks: How they are changing and why they pose an increasingly greater risk.

4.3.1 Activities carried out

This chapter contains a description of the individual popularization articles that were published on the official INNOSOC website.

4.3.1.1 Popularization article on Cybersecurity: Basics and tips on how to protect yourself against online threats

On 3 September 2025, a popularization article on the topic Cybersecurity: Basics and tips on how to protect yourself against online threats was added to the "News" section. The aim of the article was to explain the basic principles of cybersecurity to the general public in an understandable and accessible form, to point out current cyber threats and to emphasize the importance of prevention in the digital environment.

The content of the article includes:

- an explanation of the concept of cybersecurity and its importance for individuals and organizations,
- a description of the most common types of cyber attacks and threats (e.g. phishing, malware, social engineering, DDoS attacks),
- identification of the types of data at risk, including personal, health and financial information,
- the division of protection into the human and the technological factor,
- an overview of the basic principles of cybersecurity, such as strong passwords, two-factor authentication, regular updates, data backup and the use of antivirus software and a firewall,
- emphasis on prevention as a key element of protection against cyber risks.

The article serves as an educational and awareness-raising output of the project, the aim of which is to raise awareness of cybersecurity, promote responsible user behaviour in the online space and contribute to reducing the risks associated with digital threats.

The full text of the article can be found in Annex 10 – Article: Cybersecurity: Basics and tips on how to protect yourself against online threats.

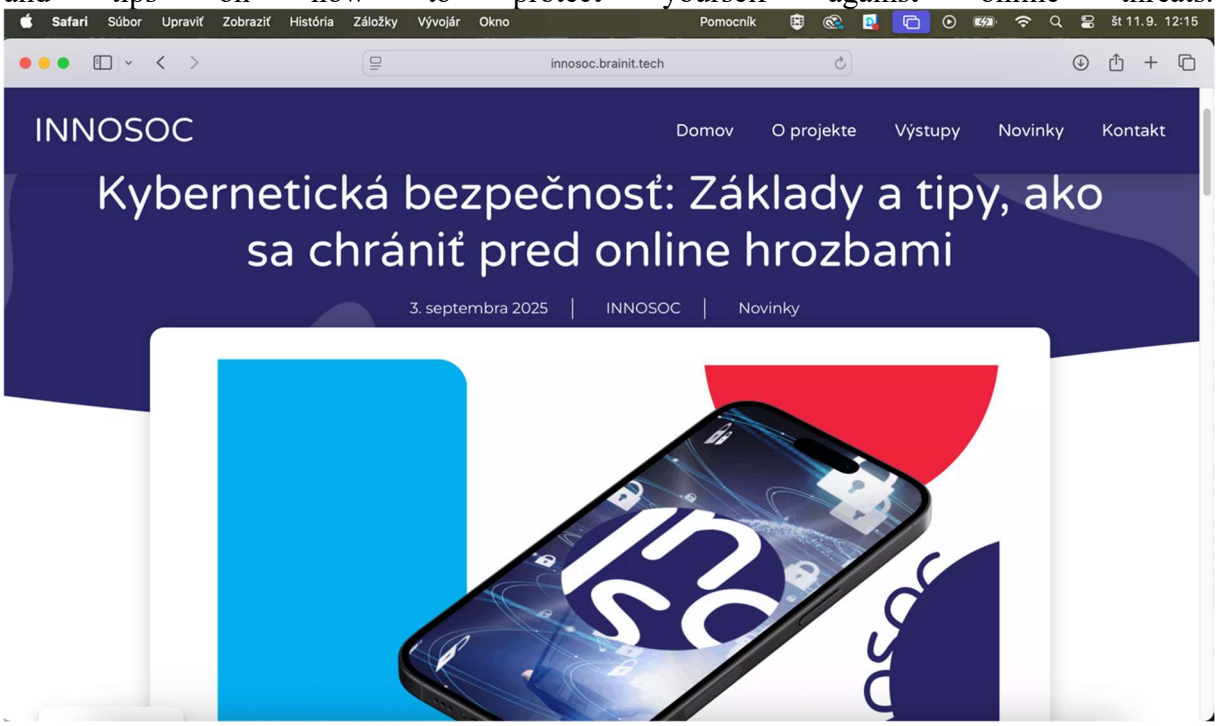


Figure 34 Popularization article on the topic of cybersecurity, Source: (BRAIN:IT, 2025)

To reach a larger audience, the same popularization text was published on the LinkedIn page @INNOSOC with the aim of reaching professionals and university students. This article was published on 8/9/2025.

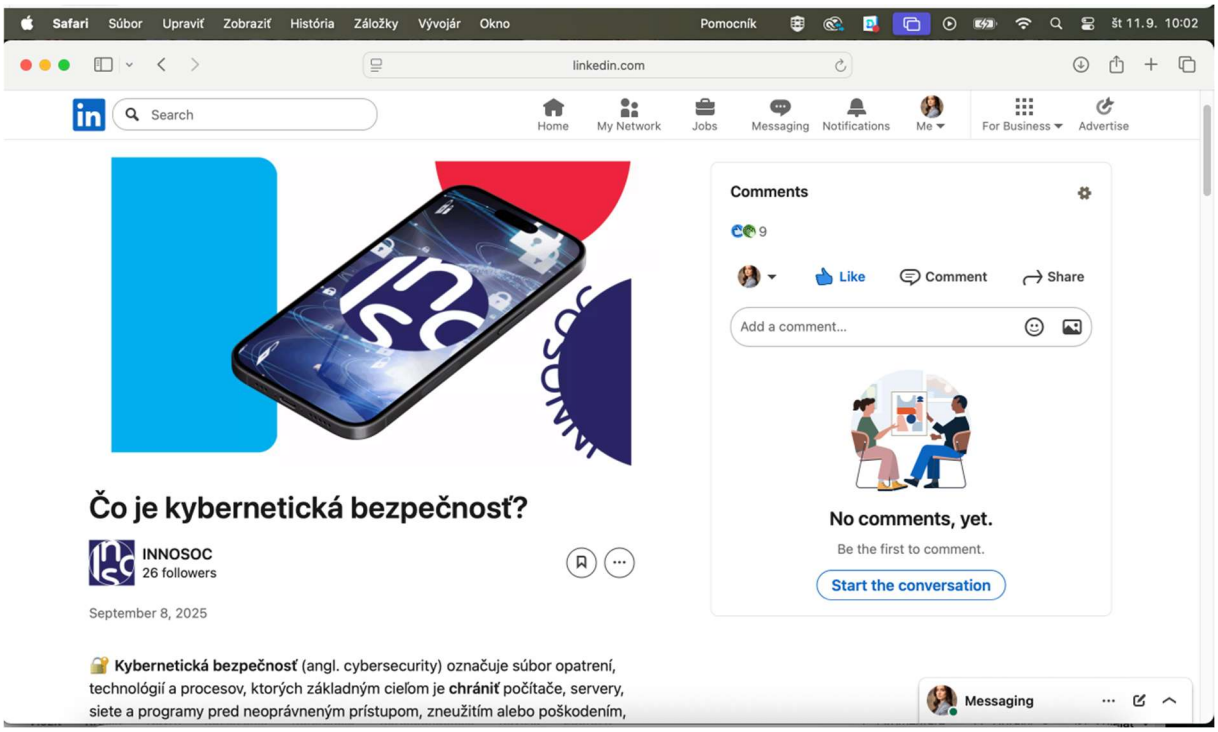


Figure 35 Popularization article on the topic of cybersecurity on the LinkedIn page @INNOSOC, Source: (BRAIN:IT, 2025)

4.3.1.2 Popularization article on Security Operations Center: what it is and how does it protect your company?

On 10 September 2025, an educational article on the topic "Security Operations Center: what it is and how it protects your company?" was published in the "News" section. The aim of the article was to introduce the concept of the Security Operations Center as a key element of a modern approach to cybersecurity and to explain its importance in protecting the digital assets of organizations in an environment of growing cyber threats.

The content of the article focuses in particular on:

- an explanation of the role of the SOC as a centralized, round-the-clock security centre,
- defining the main mission of the SOC, which is to minimize the impact of cybersecurity incidents and to protect the organization proactively,
- a description of how the SOC works, including the work of security analysts and the use of advanced security technologies,
- an introduction to the basic SOC models (internal, external and hybrid),
- an overview of the main functions of the Security Operations Center, such as incident monitoring and detection, security incident management and problem management,
- emphasizing the importance of processes, documentation and internal security policies as part of the effective operation of the SOC.

The article serves as a professional and awareness-raising output of the project, the aim of which is to increase awareness of the practical operation of the Security Operations Center, to promote a systematic approach to cybersecurity in organizations and to highlight the importance of prevention, monitoring and security incident management in the digital environment.

The full text of the article can be found in Annex 11 – Article: Security Operations Center: what it is and how does it protect your company?



Figure 36 Popularization article on the topic of the Security Operations Center, Source: (BRAIN:IT, 2025)

4.3.1.3 Popularization article on Get to know the most common internet threats for young people: Prevention and protection options

As part of the project, an educational and awareness-raising article focused on the risks of the digital and online environment for the young generation was published on 22 September and posted on the website in the "News" section. The aim of the article was to raise awareness of young people's safety in the online space, to point out the most common digital threats to which young people are exposed and to provide practical recommendations for prevention and protection in everyday digital life.

The content of the article focuses in particular on:

- the characteristics of the current generation growing up in the information and technology age,
- identification of the main threats of the digital world for young people, such as inappropriate and dangerous content, communication on social media, sharing of intimate content, internet fraud, online bullying, discrimination and hate speech,
- risks associated with dependence on technology, social media and digital relationships, including psychological impacts (e.g. FOMO, FOBO, social isolation),
- the importance of prevention and education in the field of digital safety as a fundamental tool for protecting young people,
- safety recommendations for responsible behaviour in the online space, especially when sharing personal data and photographs and when communicating with strangers,
- emphasizing the role of the family and the home environment as a key element in the prevention of digital risks.

