PROJECT

Multi-tenant Cybersecurity Operations Centre Delivered
as an Open Cloud Service with Machine Learning Elements

V21 – Available Online Awareness-Raising Materials and Outputs

KPB7 – awareness-raising activities
type – educational materials
month of submission – M2

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

Introduction **4**
1 Outreach Methods and Communication Tools **4**
1.1 Website *4*
1.1.1 Implemented Activities 4
1.2 Social Media *19*
1.2.1 Implemented Activities 19
1.3 Popularisation Texts *44*
1.3.1 Implemented Activities 45
1.4 Audiovisual Content *56*
1.4.1 Implemented Activities 57
List of Sources **66**
Annexes **70**
Annex 1 – Article: Partners' meeting 15.7.2025 ..... *70*
Annex 2 – Article: The fundamentals of the INNOSOC project: Interview with Ing. Michal Papučík *70*
Annex 3 – Article: Interview with prof. Ing. Pavol Segeč, PhD.: Cybersecurity is no longer just a topic for large companies *71*
Annex 4 – Article: Student event FRIčkovica – 8 October *72*
Annex 5 – Announcement of the INNOSOC symposium *72*
Annex 6 – Article announcing the winner of the iPad competition *72*
Annex 7 – Article: Presentation of the INNOSOC project at the student breakfast *73*
Annex 8 – Article on the presentation of the project at the Faculty of Applied Informatics, Tomas Bata University in Zlín *73*
Annex 9 – Article on the presentation of the INNOSOC project at the Jozef Murgaš Secondary Technical School in Banská Bystrica *73*
Annex 10 – Article: Cybersecurity: Basics and tips on how to protect yourself against online threats *73*
Annex 11 – Article: Security Operations Center: what is it and how does it protect your company? *76*
Annex 12 – Article: Get to know the most common internet threats for young people: Options for prevention and protection *77*
Annex 13 – Article: What is the cloud and what is it used for: Basic types and advantages of cloud storage *79*
Annex 14 – Article: Computer security and data protection – principles and practical examples *81*
Annex 15 – Interview with Ing. Michal Papučík *83*
Annex 16 – Interview with prof. Ing. Pavol Segeč, PhD *85*
Annex 17 - Article on the interview with experts Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD *87*
Annex 18 - Article on the interview about the INNOSOC project: Cybersecurity and broadening horizons with Dominika Toman *88*
Annex 19 - Article on the interview about the INNOSOC project: On scientific research and cybersecurity with Martin Mičiak *89*
Annex 20 – Article on prof. Ing. Milan Kubina, PhD. on the INNOSOC project *90*
Annex 21 – Popularisation article on the topic Linking AI and cybersecurity in practice *90*
Annex 22 – Popularisation article on the topic Cyber attacks: How they are changing and why they pose an ever-greater risk *92*
Annex 23 – Popularisation article on the topic Automation and deep machine learning in cybersecurity *95*
Annex 24 – Interview with Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD *98*

Annex 25 – Interview with Ing. Martin Mičiak, PhD. 99
Annex 26 – Interview with Ing. Dominika Toman, PhD. 100
Annex 27 – Interview with prof. Ing. Milan Kubina, PhD. 101

Introduction

This document provides an overview and description of the available online awareness-raising activities associated with the INNOSOC project. Activities and outputs which, by their very nature, were not available online are described in output V22 - Implemented Awareness-Raising Activities.

1 Outreach Methods and Communication Tools

An effective awareness-raising campaign for the INNOSOC project requires targeted and differentiated communication across several target groups. In order for the content and message of the project to reach students, the professional community, the lay public and potential customers alike, multiple communication formats and channels must be used.

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

1.1 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 links to European digital initiatives.

The website 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 subsequently follow its further development – in particular through regular content updates in the form of news items or outputs.

The website grew and was supplemented with further sections: professional and popularisation articles, downloadable documents, visualisations of the solution, research outputs, as well as calls for the public and students to get involved. It is also linked to social media, where news and awareness-raising activities aimed at various target groups are shared. The website therefore serves as an open and gradually developing platform that supports transparency, awareness and the building of interest in the topic of cybersecurity.

1.1.1 Implemented Activities

1.1.1.1 Creation of the website

For the purposes of communication with the general public, the INNOSOC website 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 implementing organisations, the duration of the project and the partners working on the project.

The “Home” section communicates the main objective of the project, its 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 learn more about the project by clicking on the “About the project” section, where the objective of the project 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 be gradually uploaded to the website and will be available for viewing.

Another section is “News”, where blog articles, popularisation articles and all news relating to implemented activities, meetings or published indexed articles and publications were posted.

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

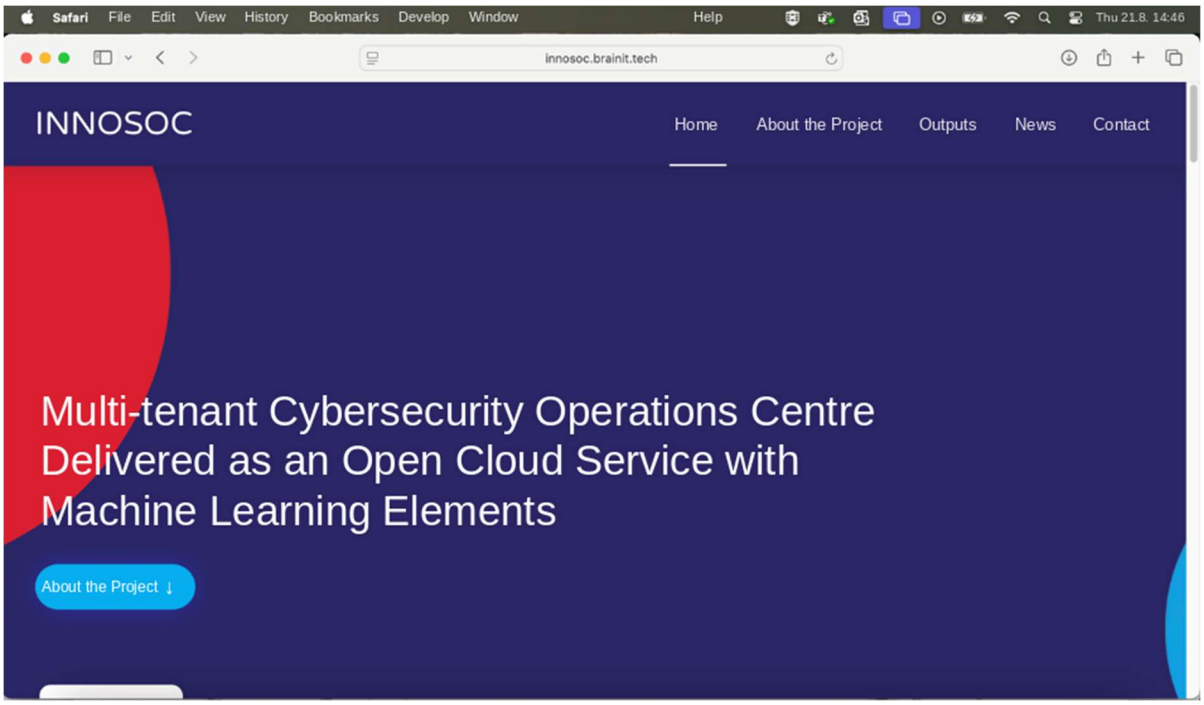


Figure 1: Preview of the INNOSOC home page, Source: (BRAIN:IT, 2025)

1.1.1.2 Article on the partners' meeting

The aim of the blog post published on 28 July 2025 was to communicate to the general public the course of the meetings of the project partners, BRAIN:IT and the Faculty of Management Science and Informatics, University of Žilina. The article on the meeting of 15.7.2025 communicates the current progress of work on the project, its further direction and the organisational 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: Partners' meeting 15.7.2025

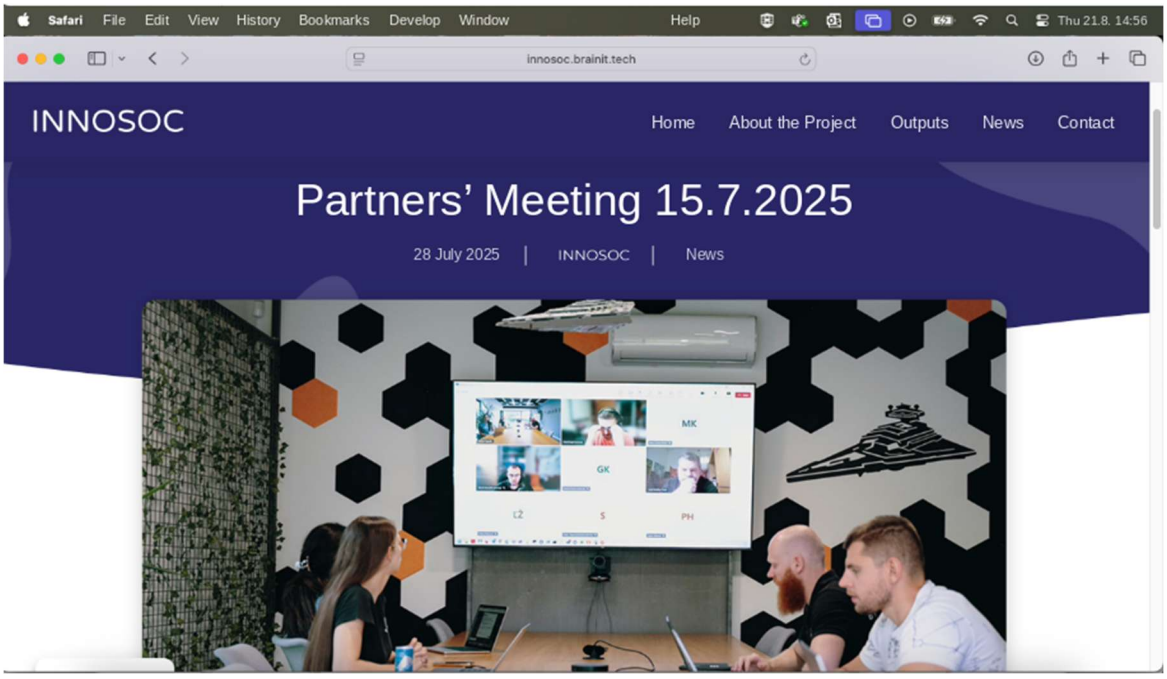


Figure 2: Article on the INNOSOC website: Partners' meeting 15.7.2025, Source: (BRAIN:IT, 2025)

1.1.1.3 Article on the interview with Ing. Michal Papučík

On 20 August, a short article was added to the "News" section communicating an informational 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 thereby also to raise awareness of the basic information about the INNOSOC project.

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

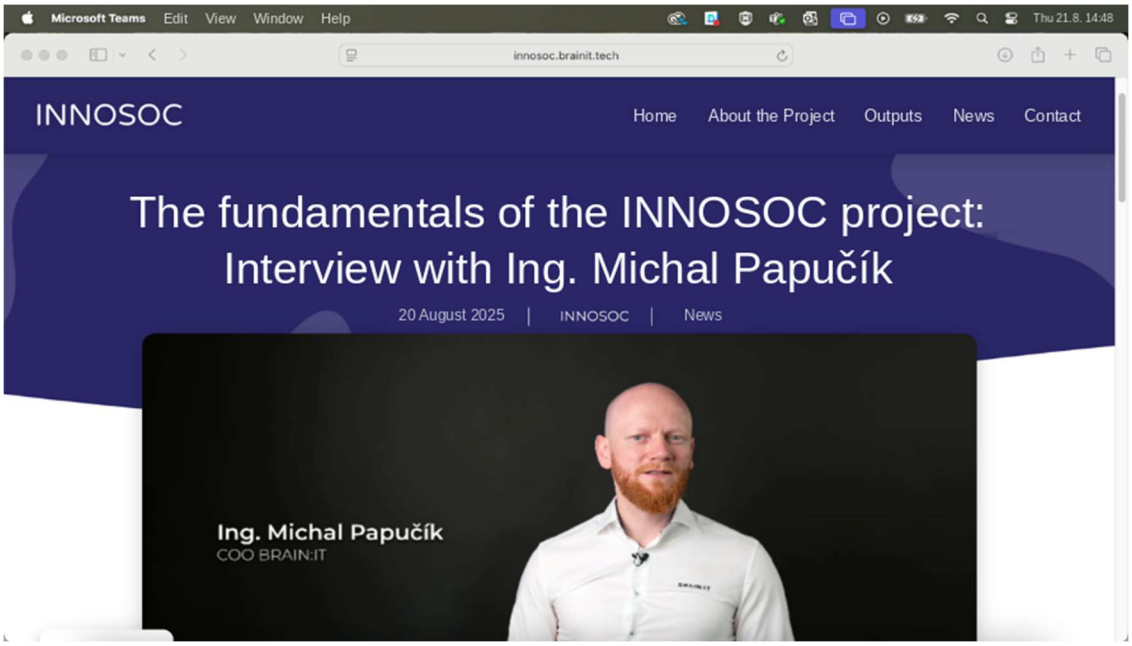


Figure 3: Article on the INNOSOC website: The fundamentals of the INNOSOC project, Source: (BRAIN:IT, 2025)

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

Within the project, an expert interview was conducted and published with prof. Ing. Pavol Segeč, PhD., Head of the Department of InfoCom Networks at the Faculty of Management Science and Informatics, University of Žilina (UNIZA), who acts as a key scientific researcher on the project. The aim of the interview was to explain the importance of cybersecurity in today's digital environment, to highlight growing cyber threats and to explain the role of the INNOSOC project in building systematic and centralised protection for organisations and educational institutions. The content of the interview focuses in particular on:

- the importance of cybersecurity for organisations of all sizes in the context of increasing digitalisation,
- the role of the Faculty of Management Science and Informatics, UNIZA, as the main partner of the project and provider of scientific research and development capacities,
- the identification of the most common cyber threats, such as phishing, ransomware and advanced persistent threats (APT),
- an explanation of the concept of a Security Operations Center (SOC) as a central element of protection, built on the pillars of people, processes and technologies,
- the impact of the new NIS2 Directive on requirements in the area of cyber incident management and reporting,
- 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, linking the scientific research perspective with the practical implications for the security of organisations. It also 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.

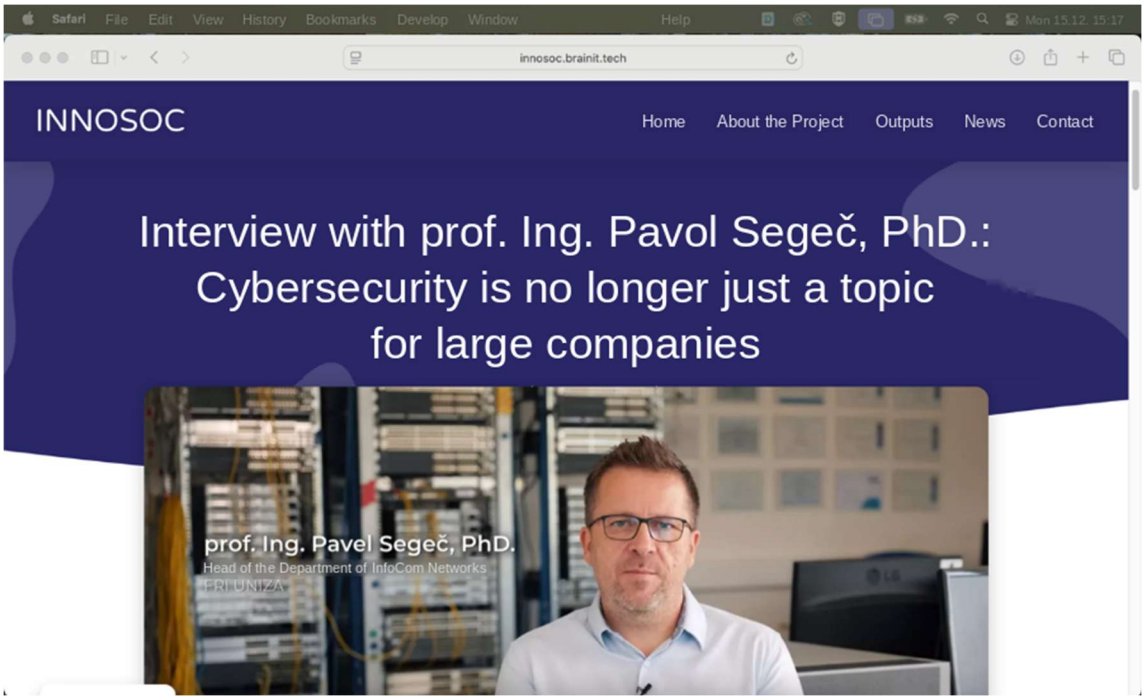


Figure 4: Article on the INNOSOC website: Interview with prof. Ing. Pavol Segeč, PhD.: Cybersecurity is no longer just a topic for large companies, Source: (BRAIN:IT, 2025)

1.1.1.5 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, 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 it addresses in the area 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 academic and applied practice and the opportunities to get involved in cybersecurity issues were communicated. The presentation also served as a tool for popularising the topic of cybersecurity among young professionals and students of technical disciplines.

The activity is a popularisation and dissemination output of the project, aimed at supporting education, building awareness of cybersecurity and strengthening the links 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.

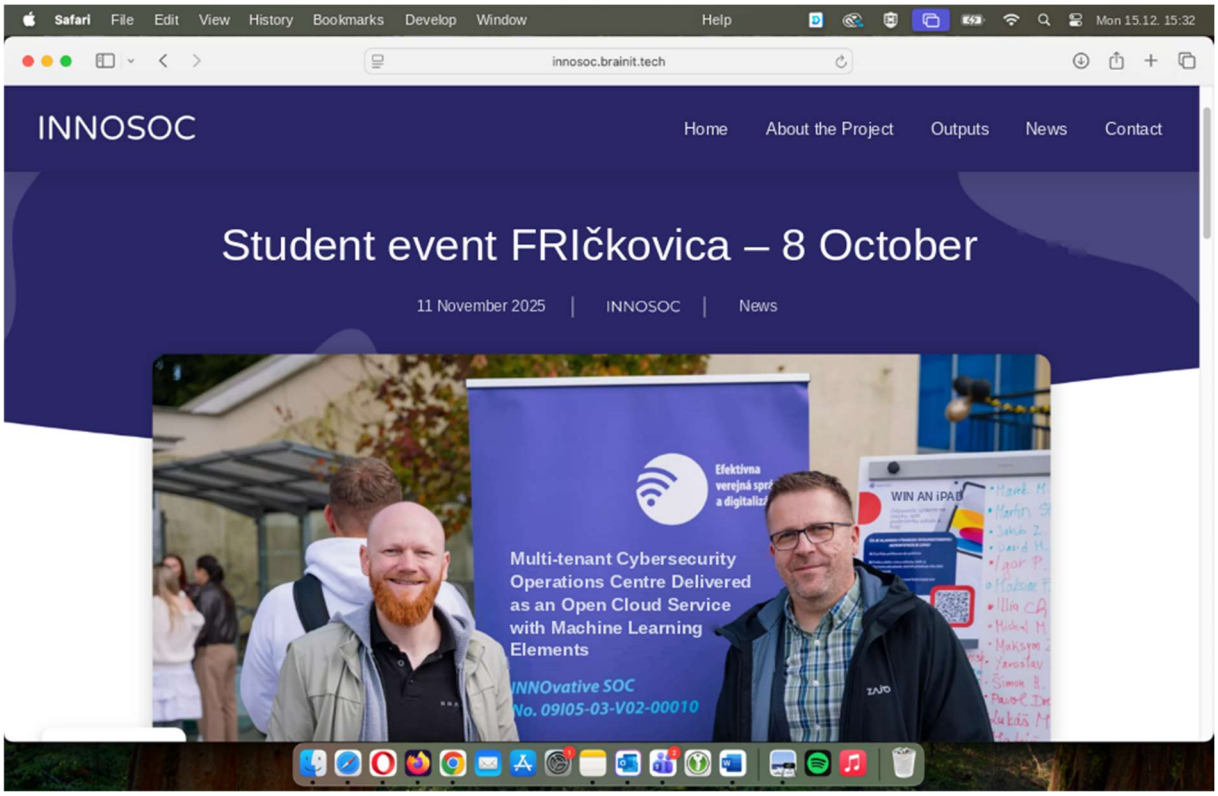


Figure 5: Article on the website: Presentation at the student event FRIčkovica, Source: (BRAIN:IT, 2025)

1.1.1.6 Information notice on the holding of the INNOSOC project symposium

On 17 November, a notice was published in the "News" section on the holding of a professional symposium on the topic Multi-tenant Cybersecurity Operations Centre Delivered 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 was to present the current state of implementation of the INNOSOC project, its interim results and research findings in the area 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 notice on the website can be found in Annex 5 – Announcement of the INNOSOC symposium.

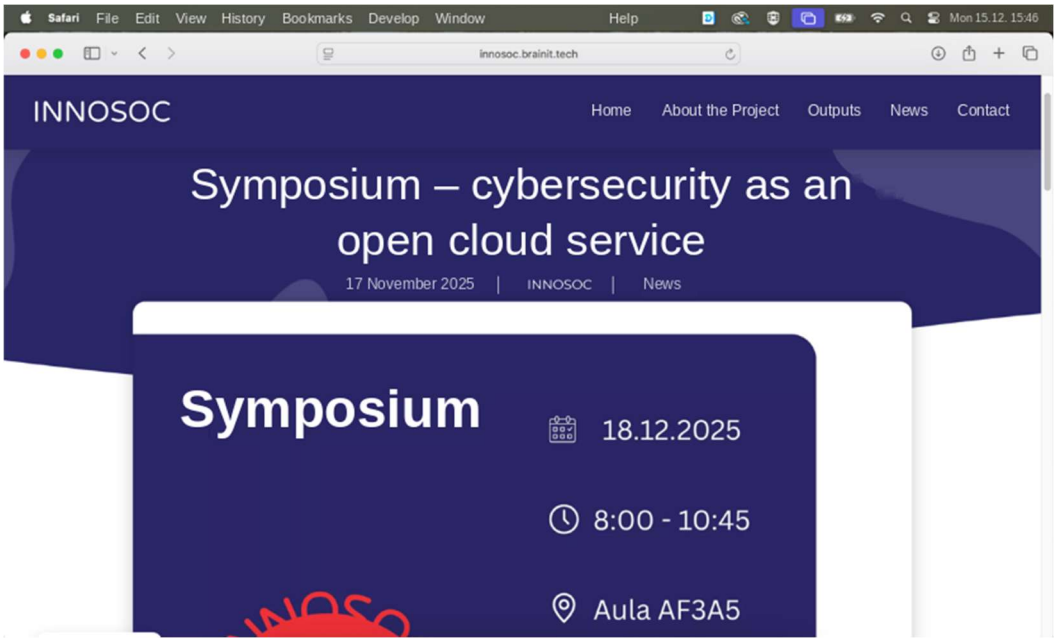


Figure 6: Article on the INNOSOC website: symposium, Source: (BRAIN:IT, 2025)

1.1.1.7 Article announcing the winner of the iPad competition

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

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

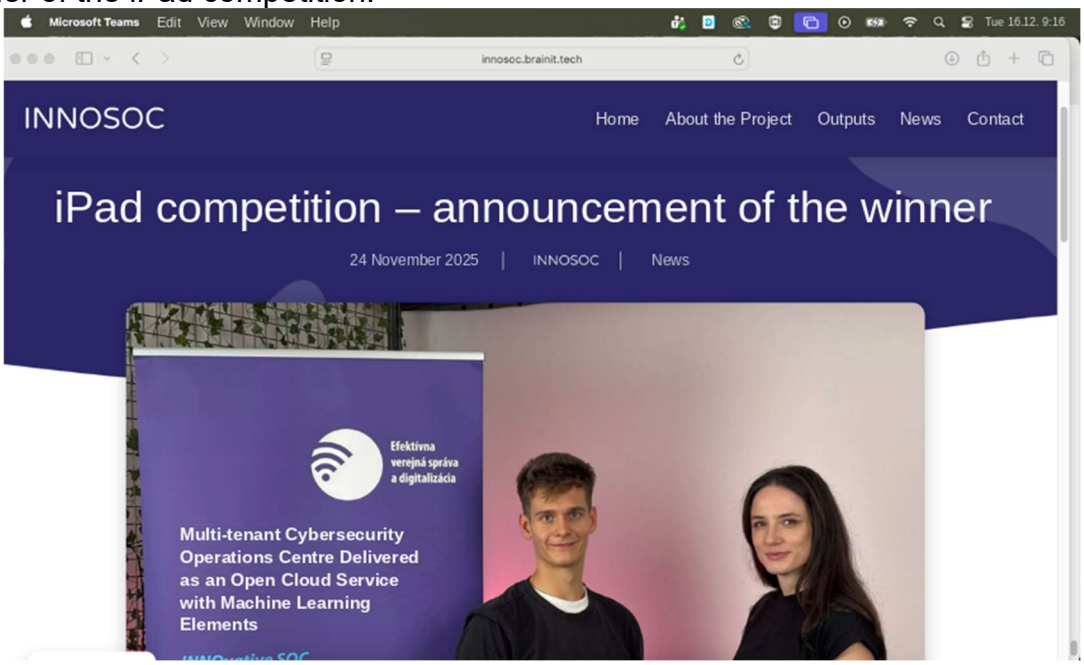


Figure 7: Article on the website: iPad competition, Source: (BRAIN:IT, 2025)

1.1.1.8 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, University of Žilina, on 4 November. The aim of the activity was to introduce the INNOSOC project informally to students of management and informatics programmes, and to acquaint them with the current state of implementation 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 presentational, popularisation and dissemination output of the project, aimed at raising awareness of cybersecurity, fostering students' interest in this field and strengthening the links 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.

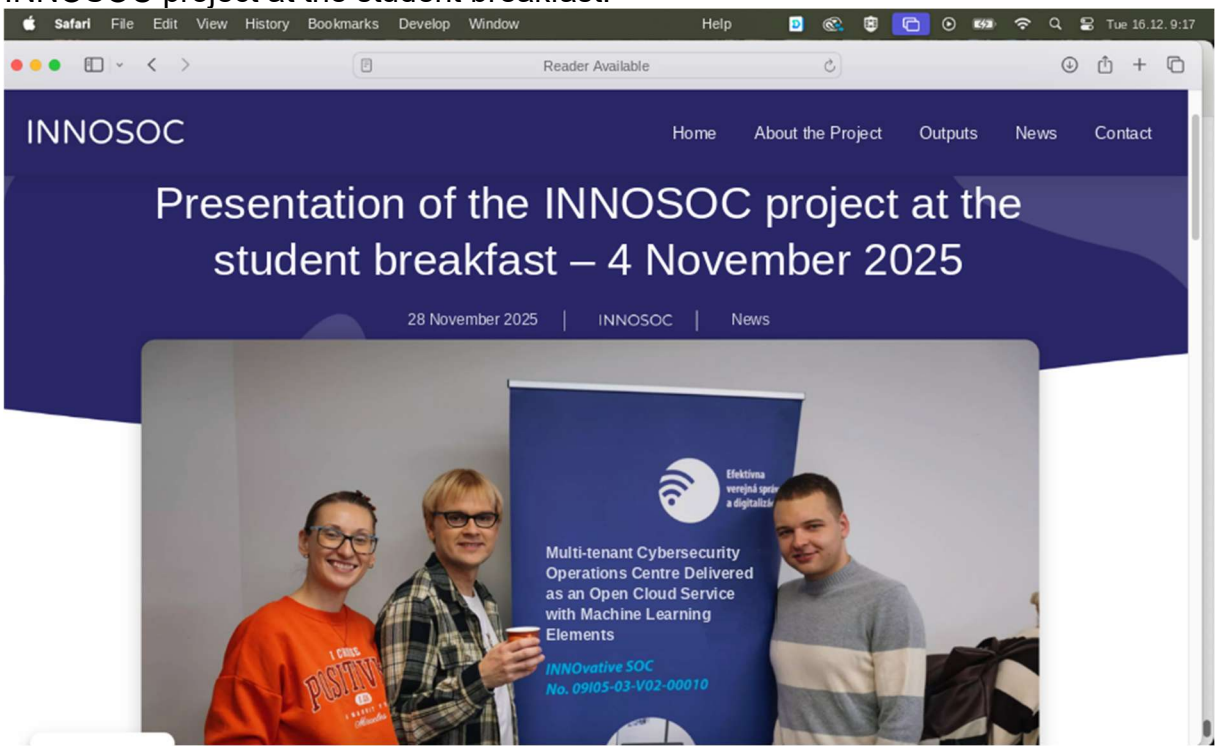


Figure 8: Article on the INNOSOC website: Presentation at the student breakfast, Source: (BRAIN:IT, 2025)

1.1.1.9 Article on the presentation of the project at the Faculty of Applied Informatics, 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 increasing the level of cybersecurity in organisations,
- the basic principles, technologies and approaches used in the INNOSOC project.

The activity is a presentational, popularisation 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, 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)

1.1.1.10 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 Jozef 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, to explain the basic principles of cybersecurity and to 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 cyber attacks at present,
- the educational and academic institutions involved,
- the importance of cybersecurity for individuals and society.

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

The activity is a popularisation, educational and dissemination output of the project, aimed at awareness-raising in the field of cybersecurity and at 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)

1.1.1.11 Article on the interview with experts Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD.

On 27 January 2026, an article entitled “Interview with experts: How the INNOSOC project connects science, practice and cybersecurity” was published on the INNOSOC website, presenting an expert view of the importance and objectives of the

project. The article takes the form of an interview with experts involved in the project and outlines its benefits for both research and applied practice.

The main idea of the interview is to present the INNOSOC project as an initiative that links the academic environment and industrial practice with the aim of strengthening the cybersecurity of organisations through modern technologies and research. The discussion focuses in particular on the importance of building a Security Operations Center (SOC), which enables centralised monitoring, analysis and resolution of cyber incidents in real time.