The article represents an educational and preventive output of the project, the aim of which is to promote safe and responsible behaviour of young people in the digital environment, strengthen the awareness of parents and teachers and contribute to building healthy boundaries and safe online behaviour in today's society.

The full text of the article can be found in Annex 12 – Article: Get to know the most common internet threats for young people: Prevention and protection options.

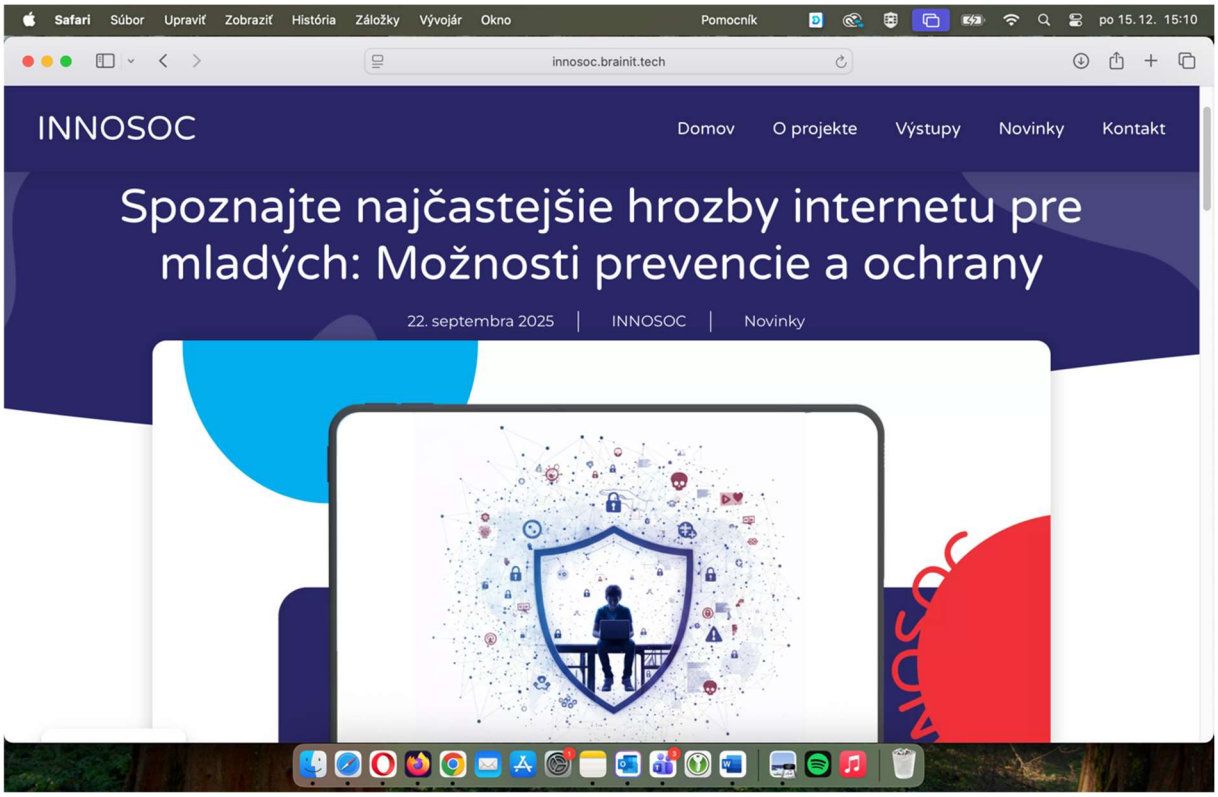


Figure 37: Article on the topic Get to know the most common internet threats for young people: Options for prevention and protection, Source: (BRAIN:IT, 2025)

4.3.1.4 Popularization article on What the cloud is and what it is used for: Basic types and advantages of cloud storage

As part of the project, a professional educational article focused on cloud services and modern methods of storing and managing data was created and published on the website created within the project. The aim of the article was to explain in an understandable form the concept of the cloud and its practical use in everyday and corporate environments, and to point out the basic advantages and risks associated with the use of cloud solutions.

The content of the article focuses in particular on:

- an explanation of the concept of the cloud and the principles of how cloud services work,
- an overview of the forms of cloud use, such as web hosting, file sharing, software distribution and cloud computing,
- an introduction to the basic types of cloud solutions (public, private and hybrid cloud), including their characteristics,
- a comparison of the advantages and disadvantages of cloud services in terms of productivity, efficiency, costs and security,
- drawing attention to security risks and the importance of protecting sensitive personal and corporate data when storing data in the cloud.

The article represents a professional and awareness-raising output of the project, the aim of which is to increase users' digital literacy, support informed decision-making when choosing cloud solutions and contribute to a better understanding of modern technologies for storing and managing data in the digital environment.

The full text of the article can be found in Annex 13 – Article: What the cloud is and what it is used for: Basic types and advantages of cloud storage.

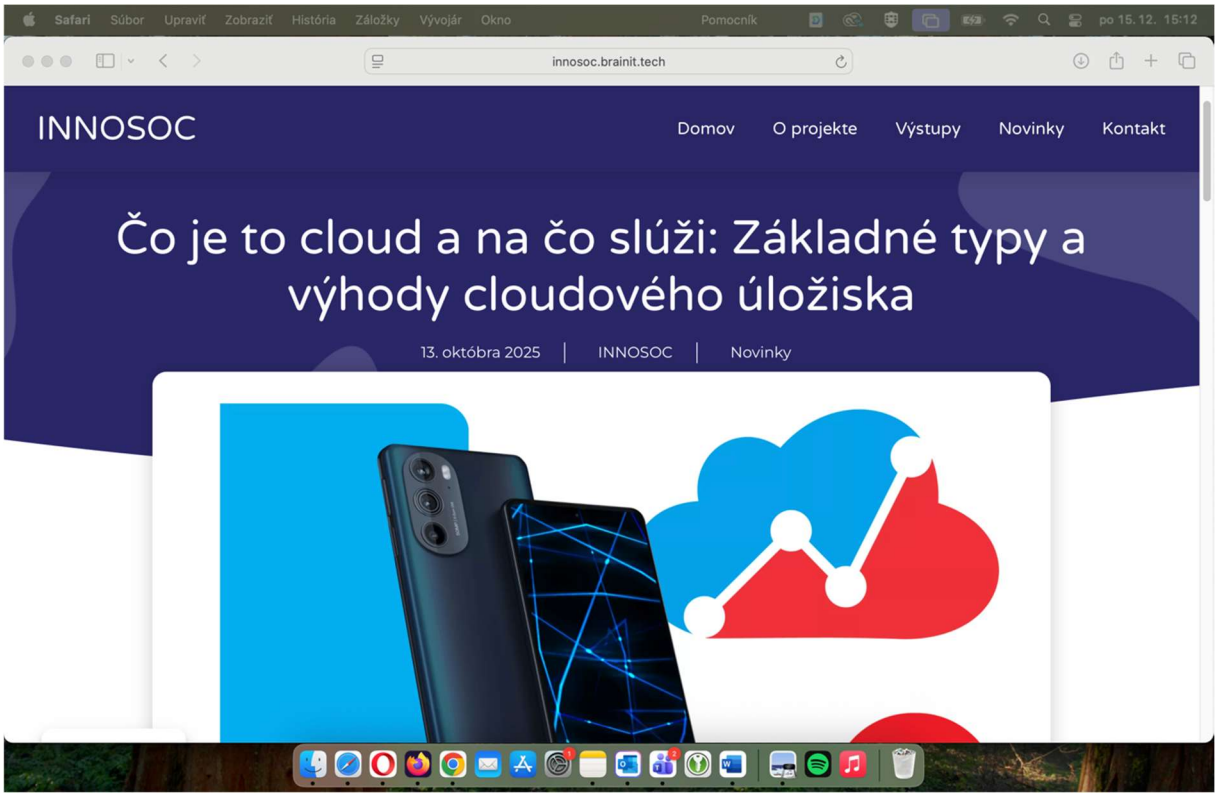


Figure 38: Article on the topic What the cloud is and what it is used for: Basic types and advantages of cloud storage, Source: (BRAIN:IT, 2025)

4.3.1.5 Popularization article on Computer security and data protection – principles and practical examples

On 10 November 2025, a professional educational article focused on computer security and data protection was created and published on the website created within the project. The aim of the article was to explain the basic principles of protecting data and information in the online environment and to introduce the concept of the security triad (CIA – confidentiality, integrity, availability) as the key foundation of every security strategy, both in organizations and in everyday digital life.

The content of the article focuses in particular on:

- an explanation of the importance of computer security and cybersecurity when working with digital data,
- defining the three basic principles of the security triad – confidentiality, integrity and availability,
- linking data protection principles to the applicable Slovak and European legislation in the field of personal data protection,
- the practical application of the individual principles in everyday practice through specific security measures,
- examples of technical and organizational data protection tools, such as encryption, access control, multi-factor authentication, electronic signature, backup and availability monitoring,
- emphasizing the need for balance between the individual elements of the security triad when designing security policies.

The article represents a professional and educational output of the project, the aim of which is to raise awareness of data and information protection, promote responsible user

behaviour in the digital environment and provide a practical basis for building effective security measures in organizations and among individuals.

The full text of the article can be found in Annex 14 – Article: Computer security and data protection – principles and practical examples.

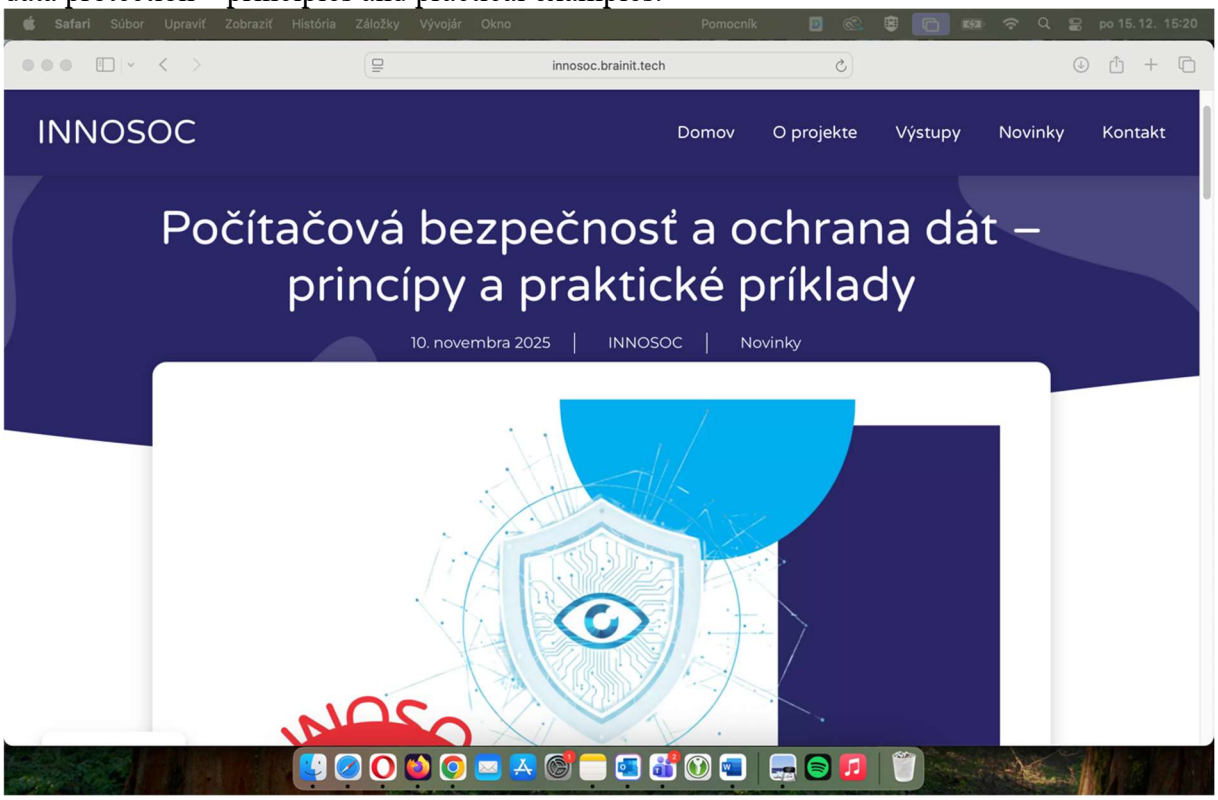


Figure 39: Article on the INNOSOC website on the topic Computer security and data protection – principles and practical examples, Source: (BRAIN:IT, 2025)

4.4 Audiovisual content

Videos and other audiovisual content are a suitable form for better capturing attention, especially when communicating simpler ideas to the general public, university students and secondary school students.

Their main role is to present complex technical processes and the advantages of the SOC solution in a dynamic and engaging way through combined audiovisual content capable of reaching a wide range of target groups. They will be shared mainly on social networks and the project website.

The videos will be adapted to the specifics of the individual platforms and target segments: shorter formats with a strong visual side will be created for social networks, while more detailed and technically oriented videos will be prepared for the website and professional presentations. The content will include explanations of how SOC systems work, demonstrations of real-time cyber threat detection, interviews with experts and testimonials from the project partners.

Promotional videos will serve as a key tool for educating students and increasing the digital literacy of the general public, explaining the basic concepts of cybersecurity through practical demonstrations and visual metaphors. Particular emphasis will be placed on demonstrating the multi-tenant architecture and the advantages of cloud solutions, which will be presented in the form of understandable animations and real use scenarios.

Strategically, the videos will be divided into several categories according to content and purpose: introductory videos presenting the project and its objectives, technical tutorials and

demonstrations for experts, educational videos for students and the lay public, as well as testimonials and case studies for potential customers. Each video will be optimized for different platforms, taking into account their specific requirements for format, length and content style.

The production of the promotional videos will involve the use of modern and professional production tools for visualization, animation and post-production, which will make it possible to present abstract cybersecurity concepts effectively. The videos will contain professionally voiced commentary, high-quality graphic elements and music that will underline the innovative character of the project.

At the same time, the videos will be available with subtitles in Slovak or English, which will extend their reach to the international level and increase their usability for various target groups.

4.4.1 Activities carried out

4.4.1.1 Creating an account on the YouTube platform

For publishing videos – especially expert interviews, video tutorials, testing videos and videos of various activities in the form of events – a channel named @INNOSOC was created on the YouTube platform. It will serve as a supporting tool and will be used for sharing the aforementioned videos in other channels, such as the website. The channel was also created to allow archiving of all video content and its easy accessibility for both the professional and the lay public.

The full transcript of the video can be found in Annex 15 – Interview with Ing. Michal Papučík.

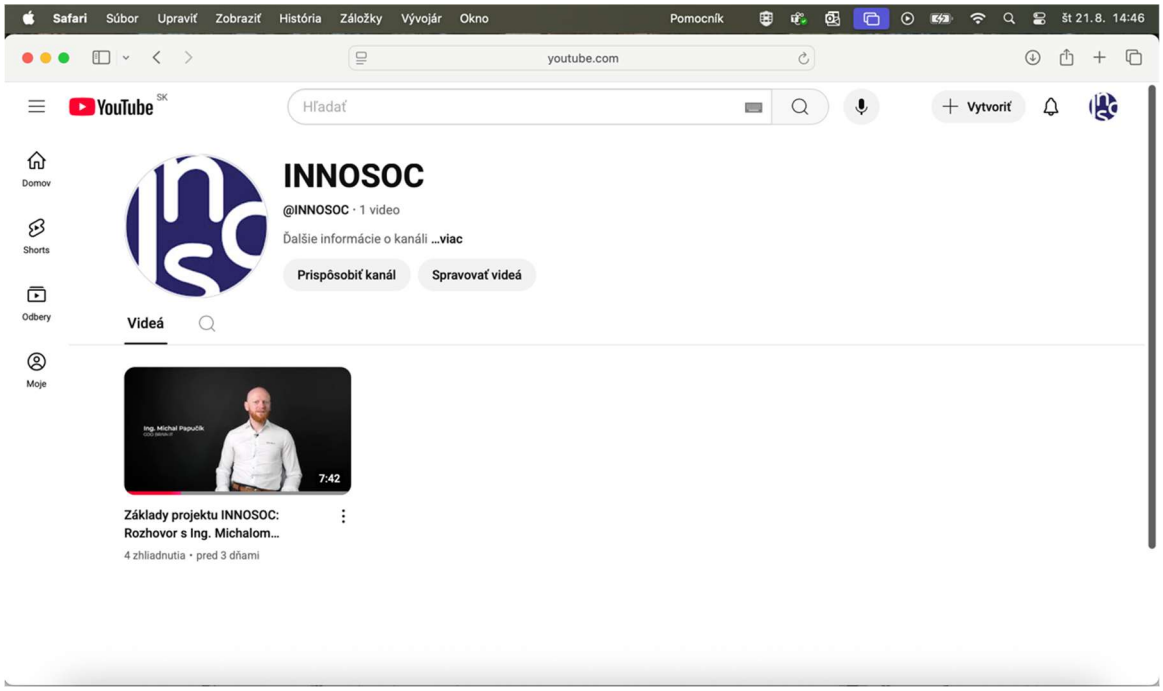


Figure 40: YouTube channel @INNOSOC, Source: (BRAIN:IT, 2025)

4.4.1.2 Video interview with Ing. Michal Papučík

The aim of the video interview with Ing. Michal Papučík, COO of BRAIN:IT, who participates in the project as a researcher, analyst and information systems architect, was to provide the general public with basic information about the project. The video interview informs about the objective, the need for the project, the challenges the project responds to, its

benefits, the technologies used, the link between the academic community and the business sphere, and the methods and international practices used in the project, and also offers a personal view of the project and the experience of Ing. Michal Papučík.

The full transcript of the interview with Ing. Michal Papučík can be found in Annex 15 - Interview with Ing. Michal Papučík.

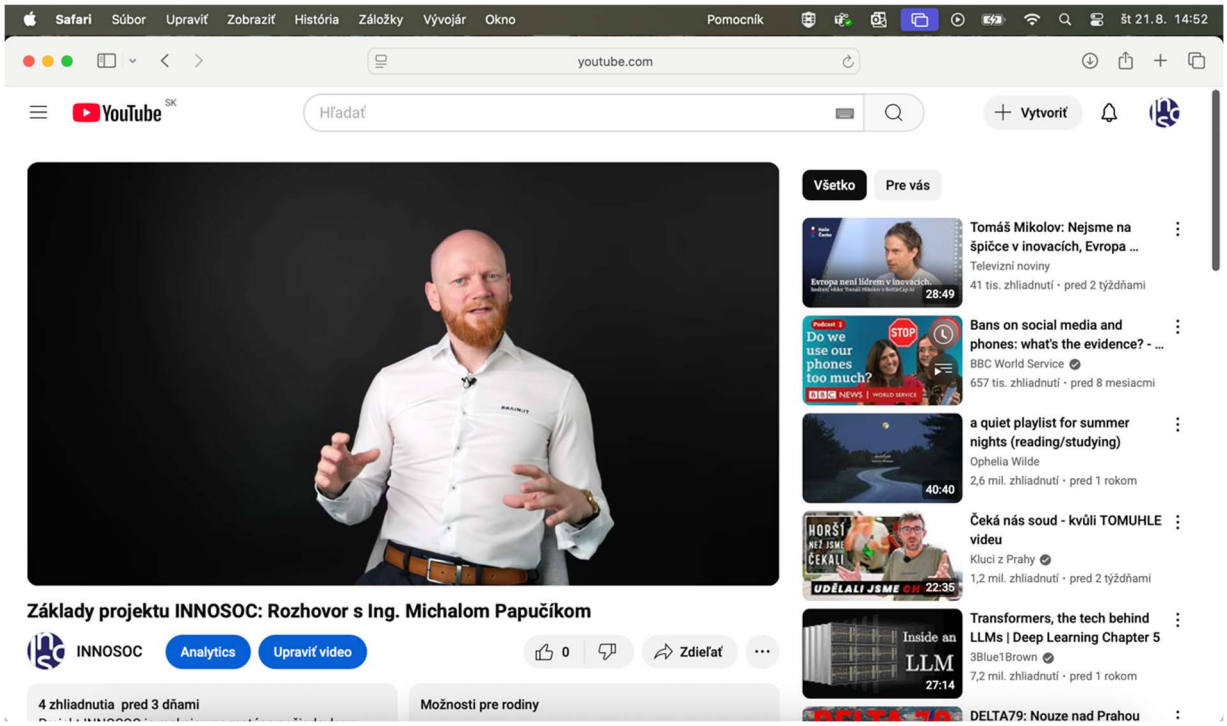


Figure 41: Video interview with Ing. Michal Papučík, Source: (BRAIN:IT, 2025)

4.4.1.2.1 Video interview with prof. Ing. Pavel segeč, PhD.

The aim of the interview was to explain the importance of cybersecurity in today's digital environment, to point out the growing cyber threats and to explain the role of the INNOSOC project in building systematic and centralized protection of organizations and educational institutions.