The interview also highlights the growing importance of cybersecurity in the digital society and the need for cooperation between research institutions and technology companies in developing new solutions. The role of education, research and the development of innovative tools that help organisations respond more effectively to modern cyber threats is also emphasised.

The publication of the article on the project website contributes to the dissemination of information about the project's activities and supports the popularisation of cybersecurity topics among both the professional community and the wider public.

The full text of the article can be found in Annex 17 – Article on the interview with experts Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD.

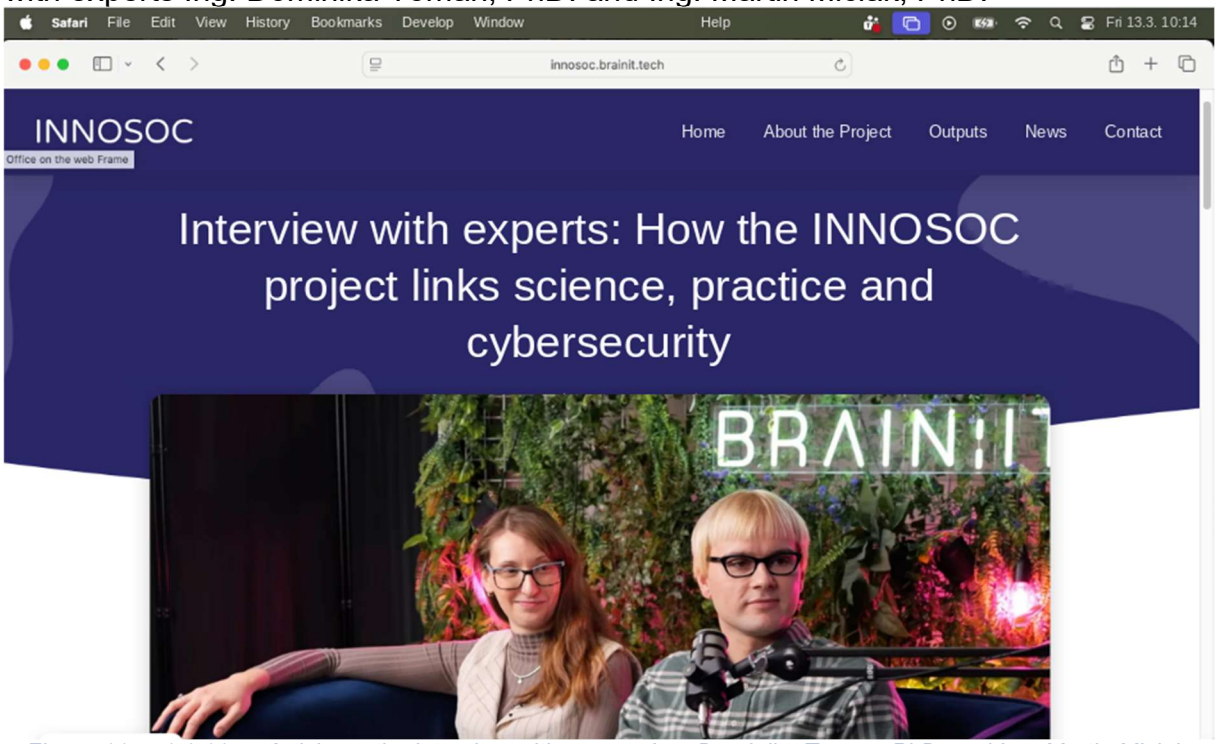


Figure 11: 4.1.1.11 Article on the interview with experts Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD., Source: (BRAIN:IT, 2025)

1.1.1.12 *Article on the interview about the INNOSOC project: Cybersecurity and broadening horizons with Dominika Toman*

On 11 February 2026, an article was published on the INNOSOC project website presenting an interview with **Ing. Dominika Toman, PhD.**, assistant professor at the Department of Management Theories of the Faculty of Management Science and Informatics, University of Žilina. The interview outlines her role in the project, particularly in supporting project management and team coordination, and also highlights the importance of the project for both the professional community and the wider public.

The article emphasises the contribution of the INNOSOC project in disseminating knowledge about cybersecurity and supporting the implementation of modern security solutions. The project focuses on the scholarly publication of results, the presentation of outputs at conferences, the preparation of analytical reviews of suitable solutions for enhancing cybersecurity and the preparation of materials for training the employees of organisations.

The interview also highlights the importance of cooperation between academia and practitioners, which makes it possible to create high-quality and practically applicable project outputs. The article also includes a reflection on the personal and professional development of the members of the project team, who, through their participation in the project, are gaining new knowledge and experience in the field of project management and cybersecurity.

The publication of the article on the project website contributes to informing the public about the project's activities and to the popularisation of cybersecurity topics.

The full text of the article can be found in Annex 18 – Article on the interview about the INNOSOC project: Cybersecurity and broadening horizons with Dominika Toman.

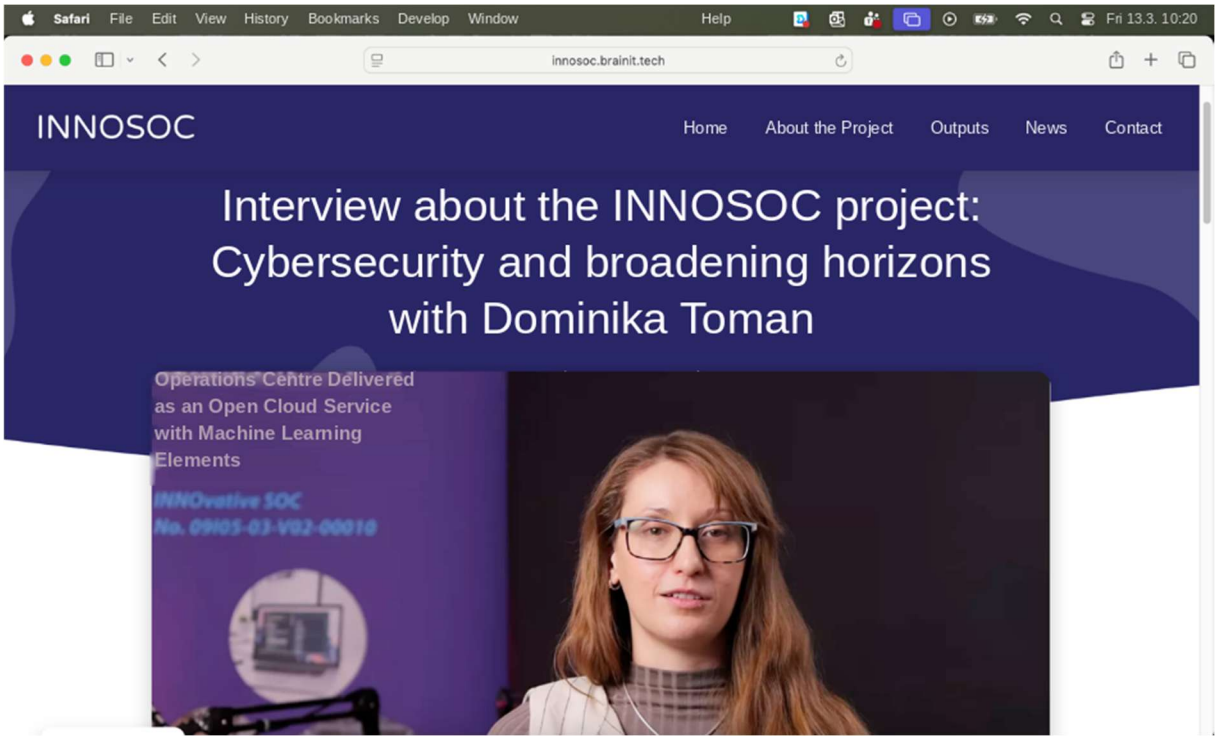


Figure 12: Article on the interview about the INNOSOC project: Cybersecurity and broadening horizons with Dominika Toman, Source: (BRAIN:IT, 2026)

1.1.1.13 Article on the interview about the INNOSOC project: On scientific research and cybersecurity with Martin Mičiak

On 12 February 2026, an article was published on the INNOSOC project website presenting an interview with Ing. Martin Mičiak, PhD., a researcher from the Department of Management Theories of the Faculty of Management Science and Informatics, University of Žilina. In the project, he works as a member of the research team and is also involved in supporting project management.

The interview outlines the main focus of the INNOSOC project in the field of cybersecurity and its effort to identify and implement effective solutions to strengthen the protection of organisations against cyber threats. Particular attention is paid to the use of open-source tools, which make it possible to build security solutions at lower cost while maintaining a high level of protection.

The article also highlights the importance of high-quality scientific outputs within the project, in particular the publication of research results in renowned scientific journals, databases and at professional conferences. The need to identify the so-called research gap, which makes it possible to bring new knowledge and advance research in the field of cybersecurity, is also emphasised.

The interview also presents the cooperation between the academic departments of the Faculty of Management Science and Informatics, University of Žilina, specifically between the Department of Management Theories and the

Department of InfoCom Networks. This interdisciplinary cooperation helps to connect the managerial and technological perspectives on cybersecurity and supports the creation of practically applicable project outputs.

The publication of the article on the project website contributes to the dissemination of information about the project's activities and to raising awareness of cybersecurity topics among both the professional community and the wider public.

The full text of the article can be found in Annex 19 – Article on the interview about the INNOSOC project: On scientific research and cybersecurity with Martin Mičiak.

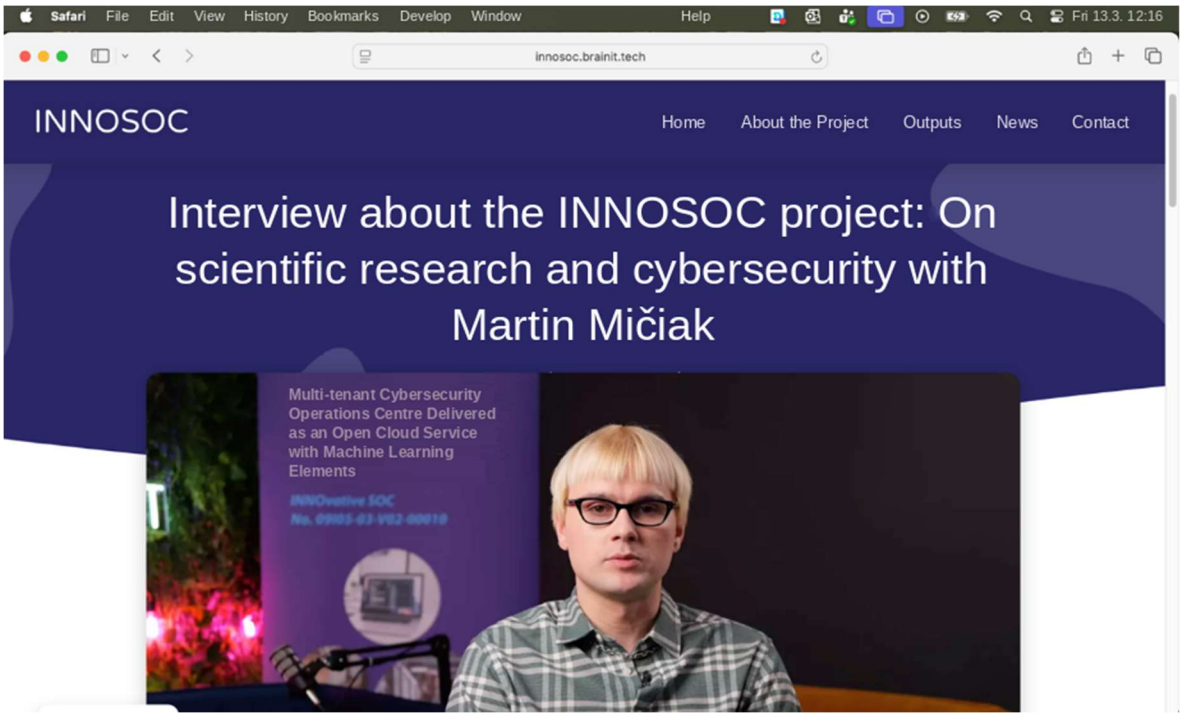


Figure 13: Article on the interview about the INNOSOC project: On scientific research and cybersecurity with Martin Mičiak. Source: (BRAIN:IT, 2026)

1.1.1.14 Article on the interview with prof. Ing. Milan Kubina, PhD. about the INNOSOC project

On 23 February 2026, an article was published on the INNOSOC project website presenting an expert interview with prof. Ing. Milan Kubina, PhD., which outlines the strategic direction of the project and its importance in the context of growing cyber threats. The interview emphasises that the project responds to the increasing risks of exploitation of system vulnerabilities in the digital environment and focuses on the development of modern tools supporting the protection of information systems.

The article presents the main objectives of the project, in particular the development of innovative solutions for the Security Operations Center (SOC) and tools for IP network management. Emphasis is placed on increasing the cyber

resilience of organisations with limited budgets, such as small and medium-sized enterprises, public administration bodies and educational institutions.

The interview also refers to the current state of development of the solution and emphasises the importance of cooperation between academia and applied practice. A key role in the project is played by the synergy between the research departments and the technology company BRAIN:IT, which makes it possible to transfer research results into practically applicable solutions.

The publication of the article on the project website contributes to informing both the professional community and the wider public about the project's activities and supports the dissemination of knowledge in the field of cybersecurity.

The full text of the article can be found in Annex 20 – Article on the interview with prof. Ing. Milan Kubina, PhD. about the INNOSOC project.

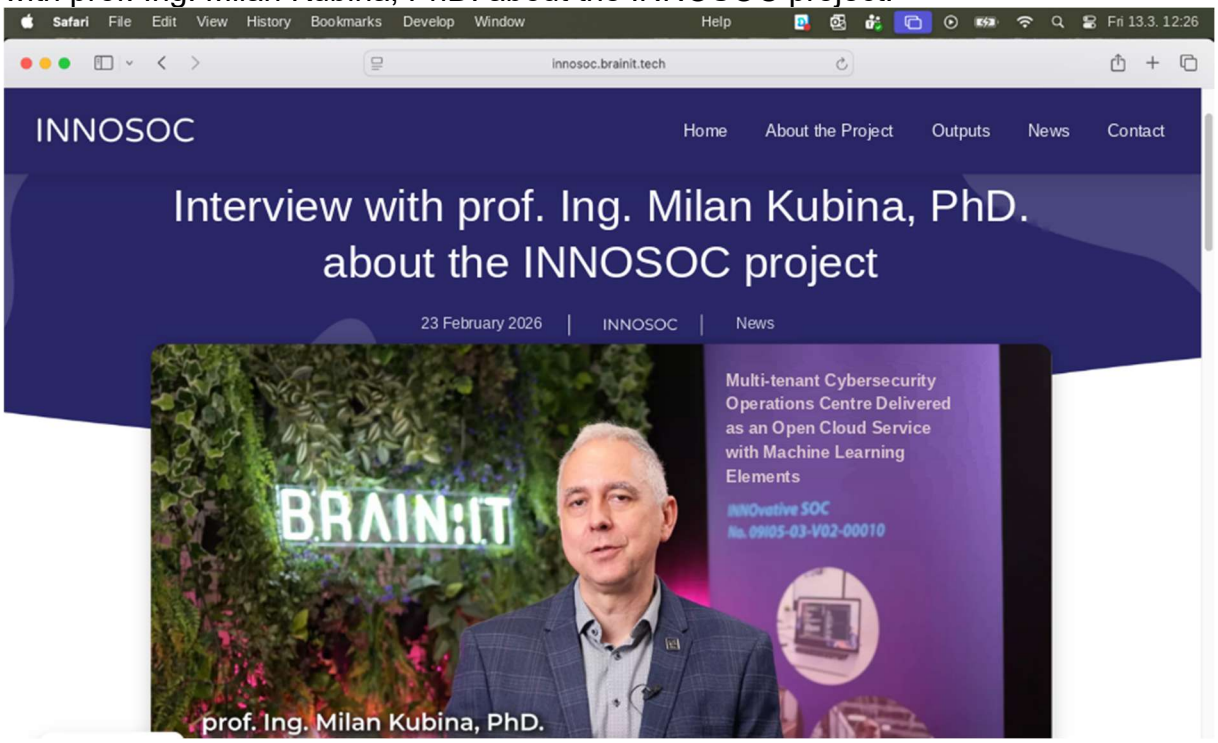


Figure 14: Article on the interview with prof. Ing. Milan Kubina, PhD. about the INNOSOC project, Source: (BRAIN:IT, 2026)

1.2 Social Media

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

1.2.1 Implemented Activities

1.2.1.1 Creation of a page on the LinkedIn social network

For communicating and sharing information with the community of professionals, which includes 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 community effectively. The page also communicates longer professional posts and articles and serves as a channel for communication with the professional community. The nature of this social network ensured a high degree of credibility.

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

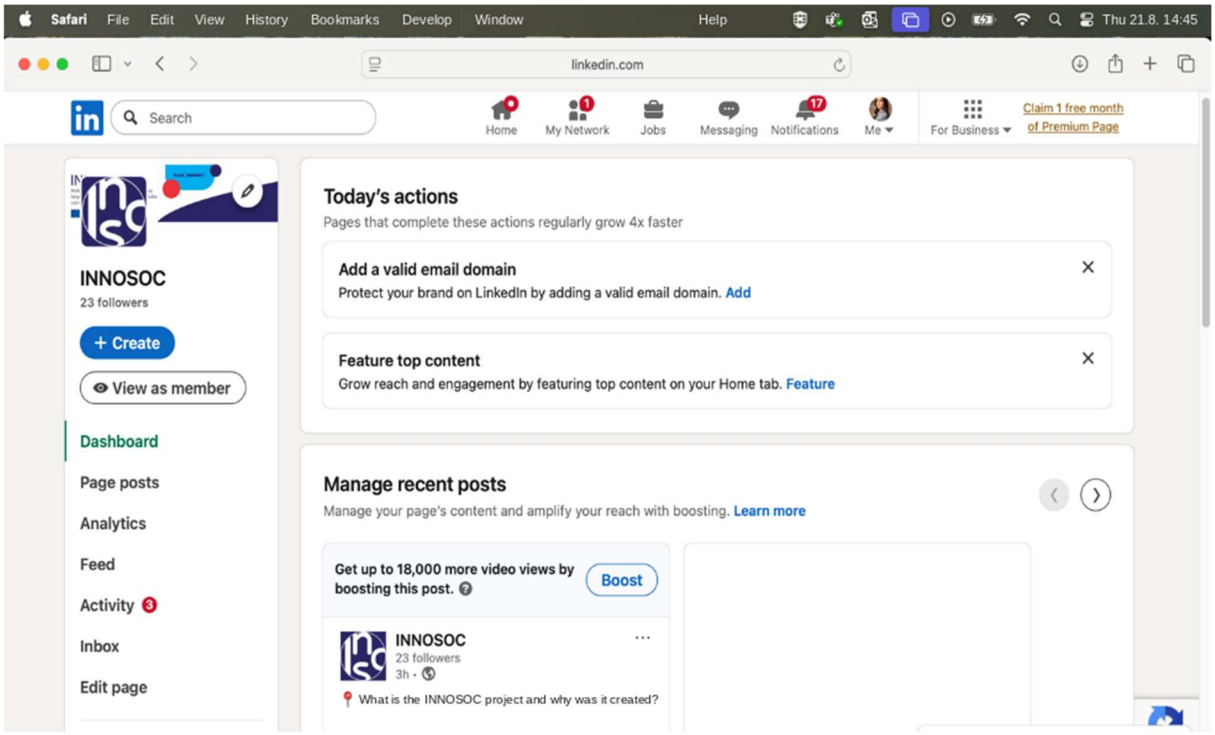


Figure 15: LinkedIn page for the INNOSOC project, Source: (BRAIN:IT, 2025)

1.2.1.2 Creation of a profile on the Instagram social network

For communication 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 that introduces it to anyone who visits the profile. The profile also contains a link to the website.

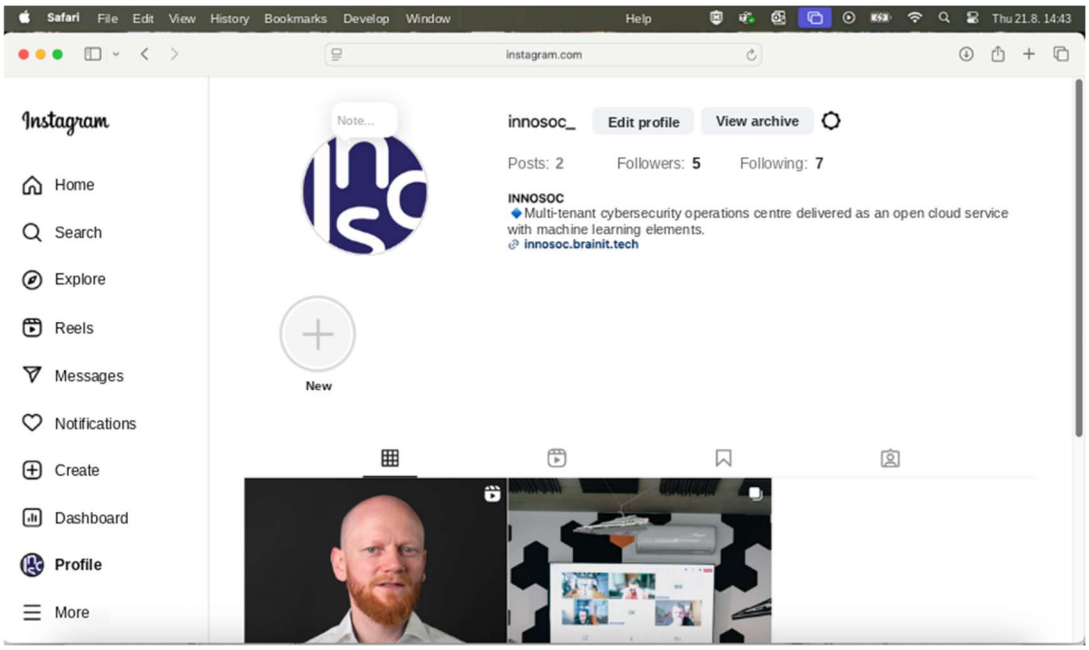


Figure 16: INNOSOC Instagram profile, Source: (BRAIN:IT, 2025)

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

The aim of the post on the @brainit.tech Instagram profile, published on 26 June 2025, was initially to 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.

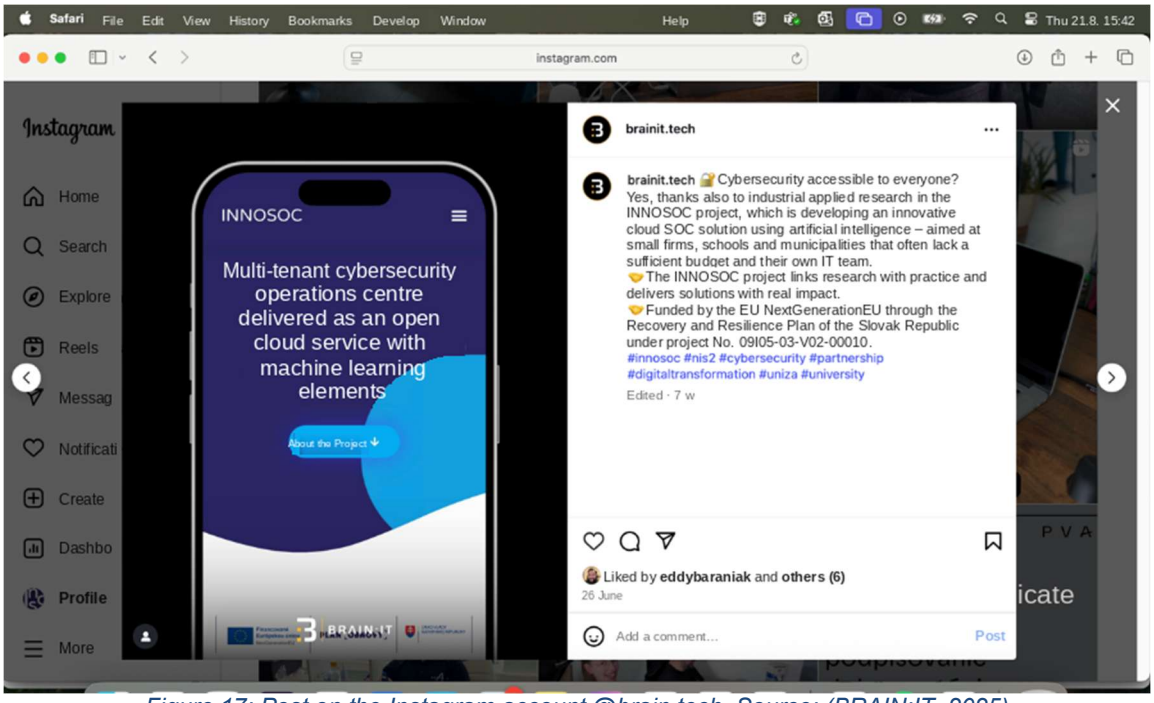


Figure 17: Post on the Instagram account @brain.tech, Source: (BRAIN:IT, 2025)

*1.2.1.4 Post on the partners' 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 on the meeting of 15 July 2025 communicates the current progress of work on the project, its further direction and the organisational activities for the following period, which were addressed 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 engage and reach secondary school and university students. The published posts can be seen in Figure 14.

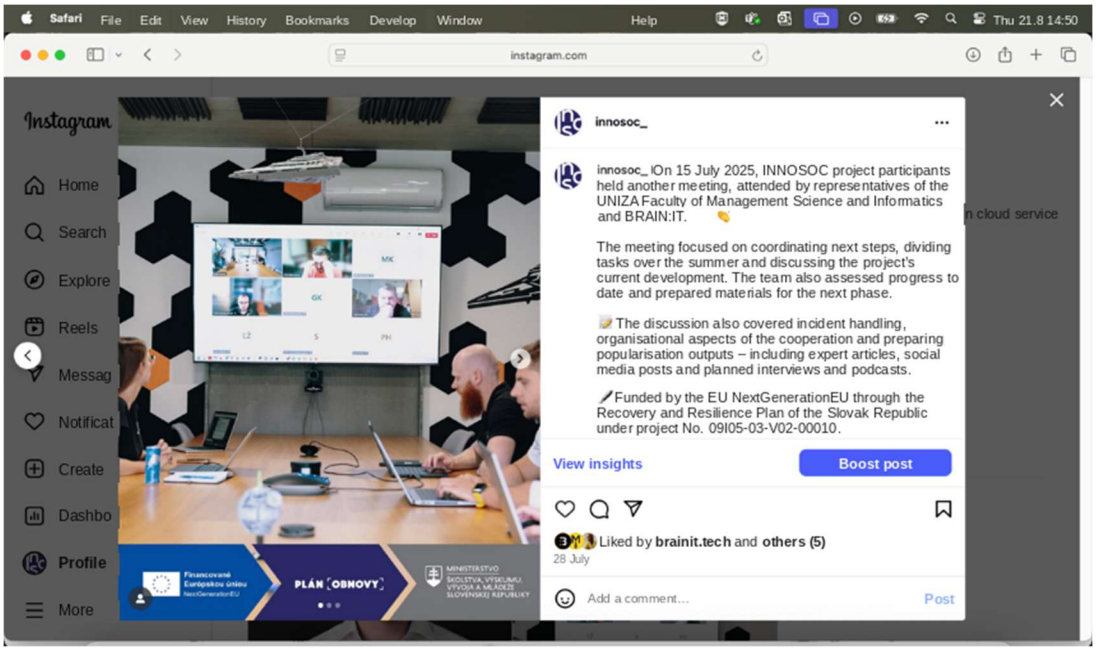


Figure 18: Post on the partners' meeting of 15.7.2025 on Instagram @innosoc_, Source: (BRAIN:IT, 2025)

1.2.1.5 Post on the partners' 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 on the meeting of 15.7.2025 communicates the current progress of work on the project, its further direction and the organisational activities for the following period, which were addressed at an online meeting. Publishing on the LinkedIn social network creates 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.

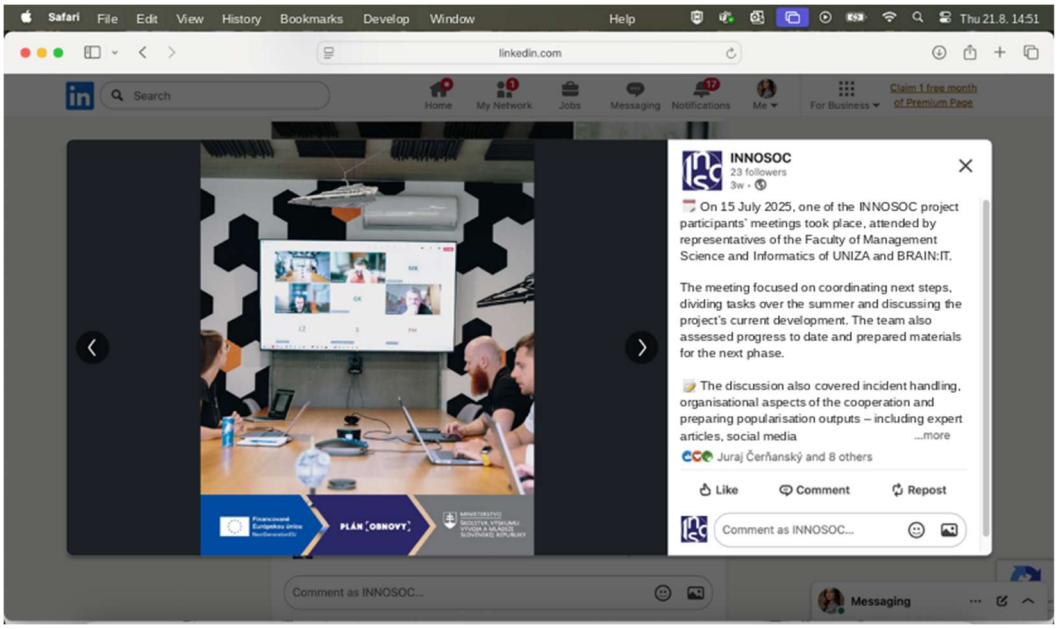


Figure 19: Post on the partners' meeting of 15.7.2025 on LinkedIn @INNOSOC, Source: (BRAIN:IT, 2025)

1.2.1.6 Post on basic information about the INNOSOC project on the @innosoc_ Instagram profile and the @INNOSOC LinkedIn page 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 can be found on the @INNOSOC YouTube channel. 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 the information to be shared more widely. The aim of the video is to raise awareness of the project and to explain its objective and importance 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.