The content of the interview focuses in particular on:

- the importance of cybersecurity for organizations of all sizes in the context of growing digitalization,
- the role of the Faculty of Management Science and Informatics of UNIZA as the main project partner and provider of scientific research and development capacities,
- identification of the most common cyber threats, such as phishing, ransomware and advanced persistent threats (APT),
- explanation of the concept of the Security Operations Center (SOC) as a central element of protection, built on the pillars of people, processes and technologies,
- the impacts of the new NIS2 directive on requirements in the area of management and reporting of cybersecurity incidents,
- the practical operation of SOC systems based on the collection, correlation and analysis of large volumes of security data in real time.

The interview is a professional, presentational and awareness-raising output of the project that links the scientific research perspective with practical impacts on the security of

organizations. At the same time, it serves as a tool for raising awareness of the importance of cybersecurity and of the benefits of the INNOSOC project for both academic and applied practice.

The full transcript of the interview can be found in Annex 16 – Interview with prof. Ing. Pavel Segeč, PhD.

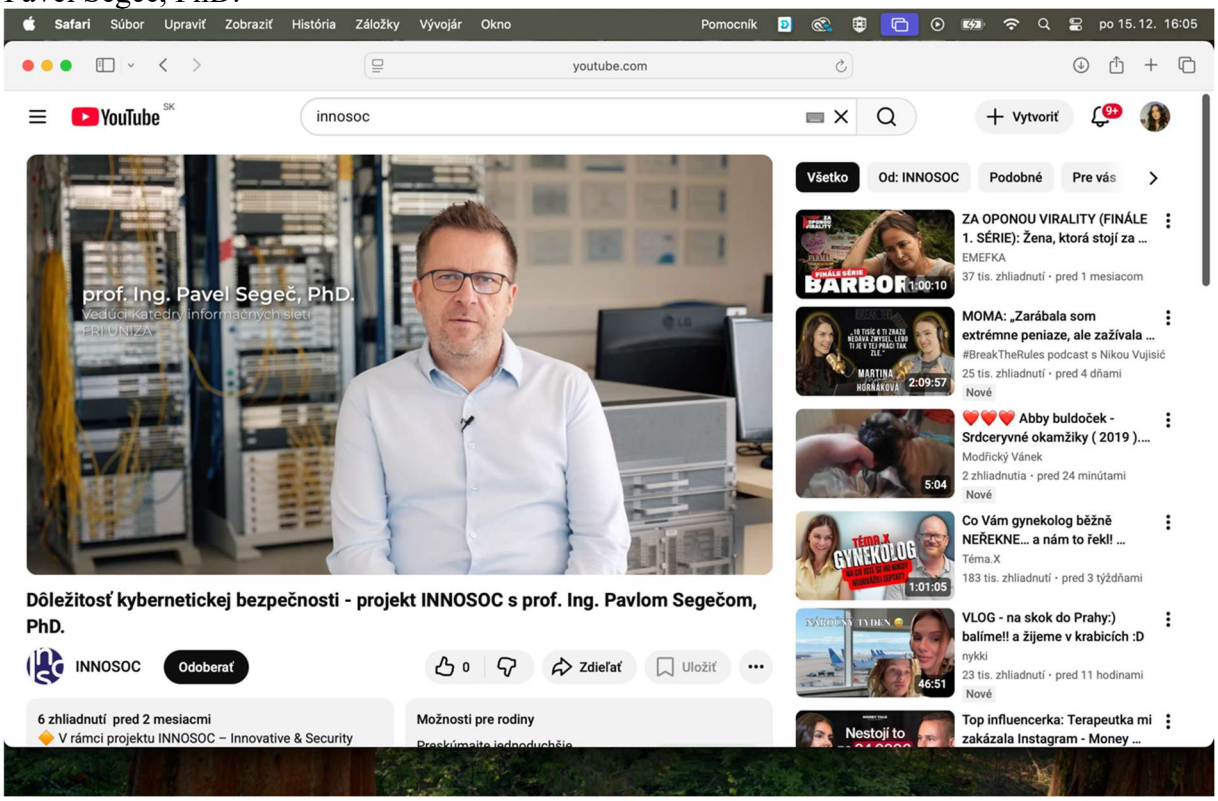


Figure 42: Video interview with prof. Ing. Pavel Segeč, PhD., Source: (BRAIN:IT, 2025)

4.5 Promotional materials

Promotional materials such as brochures, roll-ups, leaflets and other printed or digital promotional elements are an irreplaceable part of the comprehensive communication strategy of the INNOSOC project. These materials serve as tangible carriers of information that allow potential customers, partners and other target groups to obtain a complete overview of the project outside the online environment as well.

Their main role is to present, in a visually attractive and professional manner, the key advantages of the SOC solution, the technical specifications and the business potential of the project at personal meetings, conferences and business negotiations.

The design and content of the promotional materials will be strictly differentiated according to the individual target segments and the purpose of use. Technically oriented brochures with detailed architectural diagrams and research outputs will be prepared for the professional public.

For potential customers from among small and medium-sized enterprises, business-oriented leaflets will be created highlighting the cost-benefit analysis and the practical benefits of the SOCaaS solution. Colourful and visually engaging materials with gamification elements and motivational elements for their future career in cybersecurity will be intended for students.

Promotional materials will play a particularly important role in direct sales activities aimed at potential customers. Roll-ups and presentation brochures will be an indispensable tool at business meetings, where they will serve as visual support for sales presentations.

The materials will be available at professional conferences, university events and on the premises of partner organizations.

Digital versions will be available for download on the project website and will be optimized for various devices and formats. Each material will contain QR codes linking to the website and specific landing pages for measuring conversions and the effectiveness of individual campaigns.

4.5.1 Activities carried out

4.5.1.1 INNOSOC information leaflet

For the purposes of presenting the project and raising awareness of it, an information leaflet was created which communicates basic information about the project, such as its objective, sub-objectives and the issues to which the INNOSOC research project responds.



Figure 43: INNOSOC project information poster, Source:

4.5.1.2 Information poster for the symposium

A poster was created to communicate the organization of the INNOSOC symposium on the topic "Possibilities of artificial intelligence in cybersecurity", which will take place on 18 December 2025 on the premises of the University of Žilina. The information poster communicates the date, time, venue and topic of the symposium.



Figure 44: Information poster about the INNOSOC symposium, Source:

5 List of sources

BRAIN:IT. (16 October 2025). *innosoc.com*. Available on the Internet: Interview with prof. Ing. Pavel Segeč: https://innosoc.brainit.tech/kyberneticka-bezpecnost-uz-nie-je-len-temou-pre-velke-firmy/

BRAIN:IT. (2025). *innosoc.brainit.tech*. Available on the Internet: INNOSOS: https://innosoc.brainit.tech

BRAIN:IT. (11 November 2025). *innosoc.brainit.tech*. Available on the Internet: Student event FRIčkovica: https://innosoc.brainit.tech/studentska-udalost-frickovica/

BRAIN:IT. (17 November 2025). *innosoc.brainit.tech*. Available on the Internet: Home About the project Outputs News Contact Symposium – cybersecurity as an open cloud service: https://innosoc.brainit.tech/sympozium-kyberneticka-bezpecnost-ako-otvorena-cloudova-sluzba/

BRAIN:IT. (24 November 2025). *innosoc.brainit.tech*. Available on the Internet: iPad competition: https://innosoc.brainit.tech/sutaz-o-ipad-vyhlasenie-vitaza/

BRAIN:IT. (28 November 2025). *innosoc.brainit.tech*. Available on the Internet: presentation at the student breakfast: https://innosoc.brainit.tech/prezentacia-projektu-innosoc-na-studentskych-ranajkach-4-november-2025/

BRAIN:IT. (9 December 2025). *innosoc.brainit.tech*. Available on the Internet: presentation at Tomas Bata University in Zlín: https://innosoc.brainit.tech/prezentacia-projektu-na-fakulte-aplikovanej-informatiky-na-univerzite-tomase-bati-v-zline-20-november-2025/

BRAIN:IT. (12 December 2025). *innosoc.brainit.tech*. Available on the Internet: presentation at the Jozef Murgaš Secondary Technical School in BB: https://innosoc.brainit.tech/prezentacia-na-strednej-priemyselnej-skole-jozefa-murgasa-v-banskej-bystrici-28-novembra-2025/

BRAIN:IT. (13 October 2025). *innosoc.brainit.tech*. Available on the Internet: What the cloud is and what it is used for: Basic types and advantages of cloud storage: https://innosoc.brainit.tech/co-je-to-cloud-ulozisko/

BRAIN:IT. (10 November 2025). *innosoc.brainit.tech*. Available on the Internet: Computer security and data protection – principles and practical examples: https://innosoc.brainit.tech/pocitacova-bezpecnost-a-ochrana-dat/

BRAIN:IT. (2025). *Instagram @brainit.tech*. Available on the Internet: website post: https://www.instagram.com/p/DLXH_-MuL6_/

BRAIN:IT. (16 September 2025). *instagram @innosoc_*. Available on the Internet: cybersecurity quiz: https://www.instagram.com/p/DOxr6HqiFeJ/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (2025). *Instagram @innosoc_*. Available on the Internet: post published on 5/9/2025: https://www.instagram.com/reel/DONouL4owoN/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (2025). *Instagram @innosoc_*. Available on the Internet: post in the form of a quiz: https://www.instagram.com/p/DOV08sECMeh/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (2025). *Instagram @inosoc_*. Available on the Internet: post on the partners' meeting of 15/7/2025: https://www.instagram.com/p/DMpmaMAoMCj/?img_index=1

BRAIN:IT. (2025). *Instagram INNOSOC*. Available on the Internet: https://www.instagram.com/innosoc_/

BRAIN:IT. (3 October 2025). *Instagram account @innosoc_*. Available on the Internet: iPad competition: https://www.instagram.com/p/DPVvB7DiMUs/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (3 October 2025). *Instagram profile @innosoc_*. Available on the Internet: iPad competition: https://www.instagram.com/p/DPVvB7DiMUs/?utm_source=ig_web_copy_link&igsh=MWNyMTNjNWR2angwdg==

BRAIN:IT. (17 October 2025). *Instagram profile @innosoc_*. Available on the Internet: interview with prof. Ing. Pavel Segeč, PhD.: https://www.instagram.com/reel/DP5wdgFiIav/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (18 November 2025). *Instagram profile @innosoc_*. Available on the Internet: announcement of the symposium: https://www.instagram.com/p/DRMSZ4TiEZ9/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (24 November 2025). *Instagram profile @innosoc_*. Available on the Internet: competition prize-giving: https://www.instagram.com/p/DRb0_wviDyq/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (28 November 2025). *Instagram profile @innosoc_*. Available on the Internet: presentation at the student breakfast: https://www.instagram.com/p/DRmQIOPiBFh/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (9 December 2025). *Instagram profile @innosoc_*. Available on the Internet: presentation at Tomas Bata University in Zlín: https://www.instagram.com/p/DSCxvhYiKGb/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (12 December 2025). *Instagram profile @innosoc_*. Available on the Internet: presentation at the Jozef Murgaš Secondary Technical School in Banská Bystrica: https://www.instagram.com/p/DSKFfyniMg1/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (2025). *Istagram @innosoc_*. Available on the Internet: post of 21/8/2025: https://www.instagram.com/reel/DNnIx9toFCU/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Available on the Internet: post on the partners' meeting of 15/7/2025: https://www.linkedin.com/company/108018118/admin/page-posts/published/

BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Available on the Internet: post published on 21/8/2025: https://www.linkedin.com/feed/update/urn:li:activity:7364224462050795520

BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Available on the Internet: post published on 5/9/2025: https://www.linkedin.com/feed/update/urn:li:activity:7369610244873674752

BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Available on the Internet: Popularization text on cybersecurity: https://www.linkedin.com/pulse/čo-je-kybernetická-bezpečnosť-innosocinnosoc-dt6we/?trackingId=cIrSBt0YN2qcFTrPUNfmvw%3D%3D

BRAIN:IT. (2025). *LinkedIn INNOSOC*. Available on the Internet: https://www.linkedin.com/company/innosocinnosoc/posts/?feedView=all

BRAIN:IT. (17 October 2025). *LinkedIn profile @innosoc*. Available on the Internet: interview with prof. Ing. Pavel segeč, PhD.: https://www.linkedin.com/posts/innosocinnosoc_project-innosoc-nextgenerationeu-activity-7384855342083366912-IkkI?utm_source=share&utm_medium=member_desktop&rcm=ACoAADYrbuwBoKkFoArpjtWiekEoiD3FrkyXPyA

BRAIN:IT. (18 November 2025). *LinkedIn profile @innosoc*. Available on the Internet: announcement of the symposium: https://www.linkedin.com/feed/update/urn:li:activity:7396442124268961792

BRAIN:IT. (24 November 2025). *LinkedIn profile @innosoc*. Available on the Internet: competition prize-giving: https://www.linkedin.com/feed/update/urn:li:activity:7398667812409397248

BRAIN:IT. (9 December 2025). *LinkedIn profile @innosoc*. Available on the Internet: presentation at Tomas Bata University in Zlín: https://www.linkedin.com/feed/update/urn:li:activity:7404141474713325568

BRAIN:IT. (12 December 2025). *LinkedIn profile @innosoc*. Available on the Internet: presentation at the Jozef Murgaš Secondary Technical School in Banská Bystrica: https://www.linkedin.com/feed/update/urn:li:activity:7405139422440071168

BRAIN:IT. (22 September 2025). *INNOSOC website*. Available on the Internet: Get to know the most common internet threats for young people: Prevention and protection options: https://innosoc.brainit.tech/najcastejsie-digitalne-hrozby-pre-mladych/

BRAIN:IT. (2025). *INNOSOC website*. Available on the Internet: popularization article on cybersecurity: Cybersecurity: Basics and tips on how to protect yourself against online threats

BRAIN:IT. (2025). *INNOSOC website*. Available on the Internet: Popularization article: https://innosoc.brainit.tech/co-je-soc-security-operations-center/

BRAIN:IT. (2025). *YouTube @INNOSOC*. Available on the Internet: https://www.youtube.com/@INNOSOC

BRAIN:IT. (2025). *YouTube @INNOSOC*. Available on the Internet: video interview with Ing. Michal Papučík: https://youtu.be/w9W4_oNYiEQ?si=YlCKWgzX-JVkFZQK

BRAIN:IT. (15 October 2025). *YouTube @INNOSOC*. Available on the Internet: interview with prof. Ing. Pavel Segeč, PhD.: https://www.youtube.com/watch?v=aKxL-Aig6sg

6 Annexes

Annex 1 – Article: Partners' meeting 15/7/2025

On 15 July 2025, another meeting of the INNOSOC project participants took place. The meeting was attended by representatives of the Faculty of Management Science and Informatics of UNIZA and BRAIN:IT.
The meeting was attended by representatives of the Faculty of Management Science and Informatics of UNIZA and BRAIN:IT.
This meeting focused on a discussion concerning several work packages of the project:
the further direction of the project's development,
staffing,
organizational aspects of cooperation during the summer period.
The meeting evaluated the current status of the project after the interim monitoring report had been submitted. At that point, the analytical work on 2 work packages had been completed, and the analytical studies required for work package 3 and experimental studies to obtain evidence of technical feasibility were beginning.
Small-scale laboratory tests and simulations were being carried out, in which initial data on the properties of the technology were collected, and it was also necessary to fine-tune what the solution architecture itself would look like.
The following topics were opened:
Handling of and approach to incidents occurring in the project.
The work teams divided the tasks and agreed on the next individual and joint steps. At the same time, a plan of outputs and their promotion was outlined – popularization posts and professional articles are being prepared, and in the future also videos and podcasts.

Annex 2 – Article: Basics of the INNOSOC project: Interview with Ing. Michal Papučík

What is the INNOSOC project and what is its objective?
The INNOSOC project is a response to growing requirements in the field of cybersecurity. The modern environment requires advanced SaaS and cloud services that can respond effectively to new threats. And what is the name INNOSOC based on?
Innovative and Security Operation Center – these are the words behind the acronym INNOSOC, and if you are wondering why this particular name was chosen, watch the whole video, in which Ing. Michal Papučík, COO of BRAIN:IT, also answers other interesting questions concerning the foundations of the project.
What will you learn in the video?
What the INNOSOC project is and why it was created.
What the name INNOSOC represents.
What the objective of the project is.
What problem or challenge it responds to.
What benefits the project can bring.
What he enjoys most about the project.
What technologies the team works with.
What role BRAIN:IT plays in the project.
How successful the linking of the academic and business spheres is.
What methods and international standards are used.
If you would like to know more about the INNOSOC project, watch the full interview with Michal Papučík in the video below.

Annex 3 – Article: Interview with prof. Ing. Pavel Segeč, PhD.: Cybersecurity is no longer just a topic for large companies

As part of the INNOSOC – Innovative & Security Operations Center project, we spoke with prof. Ing. Pavol Segeč, PhD., head of the Department of Information Networks at the Faculty of Management Science and Informatics, UNIZA.

Professor Segeč is a key scientific researcher of the project, which focuses on strengthening cybersecurity in organizations and schools through innovative technologies and the education of a new generation of experts.

Does cybersecurity concern everyone?

At the beginning of the interview, prof. Segeč explains why the security of IT infrastructure is a topical issue even for small organizations:

"Cyber present at present is, in my view, a key topic, because we live in an age when everything is interconnected and we are in an online world, and networks are becoming digital highways that enable and support our behaviour, business and other aspects of our lives."

The role of the Faculty of Management Science and Informatics of UNIZA in the INNOSOC project

The Faculty of Management Science and Informatics (FRI) is one of the main partners of the project and covers both the scientific research part and the development activities.

"Within the INNOSOC project, we provide our capacities, and at the same time we provide our private infrastructure as a concept on which pilot deployments of the technologies used in the project can be carried out," says Professor Segeč.

The most common threats and the need for centralized protection

According to statistical data, the most common threats include phishing attacks, ransomware or APT (Advanced Persistent Threat), in which an attacker conducts long-term espionage and monitoring in the victim's network.

The Security Operations Center (SOC) as the core of defence

One of the main outputs of the INNOSOC project is the design and building of a Security Operations Center (SOC) – a central hub that monitors, analyses and responds to cybersecurity incidents in real time.

"SOCs are built on three pillars: people, processes and technologies," adds prof. Segeč.

New requirements brought by the NIS2 Directive

In the interview, he also addressed the forthcoming implementation of the NIS2 Directive, which fundamentally changes cyber protection requirements across the EU.

"Thanks to the NIS2 Directive, which has been transposed into Slovak legislation, the requirements for raising the level of security and security management in companies have been tightened. Likewise the aspects associated with reporting attacks, and it is precisely the reporting of attacks and their detection that SOCs should help with."