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

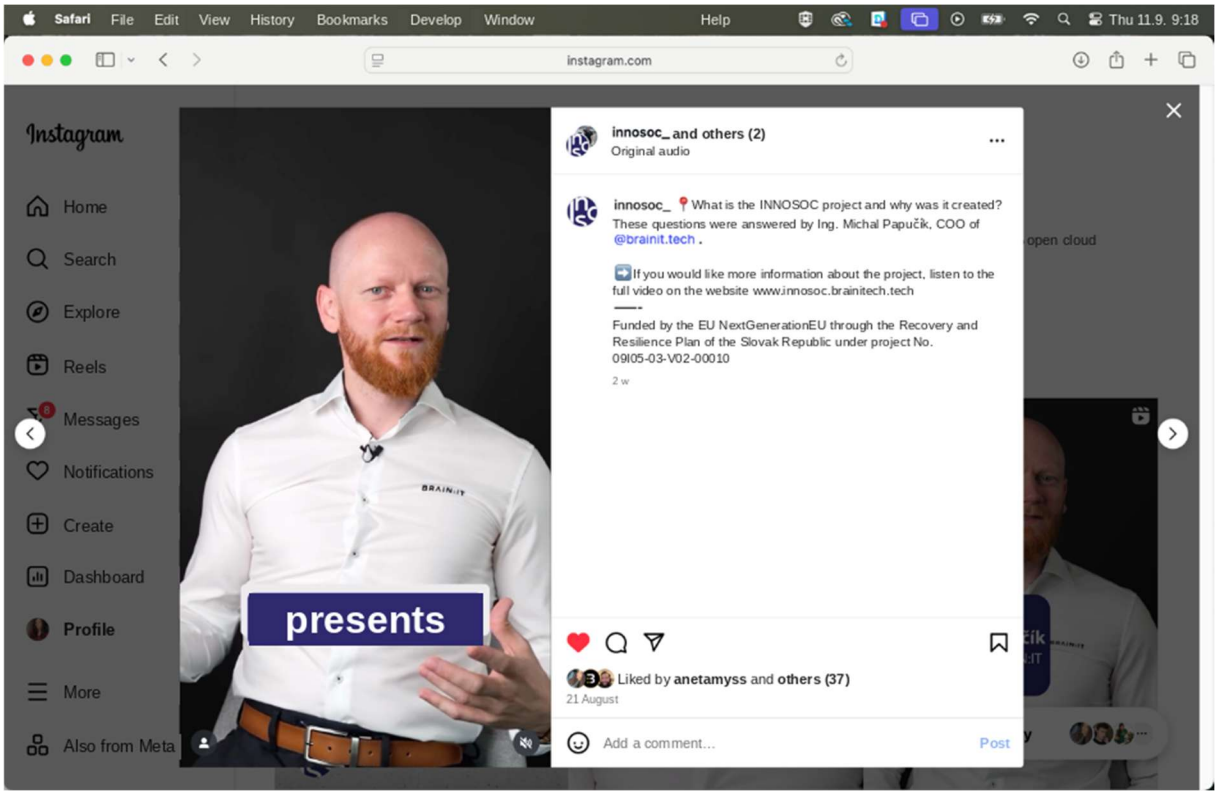


Figure 20 Post in the form of a short video on Instagram @innosoc_ of 21.8.2025, Source: (BRAIN:IT, 2025)

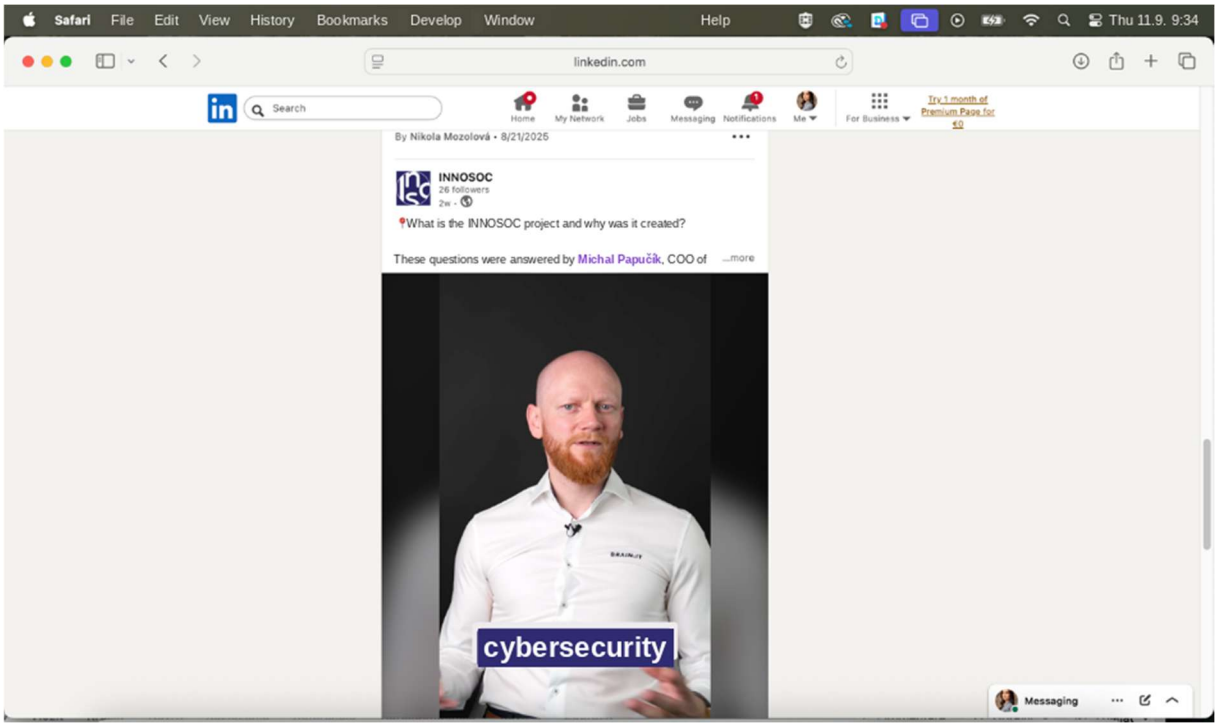


Figure 21 Post in the form of a short video on the LinkedIn page @INNOSOC of 21.8.2025 , Source: (BRAIN:IT, 2025)

1.2.1.7 *Post on basic information about the INNOSOC project on the @innosoc_ Instagram profile and the @INNOSOC LinkedIn page 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, the full version of which is published on the @INNOSOC YouTube channel. The video contains a brief explanation of the project's objective. The video has been produced in 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 community. 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.

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

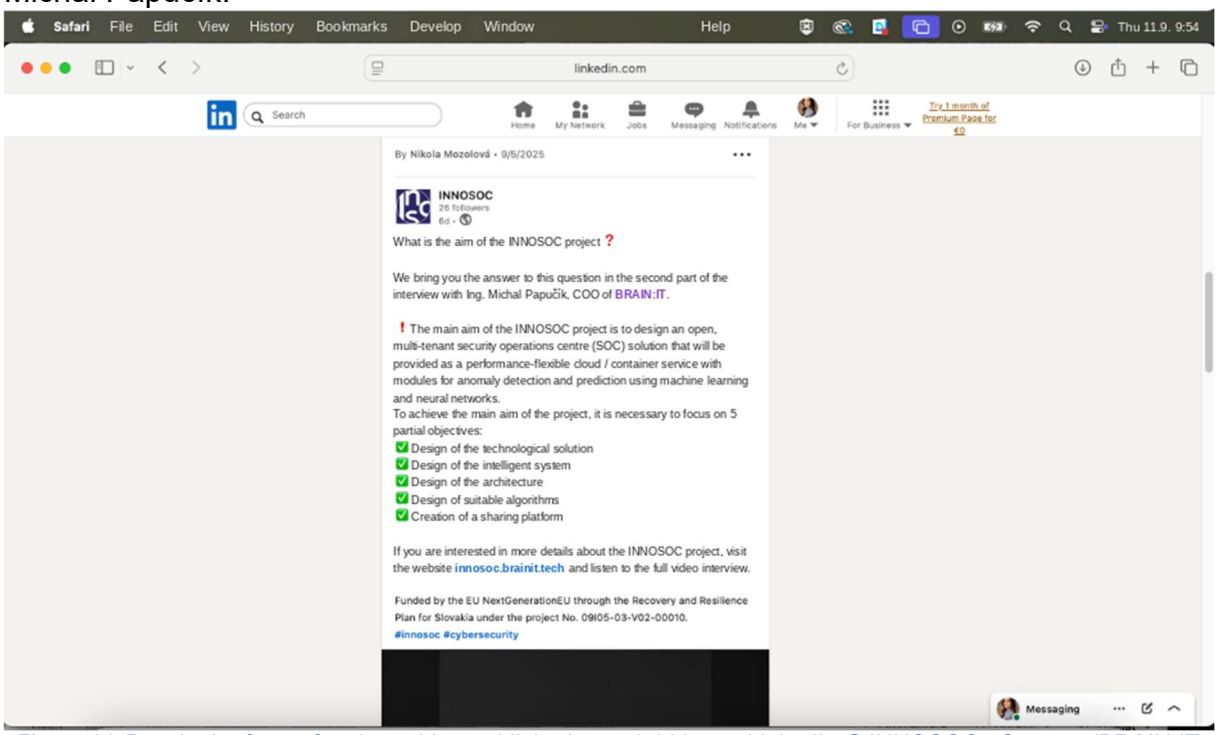


Figure 22 Post in the form of a short video published on 5.9.2025 on LinkedIn @INNOSOC , Source: (BRAIN:IT, 2025)

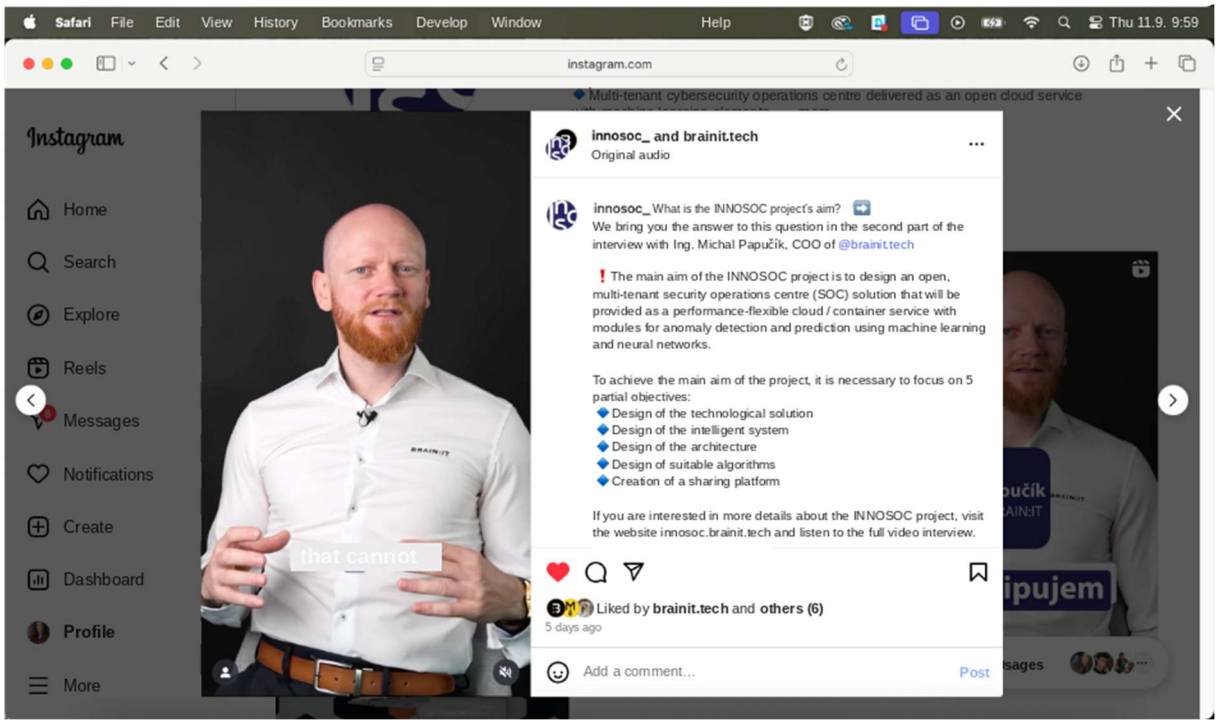


Figure 23 Post in the form of a short video published on 5.9.2025 on Instagram @innosoc_ , Source: (BRAIN:IT, 2025)

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

As part of education in the field of cybersecurity, 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, so the audience has the opportunity to think and choose the correct answer, which they can also check in the post. The aim of the post is to educate and raise awareness of threats in the cyber world. The questions in the quiz follow on from a popularisation 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.

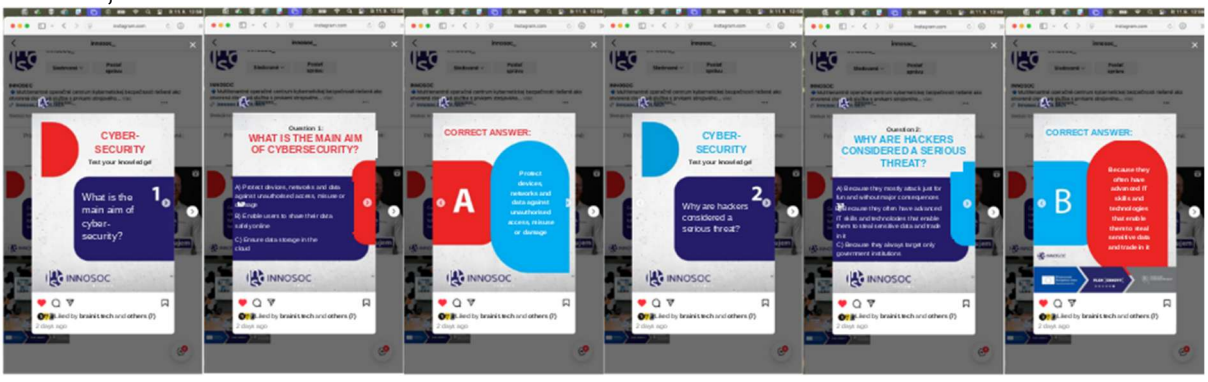


Figure 24 Post in the form of a quiz on the topic of cybersecurity published on 9.9.2025 on Instagram @innosoc_, Source: (BRAIN:IT, 2025)

1.2.1.9 *Post in the form of a quiz on the topic of cybersecurity published on 16 September 2025*

As part of education in the field of cybersecurity, 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, so the audience has the opportunity to think and choose the correct answer. The aim of the post is to educate and raise awareness of threats in the cyber world. The questions in the quiz follow on from a popularisation 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.

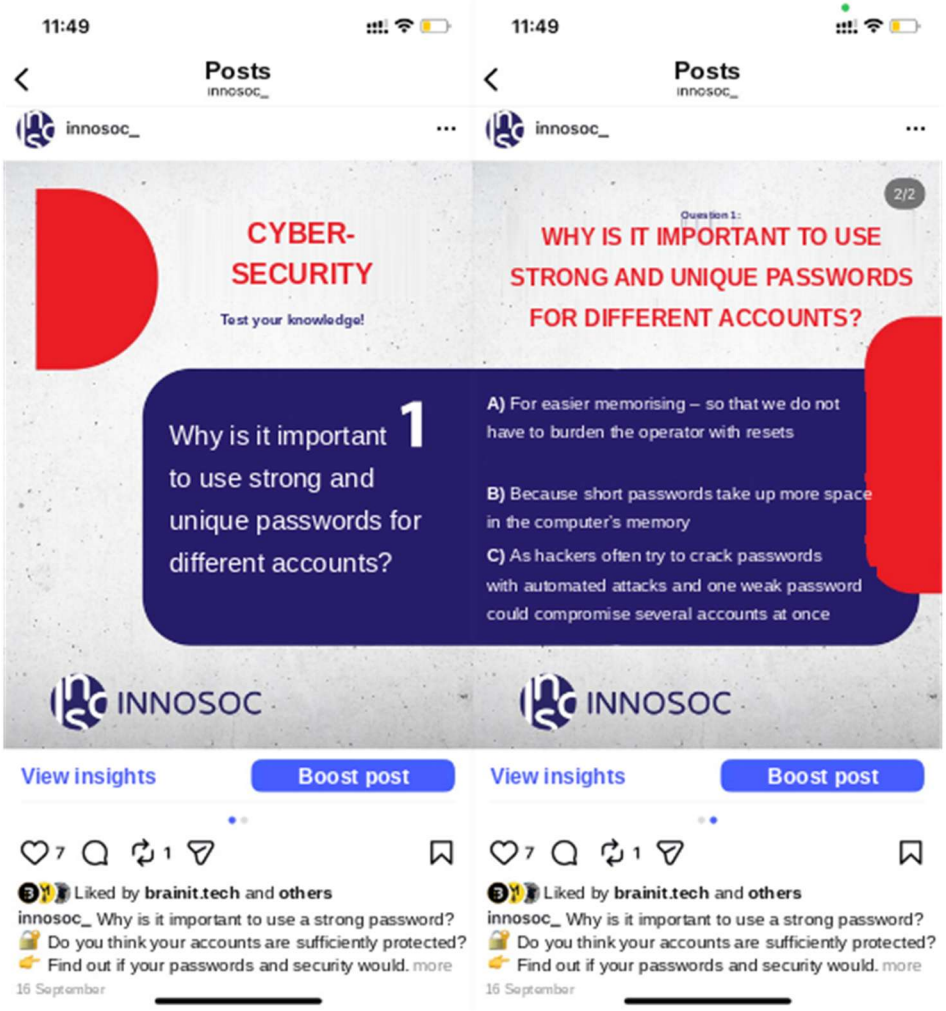


Figure 25: Post on the Instagram account @innosoc_: cybersecurity quiz, Source: (BRAIN:IT, 2025)

1.2.1.10 *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 the issue of cybersecurity. To take part in 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 correctly answer a question from the field of cybersecurity, which was communicated both in the visual of the post and in the description of the post.

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 a further layer of protection, so that 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.

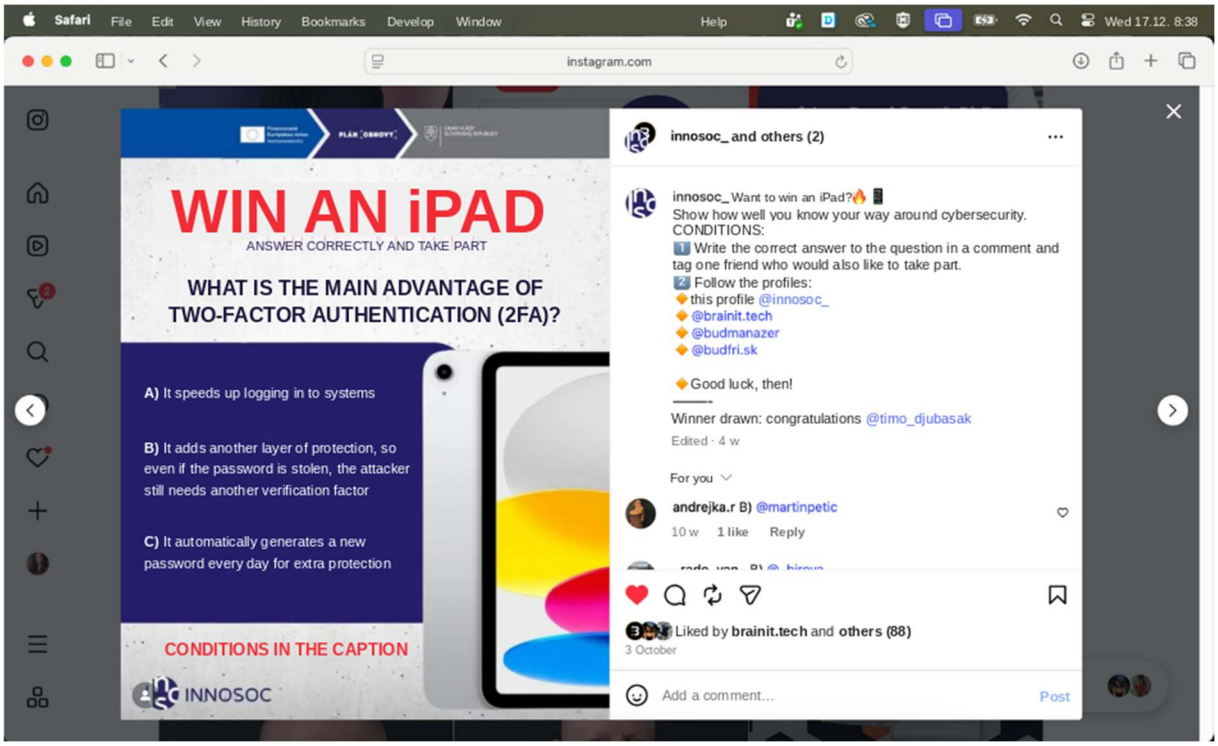


Figure 26: post on the Instagram account @innosoc_: iPad competition, Source: (BRAIN:IT, 2025)

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

On 17 October 2025, a short informational 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 entire interview is published in full on the INNOSOC YouTube channel. The short informational video communicates why cybersecurity is a key topic. The short video is 1:02 minutes long and has been produced in a form attractive for social media, with suitable 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. Pavol Segeč, PhD.

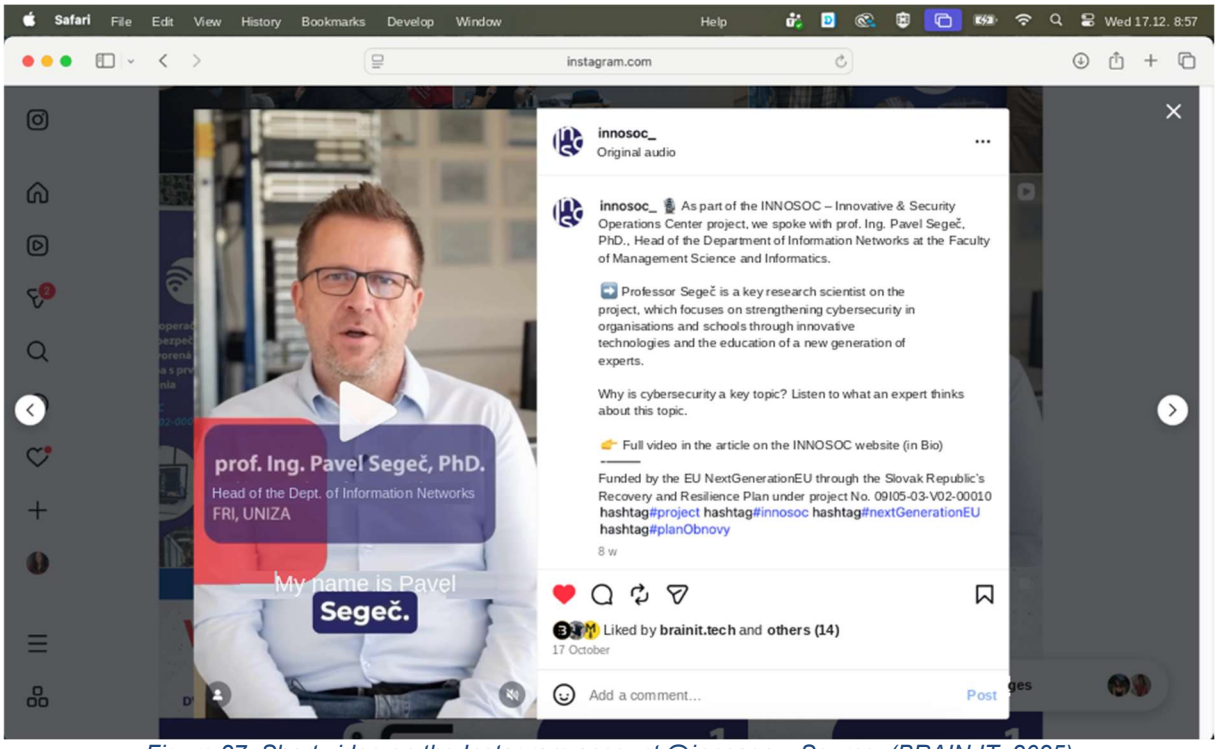


Figure 27: Short video on the Instagram account @innosoc_, Source: (BRAIN:IT, 2025)

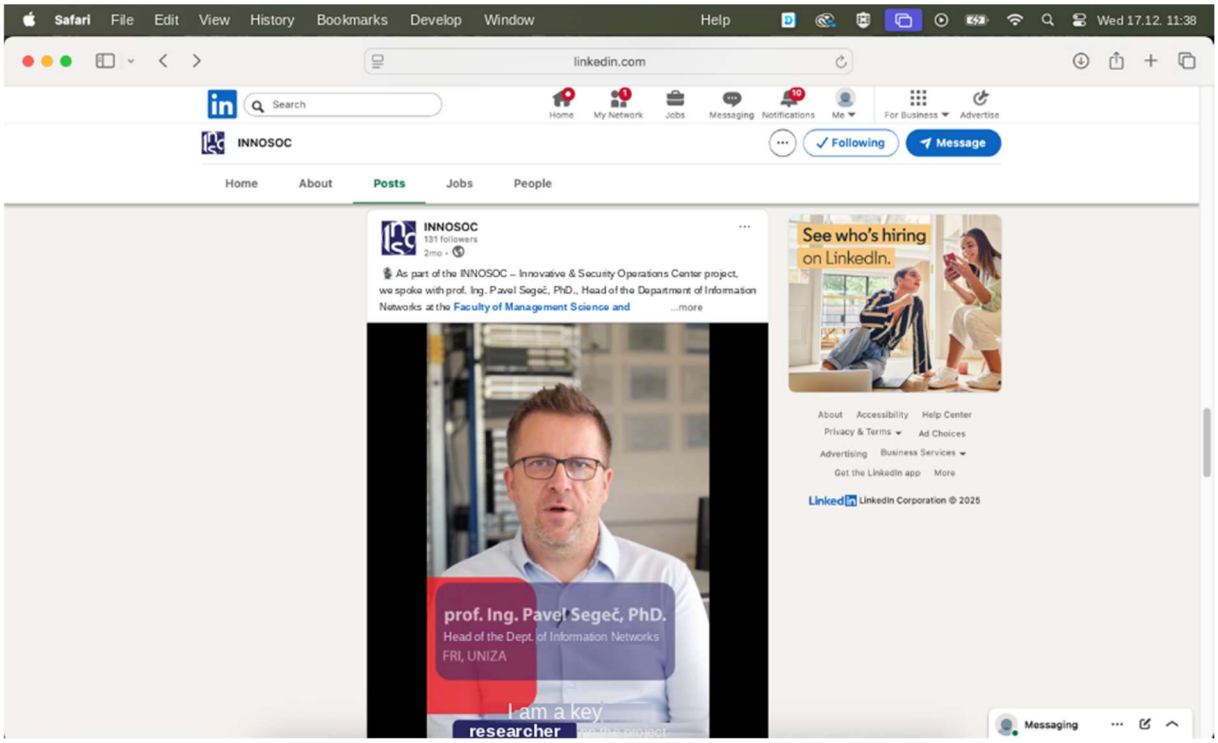


Figure 28: short video on the LinkedIn profile @innosoc: Interview with prof. Ing. Pavel Segeč, PhD., Source: (BRAIN:IT, 2025)

1.2.1.12 Informational post on the holding of the INNOSOC project symposium

On 18 November 2025, an informational and invitation post for the professional symposium on the topic “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, in particular students and the professional and academic community, about the holding of 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 via social media. The published content included:

- basic information about the symposium (date, time, venue),
- the thematic focus of the symposium in the area 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 is a dissemination and popularisation 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 target groups.