How SOC systems work

Finally, the professor explained how such systems work in practice:

"Technologically, SOCs work on the principle of telemetric collection of large amounts of data, where this data is subsequently fed into databases and enriched with various supplementary data in order to make it easier to detect and uncover anomalous behaviour."

You can watch the full interview with prof. Ing. Pavel Segeč, PhD. in the video below.

In it, he explains why cybersecurity is not just a technical topic, but an essential foundation for the trustworthy and stable operation of organizations.

Annex 4 – Article: Student event FRIčkovica – 8 October

On 8 October, the traditional annual event FRIčkovica took place at the Faculty of Management Science and Informatics; it is a place for informal meetings of students, teachers and partners of the faculty.
During the event, a stand promoting the INNOSOC research project was also prepared for students. While communicating with the students, the highlights of the project were presented, for example its intent, objectives and the problems it addresses. The presentation showed the students the importance of the project as well as its benefits. The aim of the presentation at the student event was to bring young professionals closer to knowledge in the field of cybersecurity.

Annex 5 – Announcement of the INNOSOC symposium

On 18/12/2025, a symposium on cybersecurity as an open cloud service will take place as part of the INNOSOC project. The symposium will be held on the premises of the University of Žilina in the lecture room Aula AF3A5 from 8:00 to 10:45.
During the symposium, the current status and results of the research project will be presented.

Annex 6 – Article on the announcement of the winner of the iPad competition

On 10 November 2025, the iPad competition organized through the Instagram profile @innosoc_ came to an end. The aim of the competition was to involve young students and to arouse their interest in the INNOSOC project and the field of cybersecurity.
After the official draw, the winner of the competition was Timotej Djubašák, who met all the conditions and collected the prize in person.
We congratulate the winner.

Annex 7 – Article: Presentation of the INNOSOC project at the student breakfast

On 4 November 2025, a student breakfast was held at the Faculty of Management Science and Informatics of the University of Žilina in cooperation with BRAIN:IT, during which the INNOSOC project was presented to young students of management and informatics programmes.
At this informal event, the students had the opportunity to obtain information about the project and to learn about its current status, outputs and next steps.
Likewise, the importance of cybersecurity and the significance of the Security Operation Center and cloud technologies were presented.

Annex 8 – Article on the presentation of the project at the Faculty of Applied Informatics of Tomas Bata University in Zlín

On 20 November 2025, the INNOSOC project was presented to students of the Faculty of Applied Informatics of Tomas Bata University in Zlín. The project representative who spoke about the project at the faculty was Ing. Michal Papučík.

The presentation of the project focused mainly on explaining in more detail how the project helps with and reflects on the challenges associated with the transition to a digital economy. Ing. Michal Papučík also spoke about the needs of the commercial sphere, the demand for modern IT services, the need to move society to a higher level of security and the need for IT specialists.
The students were also able to learn about the principles and technologies used in the project.

Annex 9 – Article on the presentation of the INNOSOC project at the Jozef Murgaš Secondary Technical School in Banská Bystrica

On 28 November, a presentation of the INNOSOC project took place at the Jozef Murgaš Secondary Technical School in Banská Bystrica.
During the presentation, the pupils learned:
What the project is about.
What the INNOSOC project concerns.
What types of attacks we know today.
Which primary schools are involved in the project.
Why cybersecurity is important.
The entire presentation was interactive and also involved actively engaging the young pupils in the subject.

Annex 10 – Article: Cybersecurity: Basics and tips on how to protect yourself against online threats

What is cybersecurity?
Cybersecurity (Slovak: kybernetická bezpečnosť) refers to a set of measures, technologies and processes whose basic aim is to protect computers, servers, networks and programs against unauthorized access, misuse or damage, i.e. against cyber threats and attacks. Protection is needed above all for the data, information and records stored on these devices.
The people behind cyber attacks are hackers. This group of people seeks to gain access to your devices, systems and networks in order to steal sensitive personal data from them, or other compromising material. Hackers then trade in this data, information and content, sell it or use it to blackmail the injured persons.
Hackers are often very well equipped with various IT skills and frequently have the latest technologies at their disposal. It is therefore important that you regularly take care of your data, systems, networks and devices and protect them sufficiently against misuse.
In practice, protection concerns mainly these two basic factors:

The human factor

This area includes compliance with the basic principles of personal data and privacy protection. In practice, this means paying attention to what data about your work and private life you share with others, on which platforms and in what form. This segment also includes caution when using passwords, opening suspicious messages and e-mails, receiving suspicious phone calls, as well as when clicking on various unverified websites.

The technological factor

Hackers are often ahead of you not only thanks to their advanced IT skills, but they also have modern and advanced technologies at their disposal. In practice, it can therefore help if your technologies are newer or at least regularly updated. Old technologies sometimes do not allow the use of new and sophisticated protective features. Key protection in the case of technologies is provided by a high-quality and regularly updated antivirus and firewall.

Why is cybersecurity important?

Cyber threats lurk for you at home and at work, and their insidiousness lies mainly in the fact that they can threaten your sensitive areas and, in the worst case, your entire livelihood. Cybersecurity helps you protect yourself against the misuse of personal and company data.

Information at risk

Personal and contact data relating to your identity, such as first name, surname, birth number and other personal data, as well as your contact details (telephone, e-mail, address and others)
Health data and information about your physical and mental health
Financial data, data on loans and similar sensitive information
Data on marital status, spouses, children and other family members
All of the above information, passwords, account numbers, personal data and data about work activities and companies can be misused and can cause you various physical, material, financial and psychological harm.

Basic principles of cybersecurity

Many personal and work activities take place online. Along with this, the importance of cybersecurity and the need for protection in this segment are also growing. From ordinary people to large corporations, everyone is exposed to potential cyber attacks, with children and older people forming particularly vulnerable groups.
Following the principles of cybersecurity can significantly help you reduce the likelihood of data misuse and theft.

Cybersecurity factors:

Strong and unique passwords: Using a combination of upper- and lower-case letters, numbers and special characters. Set a different strong and unique password for each service.
Two-factor authentication (2FA): This procedure adds another layer of protection when logging in to your technological devices and various accounts.
Regular updates: Regular updates keep your operating system and applications up to date, and many of them also upgrade and improve various protective features.
Data backup: Regular backup of important data, information and documents to external drives and/or the cloud also contributes to protecting your data.
Vigilance with e-mails and links: Do not click on suspicious links or attachments from unknown senders. Keeping track of various scams and hacker techniques also significantly contributes to greater awareness of potential threats and risks. Most of these scams are based on your inattention. Conscious attention, caution and fact-checking also help in this area.
Antivirus and firewall: These tools are part of the basic equipment of every device and of everyone active in the online space. They do a great deal of work for you in protecting against intrusion into your systems, networks and technological devices.

The most common types of cyber threats

Staying safe in the online environment can be challenging, but it is possible if you follow the basic principles of cybersecurity and pay conscious attention. It is also good to know what potential and real risks exist and what may threaten you.
Here are some of the ones you may commonly encounter:
Phishing: Fraudulent e-mails or messages that attempt to obtain sensitive data.
Malware (malicious software): Viruses, Trojan horses, ransomware. All of these viruses can damage your device and steal your data.
Brute-force attacks: Automated attempts to guess the passwords to your systems, accounts and applications.
Social engineering: Manipulating people in order to obtain confidential information from you.
DDoS attacks: Overloading a server in order to disable a particular service or an entire website.

XSS (Cross-Site Scripting): A cyber attack on web applications in which hackers inject malicious scripts directly into a web page.

Think about prevention

The basics of cybersecurity are as important today as locking the door of your flat or house. The more you know about this issue, the better you will protect yourself against increasing digital threats and potential cyber risks. In this segment, too, prevention is a simpler and often cheaper solution than the complicated subsequent remedying of the damage caused.

Annex 11 – Article: Security Operations Center: what it is and how does it protect your company?

What is a Security Operations Center (SOC)?

With the advent of digitalization, we are increasingly encountering various cyber threats and security risks that endanger individuals and organizations. Cybersecurity is a set of measures aimed at protecting digital systems, networks, processes and programs against data theft or other disruption of an organization's operations. In this respect, the Security Operations Center represents the executive link whose aim is the actual protection of this data.
A Security Operations Center (SOC) is a specialized centre that performs continuous security monitoring in an organization and responds to real cyber threats and incidents. A SOC is a centralized unit or team of experts who ensure round-the-clock monitoring and evaluation of potential cyber threats in real time.

What is the main role of a SOC?

The basic role of a Security Operations Center is to minimize the impact of security incidents and cyber attacks on the organization and to proactively ensure its cybersecurity and other security as needed and agreed.

How does a SOC work?

The Security Operations Center team usually consists of security analysts and IT experts who work with advanced technologies. These technologies help protect the digital and other assets of the organization.

What SOC models are used in practice?

In practice, we can find two basic models of the Security Operational Center. In the first case, the main functions of the centre are performed by the internal organization, or rather by a department of the organization designated for this purpose. In the second case, these powers are entrusted to an external entity. A combination of both models is also often used.

What are the main functions of a Security Operations Center?

A Security Operations Center provides organizations with the following main functions:
Incident monitoring and detection
As part of this function, the SOC ensures 24/7 monitoring of systems and networks. In doing so, it searches for suspicious activity using security tools that monitor network traffic and device activity.
Incident management
This function of the centre is used after a security incident has been identified and includes, for example, the following activities:
gathering information that contributes to understanding the scope and type of the incident,
taking corrective measures, such as isolating or eliminating the risk, in order to reduce the negative impact of the incident as much as possible and to prevent its recurrence,
investigating the root cause of the incident in order to determine its source and to introduce the necessary controls to limit any security gaps in the future,

verifying that the incident has been properly documented and resolved, as well as checking that all relevant processes have been updated.

Problem management

As part of this activity, the Security Operations Center focuses mainly on a deeper understanding of the causes of cybersecurity and other security incidents with the aim of eliminating the same or similar problems in the future. In doing so, it often works closely with the organization concerned, or forms its internal team.

Concluding recommendations

A Security Operational Center can also provide other security services that a given organization needs. Every organization should therefore already be addressing the issue of cybersecurity and of ensuring the security of sensitive data, processes, information, systems, networks and the devices it uses.

Every organization should create its own internal policy and procedures covering the data and areas exposed to potential theft or another cyber attack, exploitation or security threat. As part of this procedure, we recommend:

setting up processes in the area of monitoring,
setting up escalation procedures,
setting up options for responding to real incidents,
staffing,
other settings with regard to the practical needs and requirements of the specific organization and its current situation.

For this purpose, you can create your own internal guidelines, templates and processes that will help you effectively protect sensitive data, information and devices.

Annex 12 – Article: Get to know the most common internet threats for young people: Options for prevention and protection

Get to know the most common internet threats for young people: Options for prevention and protection

The current generation is growing up in the so-called information and technology age, in which various technologies are part of their everyday lives and moving around the online space is a normal status for them. Tools give them easy access to the digital world, where they communicate, search for information, learn and have fun.

Potential threats lurking for young people also spread in the online space. In order to defend themselves effectively against these risks, they should know what they are at risk of and become familiar with how they can protect themselves against these threats. Read about the most common pitfalls and about prevention and protection against them.

Threats and risks of the digital world for young people

Potential threats have long since stopped lurking for young people only beyond the gates of your homes. They are often much closer to them and more cunning than you can imagine. The digital world is relatively new territory even for many adults. If you want to protect young people effectively against digital threats, one of the ways is to educate yourself regularly about the risks and about safety in the online space. Prevention is the basis of success in this area too.

Technological development is advancing at a dynamic pace, which is why it is sometimes very difficult to recognize the risks.

Take a look at an overview of the most common threats in the digital world that endanger not only young people.

Searching (surfing) the internet

The internet is a major source of a large amount of diverse information that can have a far-reaching negative impact on young people. Young people often do not yet know how to distinguish effectively what offensive, toxic and dangerous content is, and often they also do not know how to search safely for the information they need on the internet and where it is better not to click.

Adult content

Another major threat, not only for young people, is the easy and quick availability of adult content on the internet. This content is often not only unsuitable for them but in many respects also genuinely dangerous.

Communication on social networks

Even many parents and other adults still do not have sufficient awareness of the threats present in the online space and, without much thought, routinely publish their sensitive data, information, photos of themselves and their children and the like. It is very important that you learn to protect your privacy effectively and teach this to your children as well.

Communicating intimate matters and sending intimate content

A separate chapter within communication is the sending of messages, photographs or other intimate content. If such content is misused in any way, young people often bear the consequences for the rest of their lives. Such content and information can easily be misused in many ways for blackmail and other illegal and criminal activity.

Internet fraud

Young people shop on the internet. It is convenient and often cheaper as well. However, with greater demand, the appetite of fraudsters, who use increasingly sophisticated methods in their online scams, also grows. In these scams, users may lose their personal data, which may be misused, as well as their money, privacy and more.

Other threats include the risk that young people may succumb to games and gambling, the risk associated with discrimination, various types of bullying, blackmail and abuse, as well as encountering various forms of hate speech.

Another non-negligible risk is the development of addiction to technology, to following social networks and to online relationships, which deepen the fear of missing out (FOMO) and the fear of better options (FOBO) and lead to psychological difficulties or social isolation.

Safety recommendations and protection of young people

The digital world is part of our everyday lives. You should learn to move around in it safely and pass these principles on to young people. It is important to understand that such danger exists and is hard to recognize. Learn to recognize it and to apply protection options effectively.

Responsibility for the data and content you publish on the internet, social networks and other communication websites and platforms. Do not share details such as your home address and telephone numbers publicly.

This also applies to data and information about where you regularly go, what you do there, with whom, and so on.

Sharing photographs is very popular. However, this activity carries a high risk of potential misuse in various ways. If images and photographs show young people's bodies exposed or in provocative poses, the threat increases even further. Naked photographs of small children should definitely remain part of family albums. This is not content that you should show to anyone else.

Interaction with people you do not know. The internet provides anonymity for people, and you never know with absolute certainty who we are communicating with. Not communicating with strangers and not following them is perhaps an even more essential form of prevention and protection in the online space than in the physical world.

A safe world begins at home

Be a role model and talk openly with young people about the threats in the digital world. Create a home for them in which they will not have to look for relationships, information and entertainment elsewhere. When young people are brought up in a safe, loving, inspiring and stimulating environment in which they have the opportunity to express themselves authentically and are supported in doing so, this is the basic prevention against many problems and threats. Build healthy boundaries in children.

Annex 13 – Article: What the cloud is and what it is used for: Basic types and advantages of cloud storage

What the cloud is and what it is used for: Basic types and advantages of cloud storage
Cloud is a term that denotes data storage through which users can share, store or otherwise handle large amounts of information and data. In this article, we will explain simply what the cloud is and how it can be useful to you in practice. In addition, we will also outline the basic advantages and disadvantages of using cloud services.
What is the cloud and what is it used for?
The cloud, also called cloud storage, is an online service that makes it possible to store, keep and manage your data, such as various personal or company files, documents, photographs and videos. Your data are thus stored on cloud servers connected to the internet, which are located in data centres in various places around the world. The cloud is a service that companies or individuals can use at any time through a paid rental, or as part of software or a platform service.
Forms of cloud services
Cloud-based services can take many different forms, for example the following:
Web hosting.
File sharing.
Distribution of software and other services.
Storing and keeping files, photographs, videos, personal and company records, documents, contracts, employee, business or other operational data, projects and other necessary information.
Cloud computing, which denotes the method of using several interconnected servers in order to share work activities, projects or other specific tasks.
Basic types of clouds (cloud storage)

The basic types of clouds include the public, private and hybrid cloud. Below we briefly introduce their basic functions.
Public cloud
It is a shared infrastructure operated by an external service provider. In this case, your data are stored in the external provider's data centres, which may be located anywhere in the world. The cloud service provider is responsible for the overall operation and comprehensive management of the cloud environment, including the hardware, software and the entire data centre. The customer, who usually rents the relevant storage space, is in this case only a user of the service.
Note:
However, the fact that the cloud is public does not mean that anyone has access to the stored data. For example, the customer can stipulate that their infrastructure is available only to their family, employees or the company's partners. No one else will gain access to the stored content, data and information.

Private cloud
This is a space located in the company's own data centre. In this case, the cloud is operated, managed, administered and maintained by the company itself, on its own account. In practice, such a solution is usually somewhat more expensive and requires extra costs incurred for the necessary skilled workforce, hardware and software.
Hybrid cloud
It represents a combination of both of the models mentioned above. In these cases, some of the services are operated on publicly available infrastructure at an external provider and some of the services are stored on the company's private cloud. The private cloud usually stores the company's sensitive data, and access to these data or to individual levels is also specified for particular employees of the company or other people.
Advantages and disadvantages of cloud services
The undeniable advantages of the cloud include higher productivity, which is made possible by the fast flow and circulation of data, documents and information. Sharing resources generally leads to greater efficiency in company processes, which also reduces the costs of employees and other work operations. Finally, cost reduction is also helped by the fact that a company rents cloud services, compared with the model in which it manages them itself.

Another advantage of cloud services is the possibility of storing large amounts of data in one place and enabling a larger number of people, or specified individuals and groups, to access and work with them.
In practice, a disadvantage may be above all the fact that various sensitive personal and company information, data and documents are stored on someone else's hardware and sometimes also in a place that you will never get to and that you may never have heard of. This applies to public or hybrid clouds.
A growing threat at present is also potential cyber attacks, the aim of which is above all the theft of sensitive data and information in order to misuse them in various ways against individuals and companies.
Conclusion
The cloud represents a modern way of storing and processing data over the internet, which brings companies and private individuals a number of different advantages, such as:
availability of the stored and managed data, content and information,
flexibility of working with stored and shared data,
fast access, the possibility of sharing data and collaborating over long distances,
productivity and efficiency of work and of work procedures and processes,
the possibility of storing a large volume of data in one place,
cost savings.
The cloud allows users to access stored files in their own or external data centres from any device with an internet connection. As a result, the cloud significantly simplifies many corporate processes and supports remote collaboration. The cloud is currently one of the fixtures of the digital world, and its importance will probably grow in the future along with increasing technological demands in various areas.

Annex 14 – Article: Computer security and data protection – principles and practical examples

Computer security and data protection – principles and practical examples
Computer security and data protection are among the basic areas that everyone who works with information in an online environment should understand. They focus on protecting data and information against unauthorized access, loss or misuse. Key principles such as the

confidentiality, integrity and availability of data form the basis of the so-called security triad, which helps to prevent cyber threats and to protect sensitive information. In this article, we will look at what these principles mean in practice and how to apply them effectively.

Basic principles of data and information protection

Cybersecurity deals with the protection of data and information that are primarily located in virtual space. In practice, these are data and information stored, for example, on various remote or company servers, computers, data centres, the internet or in mobile devices.

The security triad in the area of computer security and data protection consists of three key principles that everyone should know – not only an IT professional but also an ordinary user:

Confidentiality

Whenever you process any data and information, you should always observe the principle of confidentiality. This rule states that every piece of data and information we come into contact with should be provided, shared and disseminated only to persons designated and authorized for that purpose. Every piece of confidential information carries a potential risk of misuse in personal and/or working life, and it is therefore crucial to protect these data and information from those who could misuse them.

Confidential information is any non-public information whose disclosure or provision could harm an individual and/or an organization.

Integrity

The integrity of data and information represents the concept of the completeness and correctness of data and information. In ensuring data integrity, measures are applied in practice whose aim is to ensure that this information is not modified, misused or deleted throughout its entire life cycle.

Data integrity is the accuracy, completeness, consistency and reliability of data from their creation to their disposal.

Availability

The availability of consistent data and information means that they are available to authorized persons in complete form and always whenever they need them. At the same time, it indicates that this information is thus protected against misuse by unauthorized persons and/or entities.

These three principles form the basis of every security strategy. If even one of these principles is violated in practice, the data protection system is, as standard, no longer considered secure. All three areas are closely interconnected and each supports the other.