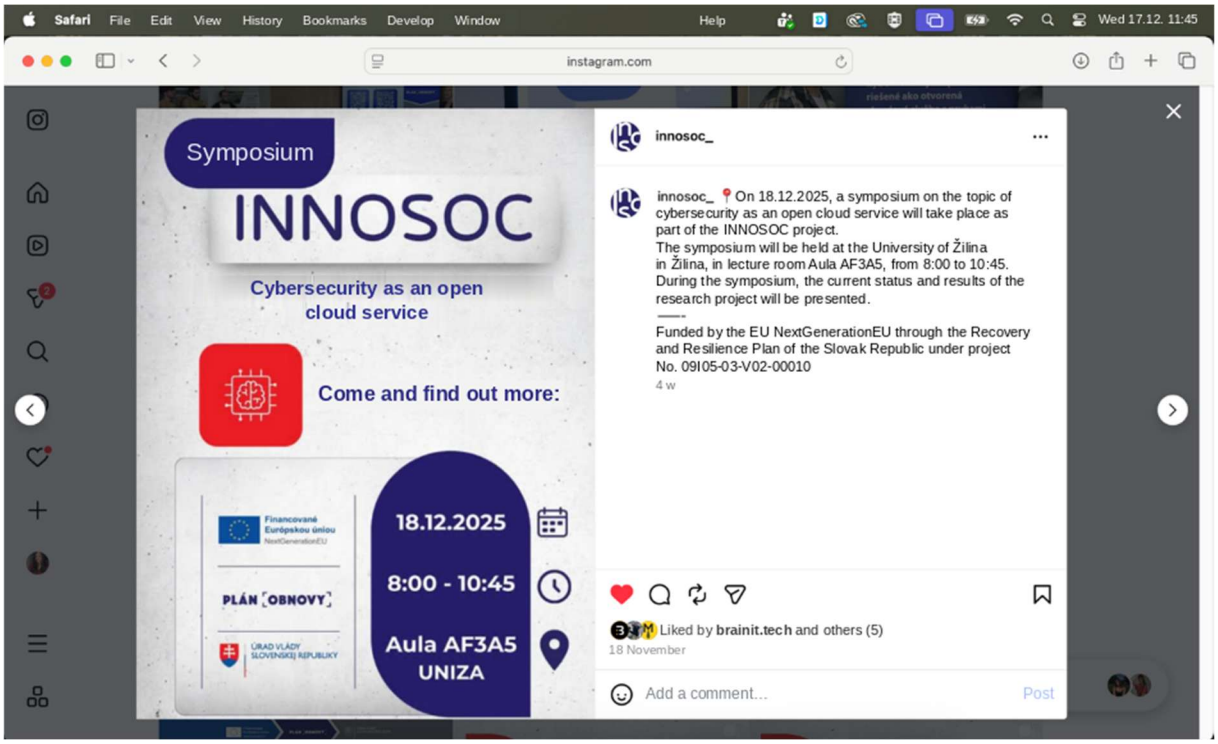


Figure 29: Post on the Instagram account @innosoc_: announcement of the symposium, Source: (BRAIN:IT, 2025)

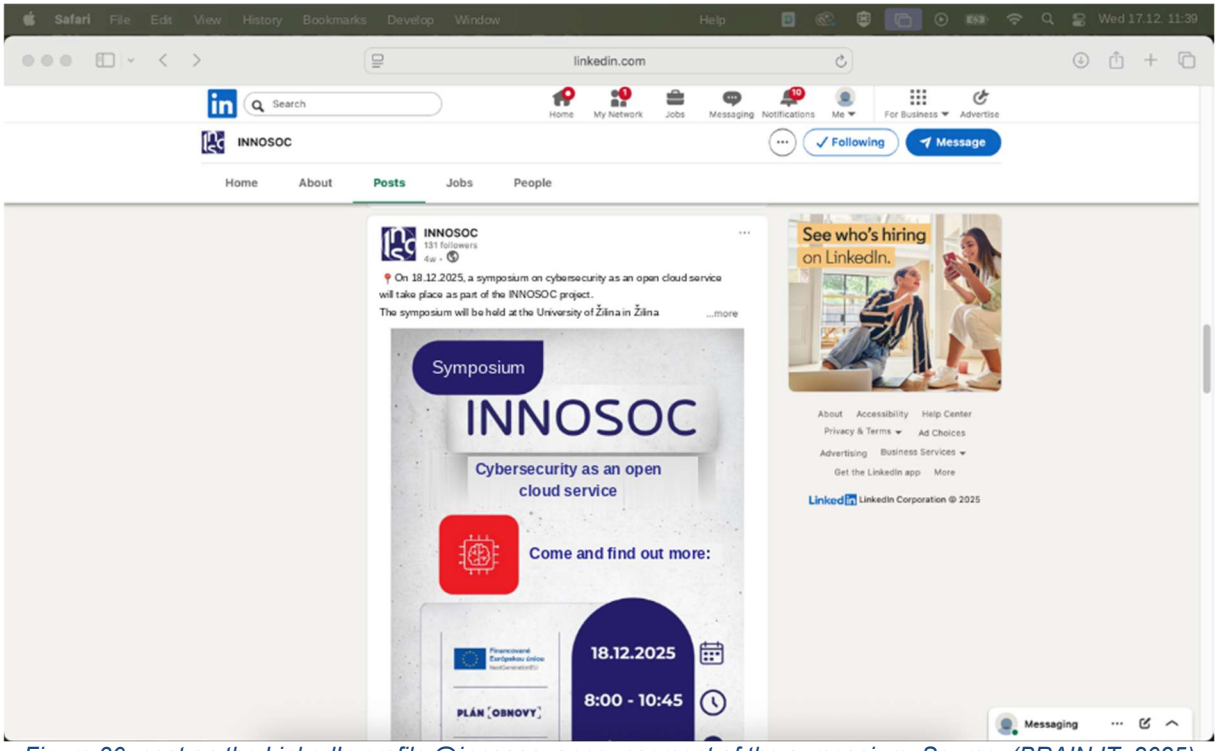


Figure 30: post on the LinkedIn profile @innosoc: announcement of the symposium, Source: (BRAIN:IT, 2025)

1.2.1.13 Post on the conclusion of the iPad competition

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

The aim of the post was to encourage young students to get involved 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 media. The published content included:

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

The post is a **dissemination and popularisation output of the project**, which contributed to the visibility of the INNOSOC project among the student public, encouraged interaction with the target group and increased the attractiveness of the project through educational and motivational activities.

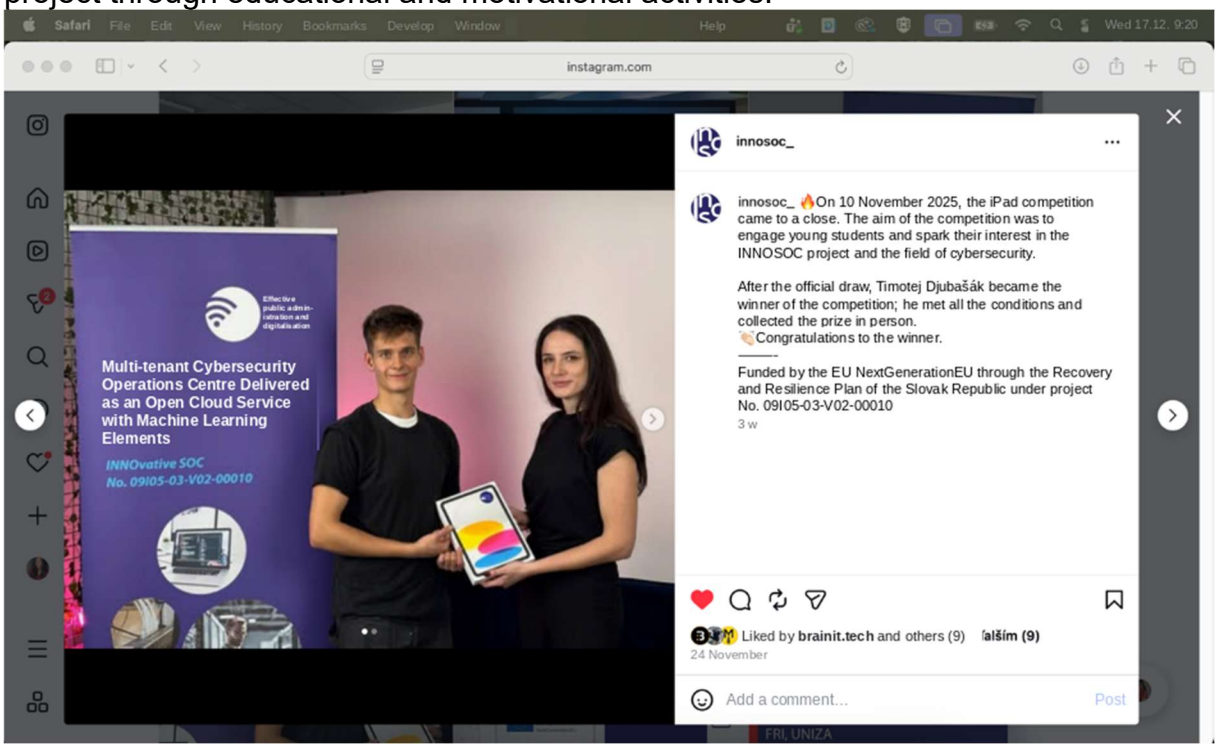


Figure 31:post on the Instagram profile @innosoc_: presentation of the competition prize, Source: (BRAIN:IT, 2025)

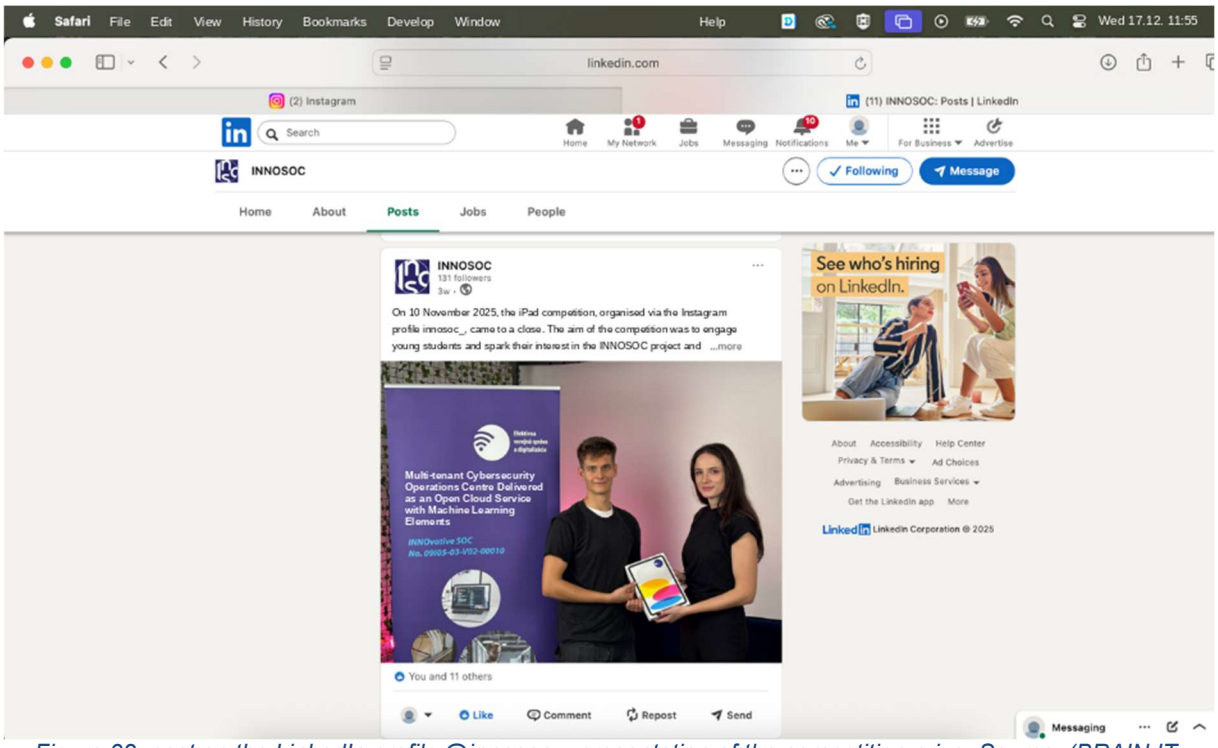


Figure 32: post on the LinkedIn profile @innosoc_: presentation of the competition prize, Source: (BRAIN:IT, 2025)

1.2.1.14 Post on the presentation of the INNOSOC project at the student breakfast

On 28 November 2025, a post was published on the Instagram profile @innosoc_ about the student breakfast that took place on 4 November 2025 at the Faculty of Management Science and Informatics, 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 acquaint them with the current state, outputs and future direction of the project in the field of cybersecurity. The published content included:

- information on the holding of the student event and its informal character,
- the 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 on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic.

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

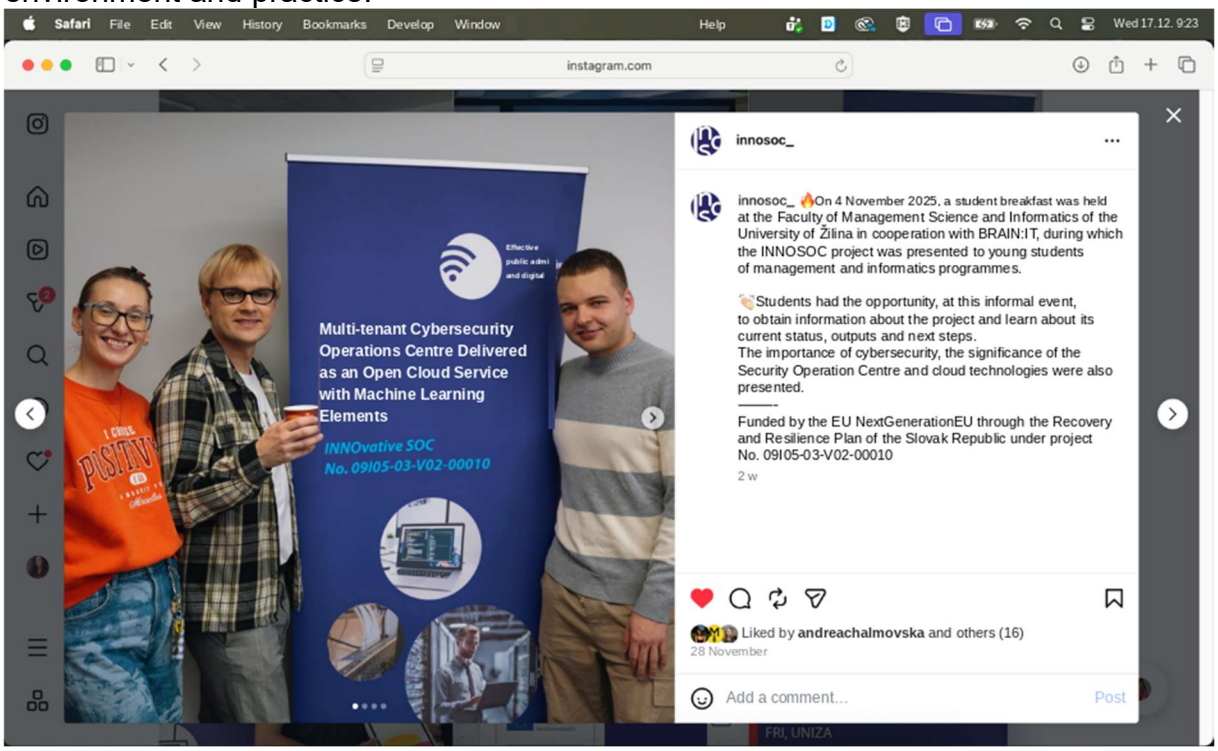


Figure 33:post on the Instagram account @innosoc_: presentation at the student breakfast, Source: (BRAIN:IT, 2025)

1.2.1.15 Post on the presentation of the INNOSOC project at Tomas Bata University in Zlín

On 10 December 2025, a post was published about the presentation of the INNOSOC project to students of the Faculty of Applied Informatics, 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 in the academic environment, to raise awareness of the INNOSOC project among students of information technology programmes and to explain to them the importance of cybersecurity in the context of digital transformation. The published content included:

- information on the presentation of the project to students of applied informatics,
- an introduction to the objectives, focus and benefits of the INNOSOC project,
- an 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,
- a presentation of the principles and technologies used in the project,
- visual documentation from the lecture,
- information on the funding of the project from EU resources – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic.

The post is a dissemination, presentational and popularisation 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.

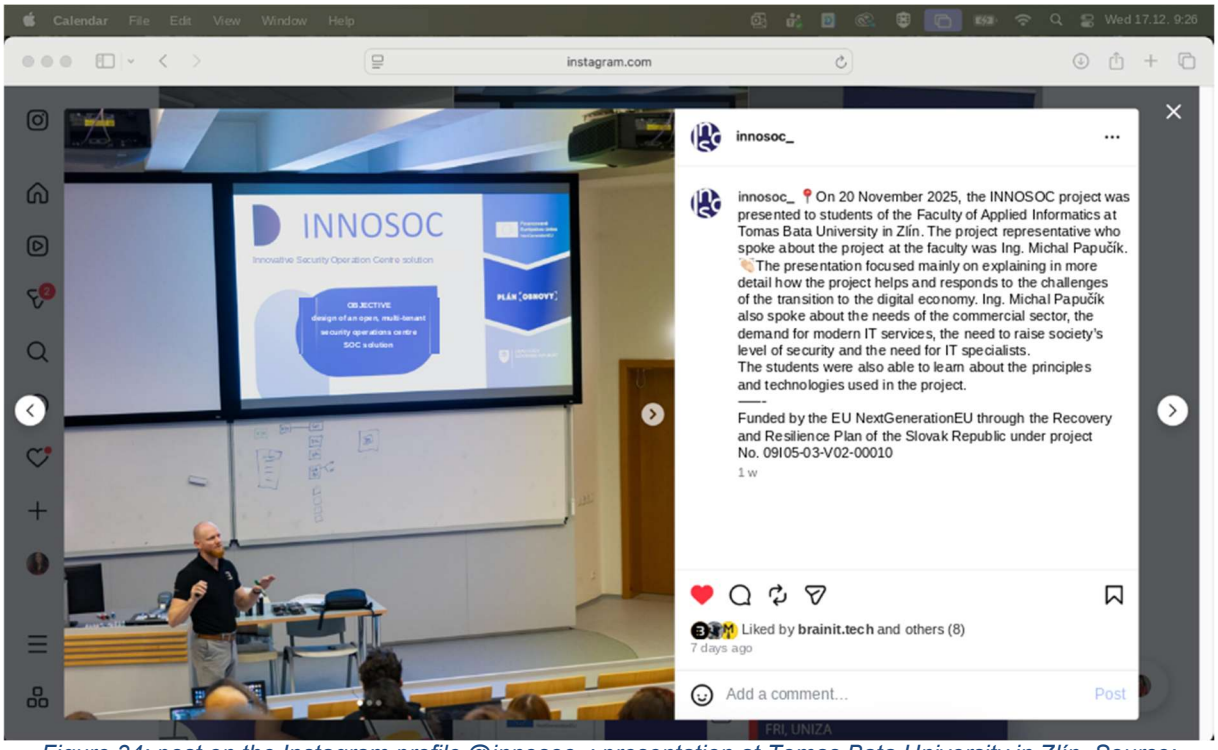


Figure 34: post on the Instagram profile @innosoc_: presentation at Tomas Bata University in Zlín, Source: (BRAIN:IT, 2025)

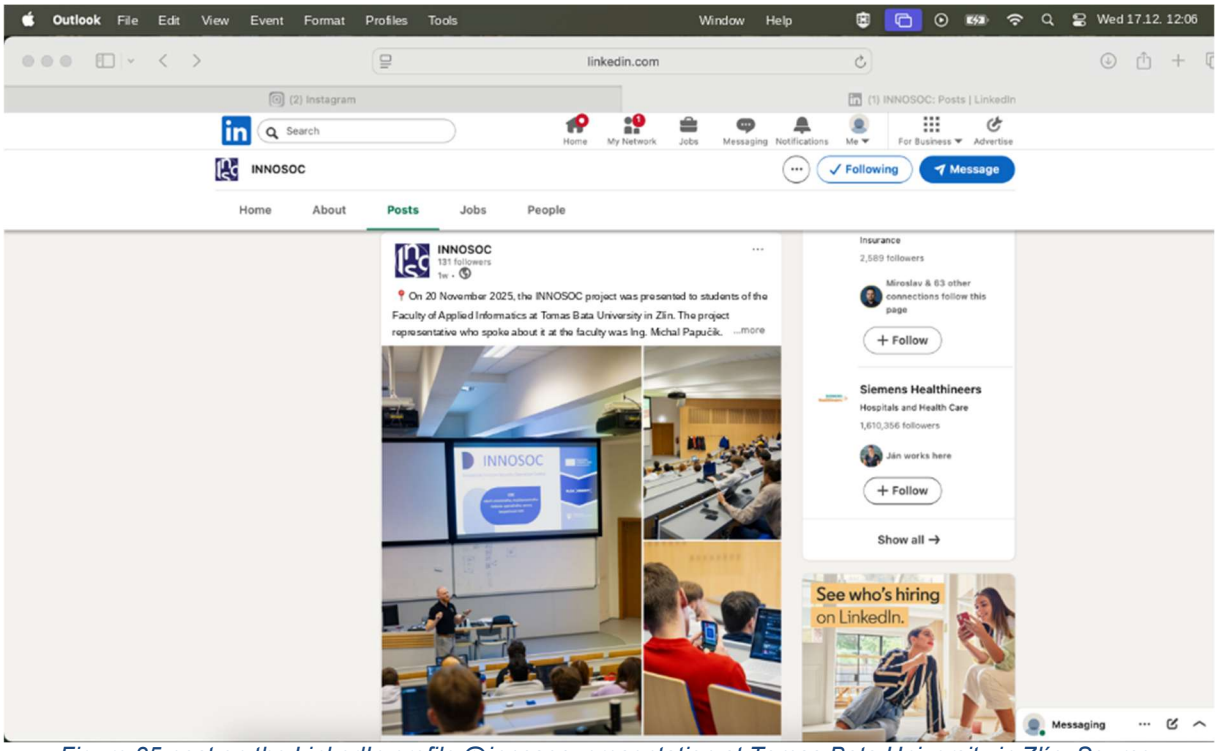


Figure 35:post on the LinkedIn profile @innosoc: presentation at Tomas Bata University in Zlín, Source: (BRAIN:IT, 2025)

1.2.1.16 Post on the presentation of the INNOSOC project at the Jozef Murgaš Secondary Technical School in Banská Bystrica

On 12 December 2025, a post was published 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 the implementation of an educational activity aimed at raising awareness of cybersecurity among secondary school pupils and to explain to them the importance of the INNOSOC project in the context of protecting the digital space. The published content included:

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

The post is a dissemination, educational and popularisation 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.

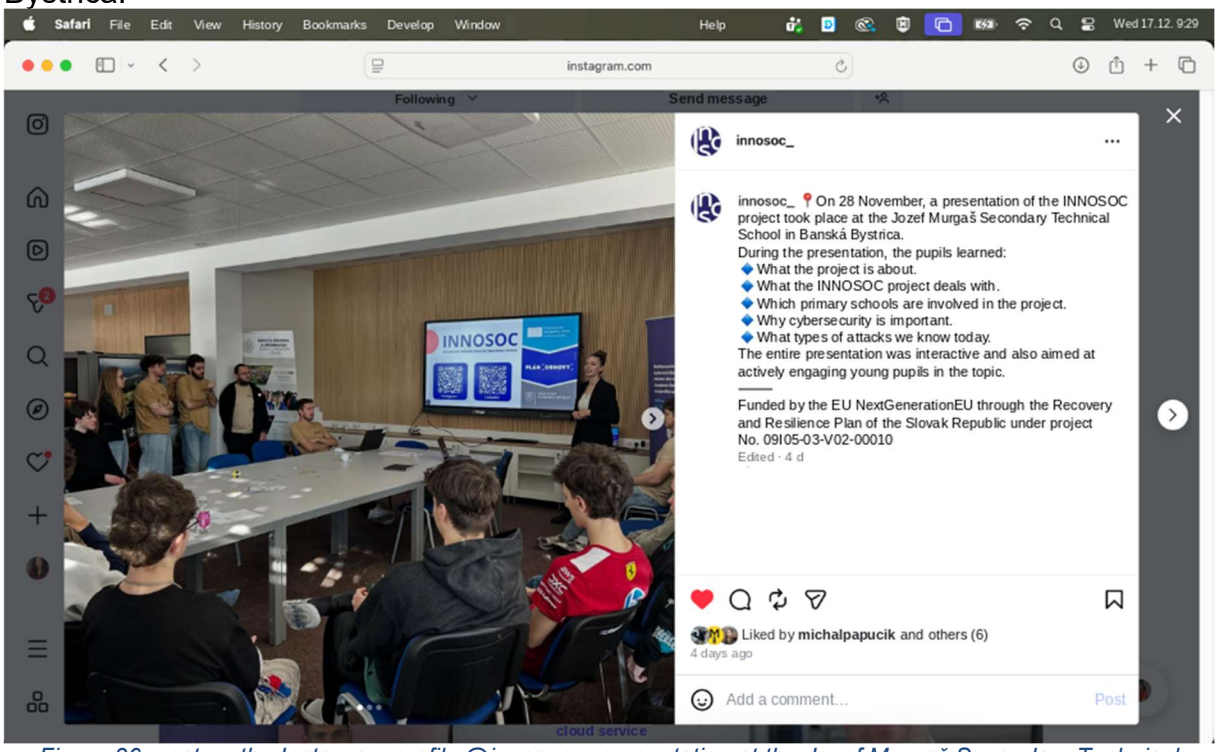


Figure 36: post on the Instagram profile @innosoc_: presentation at the Jozef Murgaš Secondary Technical School in Banská Bystrica, Source: (BRAIN:IT, 2025)

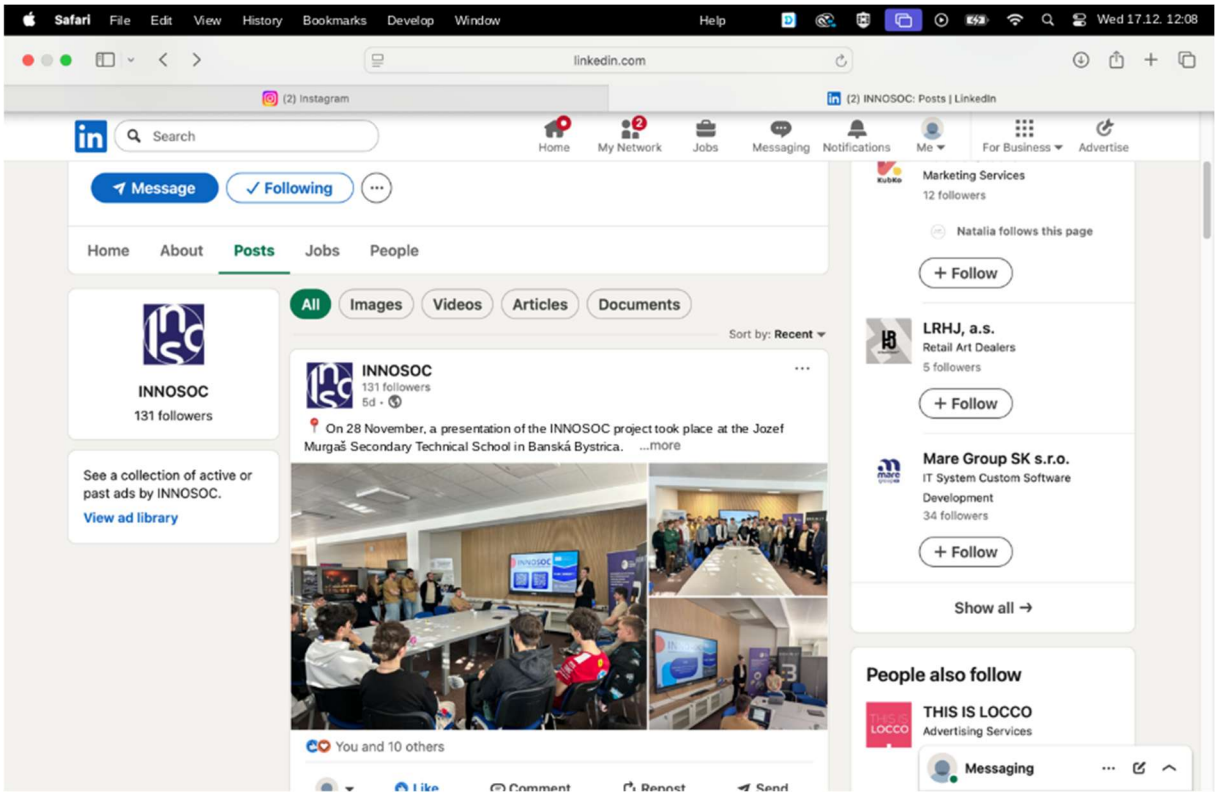


Figure 37: post on the LinkedIn profile @innosoc: presentation at the Jozef Murgaš Secondary Technical School in Banská Bystrica, Source: (BRAIN:IT, 2025)

1.2.1.17 Short video – interview with Ing. Martin Mičiak, PhD.

On 11 February 2026, as part of the communication and popularisation activities of the INNOSOC project, a post was published on the Instagram profile @innosoc_ announcing the interview conducted with experts involved in the project – Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD. from the Faculty of Management Science and Informatics, University of Žilina. The post drew attention to the availability of the video interview published on the YouTube platform on the INNOSOC project channel.

The content of the interview explains how the project works and provides a deeper insight into the link between academic research and practical needs in the field of cybersecurity. The discussion focuses in particular on the importance of cooperation between the university environment and practitioners, which makes it possible to create innovative solutions while ensuring the practical applicability of the project outputs.

The post also provided information on the funding of the project from European Union resources – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic, within the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements” (project code 09I05-03-V02-00010). The publication of the post contributed to informing the public about the project’s activities and to spreading awareness of its outputs.

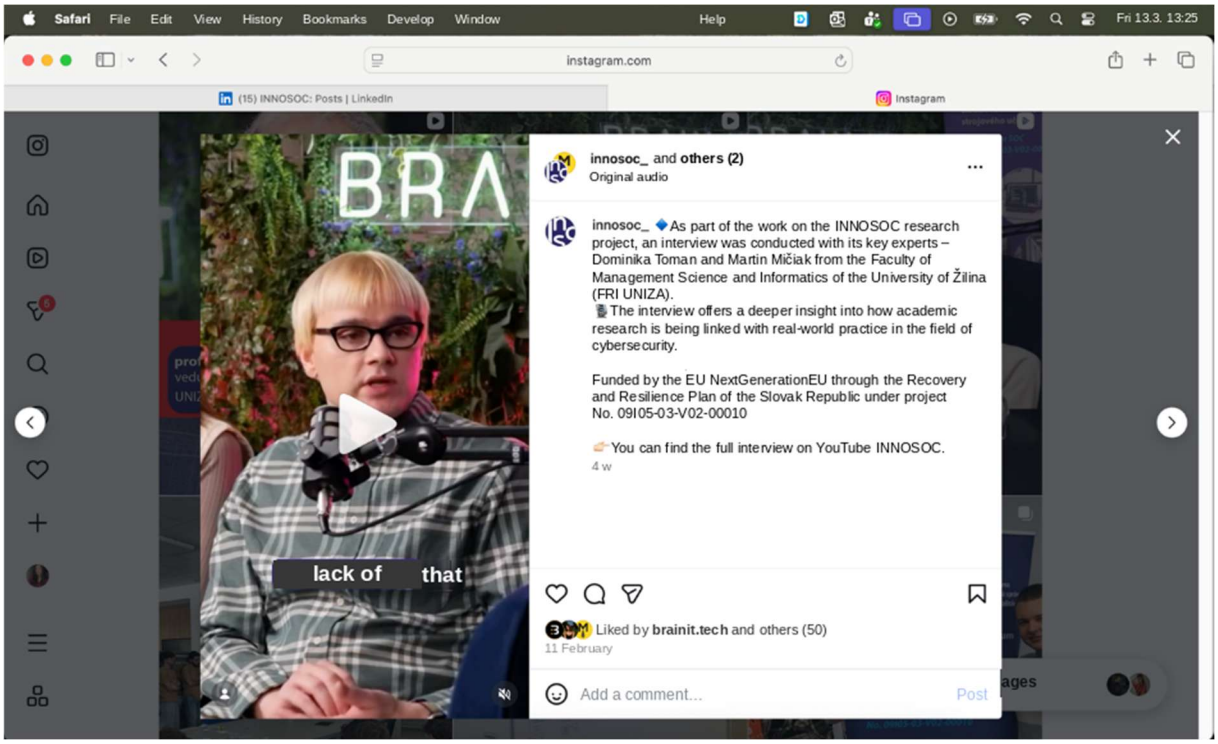


Figure 38: Post on the interview with Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD. on the Instagram profile @innosoc_, Source: (BRAIN:IT, 2026)

1.2.1.18 Short video – interview with Ing. Dominika Toman, PhD.

On 12 February 2026, as part of the communication activities of the INNOSOC project, a post was published on the Instagram profile @innosoc_ referring to the video interview with **Ing. Dominika Toman, PhD.** from the Faculty of Management Science and Informatics, University of Žilina. The post drew attention to the technical benefits of the project and to selected innovations implemented as part of its execution.