The general principles of personal data protection under Act No. 18/2018 on the protection of personal data also apply within cybersecurity, for example:

Lawfulness of the processing of personal data.

Limitation of the purpose for which the data are processed.

Minimization and accuracy of the processed data.

Limitation of the retention period of the processed data.

Restrictions in the area of providing and disseminating the processed data.

Principles, rights and obligations in accordance with the valid and effective Slovak and European legislation in the area of personal data protection.

Practical application of the basic principles of data protection

Computer security and data protection should be an everyday part of company processes, not just a theoretical concept. You can also achieve compliance with the principles of the security triad in practice through the following practical measures.

Confidentiality in practice

The main objective of this principle is to ensure that data and information are available only to authorized persons. Confidentiality is a key aspect especially for data designated as personal, banking, health, strategic, company and similar information.
You can ensure the security of data and information in several ways:
By encrypting data.
By granting access rights.
By multi-factor authentication.
By authentication using biometric data.
By segregating sensitive data.
By restricting physical access.
Integrity in practice
The basic purpose of the integrity principle is to ensure that data remain complete, accurate and unchanged throughout their existence.
You can ensure the security of data and information, for example, by:
Digital and electronic signatures.
Audit logs.
Automated checking of file changes.
Availability in practice

The basic objective of this protective principle is to ensure that authorized persons always have available the data they need.
You can ensure the security of data and information by:
Regular checking and backup of data and information.
Protection against DDoS and ransomware attacks.
Using redundant systems and servers.
Using the cloud.
Using independent power sources.
Availability monitoring.
Concluding summary
The security triad is the basis of every security policy. Every IT measure designed to protect data and information should therefore include all three security principles mentioned above, and these principles should be set in mutual balance. Excessively strong confidentiality can reduce the availability of data and vice versa. When analysing incidents, it is then important to define which part of the triad was affected and subsequently to take the necessary measures to restore or strengthen it.

Annex 15 – Interview with Ing. Michal Papučík

"My name is Michal Papučík, and I participate in the INNOSOC project as an information systems architect, analyst and scientific researcher. From a high-level perspective, the INNOSOC project is applied research in the area of cybersecurity. It is a response to what I would call today's demands in the area of cybersecurity, namely modern and secure services, SaaS cloud services, and bringing sufficient knowledge or experts in the area of cybersecurity. Originally, we wanted to create a name that would, as is standard, consist of some abbreviations of initial letters, but in the end we came to the view that it is our new innovative solution of a kind of Security Operation Centre, so we decided that INNO represents innovativeness and SOC stands for Security Operation Center, so together abbreviated as INNOSOC. The main objective of the INNOSOC project as a research project in the area of cybersecurity is to bring an open, open-source solution to entities that cannot afford standard, high-cost security solutions dealing with cybersecurity. We are trying to

bring a solution that these entities can either arrange as a service of their own or else in the form of an on-premise solution, which is built on containerization and on a simpler set-up in their own system in-house.

The project responds above all to the greatest need within cybersecurity, which is to secure our information systems. We are not doing entirely well as far as the Slovak Republic is concerned; our IT systems have countless problems. Apart from security itself, the biggest shortcomings here are that these security systems are very expensive, and the second very problematic factor is that we have few experts who would be able to operate these systems or work in some way in the area of cybersecurity. Our solution will in fact ensure that organizations that do not have the finances for those expensive solutions will be able to afford or obtain it, and at the same time, thanks to artificial intelligence or some machine learning, we will be able, so to speak, to relieve those costs or the need for those experts, and not so many of them will be needed.

For me, the very most fundamental benefit of what we will deliver from this project is that we will deliver a design or a kind of open-source solution for entities that will be able either to start using it as a SaaS service or to get it running on-premise. But for me, the other goals are mainly extensive cooperation with the university sphere. That is the connection of, let us say, the company and the university, thereby creating a functional team that is able to turn ideas and interesting suggestions into a finished solution. At the same time, for me as well as for the university, it is certainly an increase in the competence of the people who participate in the project, because everyone learns something new and moves forward in the area of cybersecurity.

What I enjoy most on this project are the joint meetings, or rather I would call them brainstorming sessions, where we all negotiate together. It is not always entirely the most pleasant and the nicest, but we always discuss what the important factors are and how we can achieve them, and we look for common ideas and consensus. Perhaps this synergy between these two teams, the one from the university, from the research environment, and ours from the corporate environment, or as I would call it, the one that deals with the practical side of things, often results in coming up with something completely new or a new approach. I am really pleased that we are not doing something ordinary, but are really going into something new that we are trying to combine from both of these worlds.

On the INNOSOC project we have encountered a really large number of technologies. Setting aside the security and cybersecurity technologies, such as security hardware and software, we very often encountered, for example, ordinary hardware and software, infrastructure hardware, network devices other than firewalls, standard routers, switches and so on, end stations, and many other devices such as tablets and mobile phones, so as standard we come into contact with these. But in the meantime we have tried out many different databases, for example, or presentation layers, various programs that represent logs, records, anomalies. And at the same time we have, so to speak, played around quite a lot with various artificial intelligence or machine learning models, otherwise known as strojové učenie.

The role of our company BRAIN:IT in the project was initially divided mainly on the basis of our competences. Right at the beginning we said, fine, we have a great advantage, or we are strong precisely in the area of being able to take researched information that someone prepares in advance, which in this case is the university, and to rework it into a product or project, or to take it further and produce a design that is usable in practice. So those are our strengths. That is also why we decided that our work packages would be mainly the configuration and installation of these submodules or modules. At the same time, it was the architecture design and its creation, and thirdly we took charge of, or we are the guarantors of,

the popularization or marketing activities, to raise people's awareness of this project and of cybersecurity and the related areas.
Of course, I must also point out that we cooperated on everything together. That was also the idea when we entered this project; there was a clear vision and agreement that we would definitely work together on every work package. If only in order to deepen the cooperation, so that it is intensive and so that everyone learns from the area in which they are not used to working. That means the university learns something from us and we learn something from the university.
In my view, connecting the academic and business spheres is entirely advantageous precisely through projects like this, which are research projects combined with something that already extends to the creation of a product. Thanks to this, for example, we have created a partnership that already goes far beyond the boundaries of the project; we are already cooperating on other projects. We will certainly continue to cooperate after its completion, in areas completely different from cybersecurity alone. And already now, for example, we have jointly written another project, which is a continuation of INNOSOC and should take it to the next level, somewhere further along in our vision of where we want to take it.
In the INNOSOC project we use a number of international standards. The very first I will mention is PRINCE2, which is the project management methodology that we follow, because at the Faculty of Management Science and Informatics it is an established process or framework. We also use it in our company BRAIN:IT for all projects, and it helps us greatly in delivering these projects. At the same time, we use ITIL V to set up certain service parameters and services, and in the area of managing the services that we plan to build in the future.
As far as architecture is concerned, we agreed that we would use an architectural framework defined by TOGAF. Most often, as far as graphical representation is concerned, we use ArchiMate 1 or UML version 2. Sometimes also BPML, but this is not entirely strictly prescribed; in this case, the vast majority is ArchiMate and UML version 2.
As far as our company's standards are concerned, the first I must certainly name is ISO 27001, which is in fact information security and is directly related to this. We also comply with 9001, 22301 and many others, as well as 20000 on service management."

Annex 16 – Interview with prof. Ing. Pavel Segeč, PhD.

My name is Pavel Segeč. I work as the head of the Department of Information Networks at the Faculty of Management Science and Informatics. In the INNOSOC project, I am a key project investigator. Cybersecurity is currently a key topic for me, because we live in a time when everything is interconnected and we are in an online community. Networks are becoming digital highways that enable and support our behaviour, business and other aspects of our lives.

In my view, cybersecurity is important for small companies for several reasons. These basic reasons may be legal requirements arising from the new amendment to the Cybersecurity Act. The second aspect is that, precisely at a time when we are all connected, secure behaviour should be the basis for everyone, since each of us has our own critical assets that we consider sensitive and that need to be protected.

In the INNOSOC project, the Faculty of Management Science and Informatics is the lead applicant of the project and at the same time the key scientific research partner. Within the INNOSOC project, we provide our research capacities as well as our private cloud

infrastructure as a concept on which pilot deployments of the technologies developed and tested in the project can be carried out.

Among the most common threats at present, if we support this with statistical data, are various phishing campaigns. Of course, a very popular topic is ransomware and cryptomware, which is currently very active. Besides that, however, I consider the topic of so-called APTs (Advanced Persistent Threats) to be very important. These are advanced attacks in which the attackers are positioned in the victim's network over the long term and carry out espionage and monitoring. Many times this involves hundreds of days during which the company in question has no idea that it has an attacker in its network.

A Security Operations Center (SOC) is not just one technology, because SOCs stand on three pillars: people, processes and technologies. As the technology partner of the project, we are, of course, interested precisely in the technologies. The role of SOCs at present is to help detect and, above all, respond to discovered attacks or attackers present in the network.

The topic of SOC is also important because, precisely through the amendment and tightening of the cybersecurity act and its decree, which is already available, the number of companies that must behave actively and protect themselves against various types of threats, and that must report the threats that have been detected, is expanding. The main objective of SOCs is precisely to help companies detect and respond to threats that have occurred in their networks.

Thanks to the NIS2 Directive, which has been transposed into Slovak legislation, the requirements for raising the level of security and security management in companies have been tightened. At the same time, the aspects related to reporting attacks have also been tightened. SOCs should help precisely with reporting attacks and detecting them, which is in fact the topic we are addressing in the INNOSOC project.

Technologically, SOCs operate on the principle of telemetric collection of large amounts of data. This data is then stored in databases and enriched with various additional data in order to make it easier to detect and uncover anomalous behaviour. However, we are still talking about a huge amount of collected data, which is why one of the current trends being implemented in SOCs is support for artificial intelligence and machine learning. It is precisely the introduction of these machine learning methods into SOC solutions that is one of the aspects we are addressing in cooperation with BRAIN:IT as part of our development in the INNOSOC project.