The content of the interview explains the technological aspects of the INNOSOC project, in particular the development and implementation of tools aimed at supporting cybersecurity and more effective monitoring of security events in information systems. It also highlights the practical benefits of the project and its technological innovations, which contribute to raising the level of protection of digital infrastructures.

The post also announced the availability of the full video interview on YouTube on the INNOSOC project channel and included information on the funding of the project by the European Union – **NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic**, under project No. 09I05-03-V02-00010. The publication of the post contributed to disseminating information about the technological outputs of the project and to raising awareness of its activities.

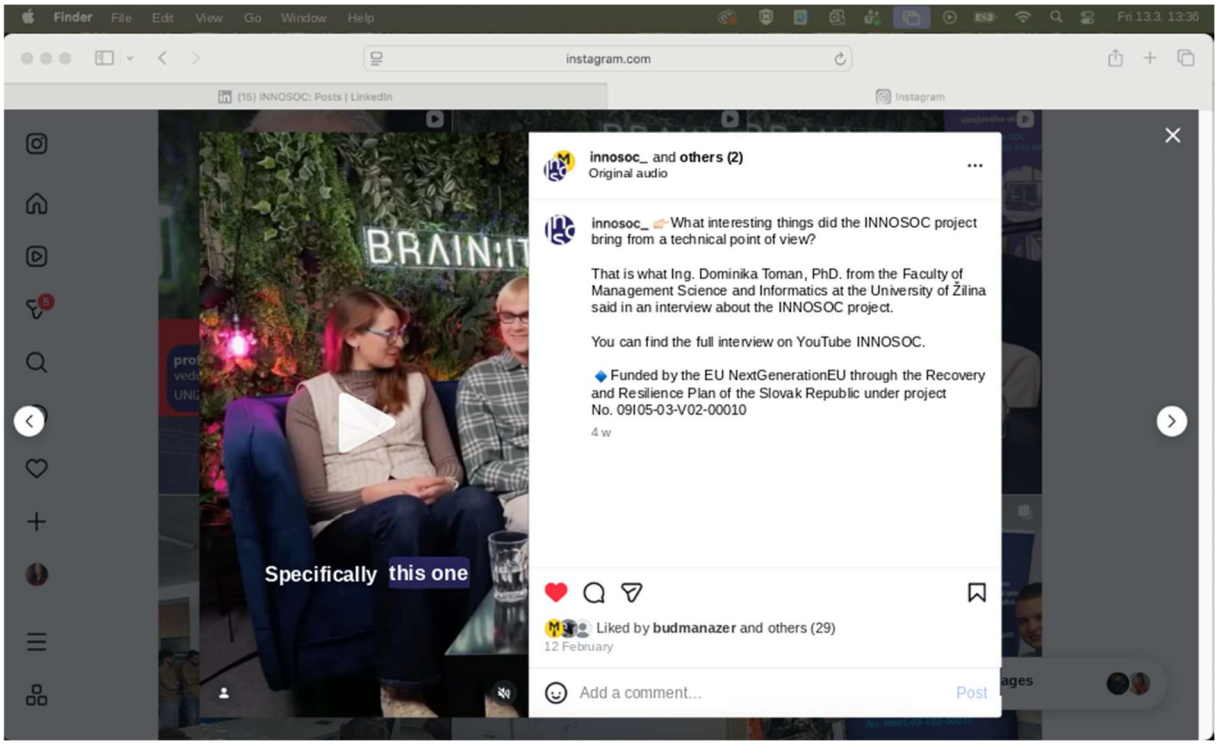


Figure 39: Post about the interview with Ing. Dominika Toman, PhD. on the Instagram profile @innosoc_, Source: (BRAIN:IT, 2026)

1.2.1.19 Short video – interview with prof. Ing. Milan Kubina, PhD.

On 25 February 2026, as part of the communication activities of the INNOSOC project, a post was published on the LinkedIn profile innosoc and the Instagram profile @innosoc_ announcing an expert interview with **prof. Ing. Milan Kubina, PhD.** The post presented the strategic direction of the project and its focus on addressing the growing risks associated with the exploitation of system vulnerabilities in the digital environment.

The content of the post presented the main objectives of the project, in particular the development of innovative tools for the Security Operations Center (SOC) and solutions for IP network management. It also highlighted the benefits of the project for organisations with limited financial resources, such as small and medium-sized enterprises, public administration bodies and educational institutions, which the project helps to increase their level of cybersecurity and resilience.

The post also pointed out the importance of cooperation between academia and practice, implemented in partnership with BRAIN:IT, which enables research results to be transferred effectively into practical solutions that can be used in practice. The communication also included information on the funding of the project by the European Union – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic under project No. 09I05-03-V02-00010.

The publication of the post contributed to informing both the professional community and the wider public about the project's activities and supported the spread of awareness of cybersecurity topics.

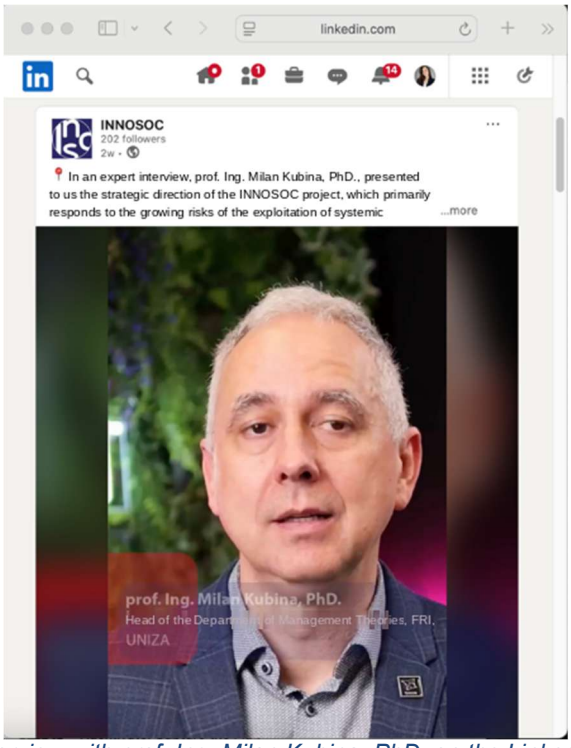


Figure 40: Post about the interview with prof. Ing. Milan Kubina, PhD. on the LinkedIn profile @innosoc, Source: (BRAIN:IT, 2026)

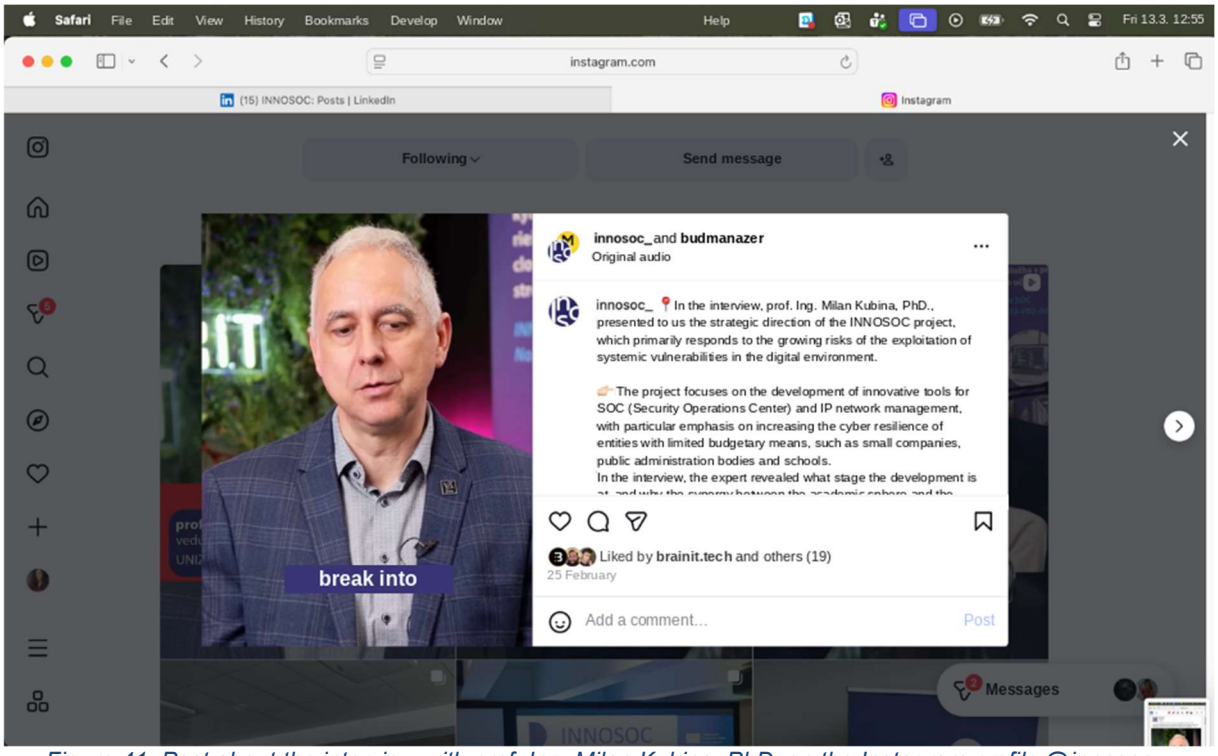


Figure 41: Post about the interview with prof. Ing. Milan Kubina, PhD. on the Instagram profile @innosoc_, Source: (BRAIN:IT, 2026)

1.3 Popularisation Texts

Popularisation texts were a key tool for effectively communicating the expert knowledge and results of the INNOSOC project to a broad range of target groups. Their main purpose was to transform complex technical information into a comprehensible and engaging form that would appeal not only to experts but also to the lay public, students and potential customers.

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

The popularisation articles were published primarily via the project website, where they created a comprehensive information resource on cybersecurity, cloud technologies and the importance of SOC solutions. At the same time, these texts were adapted for social media in the form of shorter posts, infographics and interactive content.

Particular emphasis was placed on the educational character of the texts, which explained basic terms such as "SOC", "multi-tenant architecture", "machine learning in cybersecurity" or "cloud services" in a manner accessible to different levels of technical

literacy. The objective was not only to inform, but also to educate and motivate readers to take a deeper interest in cybersecurity issues.

The content strategy of the popularisation texts was based on the principle of gradually building awareness and trust. The texts were structured into thematic units that would cover the basic concepts of cybersecurity, present the innovative solutions of the INNOSOC project and showed their practical use in real scenarios. Where appropriate, the texts were supplemented with visual elements such as infographics or illustrations, which made it easier to understand complex technical processes.

An important aspect of the popularisation texts was also their topicality and relevance to current trends in cybersecurity. This approach ensured that the content remained relevant, attractive and useful to readers in the long term, while the project website became a source of information in the field of cybersecurity in Slovakia. Topics selected for the first popularisation texts on the INNOSOC website:

- Cybersecurity: Basics and tips on how to protect yourself against online threats;
- Security Operation Center: what is it and how does it protect your company?;
- Get to know the most common internet threats for young people: Options for prevention and protection;
- What is the cloud and what is it 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 ever-greater risk.

1.3.1 Implemented Activities

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

1.3.1.1 Popularisation article on the topic Cybersecurity: Basics and tips on how to protect yourself against online threats

On 3 September 2025, a popularisation 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 a comprehensible and accessible way, to point out current cyber threats and to emphasise the importance of prevention in the digital environment. The content of the article includes:

- an explanation of the term cybersecurity and its importance for individuals and organisations,
- a description of the most common types of cyber attacks and threats (e.g. phishing, malware, social engineering, DDoS attacks),

- the 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,
- an 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.

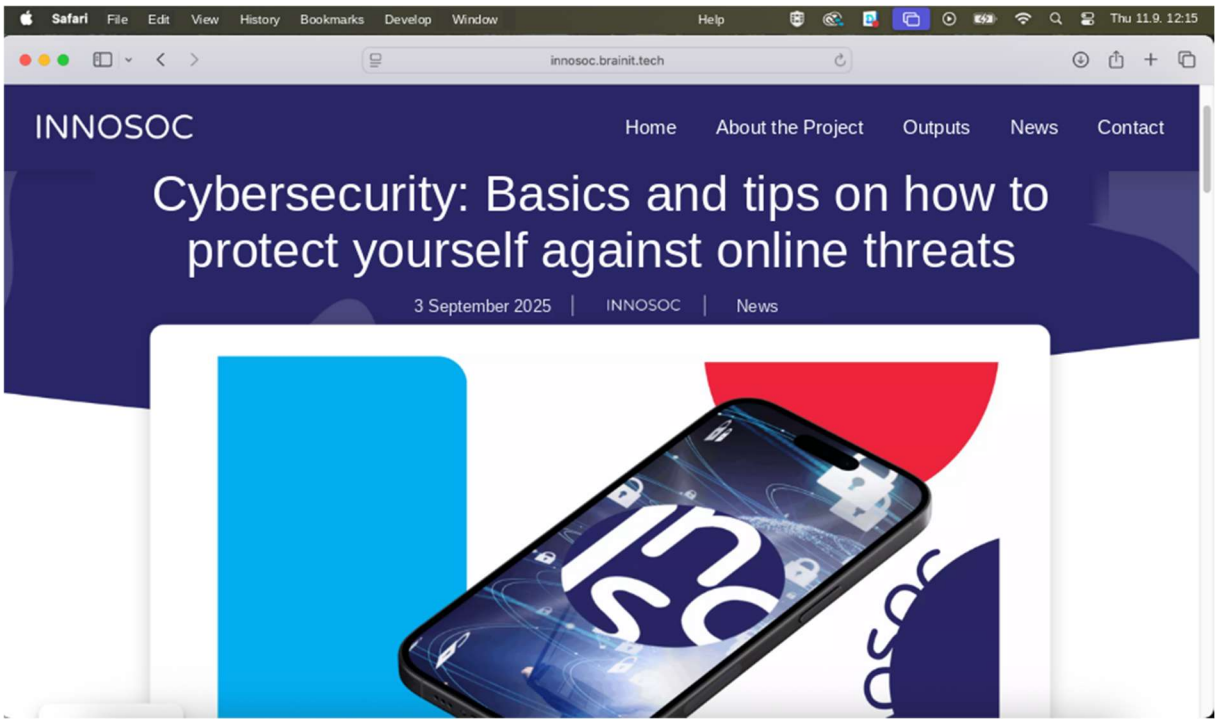


Figure 42 Popularisation article on the topic of cybersecurity, Source: (BRAIN:IT, 2025)

To reach a wider audience, the same popularisation text was published on the LinkedIn page @INNOSOC with the aim of reaching experts and university students. This article was published on 8.9.2025.

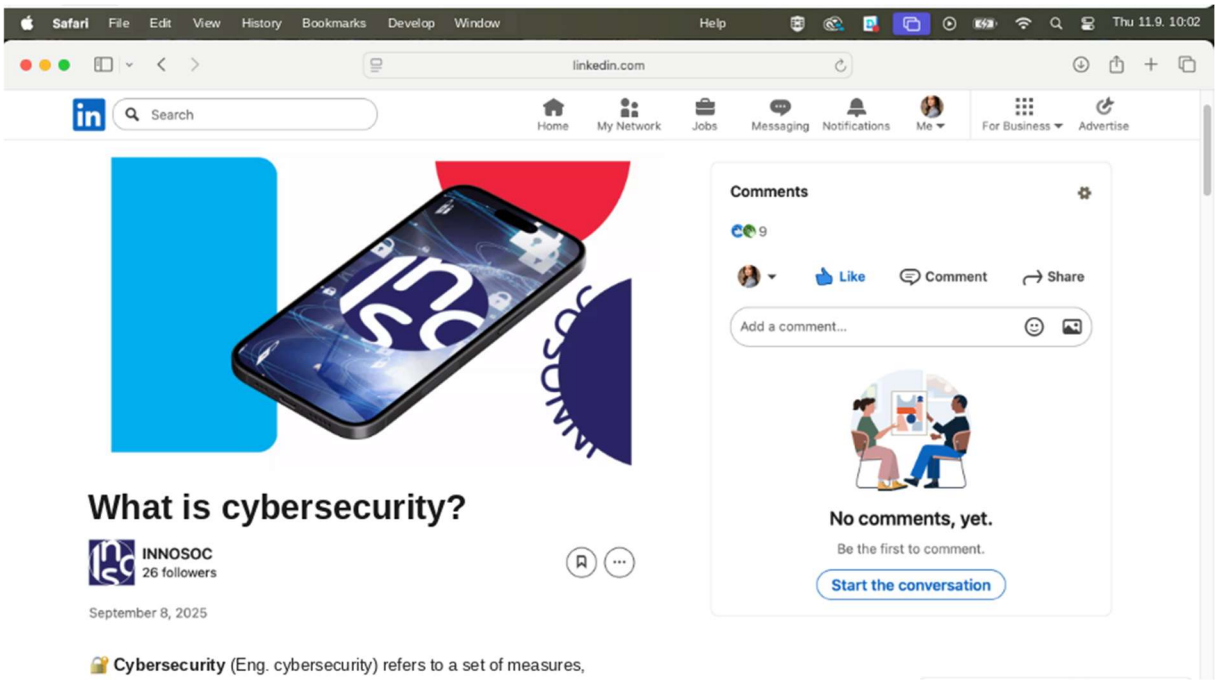


Figure 43 Popularisation article on the topic of cybersecurity on the LinkedIn page @INNOSOC, Source: (BRAIN:IT, 2025)

1.3.1.2 Popularisation article on the topic Security Operations Center: what is it and how does it protect your company?

On 10 September 2025, an educational article on the topic “Security Operations Center: what is it and how does it protect 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 the modern approach to cybersecurity and to explain its importance in protecting organisations’ digital assets in an environment of growing cyber threats. The content of the article focuses mainly on:

- an explanation of the role of the SOC as a centralised, round-the-clock security centre,
- a definition of the main mission of the SOC, which is to minimise the impact of cyber incidents and to protect the organisation proactively,
- a description of how the SOC works, including the work of security analysts and the use of advanced security technologies,
- a presentation of 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,
- an emphasis on the importance of processes, documentation and internal security policies as part of the effective functioning of the SOC.

The article serves as a professional and awareness-raising output of the project, the aim of which is to raise awareness of the practical functioning of the Security

Operations Center, promote a systematic approach to cybersecurity in organisations and 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 is it and how does it protect your company?

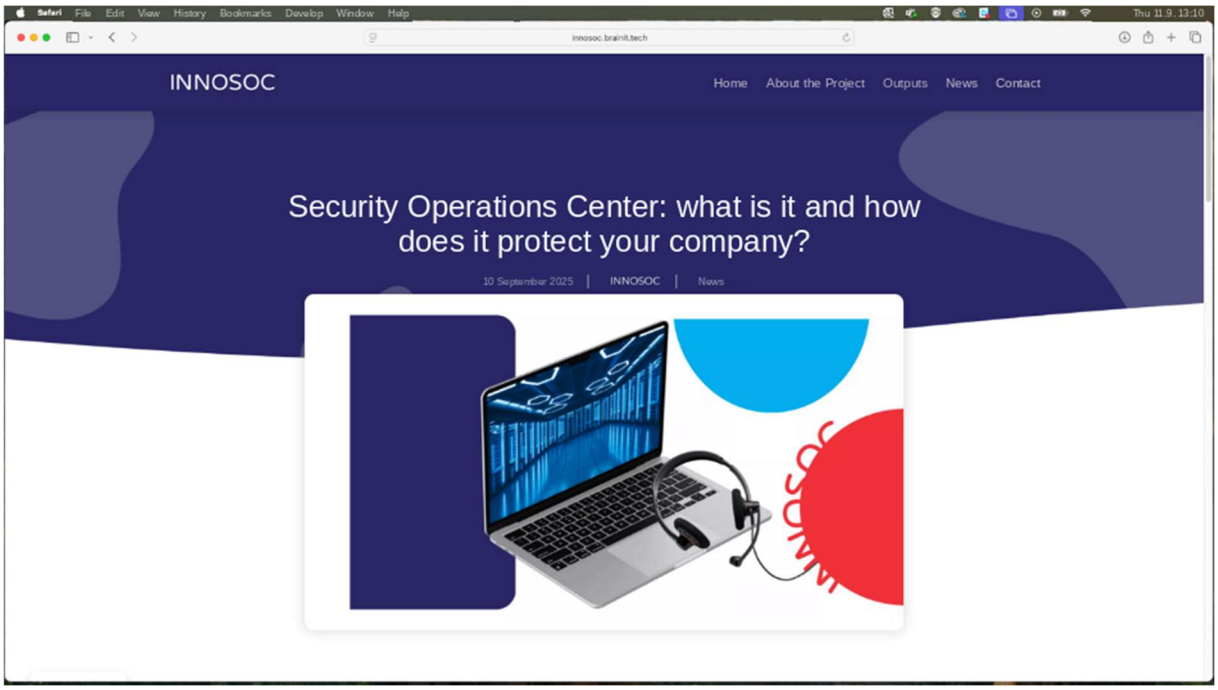


Figure 44 Popularisation article on the topic of the Security Operations Center, Source: (BRAIN:IT, 2025)

1.3.1.3 Popularisation article on the topic Get to know the most common internet threats for young people: Options for prevention and protection

As part of the project, an educational and awareness-raising article focusing on the risks of the digital and online environment for the young generation was published on 22 September in the "News" section of the website. The aim of the article was to raise awareness of the safety of young people 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 mainly on:

- a characterisation of the current generation growing up in the information and technological age,
- the 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,

- the 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, particularly when sharing personal data and photographs and when communicating with strangers,
- an emphasis on the role of the family and the home environment as a key element in the prevention of digital risks.

The article is 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, to strengthen the awareness of parents and teachers and to 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: Options for prevention and protection.

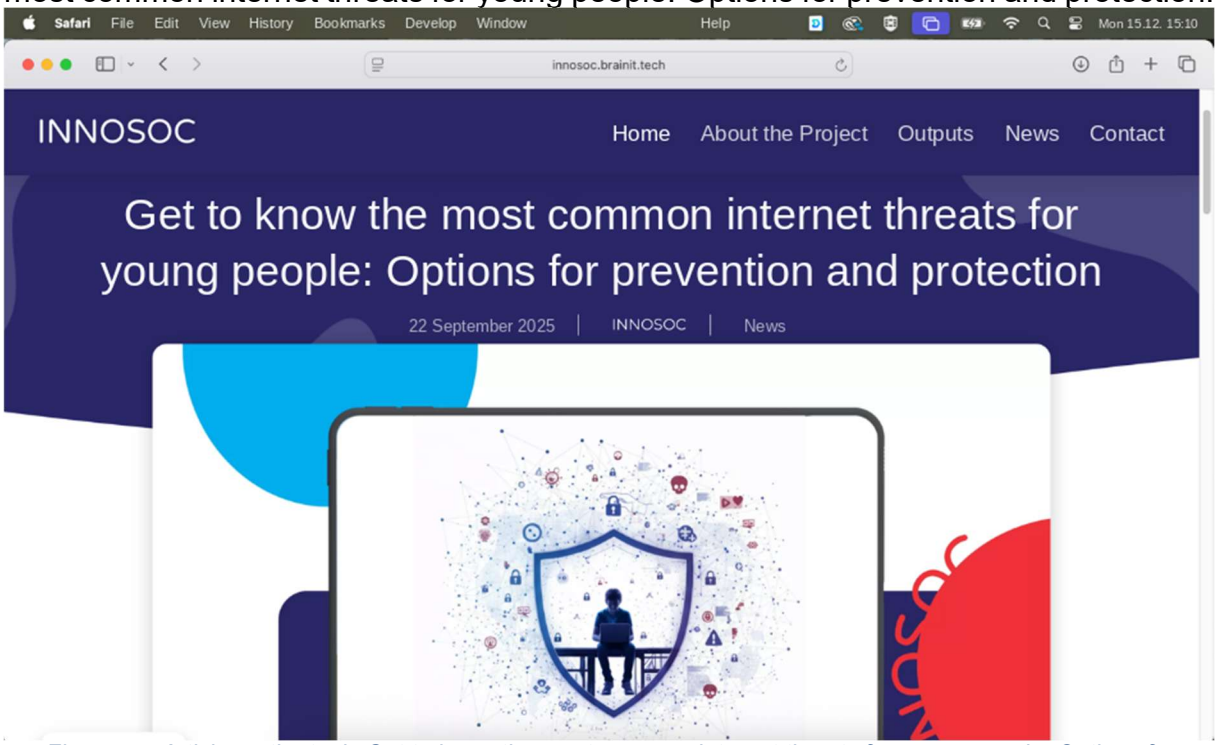


Figure 45: Article on the topic Get to know the most common internet threats for young people: Options for prevention and protection, Source: (BRAIN:IT, 2025)

1.3.1.4 Popularisation article on the topic What is the cloud and what is it used for: Basic types and advantages of cloud storage

As part of the project, a professional educational article focusing 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 a comprehensible way the concept of the cloud and its practical use in everyday and corporate settings, and to point out the basic advantages and risks associated with the use of cloud solutions. The content of the article focuses mainly 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,
- a presentation of 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 is 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 is the cloud and what is it used for: Basic types and advantages of cloud storage.

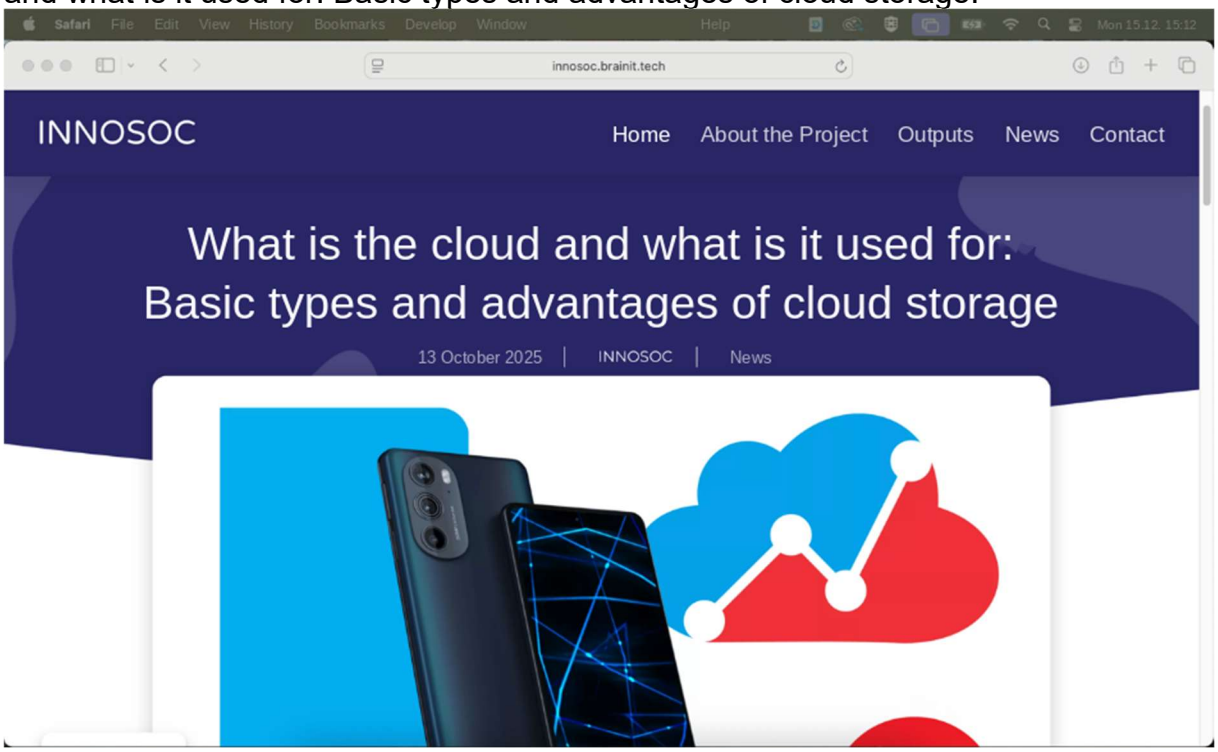


Figure 46: Article on the topic What is the cloud and what is it used for: Basic types and advantages of cloud storage, Source: (BRAIN:IT, 2025)

1.3.1.5 *Popularisation article on the topic Computer security and data protection – principles and practical examples*

On 10 November 2025, a professional educational article focusing 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 organisations and in everyday digital life. The content of the article focuses mainly on:

- an explanation of the importance of computer security and cybersecurity when working with digital data,
- a definition of the three basic principles of the security triad – confidentiality, integrity and availability,
- linking data protection principles with 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 organisational data protection tools, such as encryption, access management, multi-factor authentication, electronic signatures, backup and availability monitoring,
- an emphasis on the need for balance between the individual elements of the security triad when designing security policies.

The article is a professional and educational output of the project, the aim of which is to raise awareness of the protection of data and information, promote responsible behaviour of users in the digital environment and provide a practical basis for building effective security measures in organisations 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.

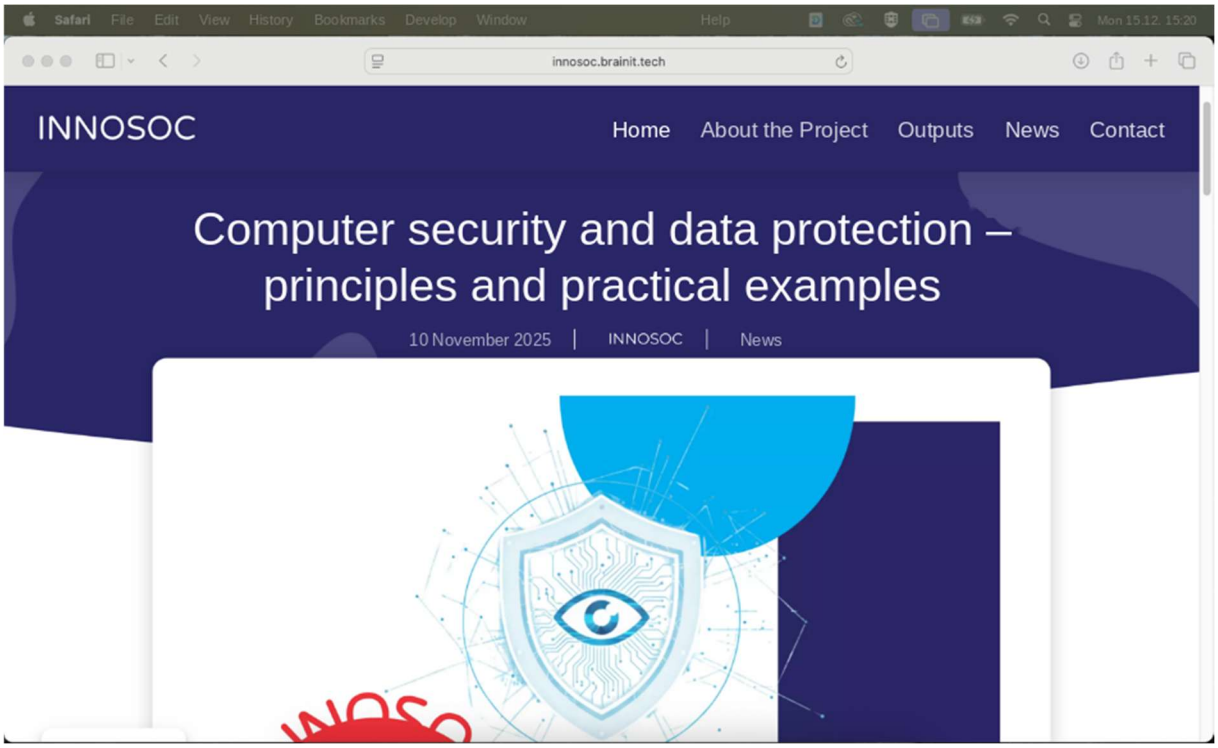


Figure 47: Article on the INNOSOC website on the topic Computer security and data protection – principles and practical examples, Source: (BRAIN:IT, 2025)

1.3.1.6 Popularisation article on the topic Linking AI and cybersecurity in practice

On 16 December 2025, a popularisation article focusing on the use of artificial intelligence in the field of cybersecurity was published in the "News" section of the INNOSOC project website. The article outlines current trends in cyber threats and highlights the growing importance of modern technological tools in protecting information systems.

The content of the article explains the possibilities of using artificial intelligence in the detection, prevention and resolution of cyber incidents. Particular emphasis is placed on the ability of AI to analyse large volumes of data in real time, identify anomalies in the behaviour of users and systems, predict potential attacks and automate responses to security incidents. At the same time, the article also draws attention to the limits of artificial intelligence and points out that AI should not function as a stand-alone solution, but as a tool supporting the work of security analysts.

The article also includes an analysis of the risks associated with the misuse of artificial intelligence by attackers, for example in automated attacks, the generation of phishing campaigns, the creation of malicious code or the use of deepfake technologies for social engineering. The article therefore emphasises the need for a balanced approach that combines artificial intelligence technology tools with expert human oversight.

The publication of the article on the project website contributes to the popularisation of cybersecurity topics, to the dissemination of knowledge about the possibilities of using artificial intelligence in this field and to raising awareness among both the professional community and the wider public of current security challenges. The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements” (project code 09I05-03-V02-00010), funded by the European Union – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic.

The full text of the article can be found in Annex 21 – Popularisation article on the topic Linking AI and cybersecurity in practice.



Figure 48:Popularisation article on the topic Linking AI and cybersecurity in practice, Source: (BRAIN:IT, 2025)

1.3.1.7 Popularisation article on the topic Cyber attacks: How they are changing and why they pose an ever-greater risk

On 19 December 2025, a popularisation article focusing on the increasing sophistication of cyber attacks and their impact on individuals, companies and public institutions was published in the “News” section of the INNOSOC project website. The article explains that today’s cyber threats are no longer the work of isolated individuals, but are often carried out by organised groups using advanced technologies, automation tools and elements of artificial intelligence.

The content of the article outlines the main factors contributing to the increasing complexity of cyber attacks, such as organised cooperation between attackers, the use of advanced techniques including social engineering, the growing digitalisation of

society and the widespread use of artificial intelligence in the preparation and execution of attacks. The article also points out the practical consequences of cyber incidents, in particular the misuse of sensitive data, financial losses, the erosion of trust and increased costs of securing information systems.

The article also explains the importance of a systematic approach to data protection and cybersecurity. It emphasises the need for a combination of technical security solutions, continuous monitoring of systems and a responsible approach by users to the management and protection of data.

The publication of the article on the project website contributes to the popularisation of cybersecurity topics, to the dissemination of information about current security threats and to raising public awareness of the need for systematic protection of digital data. The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements” (project code 09I05-03-V02-00010), funded by the European Union – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic.

The full text of the article can be found in Annex 22 – Popularisation article on the topic Linking AI and cybersecurity in practice.

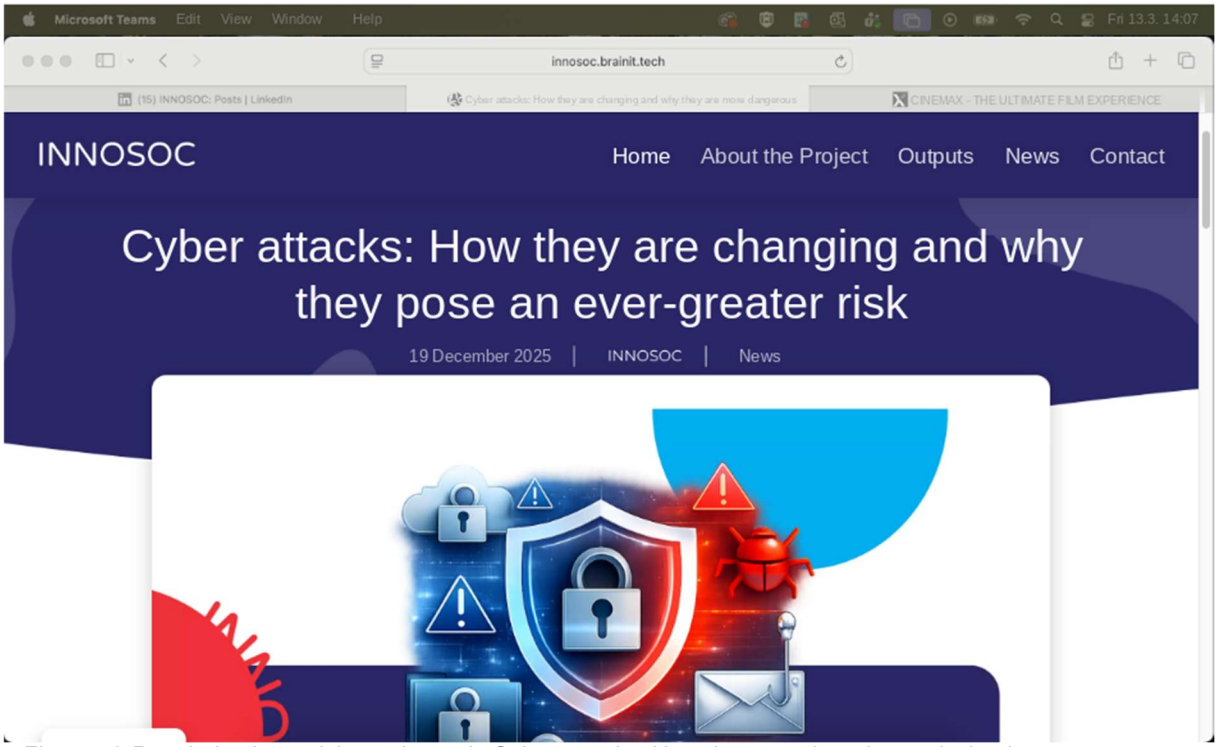


Figure 49:Popularisation article on the topic Cyber attacks: How they are changing and why they pose an ever-greater risk, Source: (BRAIN:IT, 2025)

1.3.1.8 Popularisation article on the topic Automation and deep machine learning in cybersecurity

In the **"**News**"** section of the INNOSOC project website, a popularisation article focusing on the use of automation and machine learning technologies in the field of cybersecurity was published on 21 January 2026. The article explains why automating responses to security incidents is essential in an environment where the volume of security events and data is constantly growing and processing them manually is increasingly demanding.

The content of the article outlines the principles of how machine learning and deep machine learning (deep learning) work in the detection of cyber threats. It explains how these technologies can analyse large amounts of security data, identify anomalies in the behaviour of systems, users and devices, and contribute to the early detection of cyber attacks. The article also explains the practical use of automated security tools, for example in network behaviour analysis, the prediction of security incidents or automated threat response through SOAR-type solutions.

At the same time, the article also draws attention to the limits of automation and the use of artificial intelligence in cybersecurity, in particular the risk of false alarms and the dependence of models on the quality of training data. It therefore emphasises the need for technological tools to work together with the human factor, with security analysts playing a key role in interpreting results, investigating incidents and setting security strategies.

The publication of the article on the project website contributes to the popularisation of cybersecurity topics and to the dissemination of knowledge about modern technological approaches to protecting information systems. The article is an output of the project "Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements" (project code 09I05-03-V02-00010), funded by the European Union – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic.

The full text of the article can be found in Annex 23 – Popularisation article on the topic Automation and deep machine learning in cybersecurity



Figure 50: Popularisation article on the topic Automation and deep machine learning in cybersecurity, Source: (BRAIN:IT, 2026)

1.4 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 task was to present the complex technical processes and benefits of the SOC solution in a dynamic and engaging way through combined audiovisual content intended to appeal to a wide range of target groups. They were shared mainly on social media and on the project website.

The videos were adapted to the specific features of the individual platforms and target segments: shorter formats with a strong visual element were created for social media, while more detailed and technically oriented videos were prepared for the website and professional presentations. The content included explanations of how SOC systems work, interviews with experts and statements from project partners.

The promotional videos served as a key tool for educating students and increasing the digital literacy of the general public, explaining the basic concepts of cybersecurity.

Video production involved the use of modern and professional production tools for visualisation and post-production, which made it possible to present the abstract concepts of cybersecurity effectively. The videos contained professionally recorded

voice-overs, high-quality graphic elements and music that will underline the innovative character of the project.

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

1.4.1 Implemented Activities

This chapter contains a description of the individual audiovisual outputs that were published on the official INNOSOC website, the INNOSOC YouTube channel and on social media.

1.4.1.1 Creation of an account on YouTube

For the publication of videos – in particular expert interviews and various activities in the form of events – a YouTube channel named @INNOSOC was created. It will serve as a supporting tool and will be used to share the aforementioned videos in other channels, such as the website. The channel was also created so that all video content can be archived and made easily accessible to both the professional community and the lay public.

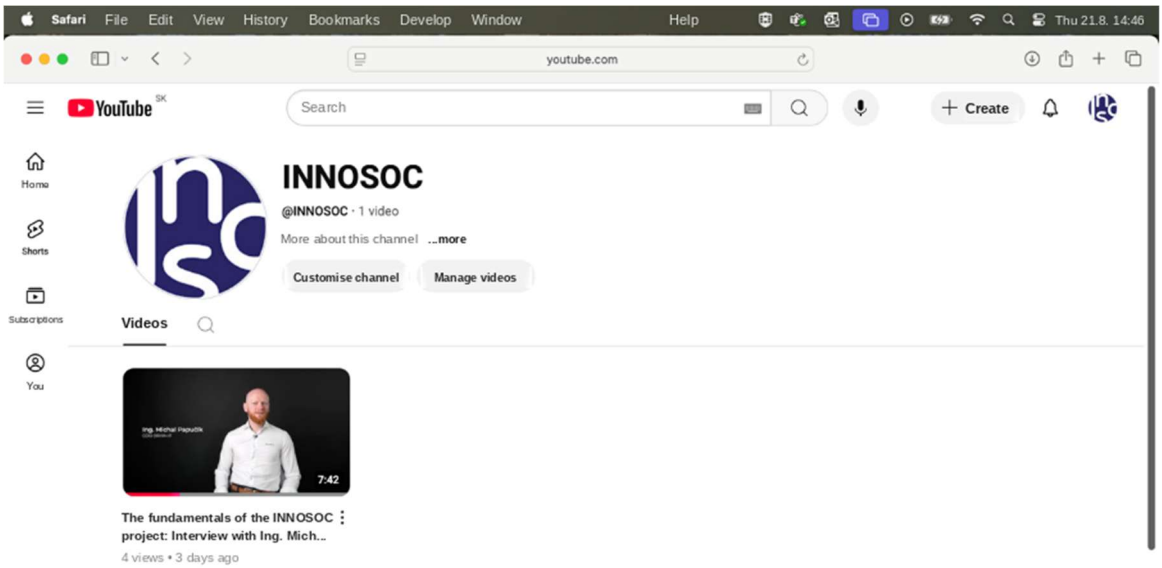


Figure 51: YouTube channel @INNOSOC, Source: (BRAIN:IT, 2025)

1.4.1.2 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 provides information on the aim of the project, the need for it, the challenges it 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, while also offering 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.

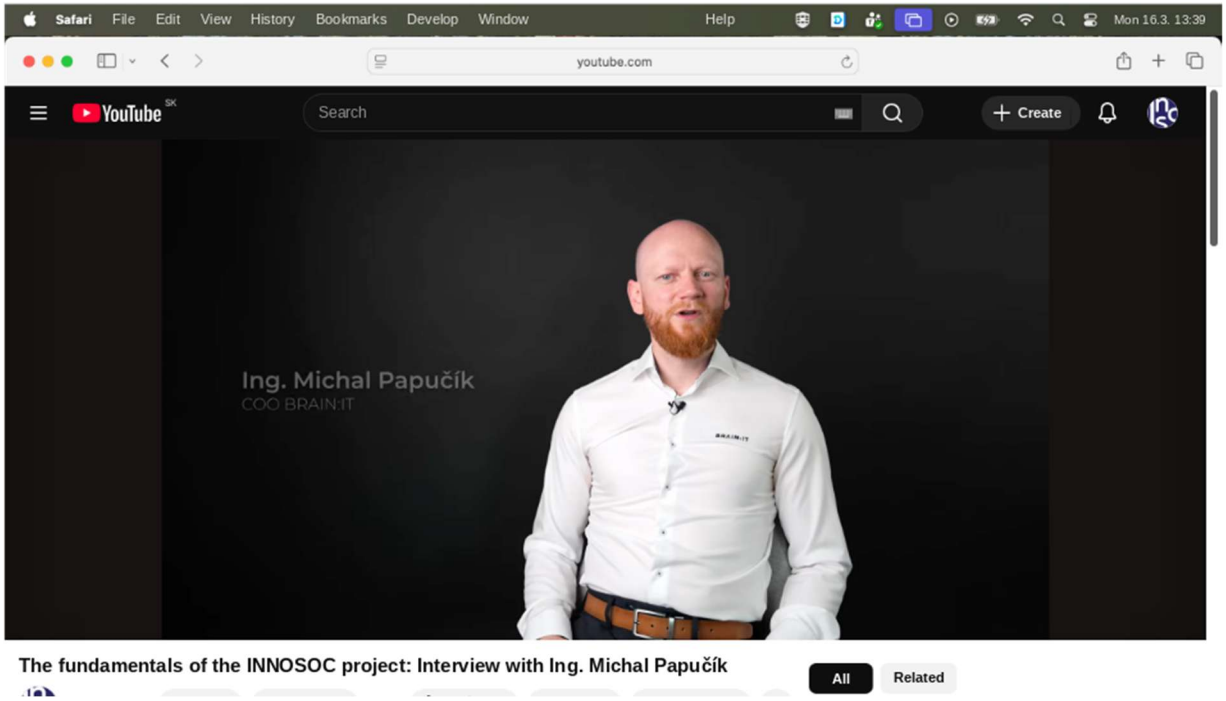


Figure 52: Video interview with Ing. Michal Papučík, Source: (BRAIN:IT, 2025)

1.4.1.3 Video interview with prof. Ing. Pavel Segeč, PhD.

The aim of the interview was to outline 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 centralised protection for organisations and educational institutions. The content of the interview focuses mainly on:

- the importance of cybersecurity for organisations of all sizes in the context of growing digitalisation,
- 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,
- the identification of the most common cyber threats, such as phishing, ransomware and advanced persistent threats (APT),
- an explanation of the concept of a Security Operations Center (SOC) as a central element of protection, built on the pillars of people, processes and technologies,
- the impact of the new NIS2 Directive on requirements in the area of cyber incident management and reporting,

- the practical functioning 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, linking the scientific research perspective with the practical implications for the security of organisations. It also 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.

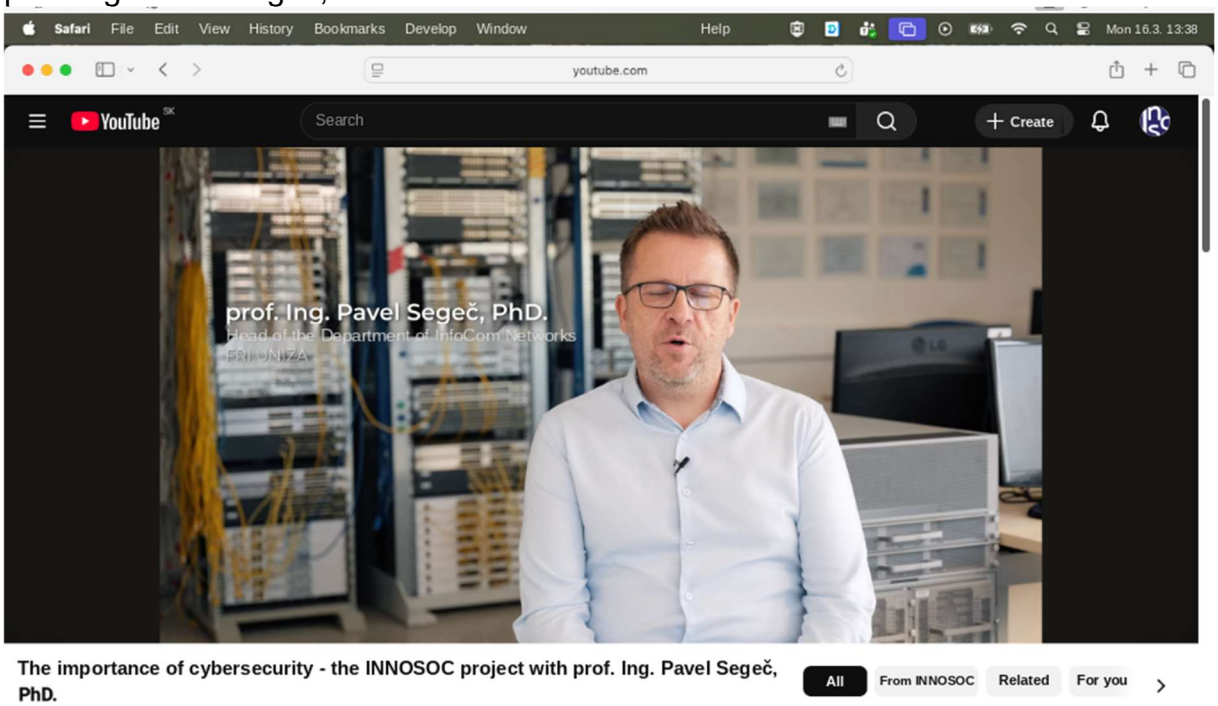


Figure 53: Video interview with prof. Ing. Pavel Segeč, PhD., Source: (BRAIN:IT, 2025)

1.4.1.4 Video interview with Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD.

On 22 January 2026, a video entitled “About the INNOSOC project with Dominika Toman and Martin Mičiak” was added to the INNOSOC YouTube channel. In the form of an interview, the video outlines the details of the research project, its objectives, practical benefits and the challenges associated with managing it. The following key topics were discussed:

- Focus and aim of the project: The INNOSOC project links research, practice and innovation in the field of cybersecurity and Security Operation Centers (SOC). Its main aim is to design a technological solution for organisations (especially public administration and businesses) that cannot afford expensive commercial solutions. This solution is built on the integration of suitable open-source components.

- Cooperation and team: The project represents a unique link between the academic environment (the Faculty of Management Science and Informatics of the University of Žilina) and a business partner (BRAIN:IT). The guests, Dominika Toman and Martin Mičiak from the Department of Management Theories, explained that their role in the project is primarily coordination, management and project management, while the technical side is covered by the Department of InfoCom Networks.

Practical benefits and outputs:

- For businesses: Companies will receive a ready-made design and an overview of components that they can use to strengthen their security without having to build a solution from scratch.
- For students: The project creates opportunities for final theses and practical teaching, where students can try out real situations from project management and IT practice.
- Scientific activity: The project includes publication activity in indexed journals and participation in conferences, which requires demanding planning due to lengthy review processes.
- Risk management and challenges: In terms of management, the team had to deal with risks in communication between several partners and with aligning schedules (for example, university holidays versus project deadlines). Ongoing monitoring and reporting for grant agencies were also demanding.
- Key result: The guests consider the most significant output to be the proof of concept – real-world testing of the proposed architecture, which confirms that the solution is applicable in practice and sustainable for end clients.

From a project management perspective, the video particularly highlights the flexibility and initiative of the team members, who were able to respond successfully to administrative requirements and time pressure.

The full transcript of the interview can be found in Annex 24 – Interview with Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD.

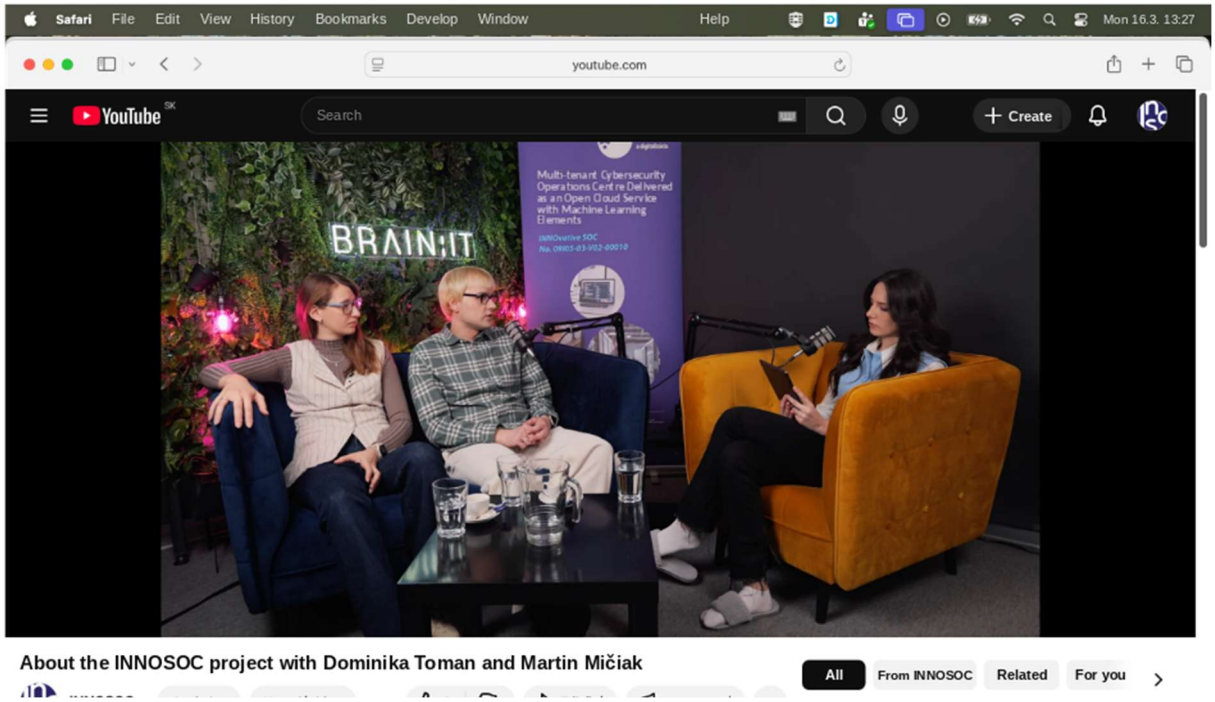


Figure 54: About the INNOSOC project with Dominika Toman and Martin Mičiak, Source: (BRAIN:IT, 2026)

1.4.1.5 Video interview with Ing. Martin Mičiak, PhD.

On 6 February 2026 a video entitled “Interview with Ing. Martin Mičiak, PhD. about the INNOSOC project” was published on the INNOSOC YouTube channel. In it, Martin Mičiak describes his dual role in the project – as a researcher and also as part of project management support. The main points and topics of the interview include:

- Focus of the project: The topic of the INNOSOC project is cybersecurity, with an emphasis on finding ways to strengthen it in organisations through open-source solutions, which leads to a reduction in overall costs.
- Scientific and publication activity: Martin Mičiak stresses that, for the relevance of the project and to spread awareness of it, it is crucial to publish outputs with renowned publishers and in indexed journals or at conferences.
- Research process: He described the research itself and the identification of the so-called research gap as the most demanding part. Each output must bring something new and examine the issue in detail in order to be of interest to both the professional community and practice.
- Interdisciplinary cooperation: The project is built on cooperation between the academic and business environments. Within the faculty, it involves cooperation between the Department of Management Theories and the Department of InfoCom Networks, which enables an effective link between management and informatics.
- Personal benefit for the researcher: Participation in the project enabled Martin Mičiak to deepen his knowledge of cybersecurity and to gain further practical experience in the field of project management support.

This interview underlines the academic dimension of the project and the importance of expert research that precedes the actual implementation of technical solutions in practice.

The full transcript of the interview can be found in Annex 25 – Interview with Ing. Martin Mičiak, PhD.

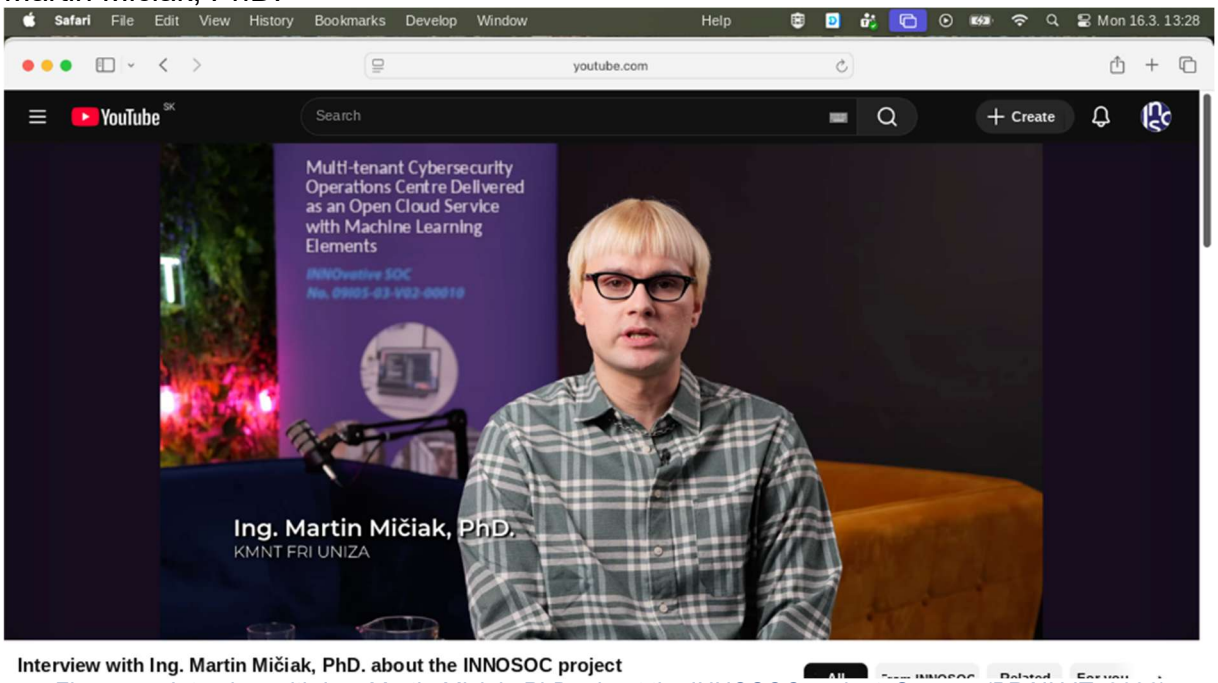


Figure 55: Interview with Ing. Martin Mičiak, PhD. about the INNOSOC project, Source: (BRAIN:IT, 2026)

1.4.1.6 Video interview with Ing. Dominika Toman, PhD.

On 6 February 2026, a video entitled “Interview with Ing. Dominika Toman, PhD. about the INNOSOC project” was published on the INNOSOC YouTube channel. In it, Dominika Toman describes her role and key activities within the project. The main points and topics of the interview include:

- Role in the project: Dominika Toman is primarily responsible for project management support and the coordination of the people involved in the research team.
- Importance of the project for practice and the public: She sees the project as a means of broadening horizons in cybersecurity and providing information on how to help effectively in this field. From the point of view of professional practice, deepening knowledge through research is key.
- Professional outputs and publications: Within the project, a number of articles and conference papers were published, focusing on:
- Reviews of solutions: Identifying the most suitable technological solutions to support cybersecurity.

- Education: Proposals for suitable training for employees of organisations so that they are able to operate the new solutions properly and use them to improve their security.
- Communication with partners: An important part of her work was intensive communication and cooperation with partners directly from the university environment as well as from real-world practice.
- Personal and professional development: Participation in the project enabled the researcher to acquire new information and improve her skills in managing and coordinating outputs.

This interview emphasises that the INNOSOC project is not only about technology, but also about the importance of management support and end-user education, without which the implementation of cybersecurity would not be effective.

The full transcript of the interview can be found in Annex 26 – Interview with Ing. Dominika Toman, PhD.

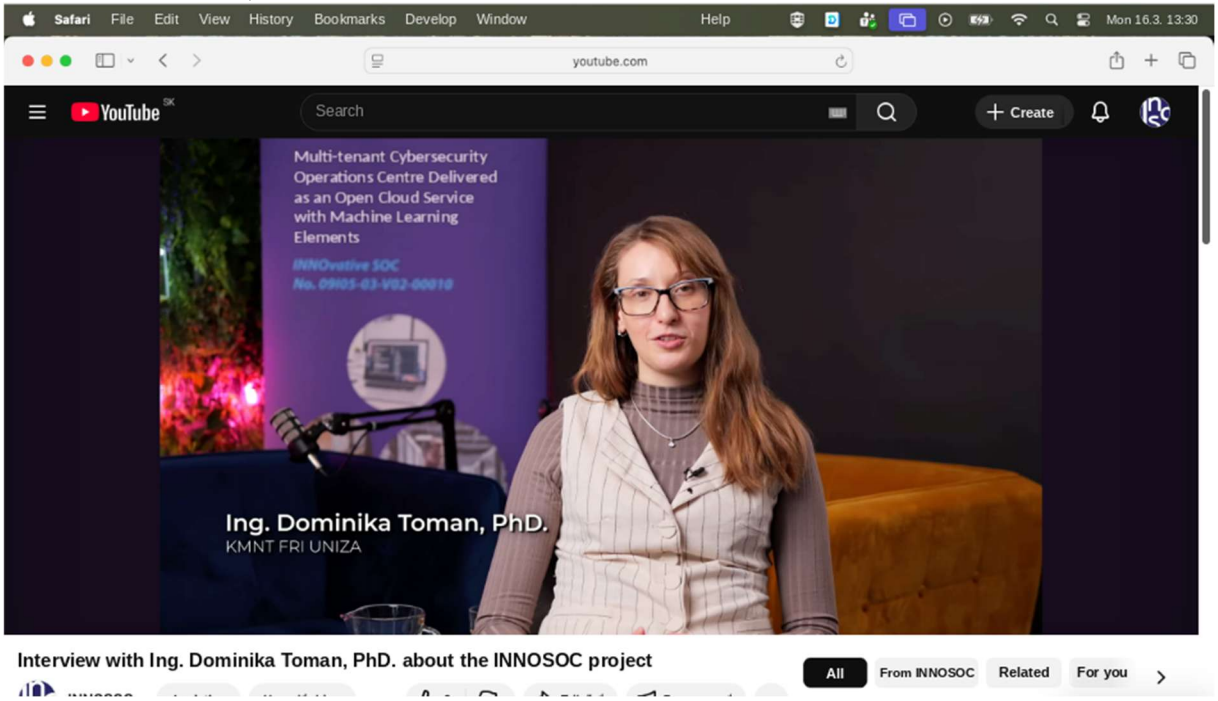


Figure 56:Interview with Ing. Dominika Toman, PhD. about the INNOSOC project, Source: (BRAIN:IT, 2026)

1.4.1.7 Video interview with prof. Ing. Milan Kubina, PhD.

For the purposes of the project documentation, we provide a summary of information from the interview with prof. Ing. Milan Kubina, PhD., Head of the Department of Management Theories at the Faculty of Management Science and Informatics of UNIZA.

On 20 February 2026, a video entitled “Interview about the INNOSOC project with prof. Ing. Milan Kubina, PhD.” was published on the INNOSOC YouTube channel. The interview outlines the strategic direction of the project and its societal significance. The key areas discussed in the interview include:

- Role and responsibility in the project: Prof. Kubina acts as one of the two key principal investigators (together with prof. Segeč). His main task is to ensure communication between the individual research teams, the partners (in particular BRAIN:IT) and the scientific grant agency.
- Societal benefit and target group: The INNOSOC project responds to the risks of the digital age, in which attackers exploit system flaws in applications. The solution is primarily intended for entities that do not have sufficient funds for expensive commercial systems – mainly small companies, public administration, municipalities and schools. The aim is for these organisations, too, to feel safer in cyberspace.
- Technical direction and innovation: The project focuses on the issue of the SOC (Security Operation Center) and the operational security of IP networks. The output is to be a solution design at TRL3 level, conceived as a cloud-based, multi-tenant service with an emphasis on low financial cost for future customers.
- Linking the university with practice: Prof. Kubina stresses the necessity of synergy between academia and real business. He supports this cooperation not only through research, but also by motivating students to tackle practical topics in their bachelor’s and master’s theses and by inviting lectures from practitioners directly at the faculty.

This interview completes the picture of the project with the perspective of the research team’s senior management and underlines the ambition to create an affordable technological solution for protecting the critical infrastructure of smaller organisations.

The full transcript of the interview can be found in Annex 27 – Interview with prof. Ing. Milan Kubina, PhD.

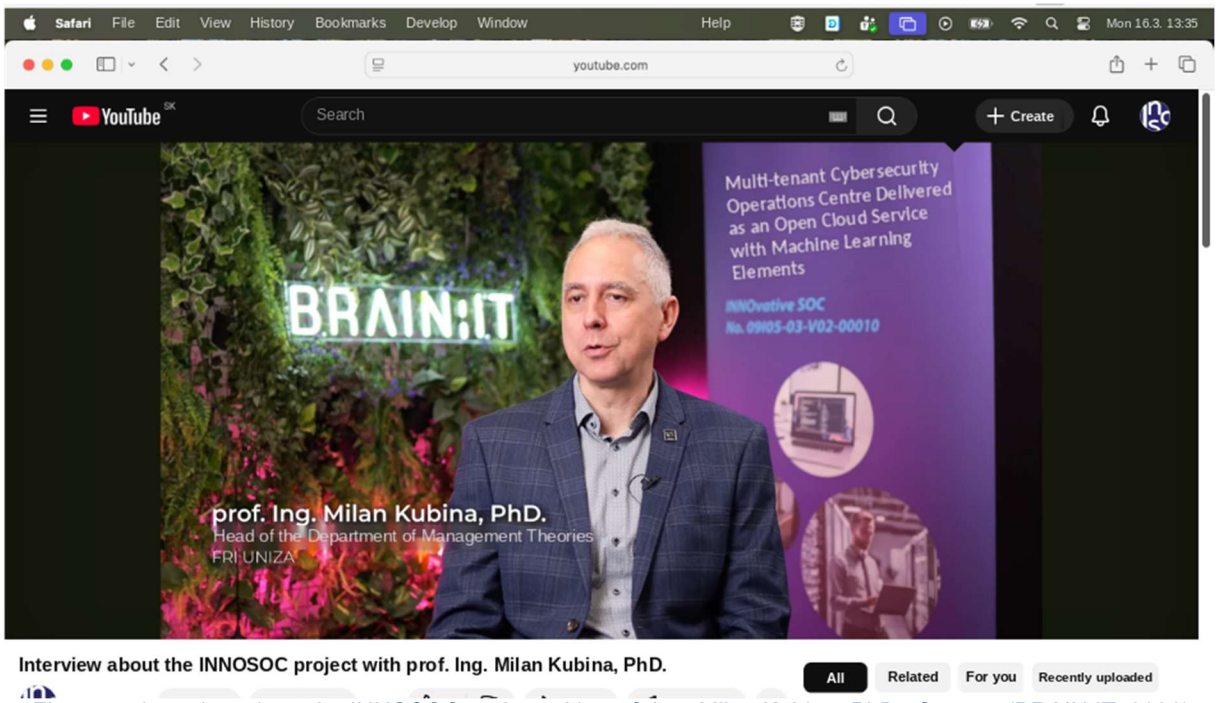


Figure 57:Interview about the INNOSOC project with prof. Ing. Milan Kubina, PhD., Source: (BRAIN:IT, 2026)

List of Sources

BRAIN:IT. (16 October 2025). *innosoc.com*. Available online: 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 online: INNOSOS: https://innosoc.brainit.tech
BRAIN:IT. (11 November 2025). *innosoc.brainit.tech*. Available online: Student event FRIčkovica: https://innosoc.brainit.tech/studentska-udalost-frickovica/
BRAIN:IT. (17 November 2025). *innosoc.brainit.tech*. Available online: 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 online: iPad competition: https://innosoc.brainit.tech/sutaz-o-ipad-vyhlasenie-vitaza/
BRAIN:IT. (28 November 2025). *innosoc.brainit.tech*. Available online: 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 online: 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 online: 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 online: What is the cloud and what is it 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 online: Computer security and data protection – principles and practical examples: https://innosoc.brainit.tech/pocitacova-bezpecnost-a-ochrana-dat/
BRAIN:IT. (2025). *innosoc.brainit.tech*. Available online: Article: Interview with experts: How the INNOSOC project connects science, practice and cybersecurity: https://innosoc.brainit.tech/rozhovor-s-odbornikmi-ako-projekt-innosoc-spaja-vedu-prax-a-kyberneticku-bezpecnost/
BRAIN:IT. (2025). *innosoc.brainit.tech*. Available online: Popularisation article on the topic Linking AI and cybersecurity in practice: https://innosoc.brainit.tech/ai-a-kyberneticka-bezpecnost/
BRAIN:IT. (2025). *innosoc.brainit.tech*. Available online: Popularisation article on the topic Cyber attacks: How they are changing and why they pose an ever-greater risk: https://innosoc.brainit.tech/kyberneticke-utoky-ako-sa-menia/
BRAIN:IT. (2025). *Instagram @brainit.tech*. Available online: post website: https://www.instagram.com/p/DLXH_-MuL6_/
BRAIN:IT. (16 September 2025). *Instagram @innosoc_*. Available online: cybersecurity quiz: https://www.instagram.com/p/DOxr6HqiFeJ/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2025). *Instagram @innosoc_*. Available online: 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 online: 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 online: post partners' meeting 15.7.2025: https://www.instagram.com/p/DMpmaMAoMCj/?img_index=1
BRAIN:IT. (2025). *Instagram INNOSOC*. Available online: https://www.instagram.com/innosoc_/

BRAIN:IT. (3 October 2025). *Instagram account @innosoc_*. Available online: 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 online: 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 online: 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 online: 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 online: 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 online: 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 online: 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 online: 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 online: 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 online: post partners' meeting 15.7.2025: https://www.linkedin.com/company/108018118/admin/page-posts/published/
BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Available online: post published on 21.8.2025: https://www.linkedin.com/feed/update/urn:li:activity:7364224462050795520
BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Available online: post published on 5.9.2025: https://www.linkedin.com/feed/update/urn:li:activity:7369610244873674752
BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Available online: Popularisation text on the topic of cybersecurity: https://www.linkedin.com/pulse/čo-je-kybernetická-bezpečnosť-innosocinnosoc-dt6we/?trackingId=cIrSBt0YN2qcFTrPUNfmvw%3D%3D
BRAIN:IT. (2025). *LinkedIn INNOSOC*. Available online: https://www.linkedin.com/company/innosocinnosoc/posts/?feedView=all
BRAIN:IT. (17 October 2025). *LinkedIn profile @innosoc*. Available online: 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 online: announcement of the symposium: https://www.linkedin.com/feed/update/urn:li:activity:7396442124268961792
BRAIN:IT. (24 November 2025). *LinkedIn profile @innosoc*. Available online: competition prize-giving: https://www.linkedin.com/feed/update/urn:li:activity:7398667812409397248

BRAIN:IT. (9 December 2025). *LinkedIn profile @innosoc*. Available online: 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 online: 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 online: Get to know the most common internet threats for young people: Options for prevention and protection: https://innosoc.brainit.tech/najcastejsie-digitalne-hrozby-pre-mladych/
BRAIN:IT. (2025). *INNOSOC website*. Available online: popularisation article on the topic of cybersecurity: Cybersecurity: Basics and tips on how to protect yourself against online threats
BRAIN:IT. (2025). *INNOSOC website*. Available online: Popularisation article: https://innosoc.brainit.tech/co-je-soc-security-operations-center/
BRAIN:IT. (2025). *YouTube @INNOSOC*. Available online: https://www.youtube.com/@INNOSOC
BRAIN:IT. (2025). *YouTube @INNOSOC*. Available online: video interview with Ing. Michal Papučík: https://youtu.be/w9W4_oNYiEQ?si=YlCKWgzX-JVkFZQK
BRAIN:IT. (15 October 2025). *YouTube @INNOSOC*. Available online: interview with prof. Ing. Pavel Segeč, PhD.: https://www.youtube.com/watch?v=aKxL-Aig6sg
BRAIN:IT. (2026). *innosoc.brainit.tech*. Available online: Article about the interview on the INNOSOC project: Cybersecurity and broadening horizons with Dominika Toman: https://innosoc.brainit.tech/rozhovor-o-projekte-innosoc-kyberneticka-bezpecnost-a-rozsirovanie-obzorov-s-dominikou-toman/
BRAIN:IT. (2026). *innosoc.brainit.tech*. Available online: Article about the interview on the INNOSOC project: On scientific research and cybersecurity with Martin Mičiak.: https://innosoc.brainit.tech/rozhovor-o-projekte-innosoc-o-vedeckom-vyskume-a-kybernetickej-bezpecnosti-s-martinom-miciakom/
BRAIN:IT. (2026). *innosoc.brainit.tech*. Available online: article about the interview with prof. Ing. Milan Kubina, PhD. on the INNOSOC project: https://innosoc.brainit.tech/rozhovor-s-prof-ing-milanom-kubinom-phd-o-projekte-innosoc/
BRAIN:IT. (2026). *innosoc.brainit.tech*. Available online: Popularisation article on the topic Automation and deep machine learning in cybersecurity: https://innosoc.brainit.tech/automatizacia-v-kybernetickej-bezpecnosti/
BRAIN:IT. (2026). *Instagram profile @innosoc*. Available online: Post about the interview with Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD. on the Instagram profile @innosoc_: https://www.instagram.com/reel/DUnIqRnCN9A/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2026). *Instagram profile @innosoc_*. Available online: Post about the interview with prof. Ing. Milan Kubina, PhD. on the Instagram profile @innosoc_: https://www.instagram.com/reel/DVLEcgECOz5/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2026). *Instagram profile @innosoc_*. Available online: post about the interview with Ing. Dominika Toman, PhD. on the Instagram profile @innosoc_: https://www.instagram.com/reel/DUp1pl0CJvB/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2026). *LinkedIn profile @innosoc*. Available online: post about the interview with prof. Ing. Milan Kubina, PhD.: https://www.linkedin.com/posts/innosocinnosoc_v-r%C3%A1mci-odborn%C3%A9ho-rozhovoru-n%C3%A1m-prof-activity-7432331789060411393-THws?utm_source=share&utm_medium=member_desktop&rcm=ACoAADYrbuwBoKkFoArpjtWiekEoiD3FrkyXPyA
BRAIN:IT. (2026). *YouTube INNOSOC*. Available online: Interview with Ing. Martin Mičiak, PhD. about the INNOSOC project: https://www.youtube.com/watch?v=UAtuHKnSQN0&t=2s
BRAIN:IT. (2026). *YouTube INNOSOC*. Available online: Interview with Ing. Dominika Toman, PhD. about the INNOSOC project: https://www.youtube.com/watch?v=hY6lIE-UNh8

Funded by the European Union NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

BRAIN:IT. (2026). *YouTube INNOSOC*. Available online: Interview about the INNOSOC project with prof. Ing. Milan Kubina, PhD.: https://www.youtube.com/watch?v=x6GnnEZXqHs
BRAIN:IT. (2026). *YouTube INNOSOC*. Available online: About the INNOSOC project with Dominika Toman and Martin Mičiak: https://www.youtube.com/watch?v=fhUuhltTAYY&t=198s

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,
organisational aspects of cooperation during the summer period.
The meeting evaluated the current state of the project following the submission of the interim monitoring report. At that point, the analytical work on the 2nd work packages had been completed, and the analytical studies needed for the 3rd work package 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 among themselves and agreed on the next individual and joint steps. At the same time, a plan of outputs and their promotion was outlined – popularisation posts, professional articles and, in the future, videos and podcasts are being prepared.

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

What is the INNOSOC project and what is its aim?
The INNOSOC project is a response to growing demands in the field of cybersecurity. The modern environment requires advanced SaaS and cloud services that can respond effectively to new threats. And what was the name INNOSOC based on?
Innovative and Security Operation Center – these are the words behind the acronym INNOSOC, and if you are interested in why this particular name was chosen, watch the full video, in which Ing. Michal Papučík, COO of BRAIN:IT, also answers other interesting questions concerning the fundamentals of the project.
What will you learn in the video?
What the INNOSOC project is and why it was created.
What the name INNOSOC stands for.
What the aim 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 successfully the academic and business spheres are being connected.
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. Pavol 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 InfoCom Networks at the Faculty of Management Science and Informatics, UNIZA. Professor Segeč is a key scientific researcher on the project, which focuses on strengthening cybersecurity in organisations and schools through innovative technologies and the education of a new generation of experts.
Does cybersecurity concern everyone?
At the start of the interview, prof. Segeč explains why the security of IT infrastructure is a topical issue even for small organisations:
“For me, cybersecurity is currently a key topic, because we live in an age when everything is interconnected, 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, UNIZA, in the INNOSOC project
The Faculty of Management Science and Informatics (FRI) is one of the main partners of the project and oversees both the scientific research part and the development activities.
“Within the INNOSOC project, we provide our capacities and, at the same time, our private infrastructure as a concept on which pilot deployments of the technologies in the project can be carried out,” says Professor Segeč.
The most common threats and the need for centralised protection
According to statistical data, the most common threats include phishing attacks, ransomware and APT (Advanced Persistent Threat), where an attacker carries out long-term espionage and monitoring in the victim’s network.
Security Operations Center (SOC) as the core of defence
One of the main outputs of the INNOSOC project is the design and construction of a Security Operations Center (SOC) – a central hub that monitors, analyses and responds to cyber 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 the requirements for cyber protection 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. This also applies to aspects connected with the reporting of attacks, and it is precisely the reporting of attacks and their detection that SOCs should help with.”
How SOC systems work
Finally, the professor described how such systems work in practice:
“Technologically, SOCs work on the principle of telemetric collection of large volumes of data, which are 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. Pavol 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 functioning of organisations.

Annex 4 – Article: Student event FRIčkovica – 8 October

On 8 October, the Faculty of Management Science and Informatics hosted its traditional annual event – FRIčkovica, which is a place for informal meetings between students, teachers and partners of the faculty.
During the event, a stand promoting the INNOSOC research project was also prepared for students. While talking with the students, the highlights of the project were presented, for example its purpose, objectives and the problems it addresses. The presentation showed the students the significance 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 Aula AF3A5 lecture room from 8:00 to 10:45.
The current status and results of the research project will be presented during the symposium.

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

On 10 November 2025, the iPad competition organised via the @innosoc_ Instagram profile came to an end. The aim of the competition was to engage young students and spark their interest in the INNOSOC project and the field of cybersecurity.
Following the official draw, the winner of the competition was Timotej Djubašák, who met all the conditions and collected the prize in person.
Congratulations to 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 from 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.
The importance of cybersecurity and the significance of the Security Operation Center and cloud technologies were also presented.

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

On 20 November 2025, the INNOSOC project was presented to students of the Faculty of Applied Informatics at 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 responds to the challenges associated with the transition to a digital economy. Ing. Michal Papučík also spoke about the needs of the commercial sector, 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 it also aimed to actively engage 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 fundamental aim is to protect computers, servers, networks and programs against unauthorised access, misuse or damage, i.e. against

cyber threats and attacks. It is above all the data and information stored on these devices that need protection.
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, or other compromising material, from them. Hackers then trade in this data, information and content, sell it, or use it to blackmail the victims.
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 look after your data, systems, networks and devices regularly and protect them sufficiently against misuse.
In practice, protection concerns mainly the following two basic factors:

The human factor

This area involves observing the basic principles of personal data protection and privacy. In practice, this means being careful about 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 and clicking on various unverified websites.

The technological factor

Hackers often have a head start on you not only thanks to their advanced IT skills, but also because they have modern and sophisticated 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. In the case of technologies, high-quality and regularly updated antivirus software and a firewall play a key protective role.

Why is cybersecurity important?

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

Information at risk

Personal and contact details relating to your identity, such as your first name, surname, birth number and other personal data, as well as your contact details (telephone, e-mail, address, etc.)
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 on work activities and companies can be misused and can cause you various kinds of physical, material, financial and psychological harm.

Basic principles of cybersecurity

A great 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 being 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: Use 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: Regularly backing up 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 contributes significantly to greater awareness of potential threats and risks. Most of these scams rely on your inattention. Conscious attention, caution and fact-checking help in this area too.

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 intrusions 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 them that 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: The manipulation of people in order to obtain confidential information from you.

DDoS attacks: Overloading a server with the aim of disabling a particular service or an entire website.

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

Think about prevention

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

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

What is a Security Operations Center (SOC)?

With the advent of digitalisation, we are increasingly encountering various cyber threats and security risks endangering individuals and organisations. Cybersecurity is a set of measures aimed at protecting digital systems, networks, processes and programs against data theft or other disruption of an organisation'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 specialised centre that performs continuous security monitoring in an organisation and responds to real cyber threats and incidents. A SOC is a centralised unit or team of experts who provide round-the-clock monitoring and evaluation of potential cyber threats in real time.

What is the main role of a SOC?

The fundamental role of a Security Operations Center is to minimise the impact of security incidents and cyber attacks on the organisation and to proactively ensure its cyber 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 organisation's digital and other assets.

What SOC models are used in practice?

In practice, we can find two basic models of Security Operational Center. In the first case, the main functions of the centre are performed by the organisation internally, or rather by a department of the organisation 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 organisations with the following main functions:

Incident monitoring and detection

As part of this function, the SOC provides 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 prevent it from recurring,

investigating the root cause of the incident in order to determine its source and 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 gaining a deeper understanding of the causes of cyber and other security incidents, with the aim of eliminating the same or similar problems in the future. It often works closely with the organisation concerned or forms its internal team.

Concluding recommendations

A Security Operational Center can also provide other security services that the organisation needs. Every organisation should therefore already be addressing the issue of cybersecurity and ensuring the security of sensitive data, processes, information, systems, networks and the devices it uses.
Every organisation should create its own internal policy and procedures covering the data and areas exposed to potential theft or other cyber attack, misuse or security threat. As part of this procedure, we recommend:
setting up monitoring processes,
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 organisation 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, when various technologies are part of their everyday lives and moving around the online space is a normal state of affairs. These 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 are also spreading in the online space. In order to defend themselves effectively against these risks, they should know what threatens them 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 ceased to lurk for young people only outside 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 regular self-education about risks and 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 recognise 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 vast amount of diverse information, which can have a far-reaching negative impact on young people. Young people often cannot yet effectively distinguish what offensive, toxic and dangerous content is, and often do not even 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, and 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, genuinely dangerous.
Communication on social media
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 so on. It is very important that you learn to protect your privacy effectively and teach your children to do the same.
Communicating intimate matters and sending intimate content
Sending messages, photos or other intimate content is a separate chapter within communication. 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 scams
Young people shop online. It is convenient and often cheaper. With greater demand, however, comes the growing appetite of fraudsters, who use increasingly sophisticated methods in their online scams. In these scams, users may lose their personal data, which can be misused, as well as their money, privacy and more.
Other threats include the risk that young people may succumb to gaming and gambling, risks associated with discrimination, various types of bullying, blackmail and abuse, as well as encountering various forms of hate speech.
Another significant risk is the development of addiction to technology, to following social media 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 the 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 difficult to recognise. Learn to recognise it and to apply the options for protection effectively.

Responsibility for what data and content you publish on the internet, social media 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 photos is very popular. However, this activity carries a high risk of potential misuse in various ways. If the pictures and photos show young people's exposed bodies or young people in provocative poses, the threat increases even further. Nude photos of small children should definitely remain part of family albums. This is not content that you should show to anyone else.
Interacting with people you do not know. The internet provides people with anonymity, and you can never know with absolute certainty who we are communicating with. Not communicating with strangers and not following them is perhaps an even more fundamental form of prevention and protection in the online space than in the physical world.

A safe world begins in your own home

Be a role model and talk openly with young people about 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 a fundamental form of prevention against many problems and threats. Build healthy boundaries in children.

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

What is the cloud and what is it used for: Basic types and advantages of cloud storage

The cloud is a term denoting data storage through which users can share, store or otherwise handle large amounts of information and data. In this article, we will explain in simple terms what the cloud is and what it can be used for 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 allows you to store, keep and manage your data, such as various personal or company files, documents, photos and videos. Your data is thus stored on internet-connected cloud servers 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, such as the following:
Web hosting.
File sharing.
Distribution of software and other services.

Storing and keeping files, photos, videos, personal and company records, documents, contracts, employee, business or other operational data, projects and other necessary information.
Cloud computing, which refers to a 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
This is a shared infrastructure operated by an external service provider. In this case, your data is 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, the software and the entire data centre. In this case, the customer, who usually rents the relevant storage space, is merely a user of the service.
Note:
However, the fact that a cloud is public does not mean that anyone has access to the stored data. For example, the customer can stipulate that their infrastructure is accessible only to their family, employees or the company's partners. No one else can access the stored content, data and information.
Private cloud
This is space located in the company's own data centre. In this case, the cloud is operated, managed, administered and maintained by the company itself, in-house. In practice, such a solution is usually somewhat more expensive and requires extra costs for the necessary skilled workforce, hardware and software.
Hybrid cloud
This is a combination of both of the above models. In these cases, some services are operated on publicly available infrastructure at an external provider and some services are stored on the company's private cloud. The company's sensitive data is usually stored on the private cloud, and access to this data or to individual levels is 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, made possible by the rapid 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 a model in which it manages them itself.

Another advantage of cloud services is the ability to store large amounts of data in one place and to allow a larger number of people, or specified individuals and groups, to access and work with it.

In practice, the main disadvantage may be the fact that various sensitive personal and company information, data and documents are stored on someone else's hardware and sometimes in a place you will never get to and may never have heard of. This applies to public or hybrid clouds.
Another growing threat at present is potential cyber attacks, aimed mainly at stealing sensitive data and information in order to misuse them in various ways against individuals and companies.

Conclusion

The cloud is a modern way of storing and processing data over the internet that brings companies and private individuals a range of benefits, such as:
availability of stored and managed data, content and information,
flexibility in working with stored and shared data,
fast access and the possibility of sharing data and collaborating over long distances,
productivity and efficiency of work and of working 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 is likely to grow in the future along with increasing technological demands in various fields.

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 the online environment should understand. They focus on protecting data and information against unauthorised 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 prevent cyber threats and protect sensitive information. In this article, we 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 located primarily in virtual space. In practice, this means data and information stored, for example, on various remote or company servers, computers, data centres, the internet or mobile devices.
The security triad in the field of computer security and data protection consists of three key principles that everyone should know – not only IT professionals but also ordinary users:
Confidentiality
Whenever you process any data and information, you should always observe the principle of confidentiality. This rule states that all data and information we come into

contact with should be provided, shared and disseminated only to designated and authorised persons. All confidential information carries a potential risk of misuse in personal and/or working life, and it is therefore crucial to protect this data and information from those who could misuse it.
Confidential information means any non-public information whose disclosure or provision could harm an individual and/or an organisation.
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 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 its creation to its destruction.
Availability
The availability of consistent data and information means that it is available to authorised persons in complete form and whenever they need it. At the same time, it indicates that this information is protected against misuse by unauthorised 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 a rule, no longer considered secure. All three areas are closely interconnected and support one another.
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 is processed.
Minimisation and accuracy of the data processed.
Limitation of the archiving period of the data processed.
Restrictions on the provision and dissemination of the data processed.
Principles, rights and obligations in accordance with the applicable Slovak and European legislation on 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 aim of this principle is to ensure that data and information are available only to authorised persons. Confidentiality is a key aspect particularly 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 fundamental purpose of the integrity principle is to ensure that data remains complete, accurate and unaltered throughout its 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 fundamental aim of this protective principle is to ensure that authorised persons always have the data they need available to them.
You can ensure the security of data and information by:
Regularly checking and backing up 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 foundation of every security policy. Every IT measure designed to protect data and information should therefore incorporate all three of the above security principles, and these principles should be set in balance with one another. 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 has been 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 field of cybersecurity. It is a response to today’s – let me call them – demands in the field of cybersecurity, namely modern and secure services, SaaS cloud services, and bringing sufficient knowledge or experts in the field 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 Center, so we decided that INNO stands for innovativeness and SOC for Security Operation Center, so put together and abbreviated, INNOSOC. The main aim of the INNOSOC project, as a research project in the field 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 in the form of a service, as their own service, or else in the form of an on-premise solution built on some kind of containerisation and a simpler set-up on their own premises, in their system.

The project responds mainly 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, our biggest shortcomings are that these security systems are very costly, and the second very problematic factor is that we have few experts who could operate these systems or work in some way in the field of cybersecurity. Our solution will actually ensure that organisations that do not have the funds for those expensive solutions will be able to afford or secure it, and at the same time, thanks to artificial intelligence or some kind of machine learning, we can, so to speak, relieve those costs or the need for those experts, and not so many of them will be needed.

For me, the most fundamental benefit of what we will deliver from this project is that we will bring a design or some kind of solution, an open-source solution, for entities that will be able either to start using it as a SaaS service or to get it running on their own premises, on-premise. But for me, the other goals are mainly extensive cooperation with the university sphere. That is the connection of – let me call them – companies and universities, and thus creating a functional team that can turn ideas and interesting suggestions into a finished solution. And at the same time, from my point of view as well as for the university, it is certainly an increase in the competence of the people participating in the project, because everyone learns something new and moves forward in the field of cybersecurity.

What I enjoy most about this project are the joint meetings, or I would rather call them brainstorming sessions, where we all reach agreement together. They are not always entirely the most pleasant and nicest, but we always discuss what the important factors are and how we can achieve them, and we look for shared ideas and consensus. Perhaps this synergy between these two teams – the one from the university, from the research environment, and ours from the corporate side or, let me call it, the side that deals with the practical aspect 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 genuinely going into something new that we are trying to bring together from both of these worlds.

On the INNOSOC project, we have really encountered a great many technologies. If I leave aside the security and cybersecurity technologies, such as hardware and software in the field of security, we very often encountered, for example, ordinary hardware and software, hardware in the infrastructure, network elements 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 tried out many different databases, for example, or presentation layers, programs that represent logs, records and anomalies. And at the same time we also had quite a bit of fun, so to speak, with artificial intelligence models or machine learning, 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 – in this case the university – and turn

it into a product or project, or take it further and produce a design that is usable in practice. So those are our strengths. That is why we decided that our work packages would be mainly the configuration and installation of these sub-modules or modules. At the same time, there was the design of the architecture and its creation, and thirdly we took charge of, or we are the guarantors of, the awareness-raising or marketing activities – getting awareness of this project, of cybersecurity and of the related areas out among people.
Of course, I must also point out that we collaborated on everything together. That was also the idea when we went into this project; there was a clear vision and agreement that we would definitely work together on every work package. If only 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 opinion, connecting the academic and business spheres is entirely advantageous precisely through projects like this, which are research projects combined with something that already extends into the creation of a product. Thanks to this, for example, we have created a partnership that already extends far beyond the boundaries of the project; we are already cooperating on other projects. Even after it ends, we will certainly cooperate in completely different areas than just cybersecurity. And already now, for example, we have jointly written another project that 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.
We use a number of international standards on the INNOSOC project. The very first I will mention is PRINCE2, which is a project management methodology that we follow, because at the Faculty of Management Science and Informatics it is an established process or framework. Likewise, at our company BRAIN:IT we use it for all projects, and it helps us a great deal in delivering these projects. At the same time, we use ITIL V for setting certain service parameters and service offerings, and in the area of managing these services that we plan to build in the future.
As far as the architecture is concerned, we said that we would use an architectural framework defined by TOGAF. Most often, as regards graphical representation, we use ArchiMate 1 or UML version 2. Sometimes also BPML, but this is not set entirely strictly; 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 actually information security, directly related to this. We also comply with 9001, 22 301 and many others, as well as 20 000 on service management."

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

My name is Pavel Segeč. I work as Head of the Department of InfoCom Networks at the Faculty of Management Science and Informatics. In the INNOSOC project, I am a key project implementer. Cybersecurity is currently a key topic for me, because we live in an age when everything is interconnected and we are part of an online community.

Networks are becoming digital motorways 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 fundamental 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, safe behaviour should be a basic principle 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 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 being developed and tested in the project can be carried out.

If we back it up with statistical data, the most common threats today include various phishing campaigns. Of course, a very popular topic is ransomware and cryptoware, which is currently very active. In addition, however, I consider so-called APTs (Advanced Persistent Threats) to be a very important topic. These are advanced attacks in which attackers are positioned in the victim's network over the long term and carry out espionage and monitoring. This often lasts hundreds of days, during which the company has no idea that there is an attacker in its network.

A Security Operations Center (SOC) is not just a single 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 today is to help detect and, above all, respond to detected attacks or attackers present in the network.

The SOC topic is also important because the amendment and tightening of the cybersecurity act and its implementing decree, which is already available, is expanding the number of companies that must actively behave in a secure manner and protect themselves against various types of threats, and must report the threats that have been detected. The main goal 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 and detecting attacks, which is in fact the topic we are addressing in the INNOSOC project.

Technologically, SOCs operate on the principle of telemetric collection of large volumes of data. This data is then stored in databases and enriched with various

supplementary data in order to make it easier to detect and uncover anomalous behaviour. However, we are still talking about enormous volumes of collected data, and therefore one of the current trends being implemented in SOCs is the support of artificial intelligence and machine learning. The introduction of these machine learning methods into SOC solutions is precisely one of the aspects we are addressing in cooperation with BRAIN:IT as part of our development in the INNOSOC project.

Annex 17 – Article on the interview with the experts Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD.

As part of the work on the INNOSOC research project, an interview was conducted with its key experts – Dominika Toman and Martin Mičiak from the Faculty of Management Science and Informatics of the University of Žilina (FRI UNIZA).
The interview offers a deeper insight into how academic research is linked with real-world practice in the field of cybersecurity.
What is the goal of the INNOSOC project?
The project focuses on linking research and innovation in the field of Security Operations Centers (SOC). Its main aims are:
To create technological solutions and designs for organisations that want to secure their cybersecurity.
To provide an alternative to expensive commercial solutions by using and integrating suitable open-source components.
To deliver usable outputs for public administration, businesses and the professional community.
The role of management in research
Although the topic of the project is decidedly technical, Dominika Toman and Martin Mičiak represent the Department of Management Theories. Their role lies primarily in the management and coordination of the entire project.
In the interview, they emphasised that the project is an excellent opportunity for them to apply knowledge of project management directly in practice. They subsequently transfer their experience of managing technical experts and cooperating with a business partner (BRAIN:IT) into their teaching and lectures for their students.
Challenges and risk management
Working on such a complex project brings a number of challenges, which were the subject of the discussion:
Partner coordination: Aligning the academic environment with the business sphere and resolving communication noise.
Timetable: One challenge, for example, was aligning compulsory leave at the university with the planned meetings of the project team.
Scientific activity: Preparing indexed scientific outputs and publications is a lengthy process that requires planning well in advance because of peer-review procedures.
Benefits for practice and the professional community
According to the experts, the most significant output of the project is the so-called “proof of concept” – verification that the proposed architecture built on open-source tools is genuinely applicable and sustainable.

For small businesses and public administration organisations, this means the possibility of increasing their protection against cyber threats even without the need for huge financial investments in licences or building their own expertise “from scratch”.

The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements.”
Project code – 09I05-03-V02-00010.

Annex 18 – Article on the interview about the INNOSOC project: Cybersecurity and broadening horizons with Dominika Toman

We bring you a behind-the-scenes look at the INNOSOC project through an interview with Ing. Dominika Toman, PhD., Assistant Professor at the Department of Management Theories of the Faculty of Management Science and Informatics of the University of Žilina. In the project, she plays a key role in supporting project management and coordinating people.

The importance of the project for the public and professional practice

According to Dominika Toman, the main benefit of the project for both the general public and the professional community is above all the broadening of horizons in the field of cybersecurity. The project focuses on passing on basic information about solutions that can help in this important sphere.

For professional practice, the following activities are particularly key:

Intensive publication activity and presentation of information at professional conferences.

Preparing literature reviews on the most suitable solutions for supporting cybersecurity.

Preparing materials for employee training that will help organisations operate new security solutions effectively.

Personal development and cooperation

Participation in the project has also brought valuable experience to the project implementers themselves. Dominika Toman highlighted that, thanks to INNOSOC, she has acquired a great deal of new information and significantly improved her skills in management and coordination.

The project also creates space for intensive communication with partners, not only within academia but also directly with practitioners, which contributes to the creation of high-quality and usable outputs.

The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements.”

Project code – 09I05-03-V02-00010.

Annex 19 – Article on the interview about the INNOSOC project: On scientific research and cybersecurity with Martin Mičiak

We continue our series of interviews about the INNOSOC project, this time with Ing. Martin Mičiak, PhD., from the Department of Management Theories of the Faculty of Management Science and Informatics of the University of Žilina. In the project, he works as a researcher and is also part of the project management support team.

Cybersecurity and the importance of high-quality science

The main topic of the INNOSOC project is cybersecurity and finding ways to strengthen it in organisations. Martin Mičiak emphasises that the project focuses mainly on open-source solutions, which make it possible to increase protection even at lower overall costs.

In his view, the quality of the scientific outputs is key to the success of the project:

Publishing with renowned publishers and in indexed journals or databases.

Increasing the relevance of and awareness about the project in the eyes of the professional community and the general public.

Emphasis on the practical applicability of the results.

The challenge of the “research gap”

In the interview, Martin Mičiak also described the demanding nature of scientific work. He considers the research itself to be the most difficult part – the ability to map the given field correctly and identify the so-called research gap. The aim is for every conference paper or article to bring something new and interesting that moves the topic of cybersecurity forward.

Linking management, informatics and business

The INNOSOC project is unique in its combination of the academic and business environments. At the faculty, it involves an important cooperation between two departments:

the Department of Management Theories

the Department of InfoCom Networks

This cooperation has enabled Martin Mičiak to link the fields of management and informatics more deeply, broaden his horizons in cybersecurity and gain further valuable practical experience in project management

The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements.”

Project code – 09I05-03-V02-00010.

Annex 20 – Article about prof. Ing. Milan Kubina, PhD. on the INNOSOC project

As part of a professional dialogue, prof. Ing. Milan Kubina, PhD., presented to us the strategic direction of the INNOSOC project, which primarily responds to the growing risks of the exploitation of system vulnerabilities in the digital environment.
The project focuses on the development of innovative tools for SOC (Security Operations Center) and IP network management, with particular emphasis on increasing the cyber resilience of entities with limited budgets, such as small companies, public administration bodies and schools.

In the interview, the expert revealed what stage the development is at, as well as why the synergy between the academic sphere and applied practice carried out with BRAIN:IT is so important.

The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements.”

Project code – 09I05-03-V02-00010.

Annex 21 – Popularisation article on the topic Linking AI and cybersecurity in practice

Cyber attacks are becoming increasingly frequent and, at the same time, more sophisticated. Although artificial intelligence can significantly streamline many processes, experts warn that it should not function as the sole solution in protection against cyber threats. The combination of and cooperation between AI and humans can bring greater balance to practice and make the most of the strengths of both of these players. In this article, we take a closer look at the link between artificial intelligence (AI) and the human factor in the field of cybersecurity.

The use of AI in the detection and prevention of cyber attacks

The use of AI in various fields can bring increased efficiency, productivity and savings of time and money. Artificial intelligence can excellently take over many work tasks that are strenuous and exhausting for humans, and in addition it is able to perform these tasks continuously and without the need for rest.

In many situations, AI can thus eliminate the risk of human error, which is often the result of fatigue and inattention. In the same breath, however, it must be added that even artificial intelligence is not infallible and may present falsehoods as facts and correct information. Such situations can arise, for example, with a poorly configured algorithm or if the AI was trained on incorrect data.

The role of AI in cybersecurity

Real-time detection of cyber threats

Traditional systems often respond only once attackers have penetrated the network or system. AI, however, can analyse the behaviour of users and devices in real time, recognise unusual patterns of behaviour and thus immediately flag risky activities.

Prediction of cyber attacks

Thanks to the large volume of data from which AI draws its knowledge, it can effectively recognise in real time patterns that preceded attacks in the past, or identify unusual patterns of behaviour and uncover these anomalies.

Automated responses

AI can automatically isolate infected devices, block communication with suspicious servers or launch incident response procedures even before a human intervenes.

The result is a faster response, timely detection of a real cyber attack and thus also the minimisation of any damage.

AI as a double-edged sword

Although AI is a powerful and effective cybersecurity tool, it also has its limits. It can also become a powerful weapon in the hands of attackers.

How do cyber attackers use AI?

Automated attacks: AI can be used for automated protection, but also for generating automated phishing e-mails and conducting other attacks on a large scale.

Deepfakes and next-generation social engineering: A major threat today is the phenomenon of so-called deepfake audio and video, which enable a kind of psychological manipulation of people that until recently we knew only from the boldest science-fiction films. Falsified identities, photographs, accounts or various sensitive personal and business information are often indistinguishable for a layperson without special technologies and can devastate people's lives and careers.

Misuse of generative models: Generative AI can also be used to create malicious code, automate malicious campaigns or circumvent detection mechanisms.

Linking AI with cybersecurity therefore lies in balanced cooperation between artificial intelligence and the human factor.

Advantages and risks of AI in the field of cybersecurity

If you use artificial intelligence in the field of cybersecurity, its greatest advantage is the ability to work with huge volumes of data in real time. AI helps to assess risks more quickly, supports the decision-making of security teams and facilitates strategic planning where manual analysis would fail.

At the same time, however, AI systems must remain under control. To minimise errors, it is necessary to understand how and why AI responds in a certain way. Transparency, auditability of decisions and regular review of outputs are important, especially in environments involving sensitive data. Equally essential is the ongoing training and updating of AI models so that they work with current and verified data.

Artificial intelligence is not meant to replace the work of security analysts, but to strengthen it. You will achieve the best results when technologies support human judgement. With the growing use of AI, there naturally also comes the need to address ethical questions, the responsible set-up of processes and clear rules for protection against the misuse of data.

The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements.” Project code – 09I05-03-V02-00010.

Annex 22 – Popularisation article on the topic Cyber attacks: How they are changing and why they pose an ever-greater risk

Today, cyber attacks are no longer just the work of technically skilled lone individuals. Behind increasingly sophisticated cyber threats stand complex organised groups and professional hackers who use state-of-the-art technologies, various automation tools, techniques and artificial intelligence. Discover the main reasons why cyber attacks are becoming increasingly sophisticated.

The main reasons for more sophisticated cyber attacks

Today, cyber attacks are not only an increasingly frequent phenomenon that spares neither individuals, companies nor various business or state organisations, but they are also increasingly sophisticated. Wherever sensitive data exists, there is a potential risk of its misuse. Much data today is also located in the online space, which is therefore increasingly becoming a target of interest for professionals trying to gain access to this data and misuse it.

Internet threats are thus, in a way, a natural consequence of our technological development. The main reasons why cyber attacks are becoming increasingly dangerous include:

Organised groups and organised cooperation

One of the main reasons is the organised nature of cyber attacks. Attacks are carried out by experienced professional hackers who are well organised, equipped with state-of-the-art technologies and possess the latest technical and IT knowledge.

Advanced techniques and trends

Many hackers and organised groups of cyber attackers exploit advanced methods, techniques and trends that extend not only into the field of information technology but also into social engineering. In doing so, attackers exploit weaknesses of the human psyche and various manipulative techniques.

Activity in the online space

As already indicated above, one of the reasons for the spread of cyber attacks is also the fact that we spend a lot of time in the online space, which widens the range of potential targets of cyber attacks.

The use of artificial intelligence (AI)

Artificial intelligence is significantly changing the way cyber attacks are created. Attackers are increasingly using it to automate attacks, create convincing phishing e-mails or falsify digital content, accounts and identities. Thanks to AI, these attacks are faster, more targeted and harder for ordinary users to recognise.

That is precisely why it is important for both individuals and companies to keep pace with this development. The foundation is ongoing education in the field of cybersecurity and the consistent application of protective measures that help prevent data misuse and security incidents.

The impacts of cyber attacks on practical life

In practice, the impacts of increasingly frequent and sophisticated cyber attacks on ordinary people, companies and other organisations can be divided into three basic groups:

Organisations and individuals face a constantly growing number of attempts to intrude into their private lives and working environments with the aim of misusing their data.

In response to these situations, there is an urgent need to address the protection of sensitive data comprehensively and in real time. It is becoming apparent that existing protective mechanisms are quickly becoming obsolete and that it is necessary to respond to new threats promptly.

The logical consequence of both of the preceding factors is increased spending by individuals and companies on security and protection against cyber threats, which are increasingly frequent and sophisticated.

In practice, it often turns out that outdated antivirus software or basic security measures are no longer sufficient against today's threats. Attackers can bypass such protections and gain access to sensitive data. The consequence is often the misuse of personal or company data for unauthorised financial transactions, administrative complications and dealing with the consequences, which may even lead to communication with the authorities or the police. In addition to financial losses, it often also involves a loss of trust and disruption to the normal functioning of individuals or companies.

Protection against cyber attacks

Today, protection against cyber attacks is not a one-off decision but a long-term approach. It is not enough to have an antivirus switched on or to use a strong password. It is important to understand where your data is located, who has access to it and how it is protected.

In practice, this means regularly asking yourself simple but essential questions:

Where is my personal or company data stored?

To whom do I provide it and for what reason?

To what extent do I share it and is it really necessary?

Ongoing oversight of systems and data also plays a significant role. Continuous monitoring makes it possible to detect suspicious behaviour in time and to respond before real problems arise. For companies and individuals alike, it thus represents a practical way of minimising financial losses, administrative complications and the erosion of trust.

Ultimately, it is precisely the combination of technical solutions and conscious handling of data that helps to cope with increasingly sophisticated cyber threats without unnecessary risk.

The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements.” Project code – 09I05-03-V02-00010.

Annex 23 – Popularisation article on the topic Automation and deep machine learning in cybersecurity

Automation in cybersecurity is a response to the growing volume of security events, which can no longer be analysed effectively by hand. Organisations are therefore increasingly using automation and deep machine learning (deep learning), which enable real-time threat detection and rapid response to incidents. In this article, we explain how automatic threat detection works, what its limitations are and why human intervention remains irreplaceable even with advanced technologies.

Why is automation in cybersecurity essential?

Automation in cybersecurity is essential mainly because the volume of threats and security data is constantly growing. Performing manual checks would be inefficient and very difficult to manage.

In addition, automatic detection of cyber attacks is also important for a number of other reasons:

more complex and more cunning cyber attacks,

the limits of manual real-time monitoring,

a lower number of false alarms,

more efficient use of human resources.

Deep machine learning in the security context

Deep machine learning (deep learning) is an advanced form of machine learning. In the field of cybersecurity, it is used for automatic threat detection and analysis of the behaviour of systems, devices and users. Thanks to the use of multi-layer neural networks, it can process even large volumes of data and identify patterns typical of cyber attacks, phishing or malware.

The difference between machine learning and deep learning

Machine learning works with predefined features that a human prepares for the model. Deep machine learning, on the other hand, can derive these features by itself, automatically and directly from the data.

Simply put, deep learning can handle more complex and less obvious patterns of behaviour. This property is extremely important in cybersecurity, especially in detecting new or unknown types of attacks.

How do models learn to recognise security threats?

Deep machine learning models are trained on large amounts of historical security data containing both normal and malicious behaviour. During training, the neural networks learn to distinguish between normal activity and anomalies that may represent a cyber attack.

The advantages of automation and deep learning in detecting cyber attacks

One of the main advantages of AI in cybersecurity is the ability to detect various types of attacks in time. In practice, these technologies work in three basic ways:

1. Real-time anomaly detection

This is one of the most important benefits of security automation. Models using deep learning know the normal behaviour of applications or networks, which enables them to detect even the smallest anomalies relatively easily. They do so in real time, thereby minimising the impact of attacks and ensuring smooth operation.

2. Analysis of user and device behaviour

This analysis has several functions. It is used primarily to monitor:

login patterns,

work with files,

movement within the network,

communication between devices.

If deviations appear in these areas that may indicate the presence of malware, the system immediately starts dealing with them. Such an approach is common in many areas, including SIEM (Security Information and Event Management) or EDR (Endpoint Detection and Response) solutions.

3. Prediction of security incidents

Predictive security analysis also plays an important role. Its aim is to estimate the probability of future incidents on the basis of historical data. The systems evaluate trends, recurring patterns and weak points in the infrastructure, which enables them to identify risks even before the attack itself occurs.

Automated incident response (SOAR) in practice

SOAR is a significant part of modern cybersecurity that shortens the time between the detection of a threat and the intervention itself. In combination with security automation, machine learning and SOAR-type tools, it is possible to respond to attacks almost immediately. In practice, this significantly reduces the extent of damage and limits the spread of an attack within the infrastructure.

Device isolation and access restriction – if the system assesses an endpoint as risky on the basis of behavioural analysis, it can automatically restrict its access to the network or disconnect it completely.

Automated security playbooks – these define specific procedures for responding to different types of incidents. When a threat arises, the system automatically launches a preset procedure.

The limits of automation and the risks of deep learning in security

Although security automation has many advantages, it also brings certain limits and risks. These include, for example, incorrect assessment of a situation and the occurrence of false alarms, as well as dependence on the quality of training data. If the data is incomplete or biased, models may learn incorrect patterns of behaviour.

Automation does not replace humans, but changes their role

Although artificial intelligence can automatically detect threats and respond to incidents, it still cannot fully understand context and lacks strategic thinking as well as a sense of responsibility. Automation therefore takes over mainly routine and time-consuming tasks, but at present it cannot fully replace security analysts. They are indispensable in interpreting results, investigating more complex incidents and setting security strategy.

The future of automation in cybersecurity

In the coming years, we can expect greater accuracy and closer cooperation between technologies and humans. Thanks to automation, threat detection should be faster and more accurate, which will lead to higher efficiency and productivity of work. A lower number of false alarms and a greater emphasis on data quality should also be a matter of course.

A significant shift will mean that we will be able to rely on artificial intelligence even more. Nevertheless, it will not act as a complete replacement for the human factor, which will remain indispensable in the coming years as well.

The article is an output of the project “Multi-tenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Elements.” Project code – 09I05-03-V02-00010.

Annex 24 – Interview with Ing. Dominika Toman, PhD. and Ing. Martin Mičiak, PhD.

The INNOSOC project links research, practice and innovation in the field of cybersecurity and Security Operation Centers. Its aim is to bring new knowledge and usable outputs for public administration, businesses and the professional community. Today we will be talking about the project with Dominika Toman and Martin Mičiak, who are among the key experts involved in the research on behalf of the project partner, the Faculty of Management Science and Informatics of the University of Žilina.

How would you describe the project to someone hearing about it for the first time?

The project focuses on creating a technological solution or design for organisations that would like to ensure their security in the course of their operations. What sets it apart is that it is also aimed at organisations that cannot afford expensive commercial solutions, and therefore a combination of suitable components from the open-source environment was sought. This brings a unique integration of the parts of the solution, and it was also interesting for us because of the combination of the academic environment with a business partner – BRAIN:IT. It shows the public that truly close cooperation between universities and businesses is possible.

What are your roles and activities in the project?

Two departments from our faculty are involved: the Department of InfoCom Networks and us – the Department of Management Theories. We are responsible for management and coordination, so less of the technical side and more of the managerial side. For us, it is an opportunity to apply knowledge from the field of project management, which I also teach. We were able to apply it to the coordination of technical experts and also to communication between the academic environment and the business partner. We were involved right from the start, in preparing the documentation before the project was approved, so as to set up its potential in such a way that it would deliver the declared effect. We are looking for links there, for example for final theses or project-based teaching of students.

Do students already have topics linked to the project?

Yes, they are being worked on all the time, and it is also a topic close to the heart of our head of department, Professor Kubina. Organisations are really interested in learning more about strengthening cybersecurity; they see it as a key priority.

Why is the project needed for public administration or businesses?

Businesses are provided with a specific solution that they have ready-made, so they do not have to start from scratch when thinking about security. The project will provide them with a design of how it would ideally be done with available non-commercial solutions, so the financial burden is not high either. Small businesses often have neither the in-house expertise nor the people. The project provides a broad overview of components, and companies do not have to test for themselves

whether the software is compatible. The human factor still matters – employees can be both a risk and an advantage, and the project outputs offer applicable solutions at lower cost precisely for those organisations that would otherwise be unable to afford the support around large solutions.

What risks affected the project?

In supporting project management, we dealt with identifying and managing risks in order to minimise negative impacts. One of the risks was ineffective communication between several partners. For example, aligning the timetable – at the university there is compulsory leave in the summer, and suddenly only three out of 20 people turned up to a scheduled meeting. People's capacities also differ depending on whether it is term time or not. We had to monitor the sequencing of outputs in the work packages so that no one held up other team members.

What was the most demanding part of preparing the scientific outputs?

The formal requirements are clearly defined, so there was no problem there. The most critical part is the research itself. Unless we have data and findings, we cannot produce publications for renowned journals. We had to plan well in advance where the research would be published (conferences, journals), because the peer-review process cannot be accelerated. We cannot rely on catching up on the outputs at the end of the project; we had to work on them in parallel and also have a fallback plan (backup) in case one of the outputs did not work out.

What has the project given you personally or as people?

On the technical side, we had to find our way around specific terms and tools; sometimes we quickly looked up key words on our phones so that we understood the topic. On the human side, it was the coordination with several partners; it was our first large project in which we cooperated on a daily basis with a partner from industry. It also strengthened relationships and respect for the expertise of colleagues from another department, because the IT field changes dynamically.

Did anything about the project surprise you?

We were surprised by the administrative background of the large Gantt charts and the requirements for reporting and ongoing monitoring on the part of the agencies. However, we were pleasantly surprised by the willingness and strength of the people, who pulled together under time pressure and were able to deliver the outputs. They showed great flexibility and initiative.

What would you do differently in the future?

Right at the start, we would set up a system of regular reporting. We would align internal progress tracking even better with the agency's official deadlines, so that we would not have to prepare documentation twice or update it in a hurry.

Which output of INNOSOC do you consider the most important?

The most important is the design itself and its testing – the proof of concept. The fact that it can really be applied in practice with the proposed architecture and is not just a solution ‘for the drawer’, but something sustainable for real clients and organisations.”

Annex 25 – Interview with Ing. Martin Mičiak, PhD.

My name is Martin Mičiak, I am from the Department of Management Theories at the Faculty of Management Science and Informatics, I am an assistant professor, and within the INNOSOC project I was both a researcher and part of the project management support. The topic of the INNOSOC project is the field of cybersecurity and the possibilities of strengthening this security in organisations even at lower overall costs on the basis of open solutions. In every project, it is important for its scientific outputs to be published with renowned publishers and in indexed journals or conferences in important databases, because this lends importance and relevance to the overall outputs and to the project as a whole, and as a result its further dissemination and, in fact, awareness of it in the professional community and in the eyes of the public will also be strengthened. In preparing each research output that is later to be published, the most demanding part is the research itself; it is necessary to come up with an idea and actually map the field so that each further output extends it and responds to, in fact, the research gap, which is what articles and conferences refer to by the phrase research gap. It is always necessary to tailor the next output so that it really contributes to the given topic that the article or conference paper examines or addresses in detail, so that it brings something new and is therefore interesting, and the community, and also the wider public and practitioners, are actually interested in opening and reading such an output. The INNOSOC project is an interesting combination of the academic and business environments, and within the faculty two departments are involved in it: our Department of Management Theories and the Department of InfoCom Networks. So overall it is a very important and interesting cooperation, which has helped me to deepen the link between the managerial and IT fields even further. It has also broadened my overall awareness of the important topic of cybersecurity and helped me to gain further practical experience in the field of project management support."

Annex 26 – Interview with Ing. Dominika Toman, PhD.

My name is Dominika Toman, I am an assistant professor at the Department of Management Theories at the Faculty of Management Science and Informatics, and within the INNOSOC project I am responsible, for example, for project management support and the coordination of people in this project. I would describe the importance of the project from the perspective of the public, whether professional or general, as broadening horizons in the field of cybersecurity, passing on basic information relating to these solutions and how to help in this area.
As far as professional practice is concerned, it involves publication activity, publishing information on cybersecurity, in other words deepening that information and knowledge. Within the project, many articles were gradually published – not only articles, but also information presented at conferences. These were either partial outputs relating to a literature review of the most suitable solutions for supporting cybersecurity, or results were gradually published concerning, for example, suitable training for employees of organisations that will be improving their cybersecurity, so that they are able to operate these solutions.

Within the INNOSOC project, I learnt a great deal of new information; I have essentially improved my skills in management and coordination and was able to develop them while creating the individual outputs and in communication with partners, whether from the university or from practice."

Annex 27 – Interview with prof. Ing. Milan Kubina, PhD.

I am Professor Kubina, I work at the Faculty of Management Science and Informatics, I am Head of the Department of Management Theories, and within INNOSOC I am a co-implementer of the project, but I am also the principal investigator, so there are two of us who are key implementers, if I may put it that way, Professor Segeč and I, plus the key implementers from our partners, such as BRAIN:IT. I am more or less responsible for communication between the teams, between the partners and, above all, with the research agency.
The main idea of the INNOSOC project was that we live in such a digital age, everyone uses these technologies, and lots of people are looking for ways to exploit some system errors or problems and inconsistencies, generally speaking, in these applications, and to break into systems and enrich themselves. So this INNOSOC was intended mainly for small companies and public administration, that is municipalities and schools, since they do not have the money, so that we could help them a little so that they feel safer in cyberspace.
It is an SOC centre, or rather a set of tools that should address the issues of cybersecurity and the operation of IP networks. In the end, it should be a cloud service; this project is at TRL3, and we are trying to design this product so that it is cloud-based and multi-tenant and so that the requirements are met for the solution not to be financially demanding for future quasi-customers.
As a kind of middle manager, since I am head of department, I see that cooperation between the university sphere and practice is very important, and I try to motivate my colleagues to connect with practice as much as possible, whether through master's or bachelor's theses or through invited lectures. I am very glad that companies such as BRAIN:IT are keen to cooperate with the Faculty of Management Science and Informatics and support both the faculty and the students, and I think the synergy is very good on both sides."